AZ-304 Exam#02

# Q.1

Azure Resource Managerテンプレートを使用するAzureリソースデプロイメントを設計しています。展開では、Azure Key Vaultを使用してシークレットを格納します。次の要件を満たすソリューションを推奨する必要があります。

* 展開を実行するITスタッフがKey Vaultから直接シークレットを取得できないようにします。
* 最小特権の原則を使用します。

どの2つのアクションをお勧めしますか？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. すべてのキーアクセス許可の取得、シークレットアクセス許可の取得、および証明書アクセス許可の取得を許可するKey Vaultアクセスポリシーを作成します。
2. Key Vaultのアクセスポリシーから、テンプレート展開用のAzure Resource Managerへのアクセスを有効にします。
3. すべてのリストキーアクセス許可、リストシークレットアクセス許可、およびリスト証明書アクセス許可を許可するKey Vaultアクセスポリシーを作成します。
4. ITスタッフに、Microsoft.Key Vault / Vaults / Deployment / Action権限を含むカスタムロールを割り当てます。
5. Key Vault Contributorの役割をITスタッフに割り当てます。

正解： *BD*

B：テンプレートの展開中にキーボールトにアクセスするには、キーボールトのenabledForTemplateDeploymentをtrueに設定します。

D：テンプレートを展開するユーザーは、リソースグループとキーボールトのスコープに対するMicrosoft.KeyVault / Vaults / Deploy / action権限を持っている必要があります。

不正解：

E：キーボールトを管理するためのアクセス権をユーザーに付与するには、特定のスコープのユーザーに事前定義されたキーボールトコントリビューターロールを割り当てます。

ユーザーがキーボールト管理プレーンへのコントリビューター権限を持っている場合、ユーザーはキーボールトアクセスポリシーを設定することにより、データプレーンへのアクセスを自分に許可できます。キーボールトへのコントリビューターロールアクセス権を持つユーザーを厳密に制御する必要があります。許可された人だけがキーボールト、キー、シークレット、および証明書にアクセスして管理できるようにします。

参照：

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

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

# Q.2

3つのAzureリージョンのWebアプリを含むAzureサブスクリプションがあります。

次の要件を満たすには、Azure Key Vaultを実装する必要があります。

* 地域が停止した場合は、すべてのキーが読み取り可能である必要があります。
* サブスクリプション内のすべてのWebアプリがKey Vaultにアクセスできる必要があります。
* 展開および管理するKey Vaultリソースの数を最小限に抑える必要があります。

Key Vaultのインスタンスをいくつ実装する必要がありますか？

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

正解： *A*

キーボールトの内容は、リージョン内と、少なくとも150マイル離れた同じ地域内の**セカンダリリージョンに複製されます**。これにより、キーとシークレットの高い耐久性が維持されます。**特定のリージョンペア**の詳細については、Azureペアリージョンのドキュメントを参照してください。

例：ヨーロッパ西部とヨーロッパ北部の両方でアプリケーションが共有する必要のあるシークレット。これらをできるだけ最小限に抑えてください。これらを2つの地域のいずれかの主要な保管庫に入れます。両方のリージョンから同じURIを使用します。**Microsoftは、Key Vaultサービスを内部でフェイルオーバーします。**

参照：

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

# Q.3

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

Azure Storageを使用して、ユーザーに共有ファイルへのアクセスを提供することを計画しています。ユーザーには、ユーザーアカウントまたはグループメンバーシップに基づいて、さまざまなAzureファイル共有へのさまざまなレベルのアクセスが提供されます。

計画された展開をサポートするために、どの追加のAzureサービスを使用する必要があるか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 ADエンタープライズアプリケーション
2. Azureの情報保護
3. Azure ADドメインサービス（Azure AD DS）インスタンス
4. Azureのフロントドアのインスタンス

正解： *C*

Azureファイルは、オンプレミスのActive Directoryドメイン

サービス（AD DS）とAzure Active Directoryドメインサービス（Azure AD DS）の2種類のドメインサービスを通じて、サーバーメッセージブロック（SMB）を介したIDベースの認証をサポートします。）。

参照：

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

# Q.4

あなたの会社には、ラップトップからリモートで作業するユーザーがいます。

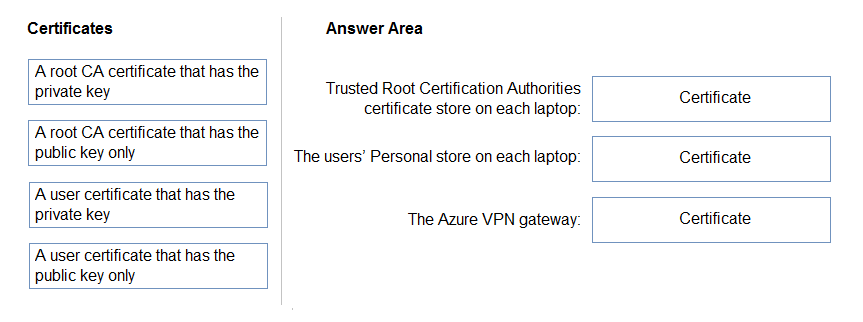
リモートユーザーがアクセスするアプリケーションの一部をAzure仮想マシンに移動することを計画しています。ユーザーは、ポイントツーサイトVPN接続を使用してAzureのアプリケーションにアクセスします。オンプレミスベースの認証局（CA）から生成された証明書を使用します。

展開に必要な証明書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？答えるには、適切な証明書を正しいターゲットにドラッグします。各証明書は、一度でも、複数回でも、まったく使用できません。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注：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：



BOX1: 各ラップトップの信頼されたルート証明機関の証明書ストア

BOX2: 各ラップトップ上のユーザーのパーソナルストア

BOX3: Azure VPN Gateway

BOX1: A root CA certificate that has the public key only.

BOX2: A user certificate that has the private key.

BOX3: A root CA certificate that has the public key only.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-rm-ps#upload>

**試験対策セミナー　テキスト　56ページに同じような問題あり**

# Q.5

仮想マシン（VM）で実行されるアプリケーションを構築しています。アプリケーションはAzure Managed Identityを使用します。

このアプリケーションは、Azure Key Vault、Azure SQL Database、およびAzure Cosmos DBを使用します。

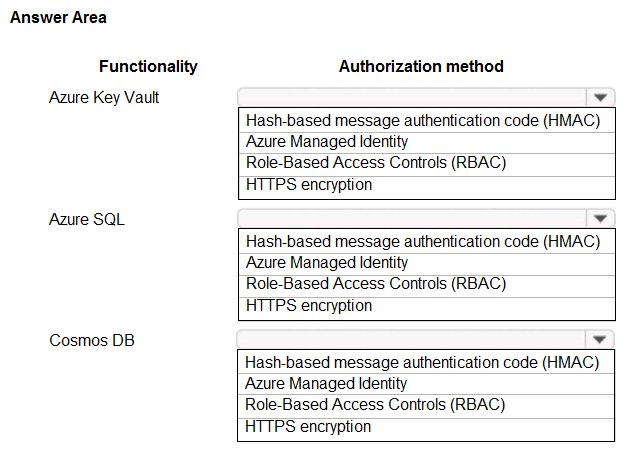
アプリケーションがこれらのサービスにアクセスするために安全な資格情報を使用できることを確認する必要があります。

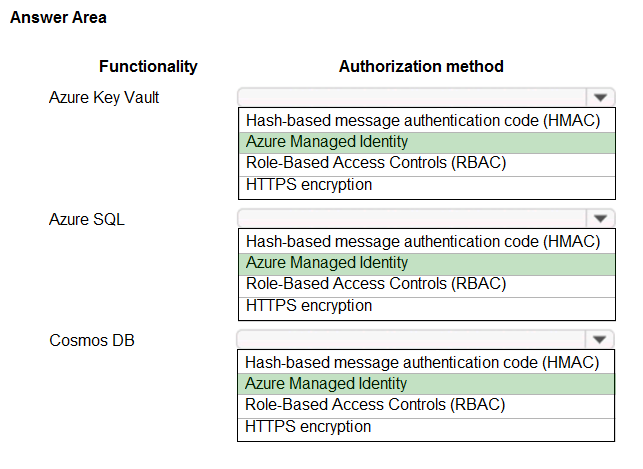
どの認証方法をお勧めしますか？

回答するには、回答領域で適切なオプションを選択します。

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： 

注：AzureリソースのマネージドIDは、以前はマネージドサービスID（MSI）と呼ばれていたサービスの新しい名前です。

参照：

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

# Q.6

Application1という名前のカスタムアプリケーションを含むAzureサブスクリプションがあります。Application1は、Fabrikam、Ltdという名前の外部企業によって開発されました。Fabrikamの開発者には、Application1コンポーネントへのロールベースのアクセス制御（RBAC）アクセス許可が割り当てられました。すべてのユーザーは、Microsoft 365E5プランのライセンスを取得しています。

Fabrikam開発者がまだApplication1へのアクセス許可を必要としているかどうかを確認するためのソリューションを推奨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。

* 開発者のマネージャーに、Application1へのアクセス許可をリストした電子メールメッセージを毎月送信します。
* マネージャーがアクセス許可を確認しない場合は、その許可を自動的に取り消します。
* 開発の労力を最小限に抑えます。

あなたは何をお勧めしますか？

1. 取得-AzureADUserAppRoleAssignmentコマンドレットを実行しますAzureのオートメーションランブックを作成します。
2. 取得-AzRoleAssignmentコマンドレットを実行しますAzureのオートメーションランブックを作成します。
3. Azure Active Directory（Azure AD）で、Application1のアクセスレビューを作成します。
4. Azure Active Directory（AD）特権ID管理で、Application1リソースのカスタムロール割り当てを作成します。

正解：C

<https://docs.microsoft.com/ja-jp/azure/active-directory/governance/manage-user-access-with-access-reviews>

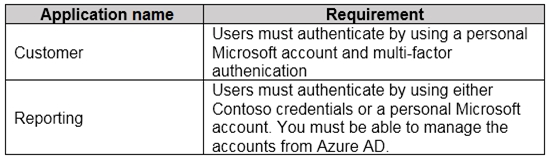
<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews>

# Q.7

Contoso,Ltd.という名前の会社には、基本ライセンスを使用するAzure Active Directory（Azure AD）テナントがあります。

2つのアプリケーションをAzureにデプロイすることを計画しています。

アプリケーションには、次の表に示す要件があります。



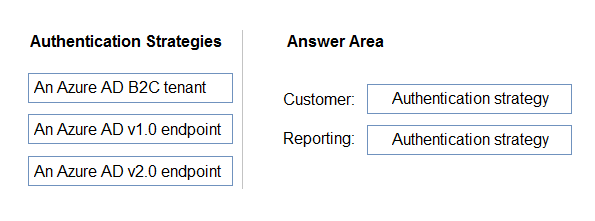
アプリケーションごとにどの認証戦略を推奨する必要がありますか？

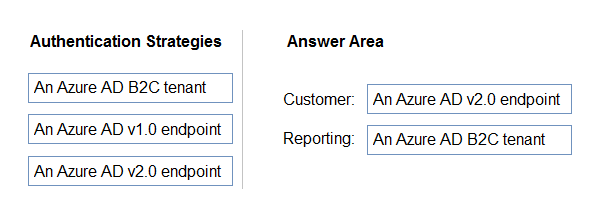
答えるには、適切な認証戦略を正しいアプリケーションにドラッグします。

各認証戦略は、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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注：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： （※参照）

ボックス1：Azure AD V2.0エンドポイント

Microsoft IDプラットフォームは、Azure Active Directory（Azure AD）開発者プラットフォームを進化させたものです。これにより、開発者は、すべてのMicrosoft IDにサインインし、MicrosoftGraphなどのMicrosoftAPIまたは開発者が作成したAPIを呼び出すためのトークンを取得するアプリケーションを構築できます。Microsoft IDプラットフォームは、OAuth2.0とOpenIDConnect標準準拠の認証サービスで構成されており、開発者は次のようなMicrosoft IDを認証できます。職場または学校のアカウント（Azure ADを通じてプロビジョニング）個人のMicrosoftアカウント（Skype、Xbox、Outlookなど） .com）ソーシャルアカウントまたはローカルアカウント（Azure AD B2C経由）

ボックス2：Azure ADB2Cテナント

Azure Active Directory B2Cは、サービスとして企業から顧客へのIDを提供します。顧客は、好みのソーシャル、エンタープライズ、またはローカルアカウントIDを使用して、アプリケーションとAPIへのシングルサインオンアクセスを取得します。Azure Active Directory B2C（Azure AD B2C）は、Azure Multi-Factor Authenticationと直接統合されているため、アプリケーションのサインアップおよびサインインエクスペリエンスにセキュリティの第2層を追加できます。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-mfa>

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

※解答

BOX1: An Azure AD B2C tenant

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/technical-overview>

BOX2: An Azure AD v2.0 endpoint

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

# Q.8

オンプレミスのActive DirectoryドメインとAzure Active Directory（Azure AD）を含むネットワークを管理します。

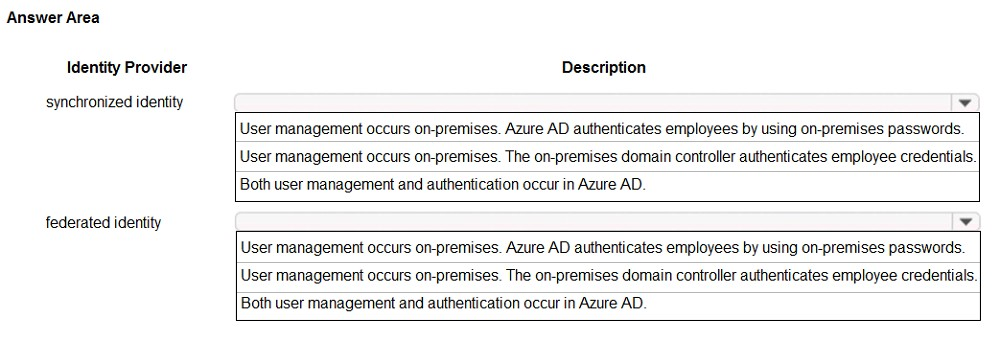
オンプレミスまたはクラウドリソースを使用する場合、従業員は異なるアカウントを使用する必要があります。従業員が単一のアカウントを使用してすべての会社のリソースにサインインできるソリューションを推奨する必要があります。ソリューションはIDプロバイダーを実装する必要があります。

さまざまなIDプロバイダーに関するガイダンスを提供する必要があります。

各IDプロバイダーをどのように説明する必要がありますか？回答するには、回答領域の各リストから適切な説明を選択します。

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：

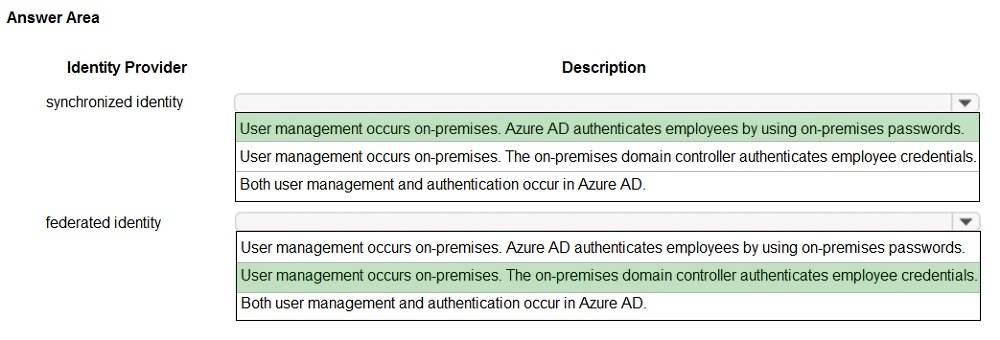


synchronized identity:

1. ユーザー管理はオンプレミスで行われます。 Azure ADは、オンプレミスのパスワードを使用して従業員を認証します。
2. ユーザー管理はオンプレミスで行われます。 オンプレミスのドメインコントローラーは、従業員の資格情報を認証します。
3. ユーザー管理と認証の両方がAzure ADで行われます。

federated identity:

1. ユーザー管理はオンプレミスで行われます。 Azure ADは、オンプレミスのパスワードを使用して従業員を認証します。
2. ユーザー管理はオンプレミスで行われます。 オンプレミスのドメインコントローラーは、従業員の資格情報を認証します。
3. ユーザー管理と認証の両方がAzure ADで行われます。

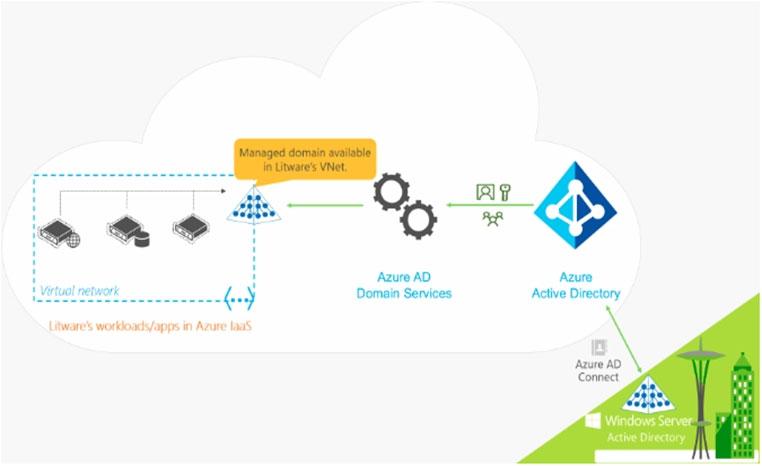
正解： 

ボックス1：ユーザー管理はオンプレミスで行われます。Azure ADは、オンプレミスのパスワードを使用して従業員を認証します。

ハイブリッド組織向けのAzureADドメインサービス

ハイブリッドITインフラストラクチャを使用している組織は、クラウドリソースとオンプレミスリソースを組み合わせて消費します。このような組織は、オンプレミスディレクトリからAzureADテナントにID情報を同期します。ハイブリッド組織は、より多くのオンプレミスアプリケーション、特にレガシーディレクトリ対応アプリケーションをクラウドに移行しようとしているため、AzureADドメインサービスが役立つ可能性があります。

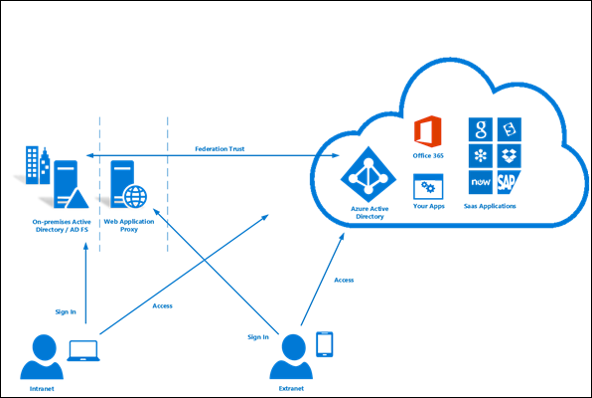
例：Litware Corporationは、オンプレミスディレクトリからAzure ADテナントにID情報を同期するために、Azure ADConnectを展開しました。同期されるID情報には、ユーザーアカウント、認証用の資格情報ハッシュ（パスワードハッシュ同期）、およびグループメンバーシップが含まれます。



Litwareのオンプレミスディレクトリのユーザーアカウント、グループメンバーシップ、および資格情報は、Azure ADConnectを介してAzureADに同期されます。これらのユーザーアカウント、グループメンバーシップ、および資格情報は、管理対象ドメイン内で自動的に使用可能になります。

ボックス2：ユーザー管理はオンプレミスで行われます。オンプロミスのドメインコントローラーは、従業員の資格情報を認証します。

オンプレミス環境をAzureADとフェデレーションし、このフェデレーションを認証と承認に使用できます。このサインイン方法により、すべてのユーザー認証がオンプレミスで確実に行われます。



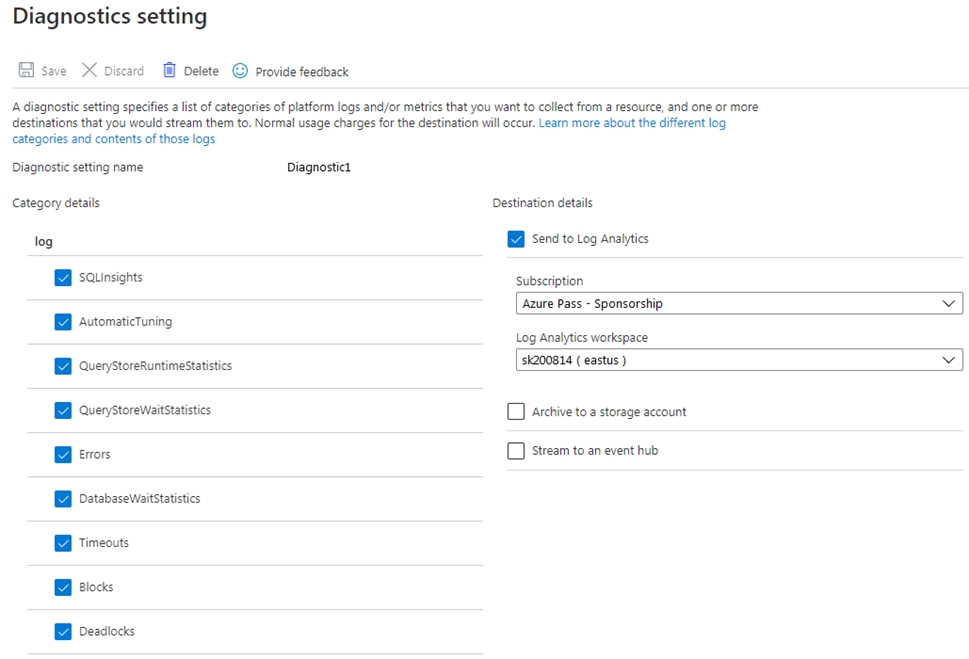
参照：

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

# Q.9

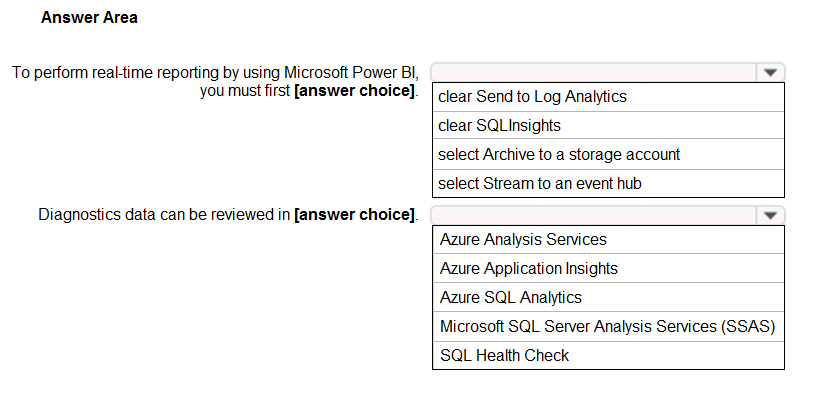
次の展示に示すように、AzureSQLデータベースの診断設定を構成します。

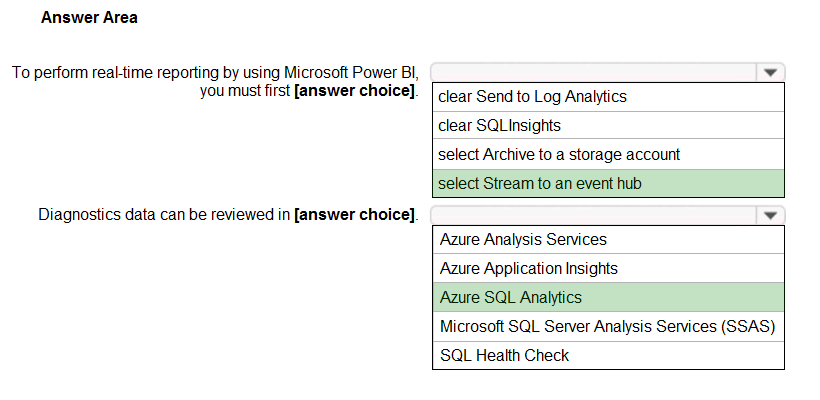


ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



正解： 

# Q.10

5台のAzure仮想マシンで実行されるApp1という名前のアプリケーションをデプロイすることを計画しています。追加の仮想マシンは、App1を実行するために後でデプロイされます。

App1を実行する仮想マシンの次の要件を満たすソリューションを推奨する必要があります。

* 仮想マシンがAzure Active Directory（Azure AD）に対して認証され、Azureキーボールト、Azure Logic Appsインスタンスにアクセスできることを確認します。およびAzure SQLデータベース。
* 追加の仮想マシンをデプロイするときは、Azureサービスに新しい役割とアクセス許可を割り当てないでください。
* 仮想マシンにシークレットと証明書を保存しないでください。
* IDを管理するための管理作業を最小限に抑えます。

どのタイプのIDを推奨に含める必要がありますか？

1. 証明書を使用するように構成されたサービスプリンシパル
2. システムによって割り当てられたマネージID
3. クライアントシークレットを使用するように構成されたサービスプリンシパル
4. ユーザーが割り当てたマネージID

正解： *D*

AzureリソースのマネージIDは、Azure ActiveDirectoryの機能です。

ユーザーが割り当てた管理IDを共有できます。同じユーザーが割り当てたマネージIDを複数のAzureリソースに関連付けることができます。

不正解：

B：システムによって割り当てられた管理対象IDを共有できません。単一のAzureリソースにのみ関連付けることができます。

参照：

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

# Q.11

多くのサブスクリプションを含む大規模なAzure環境を設計しています。

ガバナンスソリューションの一部としてAzureポリシーを使用することを計画しています。

Azureポリシー定義を割り当てることができる3つのスコープはどれですか？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. 管理グループ
2. サブスクリプション
3. Azure Active Directory（Azure AD）テナント
4. リソースグループ
5. Azure Active Directory（Azure AD）管理ユニット
6. コンピューティングリソース

正解： *ABD*

Azureポリシーは、Azureのリソースのプロパティをビジネスルールと比較することにより、それらのリソースを評価します。ビジネスルールが形成されると、ポリシー定義またはイニシアチブは、管理グループ、サブスクリプション、リソースグループ、個々のリソースなど、Azureがサポートするリソースの任意のスコープに割り当てられます。

参照：

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

# Q.12

Azure Kubernetes Service（AKS）クラスターでホストされるマイクロサービスアーキテクチャを設計しています。マイクロサービスを使用するアプリは、Azure仮想マシンでホストされます。仮想マシンとAKSクラスターは同じ仮想ネットワーク上に存在します。マイクロサービスをコンシューマーアプリに公開する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。

* マイクロサービスへの入力アクセスは、単一のプライベートIPアドレスに制限し、相互TLS認証を使用して保護する必要があります。
* 着信マイクロサービス呼び出しの数はレート制限されている必要があります。
* コスト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 Web Application Firewall（WAF）を備えたAzure App Gateway
2. 仮想ネットワーク接続を備えたAzure API Management Premium層
3. サービスエンドポイントを備えたAzureAPI管理標準層
4. Azure Web Application Firewall（WAF）を備えたAzureフロントドア

正解： *B*

1つのオプションは、クラスターVNet内にAPIM（API管理）をデプロイすることです。AKSクラスターとマイクロサービスを使用するアプリケーションは同じVNet内に存在する可能性があるため、すべてのAPIトラフィックはVNet内にとどまるため、クラスターを公開する理由はありません。

これらのシナリオでは、APIManagementをクラスターVNetにデプロイできます。API Management Premium層は、VNetデプロイメントをサポートします。

参照：

<https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes>

<https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes#option-2-install-an-ingress-controller>

仮想ネットワークへのAzureAPI Managementのデプロイは、API Managementのプレミアム層と開発者層でのみ使用できます。<https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet>

D.WAFを備えたAzure Front Door

* 要件:3）コストを最小限に抑える必要があることを考慮します。WAFを備えたFront Doorはより良いオプションです。Azure Front Doorはロードバランサーであり、そこでマイクロサービスをホストできないためです。マイクロサービスはAPIであるため、マイクロサービスをホストするにはAPI管理が必要です。

A. Azure Web Application Firewall（WAF）を備えたAzure App Gateway

* AppGatewayはレート制限をサポートしていません

B.仮想ネットワーク接続を備えたAzureAPI ManagementPremium層

* 1時間あたり3.83ドルかかります

C.Azure APIManagement標準層サービスエンドポイントあり

* 開発者およびプレミアム層でのみサポートされるレート制限

D.Azure Web Application Firewall（WAF）を備えたAzureフロントドア

* 月額$ 5〜 $ 20

# Q.13

ある会社は、WebアプリをサポートするためにHTTPベースのAPIを実装することを計画しています。Webアプリを使用すると、顧客は注文のステータスを確認できます。

APIは、次の要件を満たしている必要があります。

* Azure関数を実装します。
* パブリックな読み取り専用操作を提供します。
* 書き込み操作を許可しないでください。

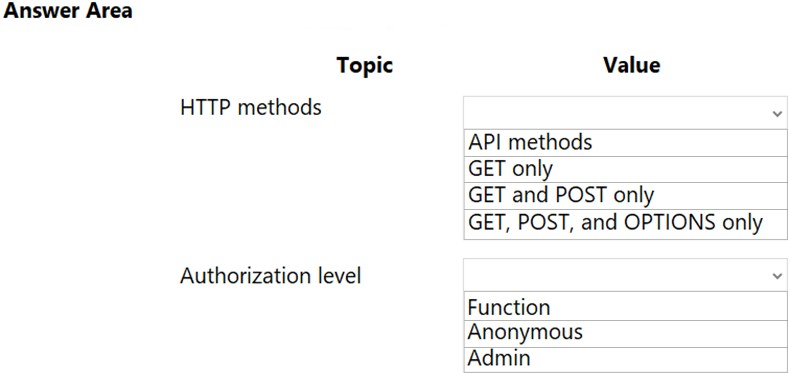
構成オプションを推奨する必要があります。

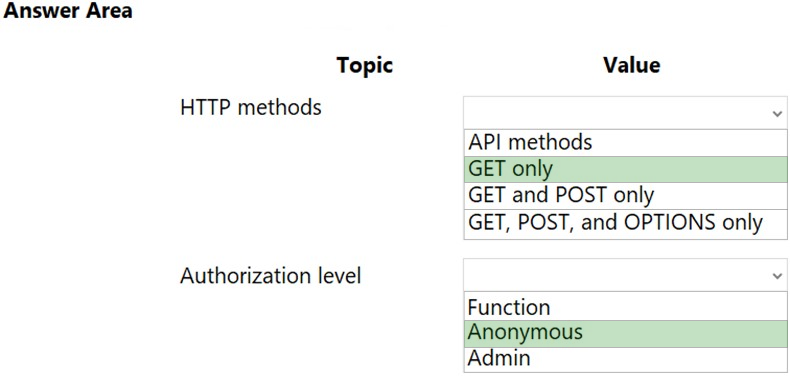
あなたは何をお勧めしますか？

回答するには、回答領域のダイアログボックスで適切なオプションを構成します。

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： 

HTTPメソッド：GETのみ

承認レベル：匿名

オプションは[匿名リクエストを許可する]です。このオプションは、App Serviceで認証と承認をオンにしますが、承認の決定はアプリケーションコードに委ねられます。認証されたリクエストの場合、AppServiceはHTTPヘッダーの認証情報も渡します。

このオプションにより、匿名リクエストの処理がより柔軟になります。

参照：

<https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>

**試験対策セミナー　テキスト　49ページ　同じような問題あり。**

# Q.14

Contoso Ltd.という名前の会社には、contoso.comという名前の単一ドメインのActive Directoryフォレストがあります。Contosoは、すべてのワークロードをAzureに移行する準備をしています。Contosoは、ユーザーがAzure Active Directory（Azure AD）と統合するクラウドベースのサービスにアクセスするときにシングルサインオン（SSO）を使用することを望んでいます。フォーマットの問題が原因でAzure ADとの同期に失敗するActive Directory内のオブジェクトを特定する必要があります。ソリューションはコストを最小限に抑える必要があります。

