AZ-500-free-Exam#01

# Q.1

注：この質問は、同じシナリオを提示する一連の質問の一部です。

シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。

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

Sub1という名前のAzureサブスクリプションがあります。

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

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

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

sa1へのすべてのアクセスを取り消す必要があります。

解決策：新しい保存済みアクセスポリシーを作成します。

これは目標を達成していますか？

**No**

新しい（追加の）保存されたアクセスポリシーを作成しても、既存のポリシーまたはそれにリンクされているSASには影響しません。

保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。 署名された識別子を変更すると、既存の署名と保存されているアクセスポリシーとの関連付けが解除されます。 保存されたアクセスポリシーを削除または名前変更すると、それに関連付けられているすべての共有アクセス署名がすぐに有効になります。

参照：

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

# Q.2

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。

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 HD Insight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ことを計画しています。

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？

**No**

代わりに、Azure仮想ネットワークとVPNゲートウェイを使用して、HD Insightをオンプレミスネットワークに接続します。

注：参加しているネットワーク内のHD Insightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。

* Azure仮想ネットワークを作成します。
* Azure仮想ネットワークにカスタムDNSサーバーを作成します。
* デフォルトのAzure Recursive Resolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
* カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。

参照：

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network>

# Q.3

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。

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 HD Insight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ことを計画しています。

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：仮想ネットワークとオンプレミスネットワークの間にサイト間VPNを作成します。

これは目標を達成していますか？

**Yes**

代わりに、Azure仮想ネットワークとVPNゲートウェイを使用して、HD Insightをオンプレミスネットワークに接続します。

注：参加しているネットワーク内のHD Insightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。

* Azure仮想ネットワークを作成します。
* Azure仮想ネットワークにカスタムDNSサーバーを作成します。
* デフォルトのAzure Recursive Resolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
* カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。

参照：

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network>

# Q.4

ネットワークには、contoso.comという名前のActiveDirectoryフォレストが含まれています。

フォレストには単一のドメインが含まれています。

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

Azure AD Connectを展開し、Active Directory と Azure AD テナントを統合することを計画しています。

次の要件を満たす統合ソリューションを推奨する必要があります。

* テナントに同期されるユーザーアカウントにパスワードポリシーとユーザーログオン制限が適用されるようにします
* ソリューションに必要なサーバーの数を最小限に抑えます。

どの認証方法を推奨に含める必要がありますか？

**password hash synchronization with seamless single sign-on (SSO)**

**シームレスなシングルサインオン（SSO）によるパスワードハッシュ同期**

パスワードハッシュの同期には、展開、保守、およびインフラストラクチャに関する最小限の労力が必要です。このレベルの作業は通常、ユーザーがOffice 365、SaaSアプリ、およびその他のAzure AD ベースのリソースにサインインするだけでよい組織に適用されます。オンにすると、パスワードハッシュ同期はAzure AD Connect 同期プロセスの一部であり、2分ごとに実行されます。

参照：

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

# Q.5

ネットワークには、corp.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。

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

すべてのオンプレミスIDをAzure ADに同期します。

TESTで始まるgivenName属性を持つユーザーがAzure ADに同期されないようにする必要があります。 この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。

何を使うべきですか？

**Synchronization Rules Editor**

**同期ルールエディタ**

同期ルールエディタを使用して、属性ベースのフィルタリングルールを記述します。

参照：

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

# Q.6

ドラッグドロップ -

条件付きアクセスポリシーを実装しています。

ポリシーを構成および実装するには、既存のAzure Active Directory（Azure AD）のリスクイベントとリスクレベルを評価する必要があります。

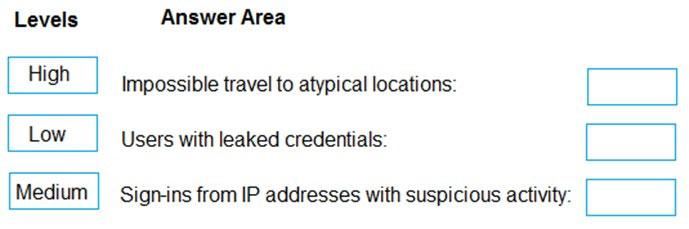
次のリスクイベントのリスクレベルを特定する必要があります。

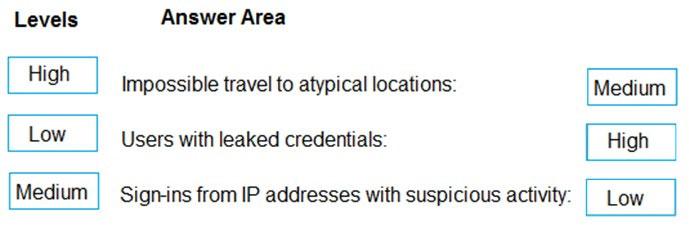
* クレデンシャルが漏洩したユーザー
* 非定型の場所への不可能な旅行
* 疑わしいアクティビティを伴うIPアドレスからのサインイン

リスクイベントごとにどのレベルを特定する必要がありますか？

答えるには、適切なレベルを正しいリスクイベントにドラッグします。 各レベルは、1回使用することも、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。

選択して配置：





Azure AD Identity Protectionは、次の6種類の疑わしいサインインアクティビティを検出できます。

* クレデンシャルが漏洩したユーザー
* 匿名IPアドレスからのサインイン
* 非定型の場所への不可能な旅行
* 感染したデバイスからのサインイン
* 疑わしいアクティビティを伴うIPアドレスからのサインイン
* 見知らぬ場所からのサインイン

これらの6種類のイベントは、高、中、低の3つのリスクレベルに分類されます。



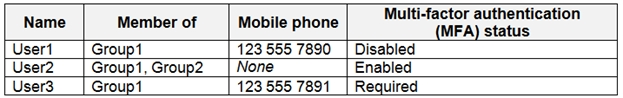
References:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

# Q.7

ホットスポット-

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。

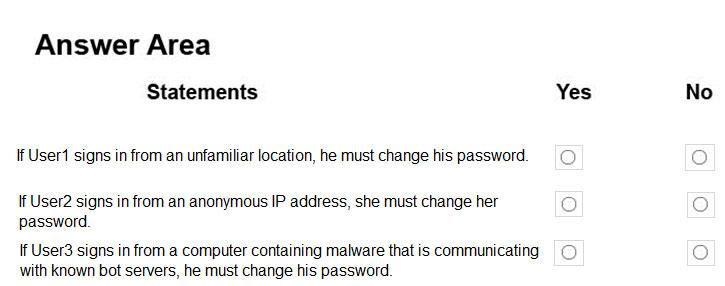


次の設定を持つ Azure AD Identity Protectionユーザーリスクポリシーを作成して適用します。

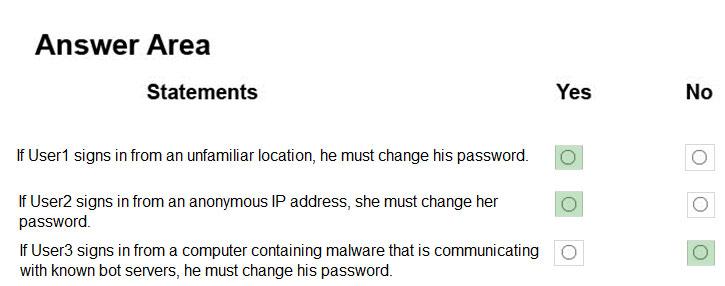
* 割り当て：グループ1を含める、グループ2を除外する
* 条件：中以上のサインインリスク
* アクセス：アクセスを許可し、パスワードの変更を要求する

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。

ホットエリア：



1. User1が見知らぬ場所からサインインする場合は、パスワードを変更する必要があります。
2. User2が匿名IPアドレスからサインインする場合、パスワードを変更する必要があります。
3. User3が既知のボットサーバーと通信しているマルウェアを含むコンピューターからサインインする場合は、パスワードを変更する必要があります。



**User1はGroup1のメンバーです。 見知らぬ場所からのサインインはリスクレベル中です。**

**User2はGroup1のメンバーです。 匿名IPアドレスからのサインインはリスクレベル中です。**

**疑わしいアクティビティのあるIPアドレスからのサインインはリスクレベル低です。**

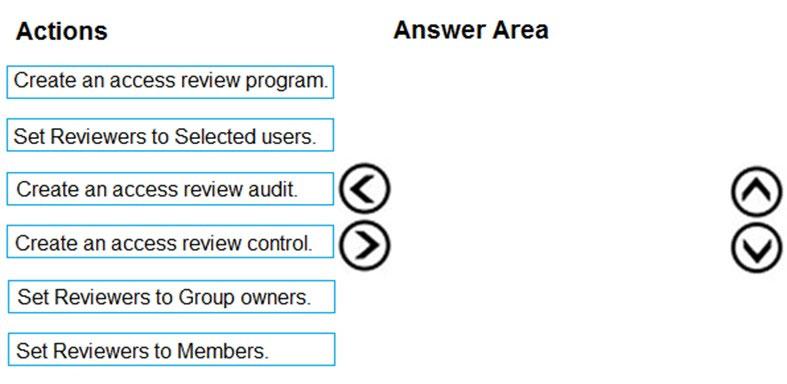
# Q.8

ドラッグドロップ -

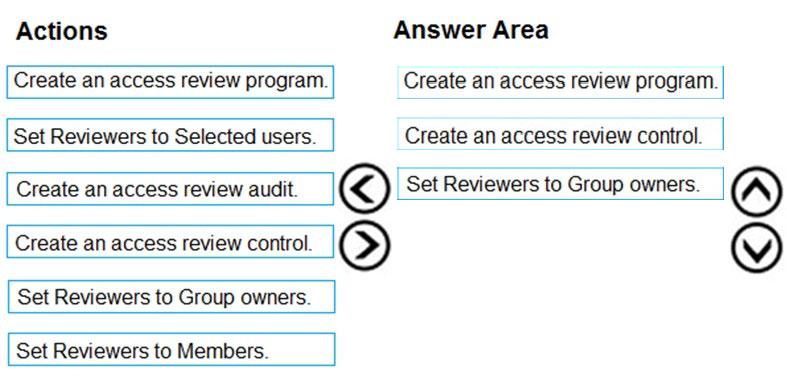
アクセスレビューを構成する必要があります。 レビューは新しいレビューのコレクションに割り当てられ、リソース所有者によってレビューされます。

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：



1. アクセスレビュープログラムを作成します。
2. レビュー担当者を選択したユーザーに設定します。
3. アクセスレビュー監査を作成します。
4. アクセスレビューコントロールを作成します。
5. レビュー担当者をグループ所有者に設定します。
6. レビュアーをメンバーに設定します。

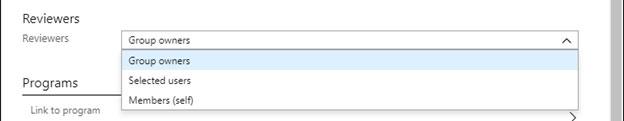


**ステップ1：アクセスレビュープログラムを作成する**

**ステップ2：アクセスレビューコントロールを作成する**

**ステップ3：レビュー担当者をグループ所有者に設定する**

[レビュー担当者]セクションで、1人以上のユーザーを選択して、スコープ内のすべてのユーザーをレビューします。 または、メンバーに自分のアクセスを確認させるように選択することもできます。 リソースがグループの場合は、グループの所有者に確認を依頼できます。



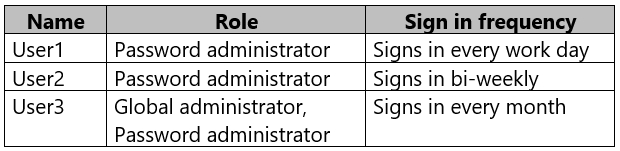
References:

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

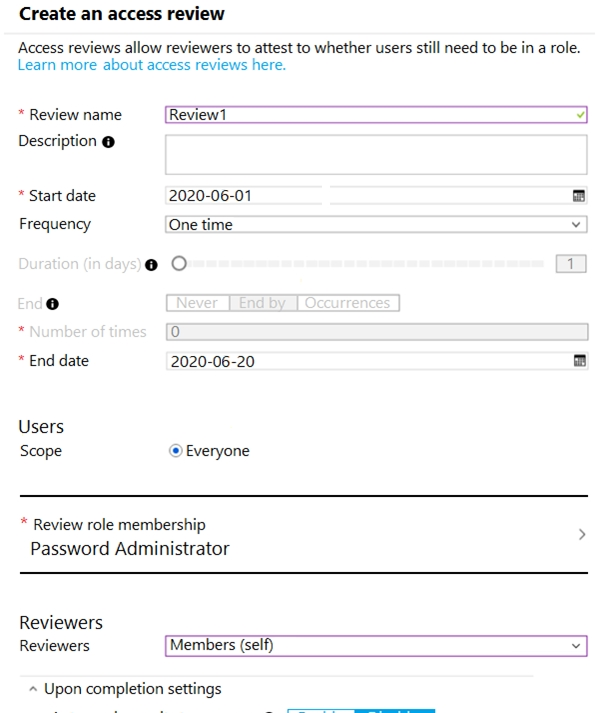
<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

