AZ-303 Exam#02

# Q.1

HOTSPOT-

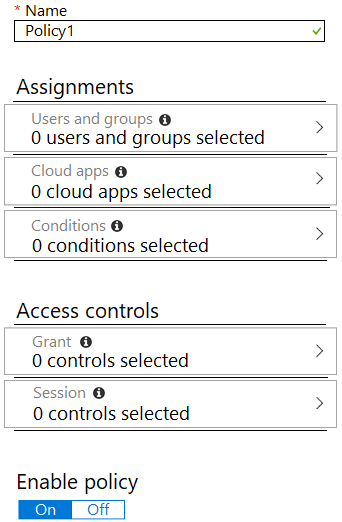
Azure Active Directory（Azure AD）テナントがあります。

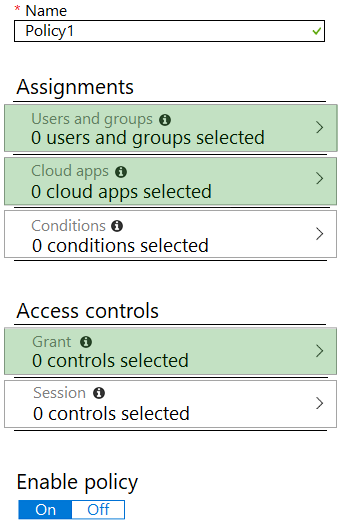
すべてのユーザーがAzureポータルにアクセスするときに多要素認証を使用することを要求する条件付きアクセスポリシーを作成する必要があります。

どの3つの設定を構成する必要がありますか？回答するには、回答領域で適切な設定を選択します。

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： 

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa>

# Q.2

社内のアプリケーションに認証を実装しています。

Azure Active Directory（Azure AD）にセルフサービスパスワードリセット（SSPR）と多要素認証（MFA）を実装することを計画しています。

MFAとSSPRの両方に使用できる認証メカニズムを選択する必要があります。

どの2つの認証方法を使用する必要がありますか？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。

1. オーセンティケーターアプリ
2. メールアドレス
3. アプリのパスワード
4. ショートメッセージサービス（SMS）メッセージ
5. セキュリティの質問

正解： *AD*

次の認証メカニズムはMFAとSSPRの両方に使用できます。

* ショートメッセージサービス（SMS）メッセージ
* Azure ADパスワード
* Microsoft Authenticator アプリ
* 音声通話

不正解：

B、E：次の認証メカニズムは次の目的で使用されます。

SSPRのみ：

* 電子メールアドレス
* セキュリティの質問

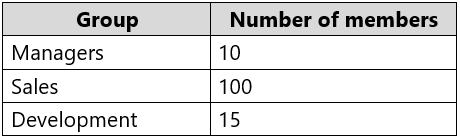
E：アプリのパスワード認証メカニズムはMFAにのみ使用できますが、特定の場合にのみ使用できます。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

# Q.3

あなたの会社には、次の表に示すグループがあります。



この会社には、contoso.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられたAzureサブスクリプションがあります。

Admin1という名前の管理者は、Managersグループのすべてのユーザーに対してエンタープライズ状態ローミングを有効にしようとします。

Admin1は、エンタープライズ状態ローミングのオプションがAzure ADから利用できないことを報告します。

Admin1にグローバル管理者の役割が割り当てられていることを確認します。

Admin1がエンタープライズ状態ローミングを有効にできることを確認する必要があります。

あなたは何をするべきか？

1. Azure ADの特権ID管理（PIM）の役割をAdmin1に割り当てます。
2. 購入Managersグループ内の各ユーザーのためのAzureの著作権管理（アズールRMS）ライセンス。
3. Admin1にAzureMulti-Factor Authentication（MFA）を適用します。
4. 購入Managersグループ内の各ユーザのためのAzure ADプレミアムP1ライセンス。

正解： *D*

Enterprise State Roamingは、Azure AD Premium

または

Enterprise Mobility + Security（EMS）ライセンスを持つすべての組織で利用できます。

参照：

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/devices/enterprise-state-roaming-enable>

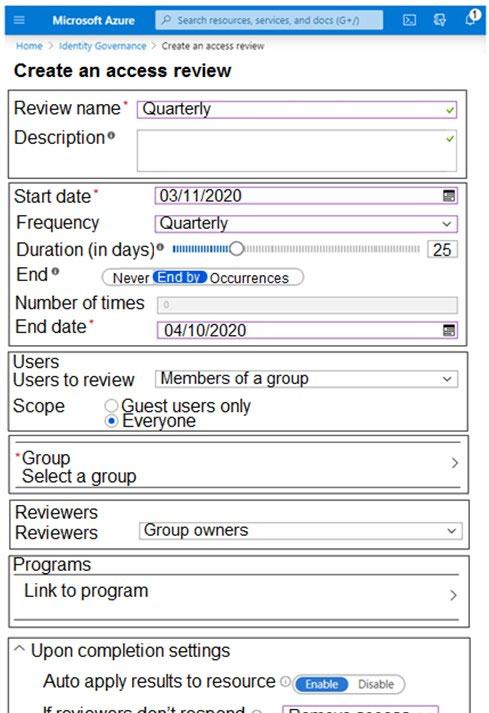
# Q.4

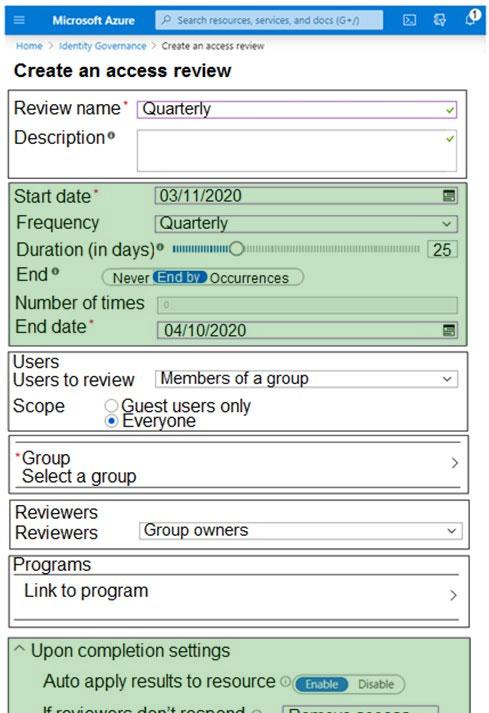
あなたは、次の要件を満たすためにアクセスレビューを実施することを計画：

* 別の設定がされるまでアクセスレビューが実施されなければなりません。
* Azure環境にアクセスできる各ユーザーまたはグループは、アクセスレビューの範囲内にある必要があります。
* アクセスレビューは2週間以内に完了する必要があります。
* 対応の欠如が運用環境の変化を引き起こしてはなりません。

管理者は、回答領域に表示されるアクセスレビューを作成します。

要件を満たすために、アクセスレビューのどの2つのセクションを変更する必要がありますか？



正解： 

エリア1：開始日..終了日

特に設定が行われるまで、アクセスレビューを実施する必要があります。End：Neverを設定しました。アクセスレビューは2週間以内に完了する必要があります。期間（日数）を14に設定します。

エリア2：完了時の設定

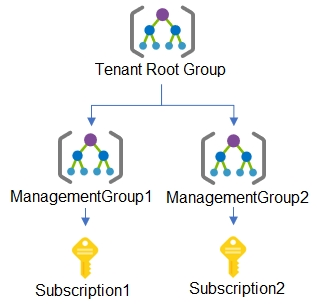
応答がなくても、運用環境に変化が生じてはなりません。「レビュー担当者が応答しない場合：変更なし（ユーザーのアクセスは変更されません）」を設定します。

参照：

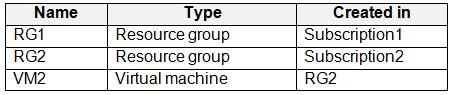
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

# Q.5

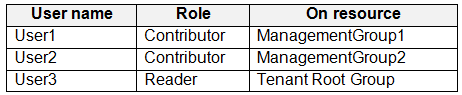
次の表に示すように、管理グループとAzureサブスクリプションの階層があります。



次の表に示すAzureリソースを作成します。



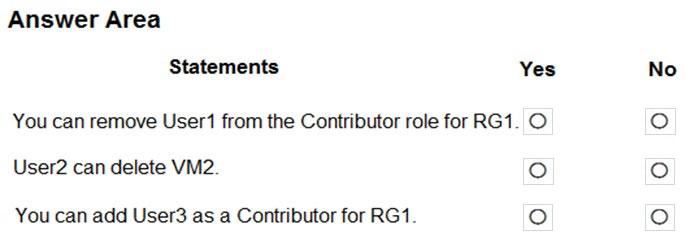
あなたには所有者の役割があります。次の表に示すように、ユーザーに役割を割り当てます。

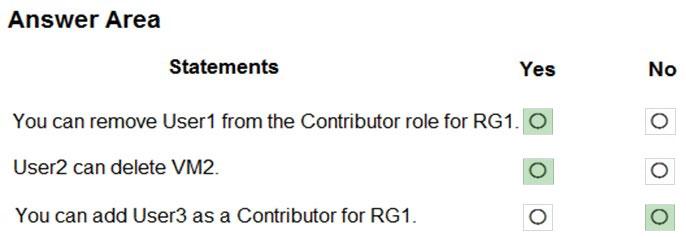


次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



正解： 

ボックス1：はい-

ロールを割り当てたので、削除できます。

ボックス2：はい-

コントリビューターの役割：すべてのリソースを管理するためのフルアクセスを許可しますが、AzureRBACで役割を割り当てることはできません。

ボックス3：いいえ-

参照：

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

議論の結果

NO、YES、YES

が賛成多数。

自分は

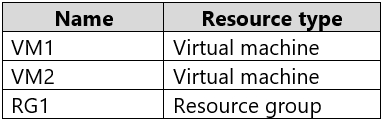
YES、YES、YES

と判断したが、、、議論の結果がいいかもしれない。

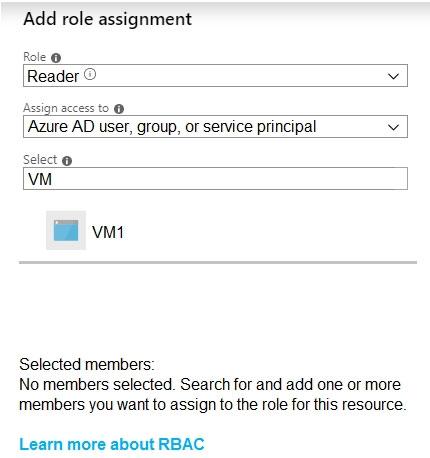
後から、対策セミナーのテキストは、問題文が違うが、No1の問題文が同じで、YESだったので、No1の解答はYESを支持する。

# Q.6

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。



次の展示に示すように、RG1に役割の割り当てを追加しようとしています。



VM2にリソースグループのリーダーロールを割り当てることができるようにするには、どうすればよいですか？

1. VM2でジャストインタイム（JIT）VMアクセスを構成します。
2. VM2でアクセス制御（IAM）を構成します。
3. 管理対象IDをVM2に割り当てます。
4. サブスクリプションレベルでリーダーの役割を変更します。

正解： *B*

マネージIDを使用してAzureリソースを構成した後、他のセキュリティプリンシパルと同様に、マネージIDに別のリソースへのアクセスを許可できます。

Azure RBAC を使用して、別のリソースへのマネージド ID アクセスを割り当てます。Azure VM や Azure 仮想マシンのスケールセットなどの Azure リソースでマネージドIDを有効にした後、次の手順を実行します。

