AZ-500-free-Exam#03

シミュレーションは、多分シミュレーション試験のこと、現在実装されていない試験

# Q.1シミュレーション-

Debbieという名前のユーザーが、モバイルデバイスにAzureアプリをインストールしています。

リソースロックが削除されたときに[debbie@contoso.com](mailto:debbie@contoso.com)にアラートが送信されるようにする必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

AzureMonitorでアラートルールを構成する必要があります。

1.検索ボックスに「モニター」と入力し、検索結果から「モニター」を選択します。

2. [アラート]をクリックします。

3. +新しいアラートルールをクリックします。

4. [スコープ]セクションで、[リソースの選択]リンクをクリックします。

5. [リソースタイプでフィルタリング]ボックスに「ロック」と入力し、フィルタリングされた結果から[管理ロック（ロック）]を選択します。

6.サブスクリプションを選択し、[完了]ボタンをクリックします。

7. [条件]セクションで、[条件の選択]リンクをクリックします。

8. [管理ロックの削除]条件を選択して、[完了]ボタンをクリックします。

9. [アクショングループ]セクションで、[アクショングループの選択]リンクをクリックします。

10. [アクショングループの作成]ボタンをクリックして、新しいアクショングループを作成します。

11.グループにDebbieMobile Appなどの名前を付け（試験に入力する名前は関係ありません）、[次へ：通知>]ボタンをクリックします。

12. [通知タイプ]ボックスで、[電子メール/ SMSメッセージ/プッシュ/音声]オプションを選択します。

13. [電子メール/ SMSメッセージ/プッシュ/音声]ウィンドウで、[Azureアプリのプッシュ通知]チェックボックスをオンにし、[Azureアカウントの電子メール]フィールドにdebbie@contoso.comと入力します。

14. [OK]ボタンをクリックしてウィンドウを閉じます。

15.通知名ボックスにDebbieMobileAppなどの名前を入力します。

16. [レビューと作成]ボタンをクリックしてから、[作成]ボタンをクリックしてアクショングループを作成します。

17. [アラートルールの作成]ウィンドウに戻り、[アラートルールの詳細]セクションで、[アラートルール名]フィールドに管理ロックの削除などの名前を入力します。

18. [アラートルールの作成]ボタンをクリックして、アラートルールを作成します。

# Q.2

Azure Storageアカウントのセキュリティ問題のトラブルシューティングを行っています。

ストレージアカウントの診断ログを有効にします。

診断ログを取得するには何を使用する必要がありますか？

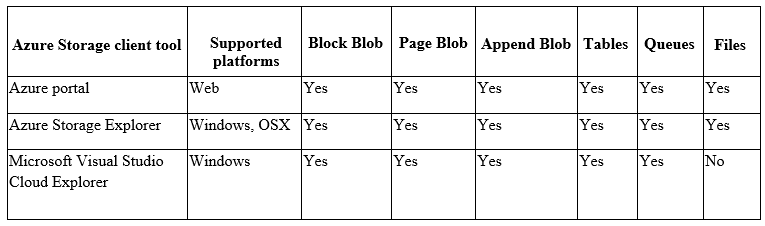
1. Azure Storage Explorer
2. Azure のSQLクエリエディター
3. Windows のファイルエクスプローラー
4. Azure Security Center

正解： *A*

長期保存用のメトリックをダウンロードしたり、ローカルで分析したりする場合は、ツールを使用するか、コードを記述してテーブルを読み取る必要があります。分析のために分のメトリックをダウンロードする必要があります。ストレージアカウントのすべてのテーブルを一覧表示すると、テーブルは表示されませんが、名前で直接アクセスできます。

多くのストレージブラウジングツールはこれらのテーブルを認識しており、それらを直接表示できます（使用可能なツールのリストについては、Azure Storage Clientツールを参照してください）。

Microsoftは、Azure Storageアカウントのデータを操作するためのグラフィカルユーザーインターフェイス（GUI）ツールをいくつか提供しています。次の表に概説されているツールはすべて無料です。



注意：

試験には、この質問のいくつかのバージョンがあります。試験の質問には、2つの異なる正解があります。

1. Azure Storage Explorer
2. AZCopy

試験で表示される可能性のあるその他の不正解オプションには、次のものがあります。

1. Azure Monitor
2. セキュリティとコンプライアンスの管理センター
3. Azure Cosmos DBエクスプローラー

リファレンス：

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

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

# Q.3シミュレーション-

複数のWindowsサーバーを WS11641655 Azure Log Analyticsワークスペースに接続することを計画しています。

Windowsサーバーに接続した後、システムイベントログのイベントがワークスペースに自動的に収集されるようにする必要があります。

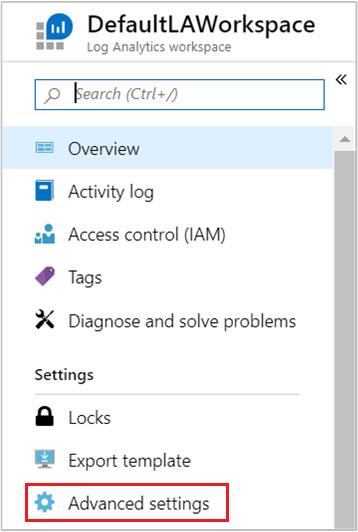
このタスクを完了するには、Azureポータルにサインインし、Azureリソースを変更します。

正解： 以下の説明を参照してください。

Azure Monitorは、WindowsイベントログまたはLinux Syslogと、長期的な分析とレポート用に指定したパフォーマンスカウンターからイベントを収集し、特定の状態が検出されたときにアクションを実行できます。次の手順に従って、WindowsシステムログとLinux Syslogからのイベントの収集、および最初にいくつかの一般的なパフォーマンスカウンターを構成します。

WindowsVMからのデータ収集

1.Azureポータルで、WS11641655 Azure Log Analyticsワークスペースを見つけて、[詳細設定]を選択します。



2. [データ]を選択してから、[Windowsイベントログ]を選択します。

3.ログの名前を入力して、イベントログを追加します。Systemと入力し、プラス記号+を選択します。

4.表で、重大度のエラーと警告を確認します。（この質問では、すべての重大度を選択して、すべてのログが確実に収集されるようにします）。

5.ページの上部にある[保存]を選択して、構成を保存します。

参照：<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

# Q.4シミュレーション-

あなたはVault1復旧サービスボールトのためのAzureBackupReportログがWS11641655 Azureのログ解析をワークスペースに格納されていることを確認する必要があります。

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

正解： *以下の説明を参照してください。*

1. Azureポータルで、検索ボックスに「Recovery Services Vaults」と入力し、検索結果から[Recovery Services Vaults]を選択して、[Vault1]を選択します。

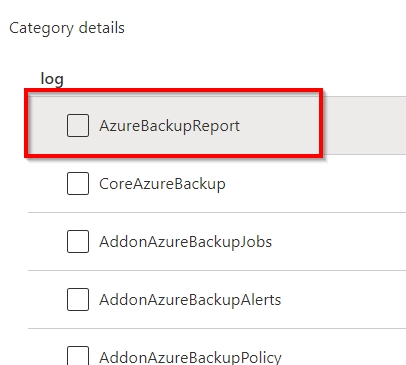
または、左側のナビゲーションペインでRecovery ServicesVaultを参照します。

2. Vault1のプロパティで、[監視]セクションまで下にスクロールし、[診断設定]を選択します。

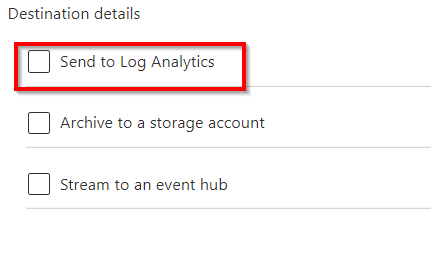
3. [診断設定の追加]リンクをクリックします。

4. [診断設定名]ボックスに名前を入力します。

5. [ログ]セクションで、[AzureBackupReport]を選択します。



6. [宛先の詳細]セクションで、[ログ分析に送信]を選択します



。7。WS11641655Azure LogAnalyticsワークスペースを選択します。

8. [保存]ボタンをクリックして、変更を保存します。

参照：

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events>

# Q.5シミュレーション-

あなたはSQLdb1 AzureのSQLデータベースから監査ログがWS11641655 Azureのログ解析をワークスペースに格納されていることを確認する必要があります。

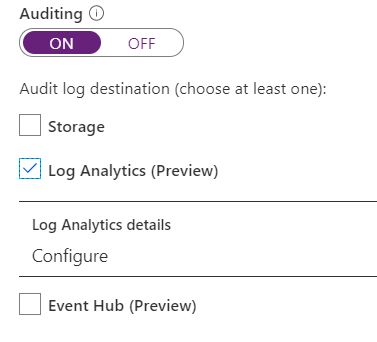
このタスクを完了するには、Azureポータルにサインインし、Azureリソースを変更します。

正解： *以下の説明を参照してください。*

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

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

3.監査がまだオンになっていない場合はオンにし、[ログ分析]チェックボックスをオンにして、[構成]をクリックします。



4. WS11641655 Azure LogAnalyticsワークスペースを選択します。

5. [保存]をクリックして変更を保存します。

# Q.6

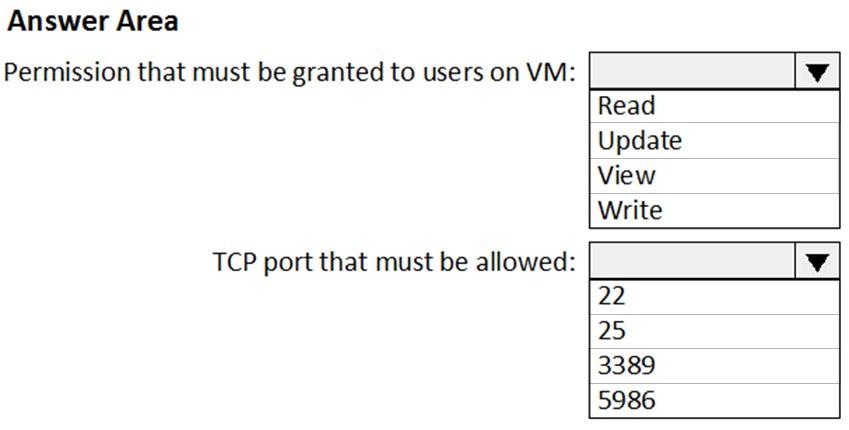
HOTSPOT-

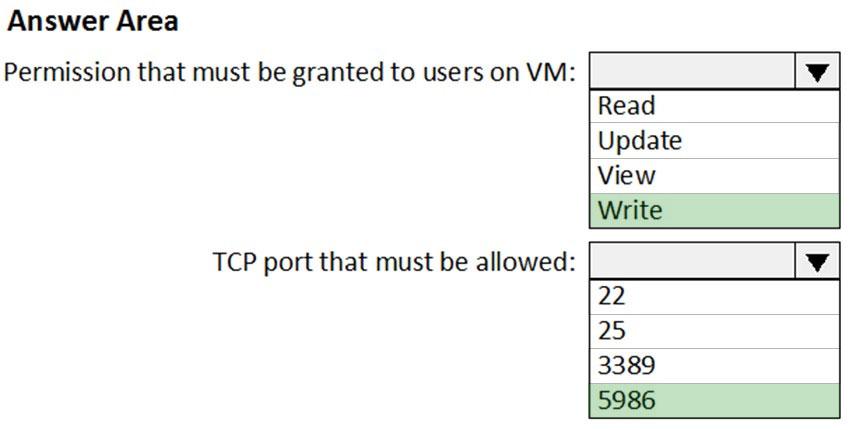
一連のAzure仮想マシンへのジャストインタイム（JIT）VMアクセスを構成しています。