# Q.9

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ています。

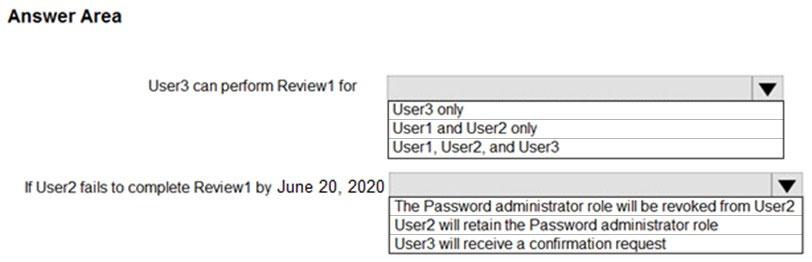


次の展示に示すように、Review1という名前のアクセスレビューを構成します。



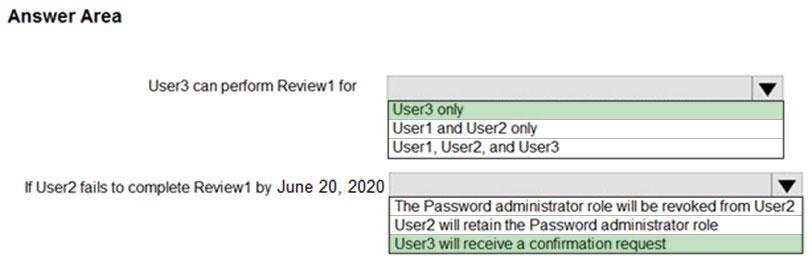
ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。

ホットエリア：



User3 can perform Review1 for User3 only.

If User2 fails to complete Review1 by June 20, 2020 User3 will receive a confirmation request.



**ボックス1：User3のみ**

メンバー（自己）オプションを使用して、ユーザーに自分の役割の割り当てを確認してもらいます。

**ボックス2：User3は確認リクエストを受け取ります**

レビュー担当者が応答しないリストを使用して、レビュー期間内にレビュー担当者によってレビューされなかったユーザーに何が起こるかを指定します。 この設定は、レビュー担当者が手動でレビューしたユーザーには影響しません。 最終レビューアの決定が拒否である場合、ユーザーのアクセスは削除されます。

変更なし-ユーザーのアクセスは変更しないでください

アクセスの削除-ユーザーのアクセスを削除します

アクセスの承認-ユーザーのアクセスを承認します

推奨事項を取得する-ユーザーの継続的なアクセスを拒否または承認する際のシステムの推奨事項を取得します

参照：

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

# Q.10

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。

Admin1という名前の管理者は、次のIDにアクセスできます。

* OpenID対応のユーザーアカウント
* Hotmailアカウント
* contoso.comのアカウント
* fabrikam.comという名前のAzureADテナントのアカウント

Azure Account Centerを使用して、Sub1の所有権をAdmin1に譲渡する予定です。

Sub1の所有権をどのアカウントに譲渡できますか？

1. contoso.comのみ
2. contoso.com、fabrikam.com、およびHotmailのみ
3. **contoso.comおよびfabrikam.comのみ**
4. contoso.com、fabrikam.com、Hotmail、およびOpenID対応のユーザーアカウント

サブスクリプションの請求所有権を別のAzureADテナントのアカウントに譲渡する場合、サブスクリプションを新しいアカウントのテナントに移動できます。 これを行うと、サブスクリプションとそのリソースを管理するためのロールベースアクセス（RBAC）を持っていたすべてのユーザー、グループ、またはサービスプリンシパルがアクセスできなくなります。 転送リクエストを受け入れる新しいアカウントのユーザーのみが、リソースを管理するためのアクセス権を持ちます。

参照：

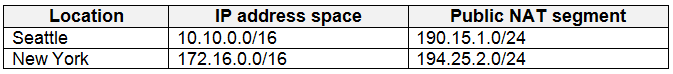
<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer>

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant>

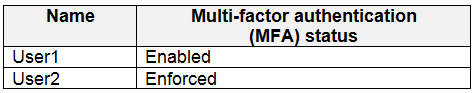
# Q.11

ホットスポット-

あなたの会社はシアトルとニューヨークに2つのオフィスを持っています。 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。 次の表に示すIPアドレスを使用します。



同社には、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ています。



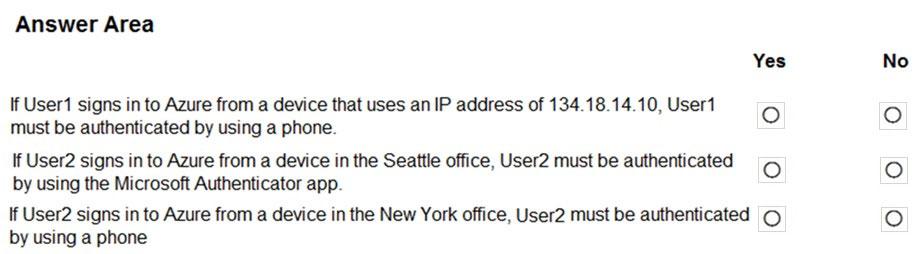
MFAサービス設定は、展示に示されているように構成されています。 （[展示]タブをクリックします。）



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：



User1が134.18.14.10のIPアドレスを使用するデバイスからAzureにサインインする場合、User1は電話を使用して認証される必要があります。

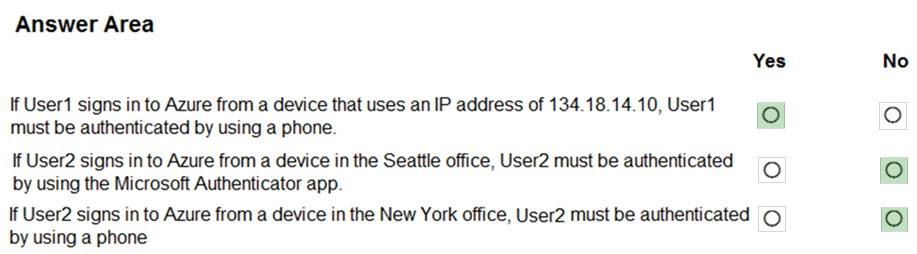
YES

User2がシアトルオフィスのデバイスからAzureにサインインする場合、User2はMicrosoft Authenticatorアプリを使用して認証される必要があります。

NO

User2がニューヨークオフィスのデバイスからAzureにサインインする場合、User2は電話を使用して認証される必要があります。

NO



ボックス1：はい

ボックス2：いいえ

MicrosoftAuthenticatorを使用する必要はありません。 MFAには、テキストメッセージまたは電話のいずれかが必要です。

注：Microsoft Authenticatorは、2段階認証プロセスで使用される時間ベースのコードを生成するモバイルデバイス用の多要素アプリです。

ボックス3：いいえ

ニューヨークのIPアドレスサブネットは、「リクエストの多要素認証をスキップする」に含まれています。

参照：

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

# Q.12

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。

同じ役割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？

1. Azure Security Center
2. Azure Policy
3. Azure AD Privileged Identity Management (PIM)
4. Azure Blueprints

正解：D

ブループリントでエンジニアやアーキテクトがプロジェクトの設計パラメーターをスケッチできるように、Azureブループリントでは、クラウドアーキテクトと中央の情報技術グループが、組織の標準、パターン、要件を実装および準拠する繰り返し可能なAzureリソースのセットを定義できます。

ブループリントは、さまざまなリソーステンプレートや、次のようなその他の成果物の展開を調整するための宣言型の方法です。

* 役割の割り当て
* ポリシーの割り当て
* Azure Resource Managerテンプレート
* リソースグループ

参照：

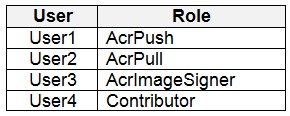
<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

# Q.13

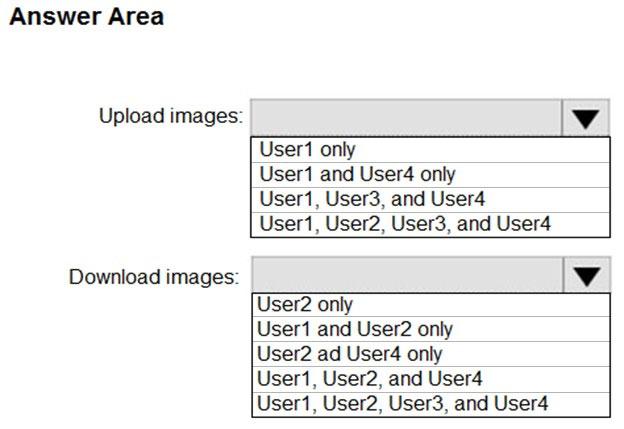
ホットスポット-

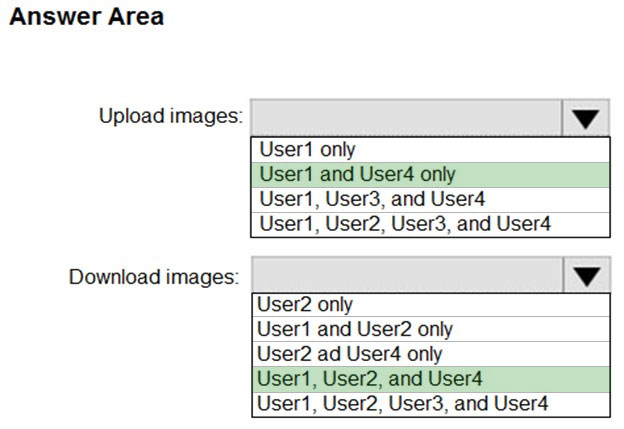
Registry1という名前のAzure Container Registryがあります。

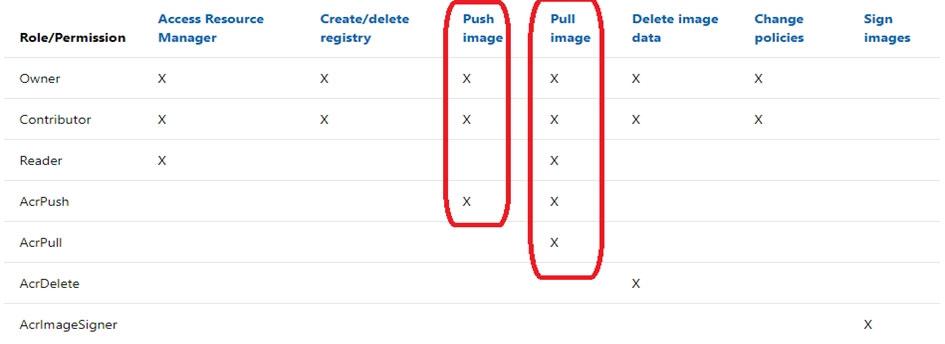
次の表に示すように、Registry1の役割の割り当てを追加します。



どのユーザーがRegistry1に画像をアップロードし、Registry1から画像をダウンロードできますか？







References:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles>

# Q.14

Azureサブスクリプションがあります。

S1 App Serviceプランを使用するContoso1812という名前のAzure Webアプリを作成します。

Contoso1812を指すwww.contoso.comの CNAME DNS レコードを作成します。

https://www.contoso.com URLを使用して、ユーザーがContoso1812にアクセス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？

1. Contoso1812 のシステム割り当ての管理対象IDをオンにします。
2. Contoso1812 にホスト名を追加します。
3. Contoso1812 の App Service プランをスケールアウトします。
4. Contoso1812 に展開スロットを追加します。
5. Contoso1812 の App Service プランをスケールアップします。
6. PFXファイルをContoso1812にアップロードします。

正解：B, F

B：WebアプリのカスタムドメインをホストするようにAzure DNSを構成できます。 たとえば、Azure Webアプリを作成し、完全修飾ドメイン名（FQDN）としてwww.contoso.comまたはcontoso.comを使用してユーザーにアクセスさせることができます。