1. 関連付けられたアカウントを使用してAzureポータルにサインインします。管理対象IDを構成したAzureサブスクリプション。
2. アクセス制御を変更する目的のリソースに移動します。この例では、Azure仮想マシンにストレージアカウントへのアクセスを許可しているため、ストレージアカウントに移動します。
3. リソースの[アクセス制御（IAM）]ページを選択し、[+役割の割り当てを追加]を選択します。次に、役割を指定し、アクセスを割り当て、対応するサブスクリプションを指定します。検索条件領域の下に、リソースが表示されます。リソースを選択し、[保存]を選択します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal>

# Q.7

AzureサブスクリプションにリンクされたAzure Active Directory（Azure AD）テナントがあります。テナントには、Adminsという名前のグループが含まれています。

管理者のメンバーを除くユーザーが、AzureポータルとAzure PowerShellを使用してサブスクリプションにアクセスできないようにする必要があります。

あなたは何をするべきか？

1. Azure ADから、ユーザー設定を構成します。
2. Azure ADから、条件付きアクセスポリシーを作成します。
3. Azureサブスクリプションから、Azureポリシーを割り当てます。
4. Azureサブスクリプションから、アクセス制御（IAM）を構成します。

正解： *B*

通常、条件付きアクセスを使用してクラウドアプリへのアクセスを制御します。ポリシーを設定して、Azure管理へのアクセスを制御することもできます。

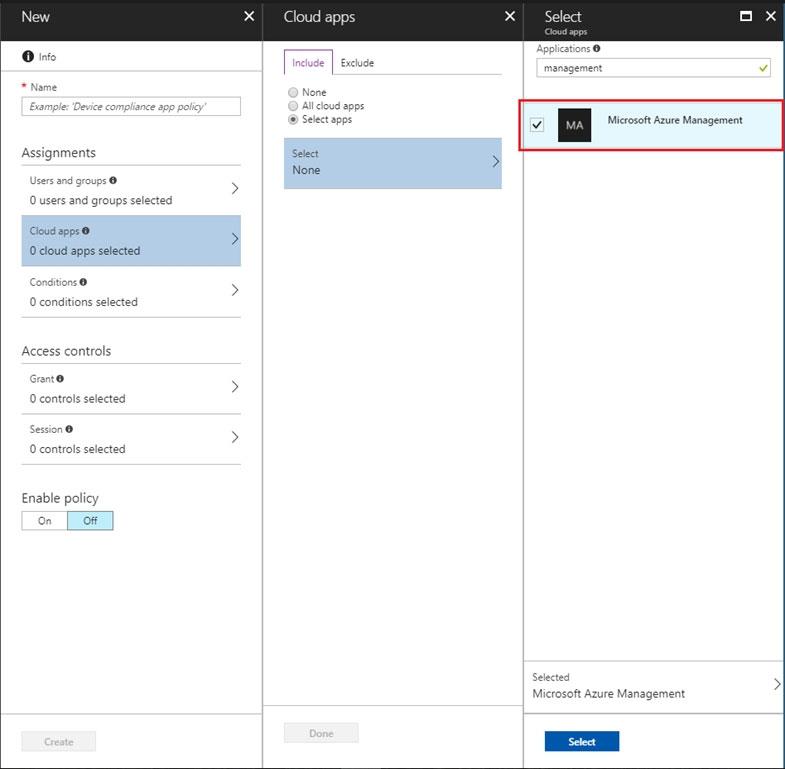
作成したポリシーは、以下を含め、すべてのAzure管理エンドポイントに適用されます。

* Azureのポータル
* Azureのリソースマネージャプロバイダ

クラシックサービス管理API

* AzureのPowerShellの
* Visual Studioのサブスクリプション管理者ポータル
* アズールDevOpsチーム
* Azureのデータファクトリーポータル

のためのポリシーを作成するにはAzure管理では、ポリシーを適用するアプリを選択するときに、[クラウドアプリ]で[MicrosoftAzure管理]を選択します。



不正解：

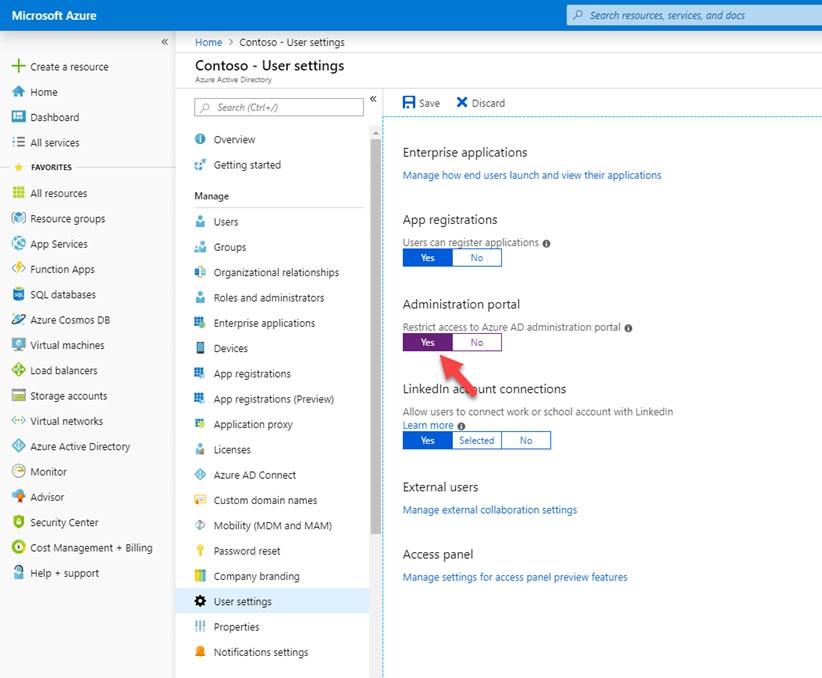
A：ユーザー設定から、Azure Portalへのアクセスのみを制限でき、AzurePowershellへのアクセスは制限できません。

注：Microsoftでは、Azure ActiveDirectory管理ポータルへの標準ユーザーアクセスを制限することを許可しています。

1.グローバル管理者としてAzureポータルにログインします。2。AzureActiveDirectoryに

移動します。ユーザー設定

3.次に、[Azure AD管理ポータルへのアクセスを制限する]の下の[はい]をクリックします。



参照：

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

<https://www.rebeladmin.com/2019/04/step-step-guide-restrict-azure-ad-administration-portal/>

# Q.8

Azure仮想マシンが3つのAzureリージョンにデプロイされています。各リージョンには、同じサブネット上に4つの仮想マシンがある単一の仮想ネットワークが含まれています。各仮想マシンは、App1という名前のアプリケーションを実行します。App1には、HTTPSを使用してアクセスできます。現在、仮想マシンはインターネットからアクセスできません。

すべての仮想マシン間でApp1のリクエストを負荷分散するには、Azure FrontDoorを使用する必要があります。

どの追加のAzureサービスをプロビジョニングする必要がありますか？

1. Azure Traffic Manager
2. 内部Azureロードバランサー
3. パブリックAzureロードバランサー
4. Azureのプライベートリンク

正解： *B*

フロントドアの背後にAzure Load Balancerをデプロイできますか？

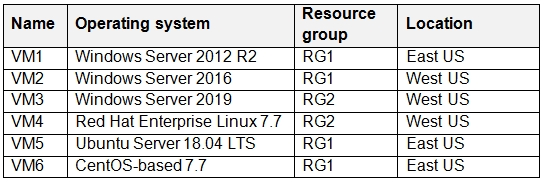
Azure Front Doorには、トラフィックをルーティングするためのパブリックVIPまたはパブリックに利用可能なDNS名が必要です。フロントドアの背後にAzureロードバランサーをデプロイすることは、一般的なユースケースです。

参照：

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

# Q.9

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



すべての重要なセキュリティ更新が毎月各仮想マシンに適用されるようにする必要があります。

作成する必要のある更新プログラムの展開の最小数はいくつですか？

1. 4
2. 6
3. 2
4. 1

正解： *A*

Windows仮想マシンの一つ、およびLinux VMの種類ごとに。

参照：

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

# Q.10

Azureサブスクリプションがあります。

次のAzure Resource Managerテンプレートを使用して、Azureでカスタムロールを作成します。



User1という名前のユーザーに役割を割り当てます。

User1はどのアクションを実行できますか？

1. 仮想マシンを作成します。
2. リソースグループを作成します。
3. 仮想マシンを削除します。
4. サポートリクエストを作成します。

正解： *D*

「Microsoft.Support / \*」操作により、ユーザーはサポートチケットを作成できます。

参照：

<https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell>

# Q.11

SQL server1という名前のAzure SQLサーバーで実行されるDb1という名前のAzure SQLデータベースがあります。

Azureポータルのクエリエディターを使用してDb1にクエリを実行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. Db1のADO.NET接続文字列をコピーして、クエリエディターに貼り付けます。
2. SQL server1のプライベートエンドポイント接続を承認します。
3. 変更DB1の高度なデータセキュリティ設定。
4. 設定SQLserver1ためのファイアウォールと仮想ネットワークの設定。

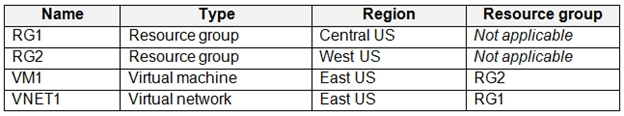
正解： *D*

リファレンス：

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-connect-query-portal>

# Q.12

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。



RG2では、VNET1に接続するVM2という名前の新しい仮想マシンを作成する必要があります。VM2は、VM2\_Interfaceという名前のネットワークインターフェイスを使用します。

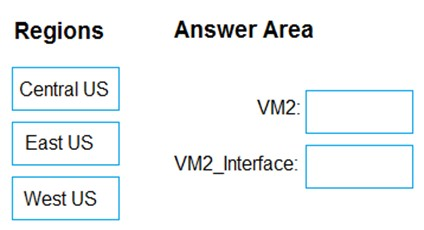
どのリージョンにVM2とVM2\_Interfaceを作成する必要がありますか？

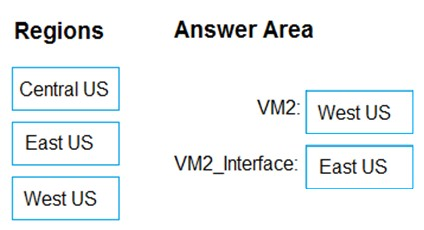
答えるには、適切な領域を正しいターゲットにドラッグします。

各リージョンは、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：正しい選択はそれぞれ1ポイントの価値があります。

選択して配置：



正解： 

VM2：米国西部

米国西部にあるRG2では、VM2という名前の新しい仮想マシンを作成する必要があります。

VM2\_interface：East US

VM2は、VM2\_Interfaceという名前のネットワークインターフェイスを使用して、EastUSにあるVNET1に接続します。

参照：

<https://docs.microsoft.com/en-us/azure/virtual-network/associate-public-ip-address-vm>

議論では、

**VM2：East US、VM2\_Interface：East US**

こちらが正しい！！

元々の解答は間違っている。

対策セミナーのテキストの86ページに同じ問題がある。

# Q.13

企業は、オンプレミスのデータセンターとAzureで仮想マシン（VM）をホストしています。オンプレミスおよびAzureベースのVMは、ExpressRouteを使用して通信します。

