Microsoft.AZ-500.v2019-08-20.q27

試験コード：	AZ-500
試験名称：	Microsoft Azure Security Technologies
認証ベンダー：	Microsoft
無料問題の数：	27
バージョン：	v2019-08-20
ページの閲覧量：	1845
問題集の閲覧量：	14077

https://www.jpnshiken.com/shiken/Microsoft.AZ-500.v2019-08-20.q27.html

質問: **1**
Azure Active Directory（Azure AD）のハイブリッド構成があります。
すべてのユーザーがWindows 10を実行し、ハイブリッドAzure ADに参加しているコンピューターを所有しています。
Azure AD認証をサポートするように構成されたAzure SQLデータベースがあります。
データベース開発者は、Microsoft SQL Server Managementを使用してSQLデータベースに接続する必要があります。
スタジオ（SSMS）で、社内のActive Directoryアカウントを使用して認証します。
SQLデータベースへの接続に使用する認証方法を開発者に知らせる必要があります。
SSMS解決策は認証プロンプトを最小限にする必要があります。
どの認証方法を使用するよう開発者に指示しますか？
A. SQLログイン
B. Active Directory - MFAをサポートするユニバーサル
C. Active Directory - 統合
D. Active Directory - パスワード
正解: **C** (コメントを発表する)
説明/参照：
Explanation:
Azure ADを最初のAzure AD管理ドメインにすることができます。Azure ADは、オンプレミスアクティブにすることもできます。
Azure ADとフェデレーションされているディレクトリドメインサービス。
Azure AD IDを使用してSSMSまたはSSDTを使用して接続する
次の手順では、Azure ADのIDを使用してSQLデータベースに接続する方法を示します。
SQL Server Management StudioまたはSQL Serverデータベースツール。
Active Directory統合認証
WindowsのAzure Active Directory認証情報を使用してWindowsにログインしている場合は、この方法を使用します。
フェデレーションドメイン

1. Management StudioまたはData Toolsを起動し、[サーバーに接続] または[データベースエンジンに接続]）で起動します。
ダイアログボックスの 認証」ボックスで、 Active Directory - 統合」を選択します。パスワードは不要です
接続に対して既存の資格情報が提示されるため、入力してください。
2. [オプション]ボタンを選択し、[接続プロパティ]ページの[データベースへの接続]ボックスに、次のように入力します。
接続したいユーザーデータベースの名前。 ADドメイン名またはテナントID」オプションは
ユニバーサルはMFA接続オプション付きでサポートされています。
参考文献：
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-
authentication-configure.md
AZ-500
AZ-500
テストレット1
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます
各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。
ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。
このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。左ペインのボタンを使用して

質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。
質問。
概要
Litware、Inc.は、シカゴ地域に500人の従業員と20人に20人の従業員を擁するデジタルメディア企業です。
サンフランシスコ周辺
既存の環境
LitwareにはSub1というAzureサブスクリプションがあり、そのサブスクリプションIDは43894a43-17c2-4a39-8cfc-です。
3540c2653ef4。
Sub1は、litwareinc.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられています。テナント
Litwareの全従業員とそのデバイスのユーザオブジェクトとデバイスオブジェクトが含まれています。各ユーザー
Azure AD Premium P2ライセンスが割り当てられています。Azure ADの特権ID管理（PIM）は
起動しました。
テナントには、以下の表に示すグループが含まれています。
Azureサブスクリプションには、次の表に示すオブジェクトが含まれています。
Azure Security Centerが無料利用枠に設定されています。
計画された変更
Litwareは、次の表に示すAzureリソースをデプロイする予定です。
Litwareは、以下のアイデンティティおよびアクセス要件を識別します。
すべてのサンフランシスコのユーザーとそのデバイスは、Group1のメンバーでなければなりません。
Group2のメンバーには、以下を使用して、リソースGroup2へのContributorの役割を割り当てる必要があります。
永久的な適格な割り当て。
ユーザーがAzure ADにアプリケーションを登録したり、アプリケーションに同意したりできないようにする必要があります。
ユーザーに代わって会社の情報にアクセスします。
プラットフォーム保護要件
Litwareは、以下のプラットフォーム保護要件を識別しています。

Microsoftマルウェア対策ソフトウェアは、リソースグループ1の仮想マシンにインストールする必要があります。
Group2のメンバーには、Azure Kubernetesサービスクラスター管理者の役割を割り当てる必要があります。
Azure ADユーザーは、Azure ADの資格情報を使用してAKS1に認証される必要があります。
計画された変更の実施に続いて、ITチームは次のようにしてVM0に接続できなければなりません。
JIT VMアクセスを使用します。
Role1という名前の新しいカスタムRBACロールを使用して、管理対象の管理を委任する必要があります。
リソースグループ1のディスク。ロール1はリソースグループ1に対してのみ使用可能でなければなりません。
セキュリティ運用要件
LitwareはAzure Security Centerでオペレーティングシステムのセキュリティ構成をカスタマイズできる必要があります。

質問: **2**
セキュリティ運用要件を確実に満たすことができるようにする必要があります。
あなたは最初に何をすべきですか？
A. セキュリティセンターで自動プロビジョニングを有効にします。
B. セキュリティセンターとMicrosoftクラウドアプリセキュリティを統合します。
C. セキュリティセンターの価格帯を標準にアップグレードします。
D. セキュリティセンターのワークスペース設定を変更します。
正解: **C** (コメントを発表する)
説明/参照：
Explanation:
Standard層は、Free層の機能をプライベートおよびその他のパブリックで実行されているワークロードに拡張します。
クラウドにより、ハイブリッドクラウドワークロード全体で統一されたセキュリティ管理と脅威からの保護を提供
Standard層には、組み込みの行動分析を使用する高度な脅威検出機能も追加されています。
攻撃とゼロデイエクスプロイト、アクセスとアプリケーションの制御を軽減するための機械学習
ネットワーク攻撃やマルウェアへの暴露など。
シナリオ :セキュリティ運用要件
LitwareはAzure Security Centerでオペレーティングシステムのセキュリティ構成をカスタマイズできる必要があります。