これを行うには、次の3つのレコードを作成する必要があります。

* contoso.comを指すルート「A」レコード
* 検証用のルート「TXT」レコード
* Aレコードを指すwww名の「CNAME」レコード

F：HTTPSを使用するには、PFXファイルをAzure Webアプリにアップロードする必要があります。PFXファイルには、HTTPSに必要なSSL証明書が含まれます。

参照：

<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>

# Q.15

注：この質問は、同じシナリオを提示する一連の質問の一部です。 シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。 一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。

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

sub1という名前のAzureサブスクリプションがあります。

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

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

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

sa1へのすべてのアクセスを取り消す必要があります。

解決策：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？

正解：No

保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。 署名された識別子を変更すると、既存の署名と保存されているアクセスポリシーとの関連付けが解除されます。 保存されたアクセスポリシーを削除または名前変更すると、それに関連付けられているすべての共有アクセス署名にすぐに影響します。

参照：

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

# Q.16

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。

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 HD Insight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ことを計画しています。

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 Active Directoryドメインサービス（Azure AD DS）をAzureサブスクリプションにデプロイします。

これは目標を達成していますか？

正解：No

代わりに、Azure仮想ネットワークとVPNゲートウェイを使用して、HD Insightをオンプレミスネットワークに接続します。

注：参加しているネットワーク内のHD Insightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。

* Azure仮想ネットワークを作成します。
* Azure仮想ネットワークにカスタムDNSサーバーを作成します。
* デフォルトのAzureRecursiveResolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
* カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。

参照：

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network>

# Q.17

ネットワークには、contoso.comという名前のActive Directoryフォレストが含まれています。 contoso.comという名前のAzure Directory（Azure AD）テナントがあります。

Azure AD ConnectのExpress Settingsインストールオプションを使用して同期を構成することを計画しています。

計画された構成を実行するために必要な役割とグループを特定する必要があります。

ソリューションは、最小特権の原則を使用する必要があります。

どの2つの役割とグループを特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。

1. Active Directoryのドメイン管理者グループ
2. Azure ADのセキュリティ管理者の役割
3. Azure ADのグローバル管理者の役割
4. Azure ADのユーザー管理者の役割
5. Active DirectoryのEnterprise Adminsグループ

正解：C, E

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

# Q.18

ドラッグドロップ -

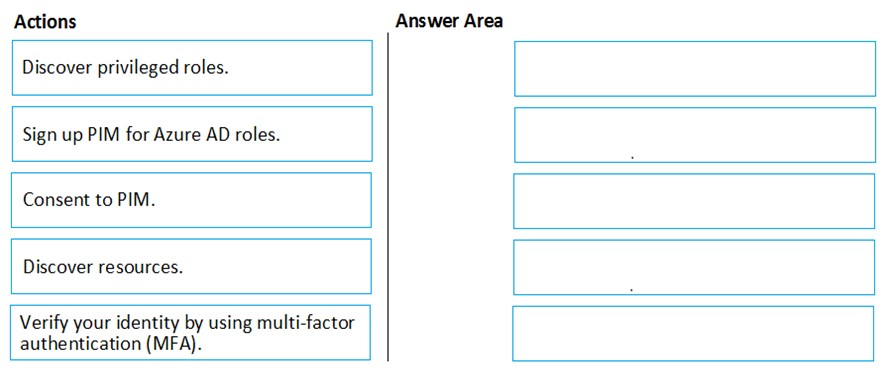
Azure AD Premium P2を使用してAzureサブスクリプションを作成します。

Azure Active Directory（Azure AD）特権ID管理（PIM）を使用してAzure ADの役割を保護できることを確認する必要があります。

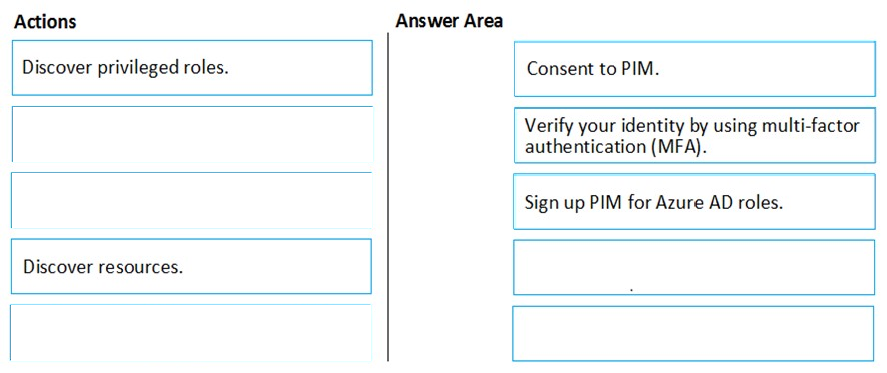
どの3つのアクションを順番に実行する必要がありますか？

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。

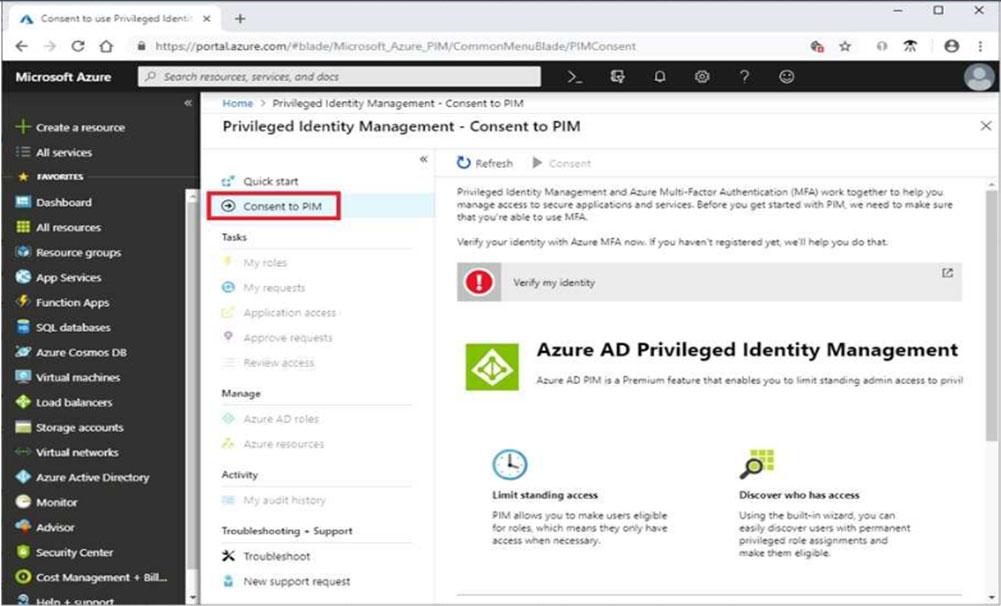
選択して配置：



* Discover privileged roles.(特権のある役割を見つけます。)
* Sign up PIM for Azure AD roles.(Azure ADロールのPIMにサインアップします。)
* Consent to PIM.(PIMへの同意。)
* Discover resources.(リソースを発見します。)
* Verify your identity by using Multi-Factor-Authentication(MFA).(Multi-Factor-Authentication（MFA）を使用して、本人確認を行ってください。)



1. PIMへの同意。
2. Multi-Factor-Authentication（MFA）を使用して、本人確認を行ってください。
3. Azure ADロールのPIMにサインアップします。



手順：2多要素認証（MFA）を使用してIDを確認します

[IDの確認]をクリックして、AzureMFでIDを確認します

アカウントを選択するように求められます。

手順3：AzureADの役割にPIMをサインアップする

ディレクトリに対してPIMを有効にしたら、AzureADの役割を管理するためにPIMにサインアップする必要があります。

# Q.19

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。

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 HD Insight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ことを計画しています。

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デプロイします。

これは目標を達成していますか？

正解：No

代わりに、Azure仮想ネットワークとVPNゲートウェイを使用して、HD Insightをオンプレミスネットワークに接続します。

注：参加しているネットワーク内のHDInsightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。

* Azure仮想ネットワークを作成します。
* Azure仮想ネットワークにカスタムDNSサーバーを作成します。
* デフォルトのAzureRecursiveResolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
* カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。

参照：

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network>

# Q.20

注：この質問は、同じシナリオを提示する一連の質問の一部です。 シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。 一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。

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

Sub1という名前のAzureサブスクリプションがあります。

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

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

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

sa1へのすべてのアクセスを取り消す必要があります。

解決策：Azureストレージアカウントのアクセスキーを再生成します。

これは目標を達成していますか？

正解：Yes

**新しいストレージアカウントキーを生成すると、以前のキーに基づいていたすべてのSASが無効になります。**

# Q.21

ホットスポット-

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。

テナントに対してAzure AD 特権ID管理（PIM）が有効になっています。

PIMでは、パスワード管理者の役割には次の設定があります。

* 最大アクティベーション期間（時間）：2
* 管理者にアクティベーションを通知するメールを送信する：無効にする
* 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：無効にする
* アクティベーションにAzureMulti-Factor認証が必要：有効にする
* この役割をアクティブ化するには承認が必要です：有効にする
* 選択された承認者：Group1

次の表に示すように、ユーザーにパスワード管理者の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。



1. User1がサインインすると、ユーザーにはパスワード管理者の役割が自動的に割り当てられます。
2. User2は、パスワード管理者の役割のアクティブ化を要求できます。
3. User3がパスワード管理者の役割をアクティブ化する場合、ユーザーは自分の要求を承認できます。



ボックス1：Yes

アクティブな割り当てでは、メンバーがロールを使用するためにアクションを実行する必要はありません。アクティブとして割り当てられたメンバーには、常にロールに割り当てられた特権があります。

ボックス2：No

User2ではMFAが無効になっており、[アクティブ化にAzure Multi-FactorAuthenticationが必要]設定が有効になっています。

注：適格な割り当てでは、役割のメンバーが役割を使用するためのアクションを実行する必要があります。 アクションには、多要素認証の実行が含まれる場合があります

（MFA）チェック、ビジネス上の正当性の提供、または指定された承認者からの承認の要求。

ボックス3：Yes

User3は、選択された承認者グループであるGroup1です。

参照：

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

# Q.22

シングルサインオン（SSO）が有効になっている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 データベースインスタンスがあります。

データベース開発者は、ドメインに参加しているデバイスからデータベースインスタンスに接続し、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。

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？

1. ActiveDirectory-パスワード
2. ActiveDirectory-MFAをサポートするユニバーサル
3. SQLServer認証
4. ActiveDirectory-統合

Active Directory 統合

正解：D

ActiveDirectory-統合-

Azure Active Directory認証は、Azure Active Directory（Azure AD）のIDを使用してMicrosoft AzureSQLデータベースに接続するメカニズムです。

フェデレーションドメインからAzureActive 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、この方法を使用してSQLデータベースに接続します。

参照：

<https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017>

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

# Q.23

Azure Resource Managerテンプレートを使用して、同じように構成されたAzure仮想マシンの複数のデプロイを実行することを計画しています。 各デプロイメントの管理者アカウントのパスワードは、さまざまなAzureキーボールトにシークレットとして保存されます。

