AZ-500-free-Exam#04

# Q.1シミュレーション-

ホームページという名前のAzureSQLデータベースの毎週のバックアップを構成する必要があります。バックアップは8週間保持する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

AzureSQLデータベースのバックアップポリシーを構成する必要があります。

1. Azureポータルで、検索ボックスに「Azure SQL Database」と入力し、検索結果から[Azure SQL Database]を選択して、[ホームページ]を選択します。または、左側のナビゲーションウィンドウでAzureSQLデータベースを参照します。

2.ホームページデータベースをホストしているサーバーを選択し、[バックアップの管理]をクリックします。

3. [ポリシーの構成]をクリックします。

4. [毎週のバックアップ]オプションがオンになっていることを確認します。

5.毎週のバックアップを保持する期間オプションを8週間に構成します。

6. [適用]をクリックして変更を保存します。

# Q.2シミュレーション-

管理者がAzureResource 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、デプロイがKV11597200という名前のAzureキーボールト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。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

キーボールトの高度なアクセスポリシーでオプションを構成する必要があります。

1. Azureポータルで、検索ボックスに「Azure Key Vault」と入力し、検索結果から[Azure Key Vault]を選択してから、KV11597200という名前のキーボールトを選択します。

または、左側のナビゲーションウィンドウでAzure KeyVaultを参照します。

2.キーボールトのプロパティで、[高度なアクセスポリシー]をクリックします。

3.テンプレート展開のためにAzureResourceManagerへのアクセスを有効にするというラベルの付いたチェックボックスをオンにします。

4. [保存]をクリックして変更を保存します。

# Q.3シミュレーション

-Homepage

-AGWという名前のAzureApplication Gatewayを介した接続で、悪意のある要求がないかどうかを確認する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

タスクが完了するのを待つ必要はありません。

正解： *以下の説明を参照してください。*

ApplicationGatewayでWebApplicationFirewallを有効にする必要があります。

1. Azureポータルで、検索ボックスに「アプリケーションゲートウェイ」と入力し、検索結果から[アプリケーションゲートウェイ]を選択してから、[

ホームページ-AGW]という名前のゲートウェイを選択します。または、左側のナビゲーションペインで[アプリケーションゲートウェイ]を参照します。

2.アプリケーションゲートウェイのプロパティで、Webアプリケーションファイアウォールをクリックします。

3. [ティア]設定で、[WAFV2]を選択します。

4. [ファイアウォールステータス]セクションで、スライダーをクリックして[有効]に切り替えます。

5. [ファイアウォールモード]セクションで、スライダーをクリックして[防止]に切り替えます。

6. [保存]をクリックして変更を保存します。

# Q.4シミュレーション-

Intranet11597200という名前のWebアプリを作成し、ユーザーがAzure Active Directory（Azure AD）を使用してWebアプリに対して認証できるようにする必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

1. Azureポータルで、検索ボックスに「アプリサービス」と入力し、検索結果から[アプリサービス]を選択します。

2. [アプリサービスの作成]ボタンをクリックして、新しいアプリサービスを作成します。

3. [リソースグループ]セクションで、[新規作成]リンクをクリックして、新しいリソースグループを作成します。

4.リソースグループにIntranet11597200RGなどの名前を付けて、[OK]をクリックします。

5. [インスタンスの詳細]セクションで、[名前]フィールドに「Intranet11597200」と入力します。

6. [ランタイムスタック]フィールドで、.NET Core3.1などのランタイムスタックを選択します。

7. [レビュー+作成]ボタンをクリックします。

8. [作成]ボタンをクリックして、Webアプリを作成します。

9. [リソースに移動]ボタンをクリックして、新しいWebアプリのプロパティを開きます。

10. [設定]セクションで、[認証/承認]をクリックします。

11. App Service認証スライダーをクリックして、オンに設定します。

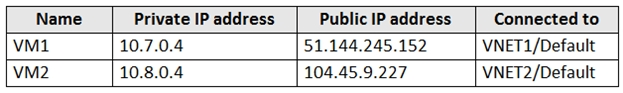
12. [要求が認証ではない場合に実行するアクション]ボックスで、[Azure ActiveDirectoryでログインする]を選択します。

13. [保存]をクリックして変更を保存します。

# Q.5

HOTSPOT-

Key Vault1という名前のAzureキーボールトと次の表に示す仮想マシンを含むAzureサブスクリプションがあります。

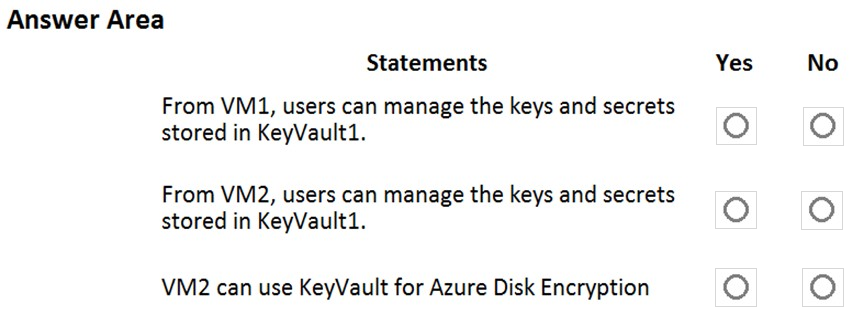


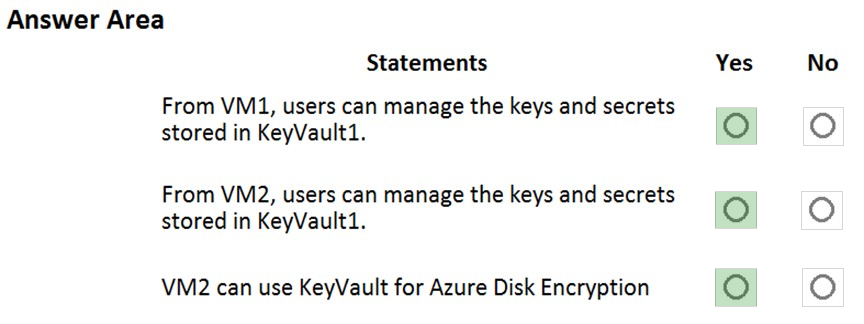
Key Vaultアクセスポリシーを、ボリューム暗号化のためにAzure Disk Encryptionへのアクセスを有効にするように設定します。

KeyVault1は、次の展示に示すように構成されています。



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



正解： 

# Q.6

DRAGDROP-

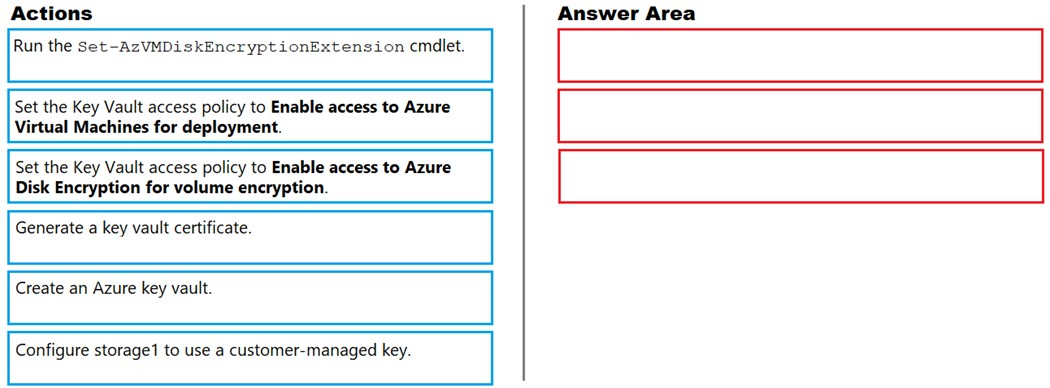
storage1という名前のAzure Storageアカウントと、VM1という名前のAzure仮想マシンがあります。VM1にはプレミアムSSDマネージドディスクがあります。

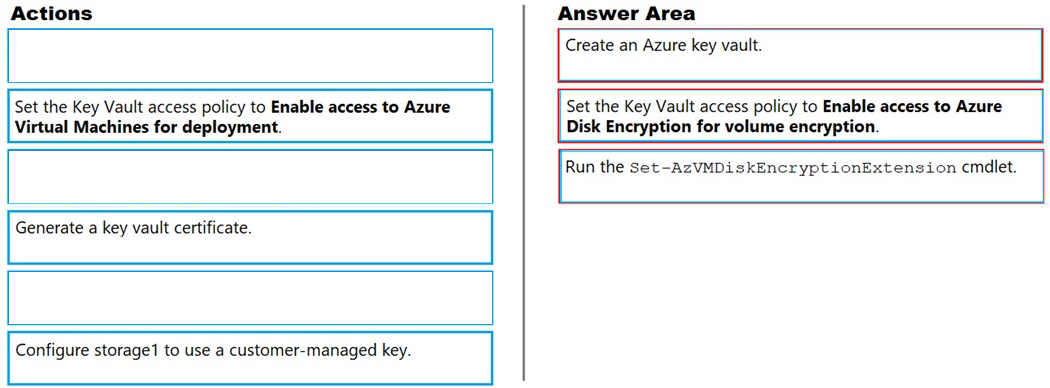
VM1に対してAzure Disk Encryptionを有効にする必要があります。

どの3つのアクションを順番に実行する必要がありますか？

回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解： 

リファレンス：

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

# Q.7シミュレーション-

あなたはSQLdb1 AzureのSQLデータベースのための高度なデータセキュリティを有効にする必要があります。このソリューションでは、Azure Advanced Threat Protection（ATP）アラートがUser1@contoso.comに送信されるようにする必要があります。