参考文献：
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing
質問セット3

質問: **3**
User2がPIMを実装できるようにする必要があります。
あなたは最初に何をすべきですか？
A. User2にグローバル管理者ロールを割り当てます。
B. contoso.comの認証方法を構成します。
C. contoso.comのID保護スコアを構成します。
D. User2の多要素認証（MFA）を有効にします。
正解: **A (**コメントを発表する**)**
説明/参照：
Explanation:
ディレクトリでPIMを使い始めるには、まずPIMを有効にする必要があります。
1.ディレクトリのグローバル管理者としてAzureポータルにサインインします。
組織アカウント（@ yourdomain.comなど）を持つグローバル管理者である必要があります。
ディレクトリに対してPIMを有効にするためのMicrosoftアカウント（たとえば、@ outlook.com）。
シナリオ：技術的な要件は次のとおりです。Azure AD特権ID管理（PIM）を有効にする
contoso.com
参考文献：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-
始まった
質問セット3

質問: **4**
Azure仮想マシンを展開するために使用するAzure Resource Managerテンプレートがあります。
仮想マシンのインスタンスは自動的に無効になるため、未使用のWindows機能を自動的に無効にする必要があります。
プロビジョニング済み
あなたは何を使うべきですか？
A. Microsoft Intuneのデバイスコンプライアンスポリシー
B. Azure Automationの状態構成
C. アプリケーションセキュリティグループ
D. Azure Advisor
正解: **(**正解を表示します**)**

説明/参照：
Explanation:
Azure Automation State Configurationを使用して、Azure VM（クラシックとリソースの両方）を管理できます。
マネージャ）、オンプレミスVM、Linuxマシン、AWS VM、およびオンプレミス物理マシン。
注：Azure Automation State Configurationは、Windows機能と同様のDSCプルサーバーを提供します。
ターゲットノードが自動的に設定を受信し、目的の状態に準拠するようにDSCサービス
彼らのコンプライアンスについて報告する。Azure Automationの組み込みプルサーバーにより、セットアップする必要がなくなります。
そしてあなた自身のpullサーバを保守します。Azure Automationは、仮想または物理のWindowsまたはLinuxをターゲットにすることができます。
クラウド、オンプレミスなどのマシン。
参考文献：
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

質問: **5**
Group1のIDとアクセスの要件を満たす必要があります。
あなたは何をするべきか？
A. Group1にメンバシップの規則を追加します。
B. Group1を削除します。Office 365のメンバシップの種類を持つGroup1という名前の新しいグループを作成します。追加
ユーザーとデバイスをグループに追加します。
C. Group1のメンバーシップ規則を変更します。
D. Group1のメンバーシップの種類を[割り当て済み]に変更します。動的なグループを2つ作成します。
メンバーシップ新しいグループをGroup1に追加します。
正解: **B** (コメントを発表する)
説明/参照：
Explanation:
間違った答え：
A、C：デバイス用またはユーザー用の動的グループを作成できますが、次のものを含むルールを作成することはできません。
ユーザーとデバイスの両方
D：割り当てられたグループには、個々のメンバーを追加することしかできません。
シナリオ：
Litwareは、以下のIDおよびアクセス要件を識別しています。サンフランシスコのすべてのユーザーとそのデバイス
Group1のメンバーである必要があります。
テナントには現在このグループが含まれています。

参考文献：
https://docs.microsoft.com/ja-jp/azure/active-directory / users-groups-ロール/ groups-dynamic -membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-
ポータル
テストレット2
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます
各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。
ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。
このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。
左ペインのボタンを使用して
質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。
質問。
概要
Contoso、Ltd.は、モントリオールに本社、シアトルに2つの支店を持つコンサルティング会社です。
そしてニューヨーク。

同社はAzureでサーバーインフラストラクチャ全体をホストしています。
Contosoには、Sub1とSub2という2つのAzureサブスクリプションがあります。両方のサブスクリプションは
contoso.comという名前のAzure Active Directory（Azure AD）テナント。
技術要件
Contosoでは、次の技術的要件を確認しています。
Sub2のVNetWork1にAzureファイアウォールを展開します。
contoso.comにApp2という名前のアプリケーションを登録します。
可能な限り、最小限の特権の原則を使用してください。
contoso.comでAzure ADの特権ID管理（PIM）を有効にする
既存の環境
Azure AD
Contoso.comには、次の表に示すユーザーが含まれています。
Contoso.comには、次の表に示すセキュリティグループが含まれています。
Sub1
Sub1には、RG1、RG2、RG3、RG4、RG5、およびRG6という名前の6つのリソースグループが含まれています。
ユーザー2は、次の表に示す仮想ネットワークを作成します。
Sub1には、次の表に示すロックが含まれています。
Sub1には、次の表に示すAzureポリシーが含まれています。
Sub2
Sub2には、次の表に示す仮想マシンが含まれています。
すべての仮想マシンにパブリックIPアドレスとWebサーバー（IIS）の役割がインストールされています。のファイアウォール
各仮想マシンはping要求とWeb要求を許可します。
Sub2には、次の表に示すネットワークセキュリティグループ（NSG）が含まれています。
NSG1には、次の表に示すインバウンドセキュリティ規則があります。
NSG2には、次の表に示すインバウンドセキュリティ規則があります。
NSG3には、次の表に示すインバウンドセキュリティ規則があります。
NSG4には、次の表に示すインバウンドセキュリティ規則があります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示す発信セキュリティ規則があります。
Contosoでは、次の技術的要件を確認しています。
Sub2のVNetwork1にAzureファイアウォールを展開します。
contoso.comにApp2という名前のアプリケーションを登録します。
可能な限り、最小限の特権の原則を使用してください。
contoso.comに対してAzure AD特権ID管理（PIM）を有効にします。