各デプロイメント中に適切なシークレットを含むキーボールトを指定するリソースIDを動的に構築する方法を特定する必要があります。

キーボールトの名前とシークレットの名前は、インラインパラメータとして提供されます。

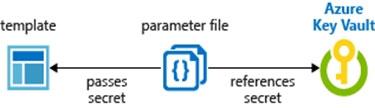
リソースIDを作成するために何を使用する必要がありますか？

1. Key Vault Access Policy
2. リンクされたテンプレート
3. パラメータファイル
4. 自動化アカウント

正解：C

テンプレートではなく、パラメータファイルでキーボールトを参照します。

次の画像は、パラメータファイルがシークレットを参照し、その値をテンプレートに渡す方法を示しています。



参照：

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter>

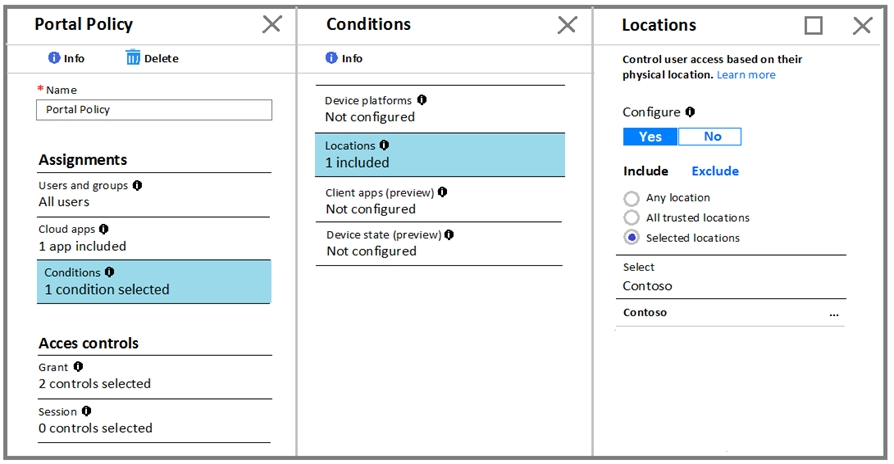
# Q.24

ホットスポット-

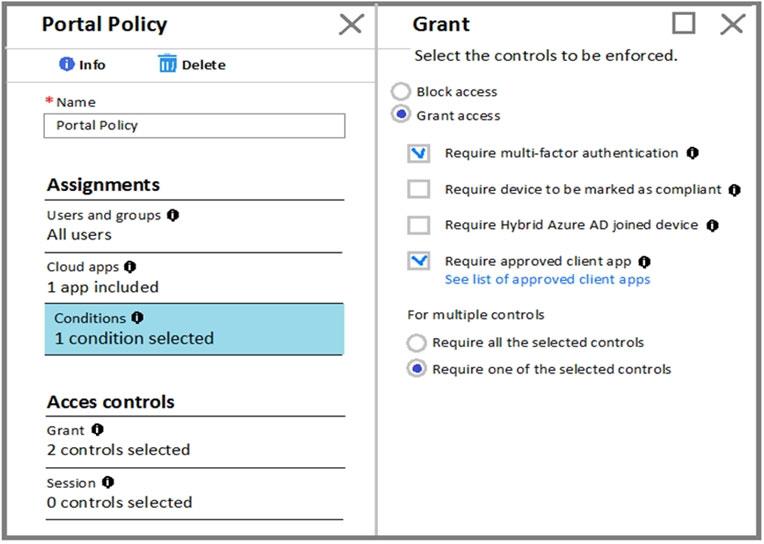
新しいAzureActive Directory（Azure AD）テナントに関連付けられた新しいAzureサブスクリプションを作成します。

PortalPolicyという名前のアクティブな条件付きアクセスポリシーを1つ作成します。 ポータルポリシーは、Microsoft AzureManagementクラウドアプリへのアクセスを提供するために使用されます。

ポータルポリシーの条件設定は、条件の展示に示されているように構成されています。 （[条件]タブをクリックします。）



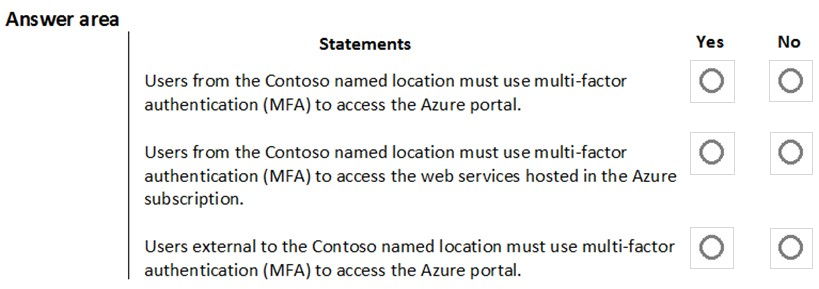
ポータルポリシーのGrant設定は、Grant展示に示されているように構成されています。 （[許可]タブをクリックします。）



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：



1. Contosoという名前の場所のユーザーは、Multi-factor-authentication（MFA）を使用してAzureポータルにアクセスする必要があります。
2. Contosoの指定された場所のユーザーは、Multi-factor-authentication（MFA）を使用して、AzureサブスクリプションでホストされているWebサービスにアクセスする必要があります。
3. Contosoという名前の場所の外部のユーザーは、Azure Portalにアクセスするためにmulti-factor-authentication（MFA）を使用する必要があります。

ボックス1：いいえ-

Contosoの場所は除外されます

ボックス2：はい-

ボックス3：はい-

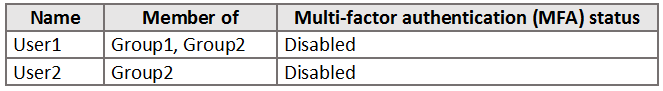
参照：

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

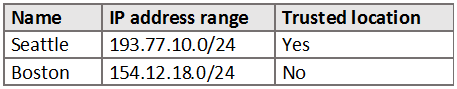
# Q.25

ホットスポット-

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。



テナントには、次の表に示す名前付きの場所が含まれています。

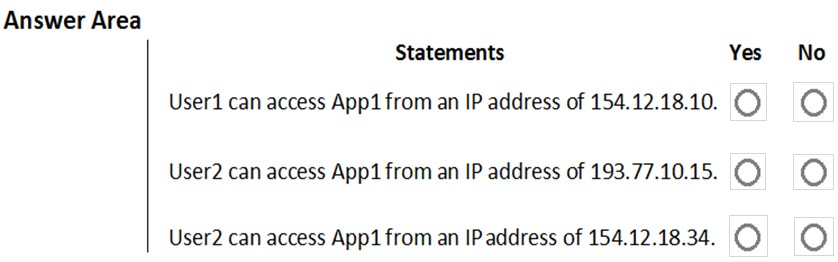


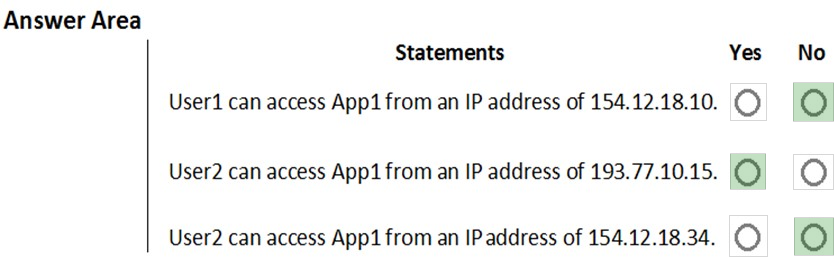
次の表に示すように、App1という名前のクラウドアプリの条件付きアクセスポリシーを作成します。



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。

ホットエリア：

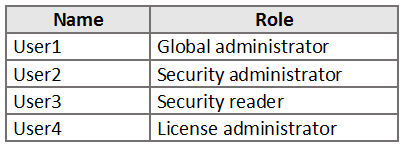




# Q.26

ホットスポット-

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。テナントには、次の表に示すユーザーが含まれています。

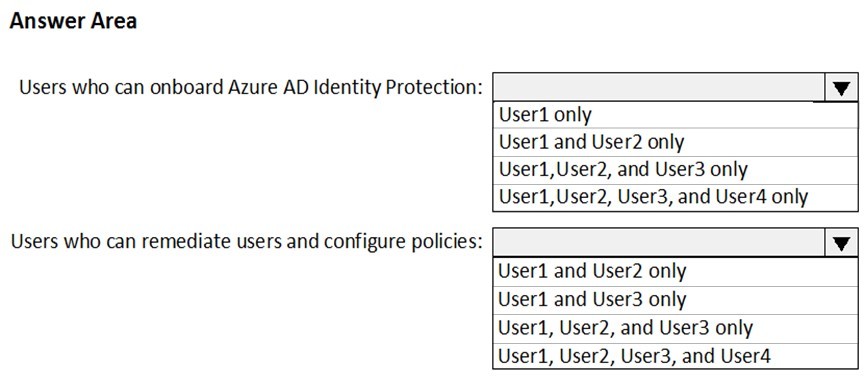


各ユーザーには、Azure AD Premium P2ライセンスが割り当てられます。

Azure AD Identity Protectionをオンボードして構成することを計画しています。

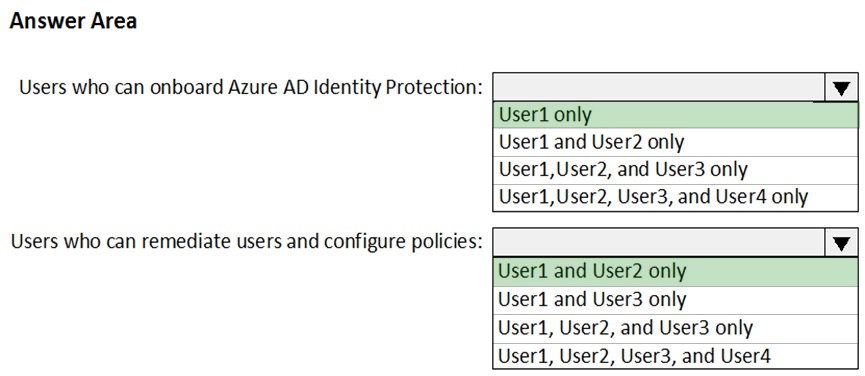
Azure AD Identity Protectionをオンボードし、ユーザーを修正し、ポリシーを構成できるユーザーはどれですか？ 回答するには、回答領域で適切なオプションを選択します。

ホットエリア：



User1 と User2←×　User1 だけ

User1 と User2



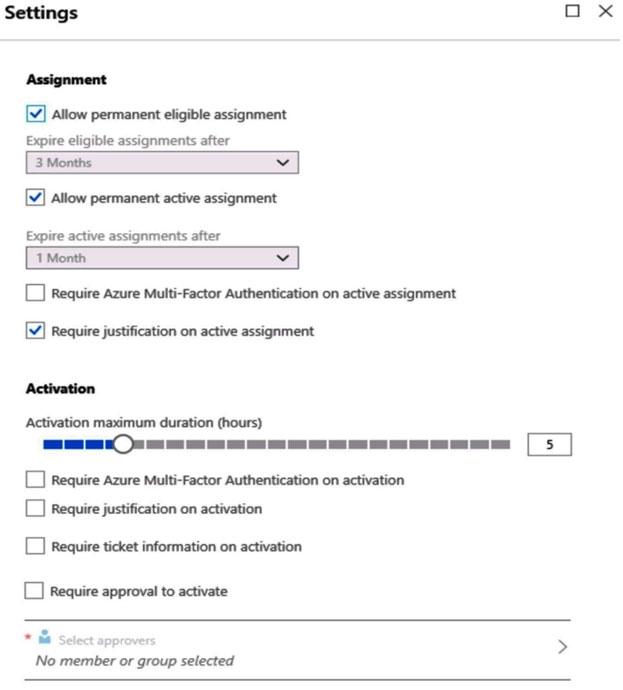
# Q.27

ホットスポット-

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



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



PIMから、セキュリティ管理者の役割を次のグループに割り当てます。

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

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。

ホットエリア：



1. User1は、5時間以内にのみセキュリティ管理者の役割をアクティブ化できます。
2. User2がセキュリティ管理者の役割をアクティブにすると、ユーザーにはすぐに役割が割り当てられます。
3. User3は、セキュリティ管理者の役割をアクティブ化できます。

ボックス1：はい

適格なタイプ：ユーザーが役割を使用するために1つ以上のアクションを実行する必要がある役割の割り当て。ユーザーがロールの資格を取得している場合、特権タスクを実行する必要があるときにロールをアクティブ化できることを意味します。永続的な役割と適格な役割が割り当てられている人に与えられるアクセスに違いはありません。唯一の違いは、一部の人々は常にそのアクセスを必要としないということです。役割の設定を構成するときに、割り当てタイプ（適格およびアクティブ）ごとに2つの割り当て期間オプションから選択できます。これらのオプションは、ユーザーが特権ID管理のロールに割り当てられている場合のデフォルトの最大期間になります。

アクティベーションの最大期間]スライダーを使用して、ロールが期限切れになる前にアクティブのままでいる最大時間を時間単位で設定します。この値は1〜24時間です。

ボックス2：はい

アクティブタイプ：ユーザーが役割を使用するためにアクションを実行する必要がない役割の割り当て。アクティブとして割り当てられたユーザーには、ロールに割り当てられた特権があります

ボックス3：はい

User3はGroup2のメンバーです。

参照：

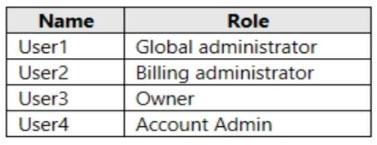
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

