Microsoft.AZ-500J.v2026-10-01.q208

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：	208
バージョン：	v2026-10-01
ページの閲覧量：	102
問題集の閲覧量：	2147

https://www.jpnshiken.com/shiken/Microsoft.AZ-500J.v2026-10-01.q208.html

質問: **1**
あなたは、新しいレビューのコレクションに割り当てることを計画しているアクセスレビューの構成を任されています。また、リソース所有者がレビューをレビューできることを確認する必要があります。
まず、アクセスレビュープログラムとアクセスレビューコントロールを作成します。
次に、レビュー担当者を構成する必要があります。
レビュアーを設定する必要があるのは次のうちどれですか？
A. 選択したユーザー。
B. メンバー（自己）
C. グループオーナー。
D. 誰でも。
正解: (正解を表示します)
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.
Graphical user interface, application Description automatically generated with medium confidence



Reference:
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: **2**
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。
WebApp1を保護するには、WAF1を使用する必要があります。

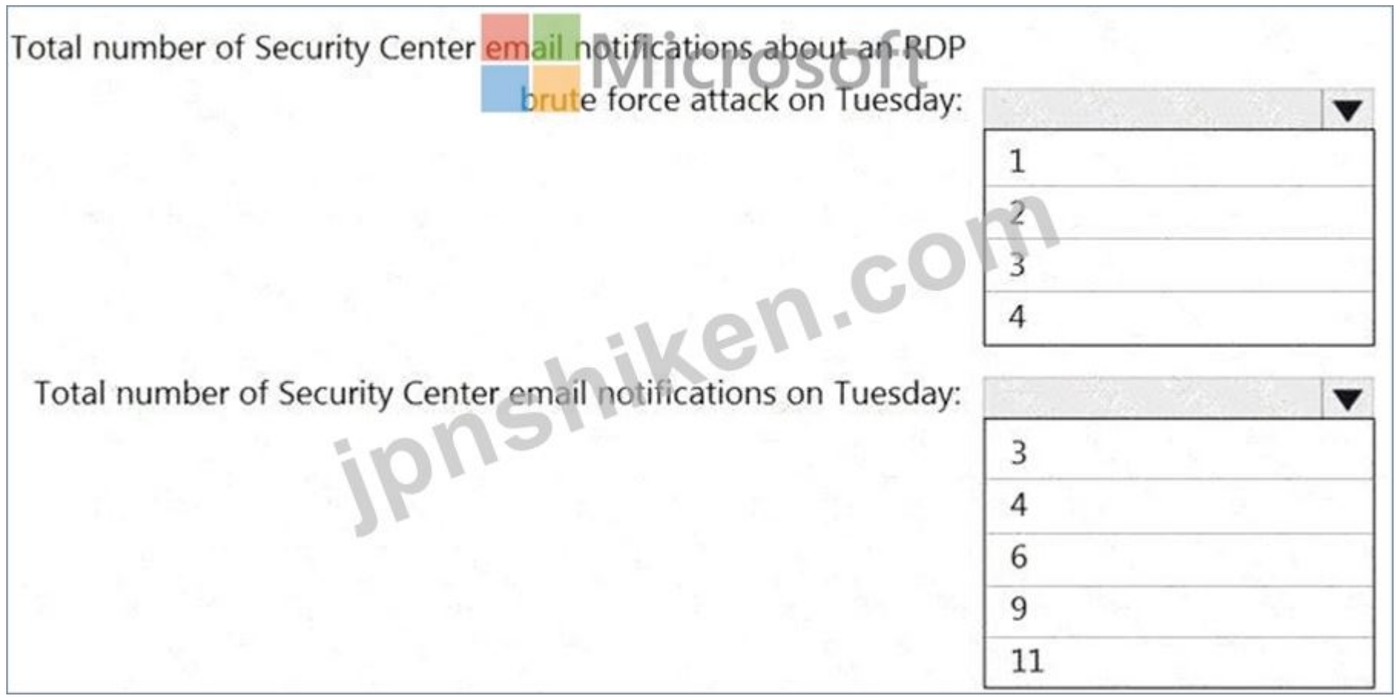
まず最初に何をすべきでしょうか？
A. Azure Front Door をデプロイします。
B. Azure Firewallをデプロイします。
C. WebApp1に拡張機能を追加します。
正解: **(**正解を表示します**)**

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: **4**
月曜日に、Azure Security Center で電子メール通知を構成して、ユーザー user1@contoso.com に通知します。
火曜日に、Security Center は次の表に示すセキュリティ アラートを生成します。

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

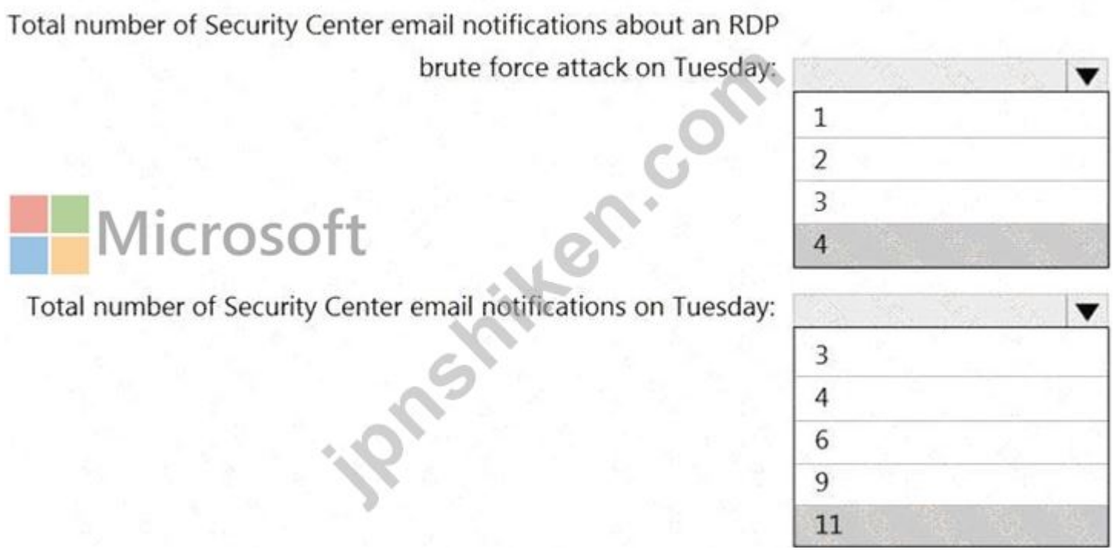
火曜日に user1@contoso.com はいくつのメール通知を受信しますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

質問: 5

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

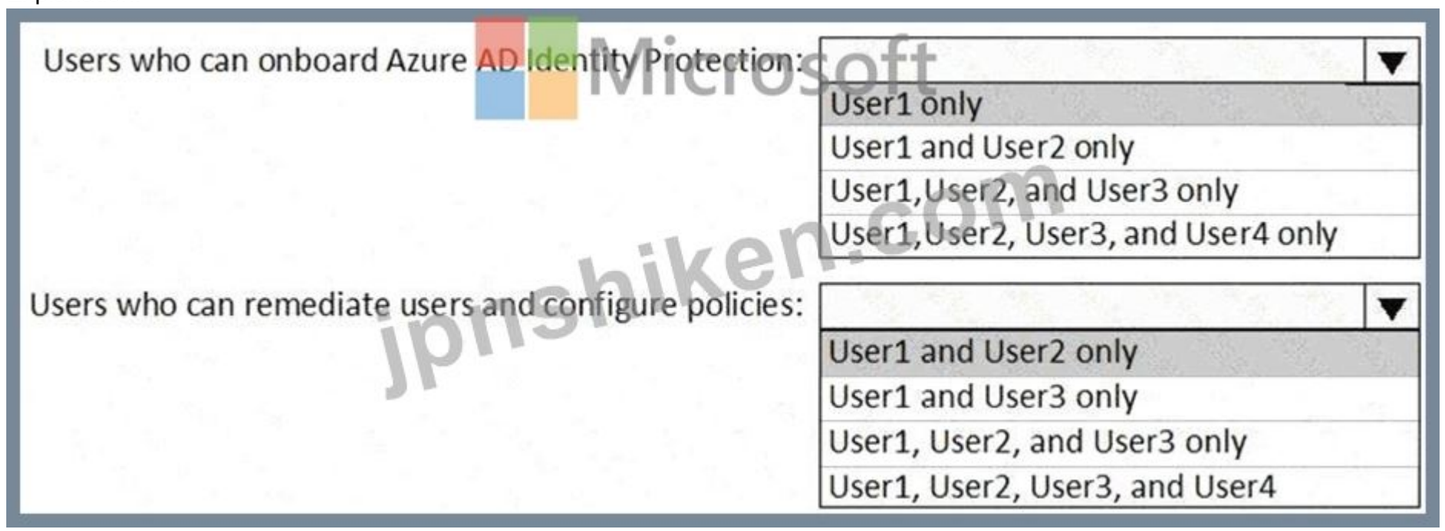


正解:

Answer Area



Explanation:



質問: 6

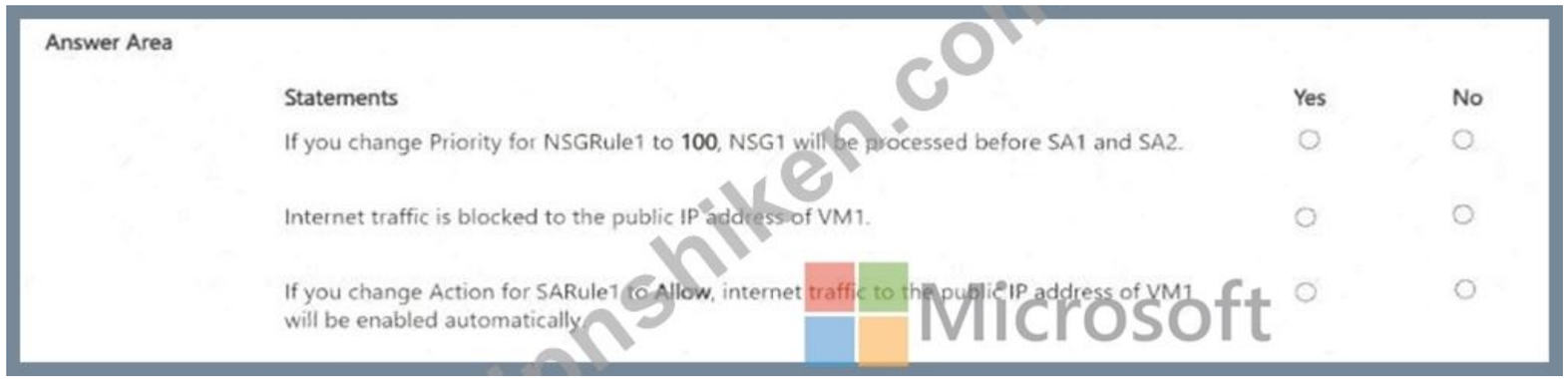
Sub1 という名前の Azure サブスクリプションが含まれる MG1 という名前の管理グループがあります。

Sub1 には、次の表に示すリソースが含まれています。

Name	Description
VM1	A virtual machine that has a public IP address.
VNet1	A virtual network that contains a subnet named Subnet1.
NSG1	A network security group (NSG) that is associated to Subnet1 and has a custom inbound security rule named NSGRule1 with the following settings: • Source: Any • Source port ranges: * • Destination: Any • Destination port ranges: * • Action: Allow • Priority: 500

次の構成を持つ AVNM1 という名前の Azure Virtual Network Manager インスタンスを作成します。

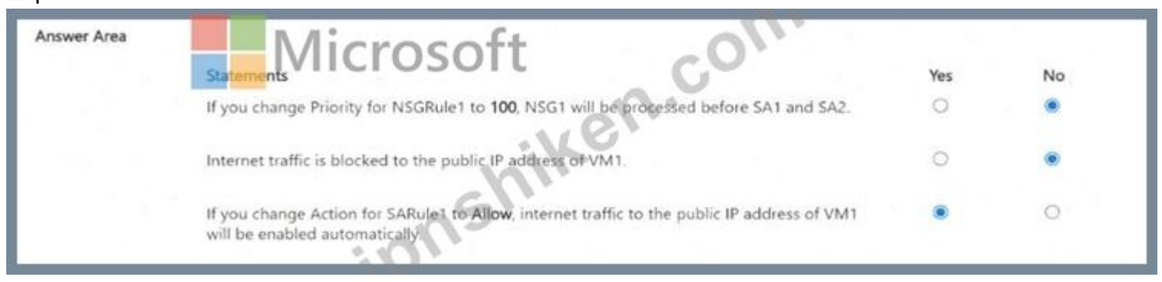
* 管理範囲 :MG1
* ネットワークグループ:
o 名前: グループ1
グループメンバー: VNet1
* セキュリティ管理者の構成:
o 名前: SAT
o ルールコレクション:
名前: SACollection1
対象ネットワークグループ: グループ1
セキュリティ管理ルール:
名前: SARule1
優先度: 500
アクション: 拒否
方向: 着信
ソースタイプ: 任意
送信元ポート *
SA1 はすべての Azure リージョンにデプロイされます。
次の構成を持つ AVNM2 という名前の Virtual Network Manager インスタンスを作成します。
* 管理範囲 :サブ1
* ネットワークグループ:
o 名前: グループ2
グループメンバー: VNet1
* セキュリティ管理者の構成:
または名前: SA2
o ルールコレクション:
名前: SACollection2
対象ネットワークグループ: グループ2
セキュリティ管理ルール:
名前: SARule2
優先度: 500
アクション: 常に許可
方向: 着信
ソースタイプ: 任意
送信元ポート: *
SA2 はすべての Azure リージョンにデプロイされます。
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: **7**

RT1 という名前のルート テーブルを含む Azure サブスクリプションがあります。RT1 には、次の構成のルートが含まれています。

* 名前: ルートA
* IPアドレスプレフィックス: 192.168.0.0/24
* ネクストホップ IP アドレス: 172.16.10.10

次の表に示すルートを追加するかどうかを評価しています。

Name	IP address prefix	Next hop IP address
Route1	192.168.0.0/16	172.16.10.20
Route2	192.168.0.0/24	172.16.10.30
Route3	192.168.0.0/28	172.16.10.40

RT1 に追加できるルートはどれですか?
A. ルート1のみ
B. Route3のみ
C. Route2とRoute3のみ
D. Route1とRoute3のみ
E. Route1とRoute2のみ
F. Route2のみ
正解: **D** (コメントを発表する)

質問: **8**
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. アプリのロール
B. 役割と管理者
C. ユーザーとグループ
D. API権限
正解: **C** (コメントを発表する)

質問: **9**
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。
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。
権限の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す。
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 :Sa1にロックを作成します。
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)
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.
Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

質問: **10**
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. 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。
B. 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。
C. NSG1 の場合、サービス タグを持つルールを構成します。
D. アプリケーション セキュリティ グループを作成します。
正解: **(**正解を表示します**)**

質問: **11**
App1という名前のWebアプリとVault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
Vault1にシークレットを保存してアクセスするようにApp1を構成する必要があります。
App1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。

Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

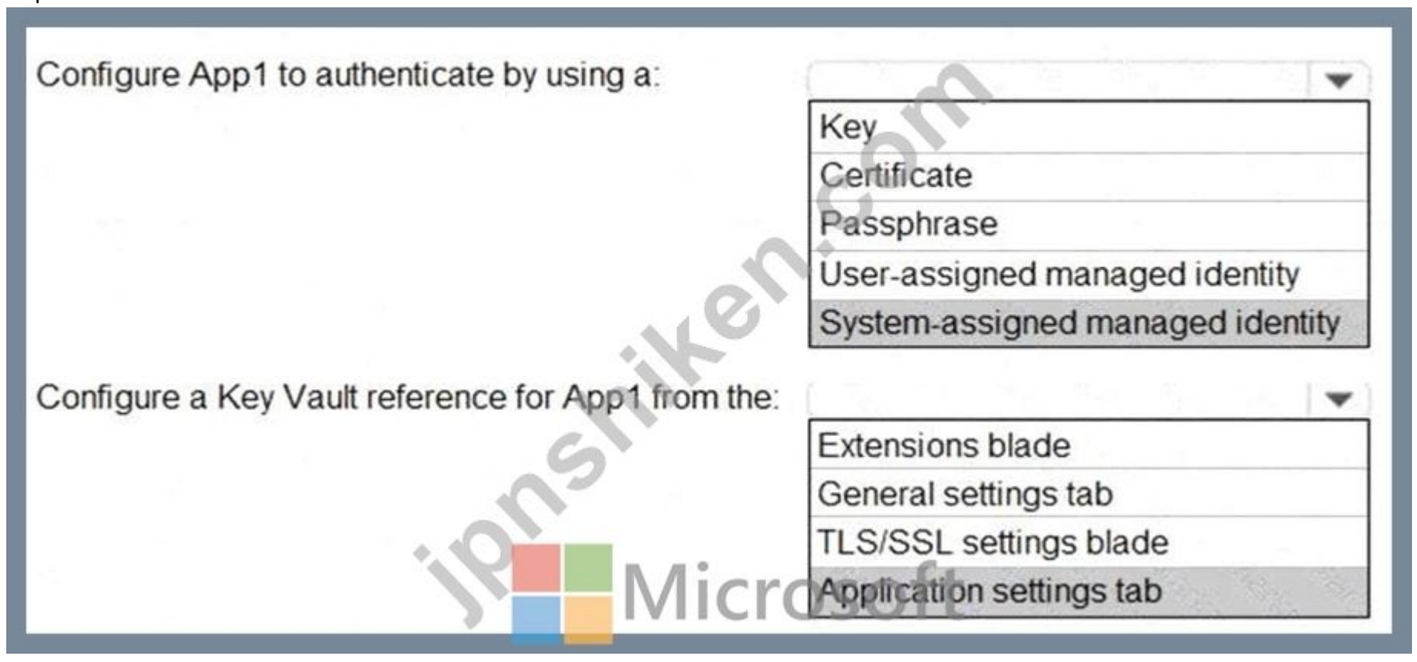
Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

正解:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

質問: **12**
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 と RG1 のみ
B. contoso.com とサブスクリプション 1 のみ

C. contoso.com. RG1. および Subscription1
D. contoso.com のみ
正解: **(**正解を表示します**)**

質問: **13**
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. 組み込みの評価を割り当てます。
B. 新しいカスタム標準を作成します。
C. 新しい顧客評価を作成します。
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: **D (**コメントを発表する**)**

質問: **14**
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。
Answer Area

Statements	Yes	No
You can use URL filtering on the network rules for VNet1.	○	○
You can use an intrusion detection and prevention system (IDPS) to monitor malicious activity on VNet2.	○	○
If you configure peering between VNet1 and VNet3, encrypted outbound traffic from VNet3 will be inspected.	○	○

正解:



Explanation:



Microsoft
ipnshiken.com

質問: 15

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. 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。
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. Defender for Cloud から、環境設定を構成します。
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: **C** (コメントを発表する)

質問: 16

VM1という名前のAzure仮想マシンがあります。
Azure Security Centerから、「仮想マシンにエンドポイント保護ソリューションをインストールする」という重要度の高い推奨事項を入手できます。
重要度の高い推奨の原因となっている問題を解決する必要があります。
あなたは何をするべきか？

A. Microsoft Antimalware拡張機能をVM1に追加します。
B. VM1にEndpoint Protection用のMicrosoft System Center Security Management Packをインストールします。
C. Network Watcher Agent for Windows拡張機能をVM1に追加します。
D. Microsoft Defender Advanced Threat Protection（Microsoft Defender ATP）へのオンボードVM1。
正解: (正解を表示します)
Reference:

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

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**」

質問: **17**
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. サーバー2のみ
D. サーバー1のみ
E. Servei2 と Servet3
F. サーバー3のみ
正解: **F** (コメントを発表する)

質問: **18**
Microsoft Entra Permissions Management を使用し、次の表に示すアカウントを含む Microsoft Entra テナントがあります。

Name	Role
Admin1	Global Administrator
Admin2	Privileged Role Administrator
Admin3	Privileged Authentication Administrator
Admin4	Exchange Administrator

Entra アクセス許可管理ポータルの Azure AD Insights タブに、高度な権限を持つロールに割り当てられていると表示されるアカウントはどれですか?
A. Admin1、Admin2、Admin3のみ
B. 管理者1のみ
C. Admin2、Admin3、Admin4のみ
D. Admin2とAdmin3のみ
E. 管理者1、管理者2、管理者3、管理者4
F. Admin2とAdmin4のみ
正解: (正解を表示します)

質問: **19**
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. コンプライアンス ポリシーを作成します。
B. 条件付きアクセス ポリシーを作成します。
C. SQLdb1 のフェデレーション クライアント ID を構成します。
D. SQLServer1 の Microsoft Entra 認証を構成します。
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: (正解を表示します)

質問: **20**
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:

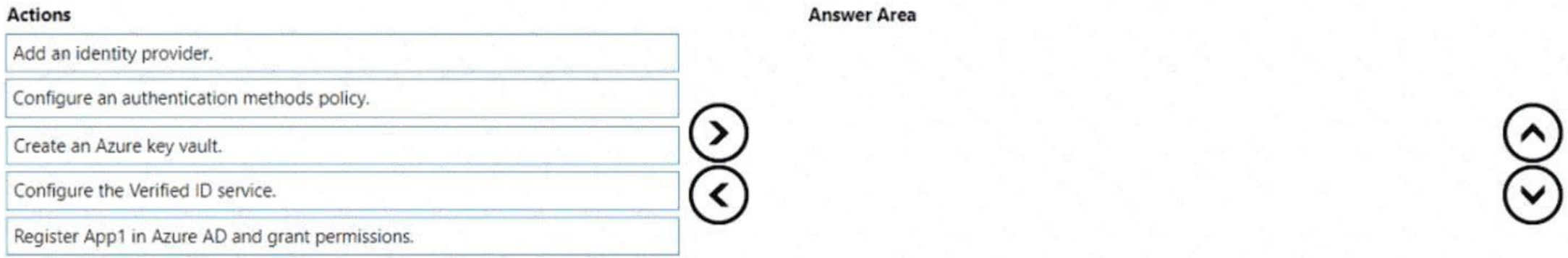


質問: 21

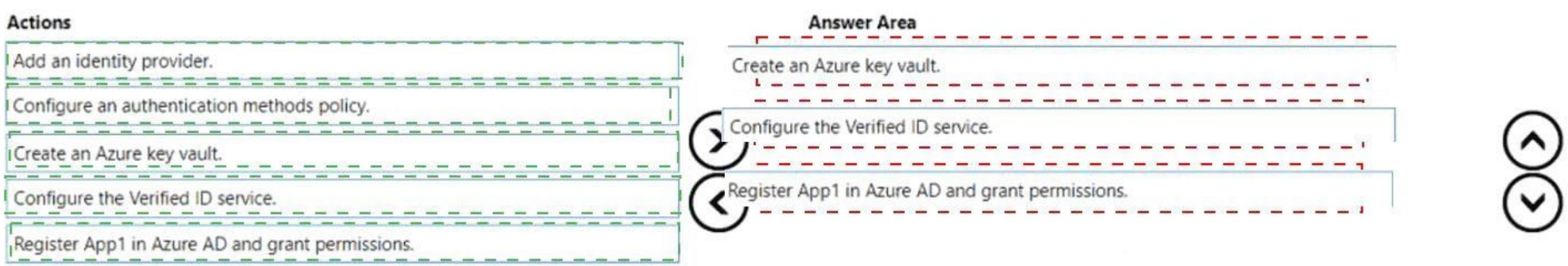
Contoso.comという名前のAzureActive Directory（Azure AD）テナントとAzure Service（AKS）クラスターAKS1があります。

Contoso.comのアカウントを使用してAKS1にアクセスできないことがわかりました。Contoso.comのアカウントを使用してAKS1にアクセスできることを確認する必要があります。ソリューションでは、管理作業を最小限に抑える必要があります。
あなたは最初に何をすべきですか？
A. AzureからAKS1を再作成します
B. AKS1から、Kubermetesのバージョンをアップグレードします。
C. Azure ADから、Azure AD PremiumP2を実装します。
D. Azure ADから、ユーザー設定を構成します
正解: **A** (コメントを発表する)
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

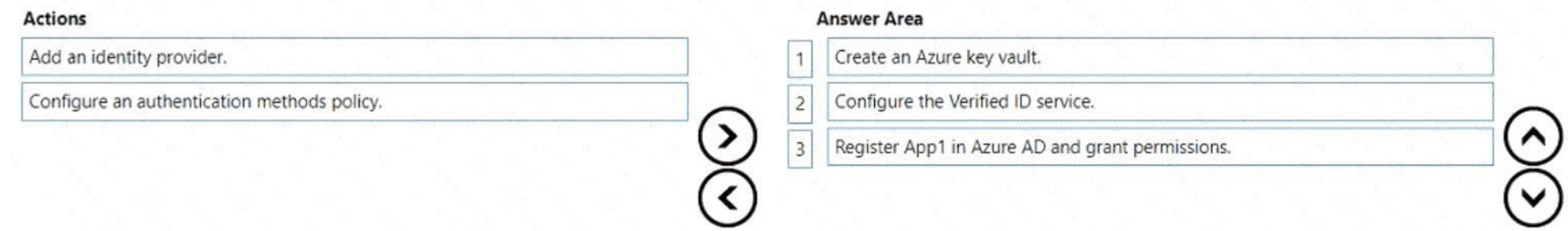
質問: **22**
Azure AD テナントと App1 という名前のアプリケーションがあります。
App1 が Microsoft Entra Verified ID を使用して資格情報を確認できることを確認する必要があります。
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。



正解:



Explanation:



https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant

質問: 23

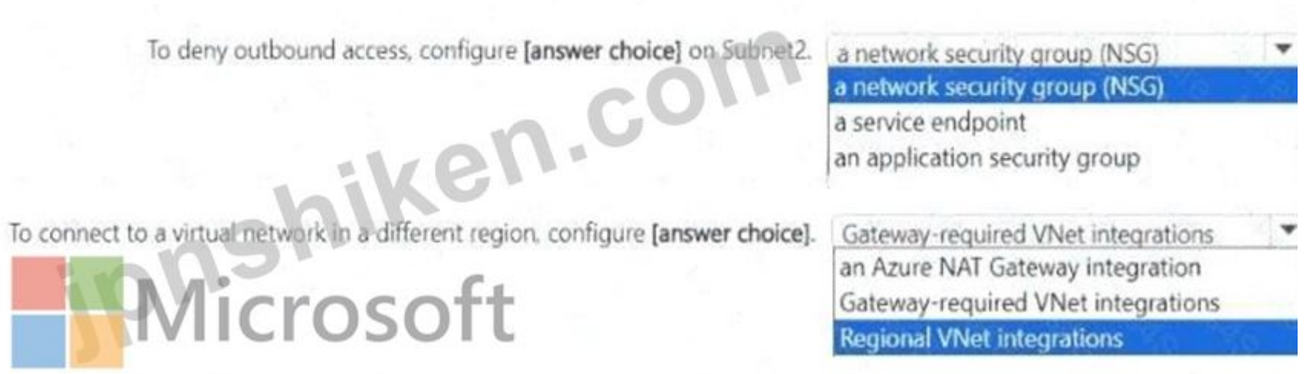
次の図に示すように、App1 という名前の Azure App Service Web アプリがあります。



サブネット 2 には VM1 という名前の仮想マシンが含まれています。

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回答の選択肢を選択します。注: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:



Explanation:



質問: 24

次のリソースを含むAzureサブスクリプションがあります。

* Azureキーボールト
* Database1という名前のAzureSQLデータベース

*システムによって割り当てられた管理IDを使用してDatabase1にアクセスするように構成されたAppSrv1およびAppSrv2という名前の2つのAzureApp ServiceWebアプリ次の要件を満たすDatabase1の暗号化ソリューションを実装する必要があります。

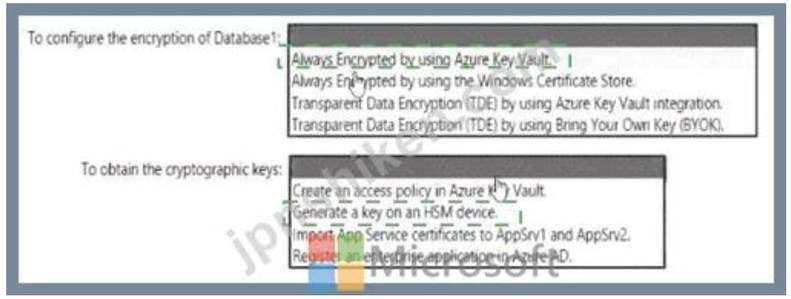
* AppSrv1のみがデータを復号化できるように、Database1のDiscountという名前の列のデータを暗号化する必要があります。
* AppSrv1およびAppSrv2は、暗号化キーを取得するために管理対象IDを使用して承認する必要があります。

Database1の暗号化設定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

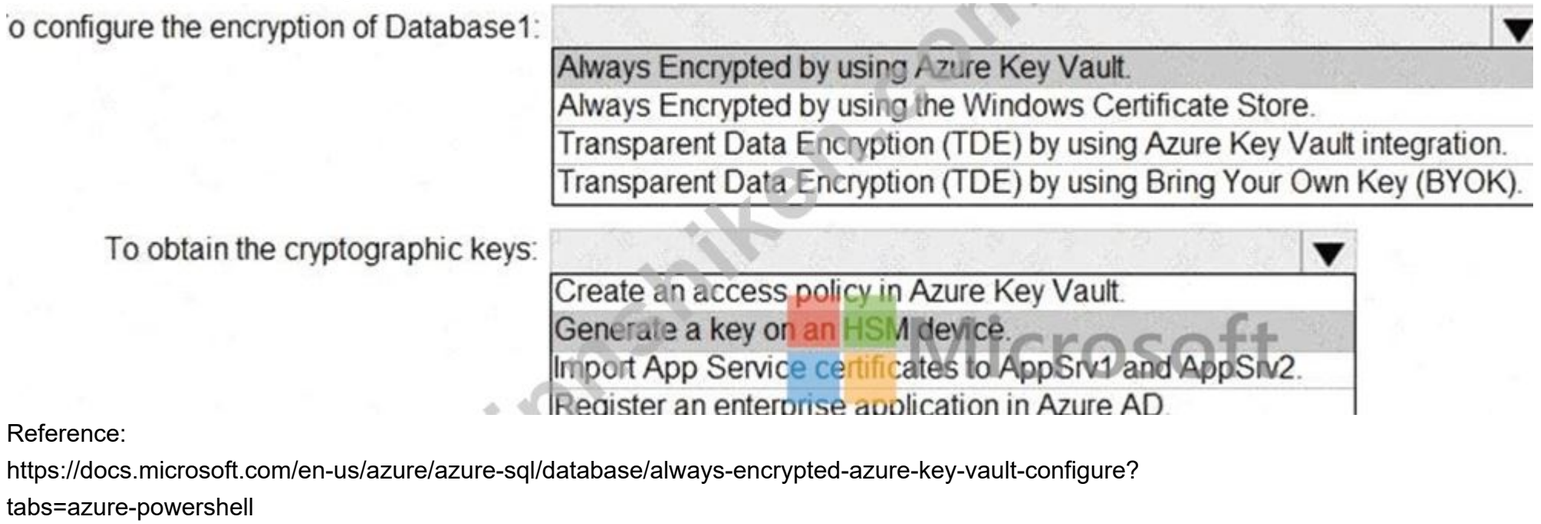


正解:



Explanation:

Text Description automatically generated with medium confidence



Reference:

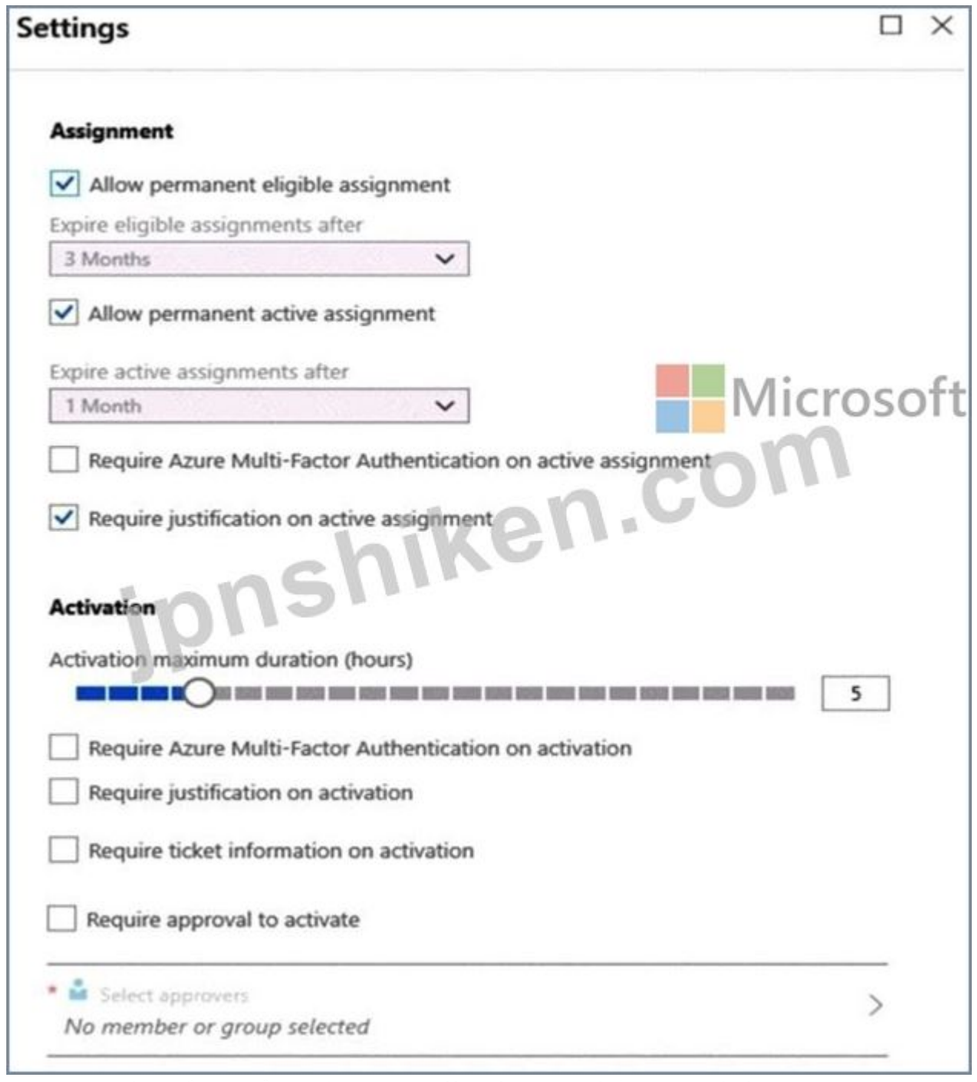
https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell

質問: **25**

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
User1	Group1
User2	Group2
User3	Group1, Group2

Azure AD Privileged Identity Management (PIM) から、次の図に示すように、セキュリティ管理者ロールの設定を構成します。



Microsoft
jpnshiken.com

PIM から、次のグループにセキュリティ管理者ロールを割り当てます。

* グループ1: アクティブな割り当てタイプ、永続的に割り当て
* グループ2: 適格な割り当てタイプ、永久に適格

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
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

正解:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Explanation:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Box 1: Yes

Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There ' s no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don ' t need that access all the time.

You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.

Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.

Box 2: Yes

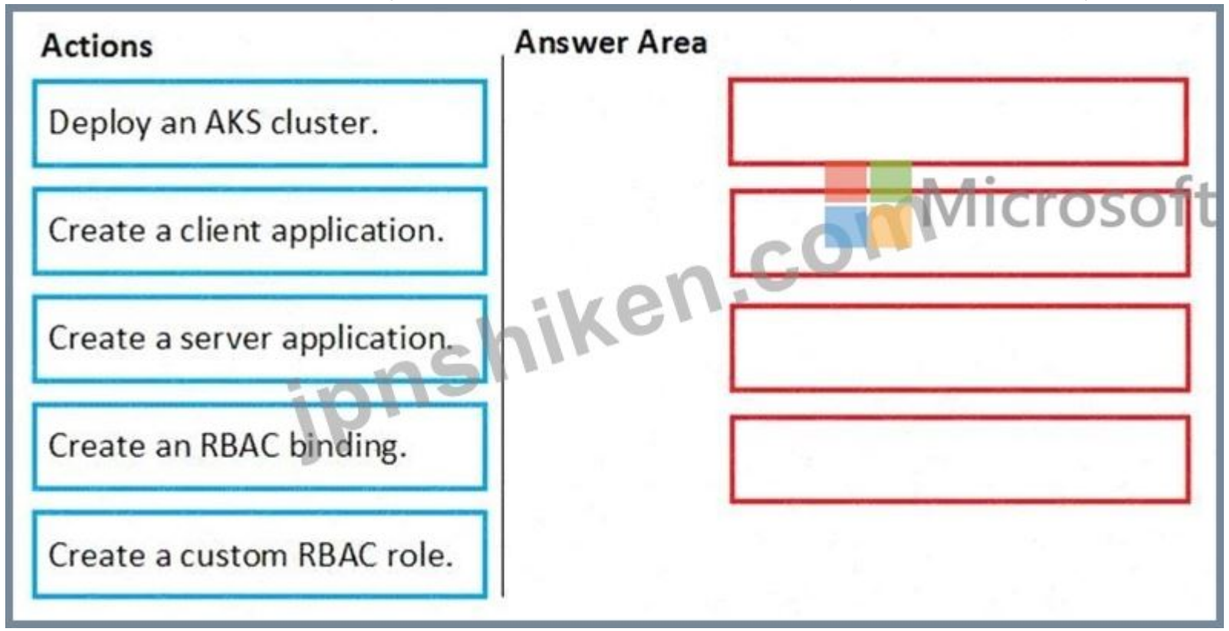
Active Type: A role assignment that doesn ' t require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role Box 3: Yes User3 is member of Group2.