同社は、ExpressRoute接続に障害が発生した場合でも、通常の運用を継続できるようにしたいと考えています。フェイルオーバー接続はインターネットを使用する必要があり、マルチプロトコルラベルスイッチング（MPLS）サポートを必要としない必要があります。

継続的な運用を提供するソリューションを推奨する必要があります。

あなたは何をお勧めしますか？

1. 既存のExpressRoute接続の帯域幅を増やします。
2. オンプレミスインターネット接続の帯域幅を増やします。
3. VPN接続をセットアップします。
4. 第2ExpressRoute接続セットアップ。

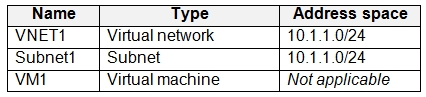
正解： *C*

リファレンス：

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>

# Q.14

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。



Subnet1はVNET1上にあります。VM1はSubnet1に接続します。

VNET1に仮想ネットワークゲートウェイを作成することを計画しています。

計画された仮想ネットワークゲートウェイの環境を準備する必要があります。

あなたは何をするべきか？

1. ローカルネットワークゲートウェイを作成します。
2. 修正Subnet1が使用するアドレス空間。
3. VNET1上GatewaySubnetという名前のサブネットを作成します。
4. 修正VNET1が使用するアドレス空間。
5. サブネット1を削除します。

正解： D

# Q.15

ネットワークには、オンプレミスのActive DirectoryとAzure Active Directory（Azure AD）テナントが含まれています。

Azure AD Connectをデプロイし、パススルー認証を構成します。

Azureサブスクリプションには、インターネットからアクセスされるいくつかのWebアプリが含まれています。

Azure ActiveDirectoryテナントでAzureMulti-Factor Authentication（MFA）を使用することを計画しています。

ユーザーがオンプレミスネットワークからWebアプリにアクセスするときにAzureMFAの入力を求められないようにするためのソリューションを推奨する必要があります。

推奨事項には何を含める必要がありますか？

1. Azureのポリシー
2. 信頼できるIP
3. オンプレミスネットワークとAzure間のサイト間VPN
4. AzureExpressRoute回線

正解： *B*

Azure Multi-Factor Authenticationの信頼できるIP機能は、管理対象またはフェデレーションテナントの管理者によって使用されます。この機能は、会社のイントラネットからサインインするユーザーの2段階認証プロセスをバイパスします。この機能は、Azure Multi-Factor Authenticationのフルバージョンで利用できますが、管理者向けの無料バージョンでは利用できません。

参照：

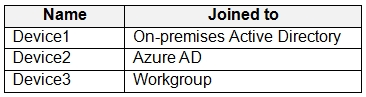
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips>

# Q.16

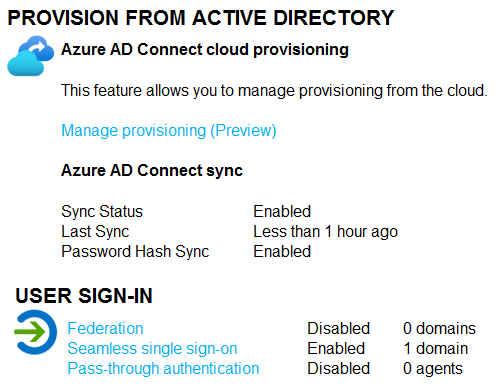
ネットワークには、User1という名前のユーザーを含むcontoso.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。ドメインはAzureActive

Directory（Azure AD）に同期します。

次の表に示すWindows10デバイスがあります。



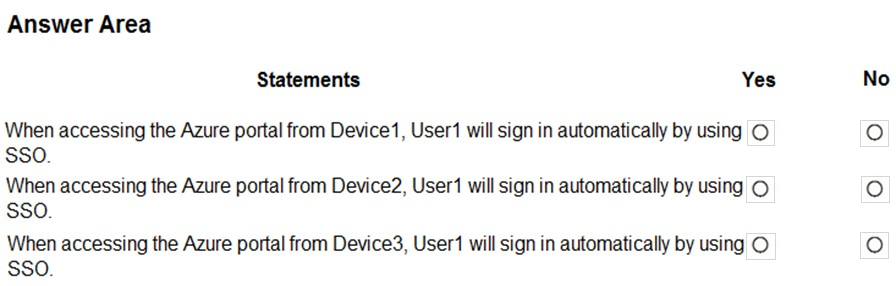
ユーザーサインイン設定は、次の図に示すように構成されています。



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。

注：正しい選択はそれぞれ1ポイントの価値があります。

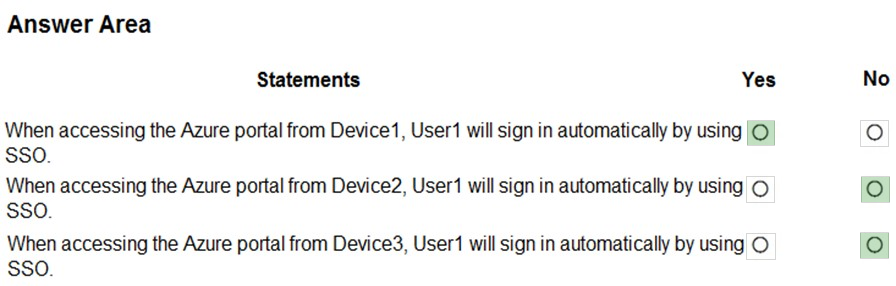
ホットエリア：



Device1からAzureポータルにアクセスすると、User1はSSOを使用して自動的にサインインします。

Device2からAzureポータルにアクセスする場合、User1はSSOを使用して自動的にサインインします。

Device3からAzureポータルにアクセスする場合、User1はSSOを使用して自動的にサインインします。

正解： 

ボックス1：はい

シームレスSSOでは、ユーザーのデバイスをドメインに参加させる必要がありますが、AzureADに参加しているデバイスやハイブリッドAzureADに参加しているデバイスでは使用されません。Azure ADのSSOが参加し、ハイブリッドAzure ADが参加し、AzureADに登録されたデバイスはプライマリ更新トークンに基づいて機能します。

ボックス2：いいえ

ボックス3：いいえ

参照：

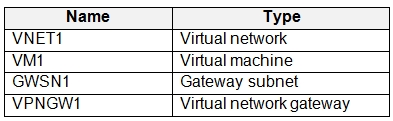
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>

上の答えは間違い **YES、YES、NO**  が正解

参照：<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso#key-benefits>

# Q.17

新しいAzureサブスクリプションを作成します。RG1という名前のリソースグループを作成します。RG1では、次の表に示すリソースを作成します。



オンプレミスネットワークとVNET1の間に暗号化されたトンネルを構成する必要があります。

Azureで作成する必要がある2つの追加リソースはどれですか？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. VPNゲートウェイ
2. サイト間の接続
3. ポイントツーサイト構成
4. VNETツーVNET接続
5. ローカルネットワークゲートウェイ

正解： *AE*

サイト間VPNゲートウェイ接続は、IPsec / IKE（IKEv1またはIKEv2）VPNトンネルを介してオンプレミスネットワークをAzure仮想ネットワークに接続するために使用されます。

このタイプの接続には、外部に面したパブリックIPアドレスが割り当てられたオンプレミスに配置されたVPNデバイス（ローカルネットワークゲートウェイ）が必要です。

最後に、仮想ネットワークゲートウェイとオンプレミスVPNデバイスの間にサイト間VPN接続を作成します。

参照：

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

解答は、AEとなっているが

VPNゲートウェイは既に作成されているので、

**解答は、B：サイト間の接続、E：ローカルネットワークゲートウェイ**

になる。

# Q.18

BLOBを格納し、Azure Databricksからアクセスされるstorage1という名前のAzureStorageアカウントを作成することを計画しています。

Azure Active Directory（Azure AD）認証を使用して、個々のBLOBにアクセス許可を設定できることを確認する必要があります。

storage1に対してどの詳細設定を有効にする必要がありますか？

1. 大きなファイル共有
2. 階層的な名前空間
3. NFS v3
4. ブロブ削除ソフト

正解： *B*

質問：ACLのサポートを有効にする必要がありますか？

いいえ。ACLを介したアクセス制御は、階層名前空間（HNS）機能がオンになっている限り、ストレージアカウントに対して有効になります。

注1：私たち[Microsoft]は、Azure Storage Blobs andQueuesのAzureActive Directory（AD）ベースのアクセス制御の一般提供を共有できることを嬉しく思います。

企業は、Azureג€™のロールベースアクセス制御

（RBAC）を使用して、AzureADテナントからユーザーとサービスIDに特定のデータアクセスアクセス許可を付与できるようになりました。

注2：Azure Data Lake Storage Gen2は、Azureロールベースのアクセス制御（Azure RBAC）とPOSIXのようなアクセス制御リスト（ACL）の両方をサポートするアクセス制御モデルを実装しています。

セキュリティプリンシパルをファイルおよびディレクトリのアクセスレベルに関連付けることができます。これらの関連付けは、アクセス制御リスト（ACL）に取り込まれます。ストレージアカウントの各ファイルとディレクトリには、アクセス制御リストがあります。セキュリティプリンシパルがファイルまたはディレクトリに対して操作を試行すると、ACLチェックにより、そのセキュリティプリンシパル（ユーザー、グループ、サービスプリンシパル、または管理対象ID）が操作を実行するための正しいアクセス許可レベルを持っているかどうかが判断されます。

不正解：

D：Blobソフト削除は、データが誤ってまたは誤って変更または削除されるのを防ぎます。ストレージアカウントでblobソフト削除が有効になっている場合、そのストレージアカウントのblob、blobバージョン、およびスナップショットは、指定した保持期間内に、削除後に復元される場合があります。

参照：

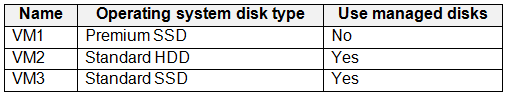
<https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-access-control#access-control-lists-on-files-and-directories>

<https://azure.microsoft.com/en-us/blog/azure-storage-support-for-azure-ad-based-access-control-now-generally-available/>

# Q.19

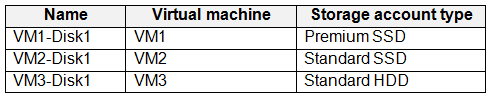
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。

次の表に示すAzure仮想マシンを作成します。



すべての仮想マシンに対してAzure Disk Encryptionを有効にし、VolumeTypeAllパラメーターを使用します。

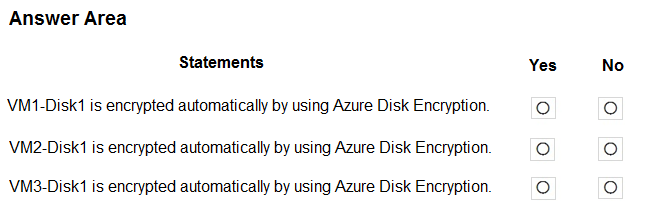
次の表に示すように、仮想マシンにデータディスクを追加します。

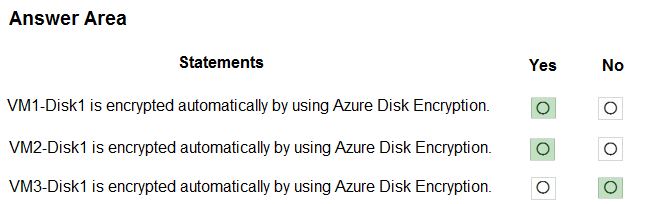


各ステートメントで、ステートメントがtrueの場合は[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

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： 

プレミアムおよび標準のアカウントタイプは、ディスク暗号化をサポートしています。

ディスク暗号化には管理対象ディスクが必要です。

参照：

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

VM1はアンマネージドディスクのため、ADEで暗号化されない。

したがって、

**No, Yes, Yes**

が正しいと考えられる。

対策セミナーのテキスト　105ページに似た問題がある。

# Q.20

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

* Contoso.onmicrosoft.com：Microsoft 365テナントにリンクされ、パスワードハッシュ同期を使用してcontoso.comという名前のActive Directoryフォレストに同期されます。
* Contosoazure.onmicrosoft.com：リンクされていますSubscription1という名前のAzureサブスクリプションへcontoso.comのユーザーにSubscription1のリソースへのアクセスを割り当てることができることを確認する必要があります。