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

正解： *以下の説明を参照してください。*

1. Azureポータルで、検索ボックスに「SQL」と入力し、検索結果から[SQLデータベース]を選択してから、[SQLdb1]を選択します。または、左側のナビゲーションペインでSQLデータベースを参照します。

2. SQLdb1のプロパティで、[セキュリティ]セクションまで下にスクロールし、[高度なデータセキュリティ]を選択します。

3. [設定]アイコンをクリックします。

4. [データベースレベルで高度なデータセキュリティを有効にする]チェックボックスをオンにします。

5.確認プロンプトで[はい]をクリックします。

6.デフォルトでストレージアカウントが選択されていない場合は、ストレージアカウントでストレージアカウントを選択します。

7. [脅威保護の詳細設定]で、[アラートの送信先]ボックスにUser1@contoso.comと入力します。

8. [保存]ボタンをクリックして、変更を保存します。

参照：

<https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security>

# Q.8シミュレーション-

複数の仮想マシンディスクにAzureDiskEncryptionを使用することを計画しています。

Azure DiskEncryptionがKeyVault11641655Azureキーボールトからシークレットを取得できることを確認する必要があります。

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

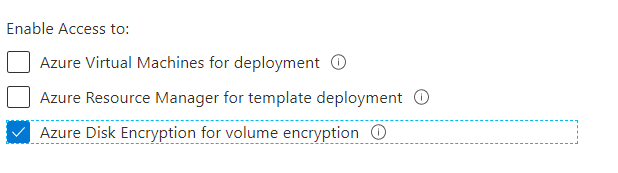
正解： *以下の説明を参照してください。*

1. Azureポータルで、検索ボックスに「Key Vaults」と入力し、検索結果から[Key Vaults]を選択してから、[KeyVault11641655]を選択します。または、

左側のナビゲーションペインで[キーボールト]を参照します。

2. Key Vaultのプロパティで、[設定]セクションまで下にスクロールし、[アクセスポリシー]を選択します。

3.ボリューム暗号化用にAzureDiskEncryptionを選択



します。

4.[保存]をクリックして変更を保存します。

# Q.9

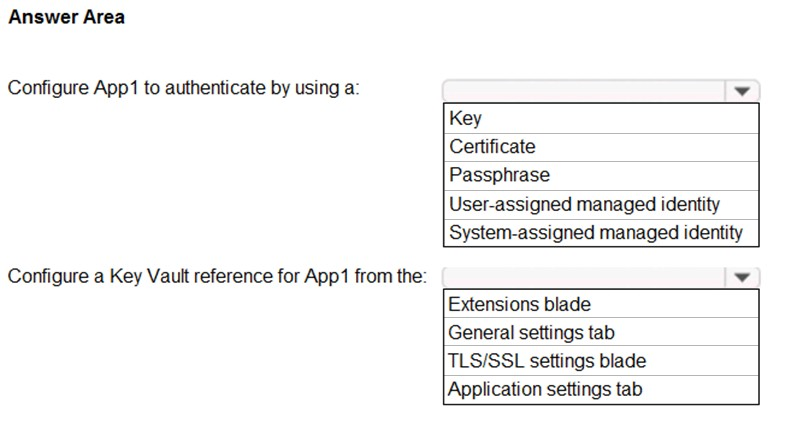
HOTSPOT-

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。



正解： 

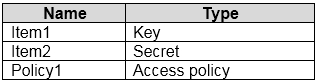
参照：

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

# Q.10

HOTSPOT -

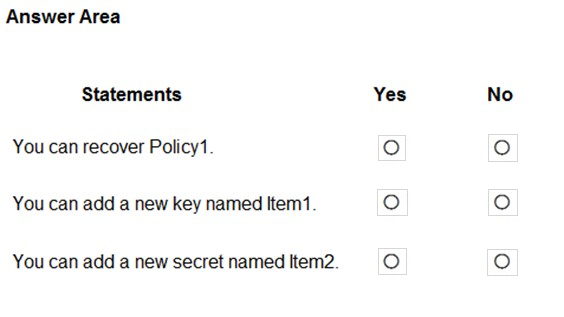
あなたは、次の表に示す項目が含まれていKeyVault1という名前アズールキー金庫を持っています。

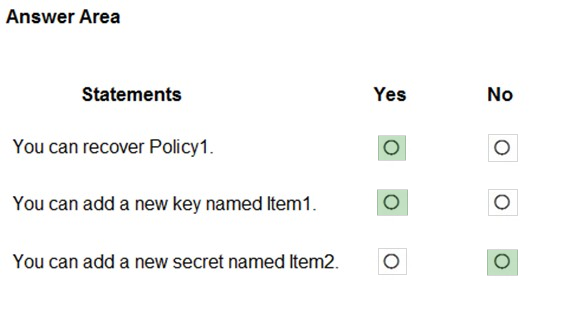


KeyVaultでは、次のイベントが順番に発生します。

* Item1が削除されます
* 管理者がソフト削除を有効にします。
* Item2とPolicy1が削除されます。

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



正解： 

参照：

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

# Q.11

SQL1という名前のAzureSQLデータベースサーバーがあります。

Advanced Threat Protection for SQL1をオンにして、すべての脅威検出タイプを検出します。

Advanced Threat Protectionはどのアクションを脅威として検出しますか？

1. ユーザーがテーブル内のレコードの50％以上を更新します。
2. ユーザーがSELECT \* FROMtable1としてサインインしようとしました。
3. ユーザーがdb\_ownerデータベースロールに追加されます。
4. ユーザーが同じテーブルから100を超えるレコードを削除します。

正解： *B*

Advanced Threat Protectionは潜在的なSQLインジェクションを検出できます：このアラートは、SQLインジェクションに対する特定されたアプリケーションの脆弱性に対してアクティブなエクスプロイトが発生したときにトリガーされます。これは、攻撃者が脆弱なアプリケーションコードまたはストアドプロシージャを使用して悪意のあるSQLステートメントを挿入しようとしていることを意味します。

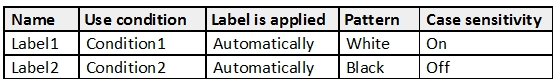
参照：

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

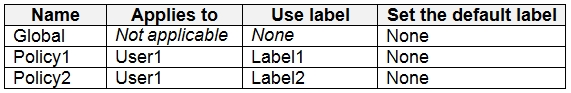
# Q.12

HOTSPOT-

次の表に示すように、Azure Information Protectionラベルがあります。



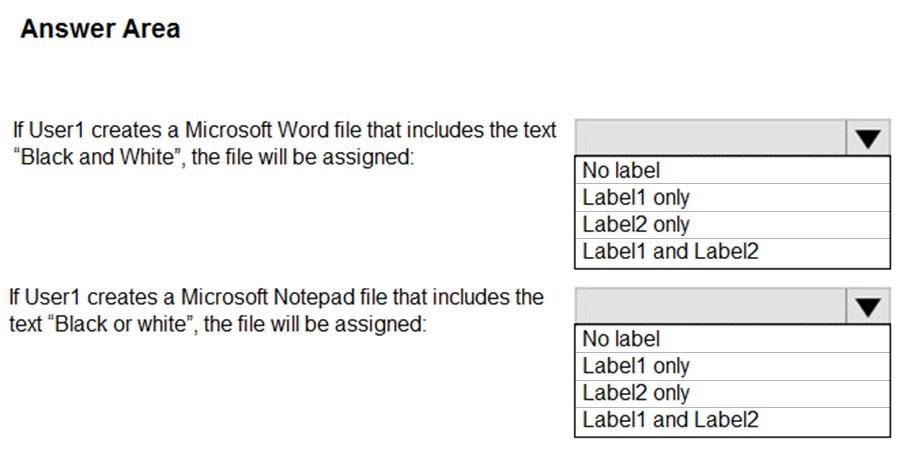
次の表に示すように、Azure Information Protectionポリシーがあります。

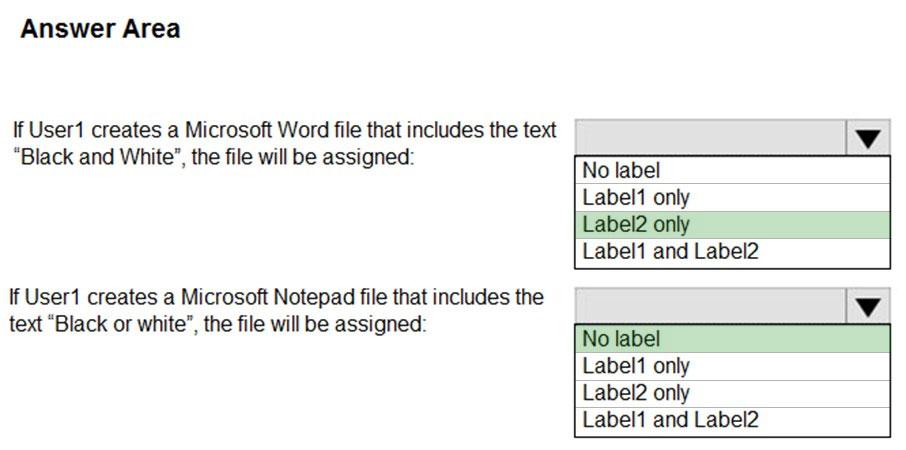


Azure Information Protectionがファイルにラベルを付ける方法を特定する必要があります。

何を特定する必要がありますか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

ボックス1：ラベル2のみ

-複数の条件が複数のラベル

1に適用される場合の評価方法ラベルは、ポリシーで指定した位置に従って、評価のために順序付けられます。最初に配置されたラベルが最も低くなります。位置（感度が最も低い）と最後に配置されたラベルの位置が最も高い（感度が最も高い）。

2.最も機密性の高いラベルが貼られています。

3.最後のサブラベルが適用されます。

ボックス2：ラベルなし

-自動分類は、ドキュメントが保存されるときにWord、Excel、およびPowerPointに適用され、電子メールが送信されるときにOutlookに適用されます。自動分類はMicrosoftメモ帳には適用されません。

参照：

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

# Q.13

あなたの会社はAzure DevOpsを使用しています。

コードが会社の品質基準および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に何を実装することをお勧めしますか？

1. ブランチフォルダ
2. ブランチのアクセス許可
3. ブランチポリシー
4. ブランチロック

正解： *C*

ブランチポリシーは、チームが開発の重要なブランチを保護するのに役立ちます。ポリシーは、チームのコード品質と変更管理基準を適用します。

参照：

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts>

# Q.14シミュレーション-

あなたはUser2-11641655がKeyVault11641655のためのすべてのキーの権限を持っていることを確認する必要があります。

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

正解： *以下の説明を参照してください。*

ユーザーにKeyVault SecretsOfficerの役割を割り当てる必要があります。

1. Azureポータルで、検索ボックスに「Key Vaults」と入力し、検索結果から[Key Vaults]を選択してから、[KeyVault11641655]を選択します。または、

左側のナビゲーションペインで[キーボールト]を参照します。

2.主要なボールトプロパティで、[アクセス制御（IAM）]を選択します。

3. [役割の割り当ての追加]セクションで、[追加]ボタンをクリックします。

4. [役割]ボックスで、ドロップダウンリストから[Key Vault SecretsOfficer]の役割を選択します。

5. [選択]ボックスで、User2-11641655と入力し始め、検索結果からUser2-11641655を選択します。

6. [保存]ボタンをクリックして、変更を保存します。

# Q.15

WebApp1という名前のAzure Webアプリがあります。

証明書をWebApp1にアップロードします。

WebApp1のアプリコードから証明書にアクセスできるようにする必要があります。

あなたは何をするべきか？

1. ユーザーが割り当てたマネージIDをWebApp1に追加します。
2. WebApp1構成にアプリの設定を追加します。
3. WebApp1のためのシステムによって割り当てられた管理対象IDを有効にします。
4. WebApp1の設定にバインディングTLS / SSL。