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

# Q.28

ホットスポット

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



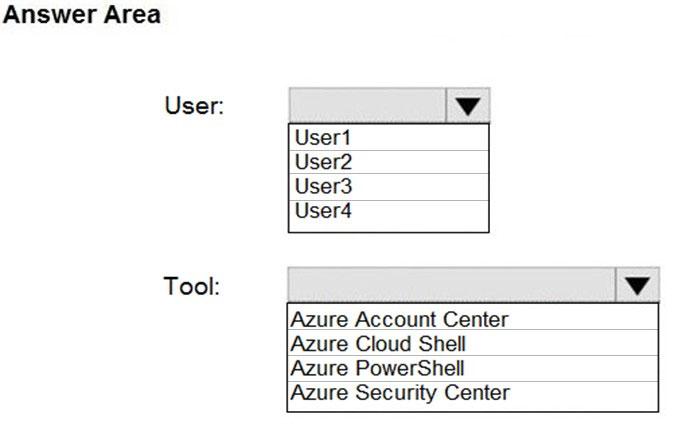
会社は新しい所有者に売却されます。

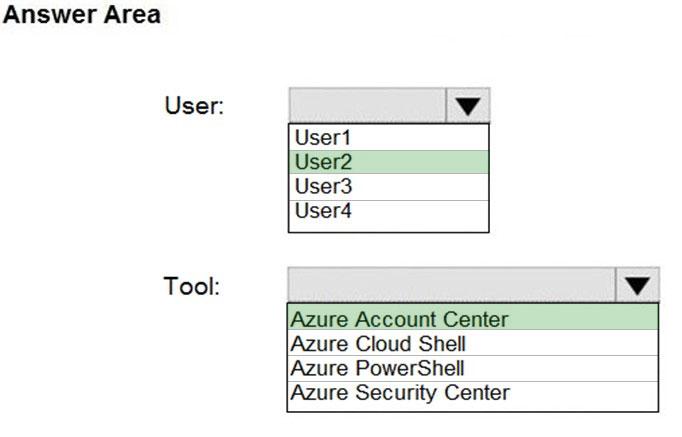
会社は Subscription1 の所有権を譲渡する必要があります。

どのユーザーが所有権を譲渡でき、どのツールを使用する必要がありますか？

回答するには、回答領域で適切なオプションを選択します。

ホットエリア：





ボックス1; User2

請求管理者(Billing Administrator)

譲渡するサブスクリプションの[請求所有権の譲渡]を選択します。

サブスクリプションの新しい所有者となるアカウントの請求管理者であるユーザーの電子メールアドレスを入力します。

ボックス2：Azureアカウントセンター

Azureアカウントセンターを使用できます。

参照：

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

# Q.29シミュレーション-

あなたの会社の開発者は、App10598168という名前のWebアプリを作成し、そのアプリをhttps://www.contoso.comに公開することを計画しています。

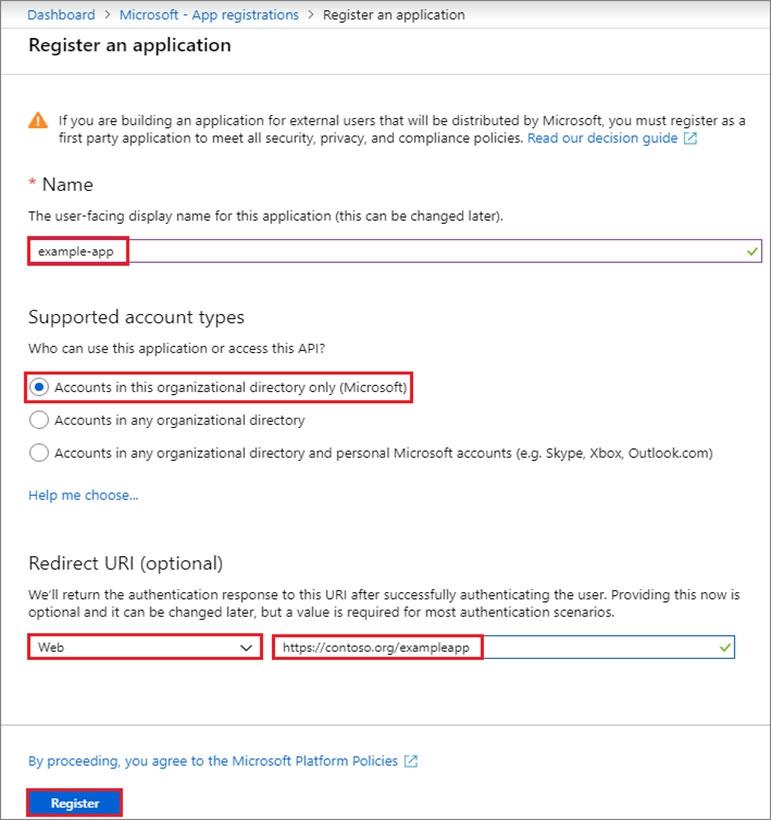
次のタスクを実行する必要があります。

* App10598168 が Azure Active Directory（Azure AD）に登録されていることを確認します。
* App10598168 のパスワードを生成します。

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。

ステップ1：アプリケーションを登録する

1. AzureポータルからAzureアカウントにサインインします。
2. Azure Active Directoryを選択します。
3. [アプリの登録]を選択します。
4. [新規登録]を選択します。
5. アプリケーションにApp10598168という名前を付けます。サポートされているアカウントタイプを選択します。これにより、アプリケーションを使用できるユーザーが決まります。 [リダイレクトURI]で、作成するアプリケーションの種類として[Web]を選択します。
6. URIを入力します：https：//[www.contoso.com、ここでアクセストークンが送信されます。](about:blank)
7. [登録]をクリックします



ステップ2：新しいアプリケーションシークレットを作成する

証明書を使用しないことを選択した場合は、新しいアプリケーションシークレットを作成できます。

1. 証明書とシークレットを選択します。
2. [クライアントシークレット]-> [新しいクライアントシークレット]を選択します。
3. 秘密の説明と期間を提供します。完了したら、[追加]を選択します。

クライアントシークレットを保存すると、クライアントシークレットの値が表示されます。

後でキーを取得できないため、この値をコピーします。

キー値にアプリケーションIDを指定して、アプリケーションとしてサインインします。

アプリケーションが取得できるキー値を格納します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

# Q.30シミュレーション

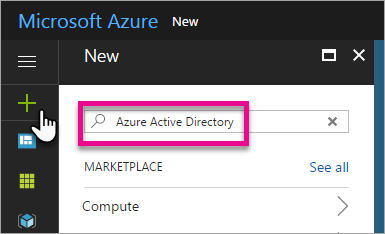
11641655.onmicrosoft.comという名前の新しいAzure Active Directory（Azure AD）ディレクトリと、新しいディレクトリにUser1という名前のユーザーを作成する必要があります。このソリューションでは、User1でAzure Multi-Factor Authentication（MFA）が有効になっていることを確認する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

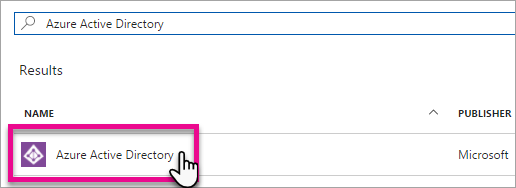
手順1：Azure ActiveDirectoryテナントを作成する

1. Azureポータルを参照し、Azureサブスクリプションを持つアカウントでサインインします。

2.プラスアイコン（+）を選択し、Azure ActiveDirectoryを検索します。

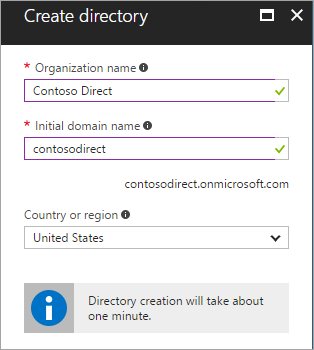


3.検索結果で[AzureActiveDirectory]を選択します。



4. [作成]を選択します。

5.組織名と初期ドメイン名（10598168）を入力します。次に、[作成]を選択します。ディレクトリが作成されます。

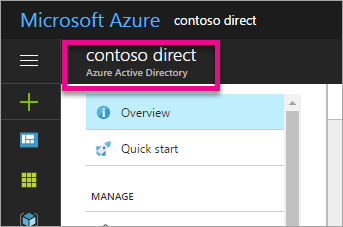


6.ディレクトリの作成が完了したら、情報ボックスを選択して新しいディレクトリを管理します。

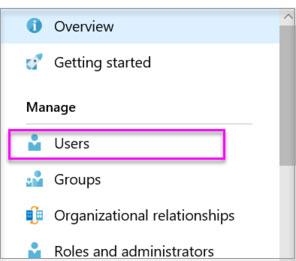
次に、テナントユーザーを追加します。

手順2：Azure ActiveDirectoryテナントユーザーを作成する

7. Azureポータルで、Azure ActiveDirectoryフライアウトを使用していることを確認します。



8. [管理]で、[ユーザー]を選択します。



9. [すべてのユーザー]を選択してから、[+新しいユーザー]を選択します。

10.通常のユーザーテナントの名前とユーザー名（user1）を入力します。一時パスワードを表示することもできます。完了したら、[作成]を選択します。

名前：user1-

ユーザー名：user1@11641655.onmicrosoft.com



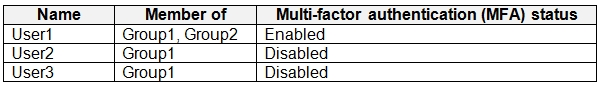
参照：

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

# Q.31

ホットスポット-

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。



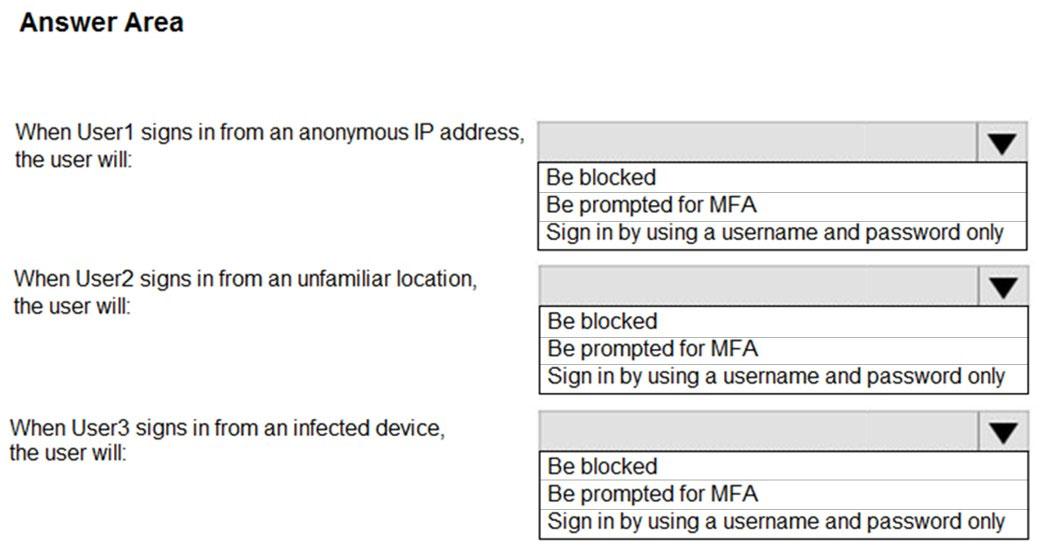
次の設定を持つAzure AD Identity Protectionサインインリスクポリシーを作成して適用します。

* 割り当て：Group1を含め、Group2を除外します
* 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し、多要素認証を要求する

ユーザーがAzureADにサインインしたときに何が発生するかを特定する必要があります。

ユーザーごとに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。

ホットエリア：





References:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

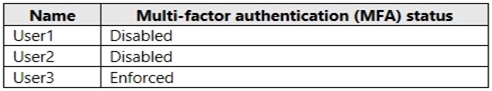
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

# Q.32

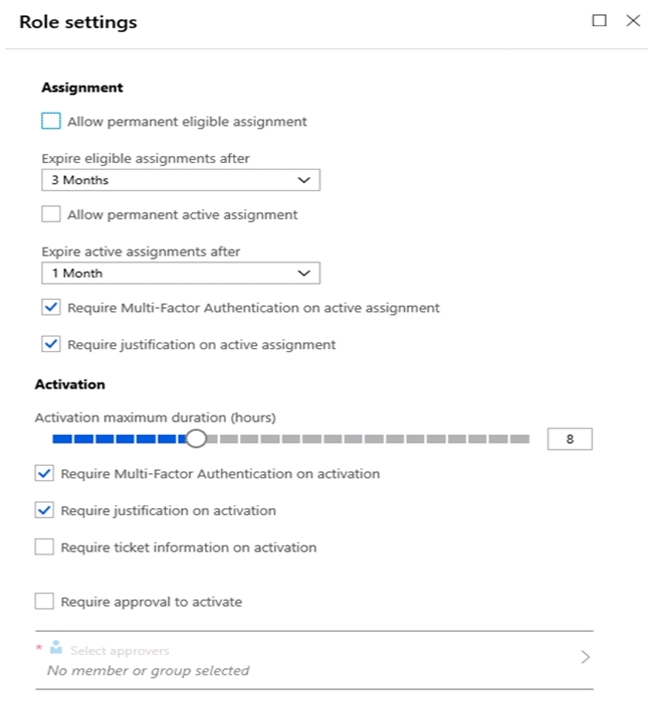
ホットスポット-

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

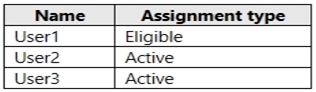


Azure AD Privileged Identity Management（PIM）では、コントリビューターロールのロール設定は、展示に示されているように構成されます。