質問: **6**

ユーザーがVM0にアクセスできることを確認する必要があります。ソリューションはプラットフォーム保護を満たす必要があります
必要条件
あなたは何をするべきか？
A. VM0をSubnet1に移動します。
B. ファイアウォールで、ネットワークトラフィックフィルタリングルールを設定します。
C. AzureFirewallSubnetにRT1を割り当てます。
D. ファイアウォールで、DNATルールを設定します。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
Azureファイアウォールには、次の既知の問題があります。
Azure Security Center（ASC）のジャストインタイム（JIT）機能と競合します。
仮想マシンがJITを使用してアクセスされ、Azureを指すユーザー定義のルートを持つサブネット内にある場合
デフォルトゲートウェイとしてのファイアウォール、ASC JITは機能しません。これは非対称ルーティングの結果です - パケット
仮想マシンのパブリックIP経由で入ってきます（JITがアクセスを開きました）が、戻りパスはファイアウォール経由です。
ファイアウォール上に確立されたセッションがないため、これはパケットをドロップします。
解決策 :この問題を回避するには、JIT仮想マシンを、存在しない別のサブネットに配置します。
ファイアウォールへのユーザー定義の経路。
シナリオ：
計画された変更の実施に続いて、ITチームは次のようにしてVM0に接続できなければなりません。
JIT VMアクセスを使用します。
参考文献：
https://docs.microsoft.com/en-us/azure/firewall/overview
テストレット2
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます
各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。

ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。
このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。
左ペインのボタンを使用して
質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。
質問。
概要
Contoso、Ltd.は、モントリオールに本社、シアトルに2つの支店を持つコンサルティング会社です。
そしてニューヨーク。
同社はAzureでサーバーインフラストラクチャ全体をホストしています。
Contosoには、Sub1とSub2という2つのAzureサブスクリプションがあります。両方のサブスクリプションは
contoso.comという名前のAzure Active Directory（Azure AD）テナント。
技術要件
Contosoでは、次の技術的要件を確認しています。
Sub2のVNetWork1にAzureファイアウォールを展開します。
contoso.comにApp2という名前のアプリケーションを登録します。
可能な限り、最小限の特権の原則を使用してください。
contoso.comでAzure ADの特権ID管理（PIM）を有効にする
既存の環境
Azure AD
Contoso.comには、次の表に示すユーザーが含まれています。

Contoso.comには、次の表に示すセキュリティグループが含まれています。
Sub1
Sub1には、RG1、RG2、RG3、RG4、RG5、およびRG6という名前の6つのリソースグループが含まれています。
ユーザー2は、次の表に示す仮想ネットワークを作成します。
Sub1には、次の表に示すロックが含まれています。
Sub1には、次の表に示すAzureポリシーが含まれています。
Sub2
Sub2には、次の表に示すネットワークセキュリティグループ（NSG）が含まれています。
NSG1には、次の表に示すインバウンドセキュリティ規則があります。
NSG2には、次の表に示すインバウンドセキュリティ規則があります。
NSG3には、次の表に示すインバウンドセキュリティ規則があります。
NSG4には、次の表に示すインバウンドセキュリティ規則があります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示す発信セキュリティ規則があります。
Contosoでは、次の技術的要件を確認しています。
Sub2のVNetwork1にAzureファイアウォールを展開します。
contoso.comにApp2という名前のアプリケーションを登録します。
可能な限り、最小限の特権の原則を使用してください。
contoso.comに対してAzure AD特権ID管理（PIM）を有効にします。
質問セット3

質問: **7**
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。各質問
シリーズの中には、述べられた目標を満たすかもしれないユニークな解決策が含まれています。いくつかの質問セット
他の人は正しい解決策を持っていないかもしれませんが1つ以上の正しい解決策があるかもしれません。
このセクションで質問に答えた後は、それに戻ることはできません。その結果、
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 Storageアカウントがあります。
ユーザーとアプリケーションは、複数の共有アクセスを使用してSa1のBLOBサービスとファイルサービスにアクセスします。
署名（SAS）および保存されたアクセスポリシー。
あなたは、権限のないユーザ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を発見しました。
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？
A. はい
B. いいえ
正解: **B** (コメントを発表する)
説明/参照：
Explanation:
代わりに、新しいストアドアクセスポリシーを作成する必要があります。
保存されているアクセスポリシーを取り消すには、それを削除するか、署名付き識別子を変更して名前を変更します。
署名付き識別子を変更すると、既存の署名と保存されている署名との関連付けが解除されます。
アクセスポリシー保存されているアクセスポリシーを削除または名前変更すると、すべての共有アクセスに即座に影響する
それに関連付けられている署名。
参考文献：
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

質問: **8**
Sub1という名前のAzureサブスクリプションがあります。
Azure Security Centerには、Play1という名前のセキュリティプレイブックがあります。
Play1はEメールを送信するように設定されています
User1という名前のユーザーへのメッセージ。
電子メールメッセージをAlertsという名前の配布グループに送信するようにPlay1を変更する必要があります。
Play1を修正するために何を使うべきですか？
A. Azure DevOps
B. Azure Application Insights
C. Azure Monitor
D. Azure Logic Appsデザイナー
正解: (正解を表示します)
説明/参照：
Explanation:
Security Centerの既存のプレイブックを変更して、アクションや条件を追加することができます。それをするにはあなただけ
PlaybookタブでLogic Appを変更したいプレイブックの名前をクリックする必要があります。
デザイナーが開きます。
参考文献：
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

質問: **9**
会社には、Azure Active Directory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。
contoso.comという名前のAzure（Azure AD）テナント。
同社はApp1という名前のモバイルアプリケーションを開発しています。App1はOAuth 2暗黙付与タイプを使用して
Azure ADアクセストークンを取得します。
App1をAzure ADに登録する必要があります。
アプリケーションを登録するために開発者からどのような情報を入手する必要がありますか？
A. リダイレクトURI
B. 返信URL
C. キー
D. アプリケーションID
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
ネイティブアプリケーションの場合は、Azure ADがトークンを返すために使用するリダイレクトURIを提供する必要があります。
反応。
参考文献：
https://docs.microsoft.com/ja-jp/azure/active- directory / developer / v1-protocol-oauth-code

質問: **10**
Sub1という名前のAzureサブスクリプションがあります。Sub1には、VNet1という名前の仮想ネットワークが含まれています。
Subnet1という名前のサブネット。
Subnet1のサービスエンドポイントを作成します。
Subnet1には、Ubuntu Server 18.04を実行するVM1という名前のAzure仮想マシンが含まれています。
DockerコンテナーをVM1にデプロイする必要があります。コンテナーはAzure Storageにアクセスできる必要があります
サービスエンドポイントを使用して、リソースとAzure SQLデータベースを作成します。
A. アプリケーションセキュリティグループとネットワークセキュリティグループ（NSG）を作成します。
B. docker-compose.ymlファイルを編集します。
C. Container Network Interface（CNI）プラグインをインストールします。
正解: **(**正解を表示します**)**
説明/参照：