あなたは何をするべきか？

1. contoso.onmicrosoft.comに関連付けSubscription1。Subscription1のすべての役割を再割り当てします。
2. 設定同期contoso.comへの既存のAzure AD Connectサーバーcontosoazure.onmicrosoft.comへ。
3. パススルー認証を使用するようにcontoso.onmicrosoft.comを構成します。
4. パススルー認証を使用するようにcontosoazure.onmicrosoft.comを構成します。

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-forests-multiple-sync-servers-to-one-azure-ad-tenant>

# Q.21

アクセスキーを使用してデータベースにアクセスするAzureWebアプリがいくつかあります。

アクセスキーをAzureKeyVaultに移行することを計画しています。各アプリは、アクセスキーにアクセスするために、Azure Active Directory（Azure AD）を使用して認証する必要があります。

アプリがアクセスキーにアクセスできるようにするには、Azureで何を作成する必要がありますか？

1. 管理されたID
2. マネージドアプリケーション
3. Azureのポリシー
4. アプリサービスプラン

正解： *A*

アズールキーVaultはしっかりストアの資格情報やその他の秘密の方法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、キーの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の概要は、AzureサービスにAzure ADで自動的に管理されたIDを提供することにより、この問題の解決に役立ちます。このIDを使用すると、コードにクレデンシャルを表示しなくても、KeyVaultを含むAzureAD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。

参照：

<https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-create-vault-azure-web-app>

# Q.22

KV1という名前のAzureキーボールトがあります。

AzureStorageに格納されているBLOBにデジタル署名するプロセスを実装する必要があります。

KV1でblobに署名するには何が必要ですか？

1. キー
2. シークレット
3. 証明書

正解： *B*

使用アズールキーボールトの秘密あなたのブロブストレージアカウントのコンテナのキーに。

参照：

<https://docs.microsoft.com/en-us/azure/key-vault/general/integrate-databricks-blob-storage>

デジタル署名するには、証明書が必要です。

正解は　**Ｃ**　です。

<https://www.rahulpnath.com/blog/signing-a-pdf-file-using-azure-key-vault/>

# Q.23

admin1@contoso.com という名前のユーザーの多要素認証ステータスを有効に設定します。

Admin1は、Webブラウザーを使用してAzureポータルにアクセスします。

Admin1がAzureポータルにアクセスするときに使用できる追加のセキュリティ検証はどれですか？

1. 電話、確認コードを含むメールメッセージ、アプリのパスワードを含むテキストメッセージ。
2. アプリのパスワード、確認コードを含むテキストメッセージ、およびMicrosoftAuthenticatorアプリから送信された確認コード。
3. アプリのパスワード、確認コードを含むテキストメッセージ、およびMicrosoftAuthenticatorアプリから送信される通知。
4. 電話、確認コードを含むテキストメッセージ、およびMicrosoftAuthenticatorアプリから送信された通知または確認コード。

正解： *D*

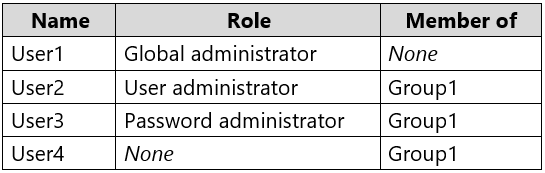
Microsoft Authenticatorアプリは、スマートフォンまたはタブレットに通知をプッシュすることで、アカウントへの不正アクセスを防止し、不正取引を阻止するのに役立ちます。ユーザーは通知を表示し、正当な場合は[確認]を選択します。それ以外の場合は、[拒否]を選択できます。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

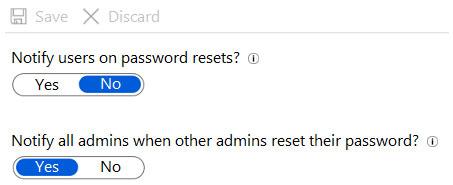
# Q.24

次の表に示すユーザーグループを含むAzureActive Directory（Azure AD）テナントがあります。



Group1のセルフサービスパスワードリセット（SSPR）を有効にします。

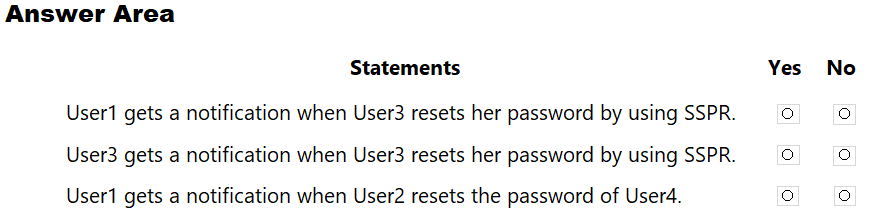
次の展示に示すように、通知設定を構成します。

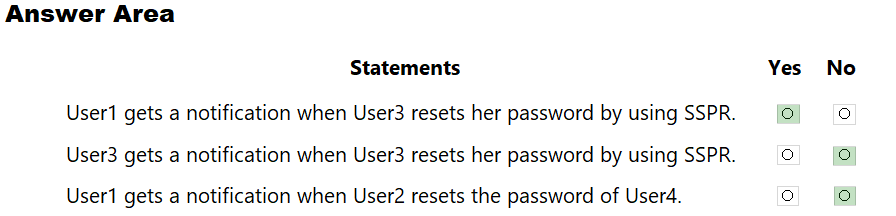


次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



正解： 

ボックス1：はい

他の管理者がパスワードをリセットしたときにすべての管理者に通知します：はい。

ボックス2：いいえ-

パスワードのリセットについてユーザーに通知する

ボックス3：いいえ

* パスワードのリセットについてユーザーに通知する = NO

このオプションが[はい]に設定されている場合、パスワードをリセットするユーザーは、パスワードが変更されたことを通知する電子メールを受け取ります。電子メールは、

SSPRポータルを介して、AzureADに登録されているプラ​​イマリおよび代替の電子メールアドレスに送信されます。リセットイベントは他の誰にも通知されません。

* 他の管理者がパスワードをリセットしたときにすべての管理者に通知する

このオプションが[はい]に設定されている場合、すべての管理者はAzureADに登録されているプラ​​イマリ電子メールアドレスに電子メールを受信します。電子メールは、別の管理者がSSPRを使用してパスワードを変更したことを通知します。

例：1つの環境に4人の管理者がいます。管理者Aは、SSPRを使用してパスワードをリセットします。管理者B、C、およびDは、パスワードのリセットを警告する電子メールを受信します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr>

対策セミナーのテキスト　156ページに同様の問題がある。

# Q.25

あなたの会社にはAzureサブスクリプションがあります。

すべてのユーザーに対して多要素認証（MFA）を有効にします。

会社のヘルプデスクは、会社の本社で作業しているときにMFA要求を受け取ったユーザーからの電話の増加を報告しています。

ユーザーがメインオフィスからサインインするときにMFA要求を受信しないようにする必要があります。

あなたは何をするべきか？

1. Azure Active Directory（Azure AD）の条件付きアクセスから、名前付きの場所を作成します。
2. MFAサービス設定から、信頼できるIP範囲を作成します。
3. Azure Active Directory（Azure AD）の条件付きアクセスから、カスタムコントロールを作成します。
4. Azure Active Directory（Azure AD）から、組織の関係を構成します。

正解： *B*

ユーザーに対して多要素認証を有効にする前に、最初に実行したいことは、使用可能な設定のいくつかを構成することを検討することです。最も重要な機能の1つは、信頼できるIPリストです。これにより、ネットワークのさまざまなIPをホワイトリストに登録できます。このように、ユーザーがオフィスにいるときはMFAのプロンプトが表示されず、デバイスを別の場所に持っていくときにもプロンプトが表示されます。方法は次のとおりです。Azure

ポータルにログインします。

[AzureAD]> [条件付きアクセス]> [名前付きの場所]に移動します。

上部のツールバーから、[MFAの信頼できるIPの構成]を選択します。

参照：

<https://www.kraftkennedy.com/implementing-azure-multi-factor-authentication/>

# Q.26

App1という名前のAzureロジックアプリとQueue1という名前のAzure Service Busキューがあります。

App1がQueue1からメッセージを読み取れることを確認する必要があります。

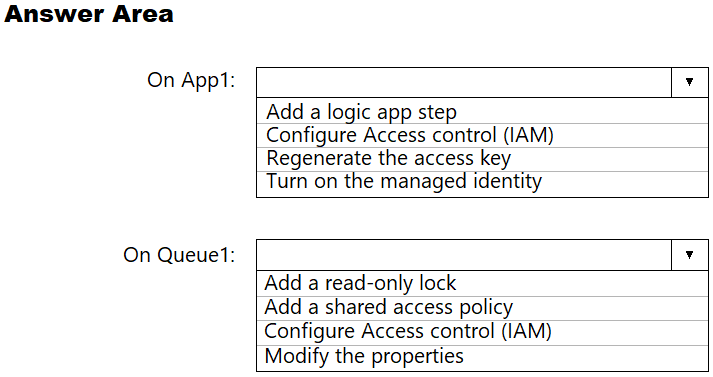
App1は、Azure Active Directory（Azure AD）を使用して認証する必要があります。

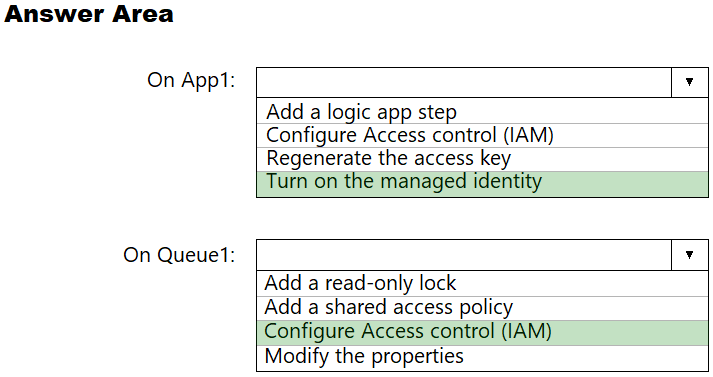
あなたは何をするべきか？

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： 

App1の場合：マネージID

をオンにするマネージIDでService Busを使用するには、IDにロールと適切なスコープを割り当てる必要があります。このセクションの手順では、マネージIDで実行され、ServiceBusリソースにアクセスする単純なアプリケーションを使用します。

