Microsoft.AZ-500.v2022-12-16.q271

試験コード:	AZ-500
試験名称:	Microsoft Azure Security Technologies
認定資格:	Microsoft
無料問題数:	271
バージョン:	v2022-12-16
アクセス数:	2160
ページビュー数:	2710
https://www.jpnpdf.com/Microsoft.AZ-500.v2022-12-16.q271-mondaishu.html	

最新問題: **1**
User1という名前のユーザーとConReg1という名前のAzureContainerRegistryを含むAzureサブスクリプションがあります。
ContReg1のコンテンツ信頼を有効にします。
User1がContReg1で信頼できるイメージを作成できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
User1に割り当てる必要がある2つの役割はどれですか？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。
A. AcrQuarantineReader
B. 寄稿者
C. AcrPush
D. AcrImageSigner
E. AcrQuarantineWriter
Answer: C,D (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

最新問題: **2**
Azure Active Directory（Azure AD）の特権ID管理（PIM）を使用するAzureサブスクリプションがあります。
ユーザーアクセス管理者の役割が割り当てられているPIMユーザーは、役割の割り当てを実行するとき、または割り当てのリストを表示するときに、承認エラーを受け取ったことを報告します。

PIMサービスプリンシパルがサブスクリプションに対して正しい権限を持っていることを確認して、問題を解決する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
PIMサービスの原則にどの役割を割り当てる必要がありますか？
A. リソースポリシーの貢献者
B. 寄稿者
C. ユーザーアクセス管理者
D. マネージドアプリケーションオペレーター
Answer: (解答を表示する**)**

最新問題**: 3**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Active Directory（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AzureHDInsightクラスターがあります。
オンプレミスのActiveDirectory資格情報を使用して、ユーザーがクラスターに対して認証できるようにすることを計画しています。
計画された認証をサポートするように環境を構成する必要があります。
解決策 :オンプレミスデータゲートウェイをオンプレミスネットワークに展開します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: (解答を表示する**)**
代わりに、Azure Virtual NetworksとVPNゲートウェイを使用して、HDInsightをオンプレミスネットワークに接続します。
注：参加しているネットワーク内のHDInsightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。
Azure仮想ネットワークを作成します。
Azure仮想ネットワークにカスタムDNSサーバーを作成します。
デフォルトのAzureRecursiveResolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。
参照：
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network

最新問題**: 4**

次の表に示すAzureInformationProtectionの条件があります。
AzureInformationProtectionがファイルにラベルを付ける方法を特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

最新問題**: 5**
Contosostorage1という名前のAzureストレージアカウントとContosokeyvault1という名前のAzureキーボールトを含むSub1という名前のAzureサブスクリプションがあります。
Contosostorage1のキーをローテーションしてcontosokeyvault1に格納するAzureAutomationRunbookを作成する予定です。
Runbookを実装できるようにするには、前提条件を実装する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
手順1：AzureAutomationアカウントを作成する
RunbookはAzureAutomationアカウント内にあり、PowerShellスクリプトを実行できます。
手順2：PowerShellモジュールをAzureAutomationアカウントにインポートする
Azure Automationアカウントの[リソース]セクションの[アセット]で、[モジュール]をRunbookに追加するために[]を選択します。Runbookでキーボールトコマンドレットを実行するには、AzureRM.profileとAzureRM.keyボールトを追加する必要があります。
手順3：AzureAutomationアカウントで接続リソースを作成する
AzureAutomationTutorialScriptサンプルRunbookから取得した以下のサンプルコードを使用して、Run Asアカウントを使用して認証し、RunbookでResourceManagerリソースを管理できます。AzureRunAsConnectionは、上記の「アカウントとして実行」を作成したときに自動的に作成された接続アセットです。
これは、[アセット]->[接続]にあります。認証コードの後で、上記と同じコードを実行して、ボールトからすべてのキーを取得します。
$ connectionName = "AzureRunAsConnection"
試す
{{
＃接続「AzureRunAsConnection」を取得します
$ servicePrincipalConnection = Get-AutomationConnection -Name $ connectionName
「Azureにログインしています...」

Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $ servicePrincipalConnection.TenantId `
-ApplicationId $ servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $ servicePrincipalConnection.CertificateThumbprint
}
参照：
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