（[展示]タブをクリックします。）

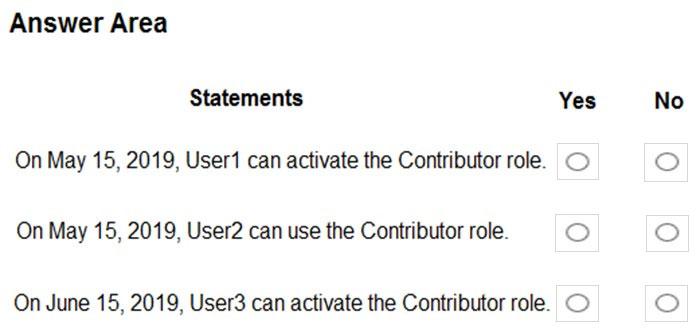


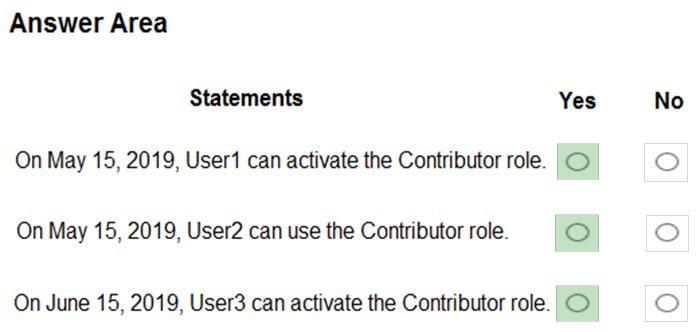
次の表に示すように、2019年5月1日にユーザーにコントリビューターの役割を割り当てます。



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。

ホットエリア：





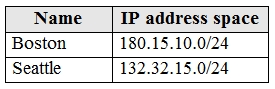
References:

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

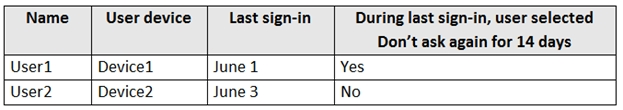
# Q.33

ホットスポット

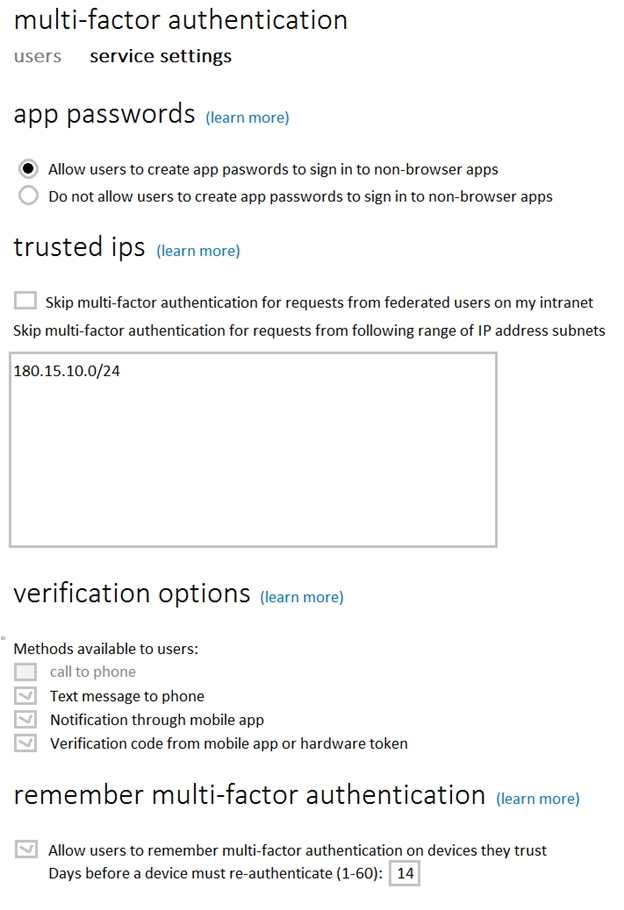
次の表に示すオフィスを持つContoso.Ltdという会社で働いています。



Contosoには、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。 すべてのcontoso.comユーザーは、Azure Multi-Factor Authentication（MFA）を有効にしています。 テナントには、次の表に示すユーザーが含まれています。



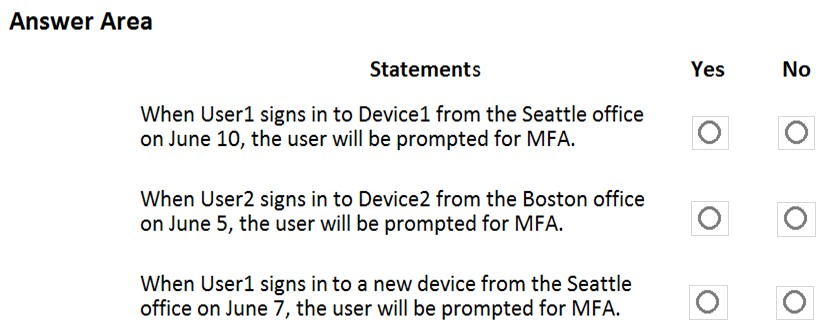
contoso.comの多要素認証設定は、次の図に示すように構成されています。



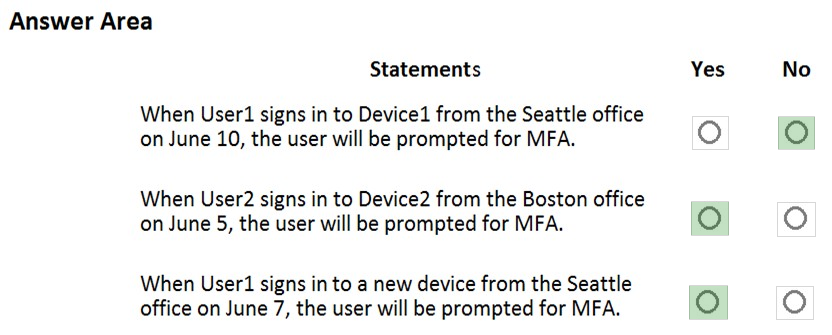
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。 それ以外の場合は、[いいえ]を選択します。

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：



1. User1が6月10日にシアトルオフィスからDevice1にサインインすると、ユーザーはMFAの入力を求められます。
2. User2が6月5日にボストンオフィスからDevice2にサインインすると、ユーザーはMFAの入力を求められます。
3. User1が6月7日にシアトルのオフィスから新しいデバイスにサインインすると、ユーザーはMFAの入力を求められます。



# Q.34

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。

変更による2つの考えられる影響は何ですか？ それぞれの正解は完全な解決策を提示します。

1. 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。
2. 仮想マシンで管理されているIDは失われます。
3. 仮想マシンのディスクスナップショットは失われます。
4. 既存のAzureリソースが削除されます。

A, B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

# Q.35

注：この質問は、同じシナリオを提示する一連の質問の一部です。 シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。 一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。

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

Sub1という名前のAzureサブスクリプションがあります。

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

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

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

sa1へのすべてのアクセスを取り消す必要があります。

解決策：新しいSASを生成します。

これは目標を達成していますか？

正解：No

代わりに、新しい保存済みアクセスポリシーを作成する必要があります。

保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。 署名された識別子を変更すると、既存の署名と保存されているアクセスポリシーとの関連付けが解除されます。 保存されたアクセスポリシーを削除または名前変更すると、それに関連付けられているすべての共有アクセス署名にすぐに影響します。

参照：

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

# Q.36

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。

あなたは最初に何をすべきですか？

1. Azure Directory（Azure AD）の特権ID管理（PIM）から、セキュリティ管理者のユーザーロールをアクティブ化します。
2. Azure Active Directory（Azure AD）特権ID管理（PIM）から、仮想マシンの所有者の役割をアクティブ化します。
3. Azureポータルから、仮想マシンを選択し、[接続]を選択してから、[アクセスの要求]を選択します。
4. 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。

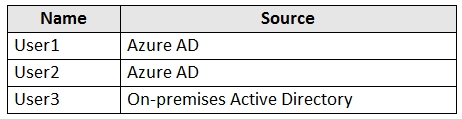
解答：C

リファレンス：

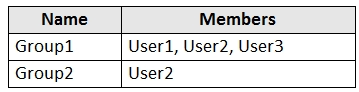
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon>

# Q.37

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



テナントには、次の表に示すグループが含まれています。

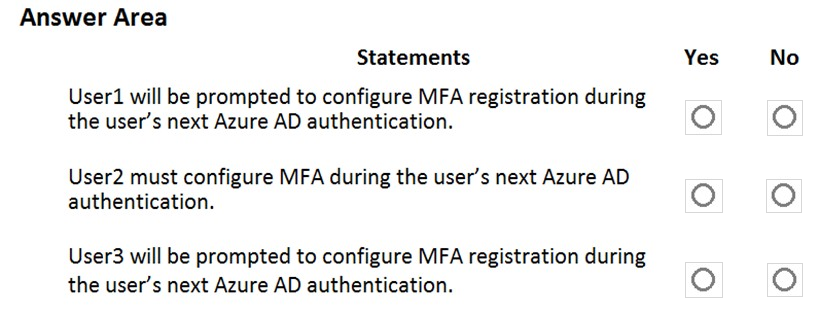


次の設定を持つ多要素認証（MFA）登録ポリシーを構成します。

割り当て：含める：グループ1、グループ2を除外する

コントロール：Azure MFA登録を要求する

ポリシーを適用する：オン



1. User1は、ユーザーの次のAzureAD認証中にMFA登録を構成するように求められます。
2. User2は、ユーザーの次のAzureAD認証中にMFAを構成する必要があります。
3. User3は、ユーザーの次のAzureAD認証中にMFA登録を構成するように求められます。

解答



# Q.38シミュレーション-

会社の開発者は、App11641655という名前のアプリをAzureに公開することを計画しています。

アプリがAzureActive Directory（Azure AD）に登録されていることを確認する必要があります。登録には、https://app.contoso.comのサインオンURLを使用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。

手順1：アプリケーションを登録する

1.AzureポータルからAzureアカウントにサインインします。

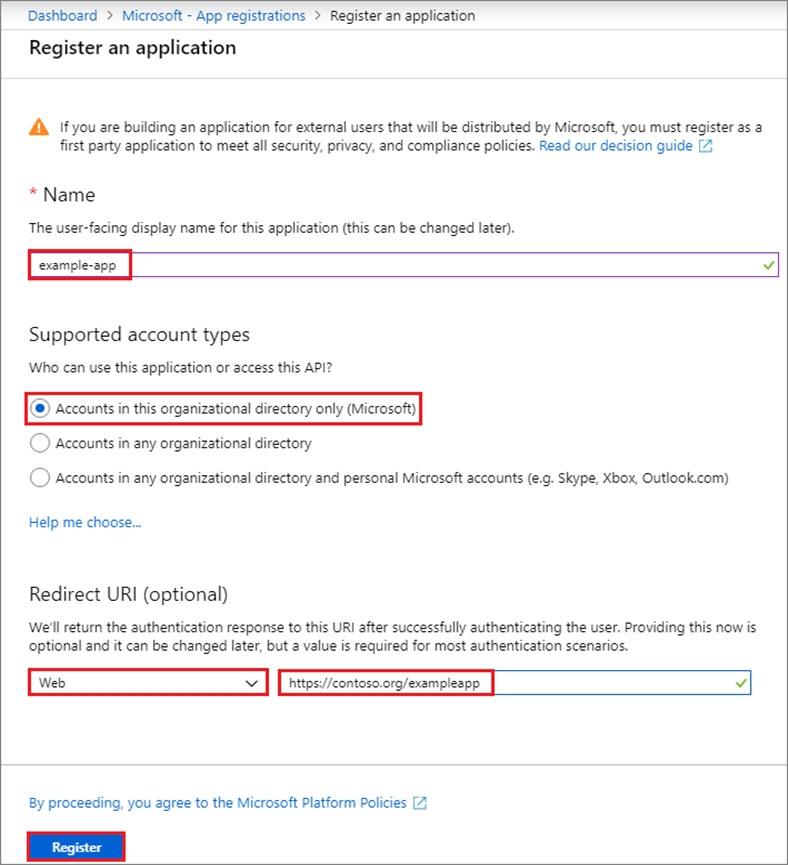
2. Azure ActiveDirectoryを選択します。

3. [アプリの登録]を選択します。

4. [新規登録]を選択します。

5.アプリケーションにApp11641655という名前を付けます。サポートされているアカウントタイプを選択します。これにより、アプリケーションを使用できるユーザーが決まります。[リダイレクトURI]で、作成するアプリケーションの種類として[Web]を選択します。URIを入力します：https：//app.contoso.com、ここでアクセストークンが送信されます。