Explanation:
Azure Virtual Networkコンテナーネットワークインターフェイス（CNI）プラグイン
は、Azure Virtual Machineにインストールされます。
このプラグインは、LinuxとWindowsの両方のプラットフォームをサポートしています。
プラグインは、仮想ネットワークからIPアドレスを仮想マシンで起動されたコンテナに割り当てます。
それらを仮想ネットワークに接続し、それらを他のコンテナーおよび仮想ネットワークに直接接続する
リソースプラグインは、接続のためにオーバーレイネットワークやルートに依存せず、同じ機能を提供します。
仮想マシンとしてのパフォーマンス。
次の図は、プラグインがどのようにしてAzure Virtual Network機能をPodに提供するかを示しています。
参考文献：
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

質問: **11**
Sub1という名前のAzureサブスクリプションに、Azure Log Analyticsワークスペースという名前のワークスペースが含まれているとします。
LAW1。
Windows Server 2012 R2およびWindows Server 2016を実行する100台のオンプレミスサーバーがあります。
サーバーはLAW1に接続します。LAW1は、セキュリティ関連のパフォーマンスカウンタをコンピュータから収集するように設定されています。
接続サーバー
LAW1によって収集されたデータに基づいてアラートを設定する必要があります。解決策は次の条件を満たす必要があります。
必要条件
アラートルールはディメンションをサポートしている必要があります。
アラートの生成にかかる時間は最小限に抑える必要があります。
アラート通知は、アラートが生成されたときとアラートが生成されたときに1回だけ生成する必要があります。
解決しました。
アラートルールを作成するときにはどの信号タイプを使用しますか？
A. ログ
B. ログ（保存されたクエリ）
C. メートル法
D. アクティビティログ
正解: **C** (コメントを発表する)
説明/参照：

Explanation:
Azureモニターのメトリックスアラートは、いずれかのメトリックスがしきい値を超えたときに通知を受ける方法を提供します。
メトリックアラートは、さまざまな多次元プラットフォームメトリック、カスタムメトリック、Application Insightsで機能します。
標準およびカスタムメトリクス
注 :シグナルはターゲットリソースによって発行され、いくつかの種類があります。メトリック、アクティビティログ、
アプリケーションインサイト、およびログ
参考文献：
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric
テストレット1
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます
各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。
ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。
このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。
左ペインのボタンを使用して
質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。

質問。
概要
Litware、Inc.は、シカゴ地域に500人の従業員と20人に20人の従業員を擁するデジタルメディア企業です。
サンフランシスコ周辺
既存の環境
LitwareにはSub1というAzureサブスクリプションがあり、そのサブスクリプションIDは43894a43-17c2-4a39-8cfc-です。
3540c2653ef4。
Sub1は、litwareinc.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられています。テナント
Litwareの全従業員とそのデバイスのユーザオブジェクトとデバイスオブジェクトが含まれています。各ユーザー
Azure AD Premium P2ライセンスが割り当てられています。Azure ADの特権ID管理（PIM）は
起動しました。
テナントには、以下の表に示すグループが含まれています。
Azureサブスクリプションには、次の表に示すオブジェクトが含まれています。
Azure Security Centerが無料利用枠に設定されています。
計画された変更
Litwareは、次の表に示すAzureリソースをデプロイする予定です。
Litwareは、以下のアイデンティティおよびアクセス要件を識別します。
すべてのサンフランシスコのユーザーとそのデバイスは、Group1のメンバーでなければなりません。
Group2のメンバーには、以下を使用して、リソースGroup2へのContributorの役割を割り当てる必要があります。
永久的な適格な割り当て。
ユーザーがAzure ADにアプリケーションを登録したり、アプリケーションに同意したりできないようにする必要があります。
ユーザーに代わって会社の情報にアクセスします。
プラットフォーム保護要件
Litwareは、以下のプラットフォーム保護要件を識別しています。
Microsoftマルウェア対策ソフトウェアは、リソースグループ1の仮想マシンにインストールする必要があります。
Group2のメンバーには、Azure Kubernetesサービスクラスター管理者の役割を割り当てる必要があります。
Azure ADユーザーは、Azure ADの資格情報を使用してAKS1に認証される必要があります。

計画された変更の実施に続いて、ITチームは次のようにしてVM0に接続できなければなりません。
JIT VMアクセスを使用します。
Role1という名前の新しいカスタムRBACロールを使用して、管理対象の管理を委任する必要があります。
リソースグループ1のディスク。ロール1はリソースグループ1に対してのみ使用可能でなければなりません。
セキュリティ運用要件
LitwareはAzure Security Centerでオペレーティングシステムのセキュリティ構成をカスタマイズできる必要があります。

質問: **12**
Azureサブスクリプションを持っています。
S1 Appサービスプランを使用するContoso1812という名前のAzure Webアプリを作成します。
Contoso1812のIPアドレスを指すwww.contoso.comのDNSレコードを作成します。
https://www.contoso.comの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？それぞれの正しい答えは解決策の一部を表しています。
注 :それぞれ正しい選択は1ポイントの価値があります。
A. Contoso 1812のシステム割り当て管理IDをオンにします。
B. Contoso 1812にホスト名を追加します。
C. Contoso 1812のApp Service計画をスケールアウトします。
D. Contoso 1812に展開スロットを追加します。
E. Contoso 1812のApp Serviceプランを拡大します。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
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、あなたは作成することができます
Azure Webアプリを作成し、www.contoso.comまたはcontoso.comのいずれかを使用してユーザーにアクセスさせます。
修飾ドメイン名（FQDN）。
これを行うには、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