ソリューションに何を含める必要がありますか？

1. Azure AD Connect Health
2. Microsoft Office 365 IdFix
3. Azure Advisor
4. Active Directory移行ツール（ADMT）のパスワードエクスポートサーバーバージョン3.1（PES v3.1）

正解：B

<https://github.com/Microsoft/idfix>

**試験対策セミナー　テキスト**

* **65ページ**
* **97ページに同じような問題あり**

# Q.15

会社には、Azureの仮想マシン（VM）で実行される既存のWebアプリケーションがあります。アプリケーションがSQLインジェクションの試行から保護され、レイヤー7ロードバランサーを使用していることを確認する必要があります。

このソリューションでは、既存のWebアプリケーションのコードの中断を最小限に抑える必要があります。

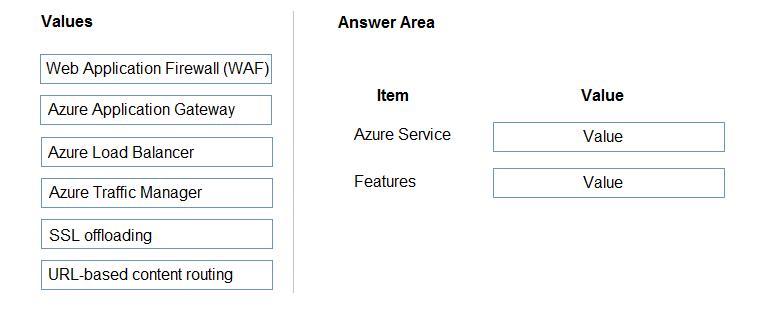
あなたは何をお勧めしますか？

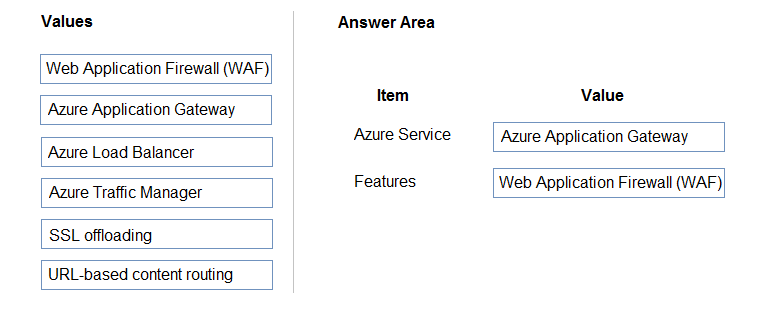
答えるには、適切な値を正しい項目にドラッグします。

各値は、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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注：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： 

ボックス1：Azure Application Gateway

Azure Application Gatewayは、サービスとしてアプリケーション配信コントローラー（ADC）を提供します。アプリケーションにさまざまなレイヤー7負荷分散機能を提供します。

ボックス2：Webアプリケーションファイアウォール（WAF）

アプリケーションゲートウェイWebアプリケーションファイアウォール（WAF）は、一般的な脆弱性やエクスプロイトからWebアプリケーションを保護します。

これは、OWASPコアルールセット3.0または2.2.9に基づいて定義されたルールを介して行われます。SQLインジェクション攻撃を検出するルールがあります。

参照：

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

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

ssl-offloadingはhttps要求を管理する

Layer7 ロードバランサー

* Azure Application Gateway
* Azure Front Door

Layer4 ロードバランサー

* Azure Load Balancer

DNSで機能する

* Azure Traffic Manager

**試験対策セミナーテキスト　39ページ**

# Q.16

Azureサブスクリプションがあります。サブスクリプションには、複数のBLOBを含むBLOBコンテナーがあります。あなたの会社の財務部門の10人のユーザーが、4月中にblobにアクセスすることを計画しています。4月のみブロブへのアクセスを有効にするソリューションを推奨する必要があります。

どのセキュリティソリューションを推奨に含める必要がありますか？

1. アクセスキー
2. 条件付きアクセスポリシー
3. 証明書
4. 共有アクセス署名（SAS）

正解： *D*

リファレンス：

<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>

**試験対策セミナー　テキスト　151ページに同じような問題**

# Q.17

Azure Active Directory（Azure AD）認証を使用するApp1という名前のAzure Webアプリを展開することを計画しています。

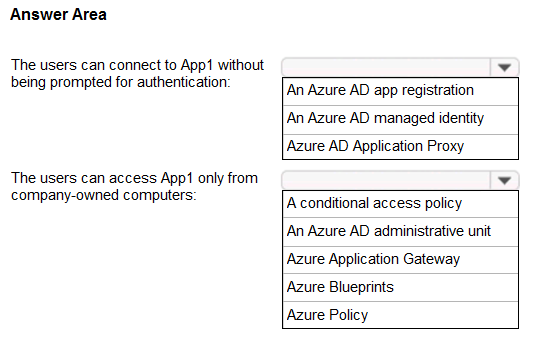
App1には、会社のユーザーがインターネットからアクセスします。すべてのユーザーは、Windows 10を実行し、Azure ADに参加しているコンピューターを持っています。

ユーザーが認証を求められることなくApp1に接続でき、会社所有のコンピューターからのみApp1にアクセスできる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。

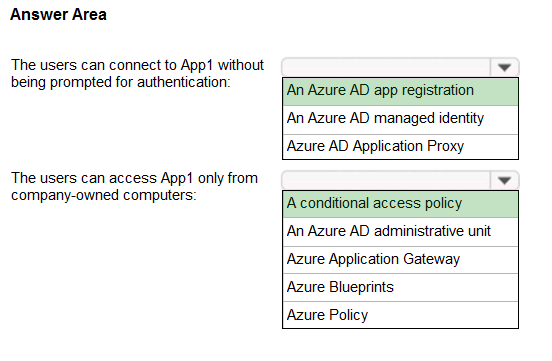
要件ごとに何をお勧めしますか？

回答するには、回答領域で適切なオプションを選択します。

ホットエリア：



1. ユーザーは、認証を求められることなくApp1に接続できます。
2. ユーザーは、会社所有のコンピューターからのみApp1にアクセスできます。

正解： 

ボックス1：Azure ADアプリの登録

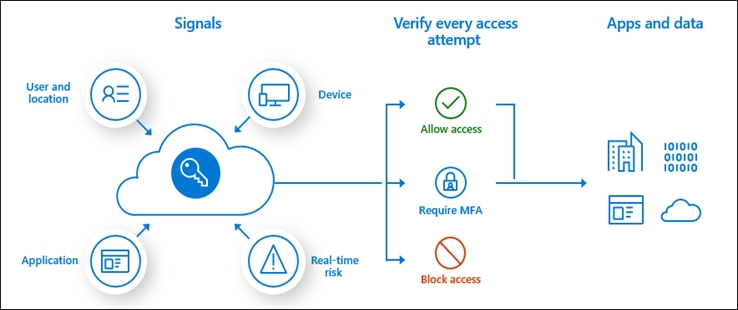
Azure Active Directory（AD）は、クラウドベースのディレクトリおよびID管理サービスを提供します。azureADを使用して、アプリケーションのユーザーを管理し、azure ActiveDirectoryを使用してアプリケーションへのアクセスを認証できます。

アプリケーションをAzureActiveDirectoryテナントに登録します。

ボックス2：条件付きアクセスポリシー

最も単純な条件付きアクセスポリシーはif-thenステートメントであり、ユーザーがリソースにアクセスしたい場合は、アクションを完了する必要があります。

条件付きアクセスポリシーを使用すると、必要に応じて適切なアクセス制御を適用して、組織を安全に保ち、不要なときにユーザーの邪魔にならないようにすることができます。



参照：

<https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/>

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

# Q.18

ルート管理グループと10個の子管理グループを含むAzure環境を作成することを計画しています。各子管理グループには、5つのAzureサブスクリプションが含まれます。各サブスクリプションに10から30のリソースグループを含めることを計画しています。

Azureガバナンス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。

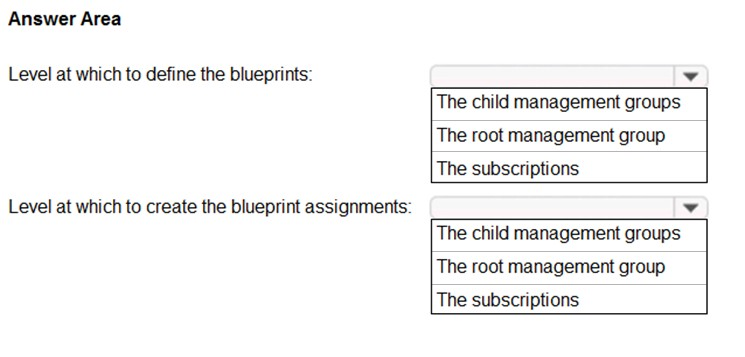
* Azureブループリントを使用して、すべてのサブスクリプションとリソースグループのガバナンスを制御します。
* ブループリントベースの構成がすべてのサブスクリプションとリソースグループで一貫していることを確認します。
* ブループリントの定義と割り当ての数を最小限に抑えます。

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。

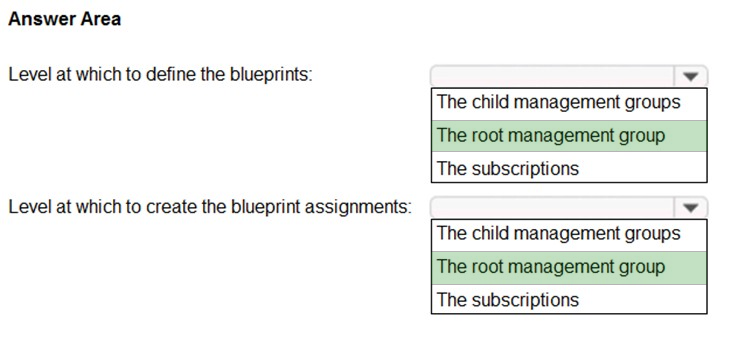
注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



ブループリントをどこに定義しますか？

ブループリントをどこに割り当てますか？

正解： 

ボックス1：ルート管理グループ

ブループリント定義を作成するときに、ブループリントを保存する場所を定義します。ブループリントは、コントリビューターがアクセスできる管理グループまたはサブスクリプションに保存できます。場所が管理グループの場合、ブループリントを使用して、その管理グループの子サブスクリプションに割り当てることができます。

ボックス2：ルート管理グループ　**※次ページ参照**

各ディレクトリには、「ルート」管理グループと呼ばれる単一の最上位管理グループが与えられます。このルート管理グループは階層に組み込まれており、すべての管理グループとサブスクリプションが階層に組み込まれます。このルート管理グループを使用すると、グローバルポリシーとAzureロールの割り当てをディレクトリレベルで適用できます。

ブループリントの各公開バージョンは、既存の管理グループまたはサブスクリプションに割り当てることができます。

参照：

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

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

解答　ボックス2：ルート管理グループは間違っていると考える。

ブループリントの割り当ては、**サブスクリプションレベル**になる。

ブループリント定義を作成するときに、ブループリントを**保存する場所**を定義します。

ブループリントは、コントリビューターがアクセスできる管理グループまたはサブスクリプションに**保存**できます。

場所が管理グループの場合、ブループリントを使用して、その**管理グループの子サブスクリプションに割り当てる**ことができます。

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

ブループリントの各公開 バージョンは、既存の管理グループまたはサブスクリプションに割り当てることができます（最大名の長さは90文字）。ポータルでは、ブループリントのデフォルトのバージョンは、最後に公開されたものになります。アーティファクトパラメータまたはブループリントパラメータがある場合、パラメータは割り当てプロセス中に定義されます。

注意

ブループリント定義を管理グループに割り当てるということは、割り当てオブジェクトが管理グループに存在することを意味します。アーティファクトのデプロイメントは、引き続きサブスクリプションを対象としています。管理グループの割り当てを実行するには、 REST APIの作成または更新を使用する必要があり、リクエストの本文properties.scopeには、ターゲットサブスクリプションを定義するための値を含める必要があります。

# Q.19

Azureサブスクリプションがあります。

開発者にAzure仮想マシンをプロビジョニングする機能を提供するソリューションを推奨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。

* 特定のリージョンでの仮想マシンの作成のみを許可します。
* 特定のサイズの仮想マシンの作成のみを許可します。

推奨事項には何を含める必要がありますか？

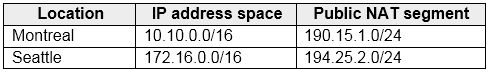
1. Azure Resource Managerテンプレート
2. Azure Policy
3. 条件付きアクセスポリシー
4. 役割ベースのアクセス制御（RBAC）

正解：B

**試験対策セミナー　テキスト　105ページに同じような問題あり**

# Q.20

あなたの会社には、次の表に示すオフィスがあります。



ネットワークには、Azure Active Directory（Azure AD）に同期されるcontoso.comという名前のActive Directoryドメインが含まれています。

すべてのユーザーがExchangeOnlineに接続します。

すべてのユーザーがAzure Multi-Factor Authentication（MFA）を使用して、いずれかのオフィスからExchangeOnlineに接続できるようにする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. 仮想ネットワークと2つのMicrosoft Cloud AppSecurity ポリシー
2. 名前付きの場所と2つのMicrosoft Cloud AppSecurity ポリシー
3. 条件付きアクセスポリシーと2つの仮想ネットワーク
4. 条件付きアクセスポリシーと2つの名前付きロケーション

正解： *D*

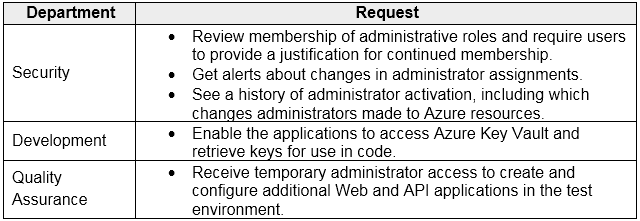
限定受信ポリシーは、最も基本的なif-thenステートメントであり、シグナルを組み合わせて、意思決定を行い、組織のポリシーを実施します。意思決定プロセスに組み込むことができる信号の1つは、ネットワークの場所です。

参照：

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

# Q.21

組織は、いくつかのAzure App Service WebおよびAPIアプリケーションを開発およびデプロイしています。アプリケーションはAzure Key Vaultを使用して、いくつかの認証、ストレージアカウント、およびデータ暗号化キーを格納します。いくつかの部門には、アプリケーションをサポートするために次のリクエストがあります。



各部門のリクエストに適切なAzureサービス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？

回答するには、回答領域のダイアログボックスで適切なオプションを構成します。

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：

Security:

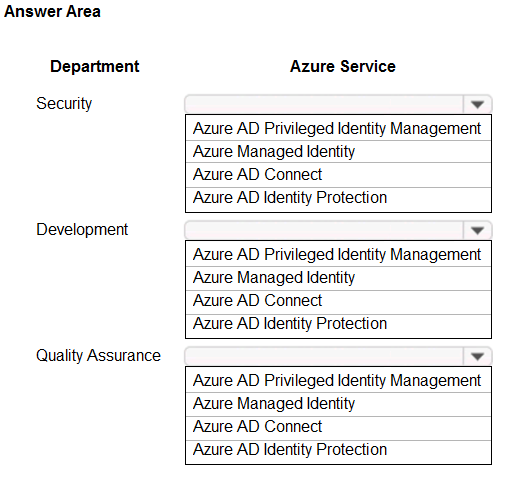
* 管理者の役割のメンバーシップを確認し、継続的なメンバーシップの正当性をユーザーに提供するように要求します。
* 管理者の割り当ての変更に関するアラートを取得します。
* 管理者がAzureリソースに加えた変更など、管理者のアクティブ化の履歴を確認します。