6. [参照の登録]をクリックします



<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

# Q.39

contoso.onmicrosoft.comという名前の Azure Active Directory（Azure AD）テナントがあります。

ユーザー管理者の役割は、Admin1という名前のユーザーに割り当てられます。

外部パートナーには、[user1@outlook.com](mailto:user1@outlook.com)サインインを使用するMicrosoftアカウントがあります。

Admin1 は外部パートナーを Azure AD テナントにサインインするように招待しようとし、次のエラーメッセージを受け取ります。

ユーザー[user1@outlook.com](mailto:user1@outlook.com)を招待できません。一般的な承認の例外

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？

1. [役割と管理者]ブレードから、セキュリティ管理者の役割をAdmin1に割り当てます。
2. 組織関係ブレードから、IDプロバイダーを追加します。
3. [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。
4. [ユーザー]ブレードから、外部コラボレーション設定を変更します。

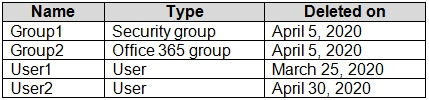
解答：D

外部コラボレーション設定でゲストの招待を許可する必要があります。

# Q.40

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

次の表に示すように、削除されたオブジェクトがあります。



2020年5月4日に、Azure Active Directory管理センターを使用して削除されたオブジェクトを復元しようとしました。

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

1. グループ1
2. グループ2
3. ユーザー2
4. ユーザー1

解答：B, C

削除されたユーザーと削除された**Office 365グループは、30日間復元できます**。

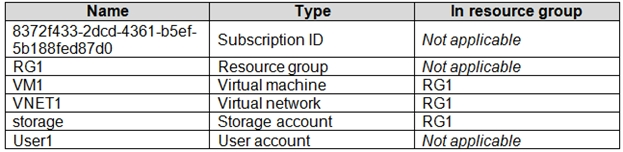
**削除したセキュリティグループを復元することはできません。**

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted>

# Q.41

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



次のJSONファイルを使用してAzureロールを作成します。

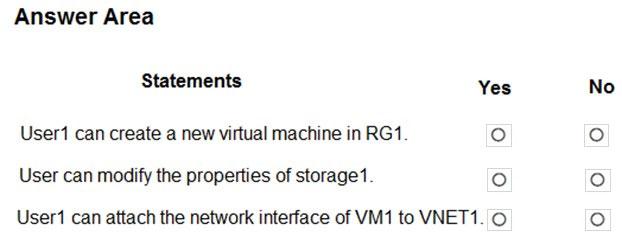


Role1をRG1のUser1に割り当てます。

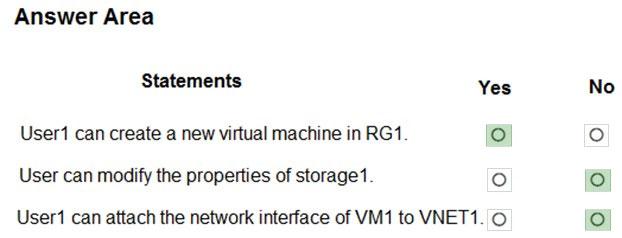
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

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：



1. User1は、RG1で新しい仮想マシンを作成できます。
2. ユーザーはstorage1のプロパティを変更できます。
3. User1は、VM1のネットワークインターフェイスをVNET1に接続できます。

正解： 

参照：

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

# Q.42

User1という名前のユーザーを含むcontoso.comという名前の Azure Active Directory（Azure AD）テナントがあります。

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。

この目標を達成するために、User1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？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. セキュリティ管理者
2. クラウドアプリケーション管理者
3. アプリケーション管理者
4. ユーザー管理者
5. アプリケーション開発者

正解： BC

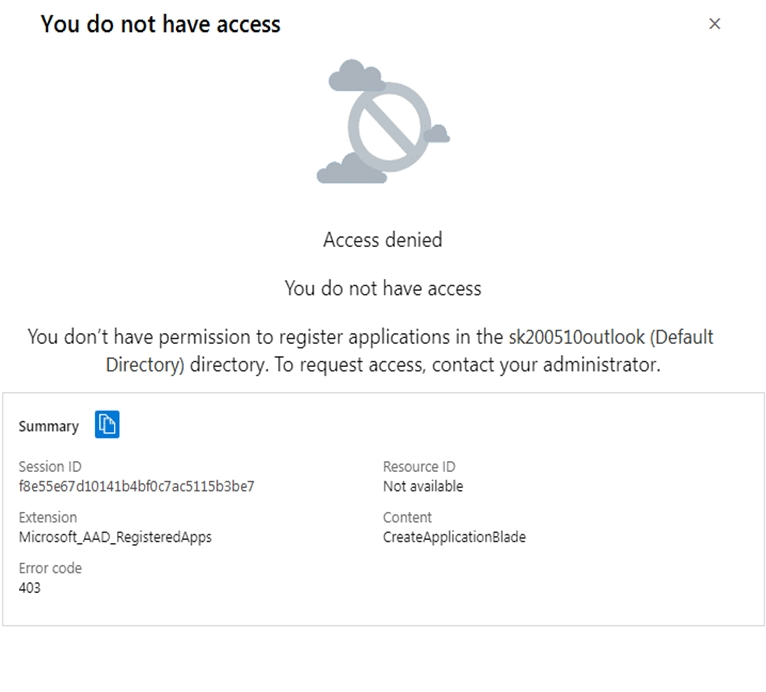
リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>

# Q.43

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、開発者は次の展示に示すエラーメッセージを受け取ります。



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。

テナントのために何をすべきですか？

1. ディレクトリのプロパティを変更します。
2. [ 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。
3. 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。
4. ユーザー設定を変更します。

正解： D

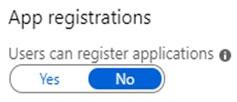
リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

# Q.44

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、次の図の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。ソリューションは、最小特権の原則を使用する必要があります。

User1にどの役割を割り当てる必要がありますか？

1. サブスクリプションのアプリ構成データの所有者
2. サブスクリプションのマネージドアプリケーションコントリビューター
3. Azure ADのクラウドアプリケーション管理者
4. Azure ADの アプリケーション開発者

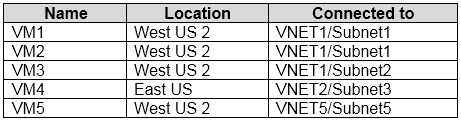
正解： D

リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

# Q.45

次の表に示すAzure仮想マシンがあります。



各仮想マシンには、単一のネットワークインターフェイスがあります。

VM1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します。

ASG1に追加できる仮想マシンのネットワークインターフェイス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？

1. VM2のみ
2. VM2とVM3のみ
3. VM2、VM3、VM4、およびVM5
4. VM2、VM3、およびVM5のみ

正解： B

リファレンス：

<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>

# Q.46シミュレーション-

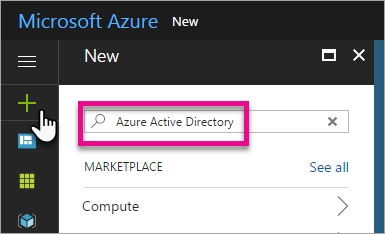
あなたは10317806.onmicrosoft.comという名前の新しいAzureのActive Directoryの（アズールAD）ディレクトリを作成する必要があります。新しいディレクトリには、Azure Multi-Factor Authentication（MFA）を使用してサインインするように構成されたuser10317806という名前のユーザーが含まれている必要があります。

正解： *以下の説明を参照してください。*

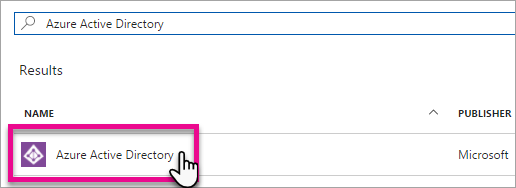
新しいAzureADテナントを作成するには：

1。Azureポータルを参照し、Azureサブスクリプションを持つアカウントでサインインします。

2.プラスアイコン（+）を選択し、Azure ActiveDirectoryを検索します。



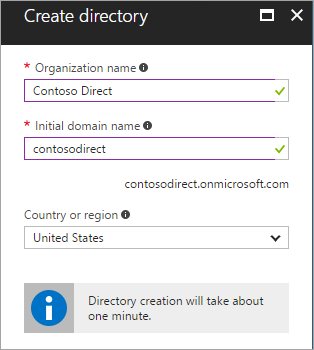
3.検索結果で[AzureActiveDirectory]を選択します。



4. [作成]を選択します。

5.組織名（10317806）と初期ドメイン名（10317806）を入力します。次に、[作成]を選択します。これにより、

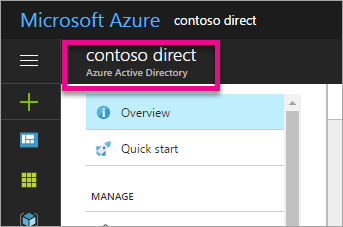
10317806.onmicrosoft.comという名前のディレクトリが作成されます。



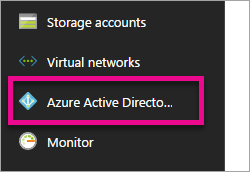
6.ディレクトリの作成が完了したら、情報ボックスを選択して新しいディレクトリを管理します。

ユーザーを作成するには

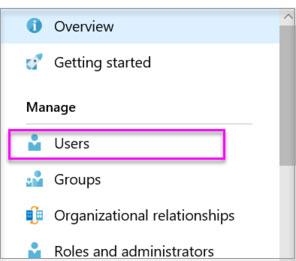
、次の手順を実行します。1。Azureポータルで、Azure ActiveDirectoryフライアウトを使用していることを確認します。



そうでない場合は、左側のサービスナビゲーションからAzure ActiveDirectoryアイコンを選択します。



2. [管理]で、[ユーザー]を選択します。

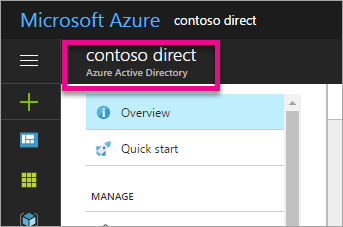


3. [すべてのユーザー]を選択してから、[+新しいユーザー]を選択します。

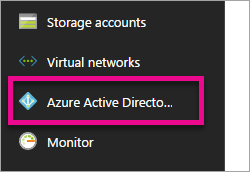
4.ユーザーの名前とユーザー名（user10317806）を入力します。完了したら、[作成]を選択します。

MFAを有効にするには：

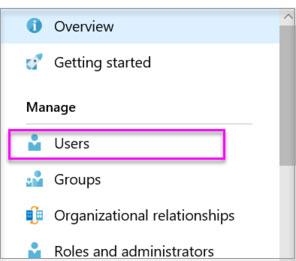
1。Azureポータルで、Azure ActiveDirectoryフライアウトを使用していることを確認します。



そうでない場合は、左側のサービスナビゲーションからAzure ActiveDirectoryアイコンを選択します。



2. [管理]で、[ユーザー]を選択します。



3. [多要素認証]リンクをクリックします。

4.ユーザーの名前の横にあるチェックボックスをオンにして、[有効にする]リンクをクリックします。

参照：

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

# Q.47

contoso.comという名前のAzureActive Directory（Azure AD）テナントと

RG1という名前のリソースグループを含むSubcription1という名前のAzureサブスクリプションがあります。

contoso.comのRole1という名前のカスタムロールを作成します。

権限の委任にRole1を使用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？

1. contoso.comのみ
2. contoso.comとRG1のみ
3. contoso.comとSubscription1のみ
4. contoso.com、RG1、およびSubcription1