Reference:

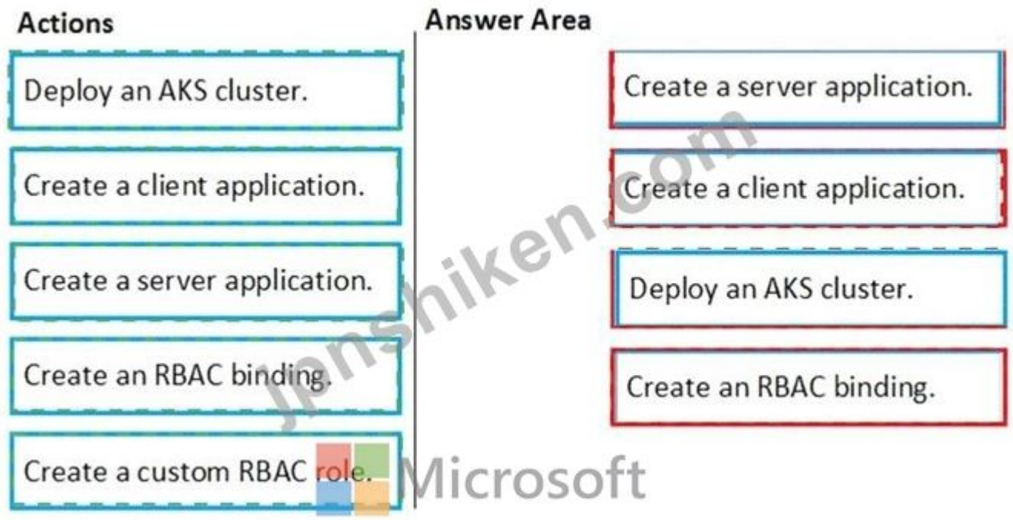
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

質問: **26**
プラットフォーム保護の要件を満たすには、AKS1 をデプロイする必要があります。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。
注意：正解の選択肢は複数あります。正解の選択肢の中からどれを選択しても、得点は加算されます。



正解:



Explanation:



Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.
Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.
Step 2: Create a client application
The second application is a client component that ' s used when you ' re prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.
Step 3: Deploy an AKS cluster.
Use the az group create command to create a resource group for the AKS cluster.
Use the az aks create command to deploy the AKS cluster.
Step 4: Create an RBAC binding.
Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration
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: **27**

Policy1という名前のAzureポリシー定義を含むAzureサブスクリプション名Sub1があります。Policy1には次の設定があります。

定義場所 :テナントルートグループ

カテゴリ :モニタリング

Policy1に準拠していないリソースがAzureSecurityCenterダッシュボードに一覧表示されてい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. Policy1のカテゴリをセキュリティセンターに変更します。

B. カスタムイニシアチブにPolicy1を追加します。

C. Policy1の定義場所をSub1に変更します。

D. Policy1をSub1に割り当てます。

正解: (正解を表示します)

Reference:

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

質問: **28**

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: (正解を表示します)
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

質問: **29**
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: **30**
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. SQL
B. VM1
C. LB1
D. VMSS1
正解: (正解を表示します)

質問: **31**
Sub1という名前のAzureサブスクリプションがあります。
Azure Security Centerには、WF1という名前のワークフローの自動化があります。WF1は、User1という名前のユーザーに電子メールメッセージを送信するように構成されています。
Alertsという名前の配布グループに電子メールメッセージを送信するには、WF1を変更する必要があります。
WF1を変更するには何を使用する必要がありますか？
A. Azure Application Insights
B. Azure Monitor
C. Azure Logic Apps Designer
D. Azure DevOps
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation
https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure-playbook

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**」

質問: **32**
ストレージ アカウントと App1 という名前の Azure Web アプリを含む Azure サブスクリプションがあります。
App1 は、Endpoint1 という名前のプライベート エンドポイントを使用する Cosmos1 という名前の Azure Cosmos DB データベースに接続します。Endpoint1 にはデフォルト設定があります。
Cosmos1 への名前解決を検証する必要があります。
どの DNS ゾーンを使用する必要がありますか?
A. エンドポイント 1。プライベートリンク、ドキュメント、azure、com
B. エンドポイント 1。プライベートリンク、ブロブ、コア、Windows、ネット
C. エンドポイント 1。プライベートリンク、azure ウェブサイト、ネット
D. エンドポイント1。プライベートリンク、データベース、azure、com
正解: (正解を表示します)

質問: **33**

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: Group1 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: **A** (コメントを発表する)

質問: **34**
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/76c42af2-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。

Answer Area

[Answer choice] can create keys in the key vault. [▼]

[Answer choice] can create secrets in the key vault. [▼]

正解:

See the answer below at Explanation.

Explanation:

Answer is as image below.



質問: **35**
Windows Server2019を実行するオンプレミスサーバーが10台あります。
サーバーにAzureSecurityCenterの脆弱性スキャンを実装することを計画しています。
最初にサーバーに何をインストールする必要がありますか？
A. AzureSentinelのセキュリティイベントデータコネクタ
B. Microsoft Endpoint ConfigurationManagerクライアント
C. AzureArc対応サーバーConnectedMachineエージェント
D. エンドポイントエージェント用のMicrosoft Defender
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview
https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

質問: **36**
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. Kustoクエリ言語クエリ
B. 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
C. 動的グループクエリ
D. 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
正解: (正解を表示します)

質問: **37**
AKS1 という名前の Azure Kubernetes Service (AKS) クラスターを含む Azure サブスクリプションがあります。
Azure DevOps Microsoft ホスト エージェントを使用してデプロイされたコンテナー イメージを格納する Azure コンテナー レジストリがあります。
管理者が特定のネットワークからのみ AKS1 にアクセスできるようにする必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。

AKS1 には何を構成する必要がありますか?
A. プライベート クラスター
B. 許可されたIPアドレス範囲
C. アプリケーション ゲートウェイ イングレス コントローラー (AGIC)
D. プライベートエンドポイント
正解: **B (**コメントを発表する**)**

質問: **38**
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: **39**
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。
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。
権限の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す。
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SASを生成します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **B (**コメントを発表する**)**
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.
Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:

https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

質問: **40**
container1という名前のコンテナーを持つstorage1という名前のAzureストレージアカウントがあります。container1のBLOBが変更されないようにする必要があります。あなたは何をするべきか？
A. container1から、アクセスレベルを変更します。
B. container1からアクセスポリシーを追加します。
C. container1から、アクセス制御（IAM）設定を変更します。
D. storage1から、ブロブのソフト削除を有効にします。
正解: (正解を表示します)
References:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal

質問: **41**
次の表に示すAzure仮想マシンがあります。

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

米国東部リージョンのRG1にAnalytics1という名前のAzure Log Analyticsワークスペースを作成します。
どの仮想マシンをAnalytics1に登録できますか？
A. VM1 only
B. VM1, VM2, and VM3 only
C. VM1, VM2, VM3, and VM4
D. VM1 and VM4 only
正解: (正解を表示します)
Note: Create a workspace
* In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.
* Click Create, and then select choices for the following items:
Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.
Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.
For Resource Group, select an existing resource group that contains one or more Azure virtual machines.
Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

質問: **42**
次の表に示すリソースが含まれる Sub1 という名前の Azure サブスクリプションがあります。

Name	Type
storage1	Storage account
storage2	Storage account
VM1	Virtual machine
VM2	Virtual machine
Analytics1	Log Analytics workspace

ストレージ アカウントと仮想マシンに対して Microsoft Defender for Cloud を有効にする必要があります。
ストレージアカウントと仮想マシンに対して、どのレベルでDefender for Cloudを有効にできますか？回答するには、回答エリアで適切なオプションを選択してください。注：正しい選択ごとに1ポイントが加算されます。

Storage accounts:
- Subscription only
- Workspace only
- Storage account only
- Subscription or storage account only
- Subscription, workspace, or storage account

Virtual machines:
- Subscription only
- Workspace only
- Virtual machine only
- Subscription or virtual machine only
- Subscription, workspace, or virtual machine

正解:



Explanation:



Microsoft
jpnshiken.com

質問: **43**

Sub1という名前のAzureサブスクリプションがあります。Sub1には、Subnet1という名前の1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が含まれています。

Subnet1のサービスエンドポイントを作成します。

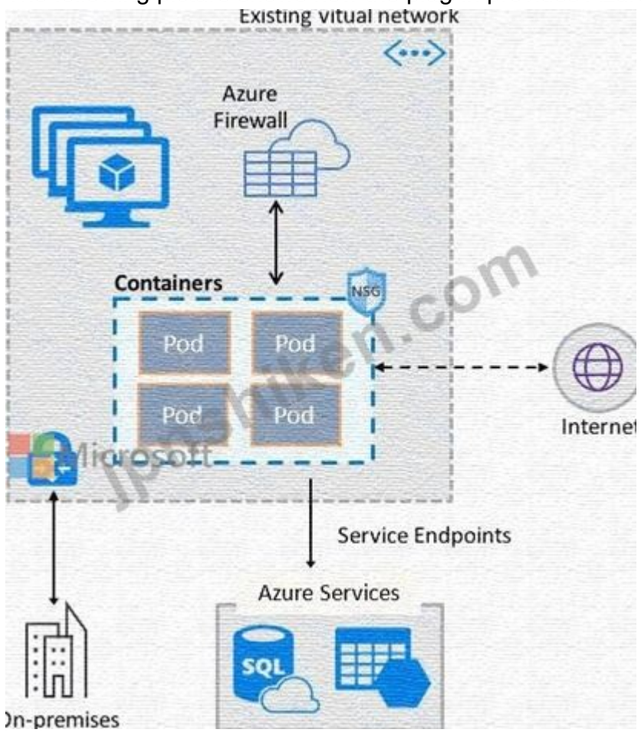
Subnet1には、Ubuntu Server 18.04を実行するVM1という名前のAzure仮想マシンが含まれています。

DockerコンテナーをVM1にデプロイする必要があります。コンテナは、サービスエンドポイントを使用してAzure StorageリソースとAzure SQLデータベースにアクセスできる必要があります。

A. アプリケーションセキュリティグループとネットワークセキュリティグループ (NSG) を作成します。

B. docker-compose.ymlファイルを編集します。

C. コンテナネットワークインターフェイス (CNI) プラグインをインストールします。
正解: (正解を表示します)
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine.
The plug-in supports both Linux and Windows platform.
The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:

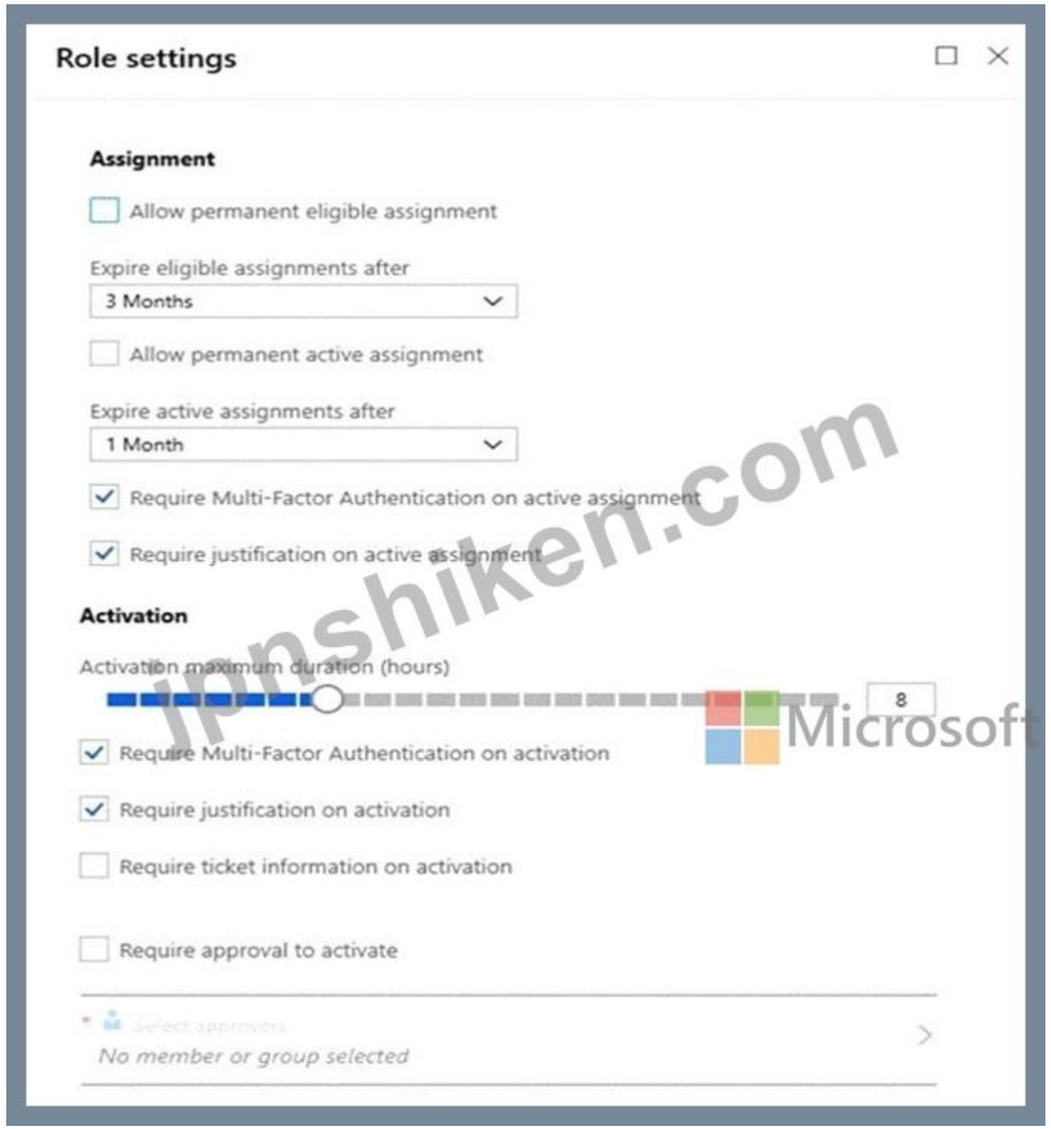


References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

質問: **44**
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。)

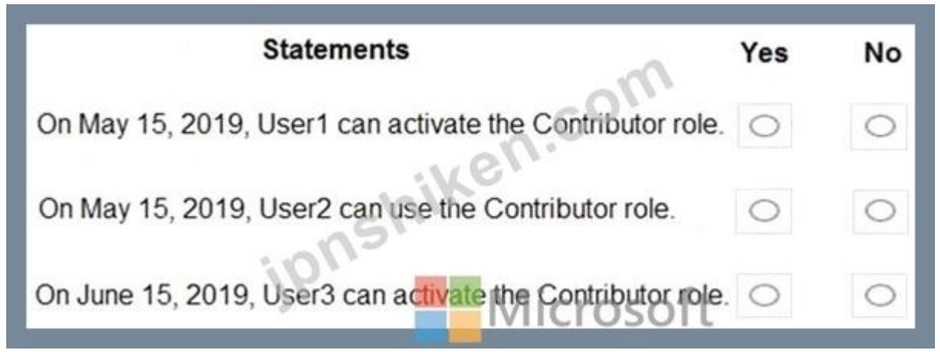


次の表に示すように、2019 年 5 月 1 日にユーザーに Contributor ロールを割り当てます。

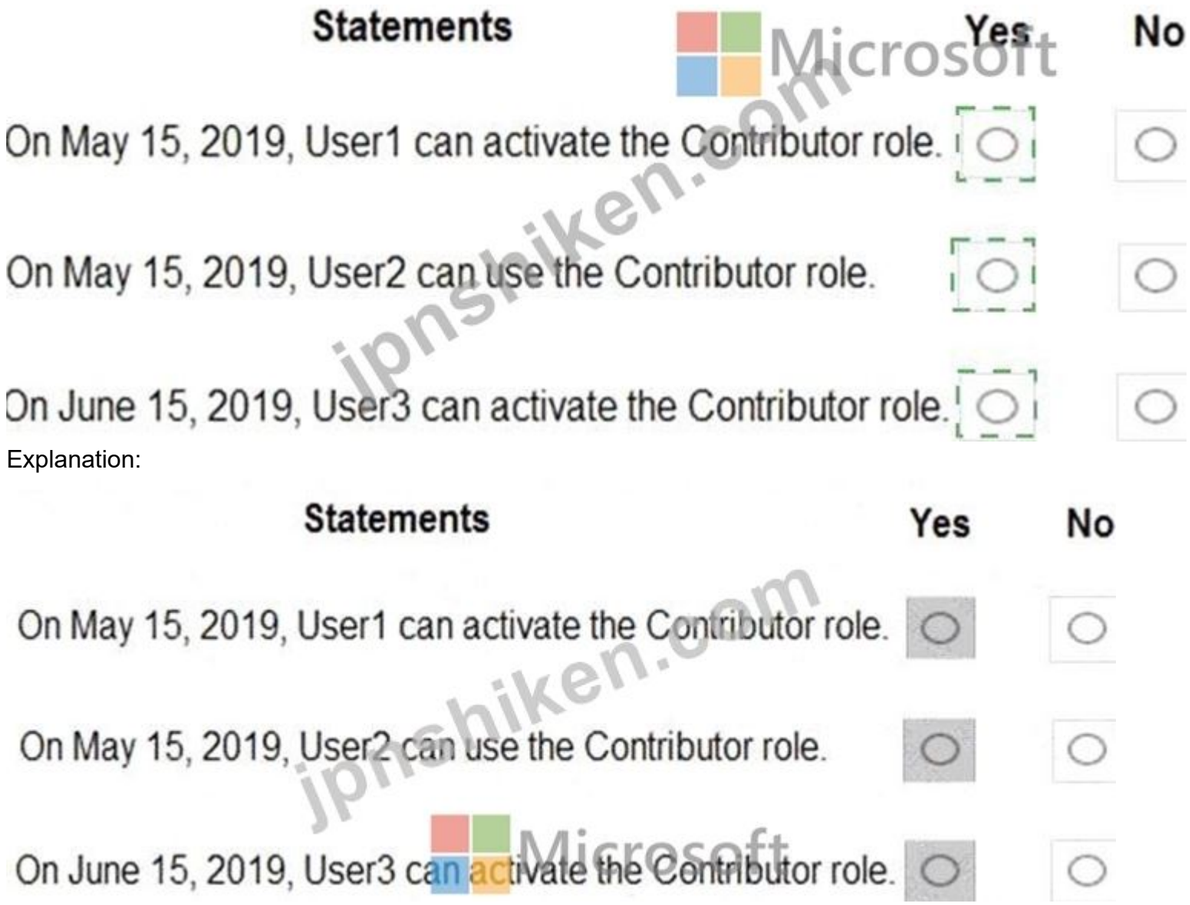
Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

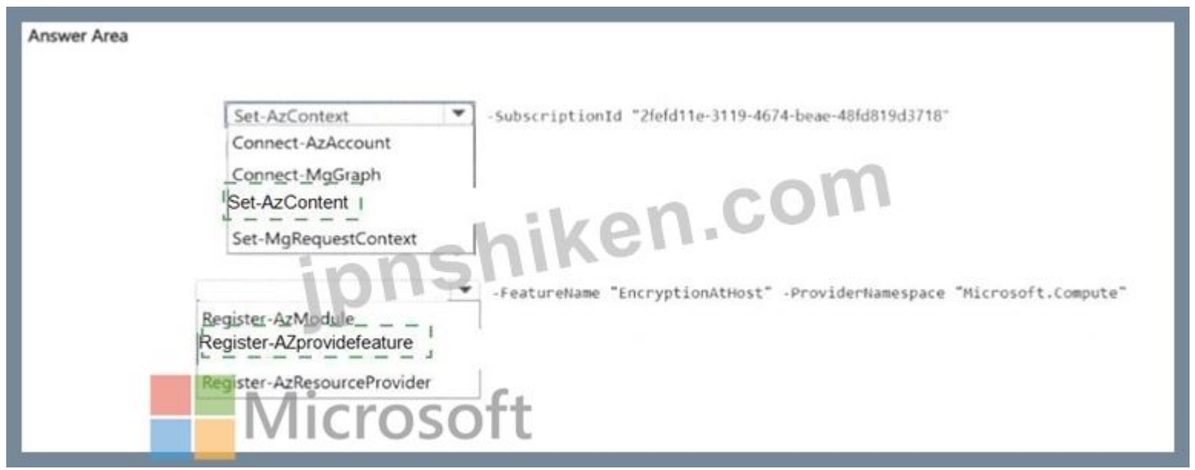
質問: 45
次の表に示すように、Microsoft Entraテナントが2つのAzureサブスクリプションにリンクされています。

Name	Subscription ID
Sub1	d3b54a99-5e2a-45f0-a3a7-9fdf12a29cf0
Sub2	2fefd11e-3119-4674-beae-48fd819d3718

Sub2では、VM1という名前の仮想マシンを作成する予定です。
VM1のホスト側で暗号化を有効にできることを確認する必要があります。
Azure Cloud Shell で最初に入力するコマンドはどのようにすればよいですか？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。
Answer Area



正解:



Explanation:



質問: **46**

Sub1 という名前の Azure サブスクリプションがあります。

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

Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

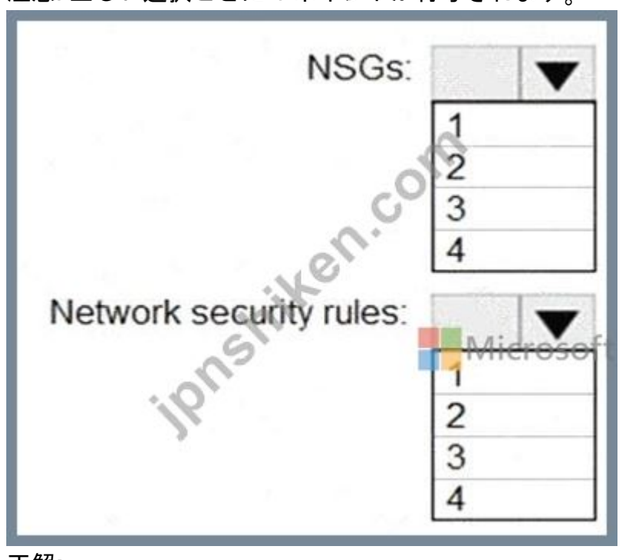
現在、ネットワーク セキュリティ グループ (NSG) はプロビジョニングされていません。

次の要件を満たすネットワーク セキュリティを実装する必要があります。

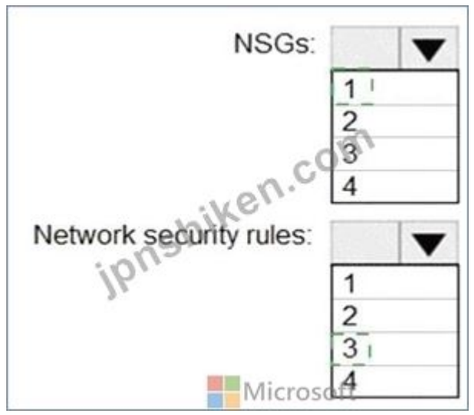
* VM3 から VM4 へのトラフィックのみを許可します。
* インターネットから VM1 および VM2 へのトラフィックのみを許可します。
* NSG とネットワーク セキュリティ ルールの数を最小限に抑えます。

NSG とネットワーク セキュリティ ルールはいくつ作成する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

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:

NSGs: 1

Network security rules: 3

Not 2: You cannot specify multiple service tags or application groups) in a security rule.

References:

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

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**」

質問: 47

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。

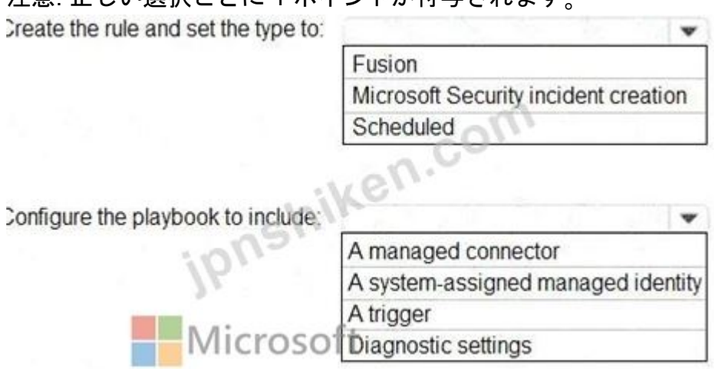
クエリ 1 は、Azure AD によって生成されたセキュリティ イベントのサブセットを返します。

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。

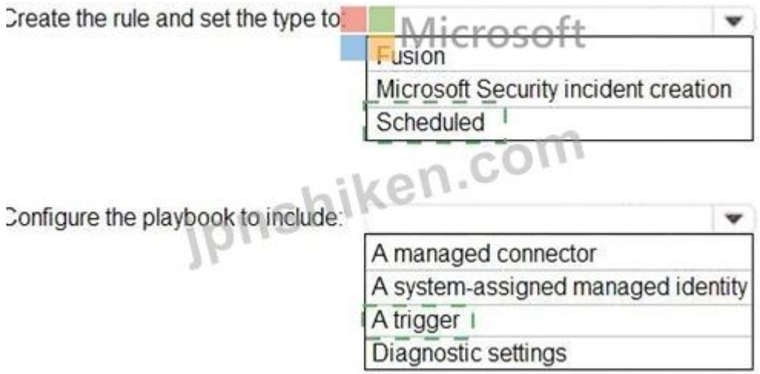
Playbook1 を新しいルールに追加できることを確認する必要があります。

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。

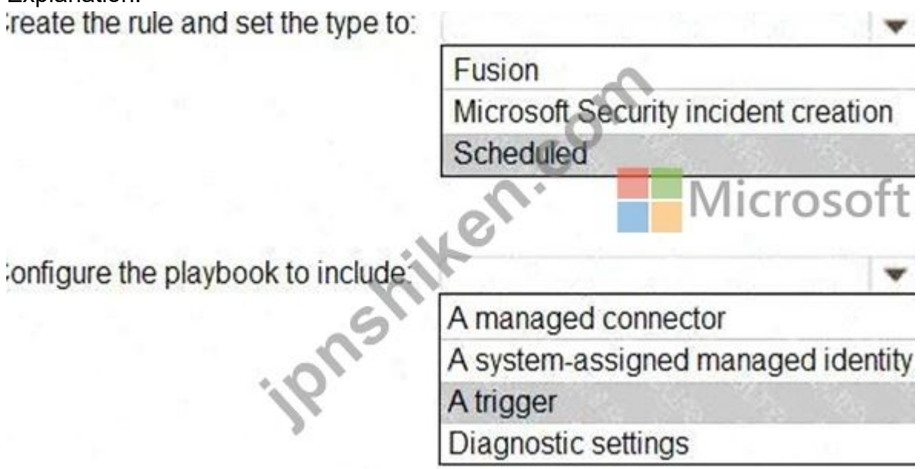
注意: 正しい選択ごとに 1 ポイントが付与されます。



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: **48**
会社には、contoso.comという名前のAzure Active Directory Azure（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。
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: **49**
Azure Active Directory (Azure AD) テナントと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。
テナントのアプリ登録設定は、次の図に示すように構成されています。



App1という名前のアプリをデプロイする予定です。
User1がApp1をAzure ADに登録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、最小限の特権の原則を使用する必要があります。
User1にどのロールを割り当てる必要がありますか。
A. サブスクリプションのアプリ構成データの所有者
B. サブスクリプションの管理対象アプリケーションの貢献者
C. Azure ADのクラウドアプリケーション管理者
D. Azure ADのアプリケーション開発者。
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

質問: **50**
次の表に示すリソースを含む Azure Active Directory (Azure AD) テナントがあります。

Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

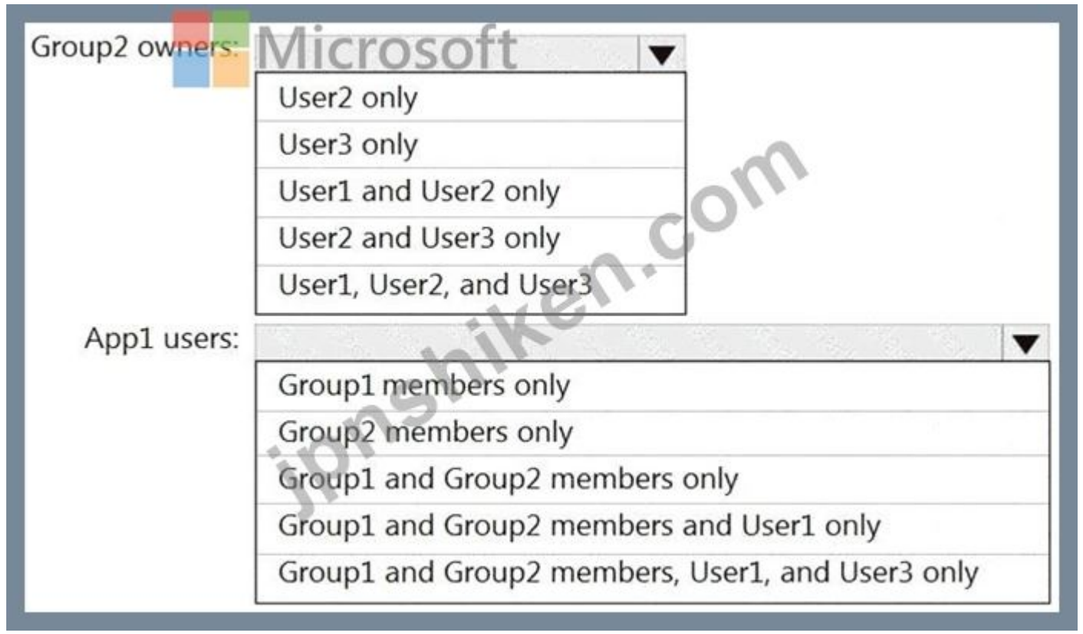
User2 は Group2 の所有者です。
App1 のユーザーとグループの設定は、次の図に示すように構成されています。



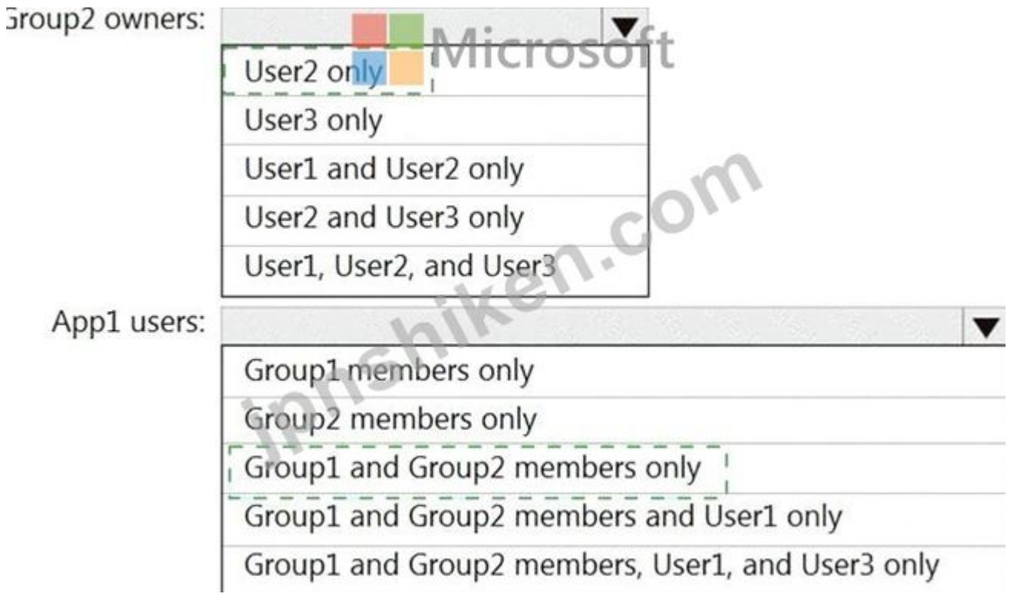
次の図に示すように、App1 のセルフサービス アプリケーション アクセスを有効にします。



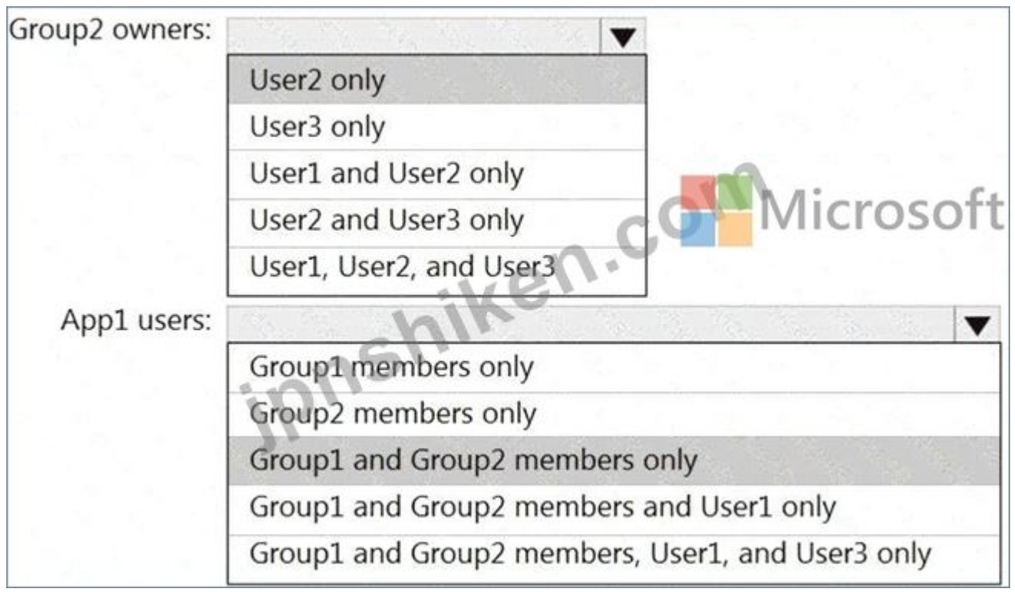
User3 は、Appl へのアクセスを承認するように構成されています。
Group2 の所有者と Appl のユーザーを特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



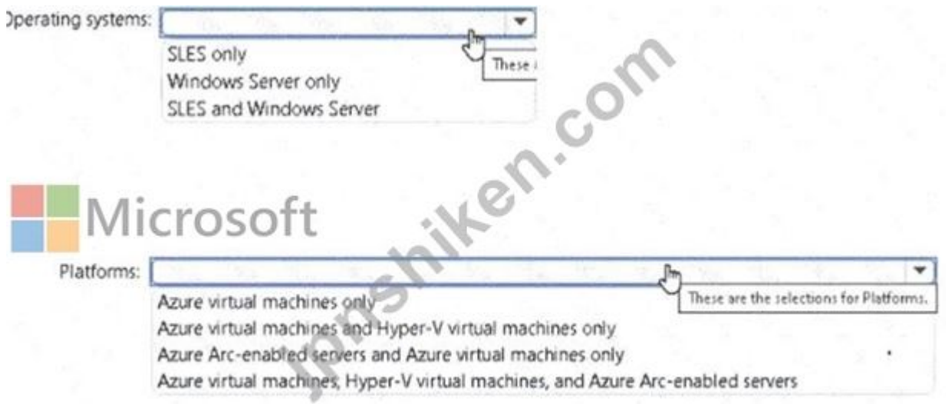
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

質問: 51

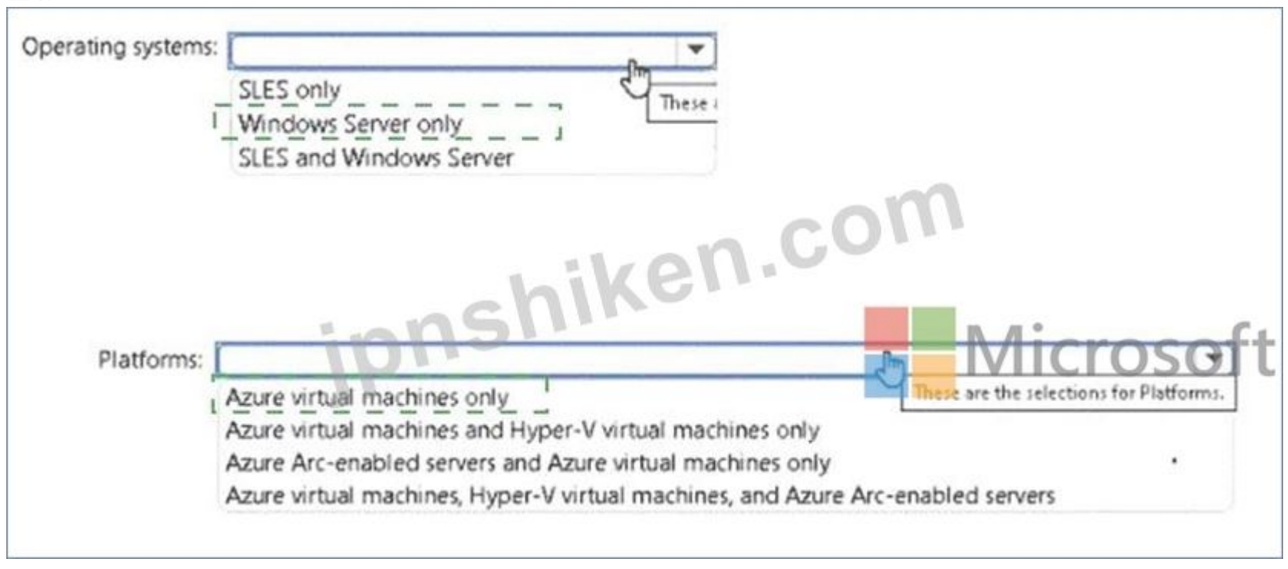
オンプレミス ネットワークには、次の表に示すサーバーが含まれています。

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: 52

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

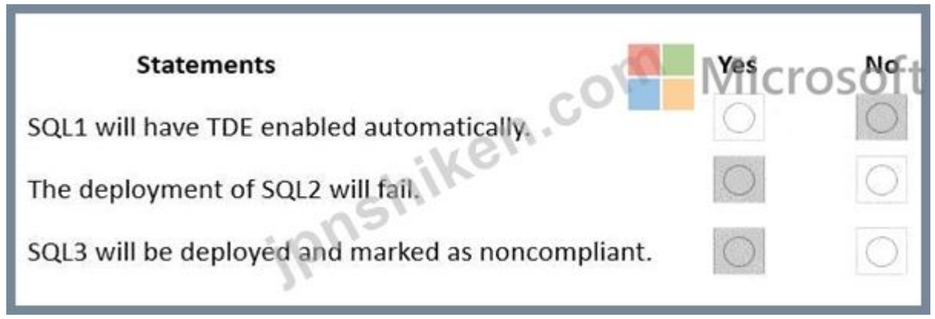
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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



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

質問**: 53**
Azure SQL データベースがあります。
Always Encrypted を実装します。
アプリケーション開発者がデータベース内のデータを取得して復号できることを確認する必要があります。
開発者に提供すべき情報は何ですか? それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. 保存されたアクセス ポリシー
B. 共有アクセス署名 (SAS)
C. 列暗号化キー
D. ユーザー認証情報
E. 列マスター キー
正解**: C,E (**コメントを発表する**)**
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

質問**: 54**
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。
テナントのグローバル管理者ロールが割り当てられます。Azure Security Centerの設定を管理する必要があります。
カスタムの機密ラベルを作成する必要があります。
最初に何をすべきですか？
A. カスタムの機密情報タイプを作成します。
B. Azure ADのグローバル管理者のアクセスを高めます。
C. セキュリティセンターの価格帯を標準にアップグレードします。
D. Microsoft Cloud App Securityとの統合を有効にします。
正解**:** (正解を表示します**)**
First, you need to create a new sensitive information type because you can't directly modify the default rules.
References:

https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

質問: **55**
技術要件を満たすには、関数アプリを実装する必要があります。
実装に含めるべきアプリはどれですか?
A. Fa1とFa3のみ
B. Fa1とFa2のみ
C. Fa2とFa3のみ
D. Fa1、Fa2、Fa3
正解: **(**正解を表示します**)**

質問: **56**
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	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com にはグループ命名ポリシーがあり、そのポリシーには 'Contoso」という単語を含むカスタムのブロック単語リストルールが設定されています。
contoso.com に Contoso Sales という名前のグループを作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。



正解:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy

質問: 57

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: **58**
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: **D** (コメントを発表する)
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

質問: **59**
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: **B (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

質問: **60**
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.