JIT VMアクセスを使用して、ユーザーに仮想マシンへのPowerShellアクセスを許可する必要があります。

何を設定する必要がありますか？

回答するには、回答領域で適切なオプションを選択します。



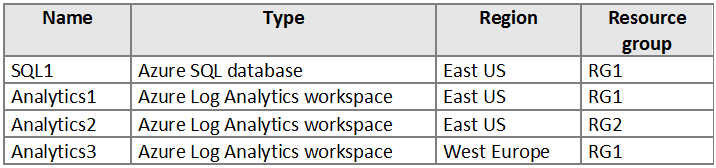
正解： 

WinRM と思って解いた

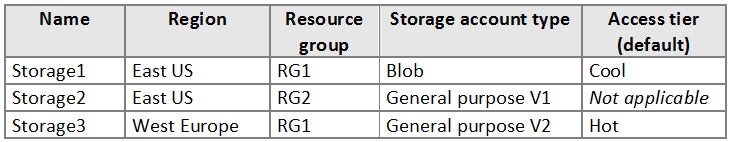
# Q.7

HOTSPOT-

次の表に示すリソースを含むAzureサブスクリプションがあります。



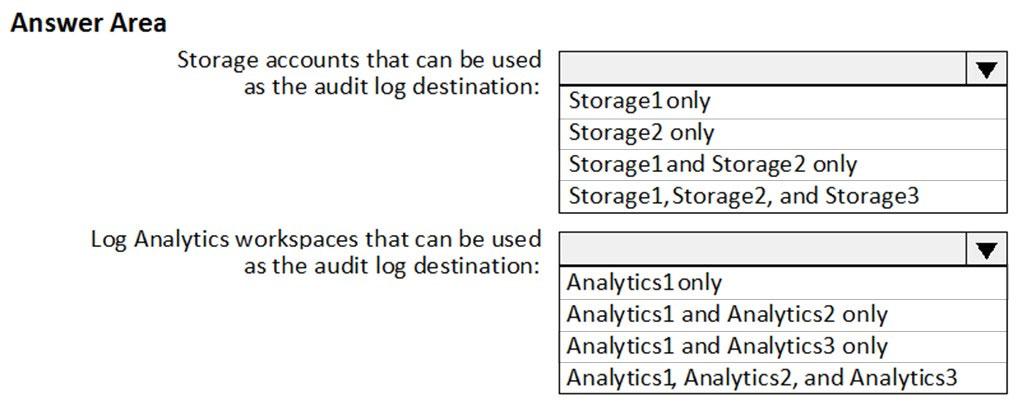
次の表に示すAzure Storageアカウントを作成します。

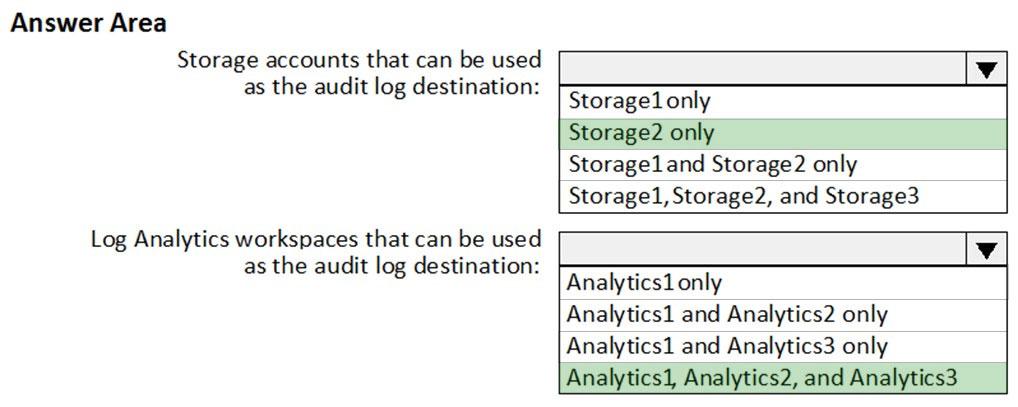


SQL1の監査を構成する必要があります。

どのストレージアカウントとLog Analytics ワークスペースを監査ログの宛先として使用できますか？

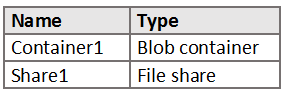
回答するには、回答領域で適切なオプションを選択します。



正解： 

# Q.8

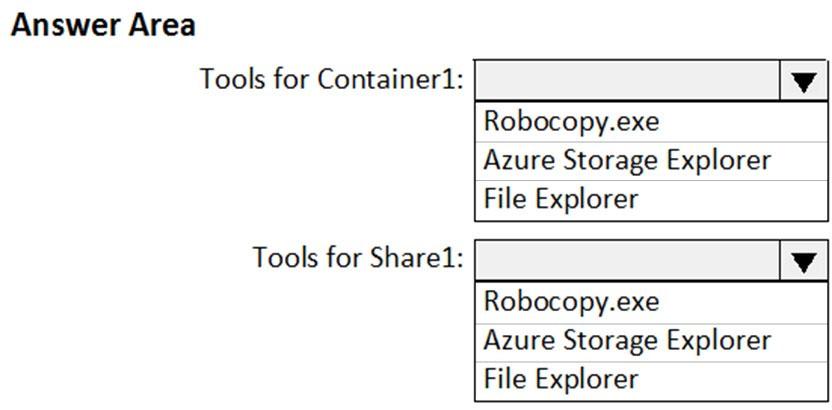
Sub1という名前のAzureサブスクリプションがあります。Sub1には、次の表に示すリソースを含むstorage1という名前のAzure Storageアカウントがあります。

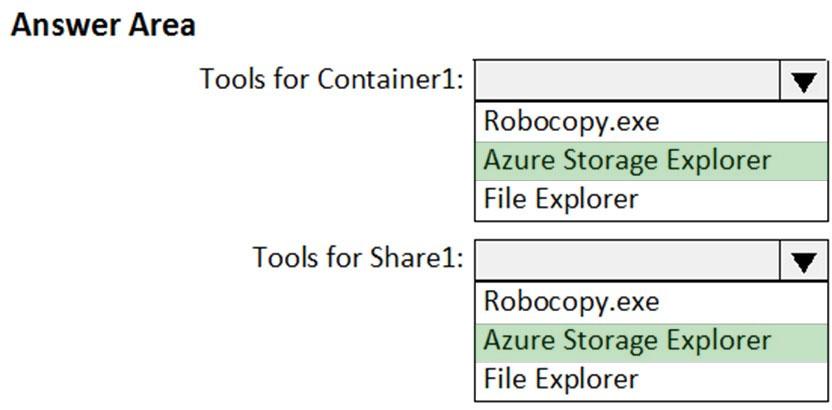


共有アクセス署名（SAS）を生成して、BLOBサービスとファイルサービスに接続します。

SASを使用してContainer1とShare1のコンテンツにアクセスするために使用できるツールはどれですか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

# Q.9

container1という名前のコンテナーを持つstorage1という名前のAzure Storageアカウントがあります。

container1のblobが変更されないようにする必要があります。

あなたは何をするべきか？

1. container1から、アクセスレベルを変更します。
2. container1から、アクセスポリシーを追加します。
3. container1から、アクセス制御（IAM）設定を変更します。
4. storage1から、blobのソフト削除を有効にします。

正解：B

参照：

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal>

# Q.10

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

Azure Monitorを使用して、いくつかのセキュリティアラートを作成する予定です。

アラート用にAzureサブスクリプションを準備する必要があります。

最初に何を作成する必要がありますか？

1. Azure Storage アカウント
2. Azure Log Analytics ワークスペース
3. Azureのイベントハブ
4. AzureAutomationアカウント

正解：B

# Q.11

あなたの会社には、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、Azure Application Insightsを使用するWebApp1という名前のAzure Webアプリが含まれています。WebApp1では、ユーザーはOAuth2.0クライアントシークレットを使用して認証する必要があります。

同社の開発者は、WebApp1へのユーザートラフィックをエミュレートする合成トランザクションを実行するマルチステップのWebテストアプリを作成することを計画しています。

Webテストが無人で実行できることを確認する必要があります。

あなたは最初に何をすべきですか？

1. Microsoft Visual Studioで、.webtestファイルを変更します。
2. Application Insights に.webtestファイルをアップロードします。
3. Web テストアプリをAzure ADに登録します。
4. プラグインをWebテストアプリに追加します。

正解：B

# Q.12

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

VM1という名前のLinux仮想マシンをSubscription1にデプロイします。

VM1のメトリックとログを監視する必要があります。

何を使うべきですか？

1. Azure Performance Diagnostics extension
2. Azure HD Insight
3. Linux Diagnostic Extension （LAD）3.0
4. Azure Analysis Services

正解： *C*

リファレンス：

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-linux>

# Q.13

Azure Sentinelをオンボードします。Azure SentinelをAzure Security Centerに接続します。

Azure Sentinelでインシデントの軽減を自動化する必要があります。

このソリューションでは、管理作業を最小限に抑える必要があります。

何を作成する必要がありますか？

1. アラートルール
2. プレイブック
3. 関数アプリ
4. ランブック

正解：*B*

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

# Q.14

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

contoso.comの診断設定を構成する必要があります。ソリューションは、次の要件を満たしている必要があります。

* ログを2年間保持します。
* Kustoクエリ言語を使用してログをクエリします。
* 管理作業を最小限に抑えます。

ログはどこに保存する必要がありますか？

1. Azure event hub
2. Azure Log Analytics workspace
3. Azure Storage account

正解：B

# Q.15

Azure Storageアカウントのセキュリティ問題のトラブルシューティングを行っています。

ストレージアカウントの診断ログを有効にします。

診断ログを取得するには何を使用する必要がありますか？

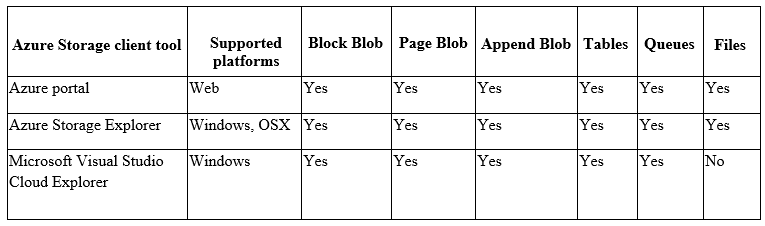
1. セキュリティおよびコンプライアンス管理センター
2. Azureのセキュリティセンター
3. Azure CosmosDB エクスプローラー
4. AzCopy

正解：D

長期保存用のメトリックをダウンロードしたり、ローカルで分析したりする場合は、ツールを使用するか、コードを記述してテーブルを読み取る必要があります。分析のために分のメトリックをダウンロードする必要があります。ストレージアカウントのすべてのテーブルを一覧表示すると、テーブルは表示されませんが、名前で直接アクセスできます。

多くのストレージブラウジングツールはこれらのテーブルを認識しており、それらを直接表示できます（使用可能なツールのリストについては、Azure Storage Clientツールを参照してください）。

Microsoftは、Azure Storageアカウントのデータを操作するためのグラフィカルユーザーインターフェイス（GUI）ツールをいくつか提供しています。次の表に概説されているツールはすべて無料です。



注意：

試験には、この質問のいくつかのバージョンがあります。試験の質問には、2つの異なる正解があります。

1. Azure Storage Explorer
2. AZCopy

試験で表示される可能性のあるその他の不正解オプションには、次のものがあります。

1. Azure Monitor
2. セキュリティとコンプライアンスの管理センター
3. Azure Cosmos DBエクスプローラー

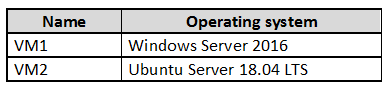
リファレンス：

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

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

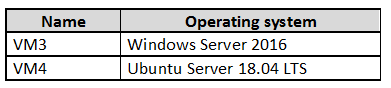
# Q.16

次の表に示す仮想マシンを含むAzureサブスクリプションがあります。



Azure Security Centerから、自動プロビジョニングをオンにします。

次の表に示す仮想マシンをデプロイします。



Microsoft Monitoring Agentはどの仮想マシンにインストールされていますか？

1. VM3だけ
2. VM1とVM3のみ
3. VM3およびVM4のみ
4. VM1、VM2、VM3、およびVM4

正解： *D*

自動プロビジョニングが有効になっている場合、セキュリティセンターは、サポートされているすべてのAzure VMと作成された新しいVMでMicrosoft Monitoring Agentをプロビジョニングします。