E :カスタムDNS名をWebアプリにマッピングするには、WebアプリのApp Serviceプランを有料層にする必要があります（共有
Azure機能の基本、標準、プレミアム、または消費量）。私
App Serviceプランをスケールアップする :フリーではない層 D1、B1、B2、B3、またはその中の任意の層）を選択します。
製造カテゴリ）
参考文献：
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain
テストレット1
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます
各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。
ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。
このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。
左ペインのボタンを使用して
質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。
質問。
概要

Litware、Inc.は、シカゴ地域に500人の従業員と20人に20人の従業員を擁するデジタルメディア企業です。
サンフランシスコ周辺
既存の環境
LitwareにはSub1というAzureサブスクリプションがあり、そのサブスクリプションIDは43894a43-17c2-4a39-8cfc-です。
3540c2653ef4。
Sub1は、litwareinc.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられています。テナント
Litwareの全従業員とそのデバイスのユーザオブジェクトとデバイスオブジェクトが含まれています。各ユーザー
Azure AD Premium P2ライセンスが割り当てられています。Azure ADの特権ID管理（PIM）は
起動しました。
テナントには、以下の表に示すグループが含まれています。
Azureサブスクリプションには、次の表に示すオブジェクトが含まれています。
Azure Security Centerが無料利用枠に設定されています。
計画された変更
Litwareは、次の表に示すAzureリソースをデプロイする予定です。
Litwareは、以下のアイデンティティおよびアクセス要件を識別します。
すべてのサンフランシスコのユーザーとそのデバイスは、Group1のメンバーでなければなりません。
Group2のメンバーには、以下を使用して、リソースGroup2へのContributorの役割を割り当てる必要があります。
永久的な適格な割り当て。
ユーザーがAzure ADにアプリケーションを登録したり、アプリケーションに同意したりできないようにする必要があります。
ユーザーに代わって会社の情報にアクセスします。
プラットフォーム保護要件
Litwareは、以下のプラットフォーム保護要件を識別しています。
Microsoftマルウェア対策ソフトウェアは、リソースグループ1の仮想マシンにインストールする必要があります。
Group2のメンバーには、Azure Kubernetesサービスクラスター管理者の役割を割り当てる必要があります。
Azure ADユーザーは、Azure ADの資格情報を使用してAKS1に認証される必要があります。
計画された変更の実施に続いて、ITチームは次のようにしてVM0に接続できなければなりません。
JIT VMアクセスを使用します。

Role1という名前の新しいカスタムRBACロールを使用して、管理対象の管理を委任する必要があります。
リソースグループ1のディスク。ロール1はリソースグループ1に対してのみ使用可能でなければなりません。
セキュリティ運用要件
LitwareはAzure Security Centerでオペレーティングシステムのセキュリティ構成をカスタマイズできる必要があります。

質問: **13**
あなたの会社は部門ごとに別々の購読を作成する予定です。各サブスクリプションはなります
同じAzure Active Directory（Azure AD）テナントに関連付けられている。
各役割を同じ役割に割り当てるように設定する必要があります。
あなたは何を使うべきですか？
A. Azureセキュリティセンター
B. Azure Blueprints
C. Azure ADの特権ID管理（PIM）
D. Azureのポリシー
正解: **C** (コメントを発表する)
説明/参照：
Explanation:
Azure ADの特権ID管理（PIM）サービスでも、特権ロール管理者は次のことができます。
恒久的な管理者ロールの割り当てを行います。
参考文献：
https://docs.microsoft.com/ja-jp/azure/active- directory / prrivileged-identity-management / pim-how-to-add-
ユーザーへの役割

質問: **14**
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。各質問
シリーズの中には、述べられた目標を満たすかもしれないユニークな解決策が含まれています。いくつかの質問セット
他の人は正しい解決策を持っていないかもしれませんが1つ以上の正しい解決策があるかもしれません。
このセクションで質問に答えた後は、それに戻ることはできません。その結果、
質問はレビュー画面に表示されません。
Azure Active Directory（AzureAD）のハイブリッド構成があります。
仮想ネットワーク上にAzure HDInsightクラスターがあります。
オンプレミスのActive Directoryを使用して、ユーザーにクラスターへの認証を許可することを計画している

資格情報。
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。
解決方法 :オンプレミスデータゲートウェイをオンプレミスネットワークに展開します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
代わりに、Azure Virtual NetworksとVPNを使用してHDInsightをオンプレミスネットワークに接続します。
ゲートウェイ。
注意 :HDInsightと参加ネットワークのリソースが名前で通信できるようにするには、次の手順を実行する必要があります。
以下のアクション
Azure Virtual Networkを作成します。
Azure Virtual Networkにカスタムdnsサーバーを作成します。
既定のAzure Recursive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。
リゾルバ。
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。
参考文献：
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

質問: **15**
Azureポータルから、Azureポリシーを構成しています。
DeployIfNotExist、AuditIfNotExist、Append、およびDenyを使用するポリシーを割り当てる予定です。
効果
割り当てに管理対象IDが必要なのはどの効果ですか。
A. AuditIfNotExist
B. 追加
C. DeployIfNotExist
D. 拒否
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
Azure PolicyがdeployIfNotExistsポリシー定義内のテンプレートを実行するときには、マネージドを使用します。
身元。

参考文献：
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

質問: **16**
Vault1という名前のAzure Key Vaultを含むAzureサブスクリプションがあります。
Vault1では、Secret1という名前の秘密を作成します。
アプリケーション開発者がAzure Active Directory（Azure AD）にアプリケーションを登録します。
アプリケーションがSecret1を使用できるようにする必要があります。
あなたは何をするべきか？
A. Azure ADで役割を作成します。
B. Azure Key Vaultでキーを作成します。
C. Azure Key Vaultでアクセスポリシーを作成します。
D. Azure ADで、Azure ADアプリケーションプロキシを有効にします。
正解: **(正解を表示します)**
説明/参照：
Explanation:
Azure Key Vaultは、資格情報やその他のキーと秘密を安全に保存する方法を提供します。
それらを取得するには、Key Vaultに認証する必要があります。
Azureリソースの概要の管理対象IDを使用することで、Azureを提供することで、この問題の解決が簡単になります。
Azure Active Directory（Azure AD）の自動管理されたIDを処理します。あなたはこのアイデンティティを使うことができます
Key Vaultを含め、Azure AD認証をサポートするすべてのサービスに対する認証を受けることなく
コード内の資格情報
例 :システム割り当ての管理対象IDとAzure VMの連携方法
VMにIDが割り当てられたら、サービスプリンシパル情報を使用してVMにAzureへのアクセスを許可します。
リソース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）を使用して割り当てます。
VMサービスプリンシパルに対する適切な役割Key Vaultを呼び出すには、特定のユーザーにコードアクセス権を付与します。
Key Vaultの秘密鍵。
参考文献：
https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net
https://docs.microsoft.com/ja-jp/azure/active-directory/managed-identities-azure-resources/overview