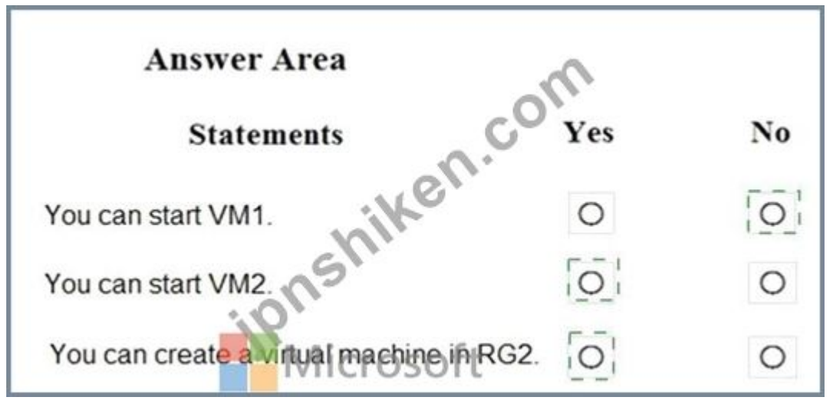
Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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。

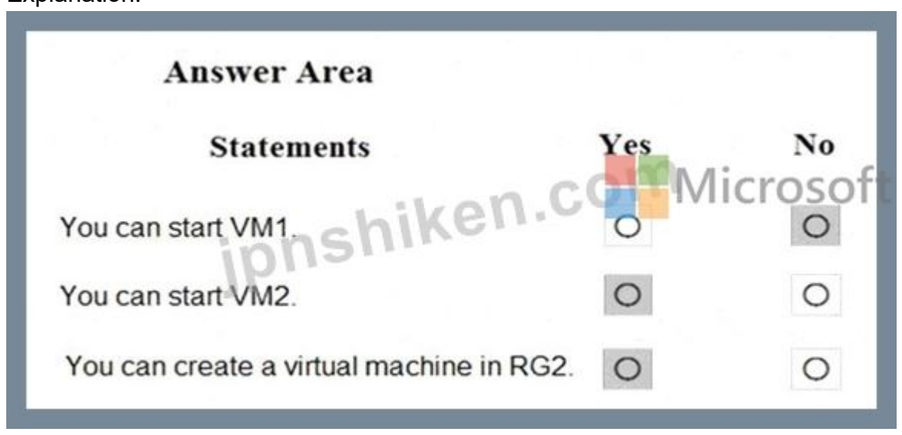
Answer Area

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

正解:

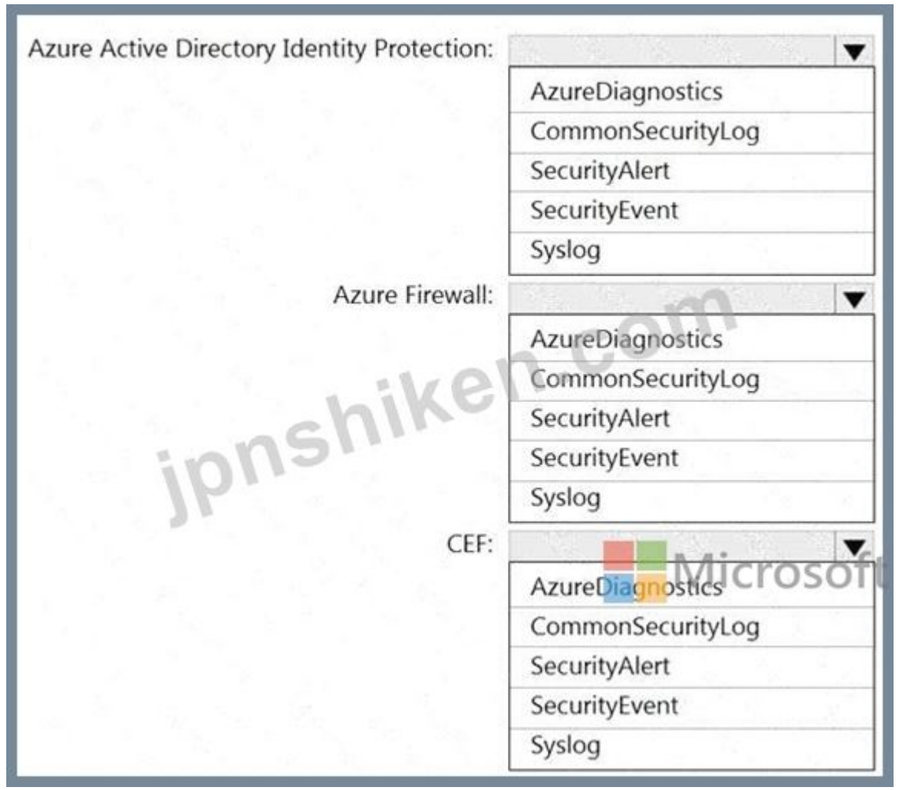


Explanation:



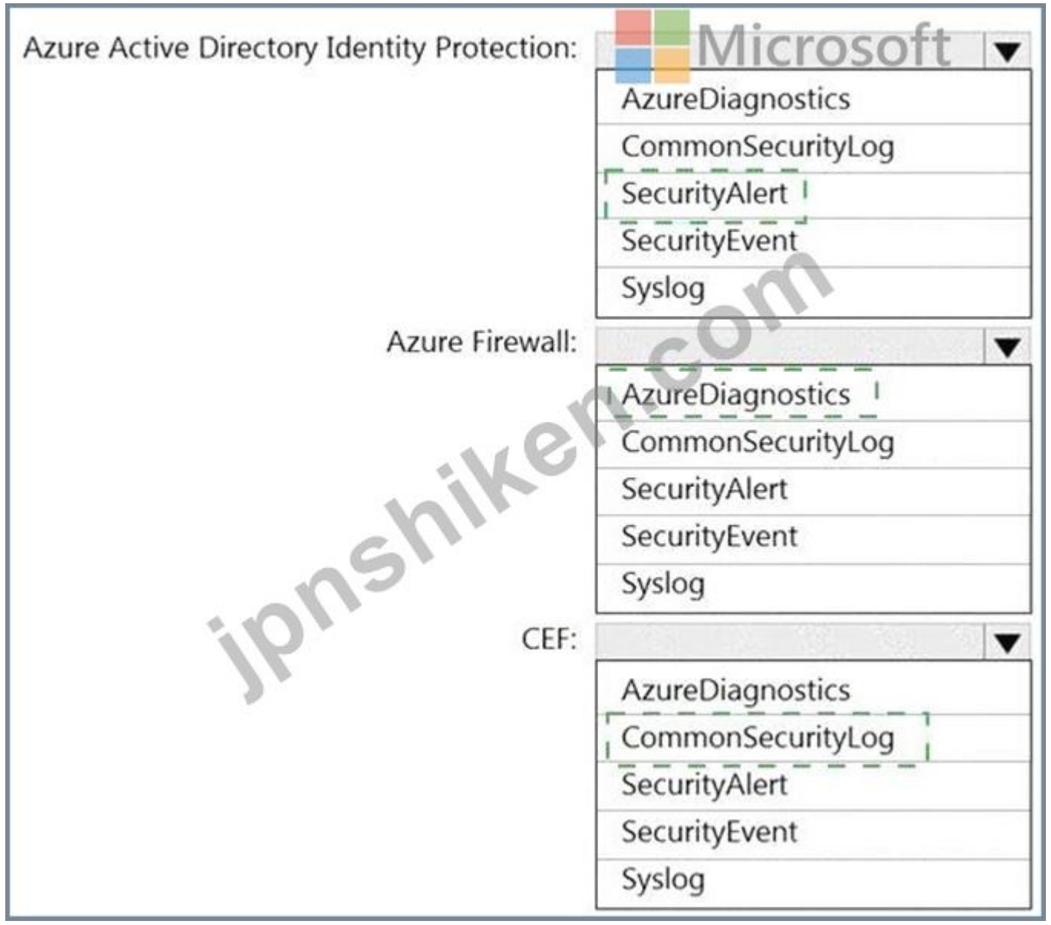
References:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

質問: **61**
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。



jpnshiken.com
Microsoft

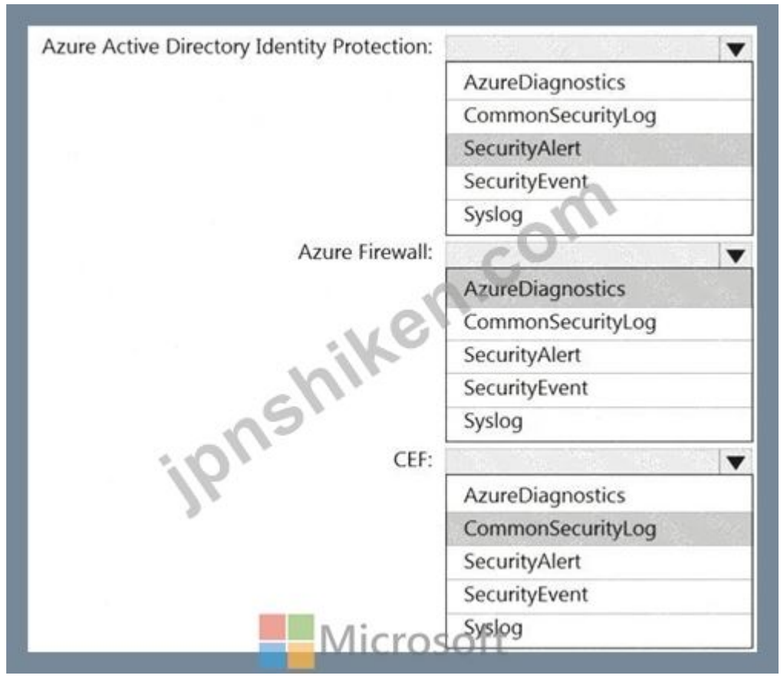
正解:



Microsoft
jpnshiken.com

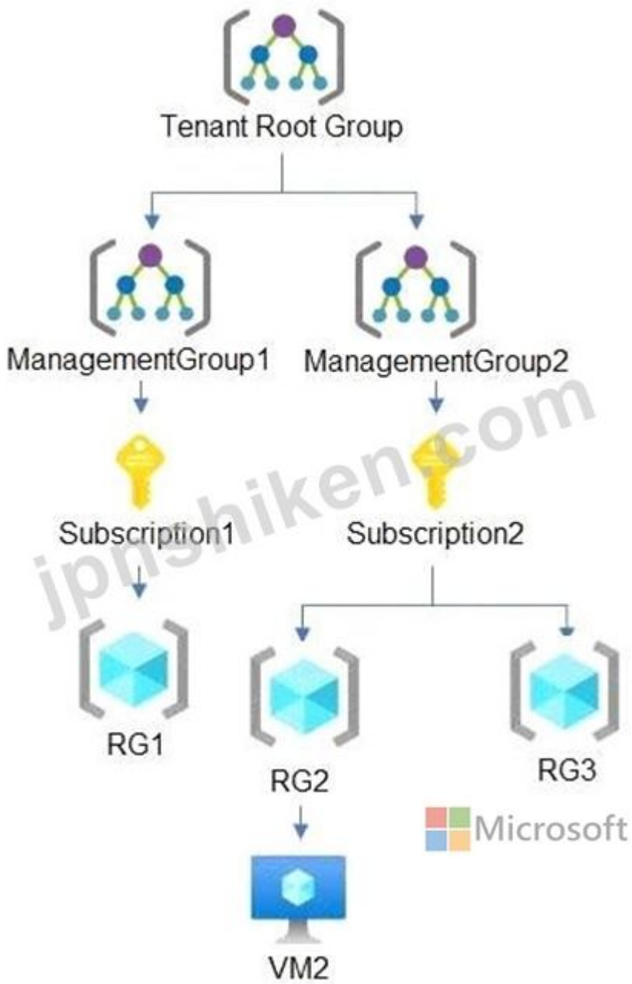
Explanation:

Graphical user interface, application, table Description automatically generated



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**」

質問: **62**
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:



質問: **63**

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	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

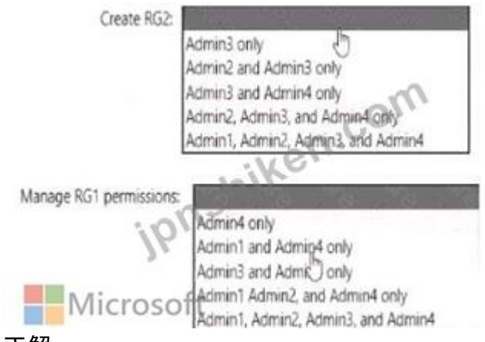
サブスクリプションには、次の表に示す仮想マシンが含まれています。

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

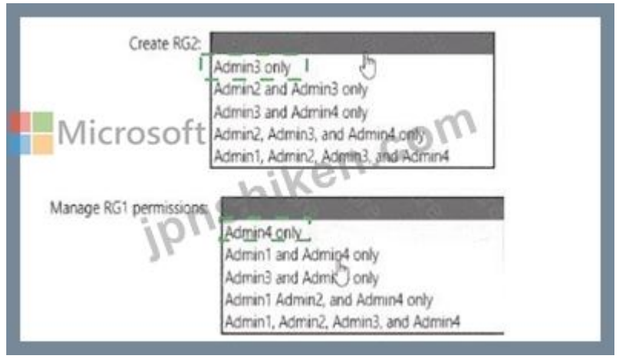
NIC1 で、ASG1 という名前のアプリケーション セキュリティ グループを構成します。
他にどのネットワーク インターフェイスで ASG1 を構成できますか?
A. NIC2のみ
B. NIC2、NIC3、NIC4、およびNIC5
C. NIC2とNIC3のみ
D. NIC2、NIC3、NIC4のみ
正解: (正解を表示します)
Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
Reference:
https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

質問: **64**
Azure Active Directory（Azure AD）のハイブリッド構成があります。Azure AD認証をサポートするように構成されたAzure SQL Databaseインスタンスがあります。
データベース開発者は、データベースインスタンスに接続し、社内のActive Directoryアカウントを使用して認証する必要があります。
開発者がMicrosoft SQL Server Management Studioを使用してインスタンス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、認証プロンプトを最小限に抑える必要があります。
どの認証方法をお勧めしますか？
A. Active Directory - Password
B. Active Directory - Universal with MFA support
C. SQL Server Authentication
D. Active Directory - Integrated
正解: (正解を表示します)
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

質問: **65**
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：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, 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: 66

Azure Active 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。

Azureポータルから、エンタープライズアプリケーションを登録します。

Azure ADで作成される追加のリソースはどれですか？

A. サービスプリンシパル

B. X.509証明書

C. 管理されたID

D. ユーザーアカウント

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: **67**
Azure Securityから、カスタムアラートルールを作成します。
アラートがトリガーされたときに電子メールメッセージを受信するユーザーを構成する必要があります。
あなたは何をするべきか？
A. From Azure Monitor, create an action group.
B. From Security Center, modify the Security policy settings of the Azure subscription.
C. From Azure Active Directory (Azure AD). modify the members of the Security Reader role group.
D. From Security Center, modify the alert rule.
正解: **A** (コメントを発表する)
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

質問: **68**
image1という名前のコンテナーイメージを含むContReg1という名前のAzureコンテナーレジストリがあります。
ContReg1のコンテンツの信頼を有効にします。
コンテンツの信頼を有効にしたら、次の表に示すように2つの画像をContReg1にプッシュします。

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

どの画像が信頼できる画像ですか？
A. image1 and image2 only
B. image2 only
C. image1, image2, and image3
正解: (正解を表示します)
Azure Container Registry implements Docker ' s content trust model, enabling pushing and pulling of signed images.
To push a trusted image tag to your container registry, enable content trust and push the image with docker push.
To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

質問: **69**
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。

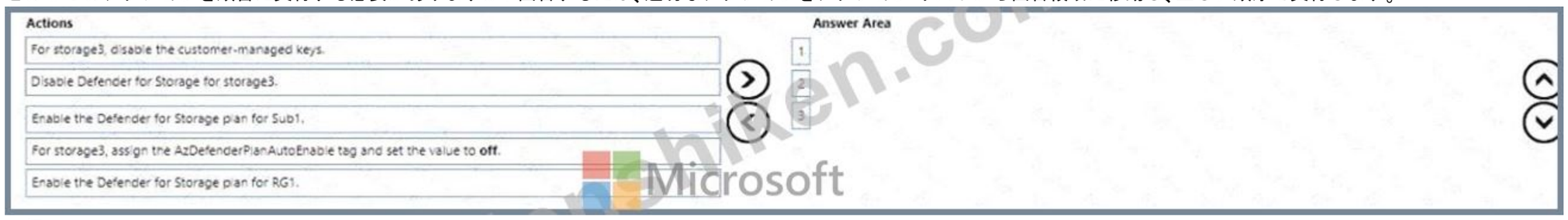
Name	Content type	Key type	Key size
Cert1	PKCS #12	RSA	2048
Cert2	PKCS #12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

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. 証明書1、証明書2、証明書3、証明書4
B. Cert3 と Cert4 のみ
C. Cert1とCert2のみ
D. Cert1とCert3のみ
正解: (正解を表示します)

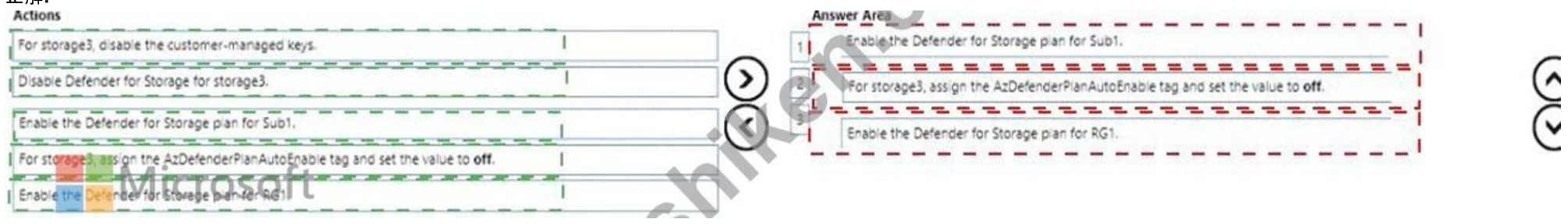
質問: **70**
次の表に示すストレージ アカウントを含む Sub1 という名前の Azure サブスクリプションがあります。

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: **71**

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。

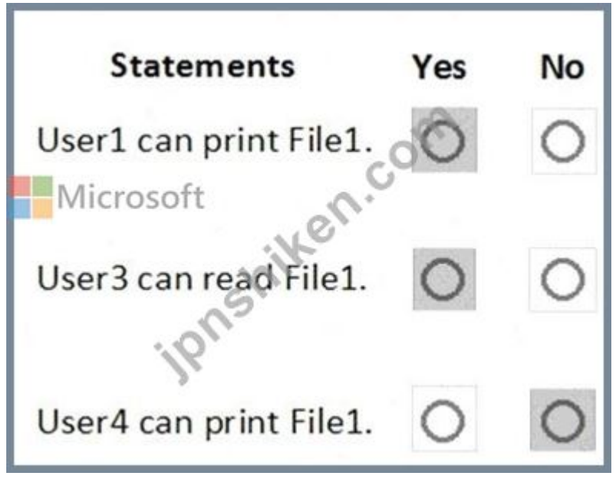
注意: 正しい選択ごとに 1 ポイントが付与されます。

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

正解:

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

Explanation:



質問: 72

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。

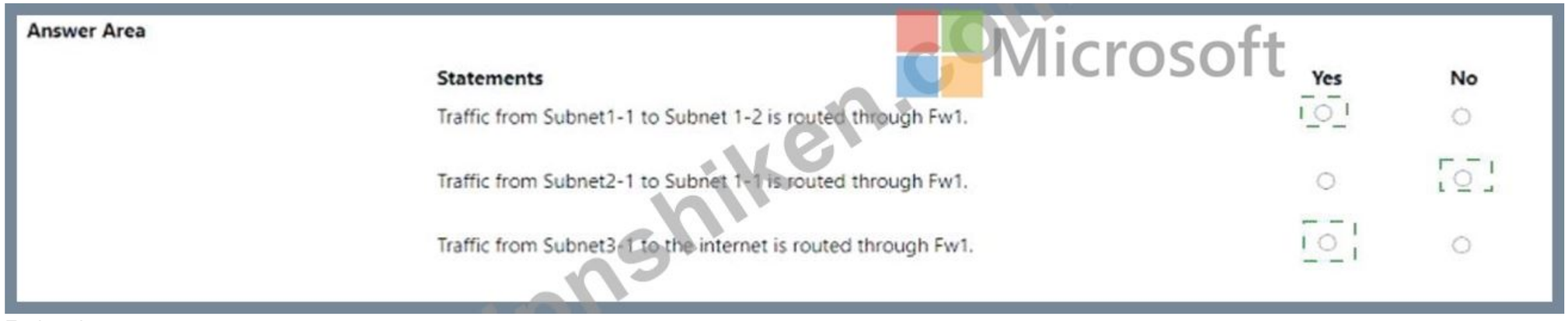
Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

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。

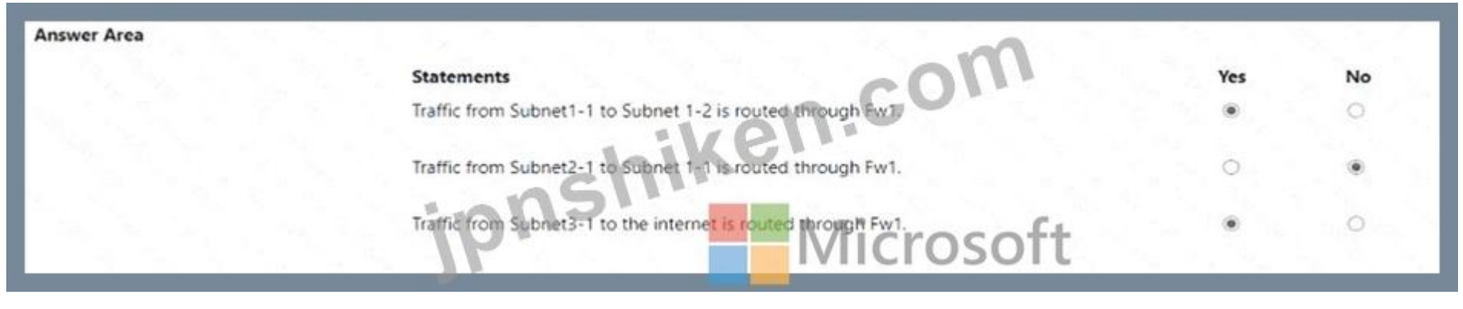
Answer Area

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:



jpnshiken.com
Microsoft

質問: **73**
EASM1 という名前の Microsoft Defender 外部攻撃対象領域管理 (Defender EASM) リソースを含む Azure サブスクリプションがあります。攻撃対象領域の概要ダッシュボードを確認します。次の洞察を特定する必要があります。
* サポートされなくなった非推奨のテクノロジー
* もうすぐ期限切れになるインフラストラクチャ
ダッシュボードのどのセクションを確認する必要がありますか?
A. クラウドの保護
B. 機密性の高いサービス
C. 攻撃対象領域の構成
D. 攻撃対象領域の優先順位
正解: (正解を表示します)

質問: **74**
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: **75**
User1、User2、User3 という名前の 3 人のユーザーを含む Microsoft Entra テナントがあります。
次の図に示すように、Microsoft Entra パスワード保護を構成します。



ユーザーは次のタスクを実行します。
* ユーザー1はパスワードをCOntOsOにリセットしようとします
* ユーザー2はパスワードをF@brikamHQにリセットしようとします
* User3 は PrOduct123 へのパスワードをリセットしようとします。
どのパスワード リセット試行が失敗しますか?
A. ユーザー1のみ
B. ユーザー2のみ
C. ユーザー1、ユーザー2、ユーザー3
D. ユーザー1とユーザー3のみ
E. ユーザー3のみ
正解: (正解を表示します)

質問: **76**
仮想ネットワークを含むAzureサブスクリプションがあります。仮想ネットワークには、次の表に示すサブネットが含まれています。

Name	Has a network security group (NSG) associated to the virtual subnet
Subnet1	Yes
Subnet2	No

サブスクリプションには、次の表に示す仮想マシンが含まれています。

Name	Has an NSG associated to the network adaptor of the virtual machine	Connected to
VM1	No	Subnet1
VM2	No	Subnet2
VM3	No	Subnet1
VM4	Yes	Subnet2

すべての仮想マシンに対してジャストインタイム (JIT) VM アクセスを有効にします。
JIT によって保護されている仮想マシンを特定する必要があります。
どの仮想マシンを識別する必要がありますか?

A. VM4のみ
B. VM1とVM3のみ
C. VM1、VM3、VM4のみ
D. VM1、VM2、VM3、VM4

正解: **C** (コメントを発表する)
An NSG needs to be enabled, either at the VM level or the subnet level.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

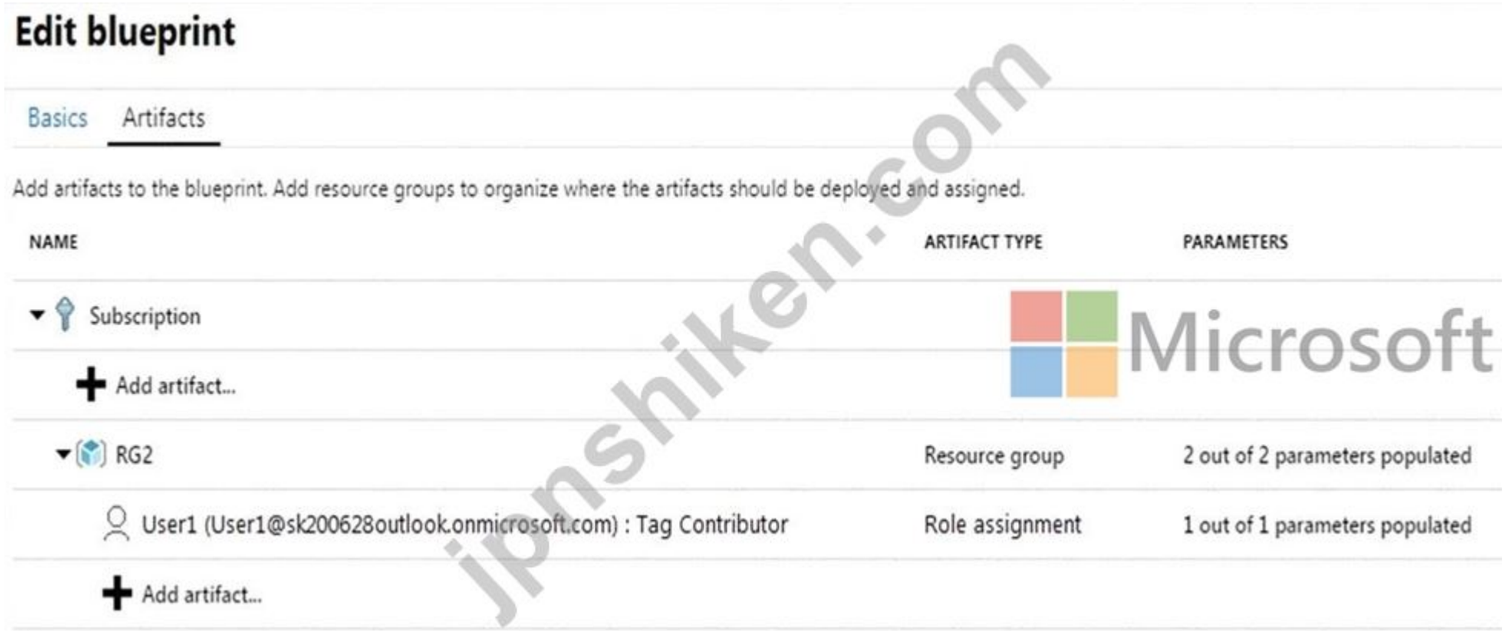
有効的な**AZ-500J**問題集はJPNTest.com提供され、**AZ-500J**試験に合格することに役に立ちます！JPNTest.comは今最新**AZ-500J**試験問題集を提供します。JPNTest.com AZ-500J試験問題集はもう更新されました。ここで**AZ-500J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AZ-500J-mondaishu　**520**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
Azureキーコンテナーと Azure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。Key Vaultには、顧客管理のキーが含まれています。ストレージアカウントは、Key Vaultに格納されている顧客管理のキーを使用するように構成されています。
次のサービスを使用してAzureにデータを格納する予定です。
* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.
NOTE: Each correct selection is worth one point.

A. Queue storage
B. Table storage
C. Azure Files
D. Blob storage
正解: (正解を表示します)
https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal

質問: **78**
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。



正解:



Explanation:

Graphical user interface, text, application Description automatically generated



Reference:

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

質問**: 79**

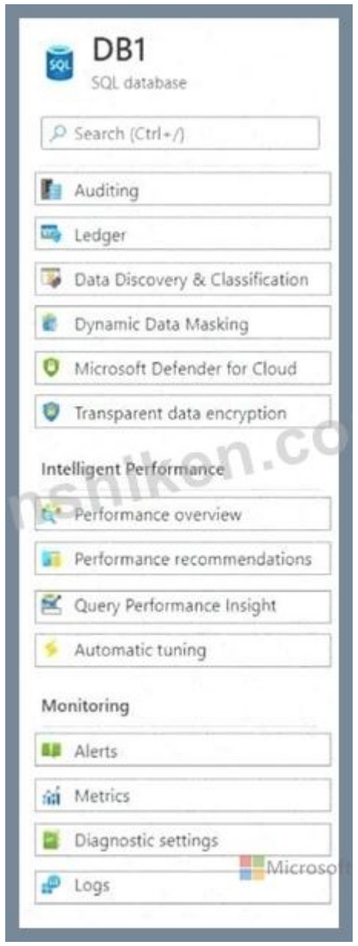
DB1 という名前の Azure SQL データベースがあり、Table という名前のテーブルが含まれています。

次の要件を満たすように DB1 を構成する必要があります。

* 表 1 の機密データは自動的に識別される必要があります。
* クエリ結果には機密データの最初の文字と最後の文字のみが表示される必要があります。

どの 2 つの機能を設定する必要がありますか? 回答するには、回答領域で特徴を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。


DB1
SQL database
Search (Ctrl+/)
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
Microsoft Defender for Cloud
Transparent data encryption
Intelligent Performance
Performance overview
Performance recommendations
Query Performance Insight
Automatic tuning
Monitoring
Alerts
Metrics
Diagnostic settings
Logs

正解:



Explanation:

1. Data Discovery & Classification
2. Dynamic Data Masking

https://learn.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azuresql

Data Discovery & Classification is built into Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It provides basic capabilities for discovering, classifying, labeling, and reporting the sensitive data in your databases.