正解： D

# Q.48

Azureサブスクリプションがあります。

Azure Active Directory（Azure AD）特権ID管理（PIM）を有効にします。

管理者アカウントに対する会社のセキュリティポリシーには、次の条件

があります。

* アカウントは多要素認証（MFA）を使用する必要があります。
* アカウントは20文字の複雑なパスワードを使用する必要があります。
* パスワードは180日ごとに変更する必要があります。
* アカウントはPIMを使用して管理する必要があります。

過去90日間にパスワードを変更していない管理者に関する複数のアラートを受け取ります。

生成されるアラートの数を最小限に抑える必要があります。

どのPIMアラートを変更する必要がありますか？

1. ロールは特権ID管理の外部で割り当てられています
2. ロールはアクティベーションに多要素認証を必要としません
3. 管理者が特権ロールを使用していない
4. 特権的な役割の潜在的な古いアカウント

正解： D

リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new>

# Q.49

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 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Azure ADの役割を割り当てる必要がありますか？

1. セキュリティ管理者
2. グローバル管理者
3. ユーザー管理者

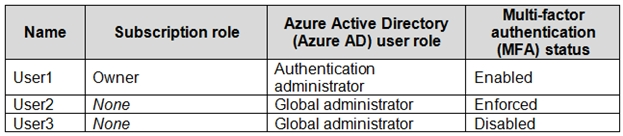
正解： B

リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

# Q.50

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。



どのユーザーが Azure AD 特権ID管理（PIM）を有効にできますか？

1. ユーザー2とユーザー3のみ
2. User1とUser2のみ
3. ユーザー2のみ
4. ユーザー1のみ

正解： D

リファレンス：

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

# Q.51

Azureサブスクリプションがあります。

Azure Storageアカウントを読み取るためのアクセス許可を提供するカスタムのロールベースのアクセス制御（RBAC）ロールを作成することを計画しています。

RBACロール定義のどのプロパティを構成する必要がありますか？

* A. NotActions
* B. DataActions
* C. 割り当て可能なスコープ
* D. アクション

正解： D

「ストレージアカウントを読み取る」、つまり**ストレージアカウントのBLOBを一覧表示するには、Action権限が必要**です。

ストレージアカウントのデータを読み取るため**BLOBを開くには、DataAction権限が必要**です。

参照：

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

# Q.52

Azure Active Directory Premium P1 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。

Azure Active Directory（Azure AD）ID保護を実装することを計画しています。

ユーザーリスクポリシーとサインインリスクポリシーを構成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. すべてのユーザー用にAzure Active Directory Premium P2ライセンスを購入します。
2. すべてのユーザーをAzure Multi-Factor Authentication（MFA）に登録します。
3. Azure ADのセキュリティの既定値を有効にします。
4. Azure Security Centerを標準階層にアップグレードします。

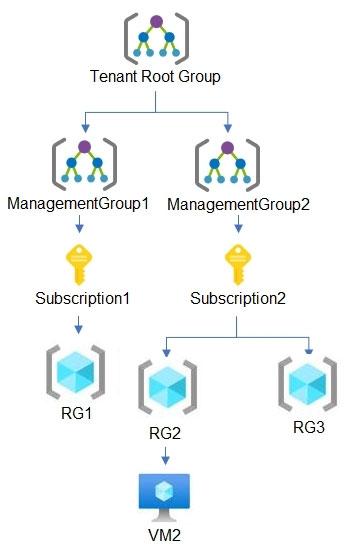
正解： A

リファレンス：

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

# Q.53

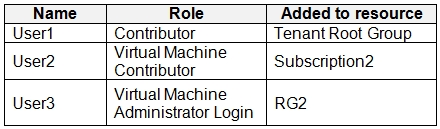
次の展示に示すAzureリソースの階層があります。



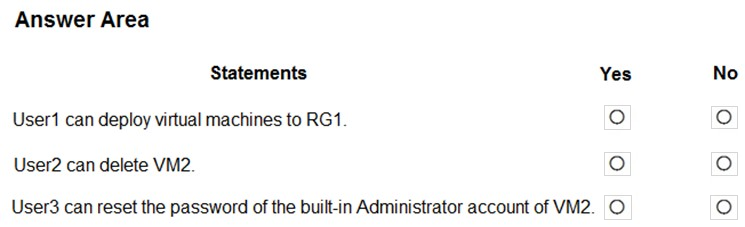
RG1、RG2、およびRG3はリソースグループです。

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。



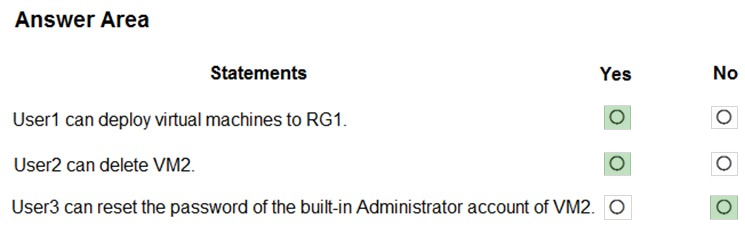
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。



User1は、仮想マシンをRG1にデプロイできます。

User2はVM2を削除できます。

User3は、VM2の組み込みの管理者アカウントのパスワードをリセットできます。

正解： 

# Q.54

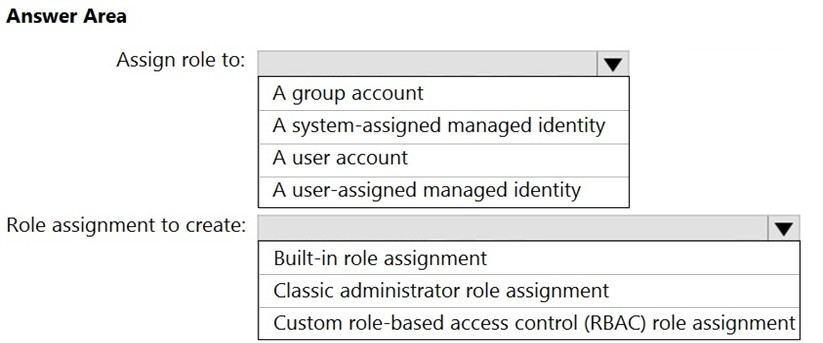
コンテナ化されたアプリケーションインスタンスの新しいストレージアカウントを作成するFunction1という名前のAzure関数を実装することを計画しています。

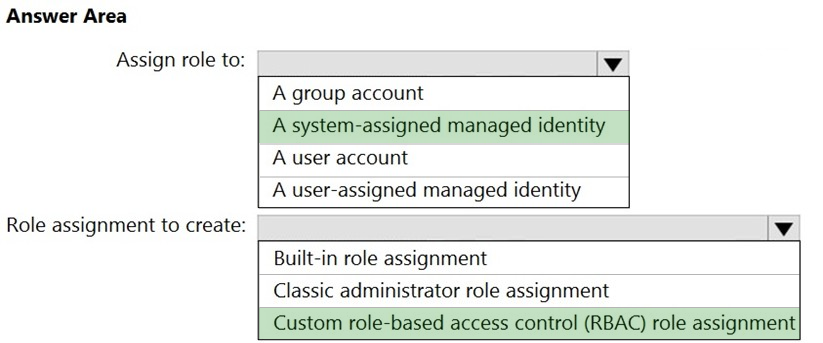
Storageアカウントを作成するには、Function1に最低限必要な権限を付与する必要があります。

この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。



正解： 

参照：

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

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

# Q.55

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？

1. サービスプリンシパル
2. X.509証明書
3. 管理されたID
4. ユーザーアカウント

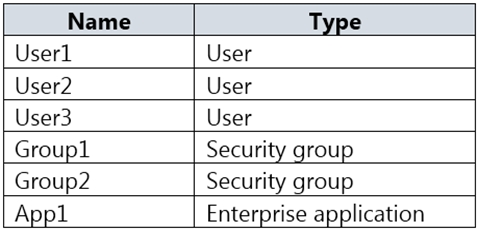
正解： A

リファレンス：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

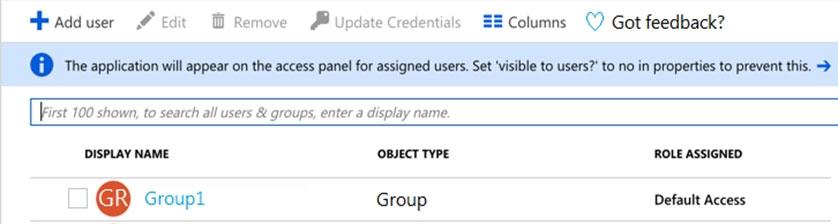
# Q.56

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

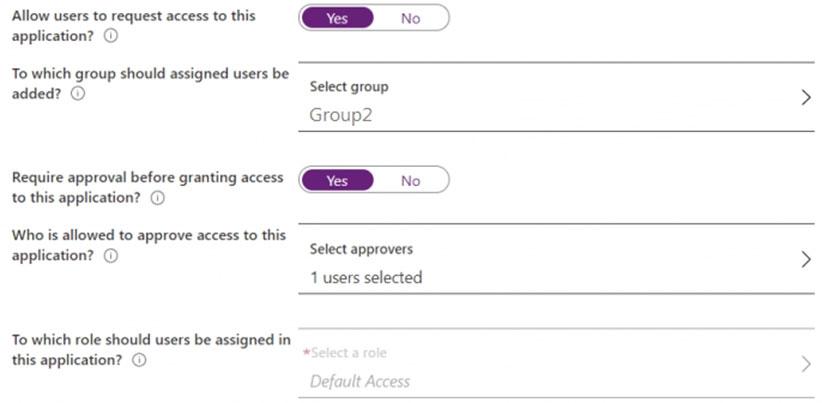


User2はGroup2の所有者です。

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。



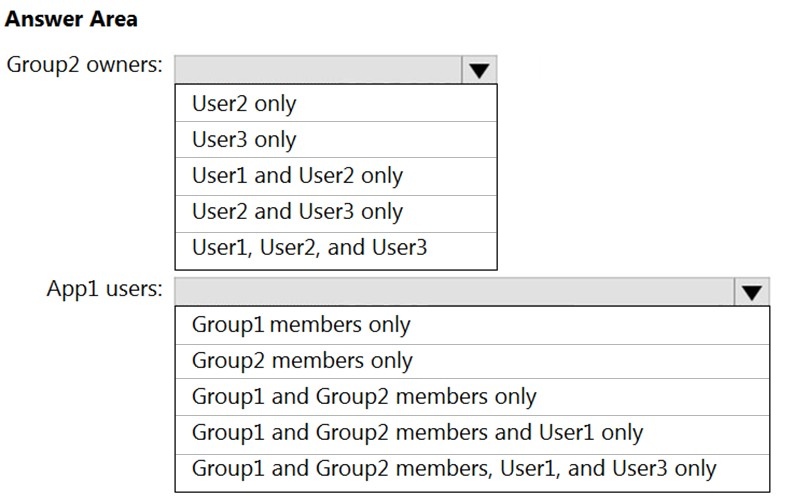
次の展示に示すように、App1のセルフサービスアプリケーションアクセスを有効にします。

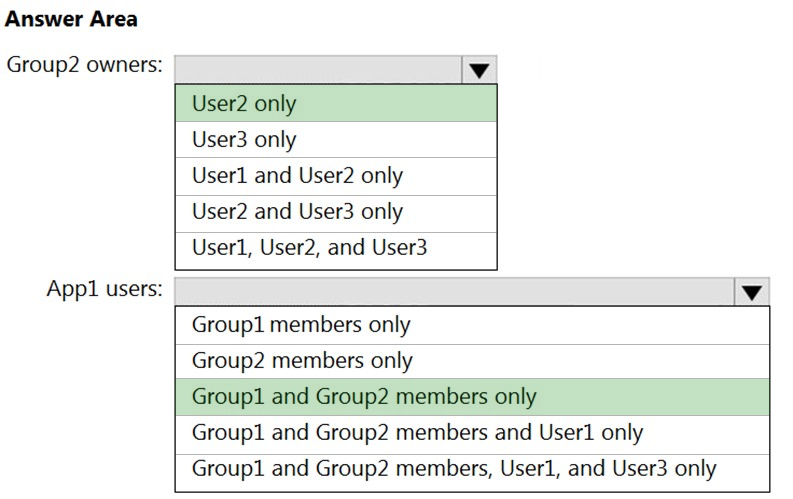


User3は、App1へのアクセスを承認するように構成されています。

Group2の所有者とApp1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、回答領域で適切なオプションを選択します。



正解： 

リファレンス：

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

プラットフォーム保護を実装する