質問: **17**
Azure SQLデータベースがあります。
Always Encryptedを実装します。
アプリケーション開発者がデータベース内のデータを取得および復号化できるようにする必要があります。
どの2つの情報を開発者に提供しますか？それぞれの正しい答えは部分を表します
ソリューションの。
注 :それぞれ正しい選択は1ポイントの価値があります。
A. 保存されているアクセスポリシー
B. 共有アクセス署名 $AS）
C. 列暗号化キー
D. ユーザー認証情報
E. 列マスタキー
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
Always Encryptedでは、列暗号化キーと列マスターキーの2種類のキーを使用します。コラム
暗号化キーは、暗号化列のデータを暗号化するために使用されます。列マスターキーはキー保護です
1つ以上の列暗号化キーを暗号化するキー。
参考文献：
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-
エンジン

質問: **18**
新しいAzureサブスクリプションを作成します。
Azure Security Centerでカスタムアラートルールを作成できることを確認する必要があります。
どの2つのアクションを実行する必要がありますか？それぞれの正しい答えは解決策の一部を表しています。
注 :それぞれ正しい選択は1ポイントの価値があります。

A. オンボードAzure Active Directory（Azure AD）ID保護。
B. Azure Storageアカウントを作成します。
C. Azure Advisorの推奨事項を実装する
D. Azure Log Analyticsワークスペースを作成します。
E. セキュリティセンターの価格帯を標準にアップグレードします。
正解: **B,D** (コメントを発表する)
説明/参照：
Explanation:
D :カスタムアラートを保存するために選択したワークスペースへの書き込み権限が必要です。
参考文献：
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

質問: **19**
ネットワークにcontoso.comという名前のActive Directory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。
Azure Active Directory（Azure AD）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。
contoso.comという名前のテナント。
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。
パスワードポリシーとユーザーログオン制限が、同期されるユーザーアカウントに適用されるようにします。
テナント
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べきですか。
A. Active Directoryフェデレーションサービス（AD FS）とのフェデレーションID
B. シームレスシングルサインオン（SSO）によるパスワードハッシュの同期
C. シームレスシングルサインオン（SSO）によるパススルー認証
正解: (正解を表示します)
説明/参照：
Explanation:
パスワードハッシュ同期では、展開、メンテナンス、および
インフラ。このレベルの作業は通常、ユーザーにサインインするだけでよい組織に適用されます。
Office 365、SaaSアプリ、およびその他のAzure ADベースのリソース。オンにすると、パスワードハッシュ
同期はAzure AD Connectの同期プロセスの一部であり、2分ごとに実行されます。
間違った答え：

A：連合認証システムは、ユーザーを認証するために外部の信頼できるシステムに依存しています。一部
企業は既存のフェデレーションシステムへの投資をAzure ADのハイブリッドIDで再利用したい
溶液。フェデレーションシステムのメンテナンスと管理はAzure ADの管理外です。
それが安全に展開されることを確実にするために連合システムを使用することによって組織次第です。
認証負荷を処理します。
C：パススルー認証には、1つ以上（3つ推奨）の軽量エージェントが必要です
既存のサーバーにインストールされています。これらのエージェントは、オンプレミスのActive Directoryにアクセスできる必要があります。
オンプレミスのADドメインコントローラを含むドメインサービス。彼らはへのアウトバウンドアクセスが必要です
インターネットとドメインコントローラへのアクセスこのため、エージェントをエージェントに展開することはサポートされていません。
境界ネットワーク。
パススルー認証には、ドメインコントローラへの制限のないネットワークアクセスが必要です。全ネットワーク
トラフィックは暗号化され、認証要求に限定されます。
参考文献：
https://docs.microsoft.com/ja-jp/azure/active- directory / hybrid / how-to-connect-pta

質問: **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。各質問
シリーズの中には、述べられた目標を満たすかもしれないユニークな解決策が含まれています。いくつかの質問セット
他の人は正しい解決策を持っていないかもしれませんが1つ以上の正しい解決策があるかもしれません。
このセクションで質問に答えた後は、それに戻ることはできません。その結果、
質問はレビュー画面に表示されません。
Azure Active Directory（AzureAD）のハイブリッド構成があります。
仮想ネットワーク上にAzure HDInsightクラスターがあります。
オンプレミスのActive Directoryを使用して、ユーザーにクラスターへの認証を許可することを計画している
資格情報。
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？
A. はい
B. いいえ

正解: **A** (コメントを発表する)
説明/参照：
Explanation:
Azure Virtual NetworksとVPNを使用して、HDInsightをオンプレミスネットワークに接続できます。
ゲートウェイ。
注意 :HDInsightと参加ネットワークのリソースが名前で通信できるようにするには、次の手順を実行する必要があります。
以下のアクション
Azure Virtual Networkを作成します。
Azure Virtual NetworkにカスタムDNSサーバーを作成します。
既定のAzure Recursive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。
リゾルバ。
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。
参考文献：
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

質問: **21**
Azure Containerに接続するAzure Kubernetes Service（AKS）クラスターを構成していますレジストリ
Azure Container Registryへの認証には、自動生成されたサービスプリンシパルを使用する必要があります。
何を作るべきですか？
A. Azure Active Directory（Azure AD）グループ
B. Azure Active Directory（Azure AD）の役割の割り当て
C. Azure Active Directory（Azure AD）ユーザー
D. Azure Key Vaultの秘密
正解: (正解を表示します)
説明/参照：
Explanation:
AKSクラスターを作成すると、Azureはクラスターの操作性をサポートするサービスプリンシパルも作成します。
その他のAzureリソースこの自動生成されたサービスプリンシパルをACRによる認証に使用できます。
レジストリ。これを行うには、クラスターのサービスを付与するAzure ADの役割の割り当てを作成する必要があります。
コンテナレジストリへのプリンシパルアクセス
参考文献：
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