アプリケーションが作成されたら、次の手順に従います。

1. [設定]に移動し、[ID]を選択します。
2. オンにするステータスを選択します。
3. [保存]を選択して設定を保存します。

Queue1：アクセス制御（IAM）の構成

Azure Active Directory（Azure AD）は、役割ベースのアクセス制御（RBAC）を介してセキュリティで保護されたリソースへのアクセス権を承認します。Azure Service Busは、Service Busエンティティへのアクセスに使用される一般的なアクセス許可のセットを含む組み込みのRBACロールのセットを定義します。また、データにアクセスするためのカスタムロールを定義することもできます。

Azureポータルを使用してRBACの役割を割り当てる

Azureポータルで、ServiceBus名前空間に移動します。左側のメニューで[アクセス制御（IAM）]を選択して、名前空間のアクセス制御設定を表示します。

ServiceBus名前空間を作成する必要がある場合。

[役割の割り当て]タブを選択して、役割の割り当てのリストを表示します。ツールバーの[追加]ボタンを選択してから、[役割の割り当てを追加]を選択します。

参照：

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/authenticate-application>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-managed-service-identity>

# Q.27

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

* Contoso.onmicrosoft.com：Microsoft 365テナントにリンクされ、パスワードハッシュ同期を使用してcontoso.comという名前のActive Directoryフォレストに同期されます
* [原文]Contoso.onmicrosoft.com: Linked to a Microsoft 365 tenant and syncs to an Active Directory forest named contoso.com by using password hash synchronization
* Contosoazure.onmicrosoft.com：Subscription1という名前のAzureサブスクリプションにリンクされています。
* [原文]Contosoazure.onmicrosoft.com: Linked to an Azure subscription named Subscription1

contoso.comのユーザーにSubscription1のリソースへのアクセスを割り当てることができることを確認する必要があります。

あなたは何をするべきか？

1. Subscription1が含まれているAzureの管理グループを作成します。
2. 設定同期contoso.comへの既存のAzure AD Connectサーバーcontosoazure.onmicrosoft.comへ。
3. 展開contosoazure.onmicrosoft.comに2番目のAzure AD Connectサーバーとの同期contoso.com。
4. contosoazure.onmicrosoft.com内のすべてのcontoso.comのユーザーのためのゲストアカウントを作成します。

A. Create an Azure management group that contains Subscription1.

B. Configure the existing Azure AD Connect server to sync contoso.com to contosoazure.onmicrosoft.com.

C. Deploy a second Azure AD Connect server and sync contoso.com to contosoazure.onmicrosoft.com.

D. Create guest accounts for all the contoso.com users in contosoazure.onmicrosoft.com.

正解： *C*

Azure AD Connectを使用すると、AzureADおよびOffice365にすばやくオンボードできます。

このトポロジでは、1つのAzure ADConnect同期サーバーが各AzureADテナントに接続されます。Azure AD Connect同期サーバーは、それぞれが操作するオブジェクトの相互に排他的なセットを持つように、フィルタリング用に構成する必要があります。たとえば、各サーバーを特定のドメインまたは組織単位にスコープすることができます。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies>

# Q.28

Azure Active Directory（Azure AD）認証をサポートしないApp1という名前のアプリケーションがあります。

App1がAzureServiceBusキューにメッセージを送信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、App1がキューをリッスンしないようにする必要があります。

あなたは何をするべきか？

1. Service Busのアクセス制御（IAM）を構成します。
2. 共有アクセスポリシーをキューに追加します。
3. キューのロックを変更します。
4. キューのアクセス制御（IAM）を構成します。

正解： *B*

Azure Service Busリソースへのアクセスを認証および承認するには、Azure Activity Directory（Azure AD）と共有アクセス署名

（SAS）の2つの方法があります。

各ServiceBus名前空間と各ServiceBusエンティティには、ルールで構成される共有アクセス許可ポリシーがあります。

参照：

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-authentication-and-authorization>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-sas>

# Q.29

管理者は、次の設定を持つ関数アプリをAzureで作成することを計画しています。

* ランタイムスタック：.NETCore
* オペレーティングシステム：Linux
* プランタイプ：消費
* アプリケーションインサイトを有効にする：はい

バックアップできることを確認する必要があります。

関数アプリを作成する前に、どの設定を変更することをお勧めしますか？

1. ランタイムスタック
2. Application Insightsを有効にする
3. オペレーティングシステム
4. プランタイプ

正解： *D*

バックアップと復元機能を使用するには、App Serviceプランが標準、プレミアム、または分離層にある必要があります。

参照：

<https://docs.microsoft.com/en-us/azure/app-service/manage-backup#requirements-and-restrictions>

# Q.30

Azureサブスクリプションがあります。

Webフロントエンドとアプリケーション層を持つアプリをデプロイすることを計画しています。

次の要件を満たす負荷分散ソリューションを推奨する必要があります。

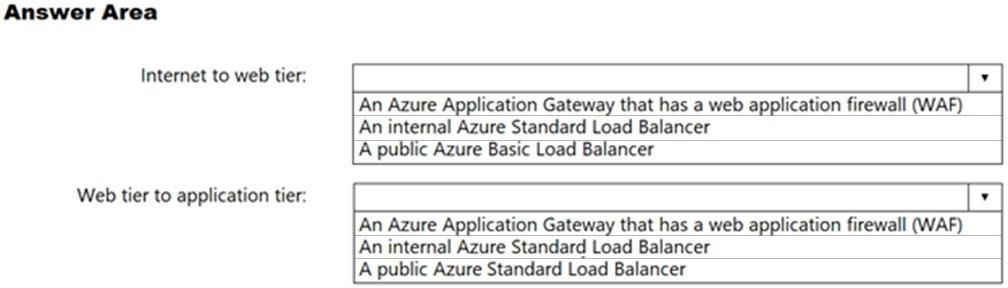
* インターネットからWeb層へ：
  + URLベースのルーティングを提供します
  + 接続のドレインをサポートします
  + SQLインジェクション攻撃を防ぎます
* Web層からアプリケーション層へ：
  + ポート転送を提供します
  + HTTPSヘルスをサポートしますプローブ
  + バックエンドプールとして設定された可用性をサポートします

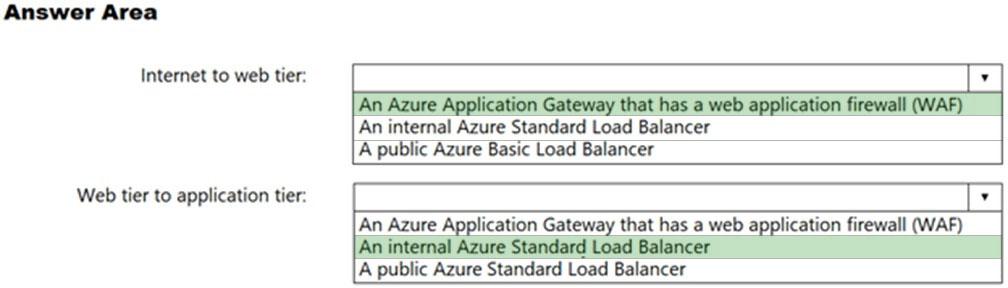
各層にどの負荷分散ソリューションを推奨する必要がありますか？

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：Webアプリケーションファイアウォール（WAF）を備えた

Azure Application Gateway Azure Application Gatewayは、一般的なエクスプロイトや脆弱性からWebアプリケーションを一元的に保護するWebアプリケーションファイアウォール（WAF）を提供します。Webアプリケーションは、一般的に知られている脆弱性を悪用する悪意のある攻撃の標的になりつつあります。SQLインジェクションとクロスサイトスクリプティングは、最も一般的な攻撃の1つです。

Application Gatewayは、アプリケーション配信コントローラー（ADC）として動作します。Secure Sockets Layer（SSL）の終了、Cookieベースのセッションアフィニティ、ラウンドロビン負荷分散、コンテンツベースのルーティング、複数のWebサイトをホストする機能、およびセキュリティの強化を提供します。

ボックス2：内部Azure標準ロードバランサー

インターネットからWeb層はパブリックインターフェイスですが、Web層からアプリケーション層は内部である必要があります。

注：Azure Load Balancerで負荷分散ルールを使用する場合は、ヘルスプローブを指定して、LoadBalancerがバックエンドエンドポイントのステータスを検出できるようにする必要があります。

ヘルスプローブは、TCP、HTTP、HTTPSプロトコルをサポートします。

参照：

<https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview>

# Q.31

Subnet1という名前のサブネット上に10台のAzure仮想マシンがあります。Subnet1は、VNet1という名前の仮想ネットワーク上にあります。

LB1という名前のパブリックAzure Standard Load Balancerを10台の仮想マシンと同じAzureリージョンにデプロイすることを計画しています。

すべての仮想マシンからインターネットへのトラフィックがLB1を通過するようにする必要があります。このソリューションでは、仮想マシンがインターネット上でアクセスできないようにする必要があります。

どの3つのアクションを実行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。

1. ヘルスプローブをLB1に追加します。
2. 仮想マシンのネットワークインターフェイスをLB1のバックエンドプールに追加します。
3. インバウンドルールをLB1に追加します。
4. アウトバウンドルールをLB1に追加します。
5. ネットワークセキュリティグループ（NSG）をSubnet1に関連付けます。
6. ユーザー定義ルートをSubnet1に関連付けます。

正解： *ABD*

A：ロードバランサーがアプリのステータスを監視できるようにするには、ヘルスプローブを使用します。ヘルスプローブは、

ヘルスチェックへの応答に基づいて、VMをロードバランサーローテーションに動的に追加またはロードバランサーローテーションから削除します。

B：トラフィックをVMに分散するために、バックエンドアドレスプールには、ロードバランサーに接続されている仮想（NIC）のIPアドレスが含まれています。

D：ロードバランサールールは、トラフィックがVMにどのように分散されるかを定義するために使用されます。アウトバウンドトラフィックのみが許可されます。

参照：

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal>

私は、**B、Ｄ、Ｅ**　が正解と考える。

Ａは明らかに必要ないと思う。また、この問題集のサイトの討論掲示板でもＢＤＥを解答する向きが多数ある。

# Q.32

SQL1という名前のAzure仮想マシン上にSQL Serverがあります。

仮想マシンにAutomated Backup v2を使用して、SQL1上のデータベースのバックアップを自動化する必要があります。バックアップは、次の要件を満たしている必要があります。

* 15分の目標復旧時点（RPO）を満たしている。
* バックアップを30日間保持します。
* 保存中のバックアップを暗号化します。

バックアップソリューションの一部として何をプロビジョニングする必要がありますか？

1. Elastic Database ジョブ
2. Azure Key Vault
3. Azure Storage アカウント
4. リカバリサービスボールト

正解： *C*

Azureストレージアカウントは、自動バックアップファイルをBLOBストレージに保存するために使用されます。この場所に、すべてのバックアップファイルを保存するためのコンテナが作成されます。バックアップファイルの命名規則には、日付、時刻、およびデータベースGUIDが含まれます。

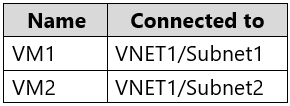
参照：

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup>

**New-AzVMSqlServerAutoBackupConfigコマンドを使用して、Azureストレージアカウントにバックアップを保存するためのAutomated Backup v2設定を有効にして構成します。**

# Q.33

KeyVault1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。



KeyVault1には、複数のユーザーにキーの作成権限を提供するアクセスポリシーがあります。

ユーザーがVM1からKeyVault1にのみシークレットを登録できるようにする必要があります。

あなたは何をするべきか？

1. Subnet1にリンクされているネットワークセキュリティグループ（NSG）を作成します。
2. 設定KeyVault1のファイアウォールおよび仮想ネットワークの設定。
3. 変更KeyVault1ためのアクセスポリシー。
4. ハードウェアセキュリティモジュール（HSM）を使用するようにKeyVault1を構成します。

正解： *C*（下の※参照）

キーボールトのキーボールトアクセスポリシーを設定して、データプレーンアクセスを許可します。

注1：VMのシステムによって割り当てられたマネージIDアクセスをKeyVaultに付与します。

1。[アクセスポリシー]を選択し、[新規追加]をクリックします。

2. [テンプレートから構成]で、[シークレット管理]を選択します。

3. [プリンシパルの選択]を選択し、検索フィールドに前に作成したVMの名前を入力します。結果リストでVMを選択し、[選択]をクリックします。

4. [OK]をクリックして新しいアクセスポリシーの追加を終了し、[OK]をクリックしてアクセスポリシーの選択を終了します。

注2：キーボールトへのアクセスは、管理プレーンとデータプレーンの2つのインターフェイスを介して制御されます。管理プレーンは、キーを管理する場所です

Vault自体。このプレーンでの操作には、キーボールトの作成と削除、キーボールトプロパティの取得、およびアクセスポリシーの更新が含まれます。データプレーンは、キーボールトに保存されているデータを操作する場所です。キー、シークレット、および証明書を追加、削除、および変更できます。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad>

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault2>

※討論より

<https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#firewalls-and-virtual-networks>

の

Although users can browse to a key vault from the Azure portal, they might not be able to list keys, secrets, or certificates if their client machine is not in the allowed list.