正解： *B*

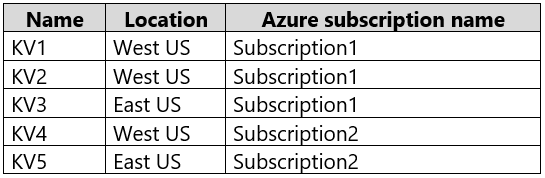
リファレンス：

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code>

# Q.16

HOTSPOT-

次の表に示すAzureキーボールトがあります。

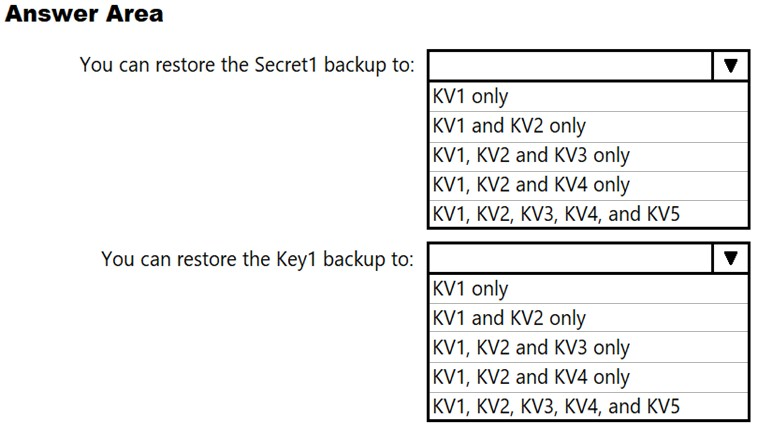


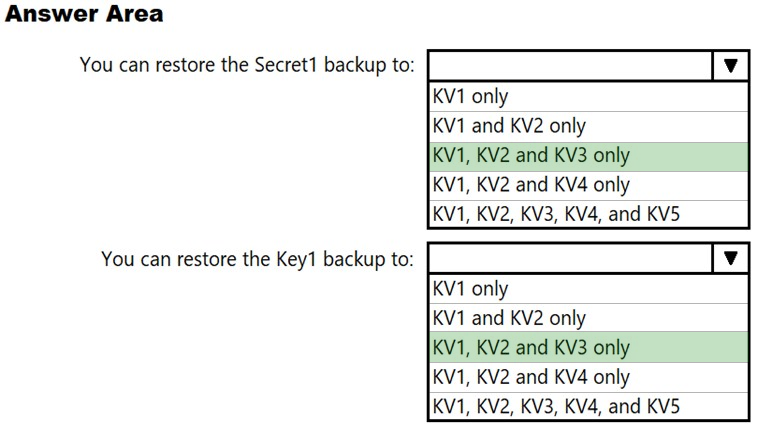
KV1は、Secret1という名前のシークレットと、Key1という名前の管理対象ストレージアカウントのキーを格納します。

Secret1とKey1をバックアップします。

各バックアップをどの主要なボールトに復元できますか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

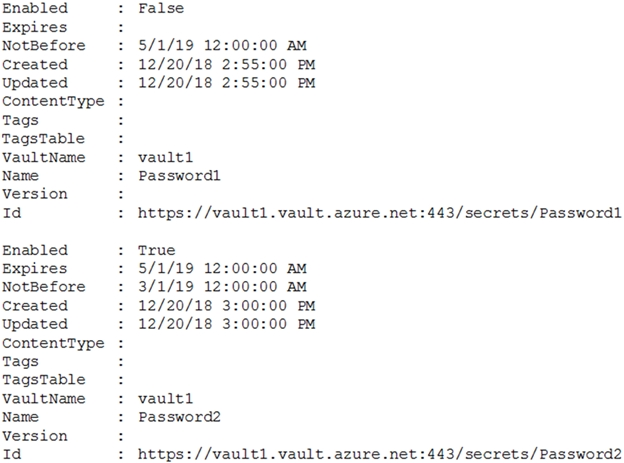
バックアップは、同じサブスクリプションおよび同じ地域の主要なボールトにのみ復元できます。同じ地域の別の地域に復元できます。

# Q.17

HOTSPOT-

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。

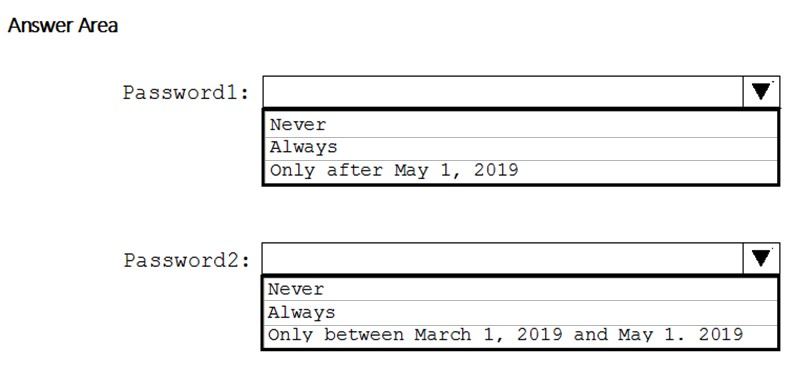
2019年1月1日、Vault1は次のシークレットを保存します。

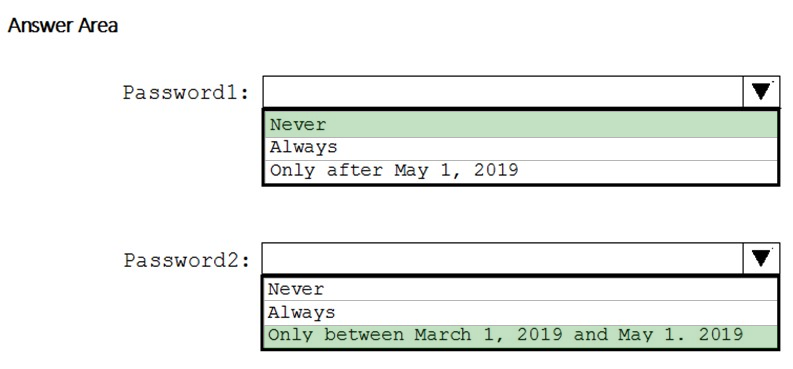


各シークレットはいつアプリケーションで使用できますか？回答するには、回答領域で適切なオプションを選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



正解： 

ボックス1：なし

-Password1は無効になっています。

ボックス2：2019年3月1日から5月1日までのみ

パスワード2：



参照：

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute>

# Q.18

webapp1という名前のAzureWebアプリがあります。

Azureリポジトリを使用して、webapp1の継続的デプロイを構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？

1. an Azure Application Insights service
2. an Azure DevOps organization
3. an Azure Storage account
4. an Azure DevTest Labs lab

正解： *B*

Azureリポジトリを使用するには、Azure DevOps組織がAzureサブスクリプションにリンクされていることを確認してください。

参照：

<https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

# Q.19

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Azure AD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Azure Key Vault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。

何を設定する必要がありますか？

1. 管理者の同意なしのアプリケーション許可
2. 管理者の同意なしに委任された権限
3. 管理者の同意が必要な委任された権限
4. 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： *B*

委任されたアクセス許可-クライアントアプリケーションは、サインインしたユーザーとしてWeb APIにアクセスする必要がありますが、アクセスは選択したアクセス許可によって制限されます。このタイプの権限は、権限に管理者の同意が必要でない限り、ユーザーが付与できます。

不正解：

A、D：アプリケーションのアクセス許可-クライアントアプリケーションは、それ自体としてWeb APIに直接アクセスする必要があります（ユーザーコンテキストはありません）。このタイプのアクセス許可には管理者の同意が必要であり、パブリック（デスクトップおよびモバイル）クライアントアプリケーションでも使用できません。

参照：

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

# Q.20

DRAGDROP-

あなたの会社にはcontoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。

同社はApp1という名前のアプリケーションを開発しています。

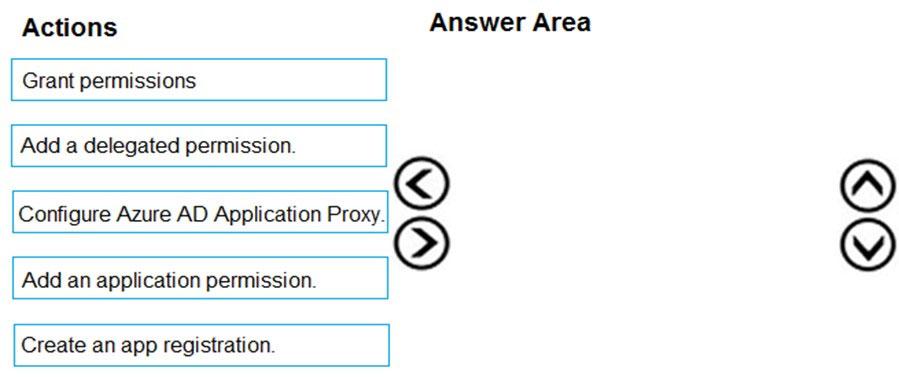
App1は、Windows Server 2016を実行するサーバー上でサービスとして実行されます。App1はcontoso.comに対して認証され、Microsoft Graphにアクセスしてディレクトリデータを読み取ります。