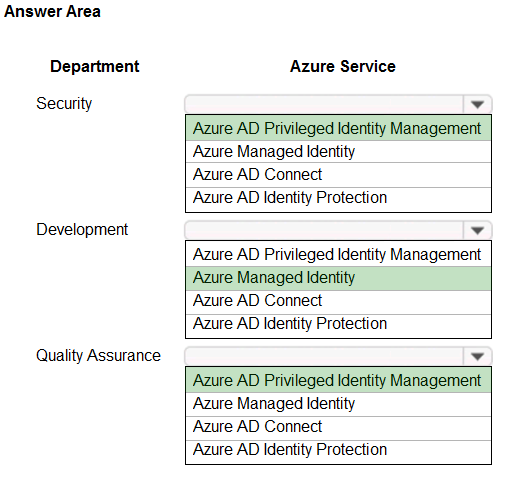
Development:

* アプリケーションがAzure Key Vaultにアクセスし、コードで使用するキーを取得できるようにします。

Quality Assurance:

* テスト環境で追加のWebおよびAPIアプリケーションを作成および構成するための一時的な管理者アクセスを受け取ります。



正解： 

アクセスレビューをカバーするのはID保護ではなく、Azure AD IdentityGovernanceです。

AzureADおよびAzureリソースへのジャストインタイムの特権アクセスを提供する

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

# Q.22

ネットワークには、オンプレミスのActive Directoryフォレストが含まれています。

ユーザーが社内で転職しても、ユーザーグループのメンバーシップが更新されていないことがわかりました。その結果、ユーザーは自分の仕事に関係のなくなったリソースにアクセスできます。

Azure AD Connectを使用して、Active DirectoryとAzure Active Directory（Azure AD）を統合することを計画しています。

グループの所有者が管理するグループメンバーシップについて毎月メールで送信される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 AD Identity Protection
2. AzureADアクセスレビュー
3. テナントの制限
4. 条件付きアクセスポリシー

正解： *B*

リファレンス：

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

# Q.23

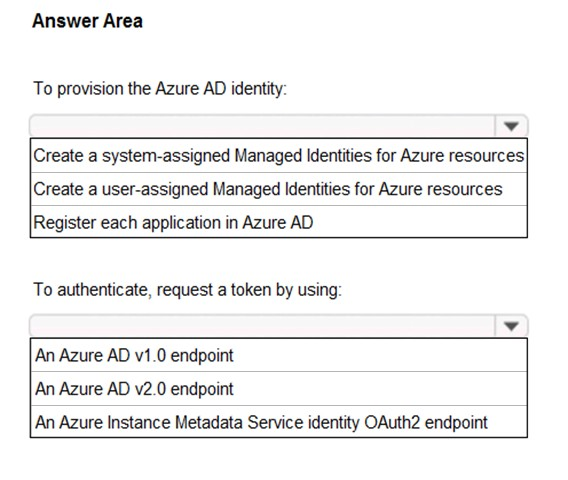
同じサブスクリプション内の10台のAzure仮想マシンで実行される5つの.NETCoreアプリケーションがあります。

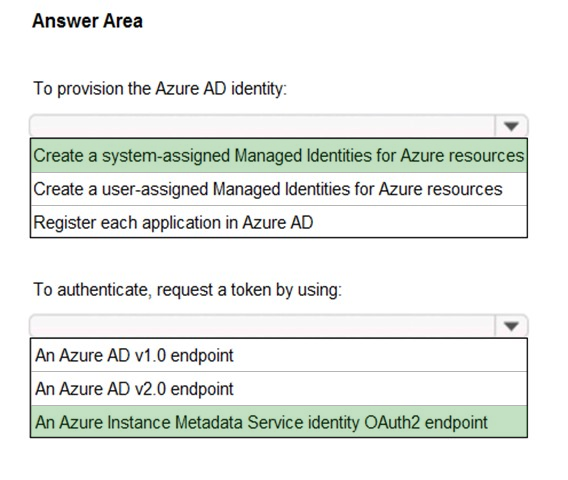
同じAzure Active Directory（Azure AD）IDを使用してアプリケーションを認証できるようにするためのソリューションを推奨する必要があります。このソリューションは、次の要件を満たしている必要があります。

* アプリケーションが10台の仮想マシンで実行されている場合にのみ認証できることを確認します。
* 管理作業を最小限に抑えます。

推奨事項には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。

ホットエリア：



正解： **次のページの※を参照**

ボックス1：Azureリソースのシステム割り当ての管理IDを作成する

Azure Active Directory（Azure AD）機能のAzureリソースの管理ID機能は、AzureサービスにAzureADの自動管理IDを提供します。IDを使用して、コードにクレデンシャルがなくても、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。

システムによって割り当てられたマネージIDは、Azureサービスインスタンスで直接有効になります。IDが有効になっている場合、Azureは、インスタンスのサブスクリプションによって信頼されているAzureADテナント内のインスタンスのIDを作成します。IDが作成された後、資格情報がインスタンスにプロビジョニングされます。

ボックス2：AzureインスタンスメタデータサービスID

以下の手順3と5を参照してください。

システムによって割り当てられたマネージIDがAzureVMでどのように機能するか

1. Azure Resource Managerは、VMでシステムによって割り当てられたマネージIDを有効にする要求を受け取ります。
2. Azure Resource Managerは、VMのID用にAzureADにサービスプリンシパルを作成します。サービスプリンシパルは、サブスクリプションによって信頼されているAzureADテナントで作成されます。
3. Azure Resource Managerは、AzureインスタンスメタデータサービスのIDエンドポイントをサービスプリンシパルクライアントIDと証明書で更新することにより、VM上のIDを構成します。
4. VMがIDを取得したら、サービスプリンシパル情報を使用して、VMにAzureリソースへのアクセスを許可します。Azure Resource Managerを呼び出すには、Azure ADでロールベースのアクセス制御（RBAC）を使用して、VMサービスプリンシパルに適切なロールを割り当てます。Key Vaultを呼び出すには、KeyVaultの特定のシークレットまたはキーへのアクセスをコードに許可します。
5. VMで実行されているコードは、Azureインスタンスメタデータサービスエンドポイントからトークンを要求できます。トークンには、VMリファレンス内からのみアクセスできます：

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

**※**

* アプリケーションが同じAzureActive Directory（Azure AD）IDを使用して認証できることを確認します。
* 10台の仮想マシンで実行している場合にのみアプリケーションが認証できることを確認します。
* 管理作業を最小限に抑えます。

これに対処するには：

* 最初の質問はユーザーが割り当てる必要があります。そうしないと、10個の異なるIDが必要になります。また、管理作業を最小限に抑えます。
* 2番目はOAUTH2エンドポイントである必要があります。そうすると、VM内からのみトークンを取得できるため、2番目のステートメントが真になります。

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

ユーザー割り当てスタンドアロンのAzureリソースとしてマネージドIDを作成することもできます。ユーザーが割り当てたマネージIDを作成し、それをAzureサービスの1つ以上のインスタンスに割り当てることができます。ユーザーが割り当てた管理対象IDの場合、IDはそれを使用するリソースとは別に管理されます。

よって

**最初の質問の回答は：Create a user-assigned Managed Identities for Azure resources**

# Q.24

Admin1とAdmin2という名前の2つの管理ユーザーアカウントを含むcontoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。

VM1とVM2という名前の2つのAzure仮想マシンを作成します。

120秒間にVM1またはVM2のセキュリティログに5つを超えるイベントが追加されたときに、Admin1とAdmin2に通知されるようにする必要があります。

ソリューションは、管理タスクを最小限に抑える必要があります。

何を作成する必要がありますか？

1. 2 つのアクショングループと2つのアラートルール
2. 1 つのアクショングループと1つのアラートルール
3. 5 つのアクショングループと1つのアラートルール
4. 2 つのアクショングループと1つのアラートルール

解答：B

アラートルールには、複数のVMをターゲットとして含めることができます。

Azureのドキュメントでも言及されています：<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview>

以下はアラートルールの主要な属性です。

ターゲットリソース

* スコープとシグナルを定義します。
* アラートに利用できます。
* ターゲットは任意のAzureリソースにすることができます。

ターゲットの例：

* 仮想マシン
* ストレージアカウント
* Log Analytics ワークスペース
* アプリケーションインサイト

特定のリソース（仮想マシンなど）の場合、アラートルールのターゲットとして複数のリソースを指定できます。また、別のAzureドキュメントによると、さまざまなアラートで、ユーザーの要件に応じて同じアクショングループまたは異なるアクショングループが使用される場合があります。

要約すると、必要なのは1つのアラートルールと1つのアクショングループだけなので、オプションBは正しいようです。

# Q.25

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。

contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。テナントには、Group1という名前のグループが含まれています。Group1には、すべての管理ユーザーアカウントが含まれています。管理ユーザーが機能していない国から、Azureポータルへのログイン試行が数回行われていることがわかりました。これらの国からAzureポータルへのすべてのログイン試行にAzureMulti-Factor Authentication（MFA）が必要であることを確認する必要があります。

解決策：Group1のアクセスレビューを作成します。

このソリューション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 AD 特権 ID 管理を実装します。

注：Azure Active Directory（Azure AD）特権ID管理（PIM）は、組織内の重要なリソースへのアクセスを管理、制御、および監視できるようにするサービスです。

参照：

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

# Q.26

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。

contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。テナントには、Group1という名前のグループが含まれています。Group1には、すべての管理ユーザーアカウントが含まれています。管理ユーザーが機能していない国から、Azureポータルへのログイン試行が数回行われていることがわかりました。これらの国からAzureポータルへのすべてのログイン試行にAzureMulti-Factor Authentication（MFA）が必要であることを確認する必要があります。

解決策：Group1にAzure AD IdentityProtectionを実装します。

このソリューション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、AzureAD特権ID管理を実装します。

注：Azure Active Directory（Azure AD）特権ID管理（PIM）は、組織内の重要なリソースへのアクセスを管理、制御、および監視できるようにするサービスです。

参照：

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

# Q.27

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。

contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。テナントには、Group1という名前のグループが含まれています。Group1には、すべての管理ユーザーアカウントが含まれています。管理ユーザーが機能していない国から、Azureポータルへのログイン試行が数回行われていることがわかりました。これらの国からAzureポータルへのすべてのログイン試行にAzureMulti-Factor Authentication（MFA）が必要であることを確認する必要があります。

解決策：アクセスパッケージを実装します。

これは目標を達成していますか？

* A. はい
* B. いいえ

正解： *B*

代わりに、AzureAD特権ID管理を実装します。

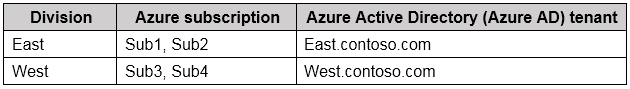
注：Azure Active Directory（Azure AD）特権ID管理（PIM）は、組織内の重要なリソースへのアクセスを管理、制御、および監視できるようにするサービスです。

参照：

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

# Q.28

あなたの会社には次の表に示す部門があります。



各サブスクリプションにカスタムアプリケーションをデプロイすることを計画しています。アプリケーションには次のものが含まれます。

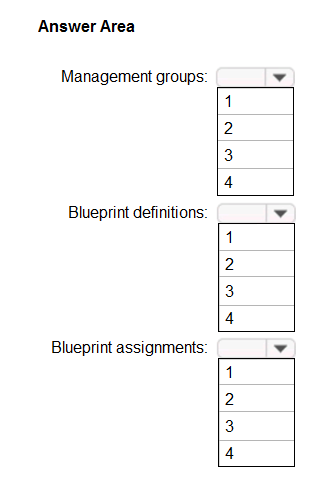
* リソースグループ
* Azure Web アプリ
* カスタムロールの割り当て
* Azure Cosmos DBアカウント

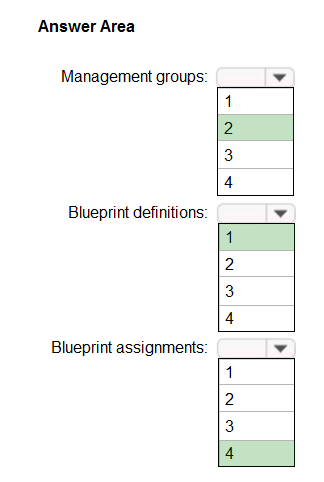
アプリケーションを各サブスクリプションにデプロイするには、Azureブループリントを使用する必要があります。

アプリケーションをデプロイするために必要なオブジェクトの最小数はいくつですか？回答するには、回答領域で適切なオプションを選択します。

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1：2

東用に1つ、西用に1つの管理グループ。

ブループリント定義を作成するときは、ブループリントを保存する場所を定義します。ブループリントは、

コントリビューターがアクセスできる管理グループまたはサブスクリプションに保存できます。場所が管理グループの場合、ブループリントを使用して、その管理グループの子サブスクリプションに割り当てることができます。

ボックス2：1

各サブスクリプションにカスタムアプリケーションをデプロイすることを計画している1つの定義。

Azureブループリントを使用すると、ブループリント定義（何をデプロイする必要があるか）とブループリント割り当て（何をデプロイするか）の間の関係が保持されます。

ボックス3：4

サブスクリプションごとに1つの割り当て。

参照：

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

※

**試験対策セミナー　テキスト　109ページに同じような問題がある**

**解答: ２、２、４**

管理グループはAADテナントにまたがることができないため、2つの管理グループが必要です。

ブループリント定義は管理グループ内に保存できます。つまり、2つのブループリント定義が必要です。

ブループリントの割り当てはサブスクリプションレベルであるため、4つ必要です。

# Q.29

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

SQL APIを使用するAzure Cosmos DBデータベースをデプロイすることを計画しています。

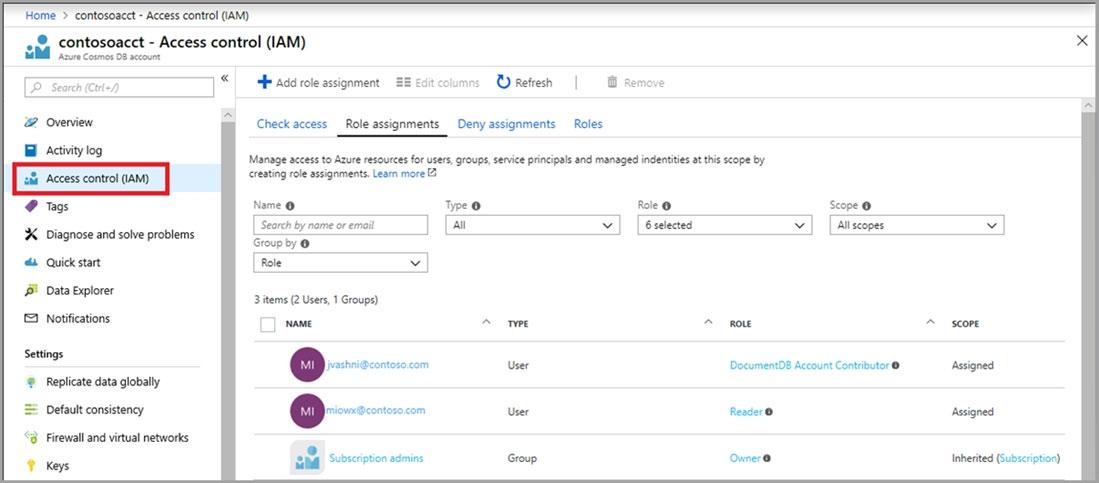
特定のAzure ADユーザーアカウントにCosmos DBデータベースへの読み取りアクセスを提供するソリューションを推奨する必要があります。

推奨事項には何を含める必要がありますか？

1. 共有アクセスシグニチャ（SAS）と条件付きアクセスポリシー
2. 証明書とAzure Key Vault
3. リソーストークンとアクセス制御（IAM）の役割の割り当て
4. マスターキーとAzure Information Protectionポリシー

正解： *C*

Azureポータルのアクセス制御（IAM）ペインは、AzureCosmosリソースでの役割ベースのアクセス制御を構成するために使用されます。ロールは、Active Directoryのユーザー、グループ、サービスプリンシパル、および管理対象IDに適用されます。個人およびグループには、組み込みの役割またはカスタムの役割を使用できます。次のスクリーンショットは、Azureポータルでアクセス制御（IAM）を使用したActive Directory統合（RBAC）を示しています。