質問: 80

お客様は、以下のリソースを含むマルチクラウド環境をお持ちです。
* Azure サブスクリプション
* Google Cloud Platform (GCP) プロジェクト
* Amazon Web Services (AWS) アカウント
セキュリティ体制を強化する規制基準を割り当てるには、Microsoft Defender for Cloud を使用する必要があります。すべてのクラウド環境に適用できる規制基準はどれですか？
A. NIST 800-53
B. システムおよび組織管理(SOC)2 タイプ2
C. ISO 27001
D. インターネットセキュリティセンター (CIS)
正解: (正解を表示します)

質問: **81**
AzureStorageアカウントのセキュリティ問題のトラブルシューティングを行っています。
ストレージアカウントの診断ログを有効にします。診断ログを取得するには何を使用する必要がありますか？
A. the Security & Compliance admin center
B. SQL query editor in Azure
C. File Explorer in Windows
D. AzCopy
正解: (正解を表示します)
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%
2fblobs%2ftoc.json

質問: **82**
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。
3つのAzureサブスクリプションの集中ポリシー管理にAzureSecurityCenterを使用します。
サブスクリプションのセキュリティを管理するには、いくつかのポリシー定義を使用します。
ポリシー定義をグループとして3つのサブスクリプションすべてに展開する必要があります。
解決策 :テナントルートグループ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: **A** (コメントを発表する)
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

質問: **83**

お客様は、3つのストレージアカウント、SQL1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Azure SQLデータベースを含むAzureサブスクリプションを所有しています。
ストレージアカウントは、以下の表に示すように構成されています。

Name	Type	Performance
storage1	StorageV2	Standard
storage2	StorageV2	Standard
storage3	BlockBlobStorage	Premium

SQL1には以下の設定があります。
* 監査: オン
* 監査ログの保存先: ストレージ!
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。

Name	On server	Auditing	Audit log destination
DB1	SQL1	Off	*None*
DB2	SQL1	On	storage2
DB3	SQL1	Off	*None*

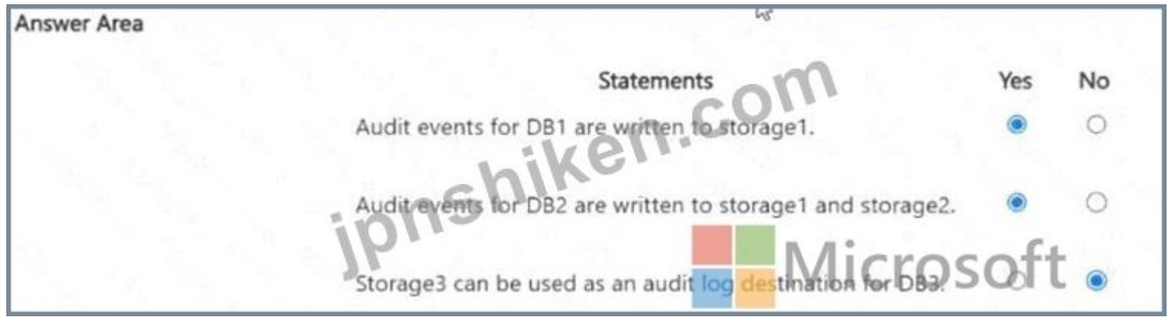
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



正解:

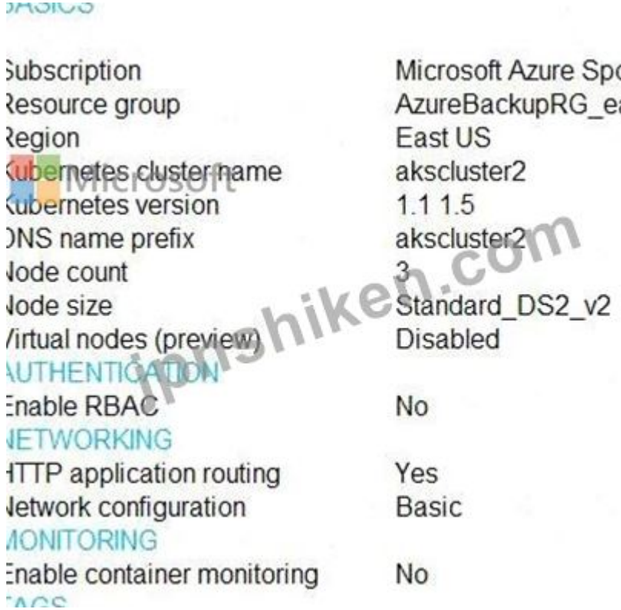


Explanation:



質問: 84

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。）



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: **85**

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	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

テナントに対して Azure AD Privileged Identity Management (PIM) が有効になっています。

PIM では、パスワード管理者ロールには次の設定があります。

* 最大有効化時間（時間）2
* 管理者に有効化を通知するメールを送信: 無効
* アクティベーション中にインシデント/リクエストチケット番号を要求する: 無効
* アクティベーションにAzure Multi-Factor Authenticationが必要: 有効
* このロールを有効にするには承認が必要: 有効
* 選択された承認者: グループ1

次の表に示すように、ユーザーにパスワード管理者ロールを割り当てます。

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

正解:



Explanation:
YES (Already active)
YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can ' t approve itself)
https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require approval section)

質問: **86**
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



jpnshiken.com

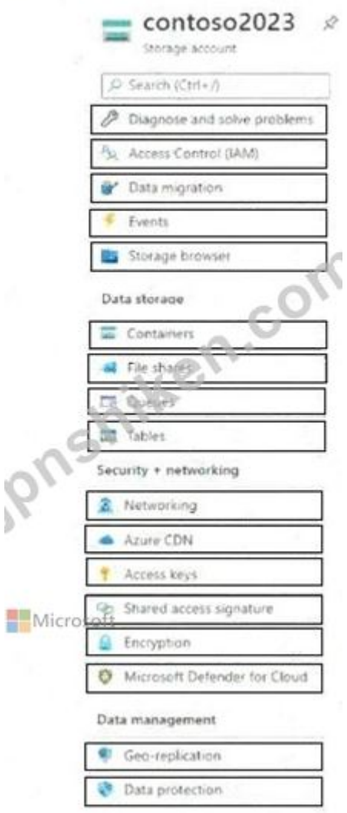
Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

質問**: 87**
ラボのタスク
タスク1
インターネットから VNET1\subnet0 への接続が TCP ポート 7777 経由でのみ許可されていることを確認する必要があります。ソリューションでは、現在デプロイされているリソースのみを使用する必要があります。
正解:
see the task answer with step by step below
Explanation:
You need to configure the Network Security Group that is associated with subnet0.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on Inbound Security Rules.
5. Click the Add button to add a new rule.
6. In the Source field, select Service Tag.
7. In the Source Service Tag field, select Internet.
8. Leave the Source port ranges and Destination field as the default values (* and All).
9. In the Destination port ranges field, enter 7777.
10.Change the Protocol to TCP.
11.Leave the Action option as Allow.
12.Change the Priority to 100.
13.Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.
14.Click the Add button to save the new rule.

質問**: 88**

contoso2023 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。次のタスクを実行する必要があります。
* SMB を介した ID ベースの認証が有効になっていることを確認します。
* 2023 年にのみユーザーに contoso2023 へのアクセスを許可します。
どの 2 つの設定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設定を選択してください。注: 正しい選択ごとに 1 ポイントの価値があります。

Answer Area



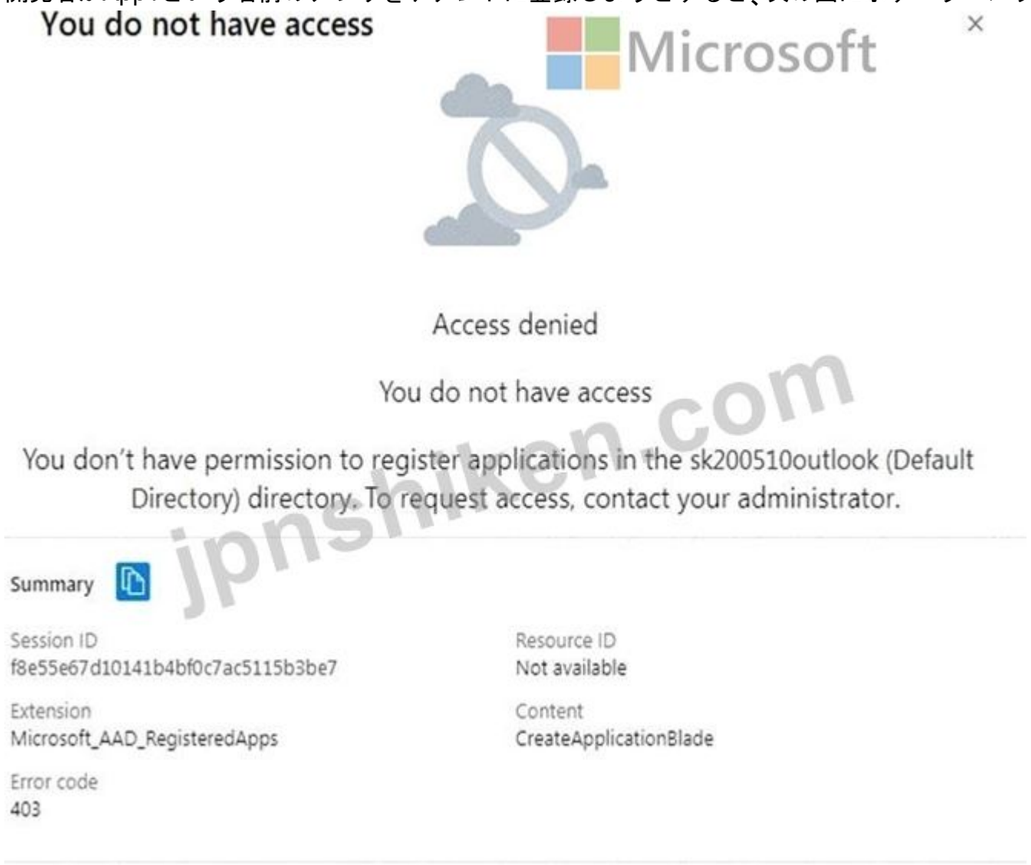
正解:



Explanation:
A screenshot of a computer Description automatically generated
Requirement: Verify that identity-based authentication over SMB is enabled Go there to configure Identity-based authentication (Active Directory) for Azure file shares.
Ref: https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview
2. Share access signature
Requirement: Only grant users access to contoso2023 in the year 2023

質問**: 89**
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: ユーザー割り当てのマネージド ID を使用するように AKS1 を構成し、そのマネージド ID に Azure Kubernetes Service クラスター管理者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**: B (**コメントを発表する**)**

質問: **90**
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: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

質問: **91**
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)

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**」

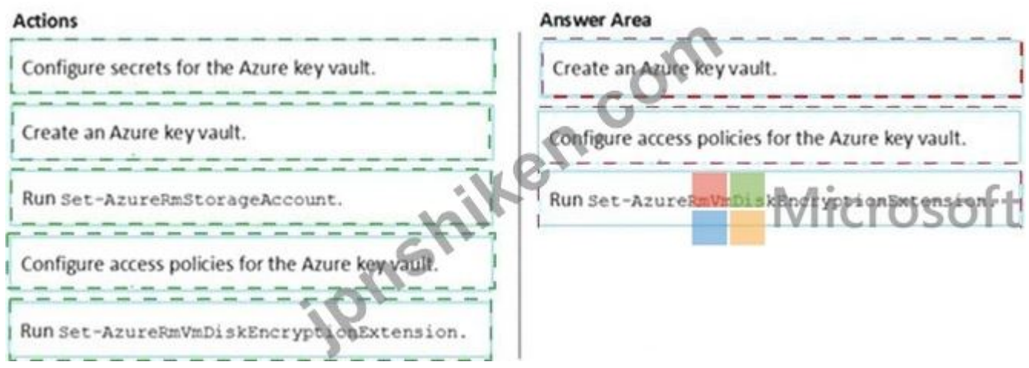
質問: **92**
あなたの会社は、部門ごとに個別のサブスクリプションを作成することを計画しています。各サブスクリプションは、同じ Azure Active Directory (Azure AD) テナントに関連付けられます。
同じロールが割り当てられるように各サブスクリプションを構成する必要があります。
何を使うべきですか？
A. Azure Security Center
B. Azure Policy
C. Azure AD Privileged Identity Management (PIM)
D. Azure Blueprints
正解: (正解を表示します)
Just as a 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: **93**
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:



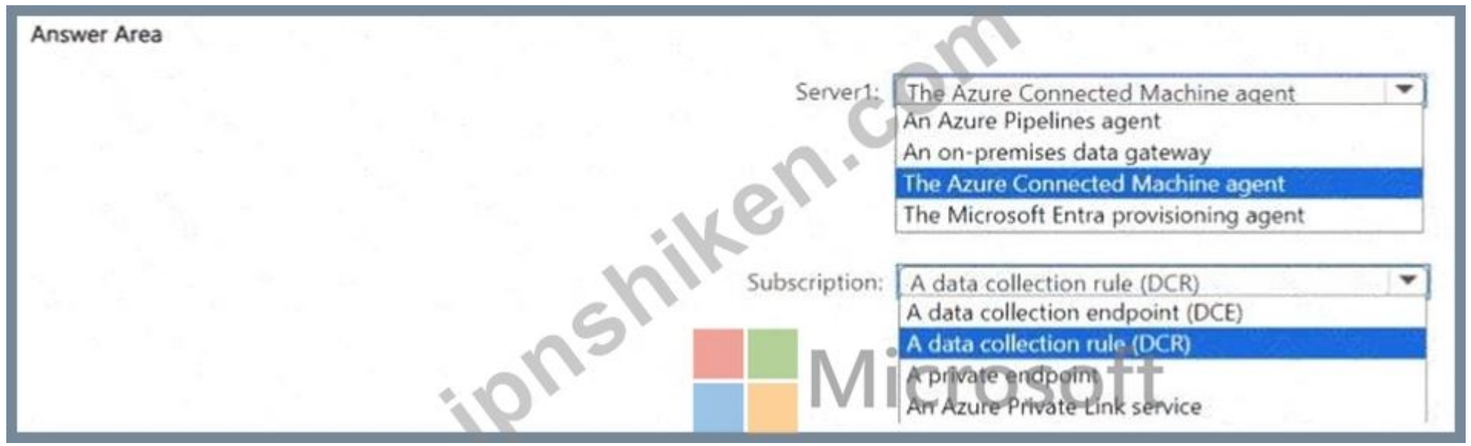
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

質問: **94**
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: (正解を表示します)
" 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: **95**
Server1 という名前のオンプレミス サーバーがあります。
Sentinel 1 という名前の Microsoft Sentinel 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。
Sentinel1 に Windows ファイアウォール ソリューションをインストールします。
Server1 上の Windows Defender ファイアウォールを監視するには、Microsoft Sentinel を使用する必要があります。
Server1 に何をインストールし、Azure サブスクリプションに何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: **96**

Azureコンテナーインスタンスを展開する予定です。

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

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

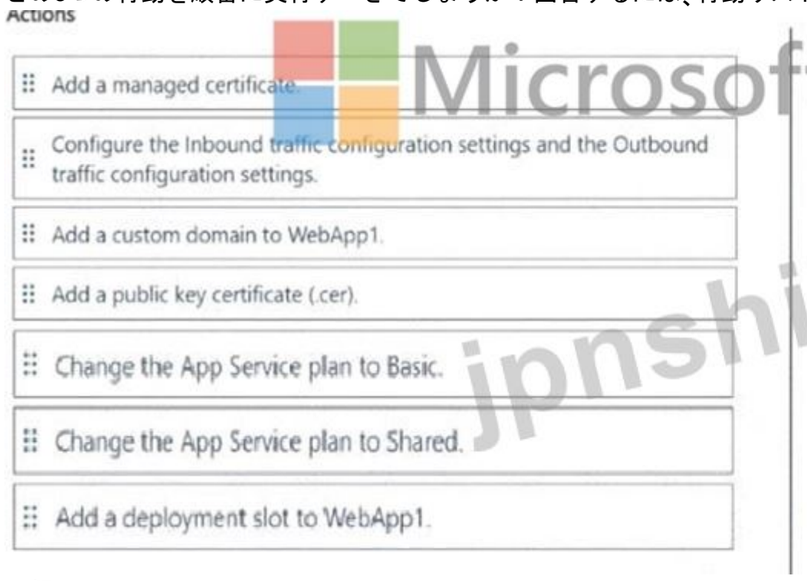
アプリケーションコンテナと検証コンテナが一緒にデプロイされるようにスケジュールされていることを確認する必要があります。コンテナは、外部に公開されていないポートでのみ互いに通信する必要があります。

展開に何を含める必要がありますか？

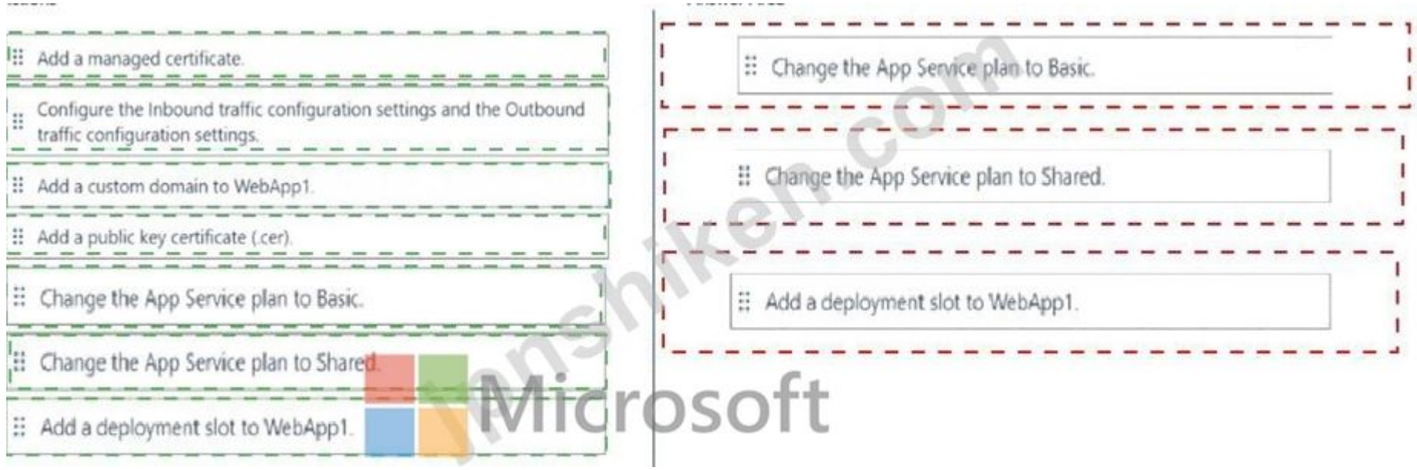
A. アプリケーションセキュリティグループ

B. ネットワークセキュリティグループ（NSG）
C. 管理グループ
D. コンテナグループ
正解: (正解を表示します)
Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

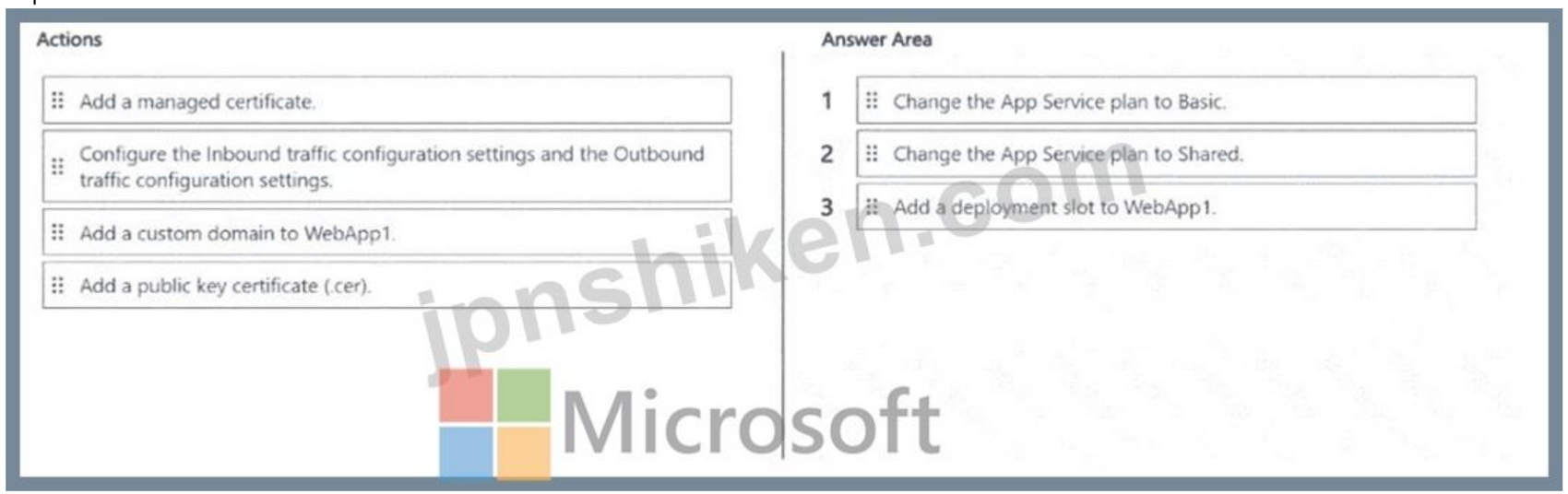
質問: **97**
お客様は、以下の Azure App Service Web アプリを含む Azure サブスクリプションをお持ちです。
* 名前: WebApp1
* アプリサービスプラン：無料
WebApp1でApp Service管理証明書を使用するように構成する必要があります。このソリューションはコストを最小限に抑える必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:



質問: 98

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。

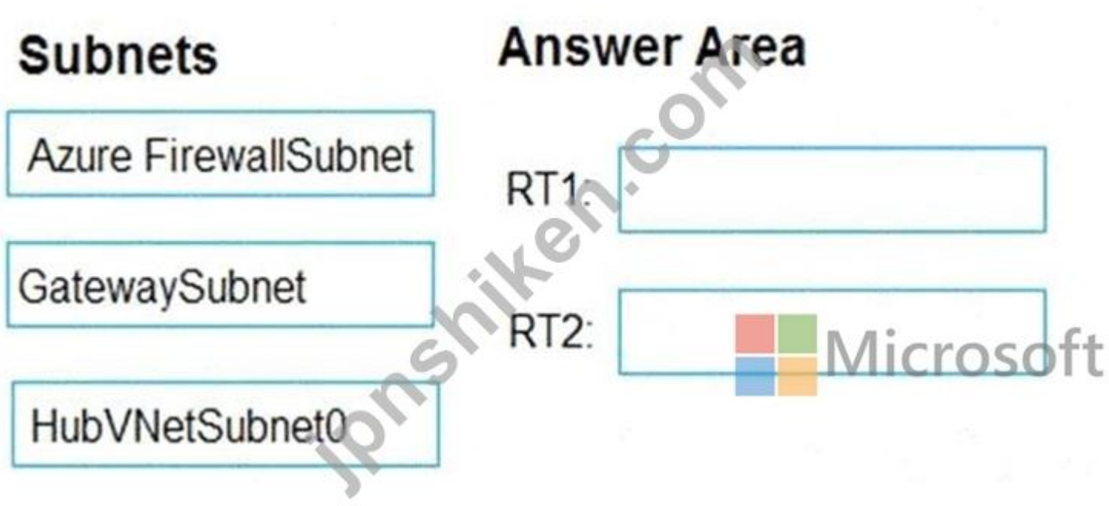
D. [ユーザー]ブレードで、外部コラボレーション設定を変更します。

正解: (正解を表示します)
You need to allow guest invitations in the External collaboration settings.

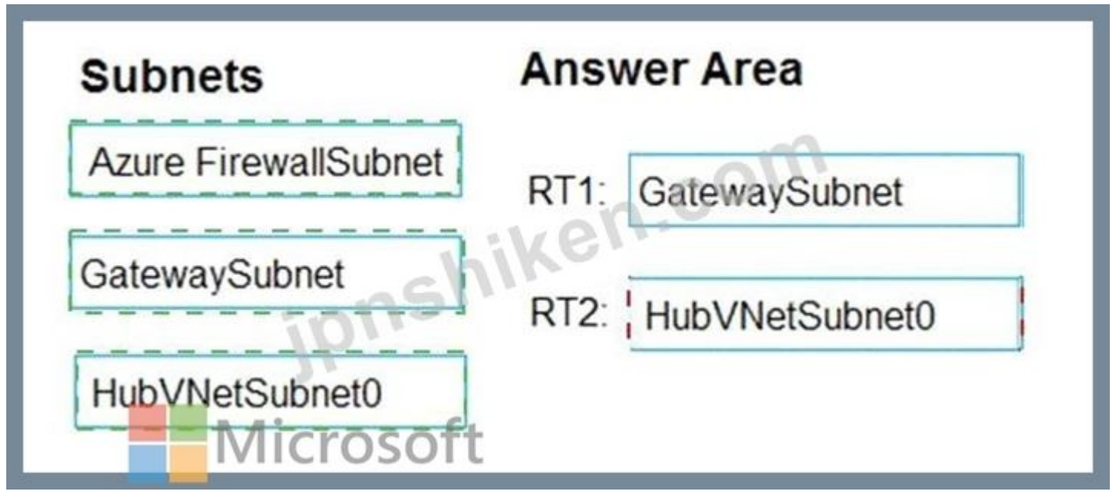
質問: **99**
次の表に示す仮想ネットワークを含むAzureサブスクリプションがあります。

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

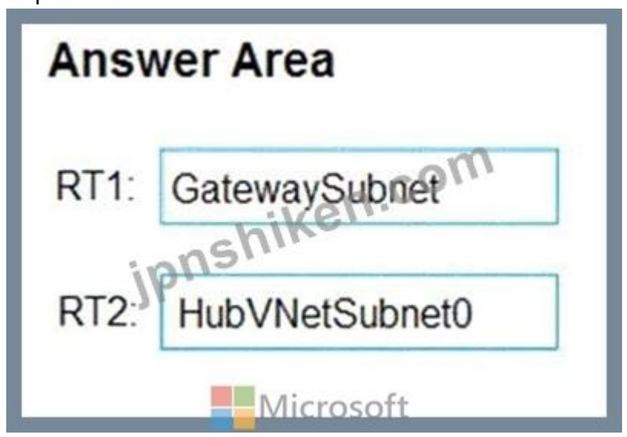
SpokeVNetSubnet0上のAzure仮想マシンは、オンプレミスネットワーク上のコンピューターと通信できます。
Azureファイアウォールを HubVNetに展開する予定です。
次の2つのルーティングテーブルを作成します。
* RT1 :ネクストホップアドレスとしてAzureファイアウォールのプライベートIPアドレスを指すユーザー定義のルートが含まれます
* RT2 :BGPルート伝播を無効にし、Azureファイアウォールのプライベート IPアドレスをデフォルトゲートウェイとして定義するSpokeVNetSubnet0とオンプレミスネットワーク間のトラフィックがAzureファイアウォールを通過することを確認する必要があります。
どのサブネットに各ルートテーブルを関連付ける必要がありますか？答えるには、適切なサブネットを正しいルートテーブルにドラッグします。各サブネットは、1回、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:



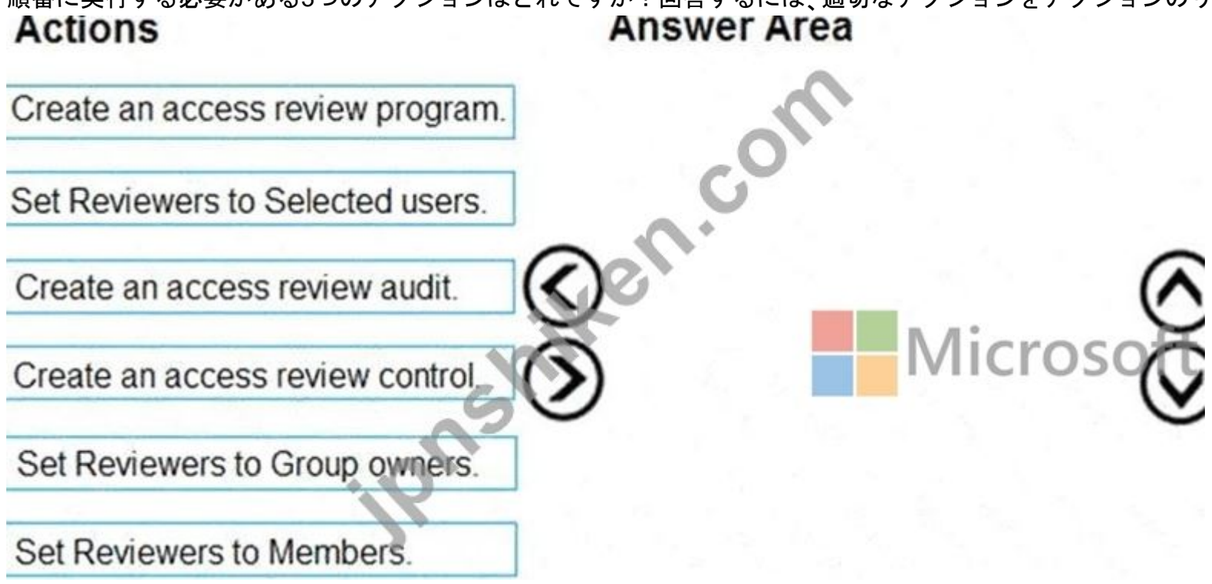
Explanation:



質問: **100**
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: **101**
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**: 102**
オンプレミスのデータセンターがあります。
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。VNet1 は、サイト間 (S2S) VPN を使用してオンプレミスのデータセンターに接続されています。
storage1 および App1 という名前の Azure ストレージ アカウントを作成する予定です。
各リソースへのネットワーク通信が次の要件を満たしていることを確認する必要があります。
* App1 への接続は、企業ネットワークの NAT アドレスからのみ許可する必要があります。
* VNet1 から storage1 への接続には、Microsoft バックボーン ネットワークを使用する必要があります。
* ソリューションはコストを最小限に抑える必要があります。
各リソースにはどのような設定が必要ですか？適切なコンポーネントを適切なリソースにドラッグしてください。各コンポーネントは1回だけ使用される場合もあれば、複数回使用される場合もあり、まったく使用されない場合もあります。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: **103**

次の設定を持つアラート ルールを作成します。

* リソース: RG1
* 条件: すべての管理操作
* アクション: このアラートルールに構成されたアクショングループ: ActionGroup1
* アラートルール名: Alert1

次の設定を持つアクション ルールを作成します。

* スコープ: VM1
* フィルター条件: リソースタイプ = "仮想マシン"
* このスコープで定義: 抑制
* 抑制設定: 今から（常に）
* 名前: アクションルール1

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

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

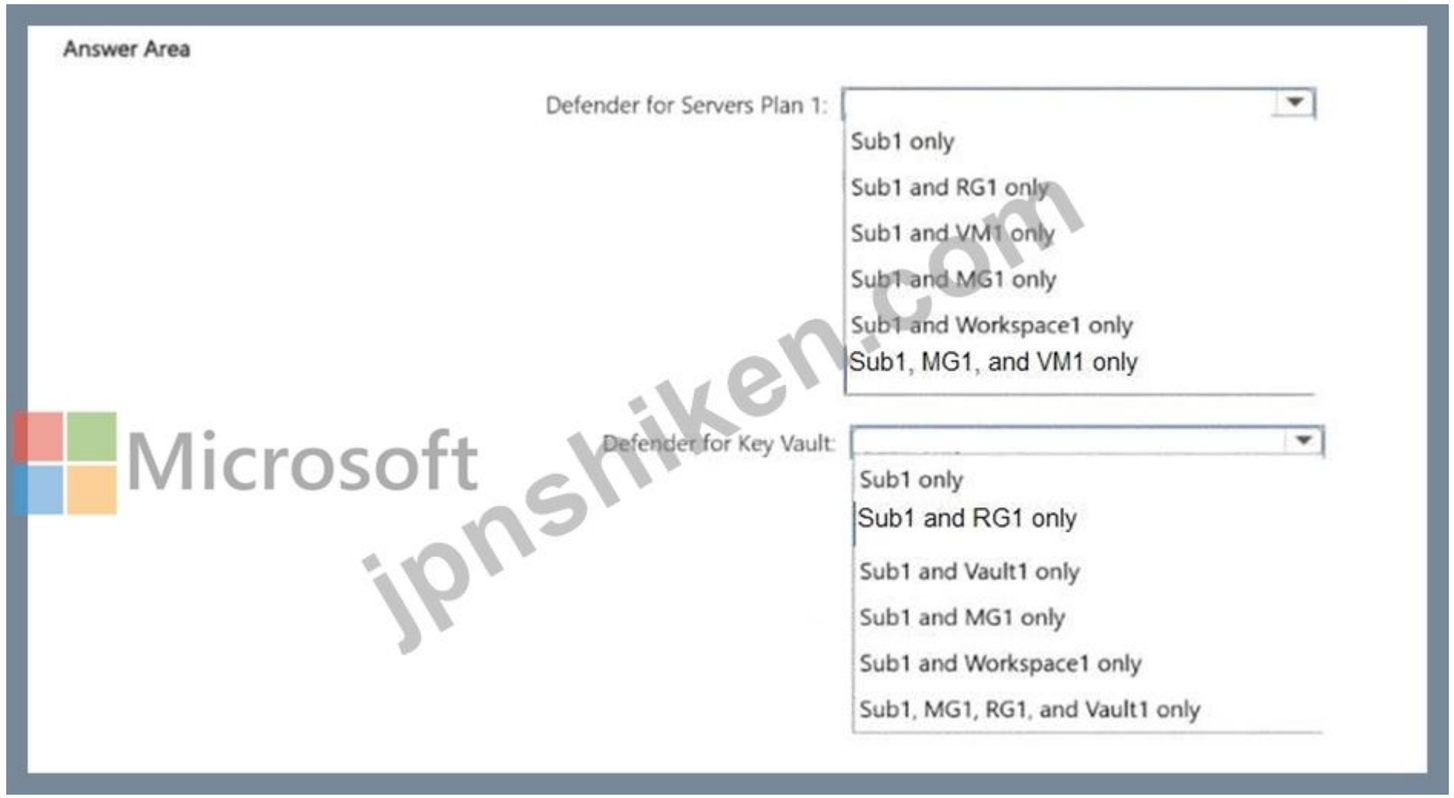


Box 1:
The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.
Box 2:
The scope for the action rule is not set to VM2.
Box 3:
Adding a tag is not an administrative operation.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules

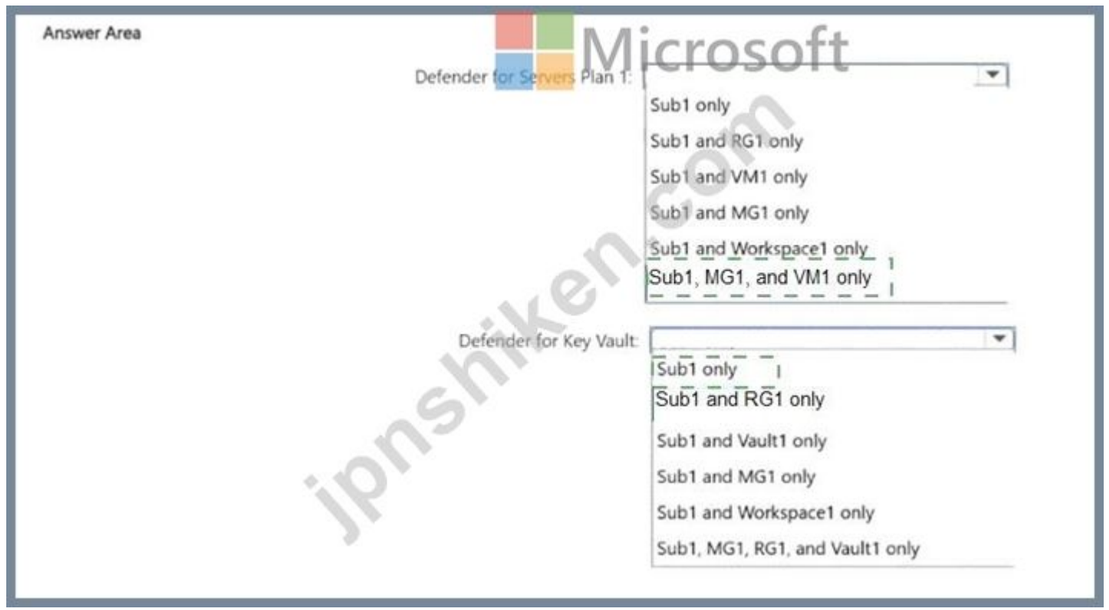
質問: **104**
MG1 という名前の管理グループがあり、その中に Sub1 という名前の Azure サブスクリプションがあります。Sub1 には、次の表に示すリソースが含まれています。

Name	Description
RG1	Resource group
VM1	Virtual machine
Vault1	Azure key vault
Workspace1	Log Analytics workspace

Sub1 のリソースを保護するには、Microsoft Defender for Servers Plan1 と Microsoft Defender for Key Vault を使用します。
Azure ポータルから、どのリソースで Defender for Servers Plan 1 を有効にできますか。また、どのリソースで Defender for Key Vault を有効にできますか。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：正解ごとに1ポイントが加算されます。



正解:



Explanation:



質問: **105**

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": []
        }
    ]
```

jpnshiken.com
Microsoft

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.	○	○

Microsoft
jpnshiken.com

正解:



Explanation:



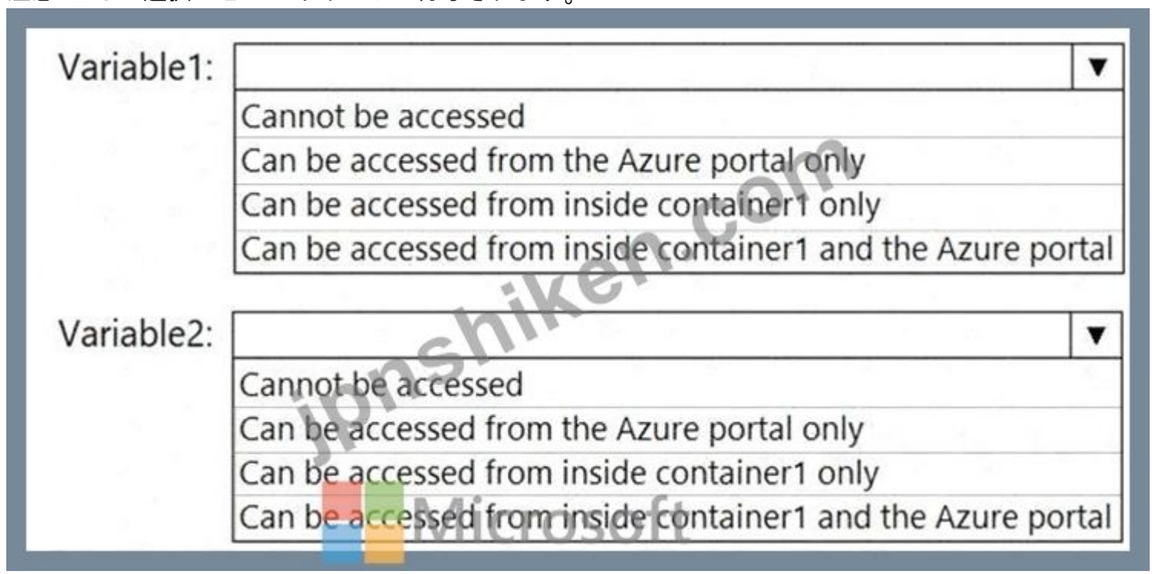
質問: 106

次の内容を含む File1.yaml という名前のファイルがあります。

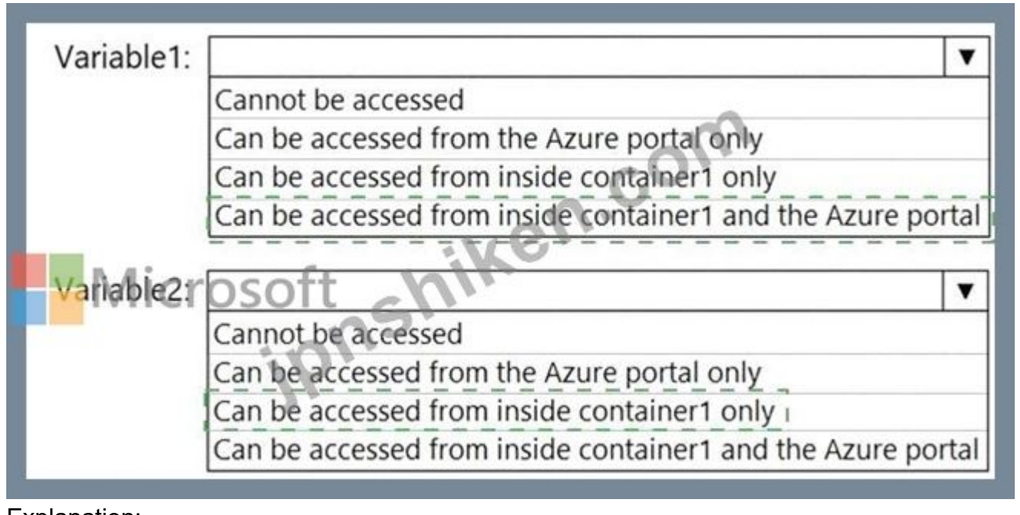
```
apiVersion: 2018-10-01
location: eastus
name: containergroup1
properties:
  containers:
  - name: container1
    properties:
      environmentVariables:
        - name: 'Variable1'
          value: 'Value1'
        - name: 'Variable2'
          secureValue: 'Value2'
      image: nginx
      ports: []
      resources:
        requests:
          cpu: 1.0
          memoryInGB: 1.5
  osType: Linux
  restartPolicy: Always
tags: null
type: Microsoft.ContainerInstance/containerGroups
```

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。

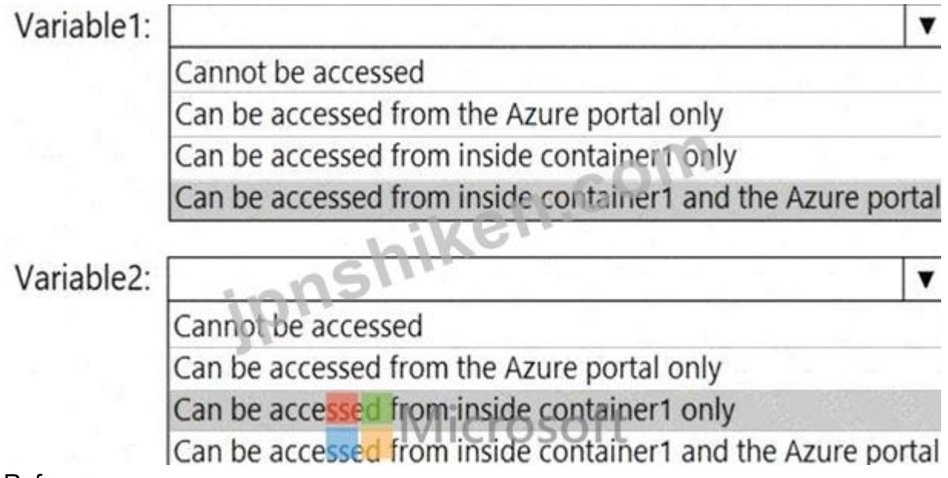
Variable1 と Variable2 の値にアクセスできる場所を特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



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

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**」

質問: **107**
仮想マシンを含む Azure サブスクリプションがあります。
すべての仮想マシンへのジャストインタイム (JIT) VM アクセスを有効にします。
リモート デスクトップを使用して仮想マシンに接続する必要があります。
まず何をすべきでしょうか?
A. Azure Directory (Azure AD) Privileged Identity Management (PIM) から、セキュリティ管理者ユーザー ロールをアクティブ化します。
B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) から、仮想マシンの所有者ロールをアクティブ化します。
C. Azure ポータルから仮想マシンを選択し、[接続] を選択して、[アクセスの要求] を選択します。
D. Azure ポータルから仮想マシンを選択し、Network Watcher Agent 仮想マシン拡張機能を追加します。
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

質問: **108**
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: **109**
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: **A** (コメントを発表する)
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

質問: **110**
MicrosoftSentinelを使用するAzureサブスクリプションがあります。
ガイド付き調査-異常ルックアップテンプレートを使用するMicrosoftSentinelノートブックを作成する必要があります。
最初に何を作成する必要がありますか？
A. AzureMachineLearningワークスペース
B. ハンティングクエリ
C. LogAnalyticsワークスペース
D. 分析ルール
正解: (正解を表示します)

質問: **111**
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 4
user2-28681041 という名前のユーザーが、RG1lod28681041 リソース グループ内の仮想マシンのプロパティを管理できるようにする必要があります。このソリューションでは、最小特権の原則を使用する必要があります。
正解:
Check below steps in explanation for Task
Explanation:
To ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group using the principle of least privilege, you can follow these steps:
In the Azure portal, search for and select the resource group named RG1lod28681041.

In the left pane, select Access control (IAM).
Select Add.
In the Add role assignment pane, enter the following information:
Role: Select the appropriate role for your scenario. For example, Virtual Machine Contributor.
Assign access to: Select User, group, or service principal.
Select: Enter the name of the user you want to assign the role to. For example, user2-28681041.
Select Save.
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

質問: **112**
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: MM 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: **113**
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: UserI -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 5
131-107.0.0/16 サブネットに接続されているデバイスのみが、rg1lod28681041 Azure ストレージ アカウントのデータにアクセスできるようにする必要があります。
正解:
Check below steps in explanation for Task
Explanation:
To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:
In the Azure portal, search for and select the storage account named rg1lod28681041.
In the left pane, select Firewalls and virtual networks.
In the Firewalls and virtual networks pane, select Selected networks.
In the Selected networks pane, select Add existing virtual network.
In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.
Select Add.
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

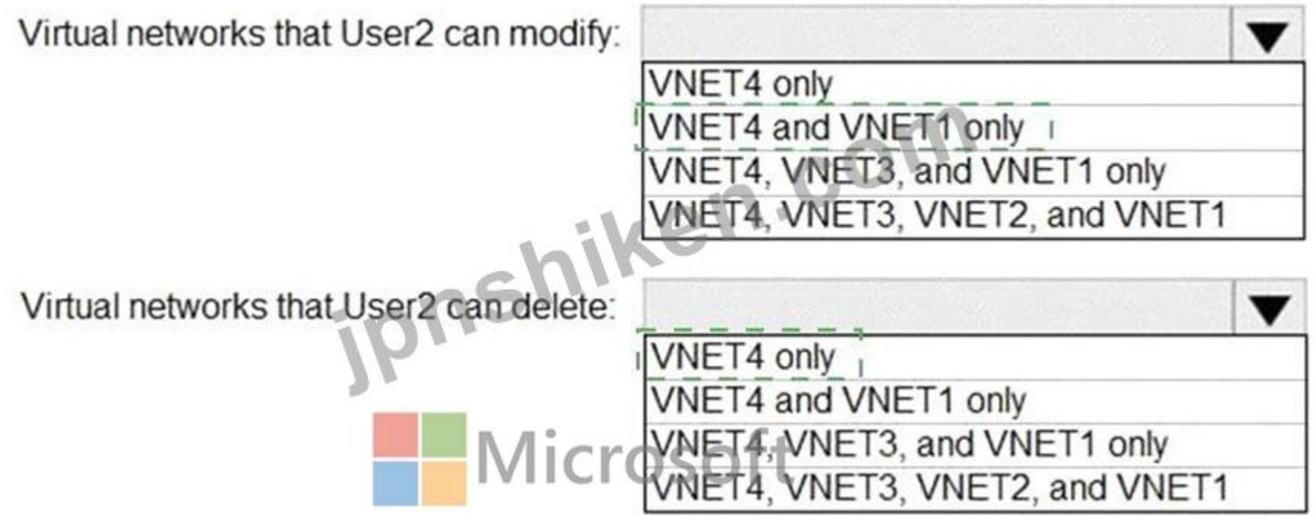
質問: **114**
ラボのタスク
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン] ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力します。[パスワードの入力] ボックスにカーソルを置き、下のパスワードをクリックします。
Azure ユーザー名: UserI -28681041@ExamUsers.com
Azure パスワード: GpOAe4@lDg
Azure portal がブラウザーに正常に読み込まれない場合は、CTRL-K を押して、新しいブラウザー タブでポータルを再読み込みします。
次の情報は、テクニカル 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1
インターネットから VM1 という名前の仮想マシンへの RDP 接続を許可するように Azure を構成する必要があります。このソリューションでは、VM1 の攻撃面を最小限に抑える必要があります。
正解:
Check below steps in explanation for Task.
Explanation
To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:
Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.
Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.
Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.
To minimize the attack surface of VM1, you can use the following best practices:
Use a strong password for the local administrator account on the virtual machine.
Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.
Use Azure Security Center to monitor and protect your virtual machines.

質問: **115**
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

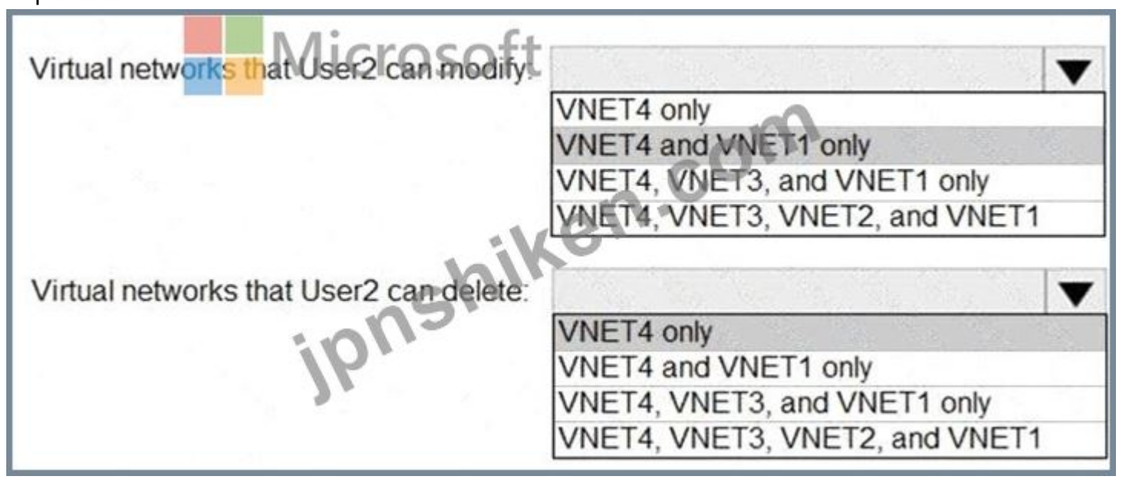
質問: **116**
現在の状態でUser2がSub1のどの仮想ネットワークを変更および削除できるか？回答するには、回答領域で適切なオプションを選択します。
注 :それぞれの正しい選択は1ポイントの価値があります。



正解:



Explanation:



Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

* CanNotDelete means authorized users can still read and modify a resource, but they can ' t delete the resource.
* ReadOnly means authorized users can read a resource, but they can ' t delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

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

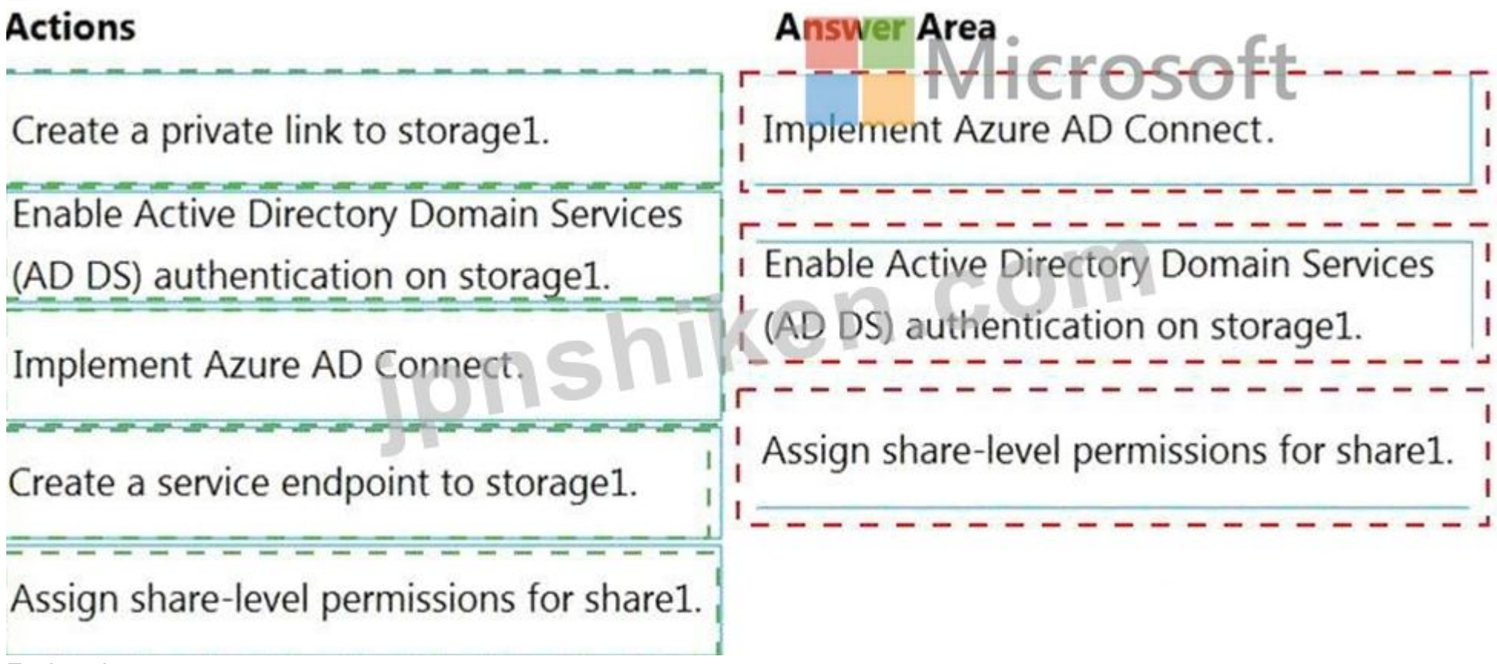
References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

質問: 117
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: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

質問: 118
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:



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

質問: **119**
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. [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。
D. [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。
正解: (正解を表示します)

質問: **120**
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: **121**

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. 新しいアプリ登録を作成します。

C. 多要素認証 (MFA) 登録ポリシーを構成します。

D. ユーザーに認証ポリシー管理者の役割を割り当てます。

正解: (正解を表示します)

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**」

質問: **122**

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 2
VM1 という名前の仮想マシンのネットワーク インターフェイスを ASG1 という名前のアプリケーション セキュリティ グループに追加する必要があります。
正解:
Check below steps in explanation for Task
Explanation:
To add the network interface of a virtual machine named VM1 to an application security group named ASG1, you can follow these steps:
In the Azure portal, search for and select the virtual machine named VM1.
In the left pane, select Networking.
In the Networking pane, select the network interface that you want to add to the application security group named ASG1.
In the network interface pane, select Application security groups.
In the Application security groups pane, select Add.
In the Add application security group pane, select the application security group named ASG1.
Select Save.
You can find more information on this topic in the following Microsoft documentation: Add a network interface to an application security group using the Azure portal.

質問: **123**
contoso.comという名前のAzure Active Directory（Azure AD）テナントを含むAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。

Name	Subscription role	Azure AD user role
User1	Owner	*None*
User2	Contributor	*None*
User3	Security Admin	*None*
User4	*None*	Service administrator

RG1という名前のリソースグループを作成します。
RG1のアクセス許可を変更できるユーザーと、RG1で仮想ネットワークを作成できるユーザーはどれですか。回答するには、回答領域で適切なオプションを選択します。
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。

Users who can modify the permissions for RG1:

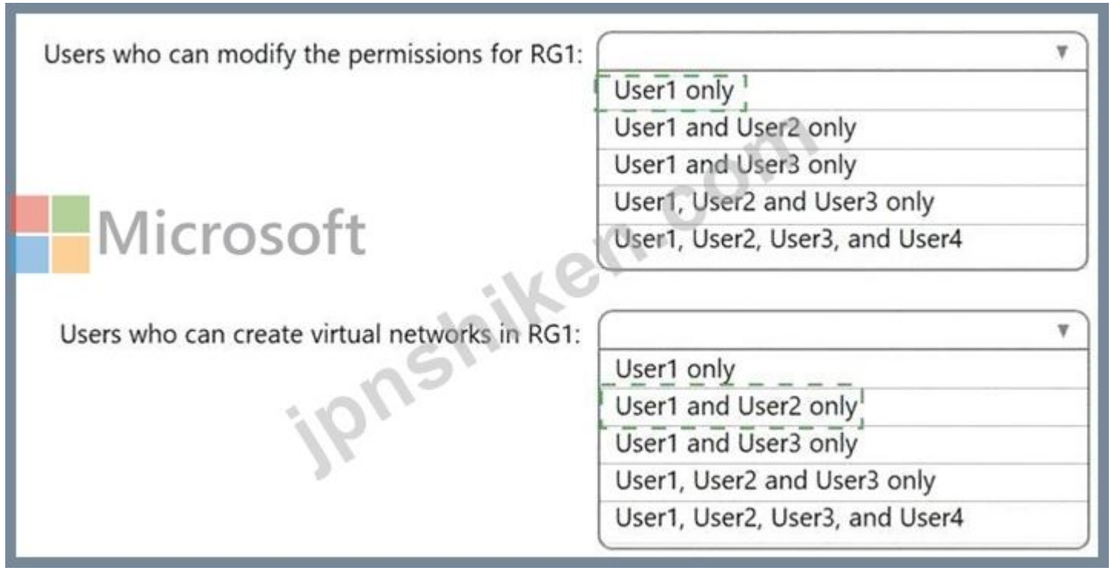
- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Users who can create virtual networks in RG1:

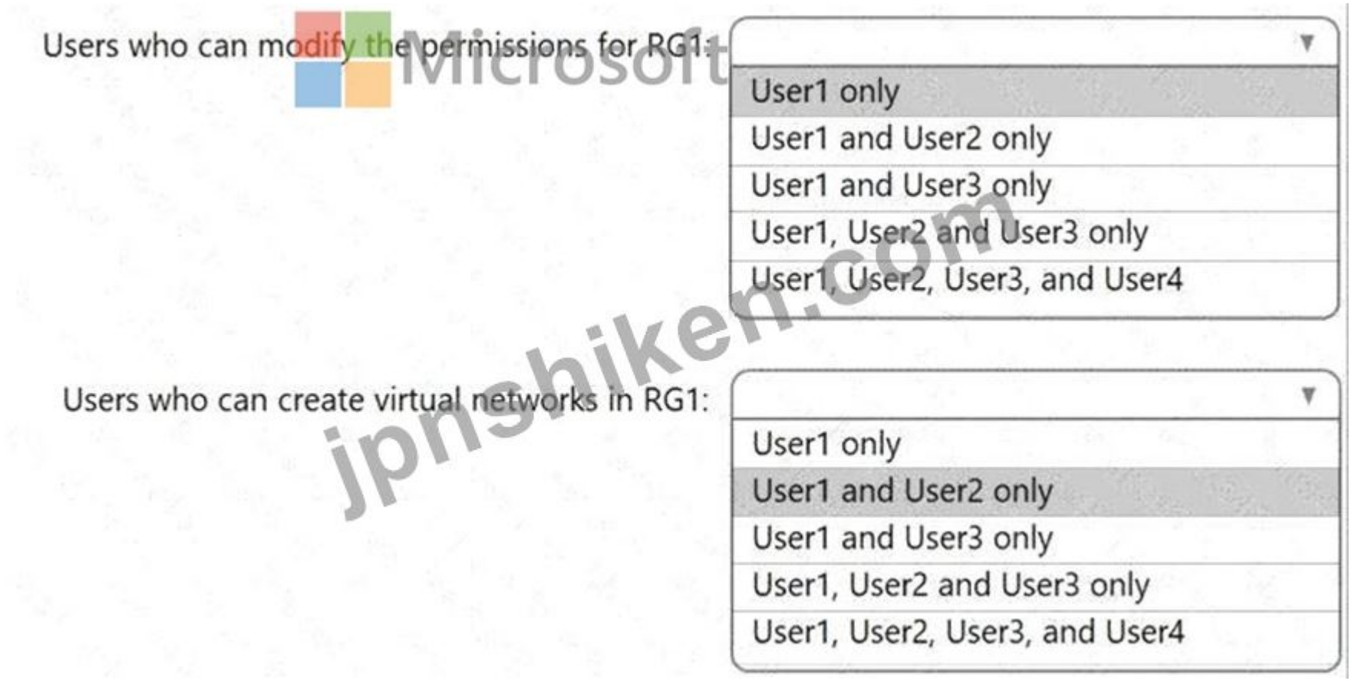
- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

jpnshiken.com
Microsoft

正解:



Explanation:



Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

質問: **124**

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

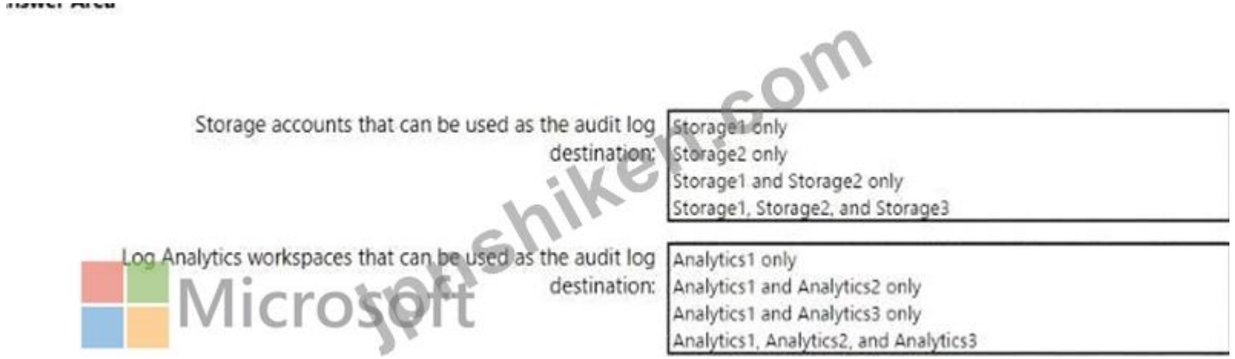
次の表に示す Azure ストレージ アカウントを作成します。

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	*Not applicable*
Storage3	West Europe	RG1	General purpose V2	Hot

SQL1 の監査を構成する必要があります。

監査ログの保存先として使用できるストレージ アカウントと Log Analytics ワークスペースはどれですか? 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。

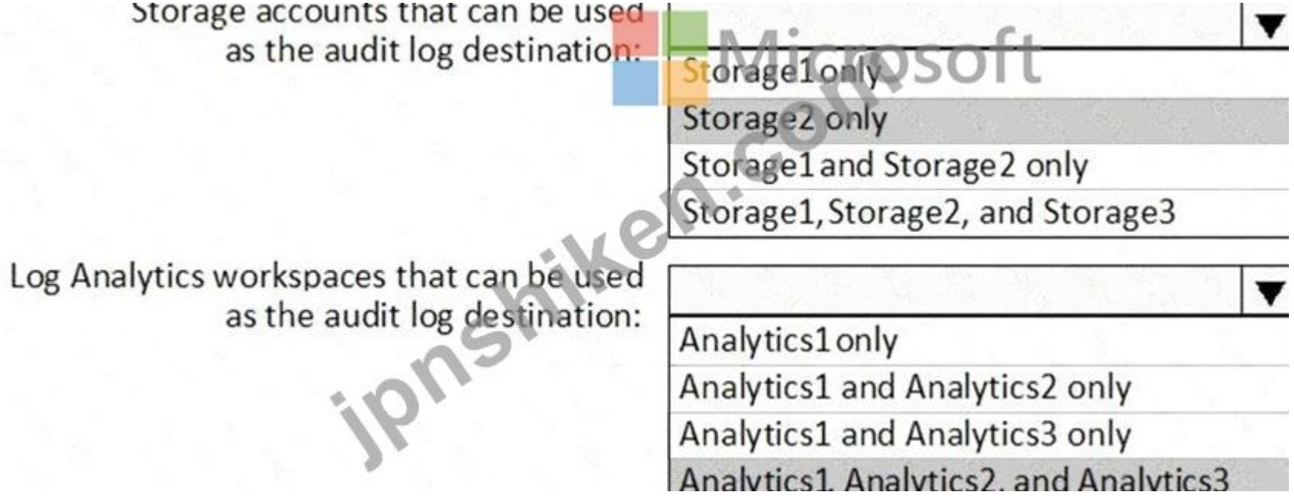
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問: **125**

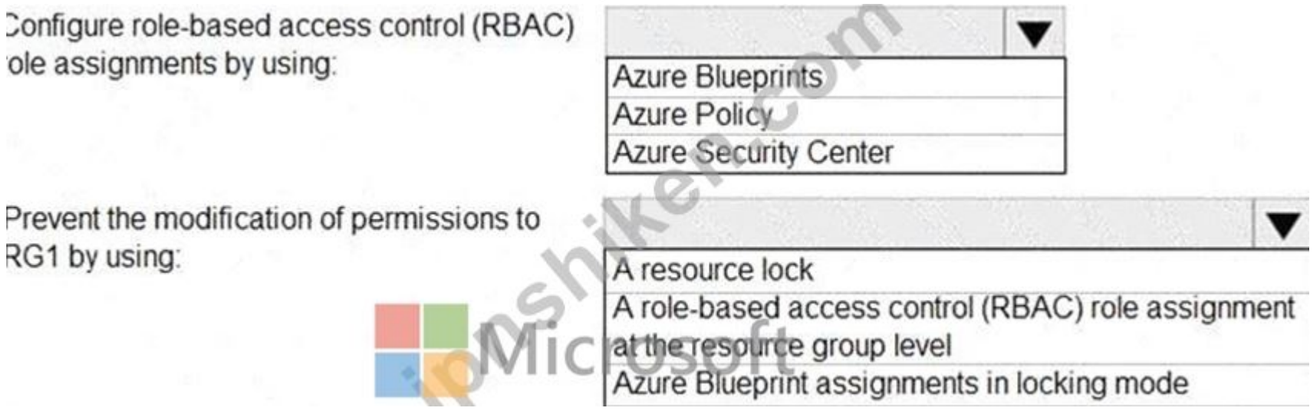
20個のAzureサブスクリプションと、Group1という名前のセキュリティグループがあります。サブスクリプションは、ルート管理グループの子です。

各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。

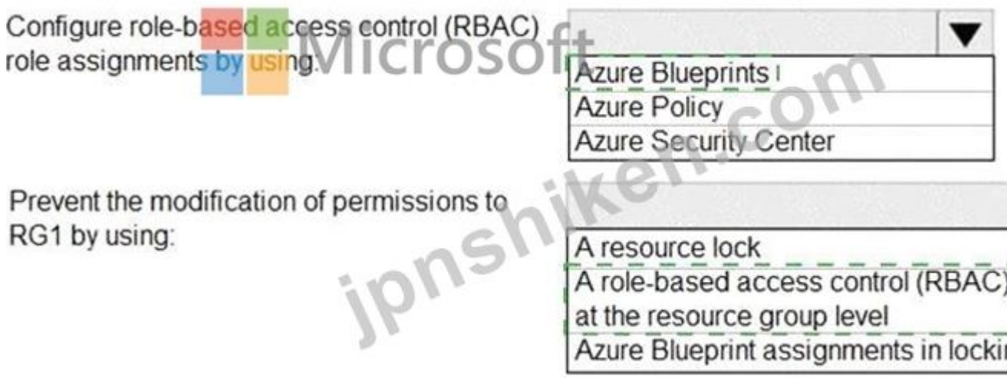
サブスクリプションごとに、RG1が次の要件を満たしていることを確認する必要があります。

* Group1のメンバーには所有者の役割が割り当てられます。
* RG1へのアクセス許可の変更は防止されます。

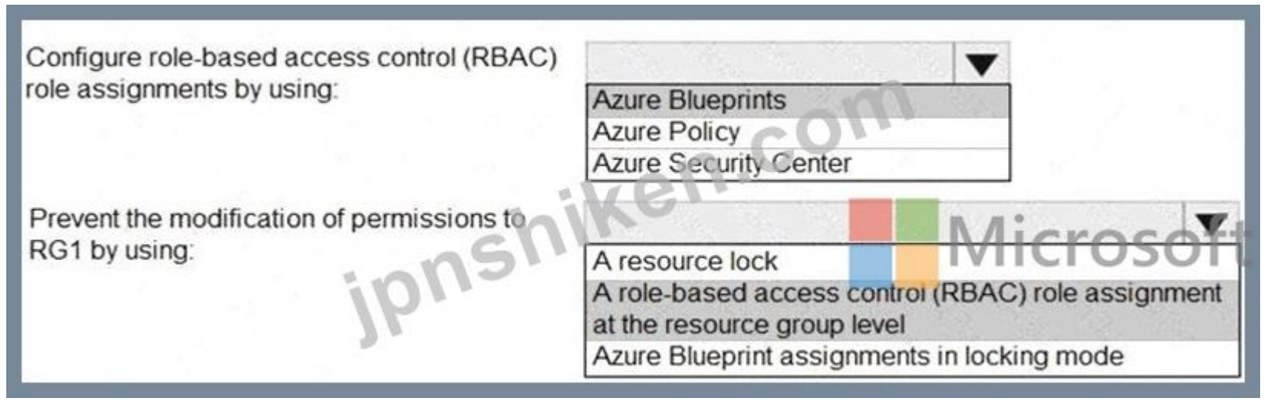
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。



正解:



Explanation:



質問: **126**
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。

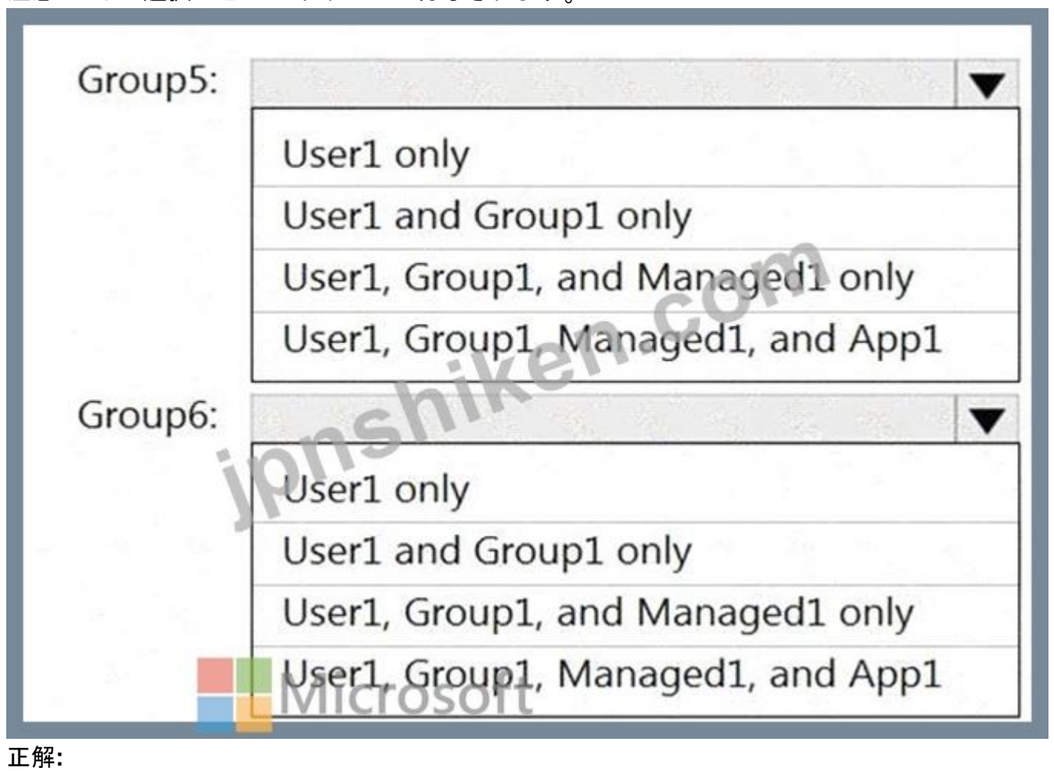
Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

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。

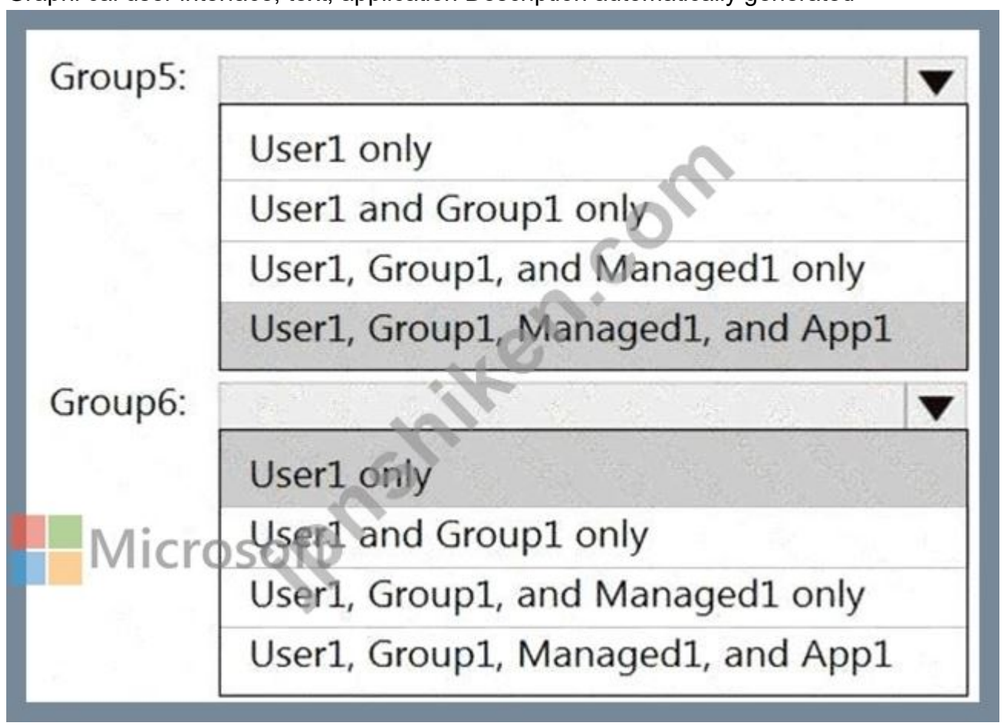


正解:



Explanation:

Graphi cal user interface, text, application Description automatically generated



質問: 127

Azure 環境があります。

ISO 27001:2013 標準に準拠していない Azure の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. Microsoft Defender for Identity
B. Microsoft Sentinel
C. Microsoft Defender for Cloud
D. Azure Active Directory (Azure AD) ID 保護
正解: **(**正解を表示します**)**

質問: **128**
次の表に示す仮想ネットワークを含む Azure サブスクリプションがあります。
サブスクリプションには、次の表に示す仮想マシンが含まれています。
次のリソースを含む contoso2024 という名前のストレージ アカウントがあります。
* File1 という名前のファイルを含む Contained という名前のコンテナ
* File2 という名前のファイルを含む Share1 という名前のファイル共有
次の図に示すように、contoso2024 のプライベート エンドポイントを作成します。

Create a private endpoint ...

Validation passed

✓ Basics ✓ Resource ✓ Virtual Network ✓ DNS ✓ Tags 6 Review + create

Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	East US
Name	PE1
Network Interface Name	PE1-nic

Resource