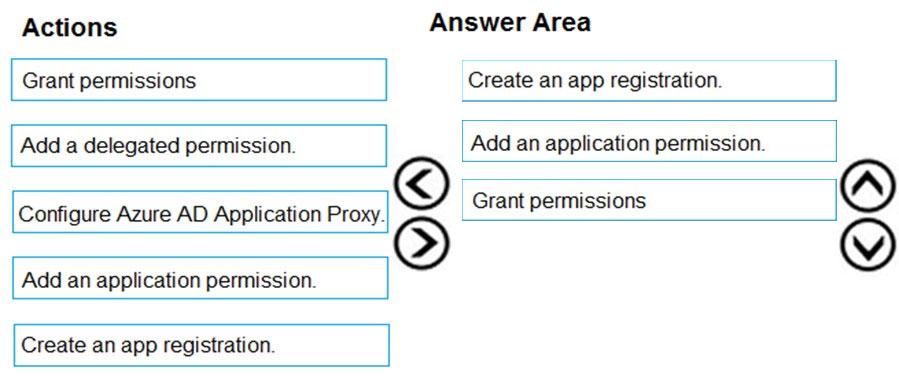
最低限必要な権限をApp1に委任する必要があります。

Azureポータルから順番に実行する必要がある3つのアクションはどれですか？

回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解： 

ステップ1：アプリ登録を作成する。最初に、アプリケーションを作成/登録する必要があります。

ステップ2：アプリケーションのアクセス許可を追加するアプリケーションのアクセス許可は、サインインしたユーザーがいない状態で実行されるアプリによって使用されます。

ステップ3：権限を付与する

不正解：

* 委任された権限は、サインインしたユーザーが存在するアプリによって使用されます。
* Azure Active Directoryのアプリケーションプロキシは、オンプレミスのWebアプリケーションへの安全なリモートアクセスを提供します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent>

# Q.21

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という名前のモバイルアプリケーションを開発しています。App1は、OAuth2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。

App1をAzure ADに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入手する必要がありますか？

1. リダイレクトURI
2. 返信URL
3. キー
4. アプリケーションID

正解： *A*

ネイティブアプリケーションの場合、AzureADがトークン応答を返すために使用するリダイレクトURIを指定する必要があります。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

# Q.22

Azureポータルから、Azureポリシーを構成しています。

DeployIfNotExist、AuditIfNotExist、Append、およびDenyエフェクトを使用するポリシーを割り当てることを計画しています。

割り当てに管理されたIDが必要な効果はどれですか？

1. AuditIfNotExist
2. append
3. DeployIfNotExist
4. deny

正解： *C*

AzureポリシーがdeployIfNotExistsポリシー定義でテンプレートを実行する場合、マネージIDを使用して実行します。

参照：

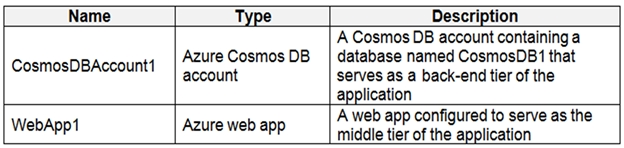
<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

# Q.23

HOTSPOT-

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。

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ことを計画しています。

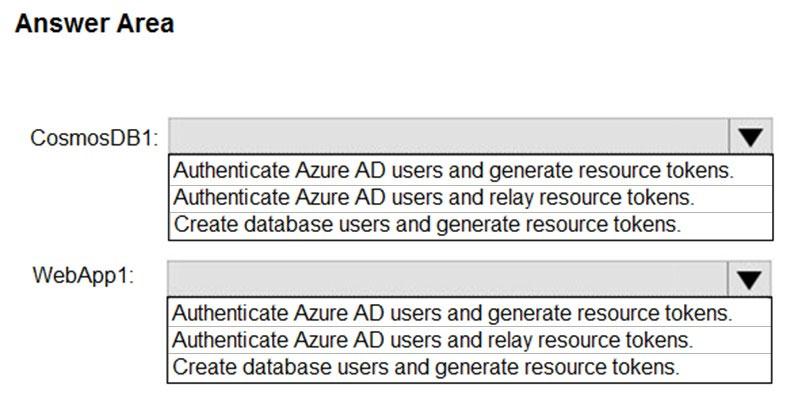


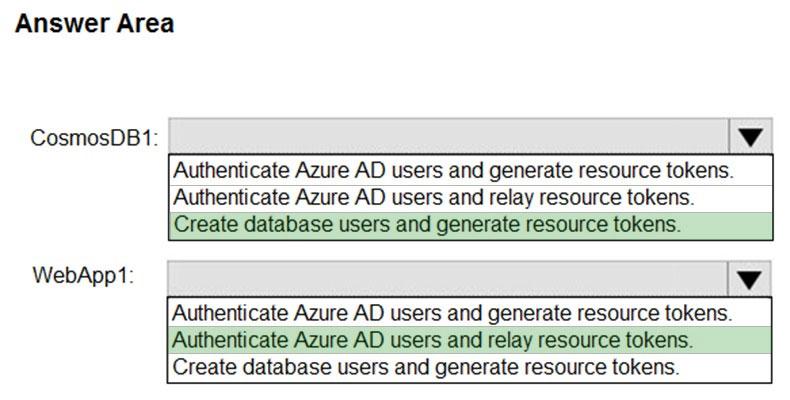
ユーザーは、Azure ADユーザーアカウントを使用して認証し、リソーストークンを使用してCosmos DBアカウントにアクセスします。

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

リソースごとに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ます。



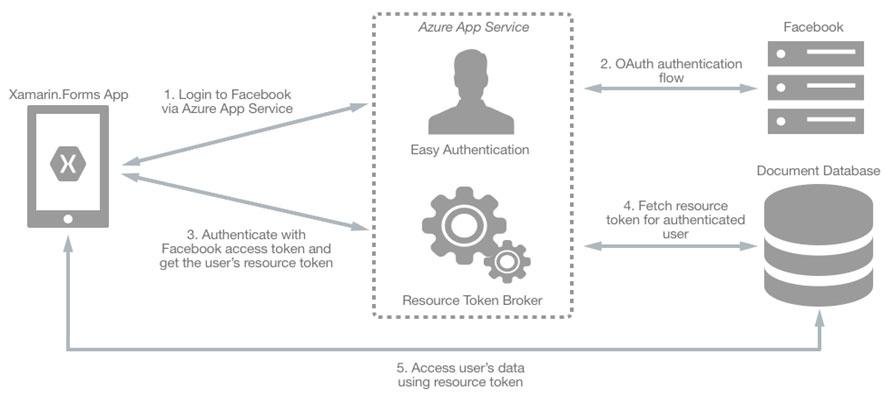
正解： 

CosmosDB1：データベースユーザーを作成し、リソーストークンを生成します。

Azure Cosmos DBリソーストークンは、クライアントが付与されたアクセス許可に従ってAzure Cosmos DBアカウント内の特定のリソースを読み取り、書き込み、および削除できるようにするための安全なメカニズムを提供します。

WebApp1：Azure ADユーザーを認証し、リソーストークンを中継するリソーストークン

を要求、生成、およびモバイルアプリケーションに配信するための一般的なアプローチは、**リソーストークンブローカー**を使用することです。次の図は、サンプルアプリケーションがリソーストークンブローカーを使用してドキュメントデータベースデータへのアクセスを管理する方法の概要を示しています。



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

# Q.24

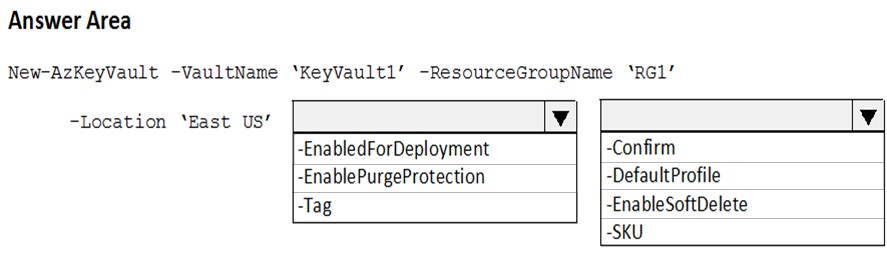
HOTSPOT-

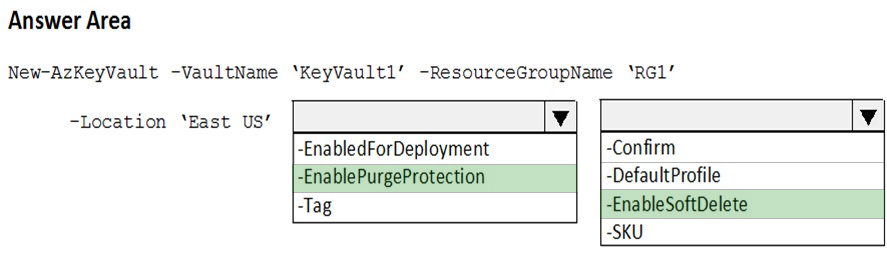
Azureキーボールトを作成する必要があります。ソリューションでは、キーボールトから削除されたオブジェクトが90日間保持されるようにする必要があります。

コマンドをどのように完了する必要がありますか？回答するには、回答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。

ホットエリア：



正解： 

ボックス1：-EnablePurgeProtection-

指定されている場合、このボールトの即時削除に対する保護が有効になります。ソフト削除も有効にする必要があります。

ボックス2：-EnableSoftDelete-

このキーボールトに対してソフト削除機能を有効にすることを指定します。ソフト削除が有効になっている場合、猶予期間中、削除後にこのキーボールトとその内容を回復できます。

参照：

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

# Q.25

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で、Secret1という名前のシークレットを作成します。

アプリケーション開発者は、アプリケーションをAzure Active Directory（Azure AD）に登録します。

アプリケーションがSecret1を使用できることを確認する必要があります。

あなたは何をするべきか？

1. Azure ADで、役割を作成します。
2. Azure Key Vaultで、キーを作成します。
3. Azure Key Vaultで、アクセスポリシーを作成します。
4. Azure ADで、AzureADアプリケーションプロキシを有効にします。

正解： *A*

Azure Key Vaultはストアの資格情報と他のキーと秘密への道を提供していますが、あなたのコードは、それらを取得するために、Key Vaultに対して認証する必要があります。

Azureリソースの管理されたIDの概要では、AzureサービスにAzure Active Directory（Azure AD）で自動的に管理されたIDを提供することにより、この問題の解決を簡単にします。このIDを使用して、コードにクレデンシャルがなくても、Key Vault を含むAzure AD認証をサポートする任意のサービスに対して認証できます。

例：システムによって割り当てられたマネージIDがAzure VMでどのように機能するかVMがIDを取得したら、サービスプリンシパル情報を使用して、VMにAzureリソースへのアクセスを許可します。Azure Resource Managerを呼び出すには、Azure ADでロールベースのアクセス制御（RBAC）を使用して、VMサービスプリンシパルに適切なロールを割り当てます。Key Vaultを呼び出すには、KeyVaultの特定のシークレットまたはキーへのアクセスをコードに許可します。