で、

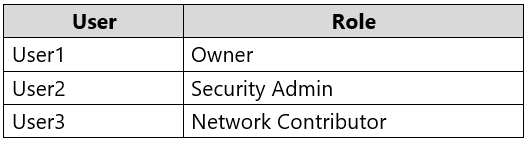
For implementation steps, see [Configure Azure Key Vault firewalls and virtual networks](https://docs.microsoft.com/en-us/azure/key-vault/general/network-security)

とあるので、**B**　が正解だと考える。

# Q.34

VNet1という名前の仮想ネットワークを含むSubscription1という名前のAzureサブスクリプションがあります。

次の表にユーザーを追加します。

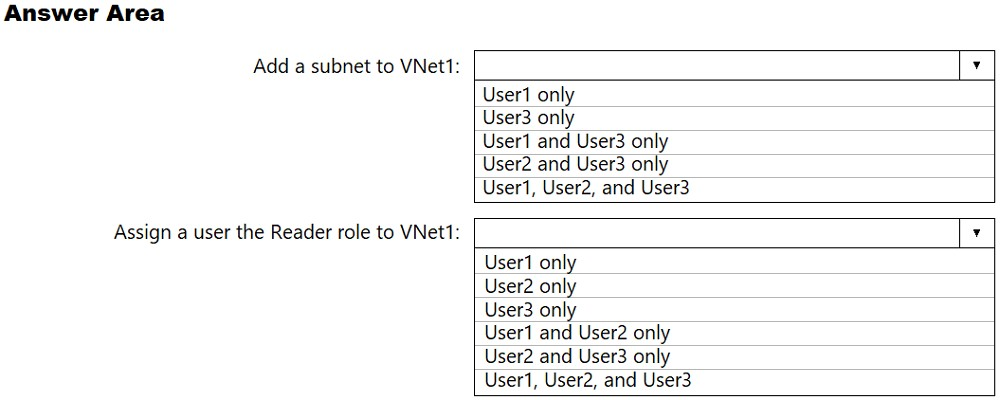


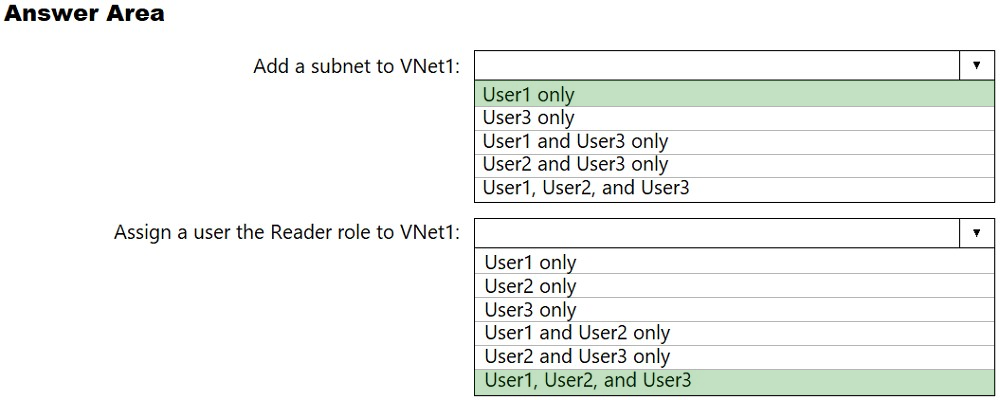
どのユーザーが各構成を実行できますか？

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。

ホットエリア：



正解： ※参照のこと

ボックス1：User1のみ。

ユーザー1：所有者の役割を使用すると、リソースへのアクセスを含むすべてを管理できます。

User3ではない：ネットワークコントリビューターの役割では、ネットワークを管理できますが、ネットワークにアクセスすることはできません。

ボックス2：

ユーザー1とユーザー2のみ-セキュリティ管理者の役割：セキュリティセンターのみ：セキュリティポリシーの表示、セキュリティ状態の表示、セキュリティポリシーの編集、アラートと推奨事項の表示、アラートと推奨事項の却下を行うことができます。

参照：

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

※

VNet1にサブネットを追加できるのは、OwnerとNetwork Contributorである。

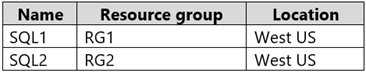
したがって、**User1　と　User3**　が正解である。

ユーザに対してロールを割り当てられるのは、Ownerのみである。

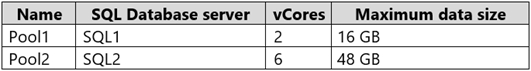
したがって、**User1**　が正解である。

# Q.35

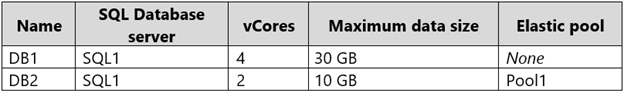
次の表に示すAzureSQLデータベースサーバーを含むAzureサブスクリプションがあります。



SQLデータベースサーバーには、次の表に示すエラスティックプールがあります。



SQL1には、次の表に示すSQLデータベースがあります。



DB1をPool1に追加するとどうなりますか？

1. DB1上のvCoresは2つに減少します。
2. pool1にの最大データサイズは22ギガバイトまで増加します。
3. DB1 の最大データサイズは6GBに減少します。
4. pool1にオンザvCoresは4つに増加します。

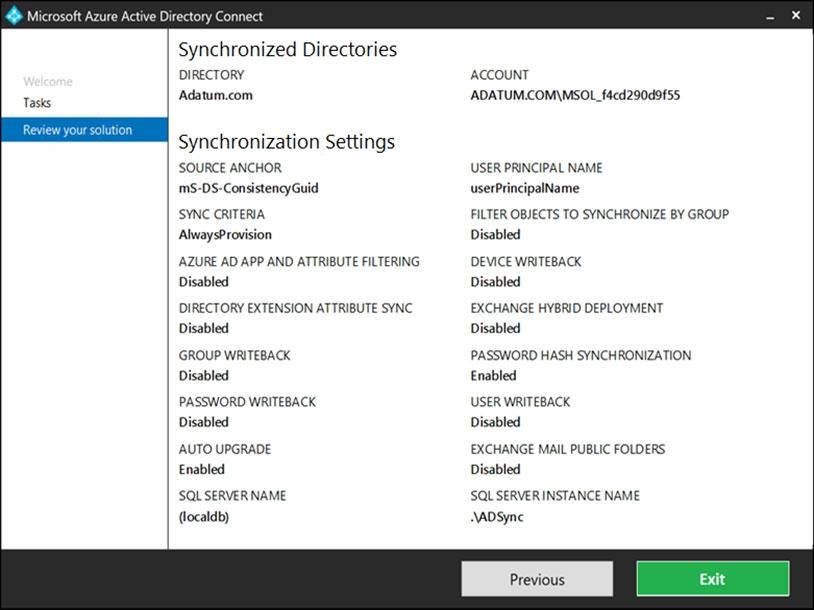
正解： *D*

DBがPOOLに合わせるのか？POOLがDBに合わせるのか？

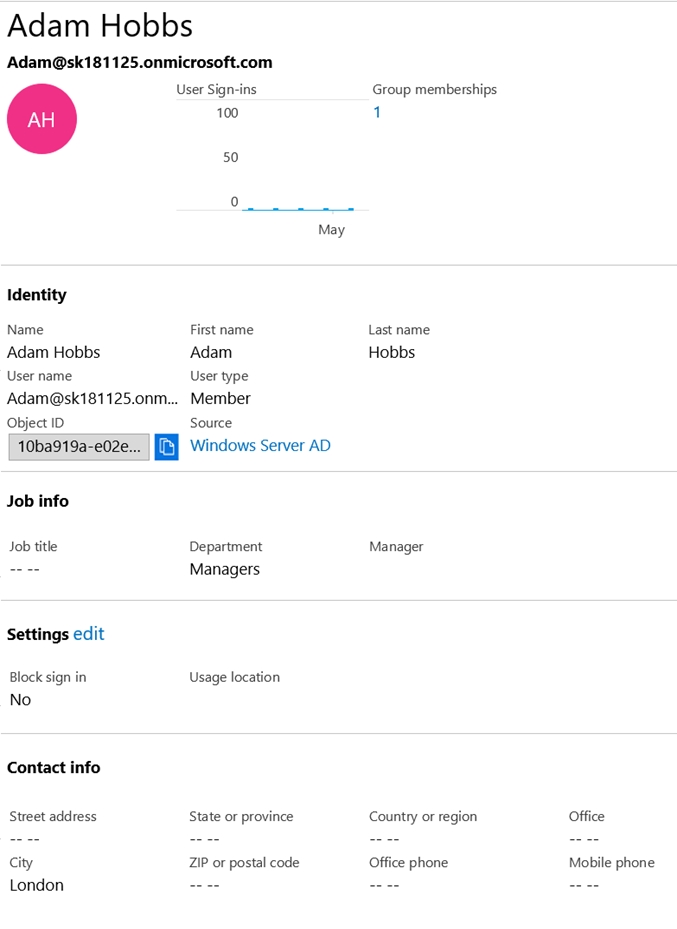
実際に試した人の意見では、**A** が正解となっており、DBがPOOLに合わせてダウンサイジングされるようです。

# Q.36

ネットワークには、次の展示に示すように、Azure Active Directory（Azure AD）に同期されるActive Directory ドメインが含まれています。