サポートされているオペレーティングシステムには、

* Ubuntu 14.04 LTS（x86 / x64）、16.04 LTS（x86 / x64）、18.04 LTS（x64）
* Windows Server 2008 R2、2012、2012 R2、2016、バージョン1709、1803

が含まれます。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-faq>

# Q.17シミュレーション-

VM1という名前の仮想マシンの平均CPU使用率が15分間70％よりも大きい場合、admin1@contoso.comユーザーにアラートを電子メールで送信する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

Azureポータル

1を使用して、メトリックにアラートルールを作成します。ポータルで、監視するリソース（ここではVM1）を見つけて選択します。

2. [監視]セクションで[アラート（クラシック）]を選択します。テキストとアイコンは、リソースによって若干異なる場合があります。

3. [メトリックアラートの追加（クラシック）]ボタンを選択し、以下のようにフィールドに入力して、[OK]をクリックします。

メトリック：CPUパーセンテージ-

条件：より大きい-

期間：過去15分間-

通知：電子メール-

追加の管理者電子メール：admin1@contoso.com



参照：

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

# Q.18シミュレーション-

VM1という名前の仮想マシンのセキュリティログからAzureStorageアカウントにすべての監査失敗データを収集する必要があります。

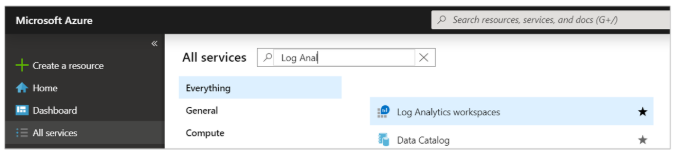
このタスクを完了するには、Azureポータルにサインインします。

このタスクは完了するまでに数分かかる場合があります。タスクの完了中に他のタスクを実行できます。

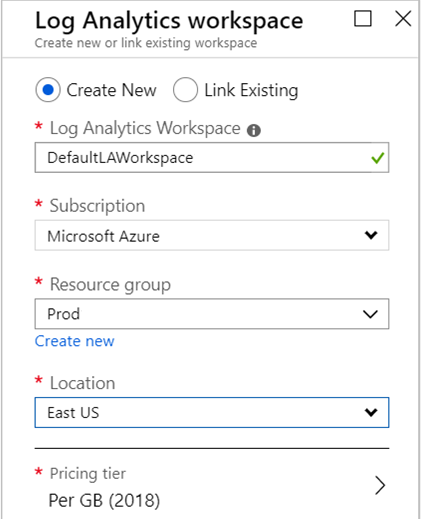
ステップ1：ワークスペースを作成する

-Azure Monitorは、詳細な分析と相関のために、Azure仮想マシンからLogAnalyticsワークスペースにデータを直接収集できます。

1. Azureポータルで、[すべてのサービス]を選択します。リソースのリストに、「LogAnalytics」と入力します。入力を開始すると、入力に基づいてリストがフィルタリングされます。LogAnalyticsワークスペースを選択します。



2. [作成]を選択し、次の項目の選択肢を



選択します。3。[ログ分析]ワークスペースペインに必要な情報を入力したら、[OK]を選択します。

情報が確認され、ワー​​クスペースが作成されている間、メニューの[通知]で進行状況を追跡できます。

手順2：Log AnalyticsVM拡張機能を有効にする

WindowsおよびLinux用のLogAnalytics VM拡張機能をインストールすると、AzureMonitorでAzureVMからデータを収集できるようになります。

1. Azureポータルで、左上隅にある[すべてのサービス]を選択します。リソースのリストに、「LogAnalytics」と入力します。入力を開始すると、入力に基づいてリストがフィルタリングされます。LogAnalyticsワークスペースを選択します。

2. Log Analyticsワークスペースのリストで、DefaultWorkspace（ステップ1で作成した名前）を選択します。

3.左側のメニューの[ワークスペースデータソース]で、[仮想マシン]を選択します。

4.仮想マシンのリストで、エージェントをインストールする仮想マシンを選択します。VMのLogAnalytics接続ステータスは、VMが接続されていないことを示していることに注意してください。

5.仮想マシンの詳細で、[接続]を選択します。エージェントは、LogAnalyticsワークスペース用に自動的にインストールおよび構成されます。このプロセスには数分かかります。その間、ステータスには「接続中」と表示されます。

エージェントをインストールして接続すると、LogAnalyticsの接続ステータスがこのワークスペースで更新されます。

参照：

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

# Q.19

単一のネットワークセキュリティグループ（NSG）を持つ単一のサブネット上に10台の仮想マシンがあります。

ネットワークトラフィックをAzure Storageアカウントに記録する必要があります。

あなたは何をするべきか？

1. ネットワークパフォーマンスモニターソリューションをインストールします。
2. Azure Log Analytics ワークスペースを作成します。
3. NSGの診断ログを有効にします。
4. NSGフローログを有効にします。

正解： *D*

ネットワークセキュリティグループ（NSG）を使用すると、仮想マシン（VM）へのインバウンドトラフィックと仮想マシン（VM）からのアウトバウンドトラフィックをフィルタリングできます。

**Network WatcherのNSGフローログ機能を使用して、NSGを通過するネットワークトラフィックをログに記録できます。**

手順は次のとおりです。

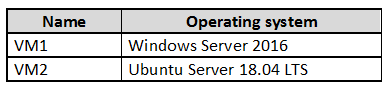
1. ネットワークセキュリティグループを使用してVMを作成する
2. NetworkWatcherを有効にし、Microsoft.Insightsプロバイダーを登録する
3. NetworkWatcherのNSGフローログ機能を使用して、NSGのトラフィックフローログを有効にする
4. ログデータをダウンロードするログデータを表示する

参照：

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal>

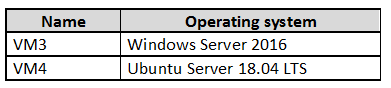
# Q.20

次の表に示す仮想マシンを含むAzureサブスクリプションがあります。



Azure Security Centerから、自動プロビジョニングをオンにします。

次の表に示す仮想マシンをデプロイします。



Log Analytics Agentはどの仮想マシンにインストールされていますか？

* A. だけVM3
* B. VM1とVM3のみ
* C. VM3およびVM4のみ
* D. VM1、VM2、VM3、およびVM4

正解： *D*

自動プロビジョニングが有効になっている場合、セキュリティセンターは、サポートされているすべてのAzure VMと作成された新しいVMでMicrosoft Monitoring Agentをプロビジョニングします。

サポートされているオペレーティングシステムには、

* Ubuntu 14.04 LTS（x86 / x64）、16.04 LTS（x86 / x64）、18.04 LTS（x64）
* Windows Server 2008 R2、2012、2012 R2、2016、バージョン1709、1803

が含まれます。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-faq>

# Q.21

HOTSPOT-

Azure Log Analyticsを使用して、Windows Server 2016を実行する200台のサーバーからログを収集する予定です。

Azure Resource Manager テンプレートを使用して、すべてのサーバーへのMicrosoft Monitoring Agentの展開を自動化する必要があります。

テンプレートをどのように完成させる必要がありますか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

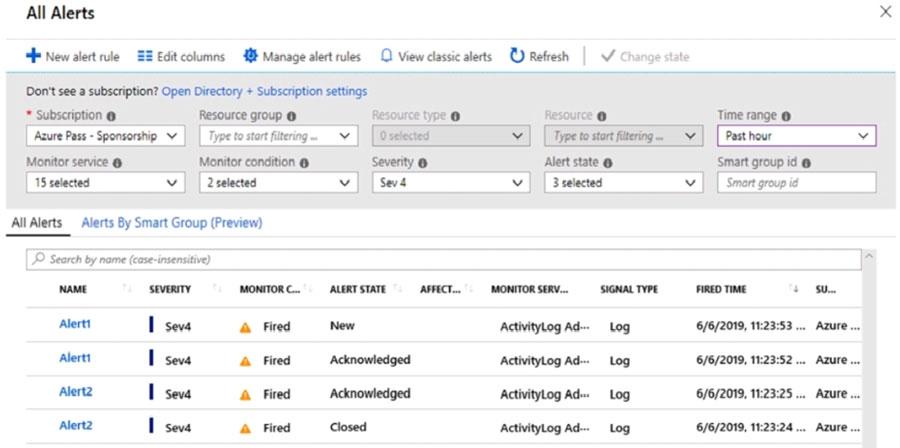
参照：

<https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/>

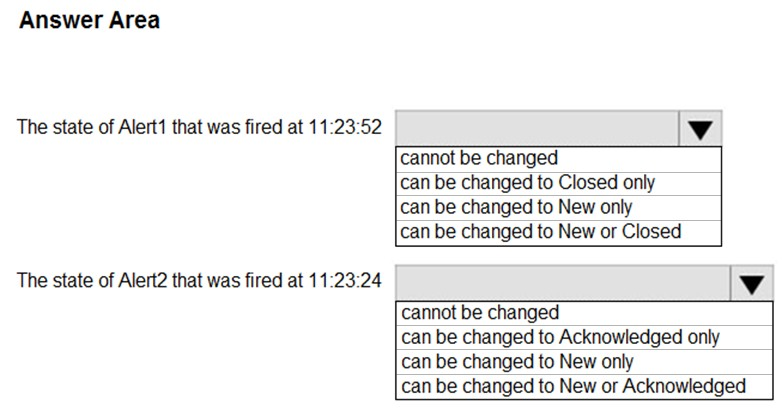
# Q.22

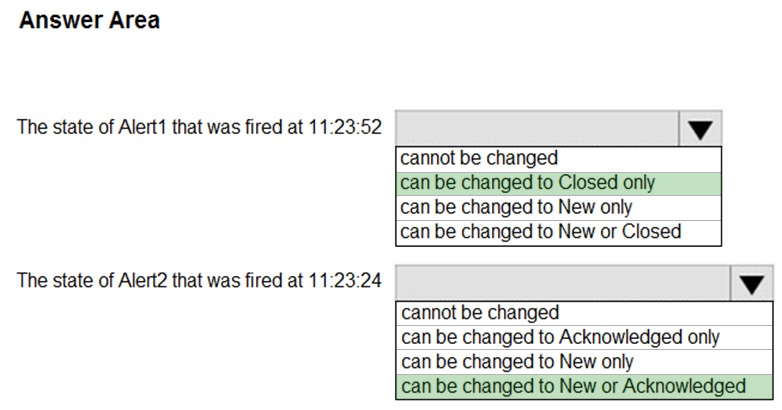
HOTSPOT-

次の展示に示されているアラートを含むAzureサブスクリプションがあります。



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。



正解： 

参照：

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

New → acknowledged → closed → new / acknowledged

# Q.23

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

テナントのグローバル管理者の役割が割り当てられます。Azure Security Centerの設定を管理する責任があります。

カスタム感度ラベルを作成する必要があります。You need to create a custom sensitivity label.