参照：

<https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net>

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

# Q.26

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および復号化できることを確認する必要があります。

開発者に提供する必要がある2つの情報はどれですか？

それぞれの正解は、解決策の一部を示しています。

注：正しい選択はそれぞれ1ポイントの価値があります。

1. 保存されたアクセスポリシー
2. 共有アクセス署名（SAS）
3. 列の暗号化キー
4. ユーザーの資格情報
5. 列マスターキー

正解： *CE*

Always Encryptedは、列暗号化キーと列マスターキーの2種類のキーを使用します。列暗号化キーは、暗号化された列のデータを暗号化するために使用されます。列マスターキーは、1つ以上の列暗号化キーを暗号化するキー保護キーです。

参照：

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

# Q.27

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

すべてのユーザーは、Windows 10を実行し、ハイブリッドAzure ADに参加しているコンピューターを持っています。

Azure AD 認証をサポートするように構成されたAzure SQL データベースがあります。

データベース開発者は、Microsoft SQL Server Management Studio（SSMS）を使用してSQLデータベースに接続し、オンプレミスのActive Directoryアカウントを使用して認証する必要があります。

SSMSからSQLデータベースに接続するために使用する認証方法を開発者に伝える必要があります。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。

開発者に使用するように指示する必要がある認証方法はどれですか？

1. SQLログイン
2. Active DirectoryのユニバーサルMFAサポート付き
3. Active Directory 統合認証
4. Active Directory パスワード

正解： *C*

Azure ADは、最初のAzureAD管理対象ドメインにすることができます。Azure ADは、Azure ADとフェデレーションされているオンプレミスのActive Directoryドメインサービスにすることもできます。

Azure AD IDを使用したSSMSまたはSSDTを使用した接続

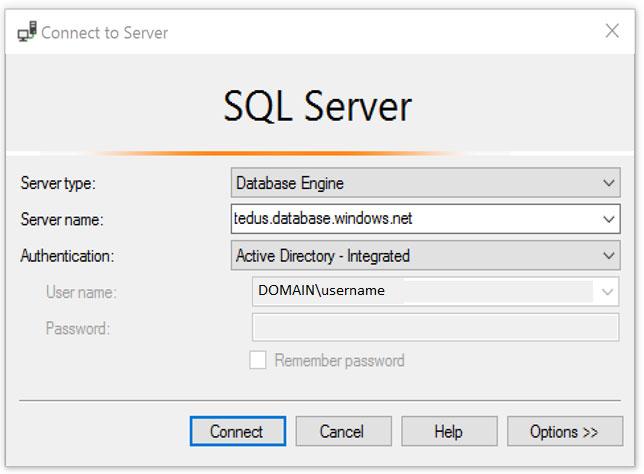
次の手順は、SQL Server ManagementStudioまたはSQLServerデータベースツールを使用して、Azure AD IDを使用してSQLデータベースに接続する方法を示しています。

**ActiveDirectory統合認証**

フェデレーションドメインからAzure Active Directoryクレデンシャルを使用してWindowsにログインしている場合は、この方法を使用します。

1. Management StudioまたはData Toolsを起動し、[サーバーに接続]（または[データベースエンジンに接続]）ダイアログボックスの[認証]ボックスで、[ActiveDirectory]

- [統合]を選択します。接続には既存のクレデンシャルが表示されるため、パスワードは不要であるか、入力できます。



2. [オプション]ボタンを選択し、[接続のプロパティ]ページの[データベースに接続]ボックスに、接続するユーザーデータベースの名前を入力します。

（ADドメイン名またはテナントIDג€オプションは、MFA接続オプションを備えたUniversalでのみサポートされます。それ以外の場合はグレー表示されます。）

参照：

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

# Q.28

DRAGのDROP -

あなたはAzureストレージは、名前のcontosostorage1とContosokeyvault1という名前Azure Key Vaultを占め含まSub1を命名Azureのサブスクリプションを持っています。

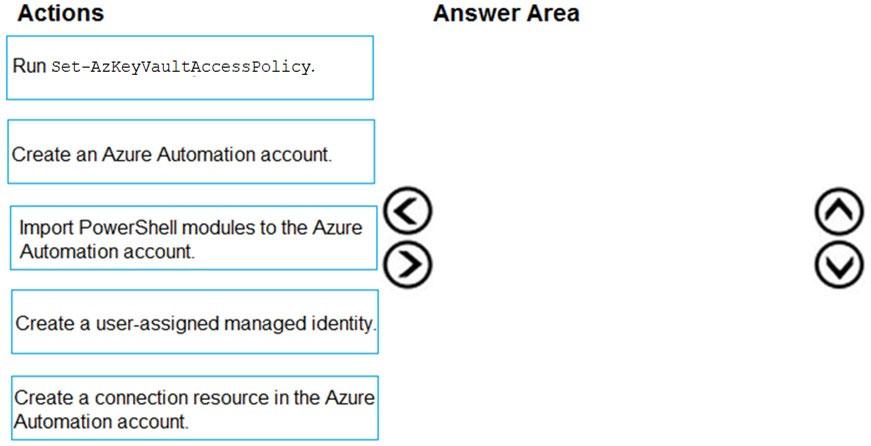
contosostorage1のキーをローテーションしてContosokeyvault1に格納するAzure Automation Runbook を作成する予定です。

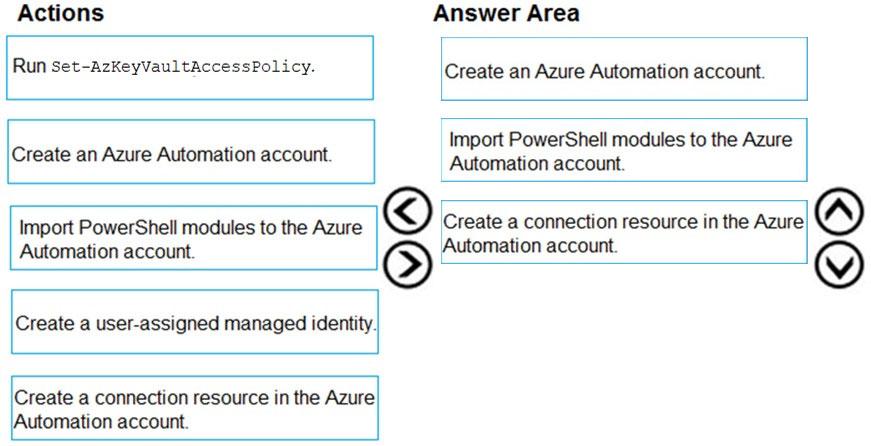
Runbookを実装できるようにするには、前提条件を実装する必要があります。

どの3つのアクションを順番に実行する必要がありますか？

回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解： 

ステップ1：Azure Automation アカウントを作成する

ステップ2：PowerShellモジュールをAzure Automationアカウントにインポートする

ステップ3：Azure Automationアカウントで接続リソースを作成する

Azure Automation Tutorial Script サンプル Runbookから取得した以下のサンプルコードを使用して、実行アカウントを使用して認証し、管理することができます。

Runbookを使用したResourceManagerリソース。AzureRunAsConnectionは、上記の「アカウントとして実行」を作成したときに自動的に作成される接続アセットです。これは、[アセット]-> [接続]にあります。認証コードの後で、上記と同じコードを実行して、ボールトからすべてのキーを取得します。

$connectionName = "AzureRunAsConnection"

try

{

# Get the connection "AzureRunAsConnection "

$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName

"Logging in to Azure..."

Add-AzureRmAccount `

-ServicePrincipal `

-TenantId $servicePrincipalConnection.TenantId `

-ApplicationId $servicePrincipalConnection.ApplicationId `

-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint

}

catch {

if (!$servicePrincipalConnection)

{

$ErrorMessage = "Connection $connectionName not found."

throw $ErrorMessage

} else{

Write-Error -Message $\_.Exception

throw $\_.Exception

}

}

Get-AzureKeyVaultKey -VaultName YoutubeVault

参照：

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

# Q.29

HOTSPOT-

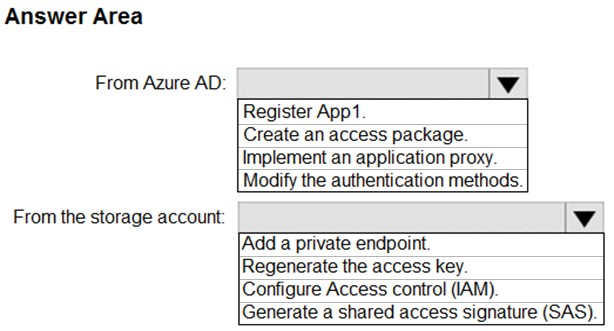
container1という名前のBLOBコンテナーとApp1という名前のクライアントアプリケーションを含むAzure Storage アカウントがあります。

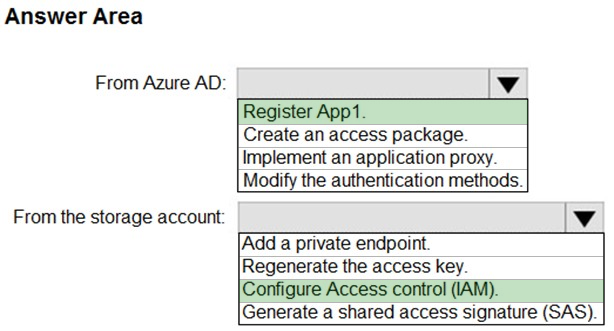
Azure Active Directory（Azure AD）認証を使用して、container1へのApp1アクセスを有効にする必要があります。

あなたは何をするべきか？回答するには、回答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。

ホットエリア：



正解： 

Reference:

<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/>

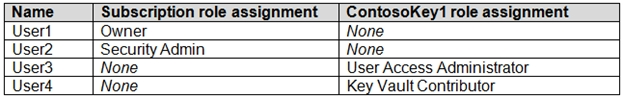
<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md>