最新問題**: 6**
次の表に示すリソースを含むSubcription1という名前のAzureサブスクリプションがあります。
次のリソースを含むSubcription2という名前のAzureサブスクリプションがあります。
AzureSentinelワークスペース
Azureイベントグリッドインスタンス
NVAからAzureSentinelにCEFメッセージを取り込む必要があります。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 7**
Azure Active Directory（Azure AD）のハイブリッド構成があります。
すべてのユーザーは、Windows 10を実行し、ハイブリッドAzureADに参加しているコンピューターを持っています。
AzureAD認証をサポートするように構成されたAzureSQL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 Studio（SSMS）を使用してSQLデータベースに接続し、オンプレミスのActiveDirectoryアカウントを使用して認証する必要があります。
SSMSからSQLデータベースに接続するために使用する認証方法を開発者に伝える必要があります。ソリューションは、認証プロンプトを最小限に抑える必要があります。
開発者に使用するように指示する必要がある認証方法はどれですか？
A. SQLログイン
B. ActiveDirectory-MFAをサポートするユニバーサル
C. ActiveDirectory-統合
D. ActiveDirectory-パスワード
Answer: (解答を表示する**)**
説明
Azure ADは、最初のAzureAD管理対象ドメインにすることができます。Azure ADは、AzureADとフェデレーションされているオンプレミスのActiveDirectoryドメインサービスにすることもできます。
AzureADIDを使用してSSMSまたはSSDTを使用して接続する

次の手順は、SQL Server ManagementStudioまたはSQLServerデータベースツールを使用して、AzureADIDでSQLデータベースに接続する方法を示しています。
ActiveDirectory統合認証
フェデレーションドメインからAzureActiveDirectoryクレデンシャルを使用してWindowsにログインしている場合は、この方法を使用します。
1. ManagementStudioまたはDataTools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]）ダイアログボックスの[認証]ボックスで、[ActiveDirectory]-[統合]を選択します。接続には既存のクレデンシャルが表示されるため、パスワードは不要であるか、入力できます。
2. [オプション]ボタンを選択し、[接続のプロパティ]ページの[データベースに接続]ボックスに、接続するユーザーデータベースの名前を入力します。 ADドメイン名またはテナントID "オプションは、MFA接続オプションを備えたユニバーサルでのみサポートされます。それ以外の場合はグレー表示されます。）参照：
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-c

最新問題**: 8**
月曜日に、Azure Security Centerで電子メール通知を構成して、ユーザーuser1@contoso.comに通知します。
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は火曜日に何通の電子メール通知を受け取りますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

最新問題**: 9**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168

Microsoft Antimalware for Virtual Machinesを使用して、VM1という名前の仮想マシンで毎週日曜日の02:00に完全なマルウェアスキャンを実行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。
Answer:
以下の説明を参照してください。
説明
AzurePortalを使用してMicrosoftAntimalwareExtensionをデプロイし、単一のVMをデプロイします
1. Azureポータルで、Azure VM1のブレードに移動し、[拡張機能]セクションに移動して、[追加]を押します。
2. Microsoft Antimalware拡張機能を選択し、[作成]を押します。
3.必要に応じて「拡張機能のインストール」フォームに入力し、「OK」を押します。スケジュール：EnableScanタイプ：FullScan日：
日曜日
参照：
https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

最新問題**: 10**
注：この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Active Directory（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AzureHDInsightクラスターがあります。
オンプレミスのActiveDirectory資格情報を使用して、ユーザーがクラスターに対して認証できるようにすることを計画しています。
計画された認証をサポートするように環境を構成する必要があります。
解決策：オンプレミスデータゲートウェイをオンプレミスネットワークに展開します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
説明
代わりに、Azure Virtual NetworksとVPNゲートウェイを使用して、HDInsightをオンプレミスネットワークに接続します。
注：参加しているネットワーク内のHDInsightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。

Azure仮想ネットワークを作成します。
Azure仮想ネットワークにカスタムDNSサーバーを作成します。
デフォルトのAzureRecursiveResolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。
参照：
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network

最新問題**: 11**
セキュリティ運用要件を確実に満たす必要があります。
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オンにします。
B. セキュリティセンターとMicrosoft CloudAppSecurityを統合します。
C. 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。
D. セキュリティセンターのワークスペース構成を変更します。
Answer: (解答を表示する**)**
標準層は、無料層の機能をプライベートクラウドやその他のパブリッククラウドで実行されているワークロードに拡張し、ハイブリッドクラウドワークロード全体で統合されたセキュリティ管理と脅威保護を提供します。標準層には、高度な脅威検出機能も追加されています。これは、組み込みの行動分析と機械学習を使用して攻撃とゼロデイエクスプロイトを識別し、アクセスとアプリケーションの制御を使用してネットワーク攻撃とマルウェアへの露出を減らします。
シナリオ :セキュリティ運用要件
Litwareは、AzureSecurityCenterの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。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing
トピック2、Contoso
技術要件
Contosoは、次の技術要件を識別します。
Sub2のVNetWork1にAzureファイアウォールをデプロイします。
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、最小特権の原則を使用してください。
contoso.comのAzureAD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。
User2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。
サブ2
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は、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。各仮想マシンのファイアウォールは、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ルールがあります。
NSG2には、次の表に示すインバウンドセキュリティルールがあります。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
NSG4には、次の表に示すインバウンドセキュリティルールがあります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示すアウトバウンドセキュリティルールがあります。
Contosoは、次の技術要件を識別します。
Sub2のVNetwork1にAzureファイアウォールをデプロイします。
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、最小特権の原則を使用してください。
contoso.comに対してAzureAD特権ID管理（PIM）を有効にします。