参照：

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

リソーストークンを使用して、Azure Cosmos DBのデータにアクセスできます。

また、Azure ADで定義されたユーザーに役割ベースのアクセス制御を提供できます。

Azure Cosmos DBは、2種類のキーを使用してユーザーを認証し、そのデータとリソースへのアクセスを提供します。

主キー管理リソースに使用されるもの：

* データベースアカウント
* データベース
* ユーザー
* アクセス許可リソーストークン

アプリケーションリソースに使用されるもの：

* コンテナー
* ドキュメント
* 添付ファイル
* ストアドプロシージャ
* トリガー
* UDF

ここでは、Cosmos DBデータベースへのアクセスを読み取るため、**ユーザー、リソース（データベース）、およびアクセス許可（読み取り）用に特別に構築されたハッシュリソーストークンを使用する**必要があります。アクセス制御（IAM）RBACを介してCosmos DBアカウントリーダーの役割をユーザーに割り当てます

# Q.30

ASP.NETアプリケーションを実行するAzure仮想マシンをデプロイします。

アプリケーションは、会社のユーザーがインターネットからアクセスします。

ユーザーがASP.NETアプリケーションに接続する前に、Azure Active Directory（Azure AD）アカウントを使用してユーザーが事前認証されていることを確認する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. パブリックAzureロードバランサー
2. Azureのアプリケーションゲートウェイ
3. Azure Traffic Manager
4. Azure ADエンタープライズアプリケーション

正解： *D*

エンタープライズアプリケーションエクスペリエンスを通じて、Azureポータルでサービスプリンシパルを管理できます。サービスプリンシパルは、Azure ADに接続するアプリケーションを管理するものであり、ディレクトリ内のアプリケーションのインスタンスと見なすことができます。

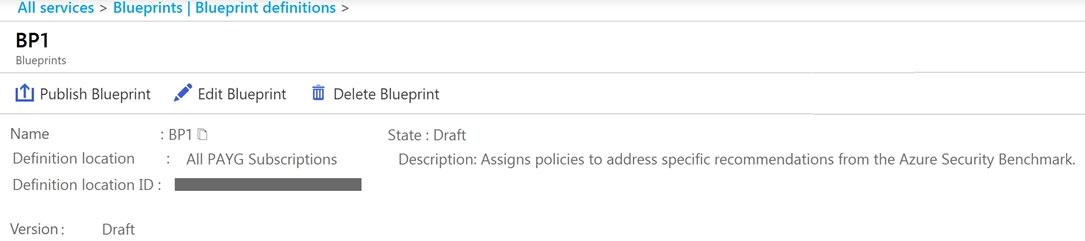
参照：

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

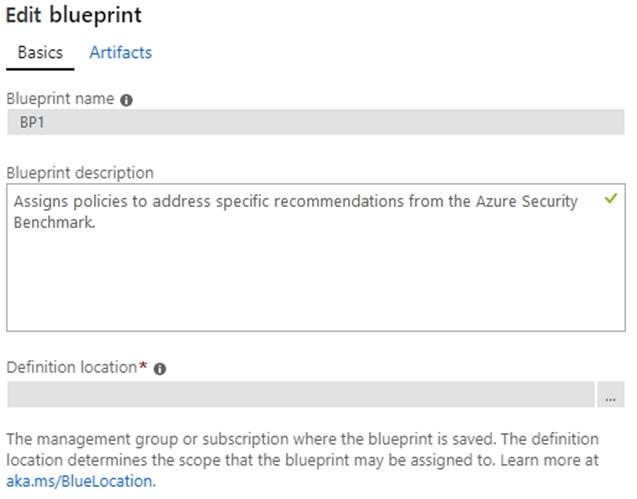
# Q.31

BP1という名前のAzureブループリントがあります。

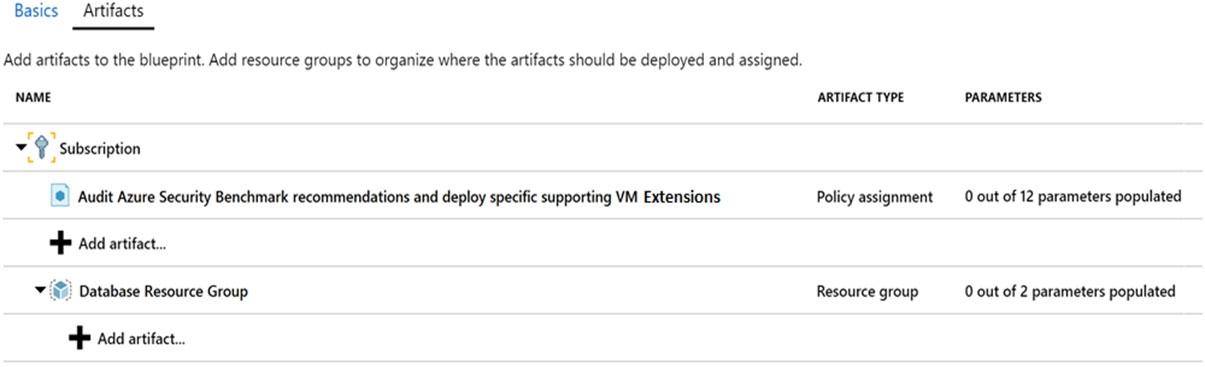
BP1のプロパティは、プロパティの展示に示されています。（[プロパティ]タブをクリックします。）



ブループリントの基本構成は、[基本]展示に示されています。（[基本]タブをクリックします。）



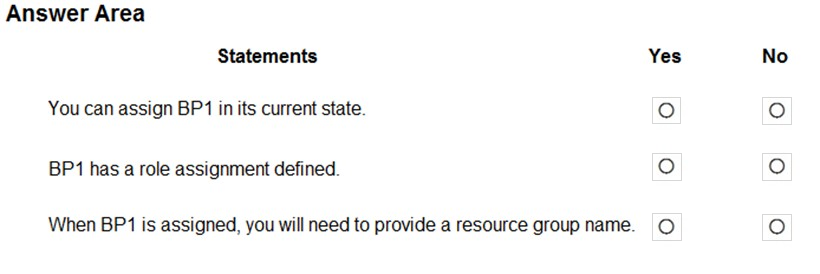
BP1に添付されているアーティファクトは、アーティファクトの展示に表示されます。（「アーティファクト」タブをクリックします。）

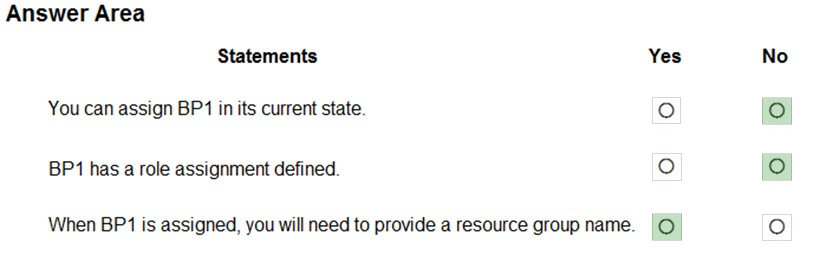


以下の各ステートメントについて、ステートメントが真の場合は「はい」を選択します。それ以外の場合は、[いいえ]を選択します。

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：いいえ

BP1は**ドラフトモード**です。

ブループリントが最初に作成されたとき、ドラフトモードであると見なされます。割り当てる準備ができたら、公開する必要があります。

ボックス2：いいえ

BP1アーティファクトには、1つのポリシー割り当てとリソースグループが含まれますが、役割の割り当ては含まれません。

注：ブループリントは、さまざまなリソーステンプレートおよびその他のアーティファクトの展開を調整するための宣言的な方法です。

* 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（ARMテンプレート）
* リソースグループ

ボックス3：はい-

はい、BP1アーティファクトにはリソースグループ。

参照：

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

# Q.32

あなたの会社は、Azure Active Directory（Azure AD）ハイブリッドIDソリューションを使用したいと考えています。

オンプレミスのActive Directoryへのインターネット接続が利用できない場合に、ユーザーが認証できることを確認する必要があります。このソリューションでは、ユーザーの認証プロンプト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. パスワードハッシュ同期とAzureADシームレスシングルサインオン（Azure ADシームレスSSO）
2. パススルー認証とAzureADシームレスシングルサインオン（Azure ADシームレスSSO）
3. Active Directoryフェデレーションサービス（AD FS）サーバー

正解： *A*

パスワードハッシュ同期+シームレスSSOを使用すると、認証はクラウドで行われます。

不正解：

パススルー認証とフェデレーションは、オンプレミスインフラストラクチャに依存しています。

参照：

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

# Q.33

あなたは、以下の機能を実装しますAzureのポリシーを設計する必要があります。

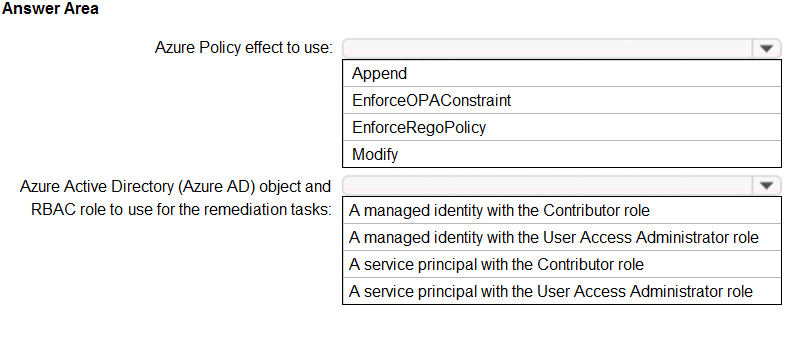
* 新しいリソースの場合は、リソースがデプロイされているリソースグループのタグと値に一致するタグと値を割り当てます。
* 既存のリソースについて、タグと値が、リソースを含むリソースグループのタグと値と一致するかどうかを確認します。
* 非準拠のリソースについては、自動生成された修復タスクをトリガーして、欠落しているタグと値を作成します。

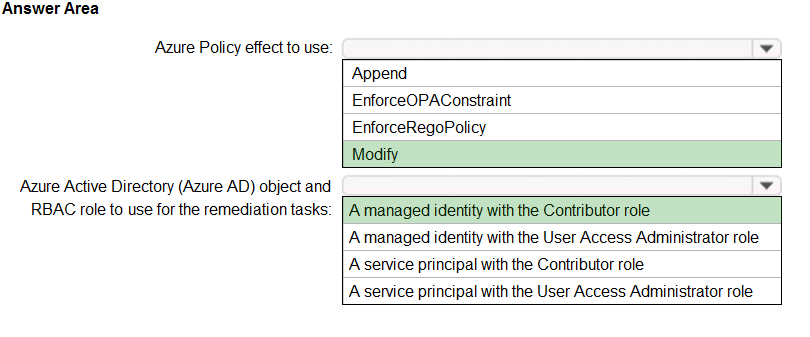
ソリューションは、最小特権の原則を使用する必要があります。

デザインに何を含めるべきですか？回答するには、回答領域で適切なオプションを選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



正解： 

ボックス1：Modfy

変更は、作成または更新中にリソースのプロパティまたはタグを追加、更新、または削除するために使用されます。一般的な例は、costCenterなどのリソースのタグを更新することです。既存の非準拠リソースは、修復タスクで修復できます。1つの変更ルールに任意の数の操作を含めることができます。

不正解：

* 次の効果は非推奨です：EnforceOPAConstraint、EnforceRegoPolicy
* Appendは、作成または更新中に要求されたリソースにフィールドを追加するために使用されます。一般的な例は、ストレージリソースに許可されるIPを指定することです。

ボックス2：コントリビューターロールを持つマネージドID

マネージドID修復セキュリティの仕組み：Azure PolicyがdeployIfNotExistsポリシー定義でテンプレートを実行する場合、マネージIDを使用して実行します。Azureポリシーは、割り当てごとにマネージIDを作成しますが、マネージIDを付与する役割に関する詳細が必要です。

コントリビューターロールは、任意のエンティティにタグを適用するために必要なアクセス権を付与します。

参照：

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

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources>

**試験対策セミナー　テキスト　108ページに同じような問題あり**

# Q.34

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。

あなたの会社には、オンプレミスのActive Directoryドメインサービス（AD DS）ドメインと、確立されたAzure Active Directory（Azure AD）環境があります。あなたの会社は、ユーザーが企業ネットワークに接続されている企業のデスクトップにいるときに、クラウドアプリに自動的にサインインすることを望んでいます。会社のユーザーに対してシングルサインオン（SSO）を有効にする必要があります。

解決策：パスワードハッシュ同期を使用するようにAzure AD Connectサーバーをインストールして構成し、[シングルサインオンを有効にする]オプションを選択します。

ソリューションは目標を達成していますか？

1. はい
2. いいえ

正解： *A*

Azure Active Directoryのシームレスなシングルサインオン（アズールADシームレスなSSO）

彼らは会社のネットワークに接続され、企業のデバイス上にあるとき自動的に署名するユーザー。有効にすると、ユーザーはAzure ADにサインインするためにパスワードを入力する必要がなく、通常はユーザー名も入力する必要があります。この機能により、ユーザーは追加のオンプレミスコンポーネントを必要とせずに、クラウドベースのアプリケーションに簡単にアクセスできます。

シームレスSSOは、パスワードハッシュ同期またはパススルー認証のサインイン方法のいずれかと組み合わせることができます。

参照：

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

# Q.35(34 と同じ)

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。

あなたの会社には、オンプレミスのActive Directoryドメインサービス（AD DS）ドメインと、確立されたAzure Active Directory（Azure AD）環境があります。あなたの会社は、ユーザーが企業ネットワークに接続されている企業のデスクトップにいるときに、クラウドアプリに自動的にサインインすることを望んでいます。会社のユーザーに対してシングルサインオン（SSO）を有効にする必要があります。

解決策：パススルー認証を使用するようにAzure AD Connectサーバーをインストールして構成し、[シングルサインオンを有効にする]オプションを選択します。

ソリューションは目標を達成していますか？

* はい
* いいえ

# Q.36

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。

あなたの会社には、オンプレミスのActive Directoryドメインサービス（AD DS）ドメインと、確立されたAzure Active Directory（Azure AD）環境があります。あなたの会社は、ユーザーが企業ネットワークに接続されている企業のデスクトップにいるときに、クラウドアプリに自動的にサインインすることを望んでいます。会社のユーザーに対してシングルサインオン（SSO）を有効にする必要があります。

解決策：Azure仮想マシン（VM）でADDSサーバーを構成します。双方向レプリケーションを構成します。

ソリューション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 ADConnectサーバーをインストールして構成します。

参照：

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

# Q.37

認証にAzureActive Directory（Azure AD）を使用するAzureWebアプリを設計しています。

複数のAzure ADテナントのユーザーにApp1へのアクセスを提供するソリューションを推奨する必要があります。このソリューションでは、ユーザーがApp1に接続するときにAzure Multi- Factor Authentication（MFA）を使用するようにする必要があります。

推奨事項に含める必要がある2つのタイプのオブジェクトはどれですか？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. Azure ADの条件付きアクセスポリシー
2. Azure ADが管理するID
3. Identity Experience Frameworkポリシー
4. Azureのアプリケーションのセキュリティグループ
5. EndpointManagerアプリの保護ポリシー
6. Azure AD ゲストアカウント

正解： *AF*

A：Azure Active Directory（Azure AD）の条件付きアクセス機能は、アプリを保護し、サービスを保護するために使用できるいくつかの方法の1つを提供します。

条件付きアクセスを使用すると、開発者と企業のお客様は、次のようなさまざまな方法でサービスを保護できます。

* 多要素認証
* Intuneに登録されたデバイスのみに特定のサービスへのアクセスを許可する
* ユーザーの場所とIP範囲を制限する
* 条件付きアクセスポリシーは強力なツールです。ポリシーの次のアカウント：
* サービスアカウントとサービスプリンシパル。