あなたは何をするべきか？

1. カスタムの機密情報タイプを作成します。
2. Azure ADのグローバル管理者のアクセスを向上させます。
3. セキュリティセンターの料金階層を標準にアップグレードします。
4. Microsoft Cloud App Securityとの統合を有効にします。

正解： *A*

最初に、デフォルトのルール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。

参照：

<https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

# Q.24

次の展示に示すAzureリソースの階層があります。

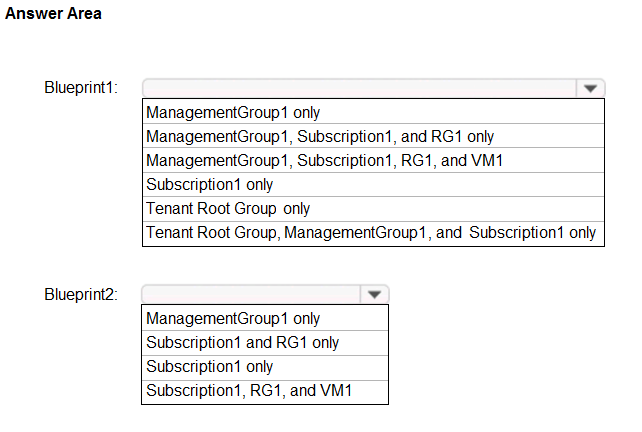


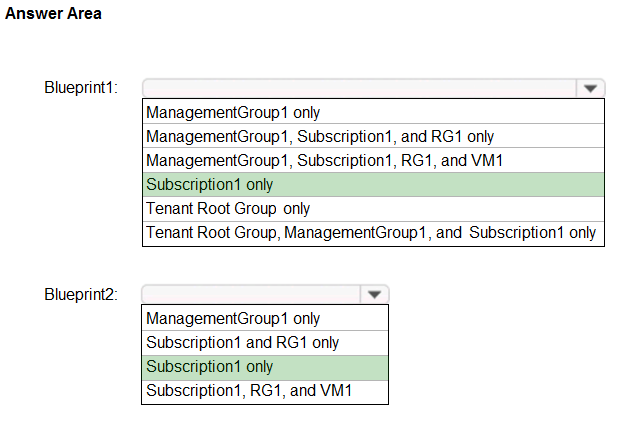
次の表に示すAzureブループリントの定義を作成します。



Blueprint1とBlueprint2をどのオブジェクトに割り当てることができますか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

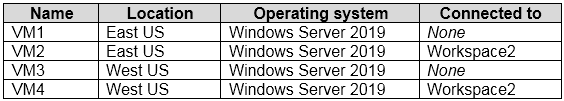
**ブループリントはサブスクリプションにのみ割り当てることができます。**

# Q.25

次の表に示すAzure Log Analyticsワークスペースを含むAzureサブスクリプションがあります。



次の表に示す仮想マシンを作成します。



Azure Sentinelを使用して、仮想マシン上のWindows Defender Firewallを監視することを計画しています。

Azure Sentinelに接続できる仮想マシンはどれですか？

1. VM1だけ
2. VM1とVM3のみ
3. VM1、VM2、VM3、およびVM4
4. VM1とVM2のみ

正解： *C*

リファレンス：

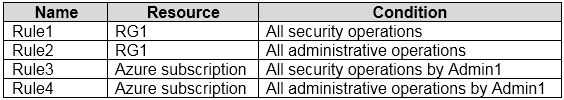
<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

# Q.26

HOTSPOT-

Admin1という名前のユーザーとRG1という名前のリソースグループを含むAzureサブスクリプションがあります。

Azure Monitorで、次の表に示すアラートルールを作成します。

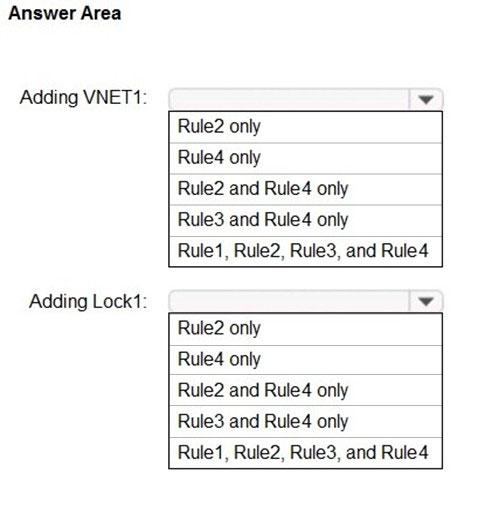


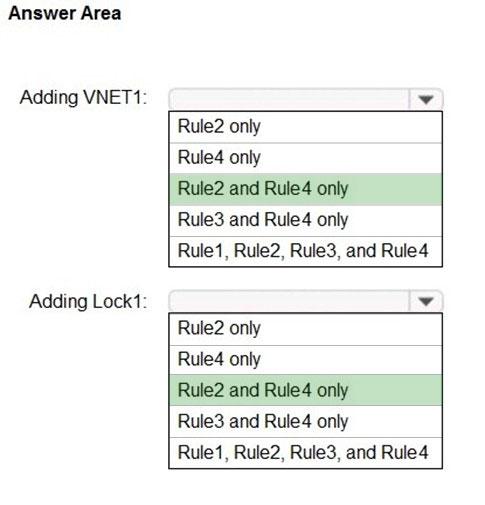
Admin1はRG1で次のアクションを実行します。

* VNET1という名前の仮想ネットワークを追加します
* Lock1という名前の削除ロックを追加します

Admin1のアクションの結果としてアラートをトリガーするルールはどれですか。

回答するには、回答領域で適切なオプションを選択します。



正解： 

# Q.27

100台の仮想マシンを含み、Azure Security Center Standard層が有効になっているAzureサブスクリプションがあります。

各仮想マシンの脆弱性スキャンを実行することを計画しています。

Azure Resource Manager テンプレートを使用して、脆弱性スキャナー拡張機能を仮想マシンにデプロイする必要があります。

仮想マシンへの拡張機能のデプロイを自動化するには、コードでどの2つの値を指定する必要がありますか？それぞれの正解は、解決策の一部を示しています。

1. ユーザーが割り当てたマネージID
2. WorkspaceID
3. Azure Active Directory（Azure AD）ID
4. Key Vault 管理ストレージアカウントキー
5. システムによって割り当てられた管理対象ID
6. プライマリ共有キー

正解：A, C

# Q.28

Admin1という名前のユーザーとVM1という名前の仮想マシンを含むAzureサブスクリプションがあります。VM1はWindows Server 2019を実行し、Azure Resource Manager テンプレートを使用してデプロイされました。VM1は、パブリックAzure Basic Load Balancerのバックエンドプールのメンバーです。

Admin1は、Azure Security CenterのジャストインタイムVMアクセスブレードでVM1がサポート対象外としてリストされていることを報告します。

Admin1がVM1のジャストインタイム（JIT）VMアクセスを有効にできることを確認する必要があります。

あなたは何をするべきか？

1. ネットワークセキュリティグループ（NSG）を作成して構成します。
2. VM1のための追加のパブリックIPアドレスを作成して構成します。
3. 基本ロードバランサーをAzure標準ロードバランサーに置き換えます。
4. Azure Active Directoryプレミアムプラン1ライセンスをAdmin1に割り当てます。

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc>

Aは正しいです。<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc>

次の理由により、VMがこのタブに表示される場合があります。

**ネットワークセキュリティグループ（NSG）がない**

JITではNSGを構成する必要がありますクラシックVM-JITは、「クラシック展開」ではなく、Azure Resource Managerを介して展開されるVMをサポートします。クラシックとAzure Resource Managerのデプロイモデルの詳細をご覧ください。

その他

**サブスクリプションまたはリソースグループのセキュリティポリシーでJITソリューションが無効になっている場合**、VMがこのタブに表示される可能性があります。サポートされていない-JITが有効になっておらず、この機能をサポートしていないVM。

# Q.29

HOTSPOT-

Azure Active Directory（Azure AD）コネクタ、Query1という名前のAzure Log Analyticsクエリ、およびPlaybook1という名前のプレイブックを含むAzure Sentinelワークスペースがあります。

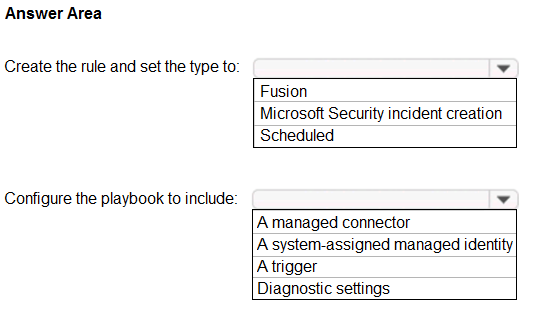
Query1は、Azure ADによって生成されたセキュリティイベントのサブセットを返します。

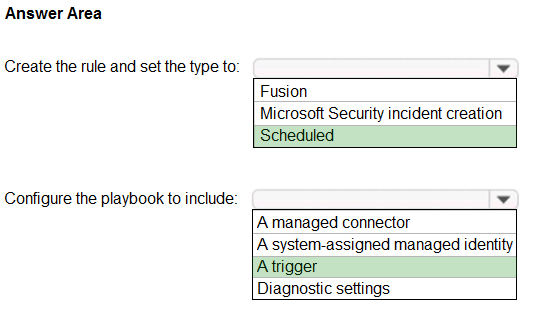
Playbook1をトリガーするQuery1に基づいてAzure Sentinel分析ルールを作成することを計画しています。

Playbook1を新しいルールに追加できることを確認する必要があります。

あなたは何をするべきか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

参照：

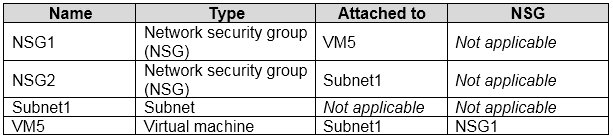
<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

# Q.30

HOTSPOT-

次の表に示すリソースを含むAzureサブスクリプションがあります。



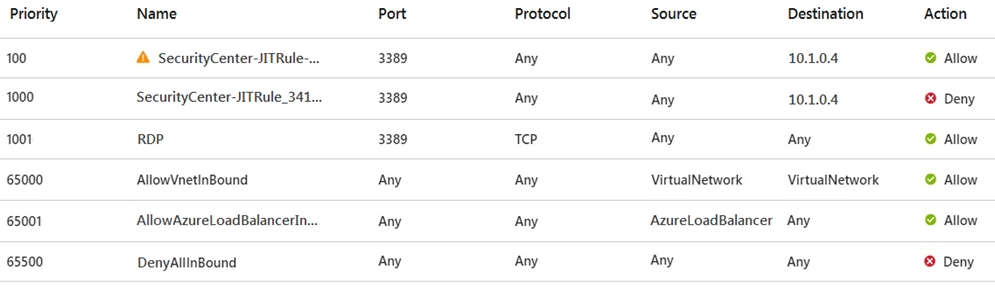
10.1.0.4のIPアドレスがVM5に割り当てられます。VM5にはパブリックIPアドレスがありません。

VM5には、次の図に示すように構成されたジャストインタイム（JIT）VMアクセスがあります。

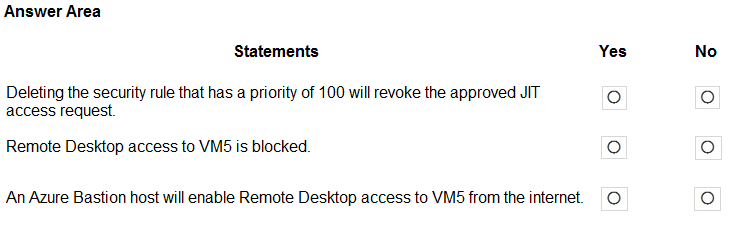


VM5のJITVMアクセスを有効にします。

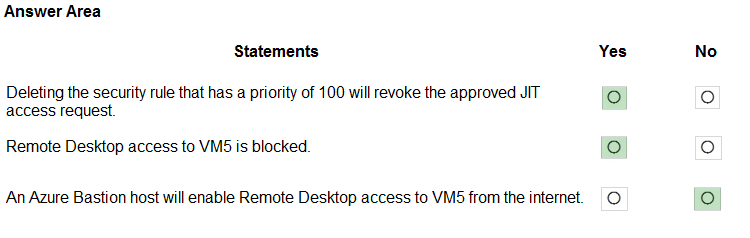
NSG1には、次の展示に示すインバウンドルールがあります。



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



1. 優先度が100のセキュリティルールを削除すると、承認されたJITアクセス要求が取り消されます。
2. VM5へのリモートデスクトップアクセスはブロックされます。
3. Azure Bastionホストは、インターネットからVM5へのリモートデスクトップアクセスを有効にします。