Subscription ID	a45b7def-a1cc-4700-afeb-80f3df1585fd (Azure Pass - Sponsorship)
Link type	Microsoft.Storage/storageAccounts
Resource group	RG1
Resource	contoso2024
Target sub-resource	blob

Virtual Network

Virtual network resource group	RG1
Virtual network	VNet2
Subnet	Subnet21
Network Policies	Disabled
Application security groups	None

jpnshiken.com
Microsoft

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: **129**
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: **130**

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をお持ちです。

VM1のネットワークインターフェイスに関連付けられたNSG1という名前のネットワークセキュリティグループ(NSG)があり、次の図に示すように構成されています。



Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

VM1ではジャストインタイム(JIT)VMアクセスが有効になっており、以下の構成になっています。

* 管理ポート: 3389、22
* 最大時間範囲 :3時間
* 許可される送信元IPアドレス: すべて

JITルールを有効にし、SSHを使用してVM1に接続します。

以下の各記述について、正しい場合は「はい」を、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
The RDP rule has priority over the NSG rule created by JIT.	○	○
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.	○	○
The SSH connection to VM1 disconnects automatically after three hours.	○	○

ipnshiken.com

正解:

Answer Area

Statements	Yes	No
The RDP rule has priority over the NSG rule created by JIT.	○	○
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.	○	○
The SSH connection to VM1 disconnects automatically after three hours.	○	○

Explanation:

Answer Area

Statements	Yes	No
The RDP rule has priority over the NSG rule created by JIT.	○	●
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.	○	●
The SSH connection to VM1 disconnects automatically after three hours.	○	●

Microsoft
jpnshiken.com

質問: **131**
storage 1 という名前の Azure Storage アカウントを作成する予定です。
ストレージ1に作成されるすべての新規オブジェクトが二重暗号化によって保護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、管理作業を最小限に抑えるものでなければなりません。
storage1を作成する際に、どのような設定を行うべきですか？
A. 暗号化タイプのオプション
B. インフラストラクチャ暗号化オプション
C. アクセス層
D. 最小TLSバージョン
正解: (正解を表示します)

質問: **132**
Azure サブスクリプションに、SQL1 という名前の Azure SQL データベースが含まれています。SQL1 を Always Encrypted を使用するように構成する必要があります。何を使用すればよいですか？
A. pgAdmin
B. Azureポータル
C. MySQL Workbench
D. Microsoft SQL Server Management Studio (SSMS)
正解: (正解を表示します)

質問: **133**
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: **(**正解を表示します**)**
References:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

質問: **134**
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。テナントには、次の表に示すグループが含まれています。

Name	Member of
Group1	*None*
Group2	Group1

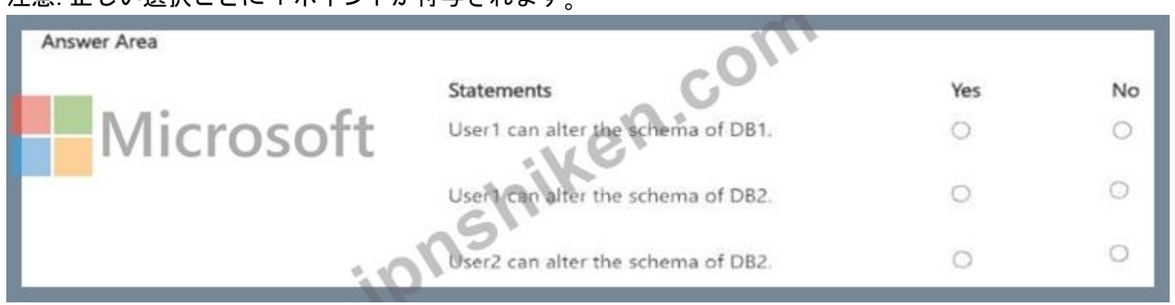
テナントには次の表に示すユーザーが含まれます。

Name	Member of
User1	Group1
User2	Group2

サブスクリプションには、次の表に示す Azure SQL サーバーが含まれています。

Name	Assigned server admin	Database
sqlsvr1	User1	DB1
sqlsvr2	Group1	DB2

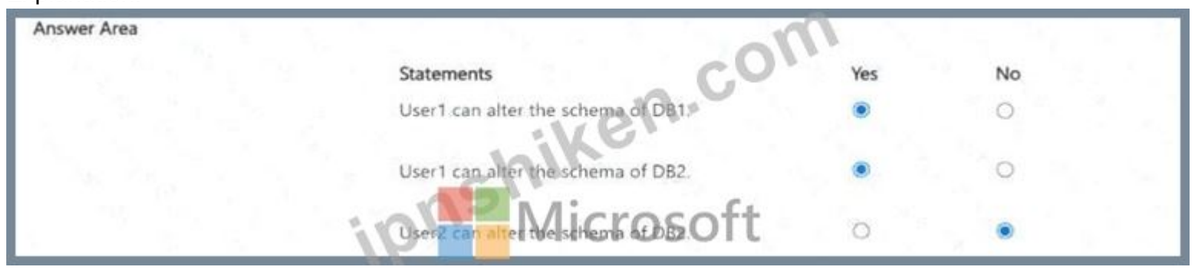
サーバーは Microsoft Entra のみの認証用に構成されています。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問: **135**

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: **D** (コメントを発表する)

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: **136**

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

すべての仮想マシンが同一のアプリケーションを実行します。

許可されていないアプリケーションやマルウェアが仮想マシンで実行され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 Active Directory (Azure AD) ID 保護を構成します。
B. Microsoft Defender for Cloud から、アダプティブ アプリケーション コントロールを構成します。
C. Azure ポリシーを RGI に適用します。
D. RGI 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**)**
Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.
Defender for Cloud helps you optimize and monitor the security of your virtual machines by:
* Providing security recommendations for the virtual machines. Example recommendations include:
apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
* Monitoring the state of your virtual machines.
https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

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**」

質問: **137**
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。



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!.	○	○

正解:



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!.	○	○

Explanation:

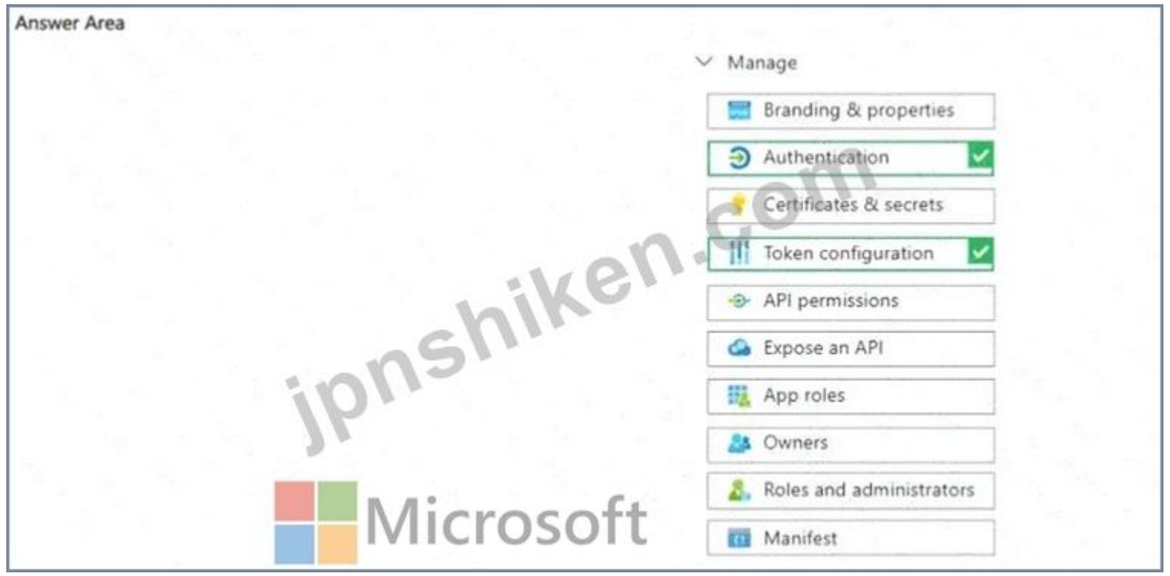
Text Description automatically generated



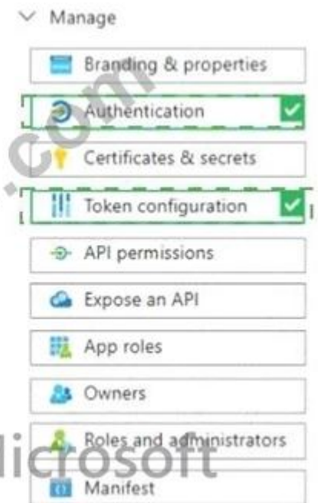
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

質問: **138**
WAF1 に対して計画された変更を実装する必要があります。
ソリューションは管理の手間を最小限に抑える必要がある
何をすべきでしょうか?
A. Azure ポリシーを作成します。
B. Azure 管理の DRS を変更します。
C. Bot Manager 1.1 ルール セットを変更します。
D. カスタムルールを追加します。
正解: **D** (コメントを発表する)

質問: **139**
contoso.com という 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。contoso.com 内です。
comでApp1というアプリを登録します。App1に対して以下のタスクを実行する必要があります。
* モバイルおよびデスクトップ アプリケーション プラットフォームを追加および構成します。
* ipaddr オプション要求を追加します。
App1 ではどの 2 つの設定を選択する必要がありますか? 回答するには、回答領域で適切な設定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: **140**

次の表に示す項目が含まれる KeyVault1 という名前の Azure キー コンテナーがあります。

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

KeyVault1 では、次のイベントが順番に発生します。

* アイテムは削除されます。
* Item2 と Policy1 は削除されます。

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。

ui

Answer Area



正解:



Explanation:



質問: 141

あなたの会社には、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。
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AzureADに登録されています。
App1がアプリケーションユーザーに代わってAzureKeyVaultのシークレットにアクセスできることを確認する必要があります。
何を構成する必要がありますか？

A. 管理者の同意なしの申請許可
B. 管理者の同意なしに委任された権限
C. 管理者の同意が必要な委任された権限
D. 管理者の同意が必要なアプリケーションのアクセス許可

正解: (正解を表示します)

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

質問: 142

Azure サブスクリプションには、storage1、storage2、storage3 という名前の 3 つのストレージ アカウント、Analytics1、Analytics2、Analytics3 という名前の 3 つの Log Analytics ワークスペース、および EventHub1、EventHub2、EventHub3 という名前の 3 つの Azure イベント ハブが含まれています。
Microsoft Entra ID の場合は、次の表に示す診断設定を作成します。

Name	Log	Storage account	Log Analytics workspace	Event hub
Setting1	AuditLogs	storage1	Analytics1	*None*
Setting2	ServicePrincipalSignInLogs, ManagedIdentitySignInLogs	*None*	Analytics2	*None*
Setting3	SignInLogs	storage2	*None*	EventHub1
Setting4	AuditLogs, ProvisioningLogs	*None*	Analytics3	EventHub2
Setting5	NonInteractiveUserSignInLogs	storage3	*None*	EventHub3

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。



正解:



Explanation:



質問: **143**

オンプレミス ネットワークには、VM1 という名前の Hyper-V 仮想マシンが含まれています。VM1 を Microsoft Defender for Cloud にオンボードするには、Azure Arc を使用する必要があります。最初に何をインストールする必要がありますか?

A. Azure Connected Machine エージェント
B. ゲスト構成エージェント
C. Azure Monitor エージェント
D. Log Analytics エージェント
正解: **(**正解を表示します**)**

質問: **144**
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: **B (**コメントを発表する**)**
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

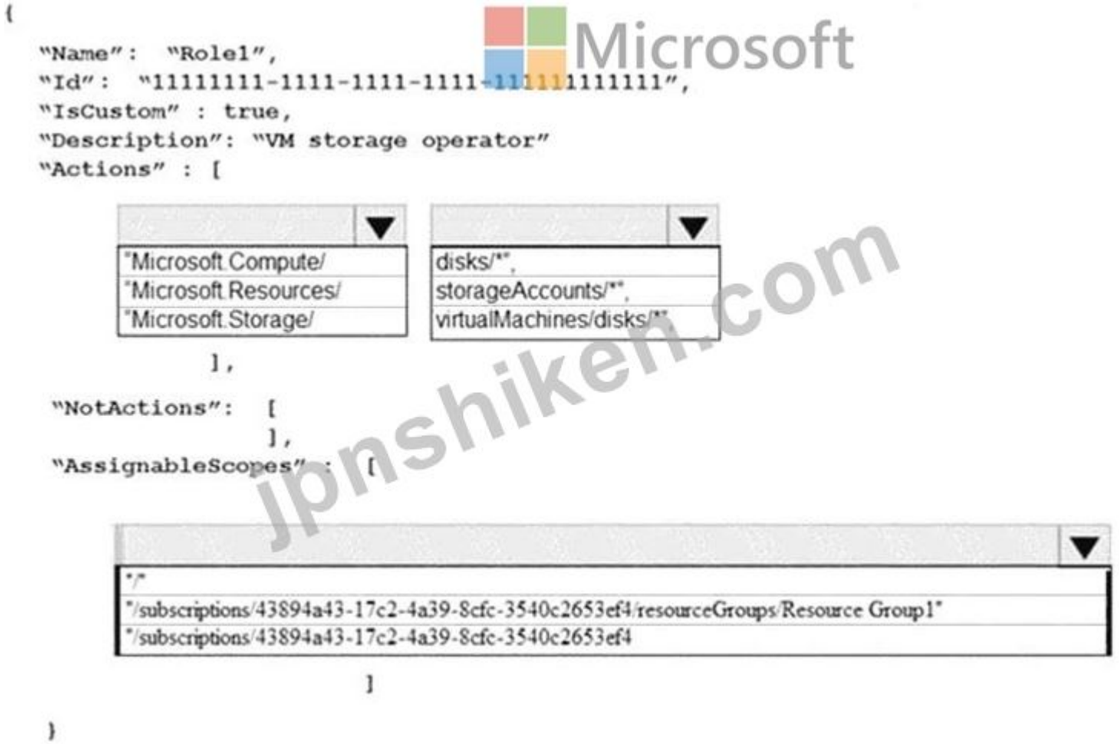
質問: **145**
次の表に示すAzure仮想マシンがあります。

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

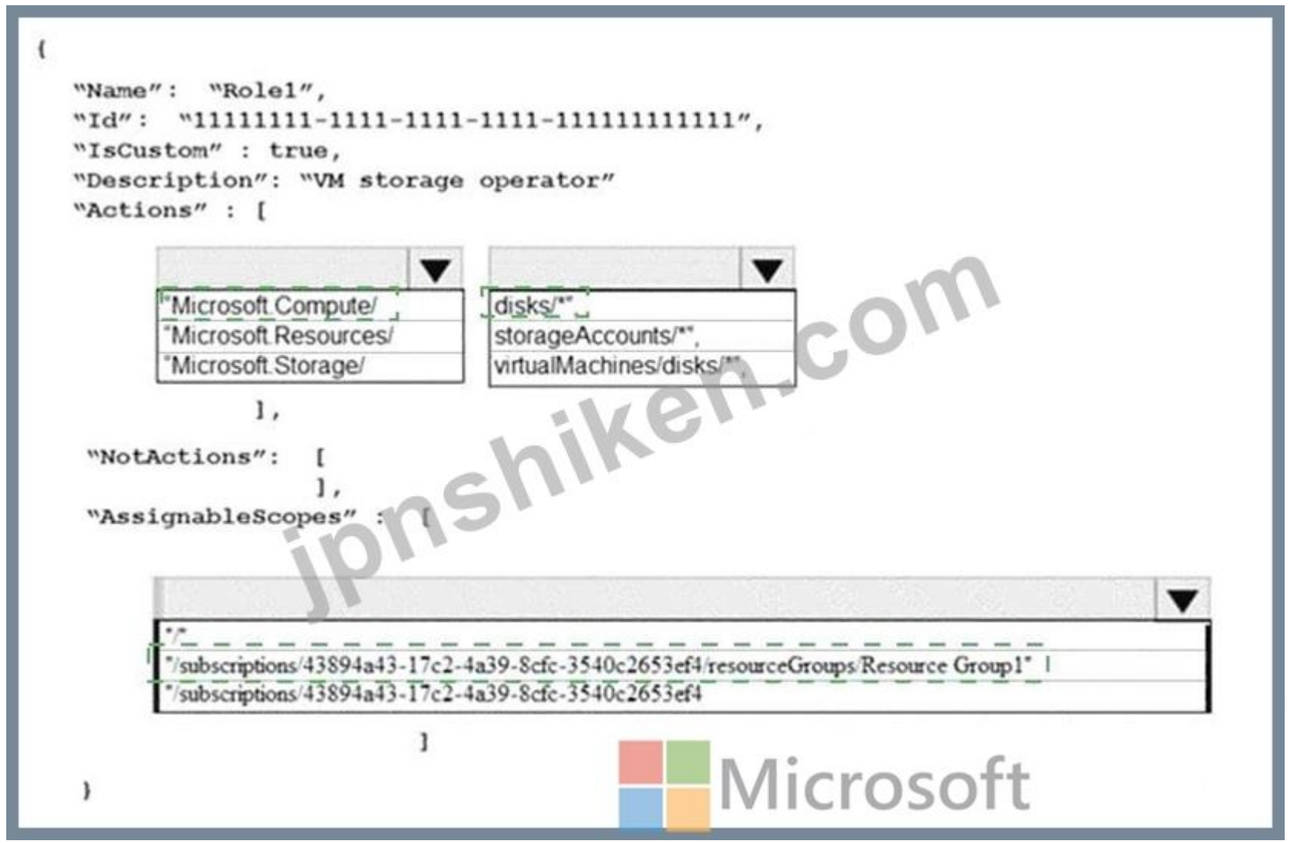
どの仮想マシンで更新管理を有効にできますか？
A. VM2およびVM3のみ
B. VM2、VM3、およびVM4のみ

C. VM1、VM2、およびVM4のみ
D. VM1、VM2、VM3、およびVM4
E. VM1、VM2、およびVM3のみ
正解: **C** (コメントを発表する)
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json

質問: **146**
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。



正解:



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.

質問: **147**

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: **148**

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？

Answer Area

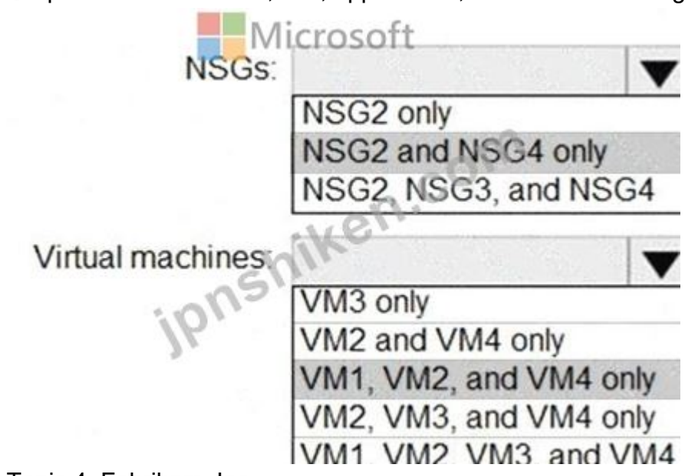


正解:



Explanation:

Graphical user interface, text, appli cation, chat or text message Description automatically generated



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: 149
次の表に示すリソースを格納する、Vault1 という名前の Azure キー コンテナーがあります。

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

ローテーション ポリシーの作成をサポートするリソースはどれですか?

A. Key1、Secret1、Cert1
B. Key1とCert1のみ
C. キー1のみ
D. Key1とSecret1のみ
E. Secret1とCert1のみ
F. Cert1のみ

正解: (正解を表示します)

質問: **150**

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、そこには Group1、Group2、Group3 という 3 つのセキュリティ グループと、次の表に示すユーザーが含まれています。

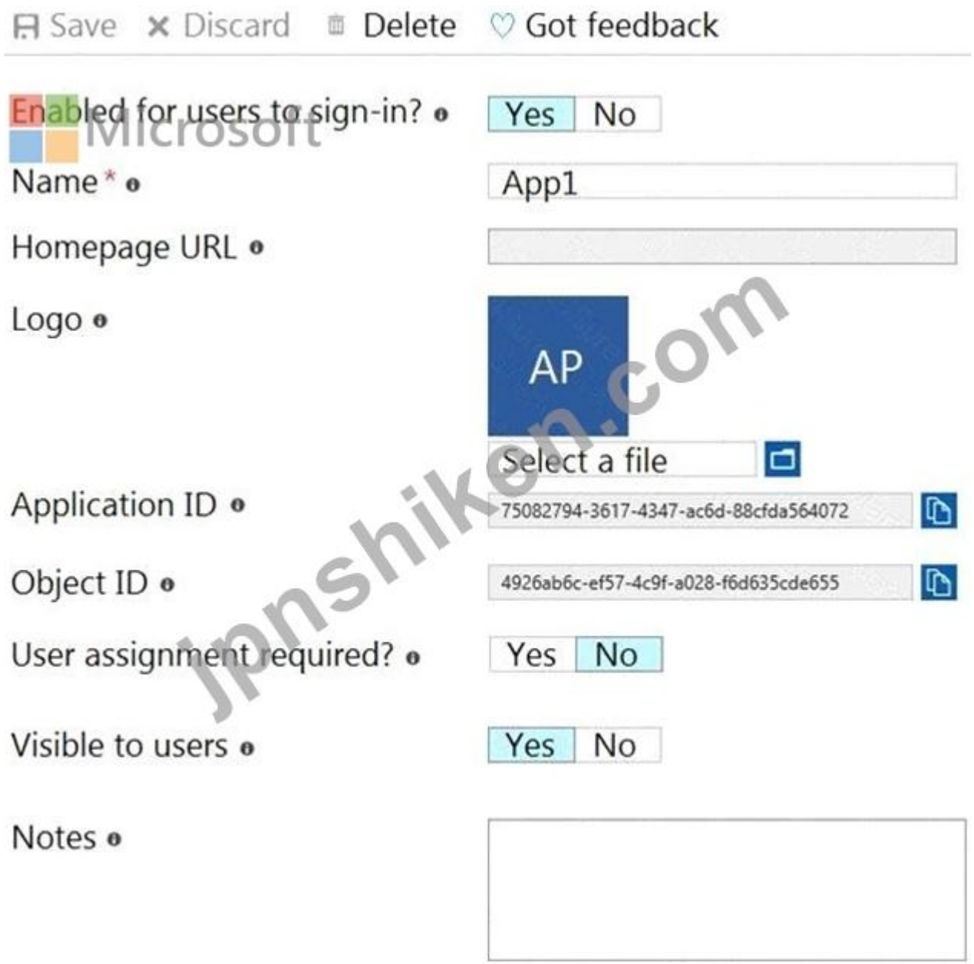
Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

グループ3はグループ2のメンバーです。

contoso.com で、次の設定を持つ App1 という名前のエンタープライズ アプリケーションを登録します。

* 所有者: ユーザー1
* ユーザーとグループ: グループ2

次の図に示すように、App1 のプロパティを構成します。



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。

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

正解:



Explanation:

Text Description automatically generated



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

質問: **151**

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。



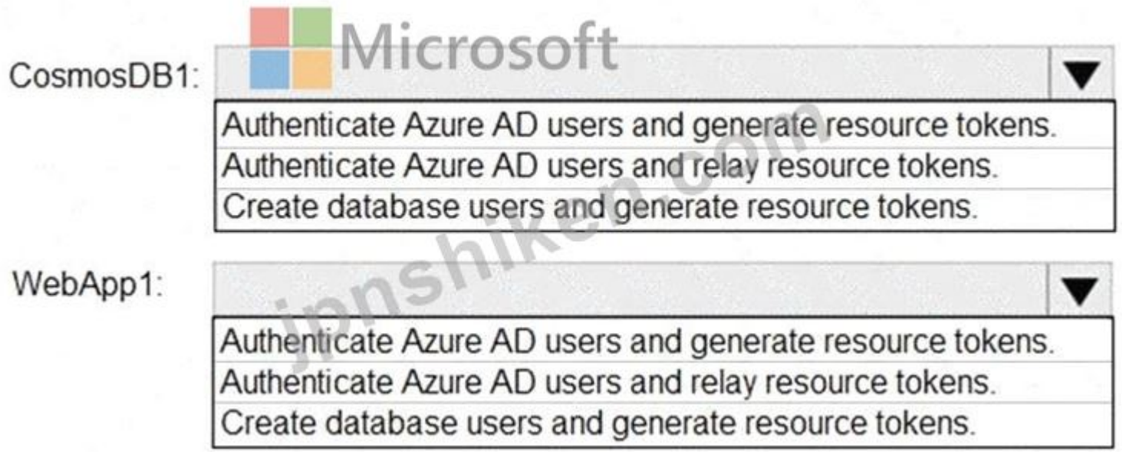
Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

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。

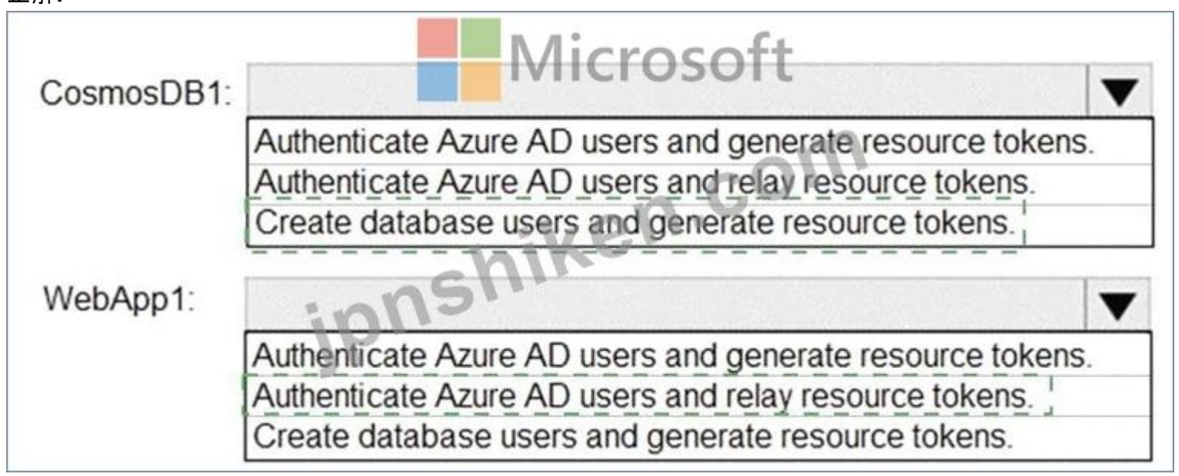
CosmosDB1 と WebApp1 に実装されるタスクを特定する必要があります。

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。

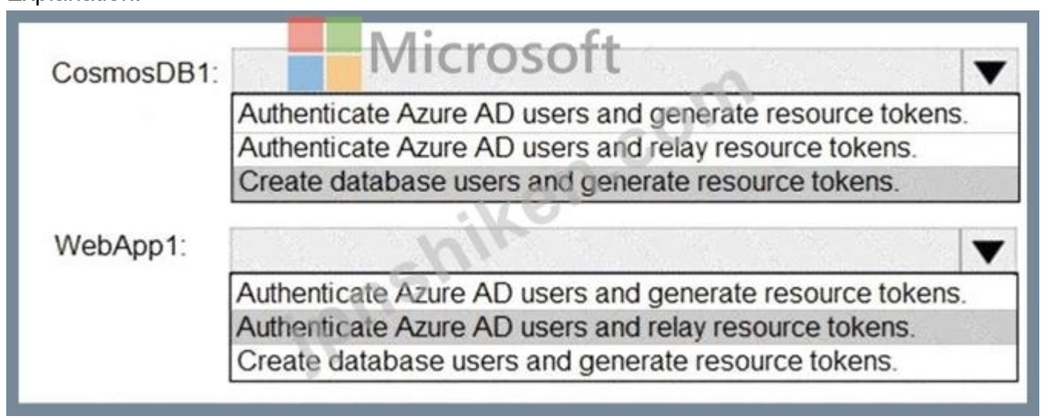
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:

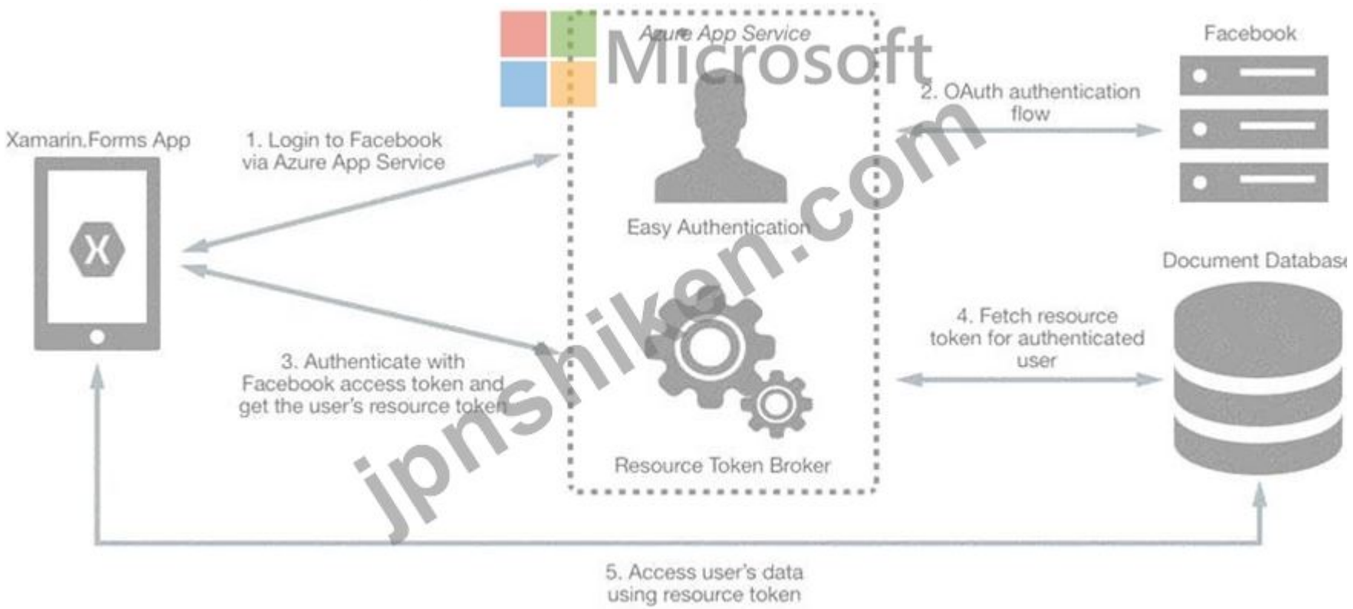


CosmosDB1: Create database users and generate resource tokens.

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:



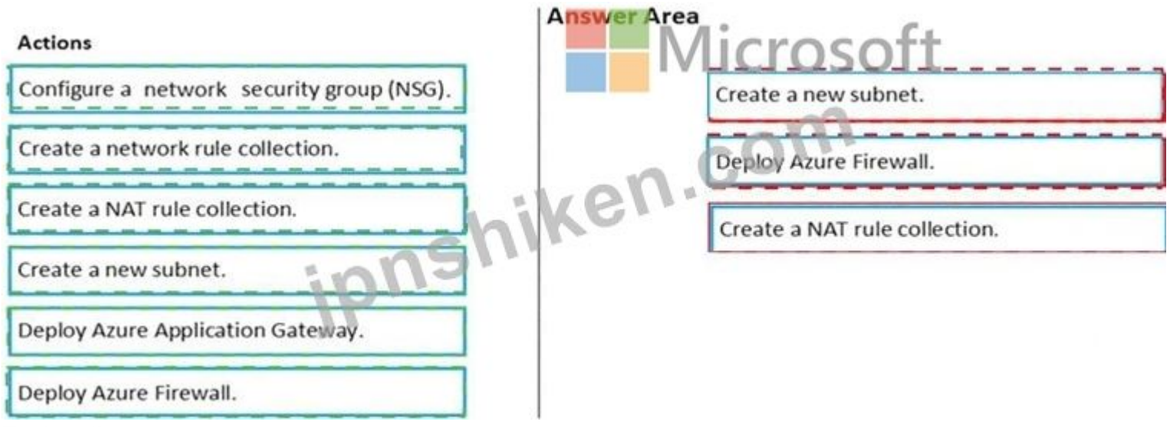
References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

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**」

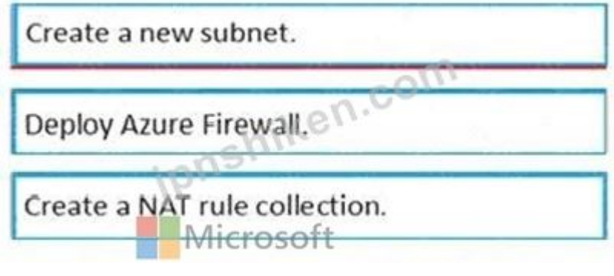
質問: **152**
次のリソースを含むAzureサブスクリプションがあります。
* Subnet1およびSubnet2という名前の2つのサブネットを含むVNET1という名前の仮想ネットワーク。
*プライベートIPアドレスのみを持ち、Subnet1に接続するVM1という名前の仮想マシン。
インターネットからVM1へのリモートデスクトップ接続を確立できるようにする必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序で並べます。



正解:



Explanation:



質問: **153**

storage1 という名前の Azure Data Lake Storage Gen2 アカウントを含む Azure サブスクリプションがあります。synapsews1 という名前の Azure Synapse Analytics ワークスペースをマネージド仮想ネットワークにデプロイします。synapsews1 から storage1 へのアクセスを有効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. ネットワーク セキュリティ グループ (NSG)

B. プライベート エンドポイント
C. peering
D. 仮想ネットワーク ゲートウェイ
正解: (正解を表示します)

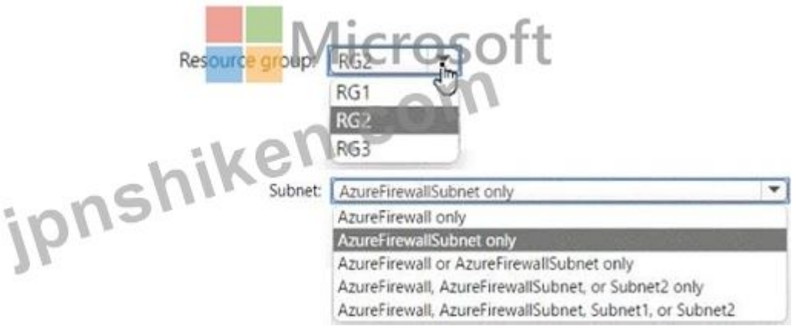
質問: **154**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

VNet1 には、次の表に示すサブネットが含まれています。

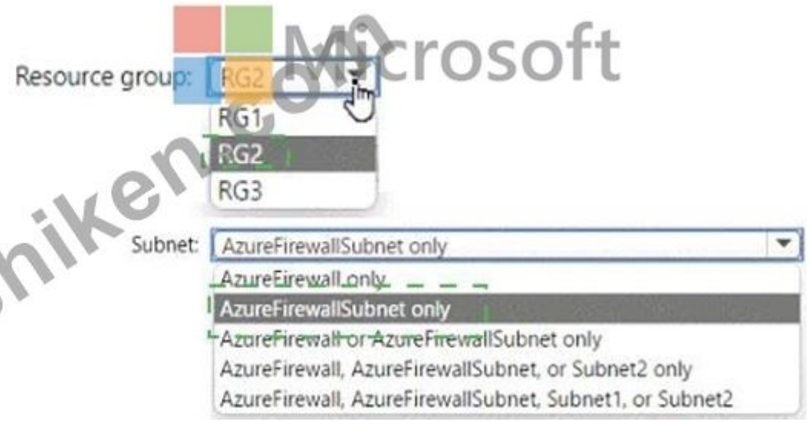
Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

Azure portal を使用して、AzFW1 という名前の Azure ファイアウォールを VNet1 にデプロイする予定です。
AzFW1 のデプロイに使用できるリソース グループとサブネットはどれですか? 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は 1 ポイントの価値があります。
Answer Area



正解:

Answer Area



Explanation:



質問: 155

500 人のユーザーと AU1 という名前の管理単位を含む Azure AD テナントがあります。
Azure Active Directory 管理センターから、メンバーの一括追加を使用してユーザーを AU1 に追加する予定です。