# Q.30

HOTSPOT-

ContosoKey1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。

次の表に示すように、ユーザーを作成してロールを割り当てます。

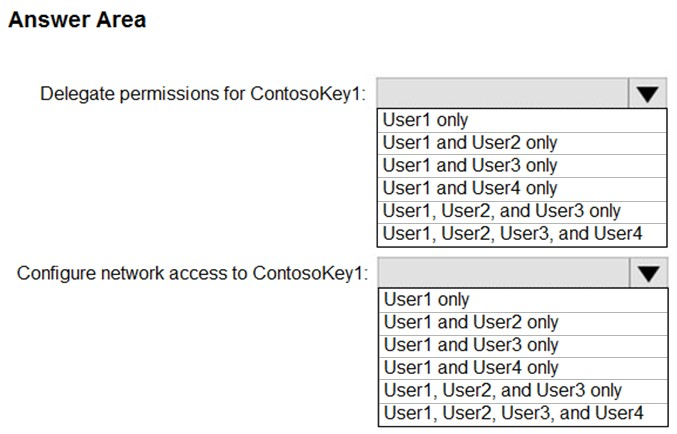


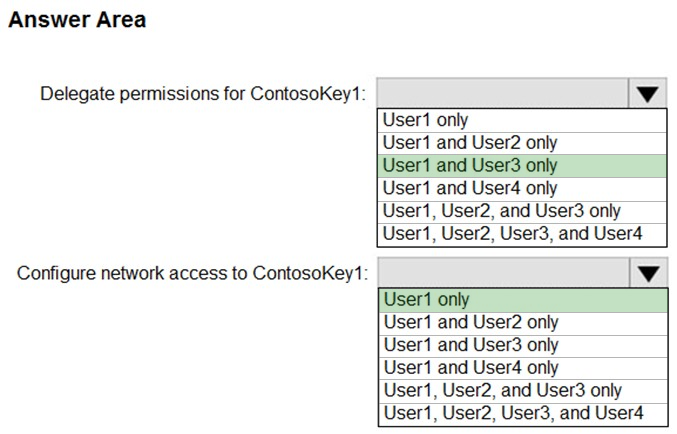
次のアクションを実行できるユーザーを特定する必要があります。

* ContosoKey1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ます。



正解： 

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

# Q.31

4つのAzure SQL マネージドインスタンスを含むAzureサブスクリプションがあります。

SQLインジェクション攻撃に対するマネージドインスタンスの脆弱性を評価する必要があります。

あなたは最初に何をすべきですか？

1. Azure Sentinel ワークスペースを作成します。
2. 高度なデータセキュリティを有効にします。
3. SQL Health CheckソリューションをAzure Monitorに追加します。
4. Azure Advanced Threat Protection（ATP）インスタンスを作成します。

正解： *B*

# Q.32

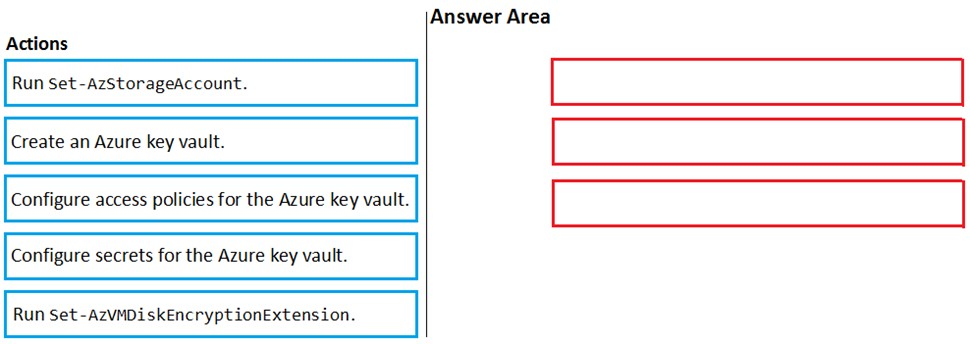
DRAGDROP-

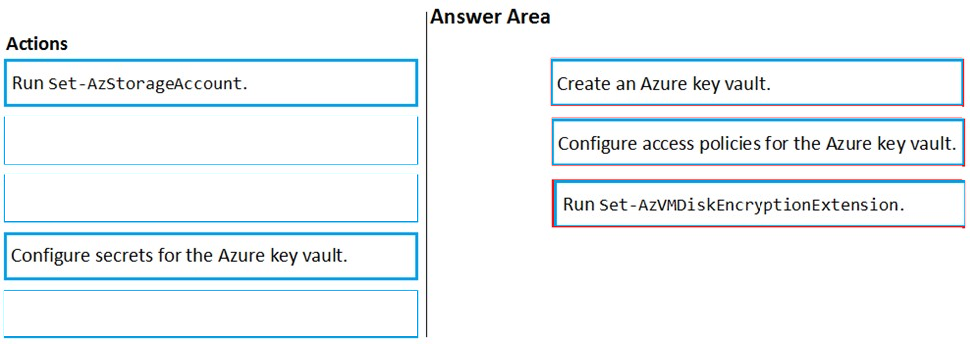
Sub1という名前のAzureサブスクリプションがあります。Sub1には、Windows Server 2016を実行するVM1という名前のAzure仮想マシンが含まれています。Azure Disk Encryptionを使用してVM1ディスクを暗号化する必要があります。

どの3つのアクションを順番に実行する必要がありますか？

回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解： 

リファレンス：

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

# Q.33

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。

次の構成を持つAzureキーボールトを作成します。

* 名前：Vault5
* リージョン：米国西部
* リソースグループ：RG1

VM1でAzureディスク暗号化を有効にするには、Vault5を使用する必要があります。ソリューションは、Azure Backupを使用したVM1のバックアップをサポートする必要があります。

どの主要な Vault 設定を構成する必要がありますか？

1. Access Policies
2. Secrets
3. Keys
4. Locks

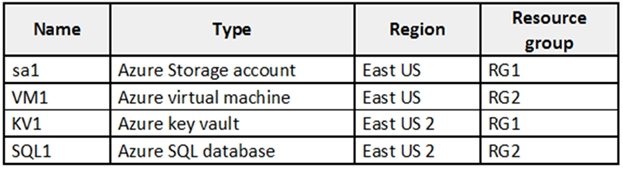
正解： *A*

リファレンス：

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

# Q.34

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。



含まれているデータベースユーザーを使用して、VM1にSQL1上のデータベースへの安全なアクセスを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？

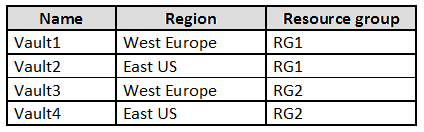
1. VM1上の管理対象IDを有効にします。
2. KV1に秘密を作成します。
3. 設定SQL1上のサービスエンドポイント。
4. KV1でキーを作成します。

正解：B

接続文字列のことを問うている。

# Q.35

次の表に示すAzureキーボールトを含むSub1という名前のAzureサブスクリプション



があります。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ボールトに保存できますか？

1. Vault1またはVault3のみ
2. Vault1、Vault2、Vault3、またはVault4
3. Vault1のみ
4. Vault1のみVault2

正解： *A*

**暗号化シークレットが地域の境界を越えないようにするために、Azure Disk Encryptionでは、KeyVaultとVMを同じ地域に同じ場所に配置する必要があります。**暗号化するVMと同じリージョンにあるKeyVaultを作成して使用します。

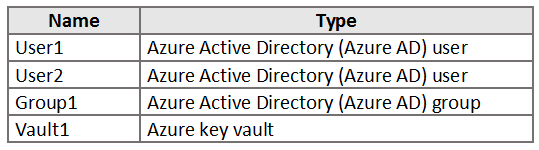
参照：

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

# Q.36

HOTSPOT-

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。



User1はGroup1のメンバーです。

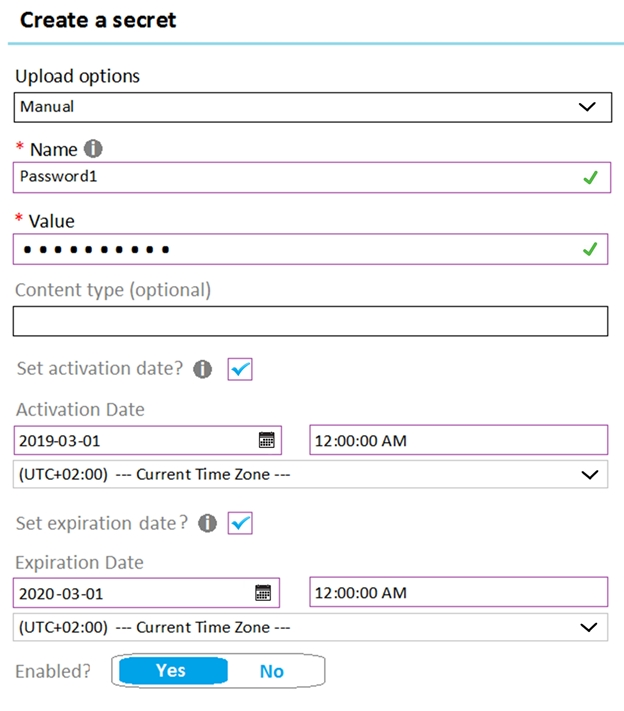
Group1とUser2には、Vault1のKey Vault Contributor ロールが割り当てられています。