正解： 

# Q.31

Azure Active Directory（Azure AD）テナントとルート管理グループがあります。

10個のAzureサブスクリプションを作成し、サブスクリプションをルート管理グループに追加します。

ルート管理グループに格納されるAzureブループリント定義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？

1. ルート管理グループの役割ベースのアクセス制御（RBAC）の役割の割り当てを変更します。
2. ルート管理グループにAzureのポリシー定義を追加します。
3. ユーザーが割り当てたIDを作成します。
4. サービスプリンシパルを作成します。

正解： *A*

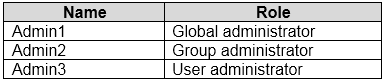
リファレンス：

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

# Q.32

HOTSPOT-

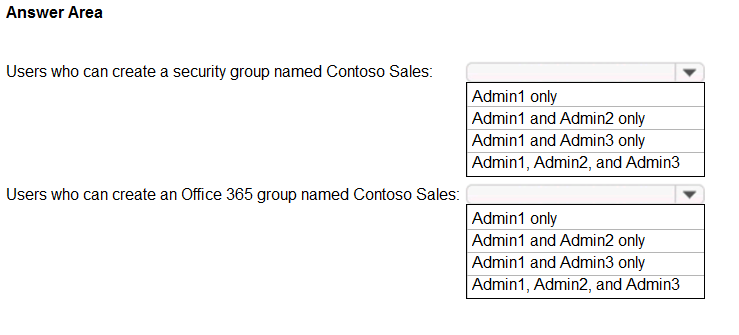
次の表に示すユーザーを含むcontoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。

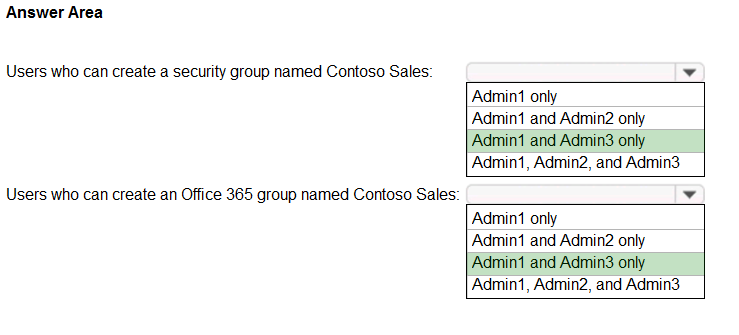


Contoso.comには、グループ命名ポリシーが含まれています。ポリシーには、Contosoという単語を含むカスタムのブロックされた単語リストルールがあります。

contoso.comでContoso Salesという名前のグループを作成できるユーザーはどれですか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

# Q.33

DRAGDROP-

単一のAzure Active Directory（Azure AD）テナントにリンクされた5つのAzureサブスクリプションがあります。

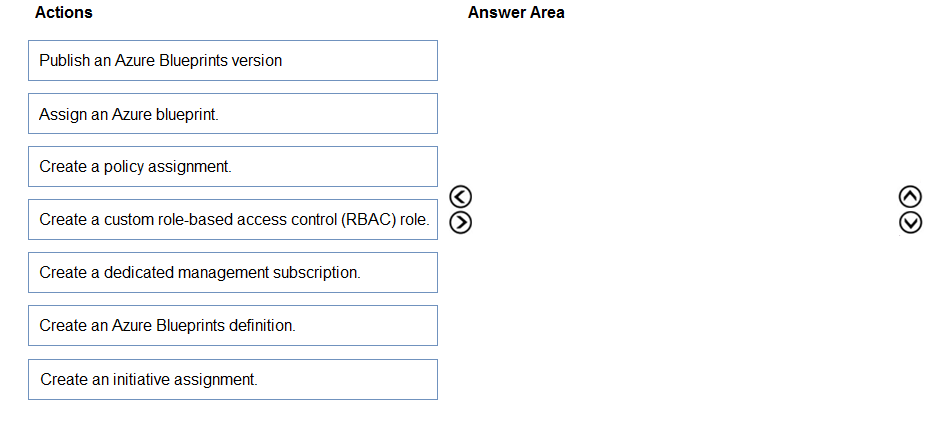
SecurityPolicyInitiative1 という名前の Azure ポリシーイニシアチブを作成します。

すべての新しいリソースグループで構成する必要がある標準の役割の割り当てを特定します。

新しいリソースグループが作成されるときに、SecurityPolicyInitiative1とロールの割り当てを適用する必要があります。

どの3つのアクションを順番に実行する必要がありますか？

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



Azureブループリントバージョンを公開します。

Azureブループリントを割り当てます。

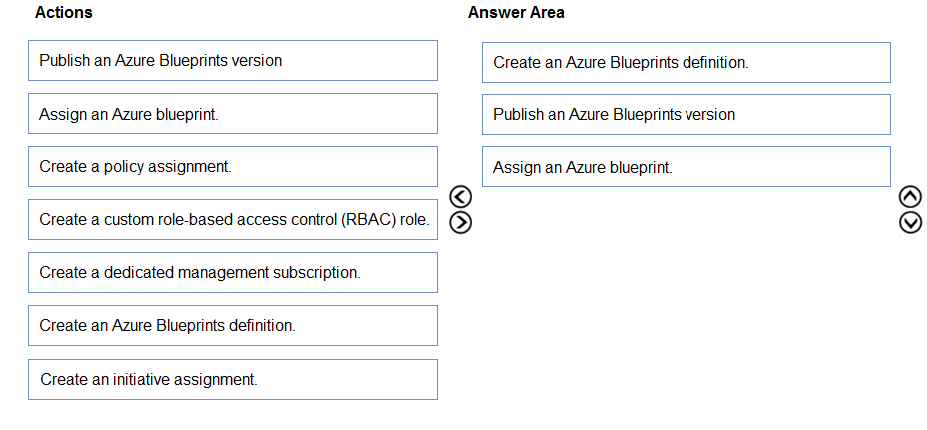
ポリシー割り当てを作成します。

カスタムのロールベースアクセス制御（RBAC）ロールを作成します。

専用の管理サブスクリプションを作成します。

Azureブループリント定義を作成します。

イニシアチブの割り当てを作成します。

正解： 

<https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal>

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

# Q.34

Windowsを実行するServer1、Server2、およびServer3という名前の3つのオンプレミスサーバーがあります。Server1とServer2で、内部ネットワーク上にあります。Server3はon-premisesネットワーク上にあります。すべてのサーバーがAzureにアクセスできます。

Azure Sentinelから、Windowsファイアウォールデータコネクタをインストールします。

Azure SentinelのサーバーからMicrosoft Defenderファイアウォールデータを収集する必要があります。

あなたは何をするべきか？

1. Server1、Server2、およびServer3からイベントサブスクリプションを作成します。
2. 各サーバーにオンプレミスデータゲートウェイをインストールします。
3. 各サーバーにMicrosoftエージェントをインストールします。
4. Server1とServer3のオンプレミスのデータゲートウェイをインストールするServer2上のMicrosoft Agentをインストールします。

Correct Answer: *C*

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

# Q.35

複数のAzure SQLデータベースとAzure Sentinelワークスペースを含むAzureサブスクリプションがあります。

Advanced Threat Protection for Azure SQL Databaseによって報告されたイベントを見つけるには、ワークスペースに保存されたクエリを作成する必要があります。

あなたは何をするべきか？

1. Azure CLIから、Get-AzOperationalInsightsworkspaceコマンドレットを実行します。
2. Azure SQLデータベースクエリエディターから、Transact-SQLクエリを作成します。
3. Azure Sentinelワークスペースから、Kustoクエリ言語クエリを作成します。
4. Microsoft SQL Server Management Studio（SSMS）から、Transact-SQLクエリを作成します。

正解：C

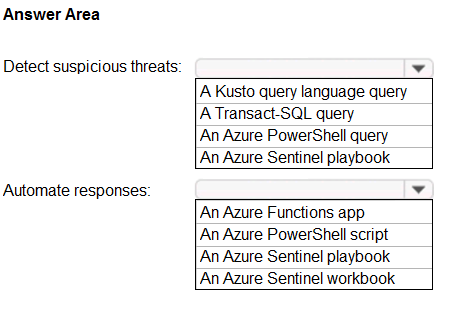
# Q.36

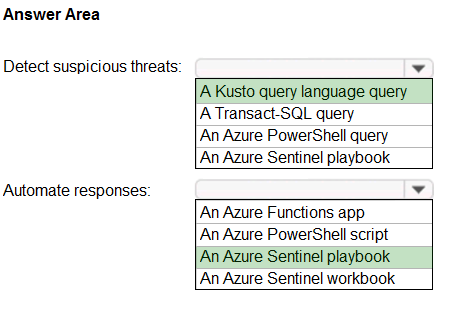
ホットスポット-

Azure Sentinelを使用して、疑わしい脅威を検出し、応答を自動化する分析ルールを作成することを計画しています。

ルールにはどのコンポーネントが必要ですか？

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。



Correct Answer: 

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

# Q.37

Azure仮想マシンからAzure Log Analyticsワークスペースにイベントを収集しています。

収集したイベントに基づいてアラートを作成することを計画しています。

アラートの作成に使用できるAzureサービスを特定する必要があります。

どの2つのサービスを特定する必要がありますか？

それぞれの正解は完全な解決策を提示します

1. Azure Monitor
2. Azure Security Center
3. Azure Analytics Services
4. Azure Sentinel
5. Azure Advisor

正解：A、D

# Q.38

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。

3つのAzureサブスクリプションの集中ポリシー管理にAzure Security Centerを使用します。

サブスクリプションのセキュリティを管理するには、いくつかのポリシー定義を使用します。

ポリシー定義をグループとして3つのサブスクリプションすべてに展開する必要があります。

解決策：管理グループを対象とするイニシアチブと割り当てを作成します。

これは目標を達成していますか？

1. はい
2. いいえ

正解：A　はい

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

# Q.39

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。

3つのAzureサブスクリプションの集中ポリシー管理にAzure Security Centerを使用します。

サブスクリプションのセキュリティを管理するには、いくつかのポリシー定義を使用します。

ポリシー定義をグループとして3つのサブスクリプションすべてに展開する必要があります。

解決策：リソースグループを対象とするポリシーイニシアチブと割り当てを作成します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *B*

代わりに**管理グループ**を使用してください。

Microsoft Azureの管理グループは、複数のAzureサブスクリプションに同時にガバナンスポリシーを課す必要があるという問題を解決します。

参照：

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

# Q.40

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。

3つのAzureサブスクリプションの集中ポリシー管理にAzure Security Centerを使用します。

サブスクリプションのセキュリティを管理するには、いくつかのポリシー定義を使用します。

ポリシー定義をグループとして3つのサブスクリプションすべてに展開する必要があります。

解決策：リソースグループを対象とするポリシー定義と割り当てを作成します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *B*

参照：

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

# Q.41

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。

3つのAzureサブスクリプションの集中ポリシー管理にAzure Security Centerを使用します。

サブスクリプションのセキュリティを管理するには、いくつかのポリシー定義を使用します。

ポリシー定義をグループとして3つのサブスクリプションすべてに展開する必要があります。

解決策：管理グループを対象とするリソースグラフと割り当てを作成します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *B*