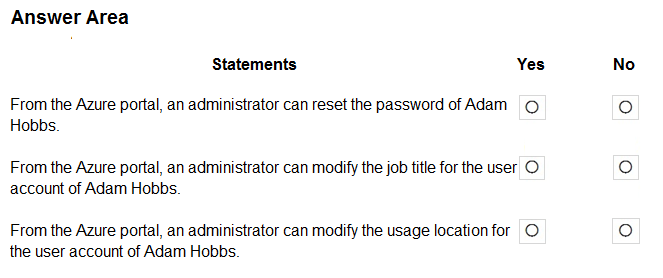
次の展示に示すように構成されたユーザーアカウントがあります。



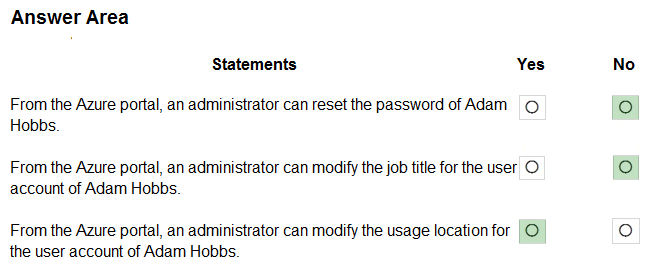
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



* 管理者は、Azureポータルから、AdamHobbsのパスワードをリセットできます。
* 管理者は、Azureポータルから、AdamHobbsのユーザーアカウントの役職を変更できます。
* 管理者は、Azureポータルから、AdamHobbsのユーザーアカウントの使用場所を変更できます。

正解： 

ボックス1：いいえ

パスワードの書き戻しは無効になっています。

注：クラウドベースのパスワードリセットユーティリティがあることは素晴らしいことですが、ほとんどの企業は、ユーザーが存在するオンプレミスディレクトリをまだ持っています。マイクロソフトは、従来のオンプレミスActive Directory（AD）をクラウドでのパスワード変更と同期させることをどのようにサポートしていますか？パスワードの書き戻しは、Azure AD Connectで有効になっている機能であり、クラウドでのパスワードの変更を既存のオンプレミスディレクトリにリアルタイムで書き戻すことができます。

ボックス2：いいえ

ボックス3：はい

はい、位置情報の編集リンクがあります。

参照：

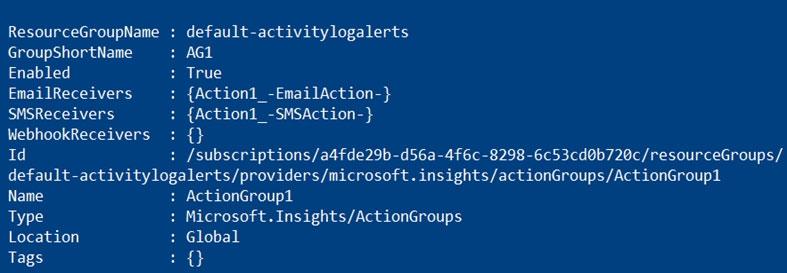
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

# Q.37

Subscription1という名前のAzureサブスクリプションがあります。

Subscription1で、Alert1という名前のアラートルールを作成します。

Alert1アクショングループは、次の図に示すように構成されています。

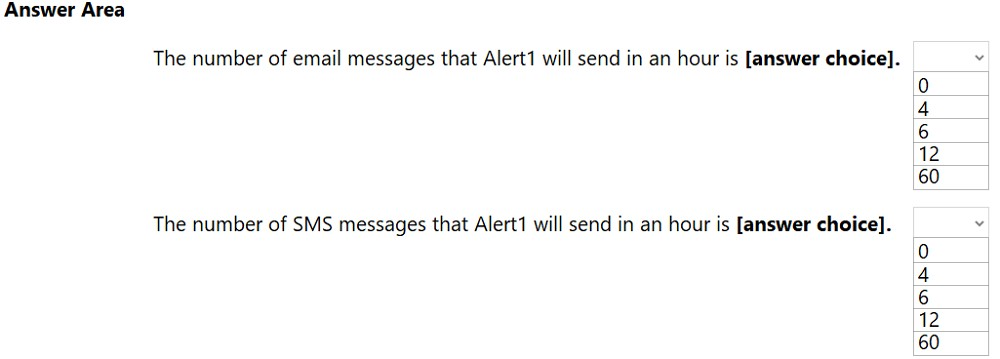


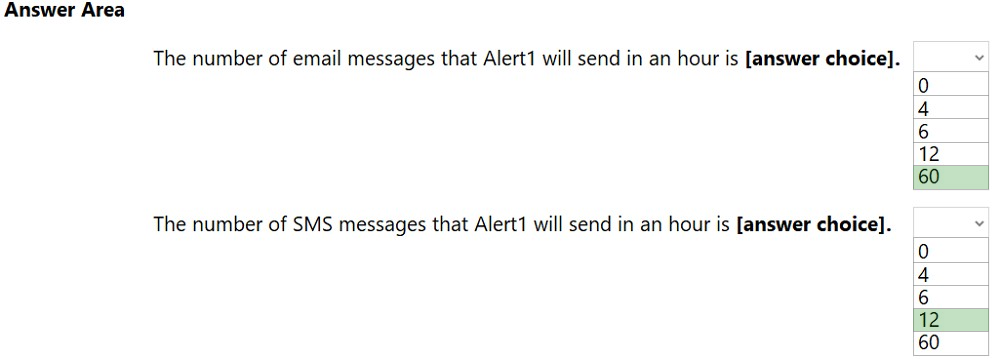
Alert1アラート基準は毎分トリガーされます。

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

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1：60

1分あたり1つのアラートにより、1分あたり1つの電子メールがトリガーされます。

ボックス2：12

5分ごとに1つ以下のSMSを送信できます。これは、1時間あたり12に相当します。

注：レート制限とは、特定の電話番号、電子メールアドレス、またはデバイスに送信される通知が多すぎる場合に発生する通知の一時停止です。レート制限により、アラートが管理可能で実行可能になります。

レート制限のしきい値は次の

とおりです。

* SMS：5分ごとに1SMS以下。
* 音声：5分ごとに1回までの音声通話。
* Eメール：1時間に100通以下のEメール。
* その他のアクションはレート制限されていません。

参照：

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/azure-monitor/overview.md>

# Q.38

既存の仮想マシンに基づいてAzure Resource Managerテンプレートをダウンロードします。テンプレートは、100台の仮想マシンを展開するために使用されます。

管理者パスワードを参照するようにテンプレートを変更する必要があります。パスワードがプレーンテキストで保存されないようにする必要があります。

パスワードを保存するために何を作成する必要がありますか？

1. Azure KeyVaultとアクセスポリシー
2. Azure Active Directory（AD）ID保護とAzureポリシー
3. リカバリサービスボールトとバックアップポリシー
4. AzureStorageアカウントとアクセスポリシー

正解： *A*

# Q.39

複数のアプリケーションからアクセスされるstorage1という名前の Azure Storage アカウントがあります。

管理者は、storage1のアクセスキーを手動でローテーションします。

ローテーション後、アプリケーションはストレージアカウントへのアクセスに失敗します。

開発者は、問題を解決するためにアプリケーションを手動で変更します。

アクセスキーを自動的にローテーションするソリューションを実装する必要があります。ソリューションは、ソリューションが実装された後、アプリケーションを更新する必要性を最小限に抑える必要があります。

ソリューションに何を含める必要がありますか？

1. Azure ADエンタープライズアプリケーション
2. Azure Key Vault
3. AzureLogicアプリ
4. AzureのDesired State Configuration（DSC）拡張機能

正解： *B*

Microsoftでは、Azure Key Vaultを使用してアクセスキーを管理し、定期的にキーをローテーションして再生成することをお勧めします。Azure Key Vaultを使用すると、アプリケーションを中断することなく、キーを簡単にローテーションできます。キーを手動で回転させることもできます。

参照：

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

# Q.40

Windows Server2019を実行するServer1という名前のオンプレミスファイルサーバーがあります。Server1はWindows Admin Centerを使用して管理します。

Server1に障害が発生した場合に、AzureからServer1ファイルを回復できることを確認する必要があります。

解決策：AzureStorageアカウントとAzureStorageSyncサービスを作成します。Server1のAzureFileSyncを構成します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *A*

Azure File Syncを使用して、オンプレミスファイルサーバーの柔軟性、パフォーマンス、互換性を維持しながら、組織のファイル共有をAzureFilesに一元化します。Azure File Syncは、WindowsServerをAzureファイル共有のクイックキャッシュに変換します。

Azure Filesは、業界標準のサーバーメッセージブロック（SMB）プロトコルを介してアクセスできる、クラウド内のフルマネージドファイル共有を提供します。Azureファイル共有は、Windows、Linux、およびmacOSのクラウドまたはオンプレミス展開によって同時にマウントできます。さらに、Azureファイル共有

をAzure File Syncを使用してWindowsServerにキャッシュし、データが使用されている場所の近くで高速アクセスすることができます。

Azureファイル共有は次の目的で使用できます。

オンプレミスファイルサーバーの置き換えまたは補足：

Azure Filesを使用して、従来のオンプレミスファイルサーバーまたはNASデバイスを完全に置き換えまたは補足できます。Windows、macOS、Linuxなどの一般的なオペレーティングシステムは、世界中のどこにいてもAzureファイル共有を直接マウントできます。Azureファイル共有は、Azure File Syncを

使用して、オンプレミスまたはクラウドのいずれかでWindows Serverにレプリケートし、使用されているデータのパフォーマンスと分散キャッシュを実現することもできます。

参照：

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

# Q.41

Windows Server2019を実行するServer1という名前のオンプレミスファイルサーバーがあります。Server1はWindowsAdminCenterを使用して管理します。

Server1に障害が発生した場合に、AzureからServer1ファイルを回復できることを確認する必要があります。

解決策：Azureポータルから、RecoveryServicesボールトを作成します。Server1に、Azure Backupエージェントをインストールすると、バックアップが正常に実行されます。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *B*

代わりに、Azure Storage Syncサービスを使用して、Azureファイルを構成します。

オンプレミスファイルサーバーの柔軟性、パフォーマンス、互換性を維持しながら、Azure FileSyncを使用して組織のファイル共有をAzureFilesに一元化します。Azure File Syncは、WindowsServerをAzureファイル共有のクイックキャッシュに変換します。

参照：

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

# Q.42

Azureサブスクリプションがあります。

Windows Server2019を実行するServer1という名前のオンプレミスファイルサーバーがあります。Server1はWindowsAdminCenterを使用して管理します。

Server1に障害が発生した場合に、AzureからServer1ファイルを回復できることを確認する必要があります。

解決策：Windows Admin CenterをAzureに登録し、AzureBackupを構成します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *B*（※参照）

代わりに、Azure Storage Syncサービスを使用して、Azureファイルを構成します。

オンプレミスファイルサーバーの柔軟性、パフォーマンス、互換性を維持しながら、Azure FileSyncを使用して組織のファイル共有をAzureFilesに一元化します。Azure File Syncは、WindowsServerをAzureファイル共有のクイックキャッシュに変換します。

参照：

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

※

正解は、**A**

<https://docs.microsoft.com/ja-jp/windows-server/manage/windows-admin-center/azure/azure-backup>

の

「Windows 管理センターでの Azure Backup の統合は、ボリュームと Windows システム状態のオンプレミス Windows 物理サーバーまたは仮想サーバーをバックアップする場合に最適です。 これにより、ファイルサーバー、ドメインコントローラー、IIS Web サーバーをバックアップするための包括的なメカニズムが実現されます。」

が示唆している。

# Q.43

オンプレミスのActiveDirectoryとAzureActive Directory（Azure AD）を統合する認証ソリューションを設計する必要があります。このソリューションは、次の要件を満たしている必要があります。