組織でこれらのアカウントをスクリプトまたはコードで使用している場合は、それらを管理対象IDに置き換えることを検討してください。

不正解：

B：マネージドIDはクロスディレクトリシナリオをサポートしていません。

E：アプリケーションセキュリティグループを使用すると、ネットワークセキュリティをアプリケーションの構造の自然な拡張として構成できるため、仮想マシンをグループ化し、それらのグループに基づいてネットワークセキュリティポリシーを定義できます。

注：正しいオプションは、Azureへのアプリケーション登録である必要があります。これにより、AD上のユーザーの認証がアプリケーションにアクセスできるようになります。デフォルトのアプリケーション登録は、ユーザーが有効なログイン資格情報を持っていることを検証します。これは、Active Directoryにすることも、マルチテナントアプリケーションの場合は、ユーザーの発信元のディレクトリにすることもできます。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-conditional-access-dev-guide>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management>

<https://www.re-mark-able.net/understanding-azure-active-directory-application-registrations/>

**他のテナントの他のユーザーがリソースを使用して条件付きアクセスを適用できるようにする必要があるため、ゲストアカウント（B2b）と条件付きアクセスを使用します。**

# Q.38

カスタム暗号化キーを使用するAzure Storageアカウントを作成する必要があります。

暗号化を実装するには何が必要ですか？

1. 統合認証局（CA）によって発行され、Azure Key Vaultに保存されている証明書
2. ストレージアカウントにアクセスするように構成されたマネージドID
3. Azure Active Directoryプレミアムサブスクリプション
4. ストレージアカウントと同じAzureリージョンにあるAzureキーボールト

~~正解：~~ *~~A~~*

~~独自の暗号化キーを使用して、ストレージアカウントのデータを保護できます。顧客管理キーを指定すると、そのキーは、データを暗号化するキーへのアクセスを保護および制御するために使用されます。~~

~~顧客が管理するキーを格納するには、Azure KeyVaultまたはAzureKey Vault管理ハードウェアセキュリティモデル（HSM）（プレビュー）のいずれかを使用する必要があります。~~

正解：D

ストレージアカウントとキーボールトまたはマネージドHSMは、同じリージョンにあり、同じAzure Active Directory（Azure AD）テナントにある必要がありますが、異なるサブスクリプションにある場合があります。

顧客が管理するキーを格納するには、Azure Key VaultまたはAzure Key Vault管理対象ハードウェアセキュリティモジュール（HSM）（プレビュー）のいずれかを使用する必要があります。

独自のキーを作成してキーボールトまたはマネージドHSMに保存するか、Azure Key Vault APIを使用してキーを生成することができます。

**ストレージアカウントとキーボールトまたはマネージドHSMは、同じリージョンにあり、同じAzure Active Directory（Azure AD）テナントにある必要がありますが、異なるサブスクリプションにある場合もあります。**

# Q.39

ルート管理グループと5つの子管理グループを持つAzure環境を作成することを計画しています。各子管理グループには、5つのAzureサブスクリプションが含まれます。各サブスクリプションに10から30のリソースグループを含めることを計画しています。

計画された環境の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。

サブスクリプションの所有者ロールが割り当てられているユーザーが、それぞれのサブスクリプションからリソースグループを削除できないようにします。

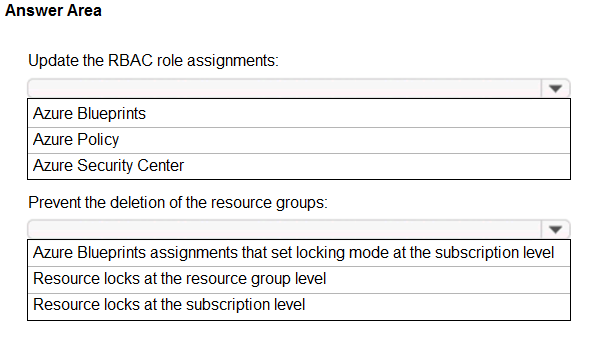
* すべてのサブスクリプションとリソースグループにわたってRBACの役割の割り当てを更新できることを確認します。
* 管理作業を最小限に抑えます。

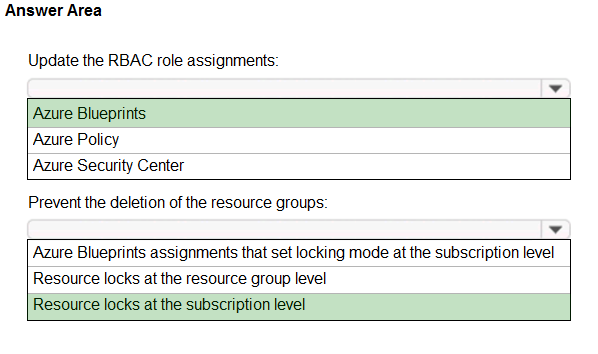
ソリューションに何を含める必要がありますか？

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：



正解： 

ボックス1：Azureブループリント

ブループリントは、さまざまなリソーステンプレートおよびその他のアーティファクトの展開を調整するための宣言的な方法です。

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（ARMテンプレート）

リソースグループ-

不正解：

ポリシーはデフォルトの許可および明示的な拒否システムは、展開中および既存のリソースのリソースプロパティに焦点を合わせています。

ボックス2：サブスクリプションレベルでのリソースロック

サブスクリプションレベルでの管理作業ロックを最小限に抑えるため。

注：管理者は、サブスクリプション、リソースグループ、またはリソースをロックして、組織内の他のユーザーが誤って重要なリソースを削除または変更するのを防ぐことができます。

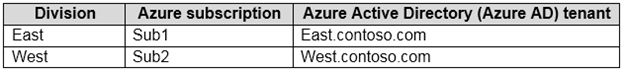
参照：

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

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

# Q.40

あなたの会社には、次の表に示す部門があります。



Sub1には、App1という名前のASP.NETアプリケーションを実行するAzure Webアプリが含まれています。App1は、Microsoft IDプラットフォーム（v2.0）を使用してユーザー認証を処理します。

east.contoso.comのユーザーは、App1に対して認証できます。

west.contoso.comのユーザーがApp1に対して認証できるようにするソリューションを推奨する必要があります。

west.contoso.com Azure ADテナントに何をお勧めしますか？

1. 条件付きアクセスポリシー
2. パススルー認証
3. ゲストアカウント
4. アプリの登録

正解： *D*

MicrosoftIDプラットフォームを構成するいくつかのコンポーネントがあります。

* OAuth2.0およびOpenIDConnect標準準拠の認証サービス

アプリケーション管理ポータル：Azureポータルでの登録と構成のエクスペリエンス、およびその他のAzure管理機能。

Azureポータルのアプリ登録エクスペリエンスを使用してアプリケーションを登録し、アプリをMicrosoft IDプラットフォームと統合して、MicrosoftGraphを呼び出すことができるようにします。

参照：

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

<https://docs.microsoft.com/en-us/graph/auth-register-app-v2>

私は、Cのゲストアカウントと考える。

アプリケーションが既に登録済みと考えたためです。

Dを解答とする根拠は

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant>

ここにあると考えられる。アプリケーションがマルチテナント対応されており、未登録であるのなら、登録時にマルチテナント対応すれば良い。

# Q.41

Group1という名前のセキュリティグループを持つcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。Group1は、割り当てられたメンバーシップ用に構成されています。Group1には、20人のゲストユーザーを含む50人のメンバーがいます。

Group1のメンバーシップを評価するためのソリューションを推奨する必要があります。ソリューションは次の要件を満たしている必要があります。

* 評価は3か月ごとに自動的に繰り返される必要があります。
* すべてのメンバーは、Group1に参加する必要があるかどうかを報告できる必要があります。
* Group1に所属する必要がないと報告したユーザーは、Group1から自動的に削除する必要があります。
* Group1に参加する必要があるかどうかを報告しないユーザーは、Group1から自動的に削除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. 変更ダイナミックユーザーにグループ1のメンバーシップタイプ。
2. Azure AD特権ID管理を実装します。
3. Azure AD Identity Protectionを実装します。
4. アクセスレビューを作成します。

正解： *A* (※参照)

Azure Active Directory（Azure AD）では、複雑な属性ベースのルールを作成して、グループの動的メンバーシップを有効にすることができます。動的なグループメンバーシップにより、ユーザーの追加と削除による管理オーバーヘッドが削減されます。

ユーザーまたはデバイスの属性が変更されると、システムはディレクトリ内のすべての動的グループルールを評価して、その変更によってグループの追加または削除がトリガーされるかどうかを確認します。ユーザーまたはデバイスがグループのルールを満たしている場合、それらはそのグループのメンバーとして追加されます。ルールを満たさなくなった場合は削除されます。

参照：

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

※

**D：アクセスレビューを作成する**

動的グループは、ユーザーの意思表明に関係なく動作するので、この問題の答えには不向きだと考える。

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#when-should-you-use-access-reviews>

<https://techcommunity.microsoft.com/t5/itops-talk-blog/dynamic-groups-in-azure-ad-and-microsoft-365/ba-p/2267494>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#where-do-you-create-reviews>

# Q.42

あなたの会社はApp1という名前のアプリを購入しています。

App1がアクセスレビューを読み取って変更できる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。

あなたは何をお勧めしますか？

1. API管理サービスから、App1のAPIを公開してから、Microsoft Graph APIに権限を委任します。
2. Azure Active Directory管理センターから、App1を登録します。アクセス制御（IAM）ブレードから、アクセス許可を委任します。
3. Azure Active Directory管理センターからApp1を登録し、Microsoft Graph APIにアクセス許可を委任します。
4. API管理サービスから、App1のAPIを公開します。アクセス制御（IAM）ブレードから、アクセス許可を委任します。

~~正解：~~ *~~B~~*

~~アプリを登録する必要があります。アプリケーションは、Azure ActiveDirectory管理センターに登録できます。~~

~~Azure ADアクセスレビュー機能には、MicrosoftGraphエンドポイントにAPIがあります。~~

~~Azure ADアプリケーションを登録し、グラフでアクセスレビューAPIを呼び出すためのアクセス許可を設定できます。~~

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

**正解：C**

<https://docs.microsoft.com/en-us/graph/use-the-api>

Microsoft Graphは、Microsoft Cloud サービスリソースへのアクセスを可能にするRESTful Web APIです。あなたが後に**アプリを登録し、ユーザーの認証トークンを取得またはサービスは、MicrosoftグラフAPIへのリクエストを行うことができます**。

重要： 条件付きアクセスポリシーがMicrosoft Graphにどのように適用されるかは変化しています。条件付きアクセスポリシーが構成されているシナリオを処理するには、アプリケーションを更新する必要があります。詳細とガイダンスについては、「Azure Active Directory条件付きアクセスの開発者向けガイダンス」を参照してください。

# Q.43

20のAzureサブスクリプションにわたって200のリソースグループがあります。

あなたの会社のセキュリティポリシーは、セキュリティ管理者が月に一度、サブスクリプションとリソースグループの所有者ロールのすべての割り当てを確認する必要があると述べています。セキュリティ管理者によって承認されていないすべての割り当ては、自動的に削除する必要があります。セキュリティ管理者は、検証を実行するように毎月求められる必要があります。

セキュリティポリシーを実装するには何を使用する必要がありますか？

1. Azure Security CenterのIDセキュアスコア
2. Identity Governanceのレビューにアクセスする
3. Azure Active Directory（Azure AD）ID保護のユーザーリスクポリシー
4. Azure Active Directory（Azure AD）での役割の割り当て特権ID管理（PIM）

正解： *B*

Azure Active Directory（Azure AD）アクセスレビューにより、組織はグループメンバーシップ、エンタープライズアプリケーションへのアクセス、および役割の割り当てを効率的に管理できます。ユーザーのアクセスを定期的に確認して、適切なユーザーだけが引き続きアクセスできるようにすることができます。

参照：

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

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#when-should-you-use-access-reviews>

# Q.44

あなたの会社には、社内で開発された20の WebAPI があります。

同社は、WebAPIを使用する10個のWebアプリを開発しています。

WebアプリとAPIは、会社のAzure Active Directory（Azure AD）テナントに登録されています。Web APIは、Azure API Managementを使用して公開されます。

Webアプリから発信された不正なリクエストがWebAPIに到達するのをブロックするソリューションを推奨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。

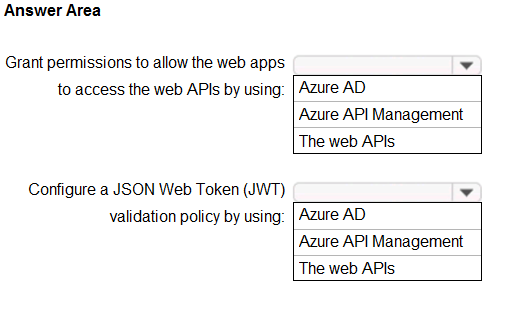
* Azure ADで生成されたクレームを使用します。
* 構成と管理の労力を最小限に抑えます。

推奨事項には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：



1. [answer]を使用して、WebアプリがWebAPIにアクセスすることを許可する権限を付与します。
2. [answer]を使用してJSONWeb Token（JWT）検証ポリシーを構成します。

解答

1、Azure AD

2、Azure API Management

試験対策セミナー　テキスト　54ページ

実行する手順：

1. Azure ADで、APIを表すアプリケーション（バックエンドアプリ）を登録します。
2. Azure ADで、APIを呼び出す必要があるクライアントアプリケーションを表す別のアプリケーション（client-app）を登録します。
3. Azure ADで、クライアントアプリがバックエンドアプリを呼び出すことを許可するアクセス許可を付与します。
4. APIMで、OAuth2.0ユーザー認証を使用してAPIを呼び出すように開発者コンソールを構成します。
5. APIMで、validate-jwtポリシーを追加して、すべての着信リクエストのOAuthトークンを検証します。

1.次を使用してアクセス許可を付与します：Azure AD（ステップ3）

2.次を使用してJWT検証ポリシーを構成します：Azure APIM（ステップ5）

# Q.45

Azureサブスクリプションのリソースガバナンスソリューションを設計する必要があります。ソリューションは、次の要件を満たしている必要があります。

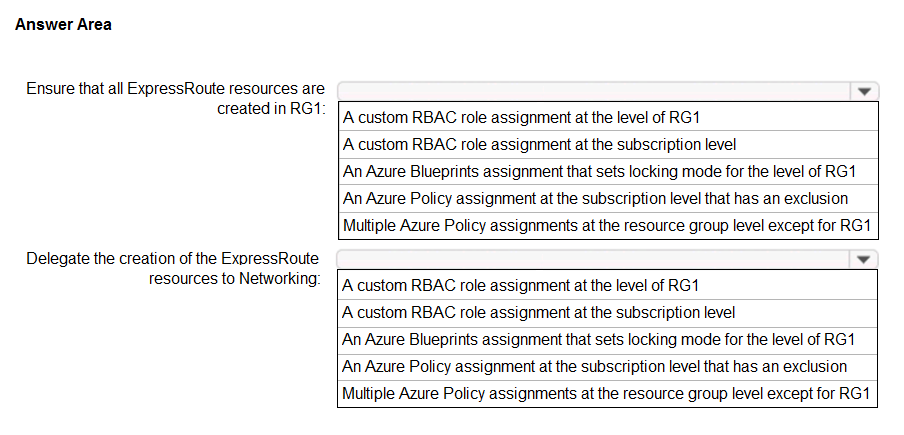
* すべてのExpressRouteリソースがRG1という名前のリソースグループに作成されていることを確認します。
* ExpressRouteリソースの作成をNetworkingという名前のAzure Active Directory（Azure AD）グループに委任します。
* 最小特権の原則を使用します。