Microsoft Azureの管理グループは、複数のAzureサブスクリプションに同時にガバナンスポリシーを課す必要があるという問題を解決します。

ただし、**管理グループに適用できるグループにポリシー定義をバンドルするには、リソースグラフではなく、イニシアチブを使用する必要があります**。

参照：

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

# Q.42

ホットスポット-

ユーザーがアクセスできないリソースにサインインしようとしている疑いがあります。

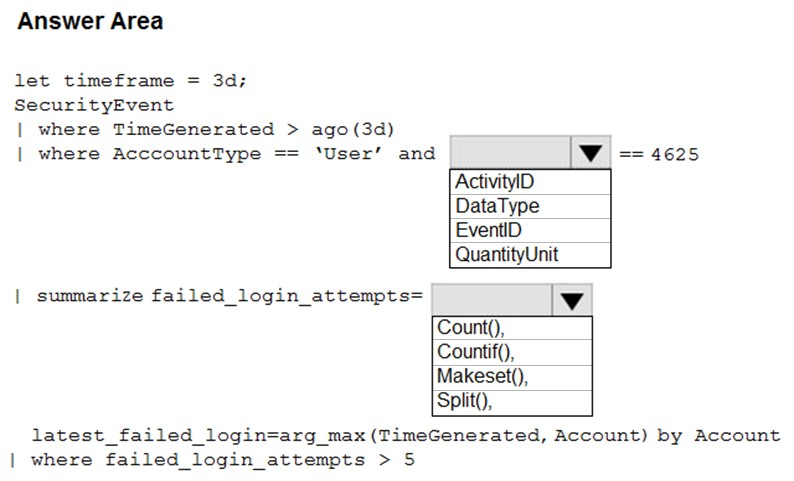
過去3日間に失敗したユーザーのサインイン試行を識別するには、

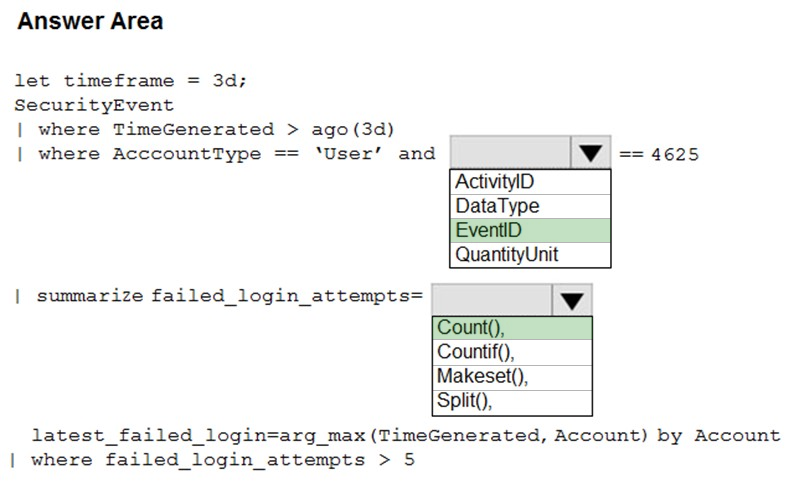
Azure Log Analytics クエリを作成する必要があります。

結果には、サインインの試行に5回以上失敗したユーザーのみが表示される必要があります。

クエリをどのように構成する必要がありますか？

回答するには、回答領域で適切なオプションを選択します。



正解： 

次の例では、前日に5回以上ログインに失敗し、最後にログインを試みたユーザーアカウントを特定します。

lettimeframe= 1d;

SecurityEvent -

| where TimeGenerated > ago(1d)

| where AccountType == 'User' and **EventID** == 4625 // 4625 - failed log in

| summarize failed\_login\_attempts=**count()**, latest\_failed\_login=arg\_max(TimeGenerated, Account) by Account

| where failed\_login\_attempts > 5

| project-away Account1

参照：

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

# Q.43

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、User1という名前のユーザーに電子メールメッセージを送信するように構成されています。

Alertsという名前の配布グループに電子メールメッセージを送信するには、Play1を変更する必要があります。

Play1を変更するには何を使用する必要がありますか？

1. Azure DevOps
2. Azure Application Insights
3. Azure Monitor
4. Azure Logic Apps Designer

正解： *D*

セキュリティセンターの既存のプレイブックを変更して、アクションまたは条件を追加できます。これを行うには、[プレイブック]タブで、変更するプレイブックの名前をクリックするだけで、Logic App Designerが開きます。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks>

# Q.44

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？

それぞれの正解は、解決策の一部を示しています。

1. オンボード Azure Active Directory（Azure AD）ID 保護。
2. Azure Storage Account を作成します。
3. Azure Advisor の推奨事項を実装します。
4. Azure Log Analytics Workspace を作成します。
5. セキュリティセンターの料金階層を標準にアップグレードします。

正解： *B、D*

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。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert>

# Q.45

LAW1という名前のAzure Log Analyticsワークスペースを含むSub1という名前のAzureサブスクリプションがあります。

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、接続されたサーバーからセキュリティ関連のパフォーマンスカウンターを収集するように構成されています。

LAW1によって収集されたデータに基づいてアラートを構成する必要があります。ソリューションは次の要件を満たしている必要があります。

* 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を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に1回、アラートが解決されたときに1回だけ生成する必要があります。

アラートルールを作成するときに、どのシグナルタイプを使用する必要がありますか？

1. ログ
2. ログ（保存されたクエリ）
3. メトリック
4. アクティビティログ

正解：Ｃ

Azure Monitorのメトリックアラートは、メトリックの1つがしきい値を超えたときに通知を受け取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標準およびカスタムメトリックで機能します。

注：シグナルはターゲットリソースによって発行され、いくつかのタイプがあります。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。

参照：

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

# Q.46

HOTSPOT-

Azure Sentinel ワークスペースを含むAzureサブスクリプションがあります。

Azure Sentinelは、複数のAzureワークロードからログを取り込むように構成されています。インシデントの管理には、サードパーティのサービス管理プラットフォームが使用されます。

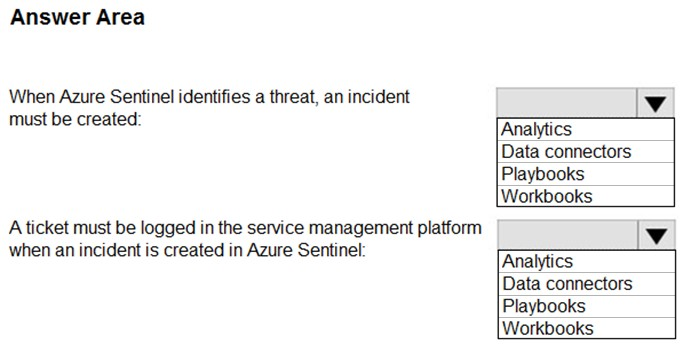
次の要件を満たすように構成する

Azure Sentinelコンポーネントを特定する必要があります。

* Azure Sentinelが脅威を特定したら、インシデントを作成する必要があります。
* Azure Sentinelでインシデントを作成するときは、チケットをサービス管理プラットフォームにログインする必要があります。

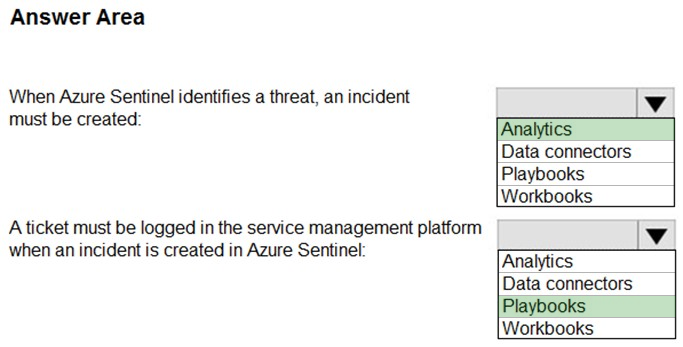
要件ごとにどのコンポーネントを特定する必要がありますか？

回答するには、回答領域で適切なオプションを選択します。



Azure Sentinelが脅威を特定したら、インシデントを作成する必要があります

Azure Sentinelでインシデントを作成するときは、チケットをサービス管理プラットフォームにログインする必要があります

正解： 

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

# Q.47

HOTSPOT-

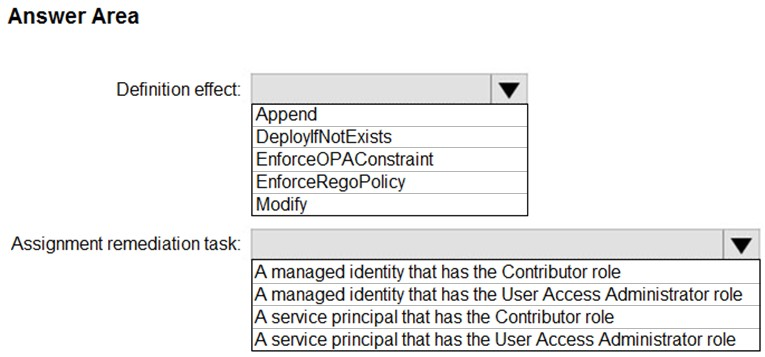
Azureサブスクリプションがあります。

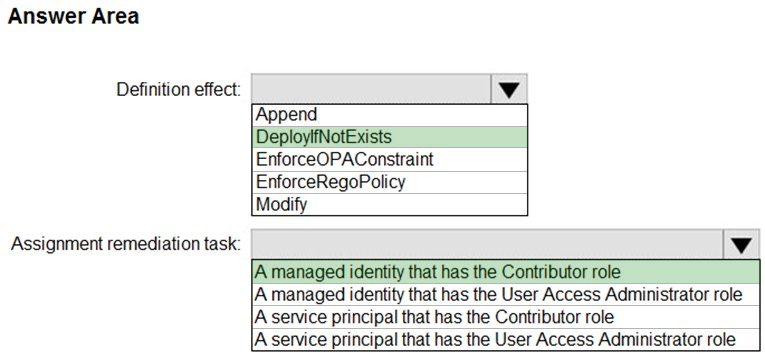
次の要件を満たすAzureポリシーを作成してデプロイする必要があります。

* 新しい仮想マシンがデプロイされると、カスタムセキュリティ拡張機能が自動的にインストールされます。
* 非準拠の仮想マシンに対して自動生成された修復タスクをトリガーして、拡張機能をインストールします。

ポリシー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。



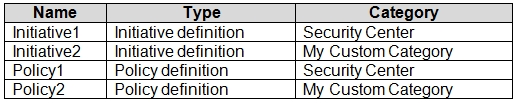
正解： 

参照：

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

# Q.48

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



Azure Security Centerを使用して、Subscription1に追加できるイニシアチブとポリシーを特定する必要があります。

何を特定する必要がありますか？

1. Policy1とPolicy2ののみ
2. イニシアチブ1のみ
3. イニシアチブ1およびイニシアチブ2のみ
4. イニシアチブ1、イニシアチブ2、Policy1、およびPolicy2

正解： *D*

リファレンス：

<https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies>

# Q.49

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、WF1という名前のワークフローの自動化があります。WF1は、User1という名前のユーザーに電子メールメッセージを送信するように構成されています。

Alertsという名前の配布グループに電子メールメッセージを送信するには、WF1を変更する必要があります。

WF1を変更するには何を使用する必要がありますか？

1. Azure Application Insights
2. Azure Monitor
3. Azure Logic Apps Designer
4. Azure DevOps

正解： *C*

リファレンス：

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>

<https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exercise-configure-playbook>

# Q.50

100台の仮想マシンを含むAzureリソースグループがあります。

複数のポリシー定義を含むInitiative1という名前のイニシアチブがあります。Initiative1はリソースグループに割り当てられます。

ポリシー定義と一致しないリソースを特定する必要があります。

あなたは何をするべきか？

1. Azure Security Centerから、規制コンプライアンスの評価を表示します。
2. Azure Active Directory管理センターの[ポリシー]ブレードから、[コンプライアンス]を選択します。
3. Azure Security Centerから、セキュアスコアを表示します。
4. Azure Active Directory管理センターの[ポリシー]ブレードから、[割り当て]を選択します。

正解： *B*

リファレンス：

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal>

# Q.51

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

デフォルトでSubscription1に割り当てられているセキュリティ設定を表示する必要があります。

どのAzureポリシーまたはイニシアチブの定義を確認する必要がありますか？

1. 監査診断設定ポリシーの定義
2. Azure Security Centerイニシアチブの定義で監視を有効にする
3. VMのイニシアチブの定義のためのAzureのモニターを有効
4. Azure Monitorソリューションの「セキュリティと監査」をデプロイする必要があるポリシー定義