一括追加用のファイルを作成してアップロードする必要があります。
ファイルには何を含める必要がありますか?
A. 各ユーザーのユーザー プリンシパル名 (UPN) のみ
B. 各ユーザーのユーザー プリンシパル名 (UPN) と表示名のみ
C. 各ユーザーの表示名のみ
D. 各ユーザーのユーザー プリンシパル名 (UPN) とオブジェクト識別子のみ
E. 各ユーザーのオブジェクト識別子のみ
正解: (正解を表示します)

質問: 156

Identityという名前の管理されたIDを持ち、Azure Active 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、次の表に示すリソースが含まれています。
AUIとAU2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ます。

Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	**None**
User1	User	**Not applicable**
Group1	Security group	**Not applicable**
Group2	Microsoft 365 group	**Not applicable**

AU1とAU2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: **157**

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
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

SQL1 には次の構成があります。

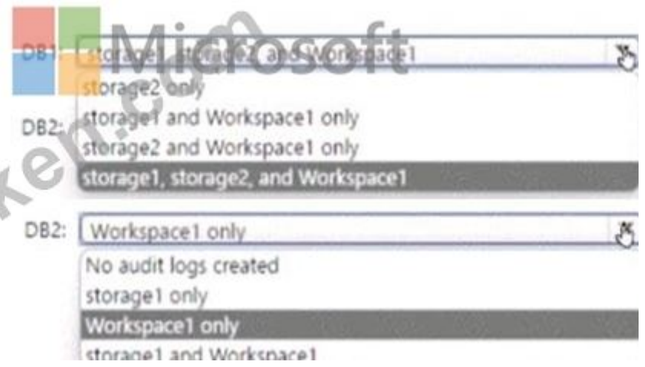
* 監査: 有効
* 監査ログの宛先: storage1、Workspace1

DB1 には次の構成があります。

* 監査: 有効
* 監査ログの保存先: storage2

DB2 では監査が無効になっています。

DB1 と DB2 の監査ログはどこに保存されますか? 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: 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: **158**

Azure サブスクリプションをお持ちです。

次の要件を満たすには、Azure 仮想 WAN をデプロイする必要があります。

* 米国東部、米国西部、および北ヨーロッパの Azure リージョンに 3 つの安全な仮想ハブを作成します。
* セキュリティ ルールがリージョン間で同期していることを確認します。

何を使えばいいのでしょうか？

A. Azure ネットワーク機能マネージャー
B. Azure ファイアウォール マネージャー
C. アズールフロントドア
D. Azure 仮想ネットワーク マネージャー

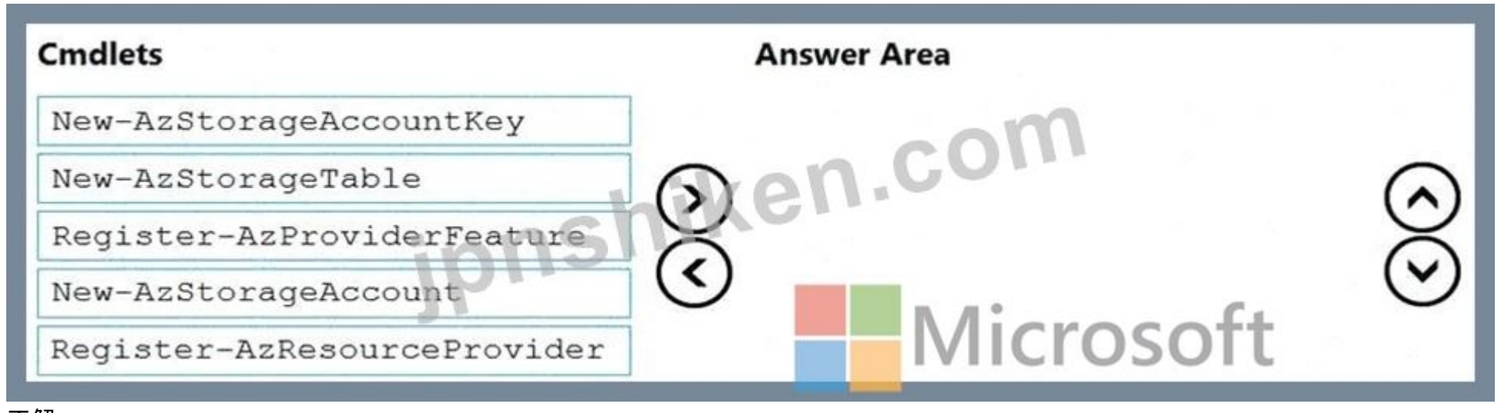
正解: **B (**コメントを発表する**)**

質問: **159**

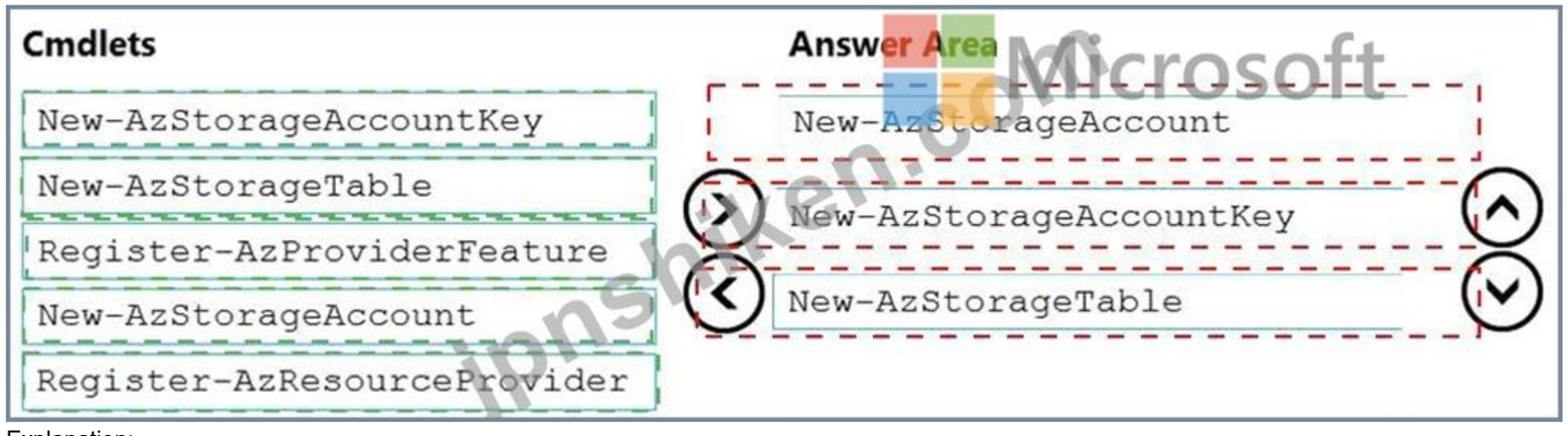
あなたは、contoso.com という名前の Microsoft Entra テナントにリンクされた Azure サブスクリプションを持っています。contoso.com に App1 という名前のアプリケーションを登録します。App1 の登録に Android アプリケーション用のプラットフォーム構成を追加する必要があります。Azure ポータルで何を構成する必要がありますか？
A. マニフェスト
B. 認証
C. トークン設定
D. ブランディングとプロパティ
正解: (正解を表示します)

質問: **160**
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、脅威インテリジェンス、および IDPS
B. TLS インスペクションのみ
C. 脅威インテリジェンスと IDPS のみ
D. TLS インスペクションと IDPS のみ
E. 脅威インテリジェンスのみ
正解: (正解を表示します)

質問: **161**
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を作成する予定です。
ストレージアカウントのテーブルを暗号化するには、顧客が管理するキーを使用する必要があります。
Azure Cloud Shellから、どの3つのコマンドレットを順番に実行する必要がありますか？回答するには、適切なコマンドレットをコマンドレット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。

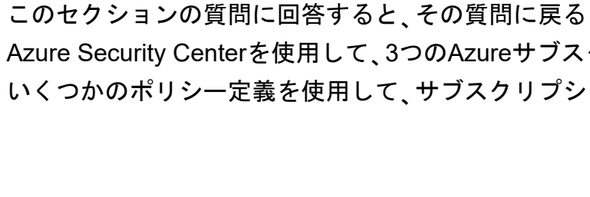


正解:



Explanation:

Text, table Description automatically generated with medium confidence



Reference:

https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=powershell

質問: **162**

User1 という名前のユーザーを含む Microsoft Entra テナントがあります。

テナントに対してパスワードなしの認証を有効にする予定です。

User1 が複合登録エクスペリエンスを有効に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、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べきですか?

A. セキュリティ管理者

B. 特権ロール管理者

C. 全体管理者

D. 認証管理者

正解: **D (**コメントを発表する**)**

質問: **163**

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 :リソースグラフと、管理グループを対象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)
References:
https://docs.microsoft.com/en-us/azure/governance/management-groups/create

質問: **164**
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: **165**

単一のネットワークセキュリティグループ (NSG) を持つ単一のサブネット上に10台の仮想マシンがあります。

ネットワークトラフィックをAzure Storageアカウントに記録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. ネットワークパフォーマンスモニターソリューションをインストールします。

B. Azure Network Watcherを有効にします。
C. NSGの診断ログを有効にします。
D. NSGフローログを有効にします。
E. Azure Log Analyticsワークスペースを作成します。
正解: **D (**コメントを発表する**)**
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
* Create a VM with a network security group
* Enable Network Watcher and register the Microsoft.Insights provider
* Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
* Download logged data
* View logged data
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

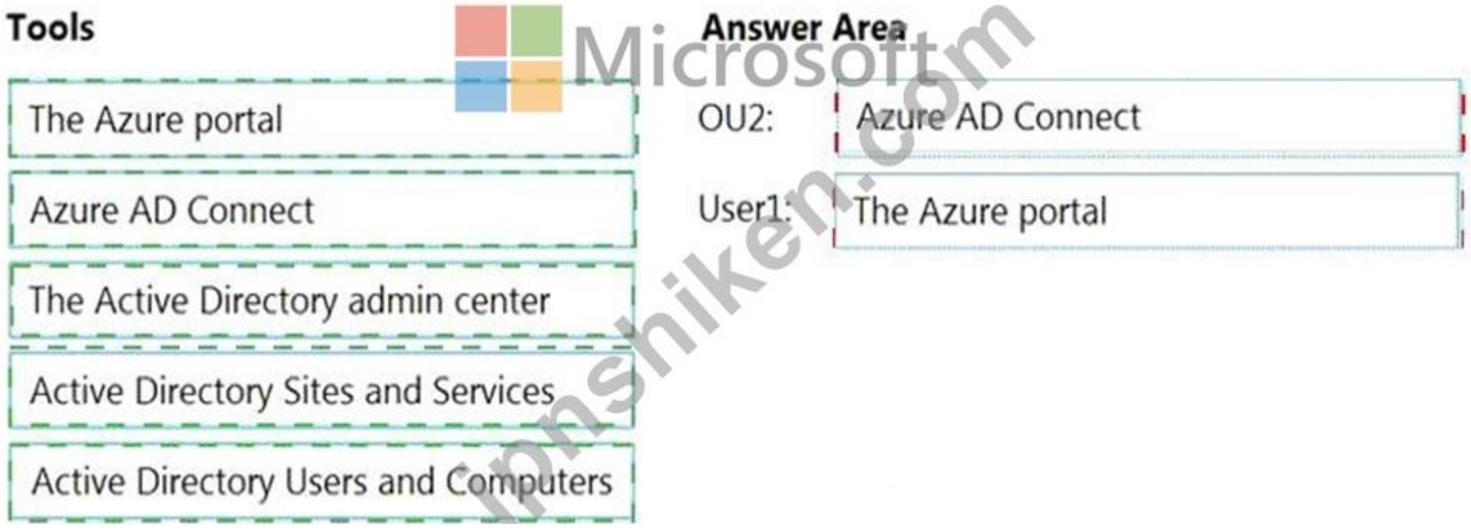
質問: **166**
会社はAzure DevOpsを使用しています。
コードが会社の品質基準とコードレビュー基準を満たしているかどうかを検証する方法を推奨する必要があります。
Azure DevOpsに実装することをお勧めしますか？
A. branch folders
B. branch permissions
C. branch policies
D. branch locking
正解: (正解を表示します)
Branch policies help teams protect their important branches of development. Policies enforce 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

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**」

質問: **167**
OU2とUser1に対して計画された変更を実行する必要があります。
どのツールを使用する必要がありますか？答えるには、適切なツールを正しいリソースにドラッグします。各ツールは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、分割バーをペイン間でドラッグするか、スクロールする必要がある場合があります。
注：丌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:

Tab le Description automatically generated



質問: **168**

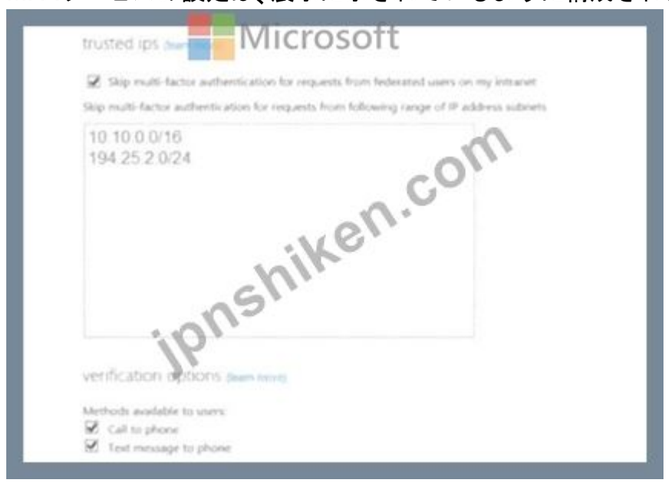
あなたの会社には、シアトルとニューヨークに2つのオフィスがあります。各オフィスは、NATデバイスを使用してインターネットに接続します。オフィスでは、次の表に示すIPアドレスを使用しています。

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

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。テナントには、次の表に示すユーザーが含まれます。

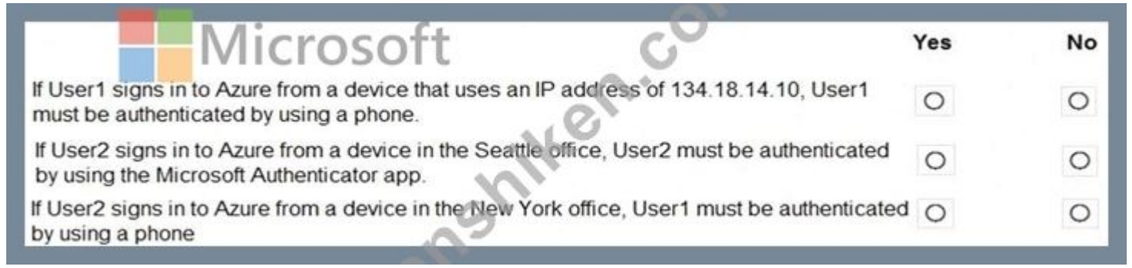
Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

MFAサービスの設定は、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。）



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:

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	○

Explanation:



Box 2: No

Use of Microsoft Authenticator is not required.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No

The New York IP address subnet is included in the " skip multi-factor authentication for request.

References:

https://www.cayosoft.com/difference-enabling-enforcing-mfa/

質問: **169**

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
AFW1	Azure firewall

VM1 から米国西部 Azure リージョンのストレージ アカウントへのトラフィックのみを許可するように AFW1 を構成する必要があります。ソリューションでは、管理作業を最小限に抑える必要があります。

何を設定すればよいでしょうか?

A. DNATルール

B. ネットワークルール

C. SNATプライベートIPアドレス範囲

D. アプリケーションルール

正解: (正解を表示します)

質問: **170**

次の表に示す仮想マシンを含む Azure サブスクリプションがあります。

Subnet1 と Subnet2 には、ネットワーク セキュリティ グループ (NSG) があります。NSG には、次の構成を持つ送信規則があります。

* ポート; どれでも
* ソース: 任意
* 優先度: 100
* アクション: 拒否
* プロトコル: 任意
* 目的地: 倉庫

サブスクリプションには、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。

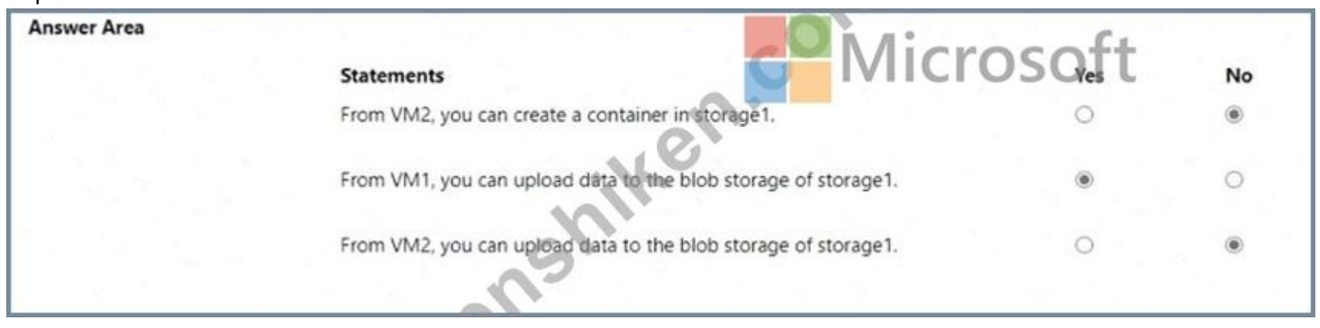
次の設定を持つ Private1 という名前のプライベート エンドポイントを作成します。
* リソースの種類: Microsoft.Storage/storageAccounts
* リソース: storage1
* ターゲット サブリソース: blob
* 仮想ネットワーク: VNet1
* サブネット: Subnet1
次の各ステートメントについて、該当する場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。
Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

正解:



Explanation:



質問: **171**
AzureSentinelがデプロイされています。
Rule1という名前のスケジュールされたクエリルールを作成する必要があります。
Rule1のクエリルールロジックを定義するには、何を使用する必要がありますか？
A. Transact-SQLステートメント
B. JSON定義
C. GraphQL
D. Kustoクエリ
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問: **172**
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 7
VM1 という名前の仮想マシンのセキュリティ ログから、すべての監査失敗データを Azure ストレージ アカウントに収集する必要があります。このタスクを完了するには、Azure portal にサインインします。
正解:
Check below steps in explanation for Task
Explanation:
To collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account, you can follow these steps:
In the Azure portal, search for and select the virtual machine named VM1.
In the left pane, select Diagnostic settings.
Select Add diagnostic setting.
In the Add diagnostic setting pane, enter the following information:
Name: Enter a name for the diagnostic setting.
Destination: Select Storage account.
Storage account: Select the storage account you want to use.
Logs: Select Windows Event Logs.
Categories: Select Security.
Event types: Select Audit Failure.
Select Save.

質問: **173**

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	Role
Admin1	Group1	Global Administrator
Admin2	Group1	Privileged Authentication Administrator
User1	*None*	*None*

次の図に示すように、一時アクセス パスの設定を構成します。



Admin2 に一時アクセス パス認証方法を追加します。

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。

Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	○
Admin2 can add the Temporary Access Pass authentication method to User1.	○	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	○

正解:

Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	○
Admin2 can add the Temporary Access Pass authentication method to User1.	○	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	○

Explanation:

Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	●
Admin2 can add the Temporary Access Pass authentication method to User1.	●	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	●

質問: **174**

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。

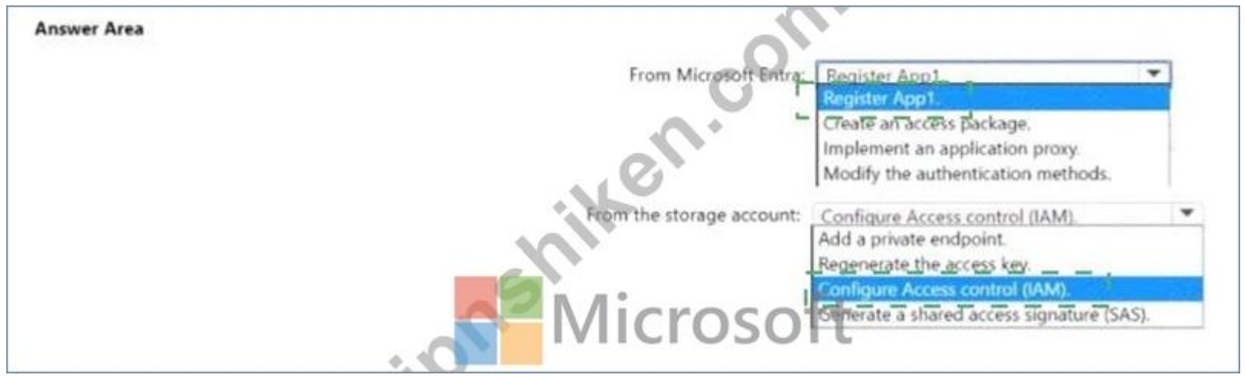
user1 は、userl@fabrikam.com の資格情報を使用してサインインできる必要があります。テナント内のリソースへのアクセス権を User1 に付与できる必要があります。管理作業を最小限に抑える必要があります。

あなたは何をするべきか？
A. テナントに fabrikamcom をカスタム ドメインとして追加します。
B. User1 の招待状を作成します。
C. user1 のユーザー アカウントを作成します。
D. 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。
正解: (正解を表示します)

質問: **175**
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: **176**
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。

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

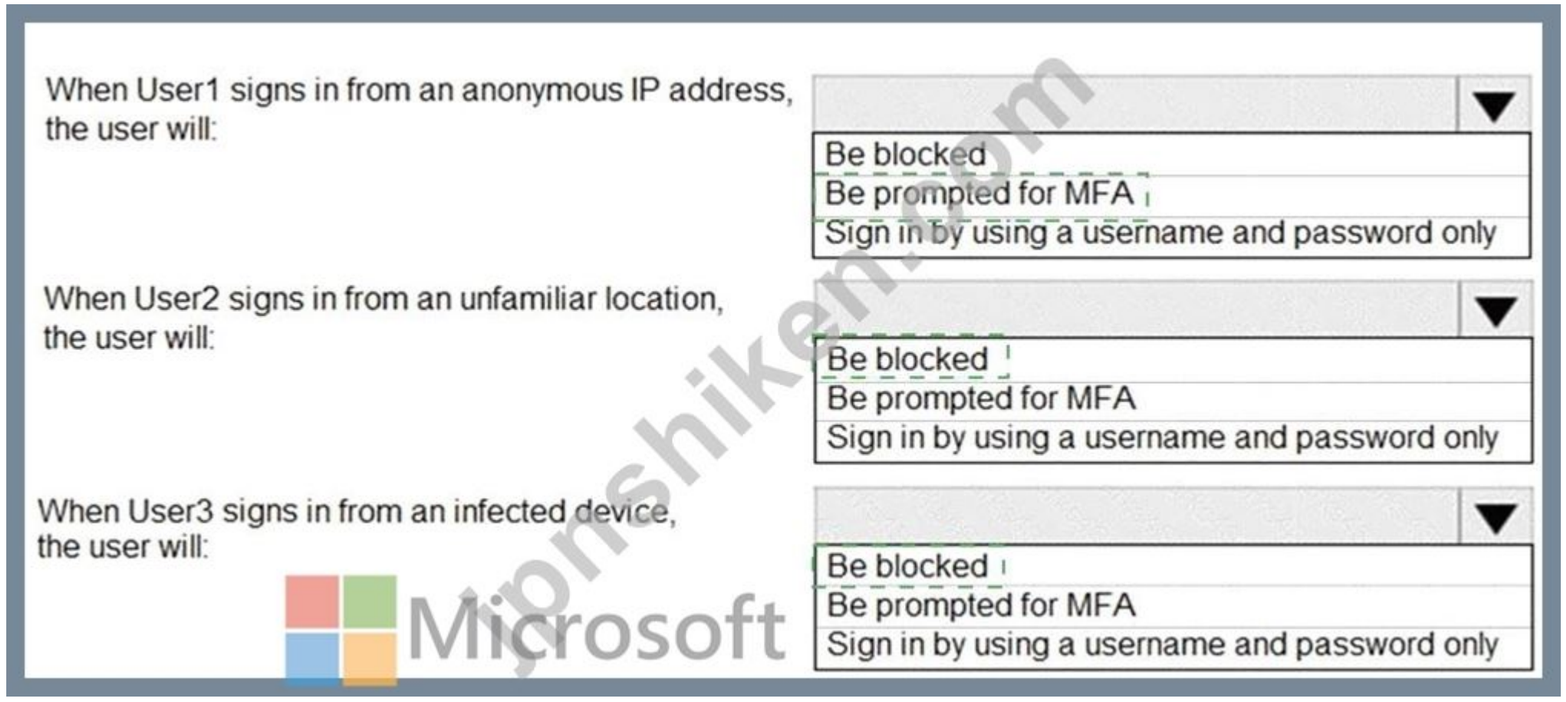
When User2 signs in from an unfamiliar location, the user will:

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

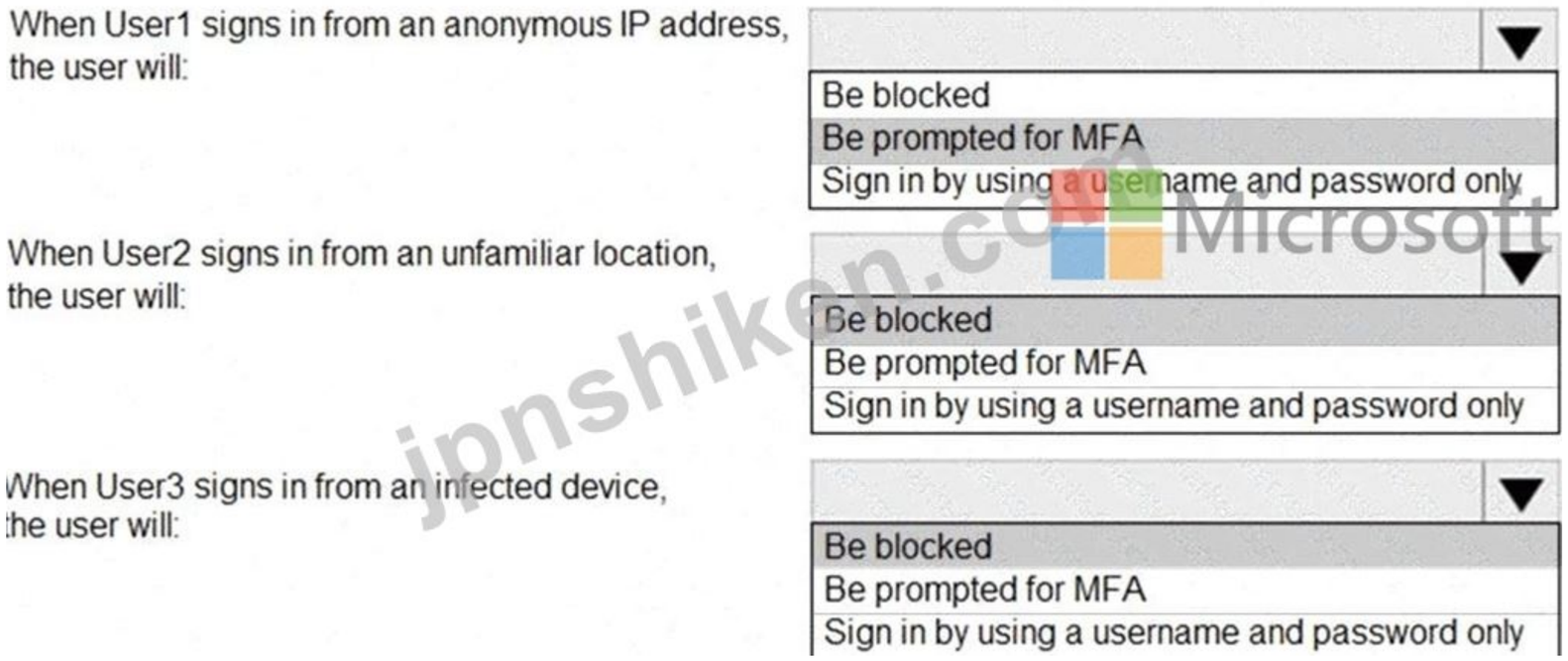
When User3 signs in from an infected device, the user will:

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

正解:



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: **177**
次の表に示すリソースを含むSub1という名前のAzureサブスクリプションがあります。

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

包含データベースユーザーを使用して、SQL1上のデータベースへの安全なアクセスをVM1に提供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. VM1でマネージドサービスIDを有効にします。
B. KV1でシークレットを作成します。
C. SQL1でサービスエンドポイントを構成します。
D. KV1でキーを作成します。
正解: (正解を表示します)
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql

質問: **178**
SQL1 という名前の Azure SQL データベースを含む Azure サブスクリプションがあります。SQL1 には、次の表に示す列が含まれています。

Name	Contains
Column1	Comments from a confidential investigation
Column2	Government ID numbers
Column3	Images
Column4	Videos

Always Encrypted を使用するように SQL! を構成します。
決定論的暗号化を設定する必要があります。
決定論的暗号化をサポートする列はどれですか?
A. 列1
B. 列2
C. 列3
D. 列4
正解: (正解を表示します)

質問: **179**
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。

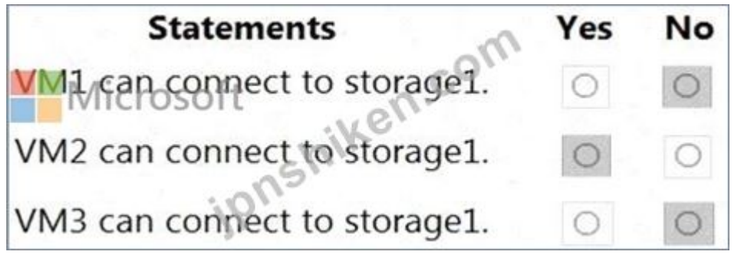
注意: 正しい選択ごとに 1 ポイントが付与されます。

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: **180**
JITVMアクセスを実装することを計画しています。どの仮想マシンがサポートされますか？
A. VM1のみ
B. VM2、VM3、およびVM4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)

質問: **181**
Microsoft Sentinel ワークスペースを含む Azure サブスクリプションを持っています。