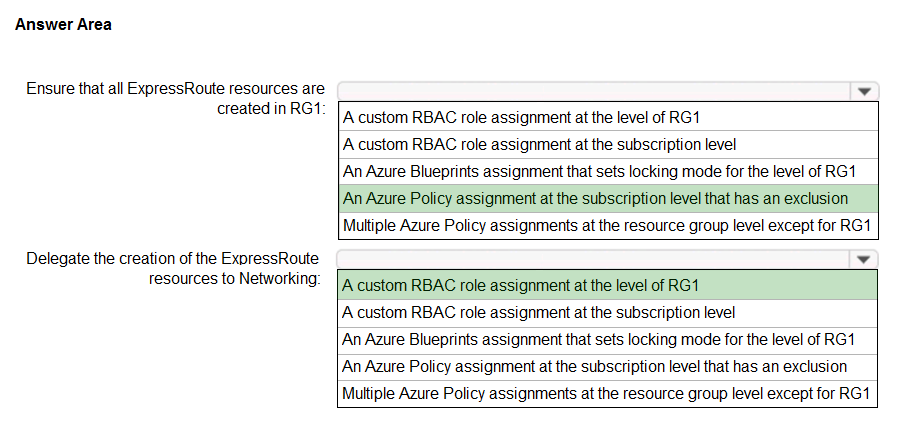
ソリューションに何を含める必要がありますか？

回答するには、回答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：除外があるサブスクリプションレベルでのAzureポリシーの割り当て

ボックス2：RG1のレベルでのカスタムRBACロール割り当て

Azureロールベースのアクセス制御（Azure RBAC）は、アクセスの管理に使用する承認システムですAzureリソースに。アクセスを許可するには、特定のスコープでユーザー、グループ、サービスプリンシパル、または管理対象IDにロールを割り当てます。

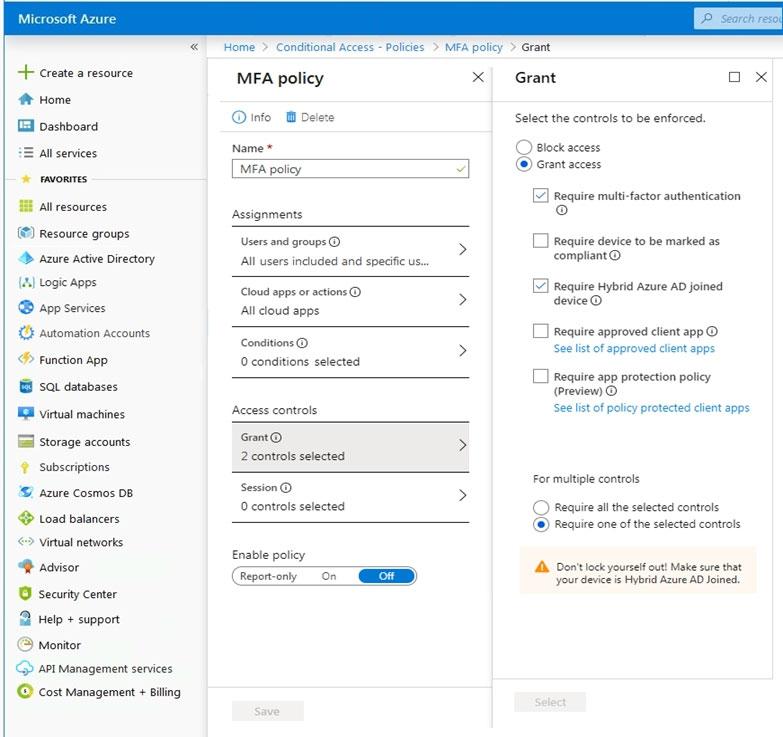
参照：

<https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

# Q.46

Azure Active Directory（Azure AD）テナントとWindows10デバイスがあります。

展示に示されているように、条件付きアクセスポリシーを構成します。（[展示]タブをクリックします。）



ポリシーの結果はどうなりますか？

1. すべてのユーザーは、常に多要素認証（MFA）の入力を求められます。
2. ユーザーは、Azure ADに参加していないデバイスからサインインした場合にのみ、多要素認証（MFA）の入力を求められます。
3. すべてのユーザーは、多要素認証（MFA）を使用せずにサインインできます。
4. ユーザーは、Azure ADに参加しているデバイスからサインインした場合にのみ、多要素認証（MFA）の入力を求められます。

解答：C

Enable policy が Off の状態です。

オリジナルの解答

正解： *B*

デバイスをAzure ADに参加させるか、MFAを使用する必要があります。

# Q.47

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

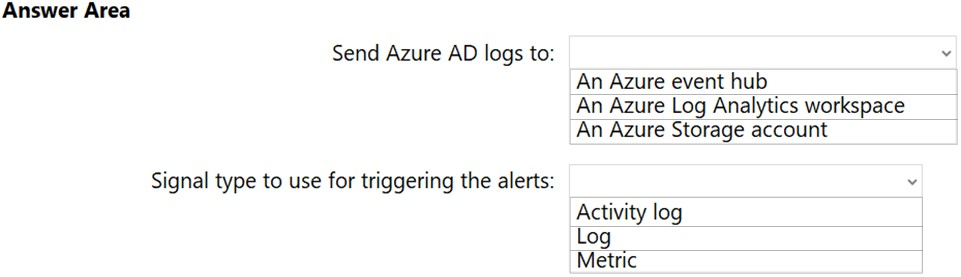
Azure Monitorを使用してユーザーのサインインを監視し、特定のユーザーのサインインイベントに基づいてアラートを生成することを計画しています。

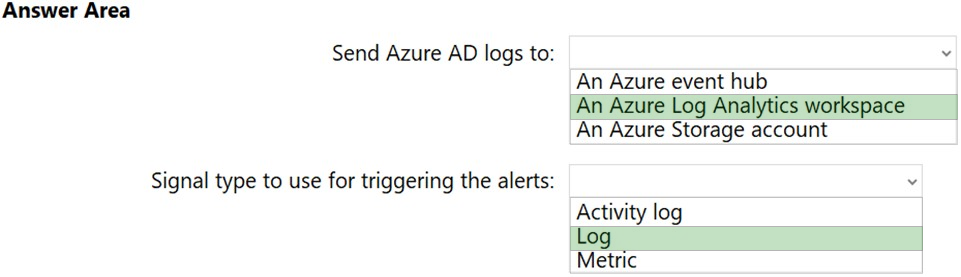
イベントに基づいてアラートをトリガーするソリューションを推奨する必要があります。

推奨事項には何を含める必要がありますか？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：Azure Log Analyticsワークスペース

アラートを作成できるようにするために、AzureADログをAzureLogAnalyticsワークスペースに送信します。

注：AADログとイベントは、Azure Storage Account、Azure Event Hub、Log Analytics、またはこれらすべての組み合わせのいずれかに転送できます。

ボックス2：ログ

リソースタイプがLog AnalyticsやApplication Insightsなどの分析ソースであり、シグナルタイプがログであることを確認します。

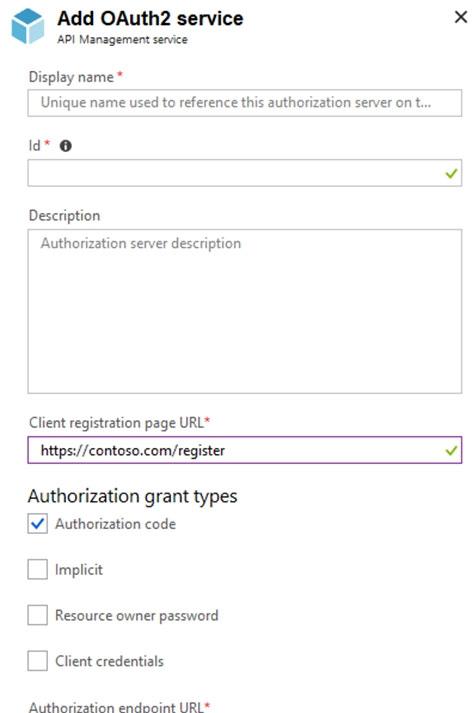
参照：

<https://4sysops.com/archives/how-to-create-an-azure-ad-admin-login-alert/>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log>

# Q.48

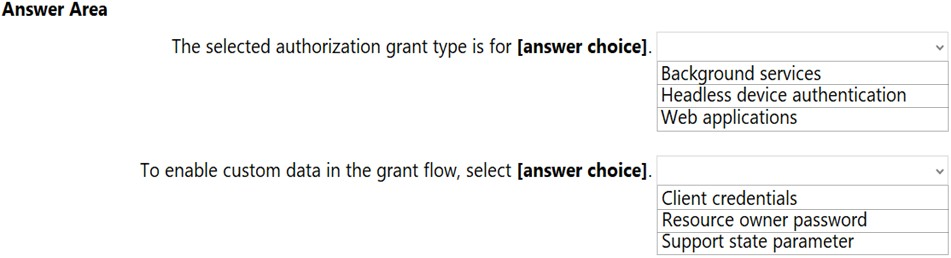
次の展示に示すように、あなたがAPI管理でのOAuth2認証を設定します。

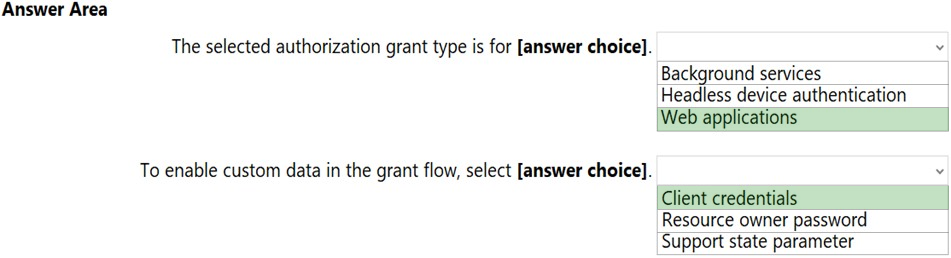


ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。

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

承認コード付与タイプは、ユーザーがアプリを承認した後にアクセストークンを取得するために、Webアプリとネイティブアプリの両方で使用されます。

注：認証コード付与タイプは、アクセストークンの認証コードを交換するために機密クライアントとパブリッククライアントによって使用されます。

ユーザーがリダイレクトURLを介してクライアントに戻った後、アプリケーションはURLから認証コードを取得し、それを使用してアクセストークンを要求します。

不正解：

ヘッドレスデバイス認証ではない：ヘッドレスシステムは、モニター、グラフィカルユーザーインターフェイス（GUI）、またはキーボードやマウスなどの周辺機器なしで動作するコンピューターです。

ヘッドレスコンピューターは通常、マルチサーバーデータセンター環境のさまざまなデバイスまたはサーバーに組み込まれたシステムです。産業機械、自動車、医療機器、カメラ、家電製品、飛行機、自動販売機、おもちゃは、組み込みシステムの無数の可能なホストの中にあります。

ボックス2：クライアントの資格情報

追加のクライアントデータを含める方法

標準のパラメーターセットに適合しないクライアントに関する追加の詳細を保存する必要がある場合は、カスタムデータパラメーターが役立ちます：

POST /c2id/clients HTTP/1.1 -

Host: demo.c2id.com -

Content-Type: application/json -

Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

{

"redirect\_uris" : [ "https://myapp.example.com/callback" ],

"data" : { "reg\_type" : "3rd-party",

"approved" : true,

"author\_id" : 792440 }

}

dataパラメーターは、JSONオブジェクトにパッケージ化された任意のコンテンツを許可します。これを設定するには、マスター登録トークンまたはclient-reg：dataスコープのワンタイムアクセストークンが必要です。

不正解：

承認プロトコルは、アプリケーションの以前の状態を復元できる状態パラメーターを提供します。stateパラメーターは、Authorization要求でクライアントによって設定された状態オブジェクトを保持し、応答でクライアントが使用できるようにします。

参照：

<https://developer.okta.com/blog/2018/04/10/oauth-authorization-code-grant-type>

<https://connect2id.com/products/server/docs/guides/client-registration>

# Q.49

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。

あなたの会社は、オンプレミスとAzureに複数の仮想マシン（VM）を展開しています。Azure ExpressRouteは、オンプレミスからAzureへの接続用にデプロイおよび構成されています。いくつかのVMでネットワーク接続の問題が発生しています。

ネットワークトラフィックを分析して、VMに対してパケットが許可されているか拒否されているかを判断する必要があります。

解決策：Azure Network Watcherを使用してIPフロー検証を実行し、ネットワークトラフィックを分析します。

ソリューションは目標を達成していますか？

1. はい
2. いいえ

正解： *A*

[ネットワークウォッチャー ネットワークパフォーマンスモニタを使用して、ネットワークインフラストラクチャのさまざまなポイント間のネットワークパフォーマンスを監視するのに役立ちます、クラウドベースのハイブリッドネットワーク監視ソリューションです。また、サービスエンドポイントとアプリケーションエンドポイントへのネットワーク接続を監視し、AzureExpressRouteのパフォーマンスを監視するのにも役立ちます。

注：

IPフロー検証では、仮想マシンとの間でパケットが許可または拒否されているかどうかがチェックされます。この情報は、方向、プロトコル、ローカルIP、リモートIP、ローカルポート、およびリモートポートで構成されます。パケットがセキュリティグループによって拒否された場合、パケットを拒否したルールの名前が返されます。任意の送信元または宛先IPを選択できますが、IPフロー検証は、管理者がインターネットとの間、およびオンプレミス環境との間の接続の問題を迅速に診断するのに役立ちます。

IPフロー検証は、サブネットや仮想マシンNICなどのネットワークインターフェイスに適用されるすべてのネットワークセキュリティグループ（NSG）のルールを調べます。次に、そのネットワークインターフェイスとの間の設定に基づいて、トラフィックフローが検証されます。IPフロー検証は、ネットワークセキュリティグループのルールが仮想マシンとの間の入力または出力トラフィックをブロックしているかどうかを確認するのに役立ちます。

参照：

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

# Q.50

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

あなたの会社は、オンプレミスとAzureに複数の仮想マシン（VM）を展開しています。Azure ExpressRouteは、オンプレミスからAzureへの接続用にデプロイおよび構成されています。いくつかのVMでネットワーク接続の問題が発生しています。

ネットワークトラフィックを分析して、VMに対してパケットが許可されているか拒否されているかを判断する必要があります。

解決策：Azure Advisorを使用してネットワークトラフィックを分析します。

ソリューション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 Network Watcherを使用してIPフロー検証を実行し、ネットワークトラフィックを分析します。

注：Advisorは、Azureのデプロイを最適化するためのベストプラクティスに従うのに役立つ、パーソナライズされたクラウドコンサルタントです。リソースの構成と使用状況のテレメトリを分析し、Azureリソースの費用対効果、パフォーマンス、高可用性、セキュリティの向上に役立つソリューションを推奨します。

Advisorを使用すると、次のことが可能になります。

プロアクティブで実用的でパーソナライズされたベストプラクティスの推奨事項を取得します。

Azure全体の支出を削減する機会を特定することで、リソースのパフォーマンス、セキュリティ、および高可用性を向上させます。

提案されたアクションをインラインで推奨します。

参照：

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

# Q.51

同じAzureリージョンに500個のAzureWebアプリがあります。アプリは、認証にプレミアムAzureキーボールトを使用します。

開発者は、一部の認証要求が抑制されていると報告しています。

キーボールトの利用可能なスループットを向上させるソリューションを推奨する必要があります。ソリューションはコストを最小限に抑える必要があります。

あなたは何をお勧めしますか？

1. 料金階層を変更します。
2. ジオレプリケーションを構成します。
3. アプリの負荷分散を構成します。
4. サブスクリプション内の主要なボールトの数を増やします。

正解： *D*

プットレートを介してKey Vaultを最大化するために、スループットを最大化するための推奨ガイドライン/ベストプラクティスを次に示します。

1. スロットルが適切に設定されていることを確認します。クライアントは、429の指数バックオフポリシーを尊重し、以下のガイダンスに従って再試行を行っていることを確認する必要があります。
2. Key Vaultトラフィックを複数のVaultと異なるリージョンに分割します。セキュリティ/可用性ドメインごとに個別のボールトを使用します。それぞれ2つのリージョンに5つのアプリがある場合は、アプリとリージョンに固有のシークレットをそれぞれ含む10個のボールトをお勧めします。