Correct Answer: *B*

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy>

<https://docs.microsoft.com/en-us/azure/security-center/policy-reference>

# Q.52

DRAGDROP-

Azure Active Directory（Azure AD）データコネクタを備えたAzure Sentinelワークスペースがあります。

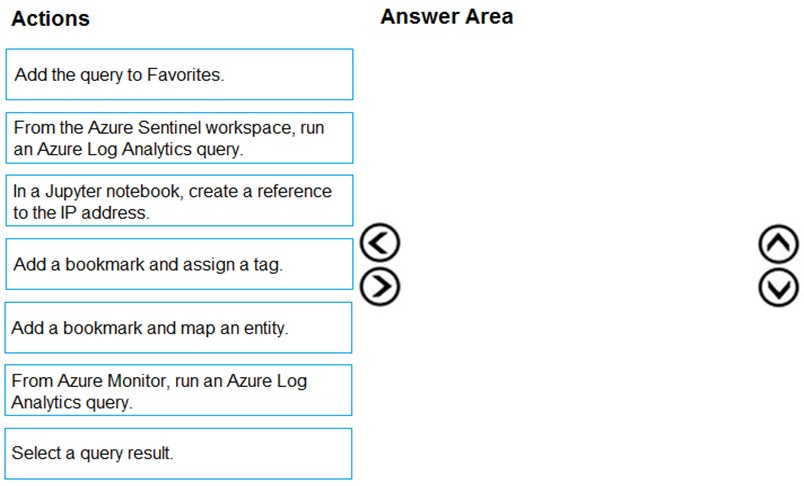
特定のIPアドレスからの疑わしいトラフィックを脅威ハンティングしています。

ワークスペースに保存されている中間イベントに注釈を付け、調査グラフをナビゲートするときにIPアドレスを参照できるようにする必要があります。

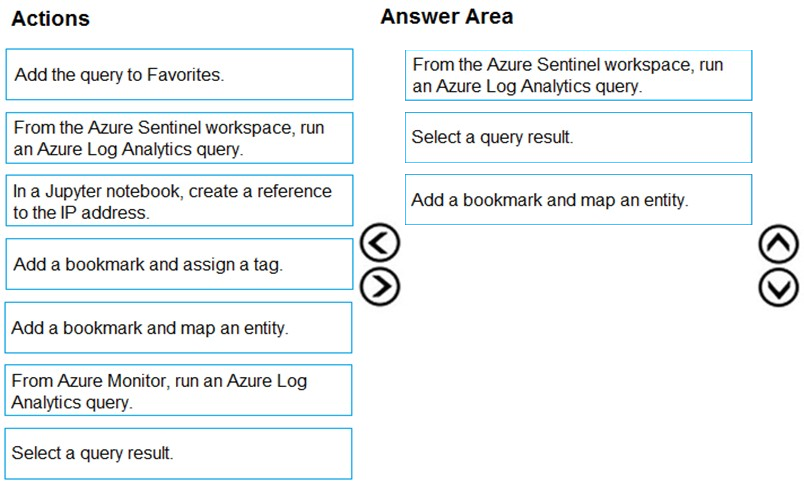
どの3つのアクションを順番に実行する必要がありますか？

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

選択して配置：



1. クエリをお気に入りに追加します。
2. Azure Sentinelワークスペースから、Azure Log Analyticsクエリを実行します。
3. Jupyterノートブックで、IPアドレスへの参照を作成します。
4. ブックマークを追加し、タグを割り当てます。
5. ブックマークを追加し、エンティティをマップします。
6. Azure Monitorから、Azure Log Analyticsクエリを実行します。
7. クエリ結果を選択します。

Correct Answer: 

**Azure Sentinelワークスペースから、Azure Log Analyticsクエリを実行します。**

**クエリ結果を選択します。**

**ブックマークを追加し、エンティティをマップします。**

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/bookmarks>

# Q.53

HOTSPOT-

20個のAzureサブスクリプションとGroup1という名前のセキュリティグループがあります。サブスクリプションは、ルート管理グループの子です。

各サブスクリプションには、RG1という名前のリソースグループが含まれています。

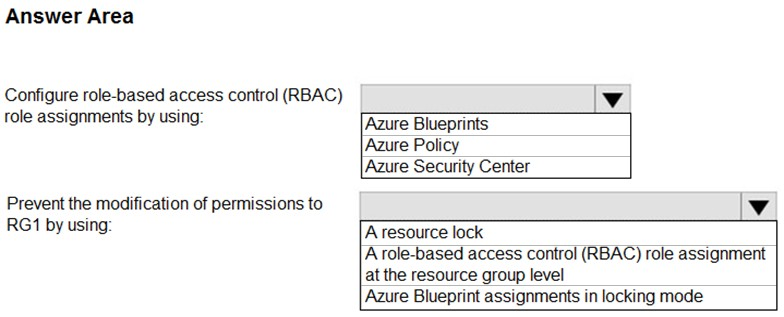
サブスクリプションごとに、RG1が次の要件を満たしていることを確認する必要があります。

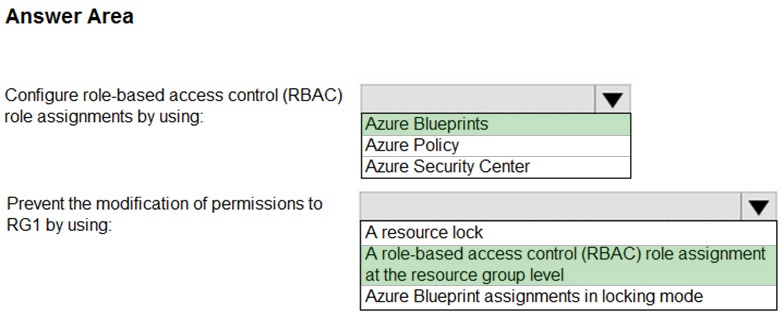
* Group1のメンバーに所有者の役割が割り当てられている。
* RG1へのアクセス許可の変更が防止されます。

あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

ホットエリア：



正解： 

# Q.54

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。

3つのAzureサブスクリプションの集中ポリシー管理にAzure Security Centerを使用します。

サブスクリプションのセキュリティを管理するには、いくつかのポリシー定義を使用します。

ポリシー定義をグループとして3つのサブスクリプションすべてに展開する必要があります。

解決策：テナントルートグループ管理グループを対象とするイニシアチブと割り当てを作成します。

これは目標を達成していますか？

1. はい
2. いいえ

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/overview <https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

# Q.55

Azure環境があります。

ISO27001標準に準拠していないAzure構成とワークロードを特定する必要があります。

何を使うべきですか？

1. Azure Sentinel
2. Azure Active Directory（Azure AD）ID保護
3. Azure Security Center
4. Azure Advanced Threat Protection（ATP）

正解： *C*

リファレンス：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard>

# Q.56

DRAGDROP-

100台の仮想マシンを含むAzureサブスクリプションがあります。Azure Diagnosticsは、すべての仮想マシンで有効になっています。

サブスクリプション内のAzureサービスの監視を計画しています。

次の詳細を取得する必要があります。

* 3週間前に仮想マシンを削除したユーザーを特定します。
* Windows Server 2016を実行する仮想マシンのセキュリティイベントをクエリします。

Azure Monitor で何を使用する必要がありますか？

答えるには、適切な構成設定を正しい詳細にドラッグします。

各構成設定は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、分割バーをペイン間でドラッグするか、スクロールする必要がある場合があります。



正解： 

ボックス1：アクティビティログ

-Azureアクティビティログは、サブスクリプション内のリソースで実行された操作に関する洞察を提供します。アクティビティログは

、サブスクリプションのコントロールプレーンイベントを報告するため、以前は「監査ログ」または「操作ログ」と呼ばれていました。

アクティビティログは、書き込み操作（つまり、PUT、POST、またはDELETE）の「何を、誰が、いつ」を決定するのに役立ちます。

ボックス2：ログ

-Log Integrationは、Windows仮想マシン、Azureアクティビティログ、Azure Security Centerアラート、およびAzureリソースプロバイダーログからAzure診断を収集します。この統合により、**オンプレミスであろうとクラウド内であろうと**、すべての資産に統合されたダッシュボードが提供されるため、セキュリティイベントを集約、関連付け、分析、およびアラートすることができます。

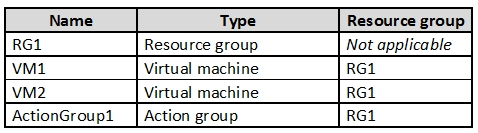
参照：

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

# Q.57

HOTSPOT-

次の表に示すリソースを含むAzureサブスクリプションがあります。



VM1とVM2が停止します。

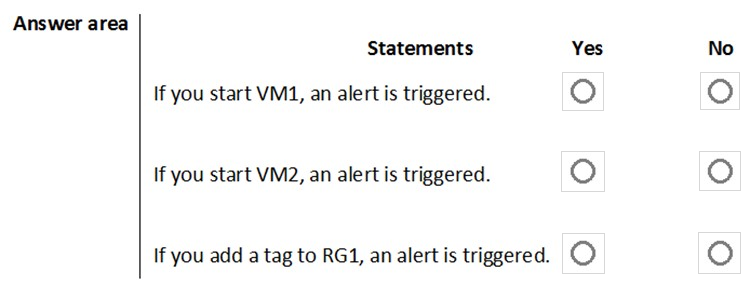
次の設定を持つアラートルールを作成します。

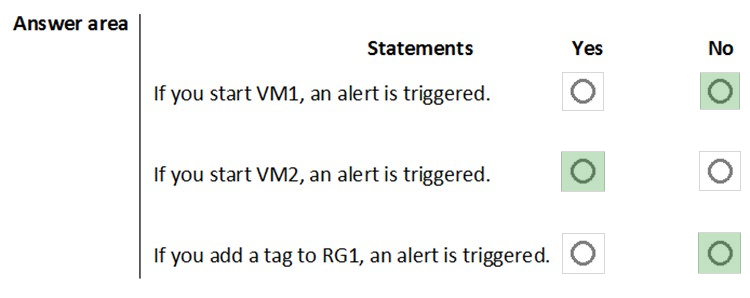
* リソース：RG1
* 条件：すべての管理操作
* アクション：このアラートルール用に構成されたアクショングループ：ActionGroup1
* アラートルール名：Alert1

次の設定を持つアクションルールを作成します。

* スコープ：VM1
* フィルター基準：リソースタイプ=「仮想マシン」
* このスコープで定義：抑制
* 抑制構成：これから（常に）
* 名前：ActionRule1

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



正解： 

ボックス1：

アクションルールのスコープはVM1に設定され、アラートを無期限に抑制するように設定されています。

ボックス2：

アクションルールのスコープがVM2に設定されていません。

ボックス3：

タグの追加は管理操作ではありません。

参照：

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

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

# Q.58

DRAGのDROP -

あなたはLAW1という名前Azureのログ解析ワークスペースが含まれてSub1を命名Azureのサブスクリプションを持っています。

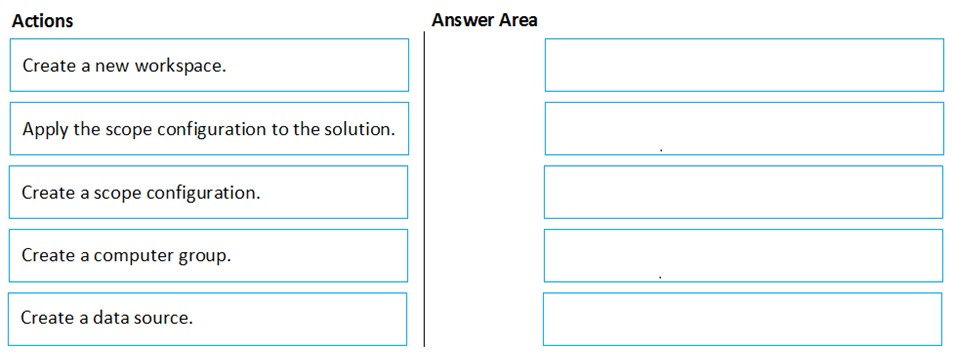
Windows Server 2016を実行し、LAW1に登録されている500台のAzure仮想マシンがあります。