Microsoft Sentinel は、複数の Azure ワークロードからログを取り込むように構成されています。インシデントの管理には、サードパーティのサービス管理プラットフォームが使用されます。
次の要件を満たすように構成する Microsoft Sentinel コンポーネントを特定する必要があります。
* Microsoft Sentinel が脅威を特定した場合は、インシデントを作成する必要があります。
* Microsoft Sentinel でインシデントが作成されると、サービス管理プラットフォームにチケットが記録される必要があります。
各要件に対してどのコンポーネント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: 正しく選択するたびに 1 ポイントの価値があります。



正解:

Answer Area

When Microsoft Sentinel identifies a threat, an incident must be created: Analytics
- Analytics
- Data connectors
- Playbooks
- Workbooks

A ticket must be logged in the service management platform when an incident is created in Microsoft Sentinel: Playbooks
- Analytics
- Data connectors
- Playbooks
- Workbooks

Explanation:



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**」

質問: **182**
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: **183**
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:



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.	○	○

Explanation:



質問: **184**
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. テーブルストレージ
B. キューストレージ
C. Azure Files
D. ブロブストレージ
正解: (正解を表示します)

質問: **185**
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。



正解:



Explanation:



質問: **186**

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。

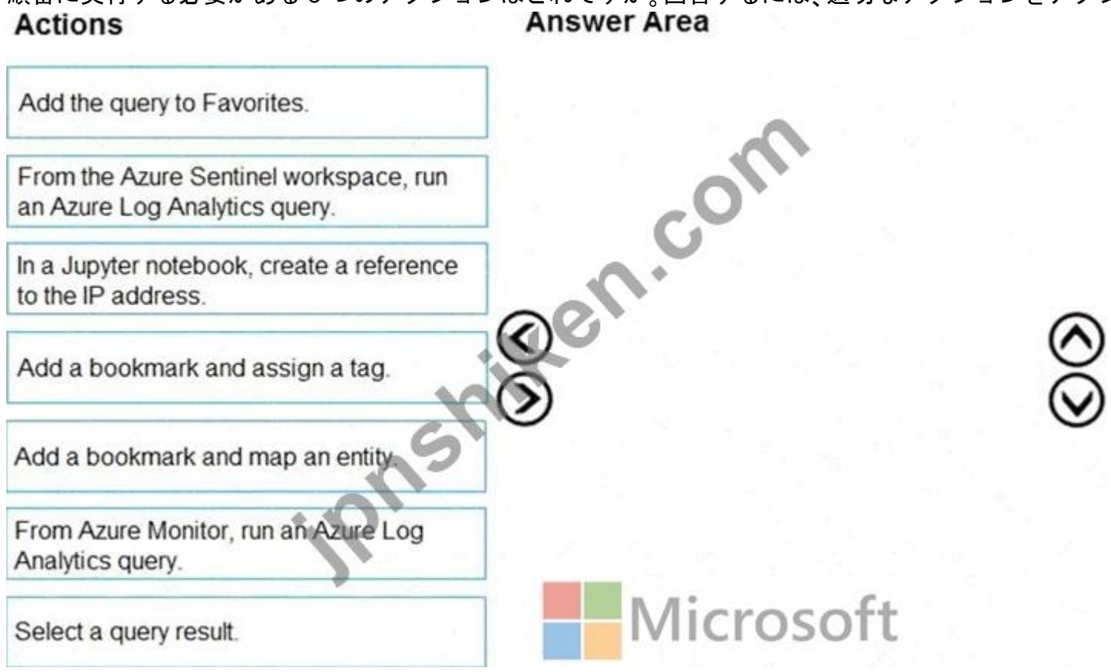
あなたは何をするべきか？

A. Azure アプリケーション ゲートウェイを作成します。

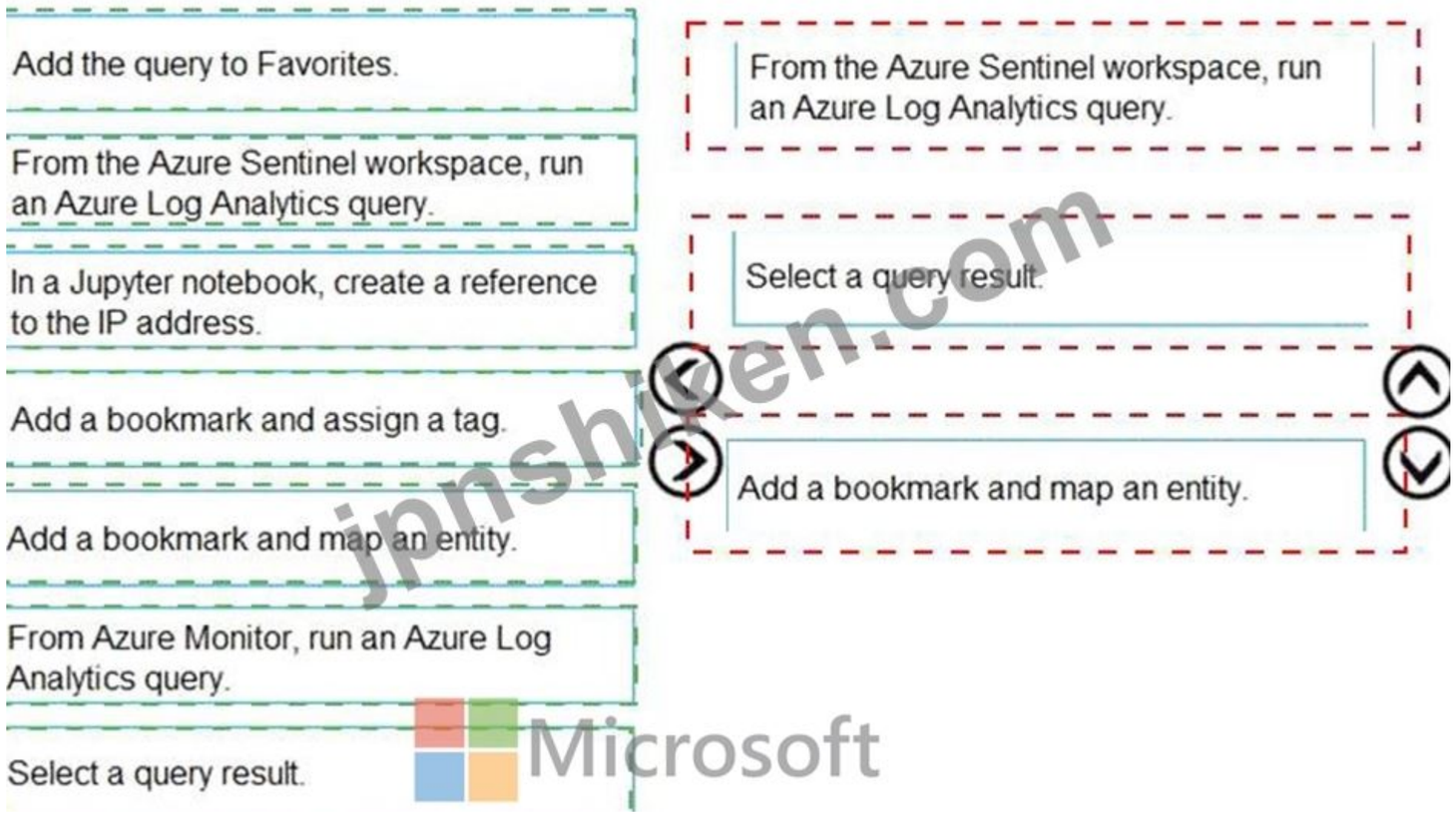
B. リージョン仮想ネットワーク統合を構成します。

C. Azure App Service ハイブリッド接続を作成します。
D. App Service 環境を作成する
正解: (正解を表示します)

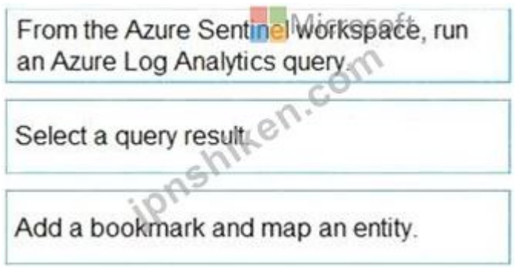
質問: **187**
Azure Active Directory (Azure AD) データ コネクタを備えた Azure Sentinel ワークスペースがあります。
特定の IP アドレスからの疑わしいトラフィックを脅威として探しています。
ワークスペースに保存されている中間イベントに注釈を付け、調査グラフ内を移動するときに IP アドレスを参照できるようにする必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



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

質問: 188

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、次の表に示すサブネットが含まれています。

Name	IP address space
Subnet1	10.10.0.0/24
Subnet2	172.16.0.0/24
Subnet3	192.168.10.0/24

サブスクリプションには、次の表に示す仮想マシンが含まれています。

Name	Connected to
VM1	Subnet1
VM2	Subnet2
VM3	Subnet3

VM3 には、ポート 8080 で接続をリッスンするサービスが含まれています。
VM1 では、次の図に示すように、ジャストインタイム (JIT) VM アクセスを構成します。



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:



Microsoft
ibnshiken.com

質問: **189**
次の表に示す仮想ネットワークを含む、Sub1 および Sub2 という名前の 2 つの Azure サブスクリプションがあります。

Name	Subscription	Tag
VNet1	Sub1	*None*
VNet2	Sub1	Red

次の構成を持つ AVNM1 という名前の Azure Virtual Network Manager インスタンスがあります。
* 管理範囲 :サブ1
* ネットワークグループ:
* NetGrp1: VNet1を含む静的メンバーシップ
* NetGrp2: 次の条件を満たす動的メンバーシップ: 赤を含むタグ
* セキュリティ管理ルールコレクション: SARule1
* すべてのAzureリージョンにデプロイ

Name	Subscription	Tag
VNet3	Sub1	Red
VNet4	Sub2	Red

次の表に示すように、2 つの新しい仮想ネットワークを作成します。
どの仮想ネットワークに SARule1 が適用されますか?
A. VNet2 と VNet3 のみ
B. VNet1、VNet2、および VNet3 のみ
C. VNet2、VNet3、および VNet4 のみ
D. VNet1、VNet2、VNet3、および VNet4
E. VNet1 と VNet2 のみ
正解: **(**正解を表示します**)**

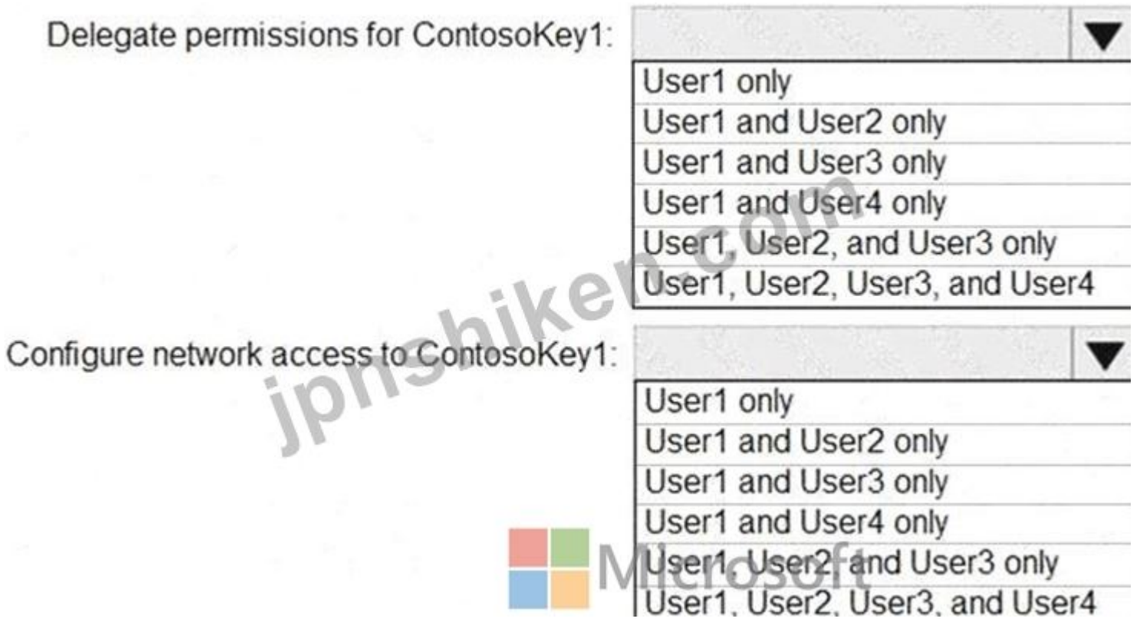
質問: **190**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。
このセクションの質問に回答すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Active Directory (AzureAD)のハイブリッド構成があります。
仮想ネットワーク上にAzure HDInsightクラスターがあります。

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**: B (**コメントを発表する**)**
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

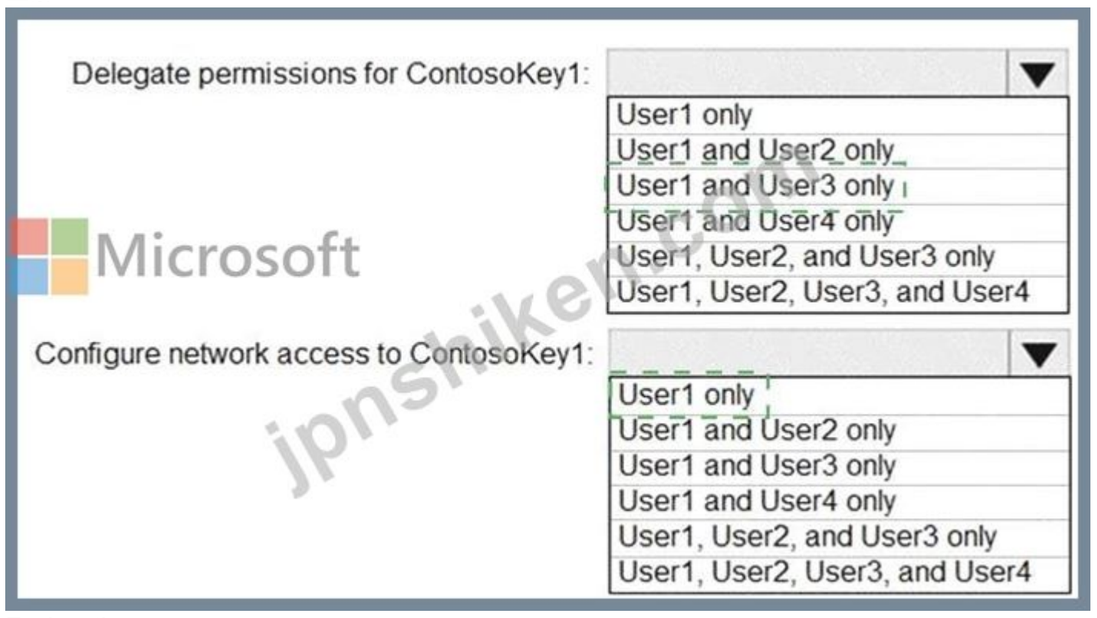
質問**: 191**
ContosoKey1 という名前の Azure キー コンテナーを含む Azure サブスクリプションがあります。
次の表に示すように、ユーザーを作成し、ロールを割り当てます。

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	*None*
User2	Security Admin	*None*
User3	*None*	User Access Administrator
User4	*None*	Key Vault Contributor

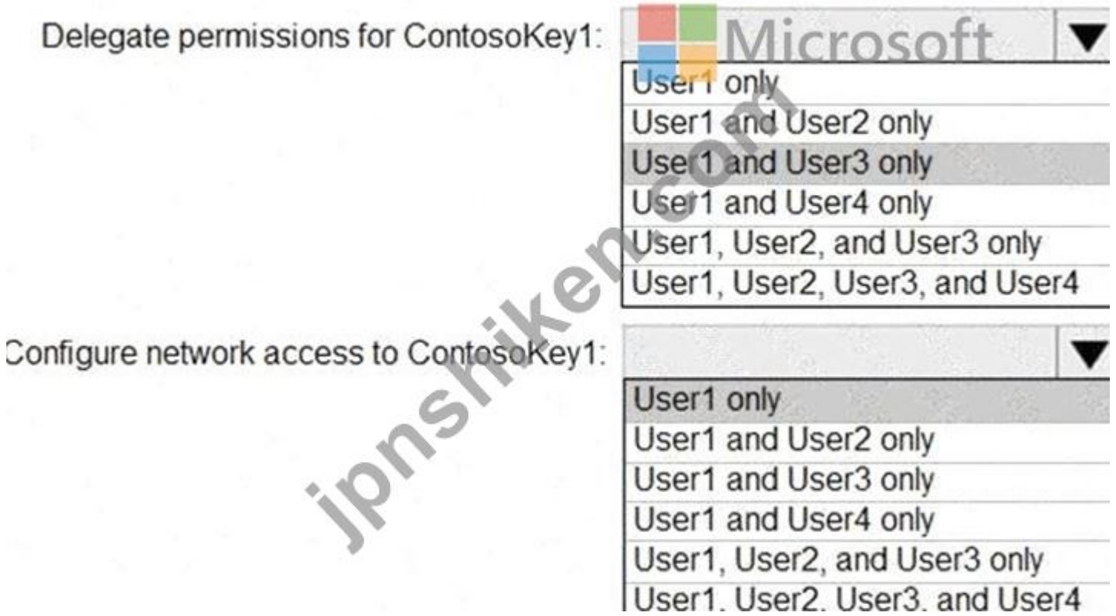
次のアクションを実行できるユーザーを特定する必要があります。
* ContsosKey1 の権限を委任します。
* ContosoKey1 へのネットワーク アクセスを構成します。
どのユーザーを識別する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:

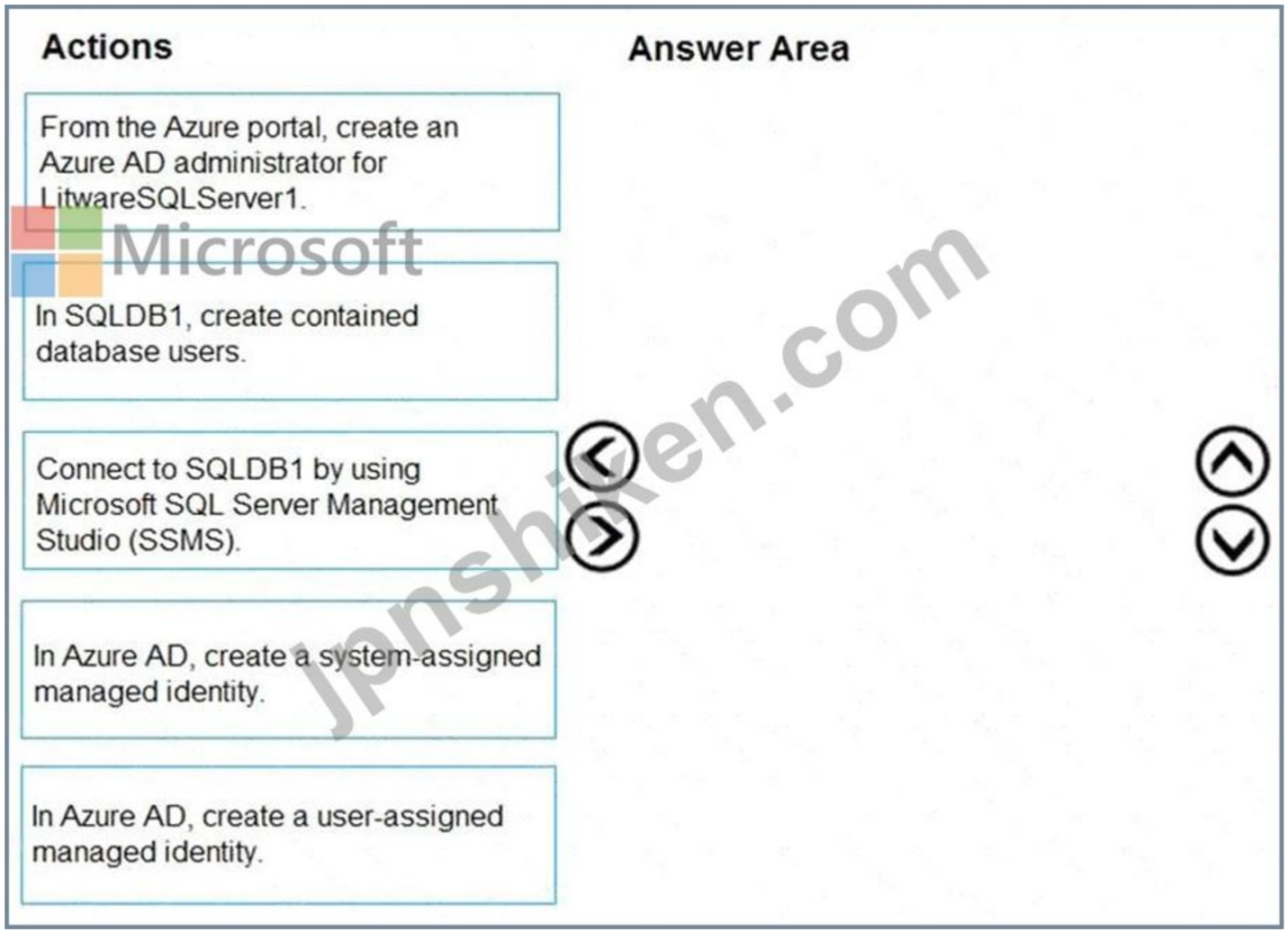


jpnshiken.com

Reference:
https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

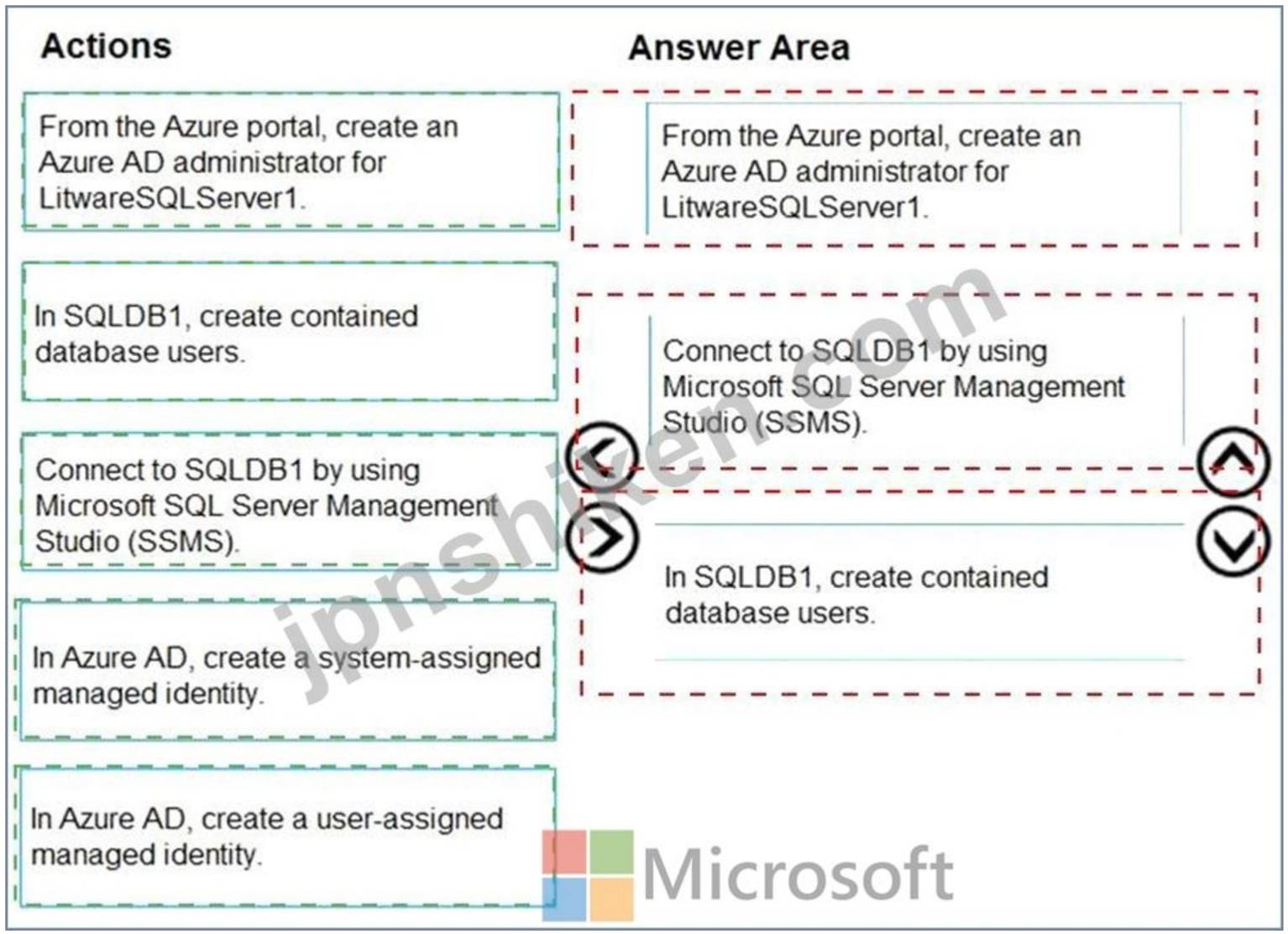
質問: **192**
Azure仮想マシンの展開に使用するAzure Resource Managerテンプレートがあります。
仮想マシンのインスタンスがプロビジョニングされると、未使用のWindows機能を自動的に無効にする必要があります。
何を使うべきですか？
A. security policies in Azure Security Center
B. Azure Logic Apps
C. an Azure Desired State Configuration (DSC) virtual machine extension
D. Azure Advisor
正解: (正解を表示します)

質問: **193**
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。



Microsoft
jpnshiken.com

正解:



Explanation:

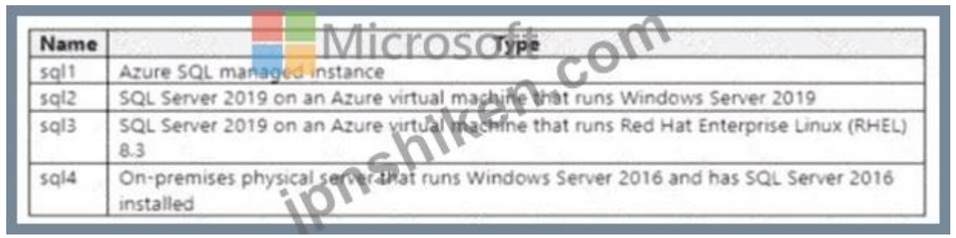
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS In SQLDB1, create contained database users

https://www.youtube.com/watch?v=pEPyPsGEevw

質問: **194**

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
ipnshinan.com

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 と sql2 のみ
C. sql1、sql2、sql3、sql4
D. sql1 sql2 および so.14 のみ
正解: (正解を表示します)

質問: **195**
Azureサブスクリプションがあります。
別のAzure Active Directory（Azure AD）テナントを使用するようにサブスクリプションを構成します。
変更の2つの可能な影響は何ですか？それぞれの正解は完全なソリューションを示します。
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。
A. サブスクリプションレベルでの役割の割り当ては失われます。
B. 仮想マシンが管理するIDが失われます。
C. 仮想マシンのディスクスナップショットは失われます。
D. 既存のAzureリソースが削除されます。
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

質問: **196**
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

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**」

質問: **197**

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	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: **198**

あなたは Sub! という名前の Azure サブスクリプションと、AWS1 という名前の Amazon Web Services (AWS) アカウントを持っています。

Admin1という名前の新しいユーザーアカウントを作成します。

Admin1が以下の操作を実行できることを確認する必要があります。

* AWS1 を Microsoft Defender for Cloud に追加します。
* 既存および将来のすべての Amazon Elastic Compute Cloud (EC2) インスタンスに対して、Azure Arc の自動プロビジョニングを有効にします。

解決策は最小権限の原則に従う必要があります。Sub1 スコープの Admin1 にはどのロールを割り当てるべきですか？

A. サービスコネクタ貢献者
B. CrossConnectionManager
C. 貢献者
D. オーナー

E. セキュリティ管理者
正解: (正解を表示します)

質問: **199**
Azure AD テナントにリンクされ、次の表に示す仮想マシンが含まれる Azure サブスクリプションがあります。

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

仮想ネットワークのサブネットには、次の表に示すサービス エンドポイントがあります。

Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

次の表に示すリソースを作成します。

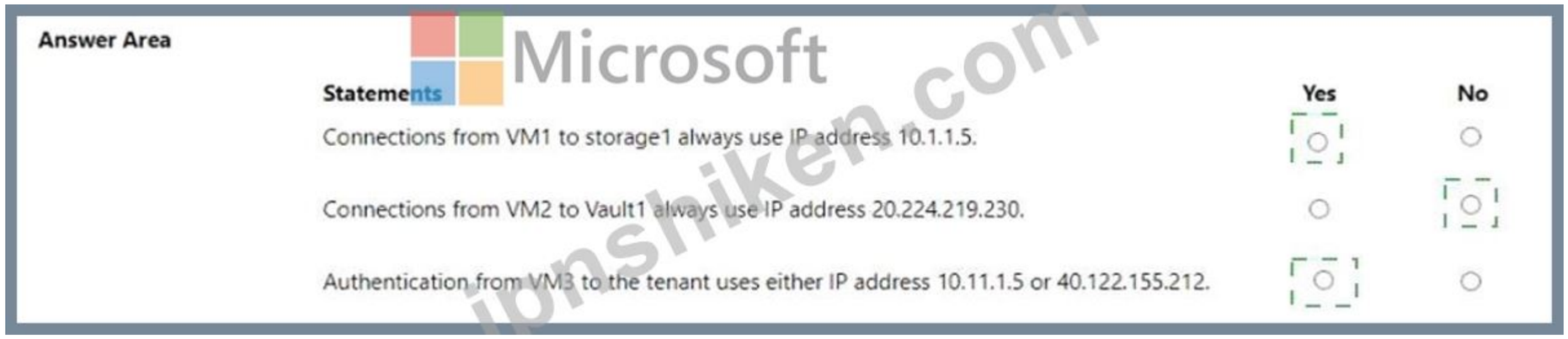
Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	○
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	○	○

正解:



Explanation:



質問: 200

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. 証明書のみ

B. シークレットと証明書のみ

C. キーのみ

D. 秘密のみ

E. キーとシークレットのみ

F. キー、シークレット、証明書

正解: **A (**コメントを発表する**)**

質問: 201

ラボのタスク

タスク 4

管理者が Azure Resource Manager テンプレートを使用してリソースをデプロイするときに、そのデプロイメントが KV31330471 という名前の Azure Key Vault 内のシークレットにアクセスでき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:

* Grant permission to the application that is used to deploy the resources to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the application at the scope of the key vault or individual secrets.

* Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the enabledForTemplateDeployment property of the key vault to true.

* Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
* Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the New-AzResourceGroupDeployment cmdlet, the az deployment group create command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters.

質問**: 202**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。

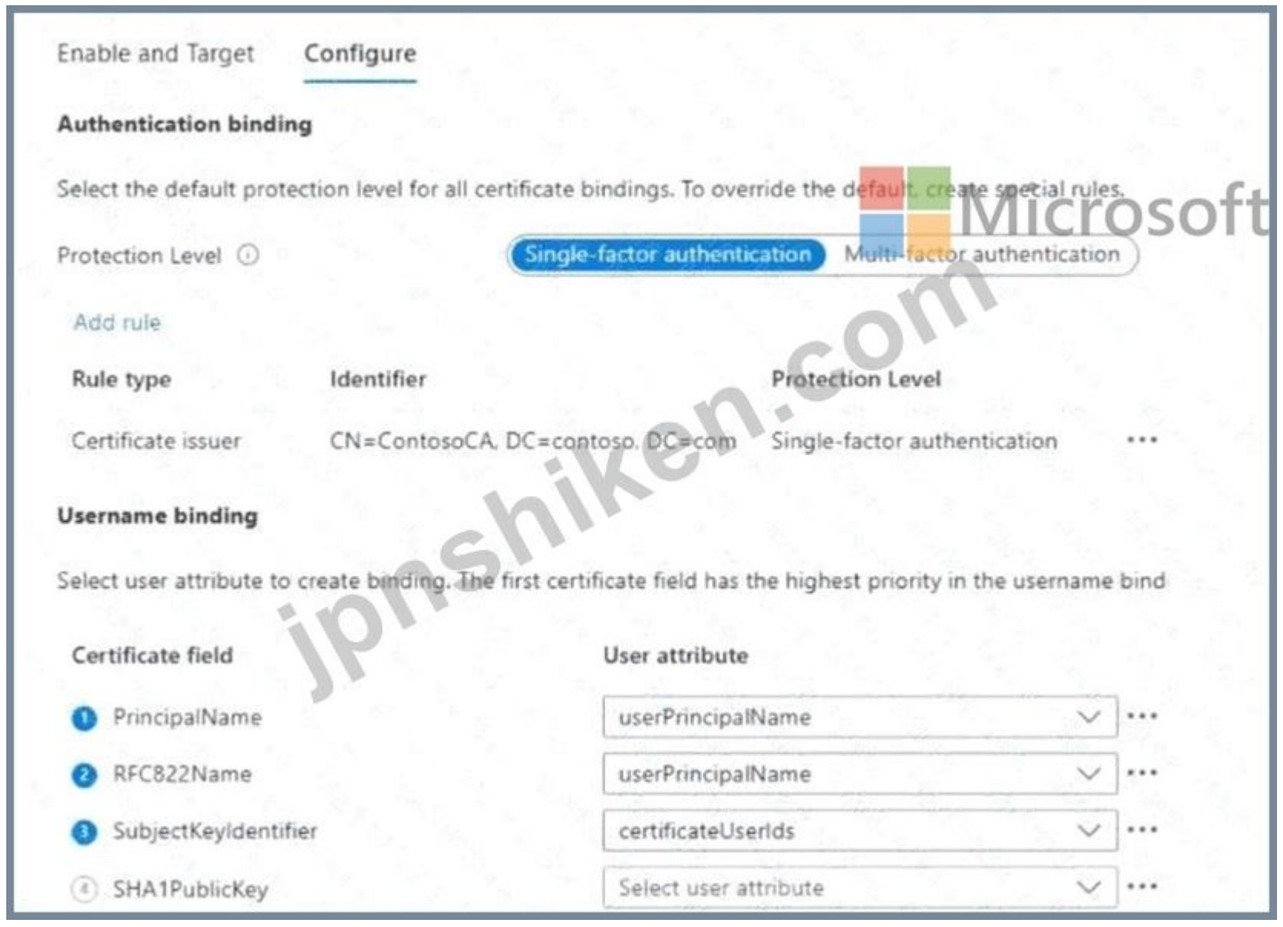
Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

すべてのユーザーは、ContosoCA という証明機関 (CA) によって発行された証明書を含むデバイスを所有しています。
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: CAPoltcy1
* 課題
o ユーザーとグループ: グループ1
o ターゲットリソース
* 対象: すべてのクラウドアプリ
アクセス制御
* アクセスを許可する: 多要素認証を要求する
o ポリシーを有効にする: オン
証明書ベースの認証を有効にしてターゲットに設定するには、有効化とターゲット」の図を参照してください。(有効化とターゲット」タブをクリックします。)



Microsoft
jpnshiken.com

証明書ベースの認証は、構成」の図に示すように構成します。(構成」タブをクリックします。)



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：正しい選択肢は1つにつき1点です。

Answer Area

Statements	Yes	No
User1 can sign in without providing a password.	○	○
User2 can choose to use a certificate or a smart card to sign in.	○	○
User3 must use a certificate during sign-in.	○	○

正解:



Explanation:



質問: **203**

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.

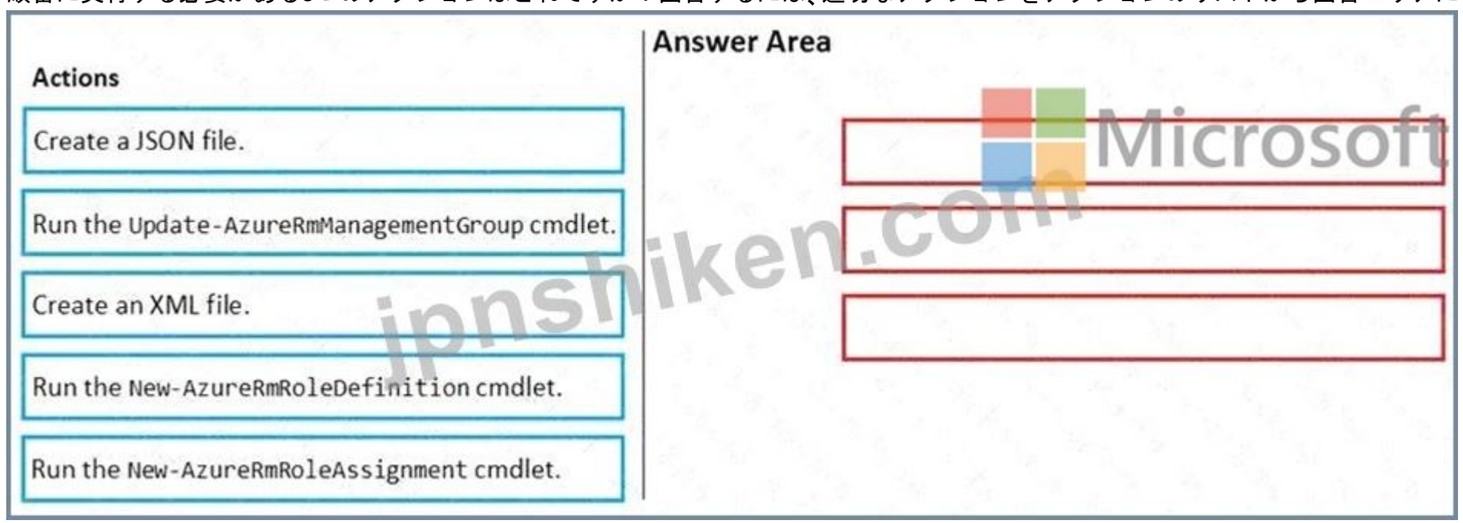
Explanation:

Answer as below.

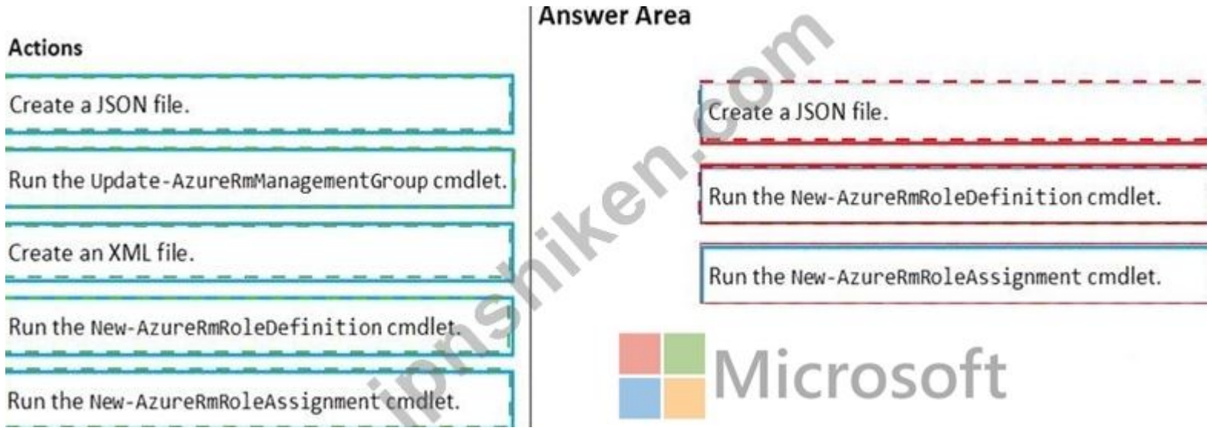


質問: **204**
お客様のAzureサブスクリプションには、EASM1という名前のMicrosoft Defender External Attack Surface Management(Defender EASM)リソースが含まれています。EASM1では検出が有効になっており、複数のインベントリアセットが含まれています。
どの在庫資産が最も重大なWebアプリケーションセキュリティリスクに対して脆弱であるかを特定する必要があります。
どのDefender EASMダッシュボードを使用すべきですか？
A. セキュリティ態勢
B. OWASPトップ10
C. 攻撃対象領域の概要
D. GDPR準拠
正解: (正解を表示します)

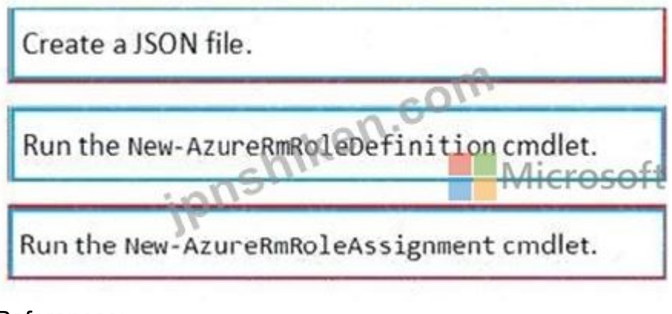
質問: **205**
Sub1という名前のAzureサブスクリプションがあります。
ITチームのすべてのメンバーを含むGroup1という名前のAzure Active Directory（Azure AD）グループがあります。
Group1のメンバーがSub1のAzure仮想マシンを停止、開始、および再起動できることを確認する必要があります。
ソリューションは、最小特権の原則を使用する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序に並べます。



正解:



Explanation:



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

質問: **206**
Sub1 という名前の Azure サブスクリプションがあり、Microsoft Defender for Cloud を使用しています。Sub1 には、User1 という名前のユーザーと RG1 という名前のリソース グループが含まれています。RG1 には、Workspace1 という名前の Log Analytics ワークスペースが含まれています。
セキュリティインシデントへの対応としてトリガーされるAzure Logic Appsワークフローを、User1が変更できるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 にはどのロールを割り当てる必要がありますか。また、どのリソースにそ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: **207**

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	Location
RG1	Resource group	**Not applicable**	West US
Managed1	Managed identity	RG1	West US

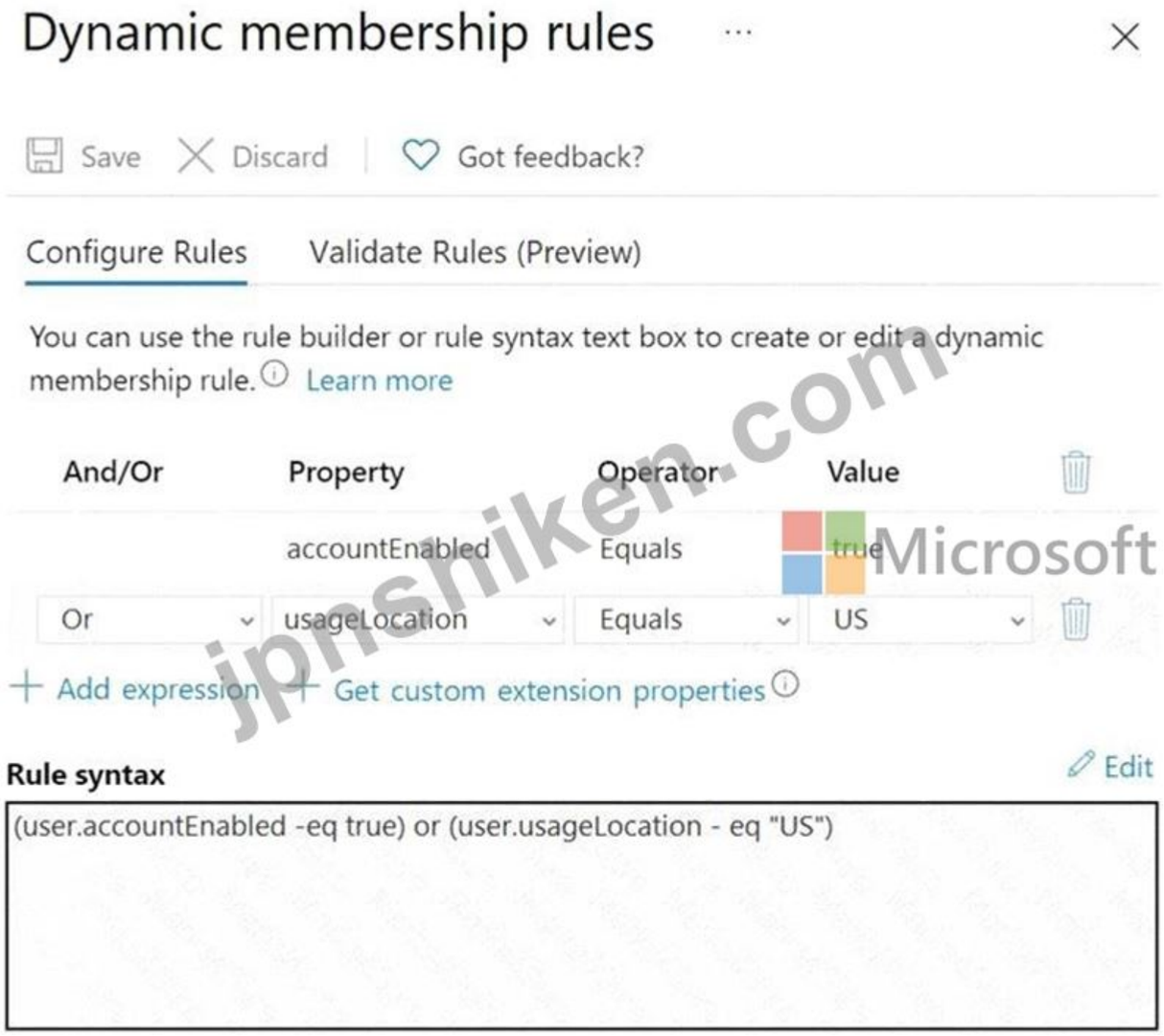
サブスクリプションは、次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントにリンクされています。

Name	Usage location
User1	United States
User2	Germany

次の表に示すグループを作成します。

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

Group1 と Group2 のメンバーシップ ルールは、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
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

正解:

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Explanation:

Text Description automatically generat ed



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

質問: **208**

Defender for Cloud の計画された変更を実装するには、ユーザーに委任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。

どのユーザーを選択すべきでしょうか?

A. 管理者1

B. 管理者3

C. 管理者2
D. 管理者4
正解: (正解を表示します)

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**」