2019年1月1日に、Vault1 にシークレットを作成します。

シークレットは、展示に示されているように構成されています。

展示では日付形式YYYY-MM-DDが使用されています。

（[Exhibit]タブをクリックします。）



User2にはVault1へのアクセスポリシーが割り当てられています。

ポリシーの構成は次のとおりです。

* キー管理操作：取得、一覧表示、および復元
* 暗号化操作：キーの復号化とアンラップ
* 秘密管理操作：取得、一覧表示、および復元

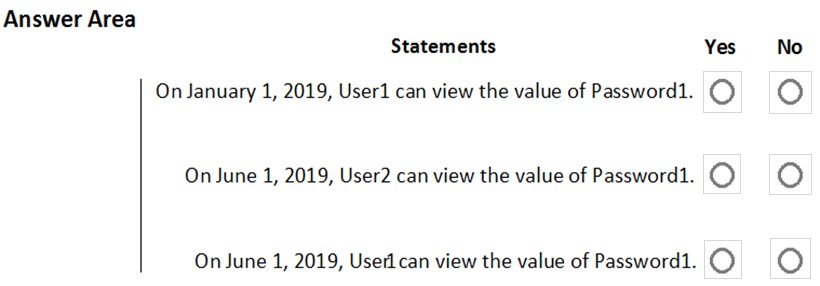
Group1には、Vault1へのアクセスポリシーが割り当てられています。

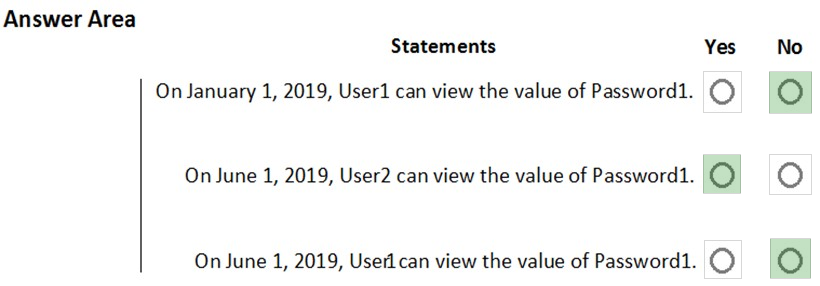
ポリシーの構成は次のとおりです。

* キー管理操作：取得と回復
* シークレット管理操作：一覧表示、バックアップ、および回復

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

それ以外の場合は、[いいえ]を選択します。

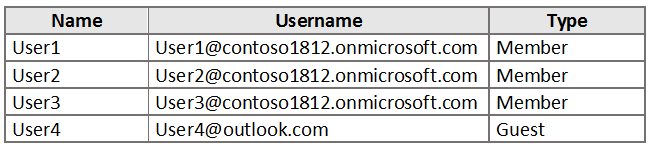


正解： 

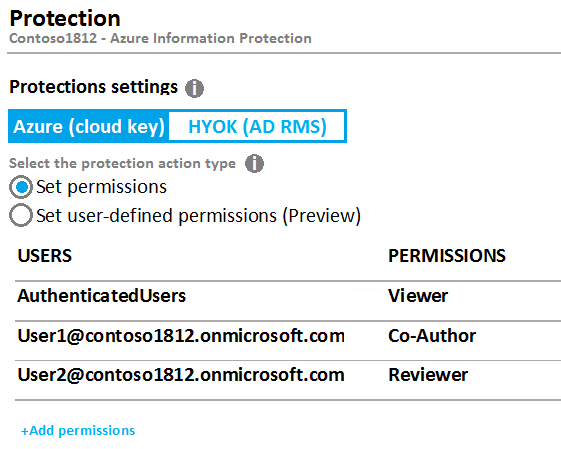
# Q.37

HOTSPOT -

あなたは、次の表に示すユーザーが含まcontoso1812.onmicrosoft.comという名前のAzure Active Directoryの（アズールAD）のテナントを持っています。



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、展示に示されているように構成されています。（[Exhibit]タブをクリックします。）

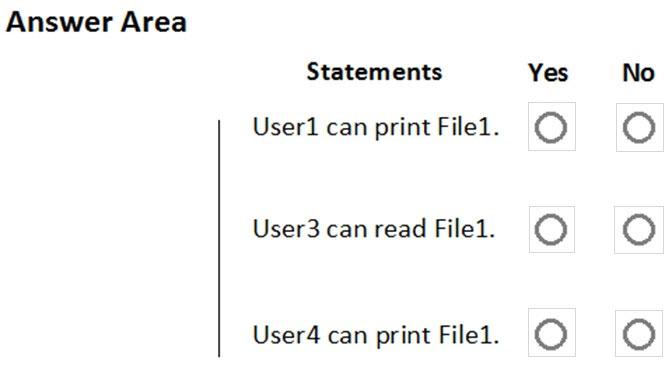


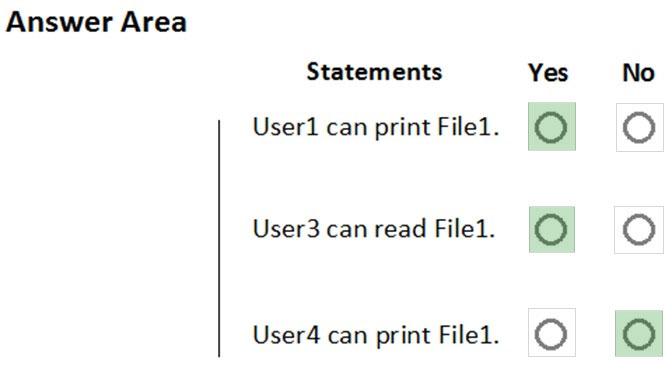
Label1はFile1という名前のファイルに適用されます。

次の各ステートメントについて、ステートメントがtrueの場合は[はい]を選択し、そうでない場合は[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。

ホットエリア：



正解： 

# Q.38シミュレーション-

あなたはHTTP rg1lod10598168n1 Azureストレージアカウントへの接続を防止する必要があります。

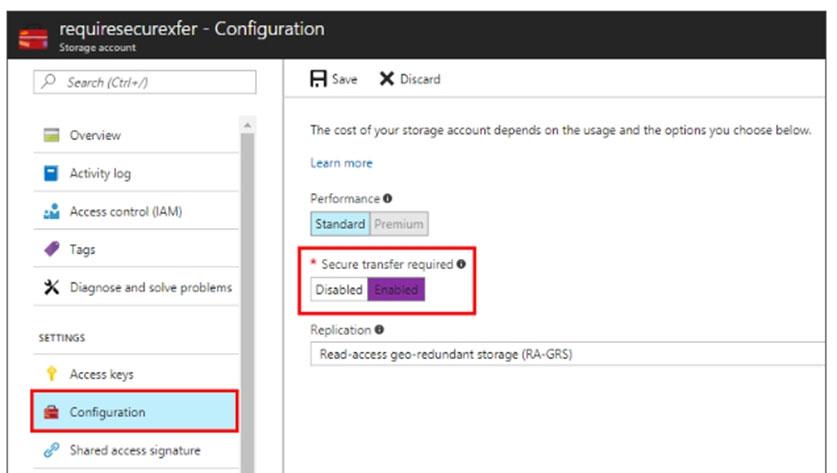
このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

「安全な転送が必要」機能がAzureStorageアカウントでサポートされるようになりました。この機能は、安全な接続を介してアカウントへのすべてのリクエストを強制することにより、ストレージアカウントのセキュリティを強化します。この機能はデフォルトで無効になっています。

1. Azure Portalで、AzureStorageアカウントrg1lod10598168n1を選択します。

2. [構成]を選択し、[セキュア転送が必要]を選択します。



参照：

<https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storage/mp/82475>

# Q.39

DRAG DROP-

ネットワークには、contoso.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。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、storage1という名前のAzure Storage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。

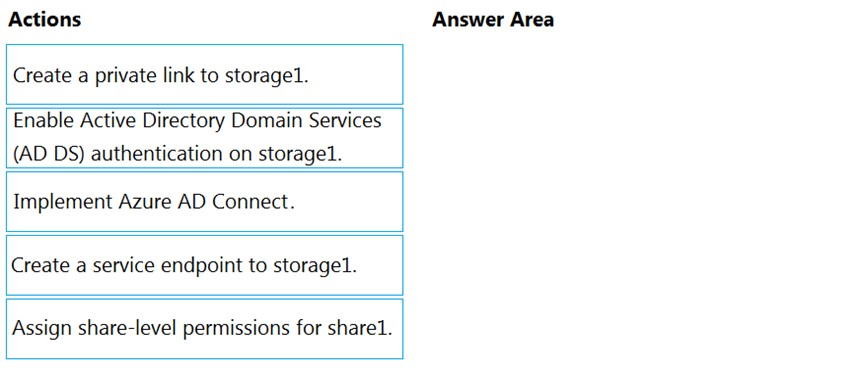
現在、ドメインとテナントは統合されていません。

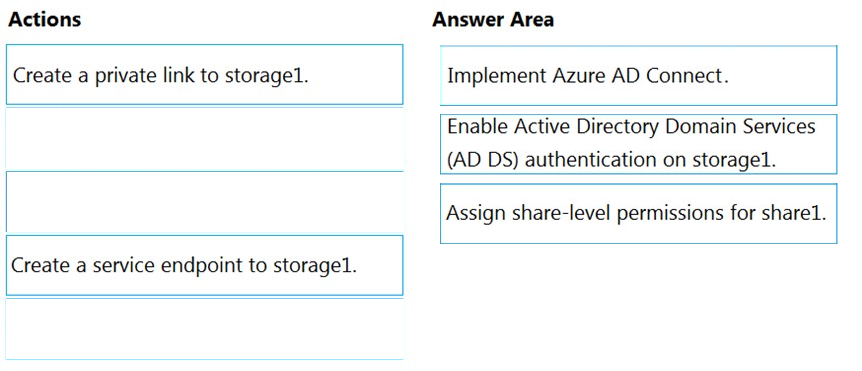
User1がドメイン資格情報を使用してshare1にアクセスできることを確認する必要があります。

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。

選択して配置：



正解： 

リファレンス：

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable>

# Q.40シミュレーション-

あなたはrg1lod10598168n1 AzureストレージアカウントがKeyVault10598168アズールキー保管庫に格納されている鍵を用いて暗号化されていることを確認する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