参照：

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

# Q.52

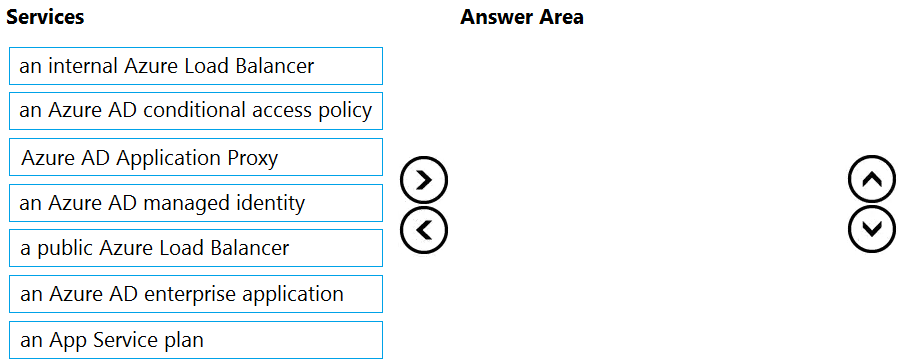
オンプレミスネットワークには、App1という名前のASP.NETアプリケーションを実行するServer1という名前のサーバーが含まれています。

Azure Active Directory（Azure AD）のハイブリッド展開があります。

ユーザーがインターネットからApp1に接続するときに、Azure ADアカウントとAzure Multi-Factor Authentication（MFA）を使用してサインインできるようにするソリューションを推奨する必要があります。

順番にデプロイして構成することをお勧めする3つのAzureサービスはどれですか？回答するには、適切なサービスをサービスのリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解：

**ステップ1：AzureADアプリケーションプロキシ**

AzureADアプリケーションプロキシは、クラウドアクセス用に公開されたオンプレミスのレガシーアプリケーションを使用するシナリオの前提条件です。

注：アプリケーションプロキシは、ユーザーがオンプレミスにアクセスできるようにするAzure ADの機能です。リモートクライアントからのWebアプリケーション。アプリケーションプロキシには、クラウドで実行されるアプリケーションプロキシサービスと、オンプレミスサーバーで実行されるアプリケーションプロキシコネクタの両方が含まれます。

**ステップ2：Azure AD マネージド ID**

MicrosoftのIDソリューションは、オンプレミスとクラウドベースの機能にまたがっています。これらのソリューションは、場所に関係なく、すべてのリソースに対する認証と承認のための共通のユーザーIDを作成します。これをハイブリッドアイデンティティと呼びます。

**ステップ3：Azure ADの条件付きアクセスポリシー**

条件付きアクセスは、Azure Active Directoryがシグナルをまとめ、意思決定を行い、組織のポリシーを適用するために使用するツールです。条件付きアクセスは、新しいID駆動型コントロールプレーンの中心です。

Azure ADへのハイブリッドIDとハイブリッドID管理により、これらのシナリオが可能になります。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

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

# Q.53

Contoso,Ltd. という名前の会社には、Microsoft 365およびAzureサブスクリプションと統合されたAzure Active Directory（Azure AD）テナントがあります。

ContosoにはオンプレミスのIDインフラストラクチャがあります。インフラストラクチャには、Active Directoryドメインサービス（AD DS）、Active Directory フェデレーションサービス（AD FS）、Azure AD Connect、およびMicrosoft Identity Manager（MIM）を実行するサーバーが含まれます。

Contosoは、Fabrikam、Incという名前の会社とパートナーシップを結んでいます。Fabrikamには、Active Directory フォレストとMicrosoft 365テナントがあります。Fabrikamには、Contosoと同じオンプレミスIDインフラストラクチャコンポーネントがあります。

Fabrikamの10人の開発者のチームが、ContosoのAzureサブスクリプションでホストされるAzureソリューションに取り組みます。開発者は、Contosoサブスクリプションのリソースグループのコントリビューターロールに追加する必要があります。

Contosoが10人のFabrikam開発者に役割を割り当てることができる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。このソリューションでは、Fabrikam開発者が既存のクレデンシャルを使用してリソースにアクセスできるようにする必要があります。

あなたは何をお勧めしますか？

1. Contoso社のアズールADテナントでは、AzureのActive Directoryドメインサービス（AD DSアズール）を有効にします。ContosoとFabrikamのActive Directoryフォレスト間で選択的認証を使用する一方向のフォレストの信頼を作成します。
2. Contoso社のアズールADテナントでは、Fabrikamの開発者向けのクラウドのみのユーザーアカウントを作成します。
3. 設定Contoso社とFabrikam社のオンプレミスのActive Directoryフォレスト間でフォレストの信頼。
4. Contoso社のアズールADテナントでは、使用MIMは、Fabrikamの開発者のためのゲストアカウントを作成します。

正解： *C*

信頼の構成

管理対象フォレストまたはドメインから管理フォレストへの信頼を構成します

* 本番環境から管理フォレストへの一方向の信頼が必要です。
* 選択的認証を使用して、管理フォレスト内のアカウントを適切な本番ホストにのみログオンするように制限する必要があります。

参照：

<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

※説明を読むと、A が正解のように見えるが・・・

# Q.54

Azureガバナンスソリューションを設計しています。

すべてのAzureリソースは、環境、所有者、部門、およびコストセンターの運用情報に基づいて簡単に識別できる必要があります。

Azureリソースのレポートを生成するときに、運用情報を使用できることを確認する必要があります。

ソリューションに何を含める必要がありますか？

1. Azure REST APIをデータソースとして使用するAzureデータカタログ
2. Azure Active Directory（Azure AD）管理ユニット
3. 親グループを使用して階層を作成するAzure管理グループ
4. タグ付けルールを適用するAzureポリシー

正解： *D*

Azureポリシーを使用して、タグ付けのルールと規則を適用します。ポリシーを作成することにより、組織に期待されるタグがないリソースがサブスクリプションにデプロイされるシナリオを回避できます。タグを手動で適用したり、準拠していないリソースを検索したりする代わりに、展開中に必要なタグを自動的に適用するポリシーを作成します。

注：クラウドベースのリソースの整理は、単純な展開しかない場合を除いて、ITにとって重要なタスクです。次の理由から、命名とタグ付けの標準を使用してリソースを整理します。

リソース管理：ITチームは、特定のワークロード、環境、所有権グループ、またはその他の重要な情報に関連するリソースをすばやく見つける必要があります。リソースの整理は、リソース管理のための組織の役割とアクセス許可を割り当てるために重要です。

参照：

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

# Q.55

あなたはあなたの会社のアクセスポリシーを設計しています。

場合によっては、会社の開発者はAzure仮想マシンを停止、起動、および再起動する必要があります。開発チームは頻繁に変わります。

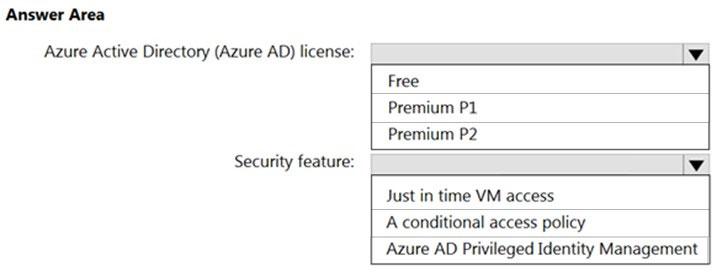
開発者に仮想マシンへの必要なアクセスを提供するソリューションを推奨する必要があります。ソリューションは、次の要件を満たしている必要があります。

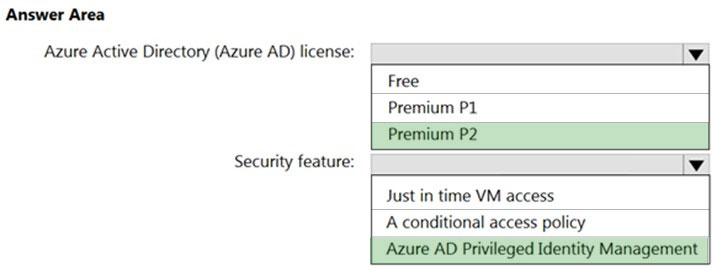
* 必要な場合にのみアクセス許可を提供します。
* 最小特権の原則を使用します。
* コストを最小限に抑えます。

推奨事項には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：



正解： 

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

ジャストインタイムVMアクセスは、ユーザーベースの割り当てを実装していません。

より良いオプションは、PIMとジャストインタイムの役割の割り当てを使用することです。

# Q.56

ハイブリッドAzure Active Directory（Azure AD）テナントの無料版があります。

テナントはパスワードハッシュ同期を使用します。

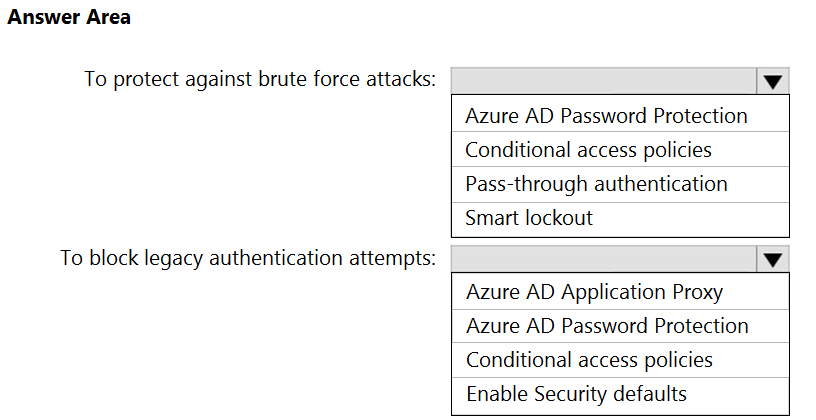
次の要件を満たすソリューションを推奨する必要があります。

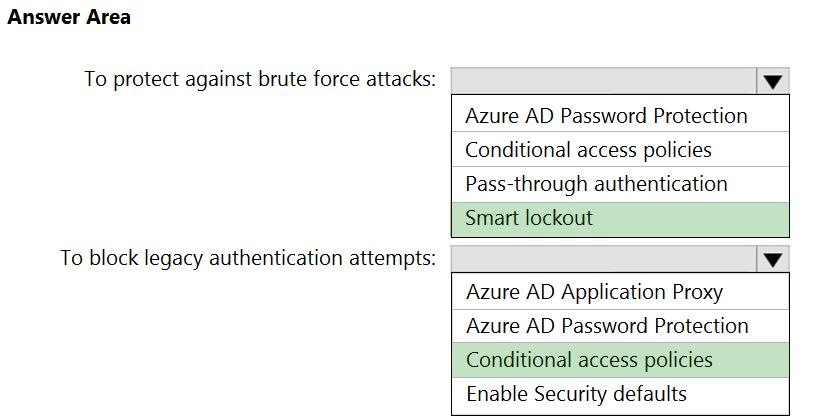
* Azure ADユーザーアカウントを標的としたブルートフォース攻撃の結果としてActive Directoryドメインユーザーアカウントがロックアウトされないようにします。
* Azure AD統合アプリに対するレガシー認証の試行をブロックします。
* コストを最小限に抑えます。

要件ごとに何をお勧めしますか？回答するには、回答領域で適切なオプションを選択します。

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：スマートロックアウト

スマートロックアウトは、ユーザーのパスワードを推測したり、ブルートフォース方式を使用して侵入しようとする悪意のある攻撃者をロックアウトするのに役立ちます。スマートロックアウトは、有効なユーザーからのサインインを認識し、それらを異なる方法で処理できます。攻撃者やその他の未知のソースよりも。攻撃者はロックアウトされますが、ユーザーは引き続きアカウントにアクセスして生産性を高めます。

ボックス2：条件付きアクセスポリシー

環境がレガシー認証をブロックしてテナントの保護を強化する準備ができている場合は、条件付きアクセスを使用してこの目標を達成できます。

従来の認証を使用するアプリがテナントのリソースにアクセスするのを防ぐにはどうすればよいですか？条件付きでブロックすることをお勧めします

アクセスポリシー。必要に応じて、特定のユーザーと特定のネットワークロケーションのみにレガシー認証に基づくアプリの使用を許可します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

# Q.57

複数の管理ユーザーアカウントを含むcontoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。

過去30日間にサインインしなかった管理ユーザーアカウントを特定するためのソリューションを推奨する必要があります。

どのサービスを推奨に含める必要がありますか？

1. Azure ADの特権ID管理（PIM）
2. Azure AD Identity Protection
3. Azure Advisor
4. Azureのアクティビティログ

正解： *A*

# Q.58

企業は、Azure Active Directory（Azure AD）Connectを展開して、オンプレミスのActive Directoryドメインサービス（AD DS）ディレクトリからAzureADテナントにID情報を同期します。同期されるID情報には、ユーザーアカウント、認証用の資格情報ハッシュ（パスワード同期）、およびグループメンバーシップが含まれます。同社は、アプリケーションをサポートするために、いくつかのWindowsおよびLinux仮想マシン（VM）を展開することを計画しています。

VMには、次の要件があります。

* ドメイン参加、LDAP読み取り、LDAPバインド、NTLMおよびKerberos認証、およびグループポリシーをサポートします。
* ユーザーが企業の資格情報を使用してドメインにサインインし、リモートデスクトップを使用してVMにリモート接続できるようにします。

VMの展開をサポートする必要があります。

どのサービスを使うべきですか？

1. Active Directory フェデレーションサービス（AD FS）
2. Azure ADの特権ID管理
3. Azureの管理アイデンティティ
4. Azure AD ドメインサービス

正解： *D*

Azure ADドメインサービスは、ドメイン参加、グループポリシー、LDAP、Kerberos / NTLM認証など、Windows Server ActiveDirectoryと完全に互換性のあるマネージドドメインサービスを提供します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

# Q.59

Azure Active Directory（Azure AD）ユーザーがオンライン調査を作成および公開できるようにするサービスとしてのソフトウェア（SaaS）アプリケーションを設計しています。

SaaSアプリケーションは、フロントエンドのWebアプリケーションとバックエンドのWeb APIを持つことになります。Webアプリは、顧客調査の更新を処理するためにWeb APIに依存します。

SaaSアプリケーションの承認フロー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。

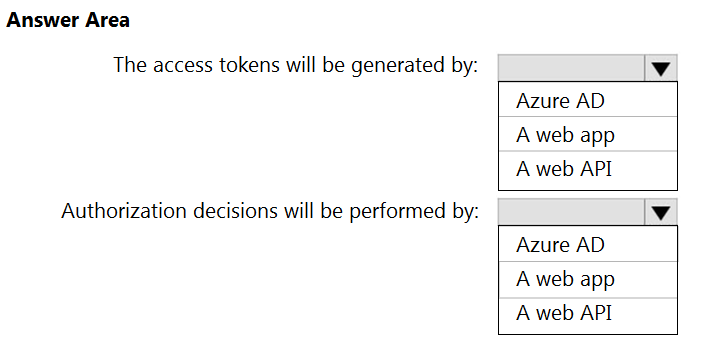
* バックエンドWeb APIにアクセスするには、WebアプリがOAuth2ベアラートークンを使用して認証する必要があります。
* Webアプリは、個々のユーザーのIDを使用して認証する必要があります。

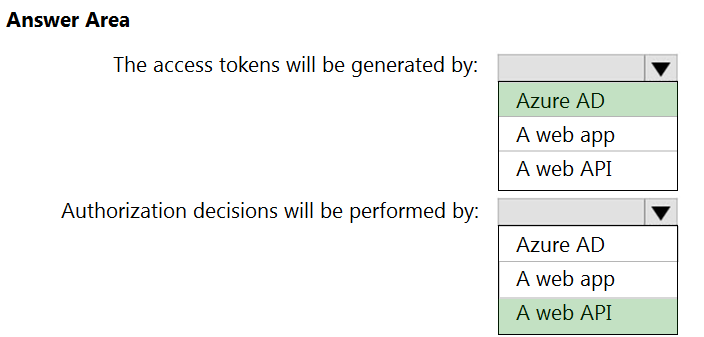
ソリューションに何を含める必要がありますか？

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：



正解： 

参照：

<https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-dotnet-webapi>

# Q.60

Azure Active Directory（Azure AD）のハイブリッド展開があります。

オンプレミスネットワーク上のコンピューターからのみAzure ADテナントを管理できるようにする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. 条件付きアクセスポリシー
2. Azure ADの役割と管理者
3. Azure ADアプリケーションプロキシ
4. Azure ADの特権ID管理

正解： *A*