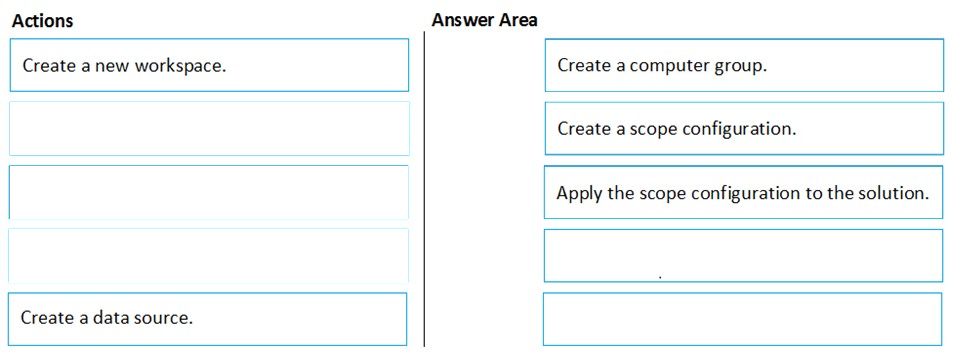
LAW1にシステム更新評価ソリューションを追加する予定です。

システム更新評価関連のログが100台の仮想マシンからのみLAW1にアップロードされていることを確認する必要があります。

どの3つのアクションを順番に実行する必要がありますか？

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



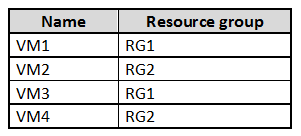
正解： 

リファレンス：

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting>

# Q.59

次の表に示す仮想マシンを含むSub1という名前のAzureサブスクリプションがあります。



承認されたユーザーがアクセスを要求するまで、RG1の仮想マシンのリモートデスクトップポートが閉じていることを確認する必要があります。

何を構成する必要がありますか？

1. Azure Active Directory（Azure AD）特権ID管理（PIM）
2. アプリケーションセキュリティグループ
3. Azure Active Directory（Azure AD）の条件付きアクセス
4. ジャストインタイム（JIT）VMアクセス

正解： *D*

ジャストインタイム（JIT）仮想マシン（VM）アクセスを使用して、Azure VMへのインバウンドトラフィックをロックダウンし、攻撃への露出を減らし、必要なときにVMに接続するための簡単なアクセスを提供できます。

注：ジャストインタイムが有効になっている場合、セキュリティセンターは、NSGルールを作成することにより、AzureVMへのインバウンドトラフィックをロックダウンします。インバウンドトラフィックがロックダウンされるVM上のポートを選択します。これらのポートは、ジャストインタイムソリューションによって制御されます。

ユーザーがVMへのアクセスを要求すると、セキュリティセンターは、ユーザーがVMへのアクセスを正常に要求できるようにするロールベースのアクセス制御（RBAC）アクセス許可を持っていることを確認します。要求が承認されると、セキュリティセンターは、ネットワークセキュリティグループ（NSG）とAzureファイアウォールを自動的に構成して、指定された期間、選択されたポートと要求された送信元IPアドレスまたは範囲へのインバウンドトラフィックを許可します。期限が切れると、セキュリティ

センターはNSGを以前の状態に復元します。ただし、すでに確立されている接続は中断されていません。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

# Q.60シミュレーション -

仮想マシン用のMicrosoft Antimalwareを使用して、web11597200がマルウェアから保護されていることを確認する必要があり、毎週金曜日の01:00にスキャンされます。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

web11597200という名前の仮想マシンにMicrosoftAntimalware拡張機能をインストールして構成する必要があります。

1. Azureポータルで、検索ボックスに「仮想マシン」と入力し、検索結果から[仮想マシン]を選択してから、[web11597200]を選択します。または、左側のナビゲーションペインで[仮想マシン]を参照します。

2. web11597200のプロパティで、[拡張機能]をクリックします。

3. [追加]ボタンをクリックして、拡張機能を追加します。

4.拡張機能のリストを下にスクロールして、MicrosoftAntimalwareを選択します。

5. [作成]ボタンをクリックします。これにより、Microsoft AntimalwareExtensionの設定ペインが開きます。

6. [スキャン日]フィールドで、[金曜日]を選択します。

7. [スキャン時間]フィールドに60と入力します。スキャン時間は深夜0時以降の分単位で測定されるため、60は01：00、120は02:00などになります。

8.[OK]ボタンをクリックして構成を保存し、拡張機能をインストールします。

# Q.61シミュレーション

あなたはVNET01-Subnet0-NSGのネットワーク・セキュリティ・グループ（NSG）のNetworkSecurityGroupRuleCounterログのイベントは、30日間logs11597200 Azureストレージアカウントに保存されていることを確認する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

NetworkSecurityGroupRuleCounterログの診断ログを構成する必要があります。

1. Azureポータルで、検索ボックスに「ネットワークセキュリティグループ」と入力し、検索結果から[ネットワークセキュリティグループ]を選択してから、[

VNET01-Subnet0-NSG]を選択します。または、左側のナビゲーションペインで[ネットワークセキュリティグループ]を参照します。

2.ネットワークセキュリティグループのプロパティで、[診断設定]をクリックします。

3. [診断設定の追加]リンクをクリックします。

4. [診断設定名]フィールドに名前を入力します。試験にどのような名前を付けてもかまいません。

5. [ログ]セクションで、[NetworkSecurityGroupRuleCounter]を選択します。

6. [宛先の詳細]セクションで、[ストレージアカウントにアーカイブ]を選択します。

7. [ストレージアカウント]フィールドで、logs11597200ストレージアカウントを選択します。

8. [保持（日）]フィールドに30と入力します。

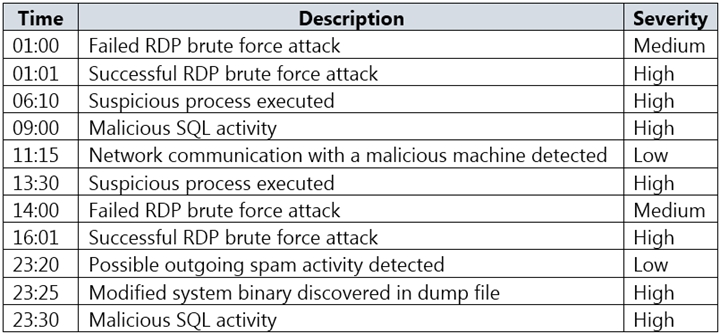
9.[保存]ボタンをクリックして変更を保存します。

# Q.62

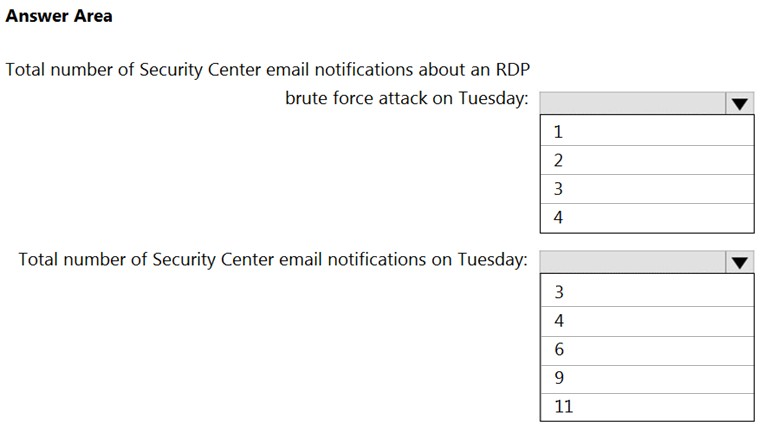
ホットスポット-

月曜日に、Azure Security Centerで、user1 @ contoso.comに通知を電子メールで送信するように電子メール通知を構成します。

火曜日に、セキュリティセンターは次の表に示すセキュリティアラートを生成します。user1@contoso.comは火曜日にいくつの電子メール通知を受け取りますか？

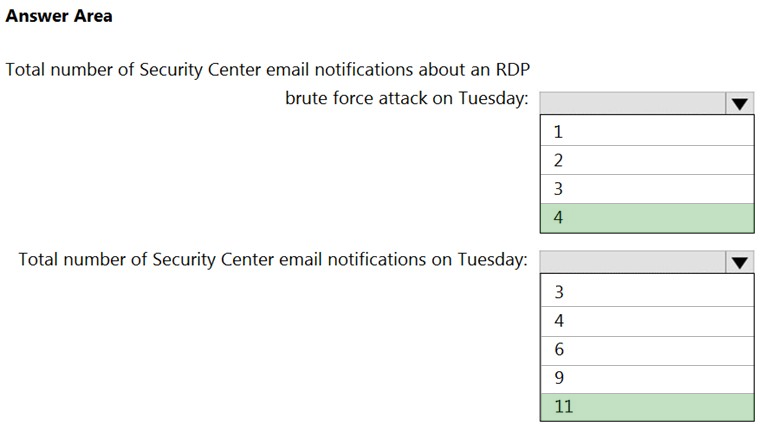


回答するには、回答領域で適切なオプションを選択します。



火曜日のRDPブルートフォース攻撃に関するセキュリティセンターの電子メール通知の総数。

火曜日のセキュリティセンターの電子メール通知の総数。

正解： 

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

# Q.63

AzureStorageアカウントのセキュリティ問題のトラブルシューティングを行っています。

ストレージアカウントの診断ログを有効にします。

診断ログを取得するには何を使用する必要がありますか？

1. Azure Security Center
2. Azure Monitor
3. the Security admin center
4. Azure Storage Explorer

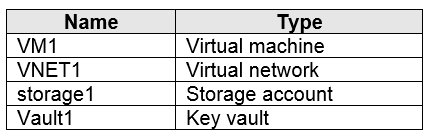
正解： *B*

リファレンス：

<https://docs.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal>

# Q.64

次の表に示すリソースを含むAzureサブスクリプションがあります。



サブスクリプションで Azure Defender を有効にする予定です。

Azure Defender を使用して保護できるリソースはどれですか？

1. VM1、VNET1、storage1、およびVault1
2. VM1、VNET1、およびstorage1のみ
3. VM1、storage1、およびVault1のみ
4. VM1とVNET1のみ
5. VM1とストレージ1のみ

~~Correct Answer: A~~

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

Secure data and applications

討論では、**正解：C**　となっている。

Azure Defenderはどのリソースタイプを保護できますか？

Azure Defenderは、

* 仮想マシン
* SQLデータベース
* コンテナー
* Webアプリケーション
* ネットワーク

などにセキュリティアラートと高度な脅威保護を提供します。

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender#:~:text=What%20resource%20types%20can%20Azure,%2C%20your%20network%2C%20and%20more>

* [Azure Defender for servers](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction)
* [Azure Defender for App Service](https://docs.microsoft.com/en-us/azure/security-center/defender-for-app-service-introduction)
* [Azure Defender for Storage](https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction)
* [Azure Defender for SQL](https://docs.microsoft.com/en-us/azure/security-center/defender-for-sql-introduction)
* [Azure Defender for Kubernetes](https://docs.microsoft.com/en-us/azure/security-center/defender-for-kubernetes-introduction)
* [Azure Defender for container registries](https://docs.microsoft.com/en-us/azure/security-center/defender-for-container-registries-introduction)
* [Azure Defender for Key Vault](https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-introduction)
* [Azure Defender for Resource Manager](https://docs.microsoft.com/en-us/azure/security-center/defender-for-resource-manager-introduction)
* [Azure Defender for DNS](https://docs.microsoft.com/en-us/azure/security-center/defender-for-dns-introduction)