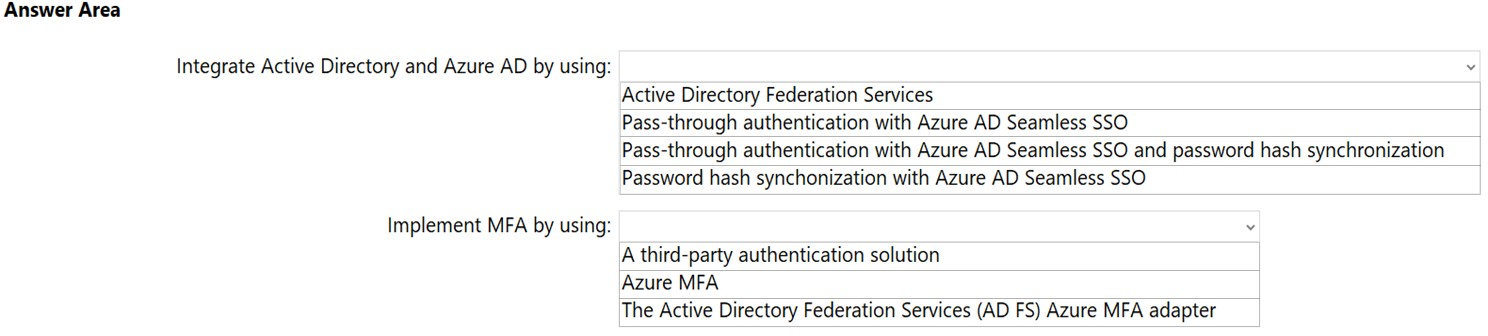
* ActiveDirectoryユーザーは、ActiveDirectoryユーザーアカウントで構成されたサインイン時間外にAzureAD統合アプリにサインインできないようにする必要があります。
* ActiveDirectoryユーザーは、Azure AD統合アプリにサインインするときに、多要素認証（MFA）を使用して認証する必要があります。
* 管理者は、資格情報を漏えいしたActiveDirectoryユーザーを一覧表示するAzureADで生成されたレポートを取得できる必要があります。
* ソリューションの実装と保守に必要なインフラストラクチャを最小限に抑える必要があります。

ソリューションに何を含める必要がありますか？

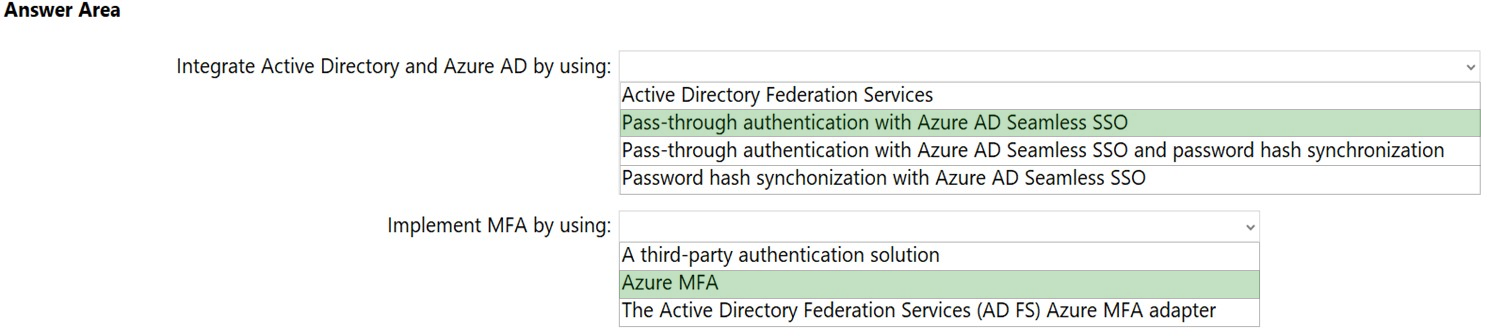
回答するには、回答領域で適切なオプションを選択します。

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：



<https://www.examtopics.com/exams/microsoft/az-303/view/25/>

正解： （※参照）

ボックス1：AzureADシームレスSSOを使用したパススルー認証

AzureADシームレスSSOとActiveDirectoryフェデレーションサービス

オンプレミスのユーザーアカウントの状態、パスワードポリシー、およびサインイン時間をすぐに適用するセキュリティ要件を持つ企業は、Azureを使用する場合がありますADパススルー認証。

パススルー認証をシームレスなシングルサインオン機能と組み合わせることができます。

注：Azure ADは、ハイブリッドIDソリューションに対して次の認証方法をサポートしています。

* AzureADパスワードハッシュ同期
* AzureADパススルー認証

ボックス2：AzureMFA

Azure ADパススルー認証の主な利点の1つは、AzureMFAとシームレスに連携することです。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

最初の解答は、

**Pass-Through authentication with Azure AD Seamless SSO and password hash synchronization.**

上記参照URLの

Cloud authentication: Password hash synchronization

と

Cloud authentication: Pass-through Authentication

に記述があり、両方使わないと実現できないと読める。

# Q.44

3つのAzureリージョンにリソースがあります。各リージョンには2つの仮想マシンが含まれています。各仮想マシンには、ネットワークインターフェイスに割り当てられたパブリックIPアドレスと、ローカルにインストールされたApp1という名前のアプリケーションがあります。

すべての仮想マシンにAzureFrontDoorベースの負荷分散を実装することを計画しています。

仮想マシン上のApp1がAzureFrontDoorからルーティングされたトラフィックのみを受け入れるようにする必要があります。

何を実装する必要がありますか？

1. Azureのプライベートリンク
2. サービスエンドポイント
3. サービスタグ付きのネットワークセキュリティグループ（NSG）
4. アプリケーションセキュリティグループを含むネットワークセキュリティグループ（NSG）

正解： *C*

バックエンドのIP ACLを構成して、Azure FrontDoorのバックエンドIPアドレス空間とAzureのインフラストラクチャサービスからのトラフィックのみを受け入れるようにします。バックエンドのACLについては、以下のIPの詳細を参照してください。

* フロントドアのIPv4バックエンドIPアドレス範囲についてはAzure IP範囲とサービスタグのAzureFrontDoor.Backendセクションを参照するか、ネットワークセキュリティグループでサービスタグAzureFrontDoor.Backendを使用することもできます。

参照：

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

# Q.45

KV1という名前のAzureキーボールトがあります。

アプリケーションがKV1を使用して、外部の証明機関（CA）から証明書を自動的にプロビジョニングできることを確認する必要があります。

どの2つのアクションを実行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。

1. KV1から、証明書発行者リソースを作成します。
2. CAアカウントの資格情報を取得します。
3. ルートCA証明書を取得します。
4. KV1から、証明書署名要求（CSR）を作成します。
5. KV1から、秘密鍵を作成

正解： *CD*

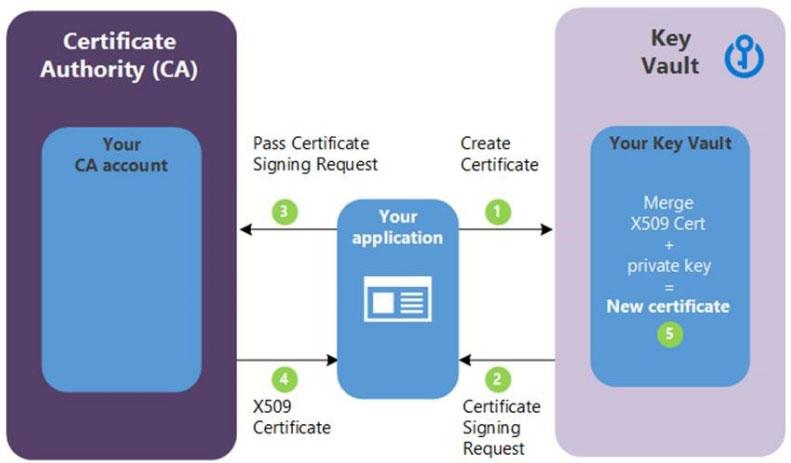
C：ルートCA証明書を取得します（下の図の手順4）

D：KV1から、証明書署名要求（CSR）を作成します（下の図の手順2）

注：

提携していないCAを使用して証明書を作成しますKey Vaultを使用する

この方法では、Key Vaultのパートナープロバイダー以外のCAを使用できます。つまり、組織は選択したCAを使用できます。



次の手順の説明は、前の図の緑色の文字の手順に対応しています。

1.上の図では、アプリケーションが証明書を作成しています。証明書は、内部的にキーボールトにキーを作成することから始まります。

2. Key Vaultは、証明書署名要求（CSR）をアプリケーションに返します。

3.アプリケーションはCSRを選択したCAに渡します。

4.選択したCAはX509証明書で応答します。

5.アプリケーションは、CAからのX509証明書をマージして、新しい証明書の作成を完了します。

参照：

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

# Q.46

次のAzureロール定義を作成します。



ロール定義を使用してRole1を作成する必要があります。

Role1を作成する前に、どの2つの値を変更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。

1. AssignableScopes
2. Description
3. DataActions
4. IsCustom
5. ID

正解： *AD*

例の一部：

"IsCustom": true,

"AssignableScopes": [

"/subscriptions/{subscriptionId1}",

"/subscriptions/{subscriptionId2}",

"/subscriptions/{subscriptionId3}"

The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

{

"Name": "Virtual Machine Operator",

"Id": "88888888-8888-8888-8888-888888888888",

"IsCustom": true,

"Description": "Can monitor and restart virtual machines.",

"Actions": [

"Microsoft.Storage/\*/read",

"Microsoft.Network/\*/read",

"Microsoft.Compute/\*/read",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Authorization/\*/read",

"Microsoft.ResourceHealth/availabilityStatuses/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Insights/alertRules/\*",

"Microsoft.Insights/diagnosticSettings/\*",

"Microsoft.Support/\*"

],

"NotActions": [],

"DataActions": [],

"NotDataActions": [],

"AssignableScopes": [

"/subscriptions/{subscriptionId1}",

"/subscriptions/{subscriptionId2}",

"/subscriptions/{subscriptionId3}"

]

}

Reference:

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

# Q.47

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

* Contoso.onmicrosoft.com：Microsoft 365テナントにリンクされ、パスワードハッシュ同期を使用してcontoso.comという名前のActiveDirectoryフォレストに同期されます
* Contosoazure.onmicrosoft.com：Subscription1という名前のAzureサブスクリプションにリンクされています

contoso.comのユーザーにSubscription1のリソースへのアクセスを割り当てることができることを確認する必要があります。

あなたは何をするべきか？

1. Subscription1が含まれているAzureの管理グループを作成します。
2. パススルー認証を使用するようにcontoso.onmicrosoft.comを構成します。
3. contosoazure.onmicrosoft.com内のすべてのcontoso.comのユーザーのためのゲストアカウントを作成します。
4. contosoazure.onmicrosoft.comとcontoso.comの間で設定Active Directoryフェデレーションサービス（AD FS）フェデレーション。

解答：D

# Q.48

ユーザーがAzureStorageアカウントからコンテンツをダウンロードできるようにするアプリケーションを開発しています。

ユーザーは、7日間のみコンテンツをダウンロードできる必要があります。

ストレージアカウントにアクセスするには、認証ソリューションを推奨する必要があります。

推奨事項には何を含める必要がありますか？

1. 共有アクセス署名（SAS）トークン
2. Active Directoryドメインサービス（AD DS）を使用するIDベースの認証
3. ストレージアクセスキー
4. Azure Active Directory（Azure AD）を使用するIDベースの認証

解答：A

# 