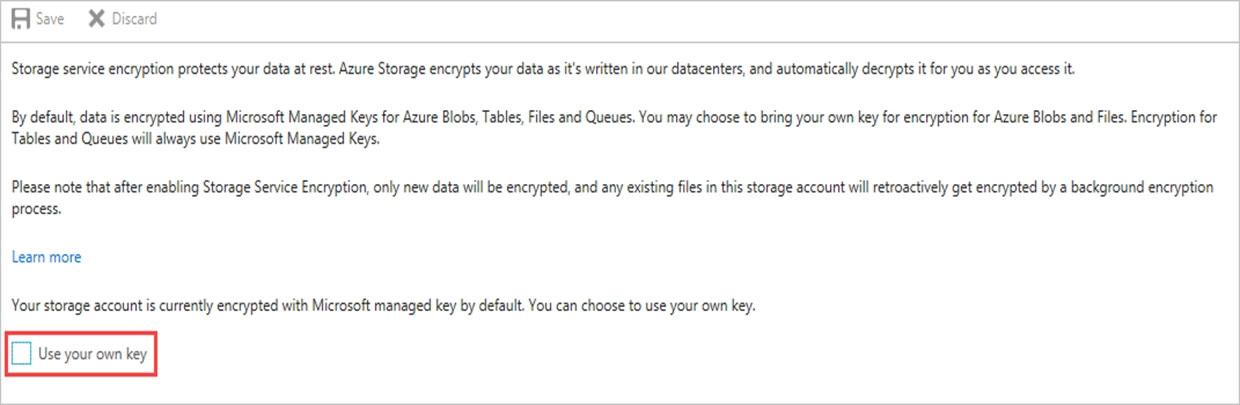
正解： *以下の説明を参照してください。*

手順1：Azureポータルで顧客管理キーを有効にするには、次の手順に従い

ます。

1.ストレージアカウントrg1lod10598168n1に移動します。

2.ストレージアカウントの[設定]ブレードで、[暗号化]をクリックします。次の図に示すように、[独自のキーを使用する]オプションを選択します。



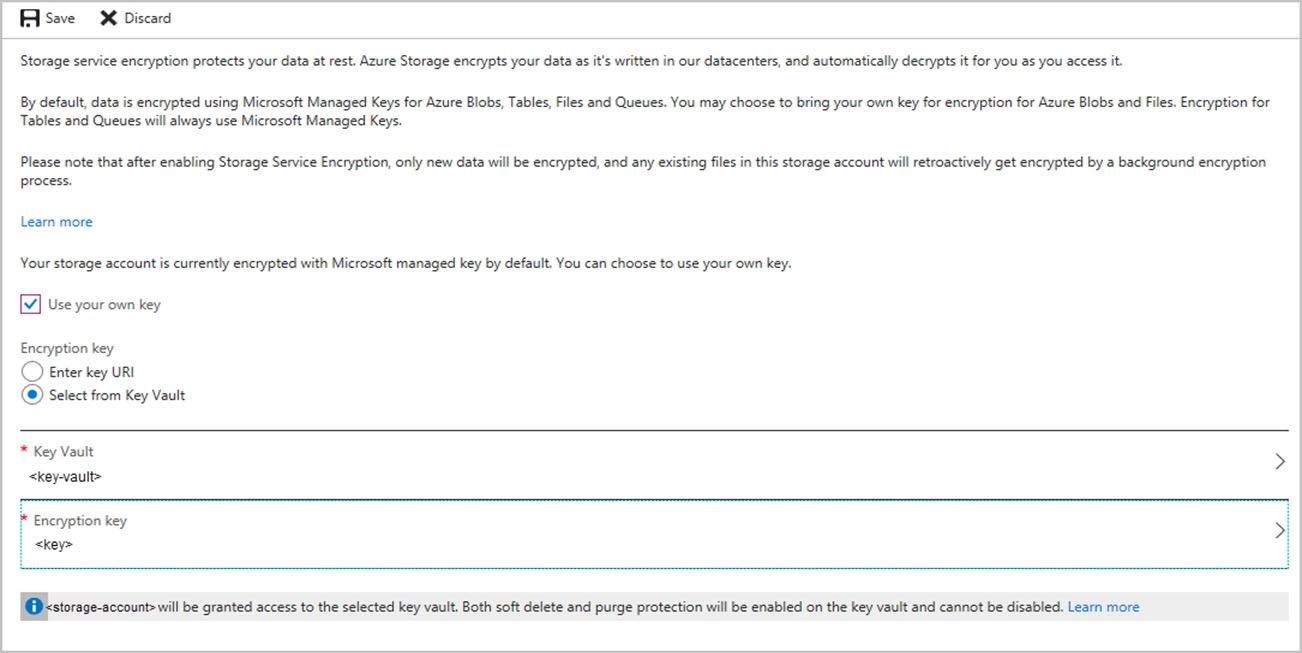
手順2：キーボールトからキー

を指定するキーボールトからキーを指定するには、最初に、キーを含むキーボールトがあることを確認します。キーボールトからキーを指定するには、次の手順に従います。

4.[キーボールトから選択]オプションを選択します。

5.使用するキーを含むキーボールトKeyVault10598168を選択します。

6.キーボールトからキーを選択します。



参照：

<https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal>

# Q.41

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。

あなたは最初に何をすべきですか？

1. Azure Front Door をデプロイします。
2. WebApp1に拡張子を追加します。
3. Azure Firewall をデプロイします。

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

# Q.42

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を監査する予定です。

監査ログの宛先を構成する必要があります。ソリューションは、次の要件を満たしている必要があります。

* Kustoクエリ言語を使用したイベントのクエリをサポートします。
* 管理作業を最小限に抑えます。

何を設定する必要がありますか？

1. イベントハブ
2. ストレージアカウント
3. Log Analytics ワークスペース

正解： *C*

リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

# 質問文

紹介情報

ケーススタディ-

これはケーススタディです。ケーススタディは個別にタイミングを合わせていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。この試験に含まれるすべての質問を指定された時間内に確実に完了することができるように、時間を管理する必要があります。

ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。

このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。

ケーススタディを開始するには-

このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたら、[質問]ボタンをクリックして質問に戻ります。

概要

-Contoso、Ltd。は、モントリオールに本社を置き、シアトルとニューヨークに2つの支店を持つコンサルティング会社です。

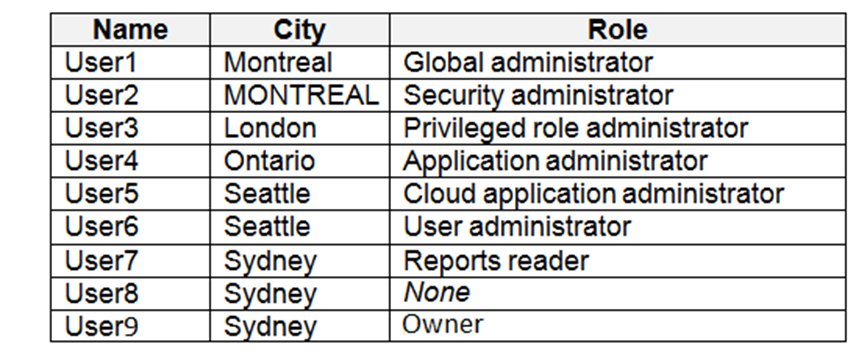
同社は、サーバーインフラストラクチャ全体をAzureでホストしています。

Contosoには、Sub1と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。両方のサブスクリプションは、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ます。

環境を既存の-

AzureのAD -

Contoso.comは、次の表に示すユーザーが含まれています。



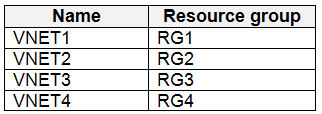
Contoso.comには、次の表に示すセキュリティグループが含まれています。



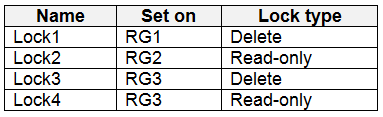
Sub1-

Sub1には、RG1、RG2、RG3、RG4、RG5、およびRG6という名前の6つのリソースグループが含まれています。

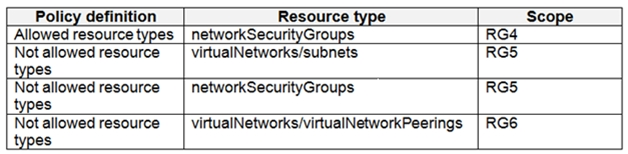
User9は、次の表に示す仮想ネットワークを作成します。



Sub1には、次の表に示すロックが含まれています。

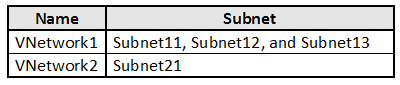


Sub1には、次の表に示すAzureポリシーが含まれています。

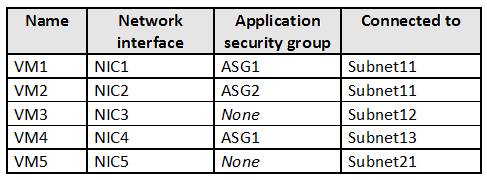


Sub2-

Sub2には、次の表に示す仮想ネットワークが含まれています。

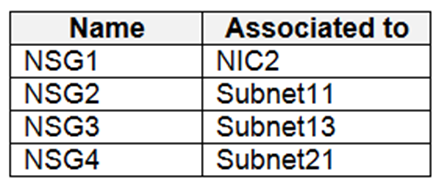


Sub2には、次の表に示す仮想マシンが含まれています。

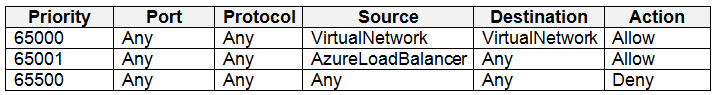


すべての仮想マシンには、パブリックIPアドレスとWebサーバー（IIS）の役割がインストールされています。各仮想マシンのファイアウォールは、ping要求とWeb要求を許可します。

Sub2には、次の表に示すネットワークセキュリティグループ（NSG）が含まれています。



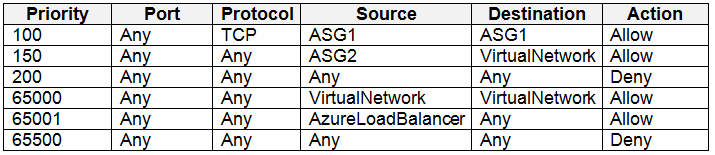
NSG1には、次の表に示すインバウンドセキュリティルールがあります。



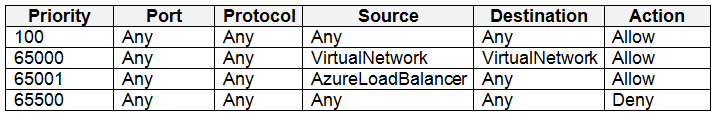
NSG2には、次の表に示すインバウンドセキュリティルールがあります。



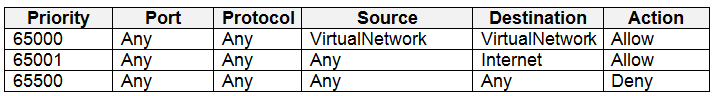
NSG3には、次の表に示すインバウンドセキュリティルールがあります。



NSG4には、次の表に示すインバウンドセキュリティルールがあります。



NSG1、NSG2、NSG3、およびNSG4には、次の表に示すアウトバウンドセキュリティルールがあります。



技術要件-Contosoは、次の技術要件を識別します。

AzureファイアウォールをSub2のVNetwork1にデプロイします。

contoso.comにApp2という名前のアプリケーションを登録します。

可能な限り、最小特権の原則を使用してください。

contoso.comのAzureAD特権ID管理（PIM）を有効にします。

# 質問.1

User2がPIMを実装できることを確認する必要があります。

あなたは最初に何をすべきですか？

1. 割り当てUser2のグローバル管理者の役割。
2. 設定contoso.comのための認証方法。
3. 設定contoso.comのためのアイデンティティの安全なスコア。
4. User2の多要素認証（MFA）を有効にします。

正解： *A*

ディレクトリでPIMの使用を開始するには、最初にPIMを有効にする必要があります。

1.ディレクトリのグローバル管理者としてAzureポータルにサインインします。

ディレクトリのPIMを有効にするには、Microsoftアカウント（@ outlook.comなど）ではなく、組織アカウント（@ yourdomain.comなど）を持つグローバル管理者である必要があります。

シナリオ：技術要件は次のとおりです。contoso.comに対してAzure AD特権ID管理（PIM）を有効にする

参照：

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

Manage identity and access