質問: **22**
次の表に示すAzure仮想マシンがあります。
米国東部地域のRG1にAnalytics1というAzure Log Analyticsワークスペースを作成します。
Analytics1に登録できる仮想マシンはどれですか。
A. VM1のみ
B. VM1、VM2、およびVM3のみ
C. VM1、VM2、VM3、およびVM4
D. VM1とVM4のみ
正解: **A** (コメントを発表する)
説明/参照：
Explanation:
注意 :ワークスペースを作成する
Azureポータルで、[すべてのサービス]をクリックします。リソースの一覧にLog Analytics と入力します。入力を始めると、
リストは入力に基づいてフィルタリングします。ログ分析を選択します。
「作成」をクリックしてから、以下の項目の選択肢を選択します。
DefaultLAWorkspaceなど、新しいLog Analyticsワークスペースの名前を入力します。OMS ワークスペース
Log Analyticsワークスペースと呼ばれるようになりました。
選択されているデフォルトがそうでない場合は、ドロップダウンリストから選択してリンク先の購読を選択します。
適切な。
[リソースグループ]で、1つ以上のAzure仮想マシンを含む既存のリソースグループを選択します。
VMが展開されている場所を選択します。追加情報については、どの領域のLog Analyticsを参照してください。
で利用可能です。
間違った答え：
B、C :Log Analyticsワークスペースは、データを保存するための地理的な場所を提供します。VM2とVM3は
別の場所
D :VM4は別のリソースグループです。
参考文献：
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access
トピック3、セキュリティ運用を管理する
テストレット1
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます

各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。
ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。
このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。
左ペインのボタンを使用して
質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。
質問。
概要
Contoso、Ltd.は、モントリオールに本社、シアトルに2つの支店を持つコンサルティング会社です。
そしてニューヨーク。
同社はAzureでサーバーインフラストラクチャ全体をホストしています。
Contosoには、Sub1とSub2という2つのAzureサブスクリプションがあります。両方のサブスクリプションは
contoso.comという名前のAzure Active Directory（Azure AD）テナント。
技術要件
Contosoでは、次の技術的要件を確認しています。
Sub2のVNetWork1にAzureファイアウォールを展開します。
contoso.comにApp2という名前のアプリケーションを登録します。

可能な限り、最小限の特権の原則を使用してください。
contoso.comでAzure ADの特権ID管理（PIM）を有効にする
既存の環境
Azure AD
Contoso.comには、次の表に示すユーザーが含まれています。
Contoso.comには、次の表に示すセキュリティグループが含まれています。
Sub1
Sub1には、RG1、RG2、RG3、RG4、RG5、およびRG6という名前の6つのリソースグループが含まれています。
ユーザー2は、次の表に示す仮想ネットワークを作成します。
Sub1には、次の表に示すロックが含まれています。
Sub1には、次の表に示すAzureポリシーが含まれています。
Sub2
Sub2には、次の表に示すネットワークセキュリティグループ（NSG）が含まれています。
NSG1には、次の表に示すインバウンドセキュリティ規則があります。
NSG2には、次の表に示すインバウンドセキュリティ規則があります。
NSG3には、次の表に示すインバウンドセキュリティ規則があります。
NSG4には、次の表に示すインバウンドセキュリティ規則があります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示す発信セキュリティ規則があります。
Contosoでは、次の技術的要件を確認しています。
Sub2のVNetwork1にAzureファイアウォールを展開します。
contoso.comにApp2という名前のアプリケーションを登録します。
可能な限り、最小限の特権の原則を使用してください。
contoso.comに対してAzure AD特権ID管理（PIM）を有効にします。
テストレット2
これはケーススタディです。ケーススタディは別々には計時されません。試験時間はできるだけ長くすることができます
各ケースを完成させるのが好きです。ただし、この試験に関する追加のケーススタディやセクションがあるかもしれません。君は
この試験に含まれているすべての質問をに記入できるように、時間を管理する必要があります。
提供された時間。
ケーススタディに含まれている質問に答えるには、で提供されている情報を参照する必要があります。
ケーススタディケーススタディには、展示物や詳細情報を提供するその他のリソースが含まれる場合があります。
ケーススタディに記載されているシナリオについて。各質問は他の質問から独立しています
このケーススタディについて。

このケーススタディの最後に、レビュー画面が表示されます。この画面で回答を確認できます
また、試験の次のセクションに進む前に変更を加えることもできます。新しいセクションを始めたら、
このセクションに戻ることはできません。
ケーススタディを開始する
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックしてください。
左ペインのボタンを使用して
質問に答える前に、ケーススタディの内容を調べてください。これらのボタンをクリックすると表示されます
ビジネス要件、既存の環境、および問題の記述などの情報。その場合
スタディには[すべての情報]タブがあります。表示される情報は表示される情報と同じです。
後続のタブで。質問に答える準備ができたら、[質問]ボタンをクリックしてに戻ります。
質問。
概要
Litware、Inc.は、シカゴ地域に500人の従業員と20人に20人の従業員を擁するデジタルメディア企業です。
サンフランシスコ周辺
既存の環境
LitwareにはSub1というAzureサブスクリプションがあり、そのサブスクリプションIDは
43894a43-17c2-4a39-8cfc-です。
3540c2653ef4。
Sub1は、litwareinc.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられています。テナント
Litwareの全従業員とそのデバイスのユーザオブジェクトとデバイスオブジェクトが含まれています。各ユーザー
Azure AD Premium P2ライセンスが割り当てられています。Azure ADの特権ID管理（PIM）は
起動しました。
テナントには、以下の表に示すグループが含まれています。
Azureサブスクリプションには、次の表に示すオブジェクトが含まれています。
Azure Security Centerが無料利用枠に設定されています。
計画された変更
Litwareは、次の表に示すAzureリソースをデプロイする予定です。
Litwareは、以下のアイデンティティおよびアクセス要件を識別します。
すべてのサンフランシスコのユーザーとそのデバイスは、Group1のメンバーでなければなりません。

Group2のメンバーには、以下を使用して、リソースGroup2へのContributorの役割を割り当てる必要があります。
永久的な適格な割り当て。
ユーザーがAzure ADにアプリケーションを登録したり、アプリケーションに同意したりできないようにする必要があります。
ユーザーに代わって会社の情報にアクセスします。
プラットフォーム保護要件
Litwareは、以下のプラットフォーム保護要件を識別しています。
Microsoftマルウェア対策ソフトウェアは、リソースグループ1の仮想マシンにインストールする必要があります。
Group2のメンバーには、Azure Kubernetesサービスクラスター管理者の役割を割り当てる必要があります。
Azure ADユーザーは、Azure ADの資格情報を使用してAKS1に認証される必要があります。
計画された変更の実施に続いて、ITチームは次のようにしてVM0に接続できなければなりません。
JIT VMアクセスを使用します。
Role1という名前の新しいカスタムRBACロールを使用して、管理対象の管理を委任する必要があります。
リソースグループ1のディスク。ロール1はリソースグループ1に対してのみ使用可能でなければなりません。
セキュリティ運用要件
LitwareはAzure Security Centerでオペレーティングシステムのセキュリティ構成をカスタマイズできる必要があります。

質問: **23**
Azure Active Directory（Azure AD）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。
contoso.comという名前のテナント。
テナントのグローバル管理者ロールが割り当てられています。あなたはAzureを管理する責任があります
セキュリティセンターの設定
カスタム機密ラベルを作成する必要があります。
あなたは最初に何をすべきですか？
A. カスタムの機密情報の種類を作成します。
B. Azure ADのグローバル管理者のアクセスを高めます。
C. セキュリティセンターの価格帯を標準にアップグレードします。
D. Microsoft Cloud App Securityとの統合を有効にします。
正解: **(**正解を表示します**)**

説明/参照：
Explanation:
まず、デフォルトを直接変更することはできないため、新しい機密情報タイプを作成する必要があります。
ルール
参考文献：
https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-
タイプ

質問: **24**
データとアプリケーションの要件を満たすようにWebApp1を構成する必要があります。どの2つのアクションを実行する必要がありますか？それぞれの正しい答えは解決策の一部を表しています。
注 :それぞれ正しい選択は1ポイントの価値があります。
A. 公開証明書をアップロードします。
B. HTTPSのみのプロトコル設定を有効にします。
C. Minimum TLS Versionプロトコル設定を1.2に設定します。
D. App Serviceプランの価格帯を変更します。
E. 受信クライアント証明書プロトコル設定をオンにします。
正解: (正解を表示します)
説明/参照：
Explanation:
A :Azure Webサイトアプリケーションで使用するために証明書を構成するには、公開証明書をアップロードする必要があります。
C：時が経てば、さまざまな脆弱性を軽減するために、TLSの複数のバージョンがリリースされました。TLS 1.2は
Azure App Serviceで実行されているアプリで利用可能な最新バージョン。
間違った答え：
B :httpのURLもサポートする必要があります。
注意：
参考文献：
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth
https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-
バージョン/
質問セット2

質問: **25**

ネットワークに、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。
Azure Active Directory（Azure AD）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。
contoso.comという名前のテナント。
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に同期されないようにする必要があります。
紺碧の広告。解決策は、管理作業を最小限に抑える必要があります。
あなたは何を使うべきですか？
A. 同期ルールエディタ
B. Webサービス設定ツール
C. Azure AD Connectウィザード
D. Active Directoryユーザーとコンピュータ
正解**: (**正解を表示します**)**
説明/参照：
Explanation:
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作成します。
参考文献：
https://docs.microsoft.com/en-us/azure/active- directory / hybrid / how-to-connect-sync-change-the-
構成

質問**: 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。各質問
シリーズの中には、述べられた目標を満たすかもしれないユニークな解決策が含まれています。いくつかの質問セット
他の人は正しい解決策を持っていないかもしれませんが1つ以上の正しい解決策があるかもしれません。
このセクションで質問に答えた後は、それに戻ることはできません。その結果、
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 Storageアカウントがあります。
ユーザーとアプリケーションは、複数の共有アクセスを使用してSa1のBLOBサービスとファイルサービスにアクセスします。
署名（SAS）および保存されたアクセスポリシー。
あなたは、権限のないユーザ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を発見しました。
Sa1へのすべてのアクセスを取り消す必要があります。

解決方法：新しいストアド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？
A. はい
B. いいえ
正解**: (**正解を表示します**)**
説明/参照：
Explanation:
保存されているアクセスポリシーを取り消すには、それを削除するか、署名付き識別子を変更して名前を変更します。
署名付き識別子を変更すると、既存の署名と保存されている署名との関連付けが解除されます。
アクセスポリシー保存されているアクセスポリシーを削除または名前変更すると、すべての共有アクセスに直ちに影響します。
それに関連付けられている署名。
参考文献：
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

質問**: 27**
Azure Kubernetes Service（AKS）クラスターをテストしています。クラスタは次のように構成されています。
示す。（展示タブをクリックしてください。）
クラスタを運用環境にデプロイする予定です。HTTPアプリケーションルーティングを無効にします。
AKSにリバースプロキシとTLS終了を提供するアプリケーションルーティングを実装する必要があります。
単一のIPアドレスを使用してサービスを提供します。
あなたは何をするべきか？
A. AKS Ingressコントローラを作成します。
B. コンテナネットワークインタフェース（CNI）プラグインをインストールします。
C. Azure Standard Load Balancerを作成します。
D. Azure Basicロードバランサーを作成します。
正解**: (**正解を表示します**)**
説明/参照：
Explanation:
入力コントローラは、リバースプロキシ、設定可能なトラフィックルーティング、およびKubernetesサービス用のTLS終了
参考文献：
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

有効的な**AZ-500**問題集はJPNTest.com提供され、**AZ-500**試験に合格することに役に立ちます！JPNTest.comは今最新**AZ-500**試験問題集を提供します。JPNTest.com AZ-500試験問題集はもう更新されました。ここで**AZ-500**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AZ-500-mondaishu　**497**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」