最新問題**: 12**
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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 13**
管理者がホームページアプリのサービスプランに誤って変更を加えない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。
Answer:
以下の説明を参照してください。
説明

アプリサービスプランの「ロック」を構成する必要があります。読み取り専用ロックを使用すると、最初にロックを削除せずにアプリサービスプランを変更することはできません。
* Azureポータルで、検索ボックスに「App Service Plans」と入力し、検索結果から[App Service Plans]を選択して、[ホームページ]を選択します。または、左側のナビゲーションペインで[AppServicePlans]を参照します。
*アプリサービスプランのプロパティで、[ロック]をクリックします。
* [追加]ボタンをクリックして、新しいロックを追加します。
*[ロック名]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構いません。
* [ロックの種類]で、[読み取り専用]を選択します。
*[OK]をクリックして変更を保存します。

最新問題**: 14**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
Azure AD Privileged Identity Management（PIM）では、コントリビューターロールのロール設定は、展示に示されているように構成されます。（[展示]タブをクリックします。）
次の表に示すように、2019年5月1日にユーザーにコントリビューターの役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
Explanation:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

最新問題**: 15**
次のリソースを含むAzureサブスクリプションがあります。
*Azureキーボールト
*Database1という名前のAzureSQLデータベース
*システムによって割り当てられた管理対象IDを使用してDatabase1にアクセスするように構成されたAppSrv1およびAppSrv2という名前の2つのAzureAppServiceWebアプリ次の要件を満たすDatabase1の暗号化ソリューションを実装する必要があります。
* AppSrv1のみがデータを復号化できるように、Database1のDiscountという名前の列のデータを暗号化する必要があります。
* AppSrv1およびAppSrv2は、暗号化キーを取得するために管理対象IDを使用して承認される必要があります。
Database1の暗号化設定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てください。

注：正しい選択はそれぞれ1ポイントの価値があります
Answer:
参照：
https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell

最新問題: **16**
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がリソースグループに割り当てられます。
どのリソースが行うかを特定する必要があります
あなたは何をするべきか？
A. Azure Security Centerから、規制コンプライアンス評価を表示します。
B. 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。
C. Azure Security Centerから、セキュアスコアを表示します。
D. 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。
Answer: B (メーッセージを残す)
参照：
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal

最新問題: **17**
Azureサブスクリプションがあります。
S1Appサービスプランを使用するContoso1812という名前のAzureWeb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 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。
実行する必要がある2つのアクションはどれですか？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。
A. Contoso1812のシステム割り当ての管理対象IDをオンにします。
B. Contoso1812にホスト名を追加します。
C. Contoso1812のAppServiceプランをスケールアウトします。
D. Contoso1812に展開スロットを追加します。
E. Contoso1812のAppServiceプランをスケールアップします。
Answer: B,E (メーッセージを残す**)**
B :Webアプリのカスタムドメインをホストするようにに AzureDNSを構成できます。たとえば、次のように作成できます。
Azure Webアプリを使用して、www.contoso.comまたはcontoso.comのいずれかを完全に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、次の3つのレコードを作成する必要があります。
contoso.comを指すルート「A」レコード
検証用のルート「TXT」レコード
Aレコードを指すwww名の「CNAME」レコード
E :カスタムDNS名をWebアプリにマップするには、WebアプリのApp Serviceプランが有料階層（共有
Azure Functionsの基本、標準、プレミアム、または消費）。私
App Serviceプランをスケールアップする：非フリー階層（D1、B1、B2、B3、または本番環境の任意の階層）のいずれかを選択します
カテゴリー）。
参照：
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

最新問題**: 18**
App1という名前のWebアプリとVault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
Vault1にシークレットを保存してアクセスするようにApp1を構成する必要があります。
App1をどのように構成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

最新問題**: 19**
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？
A. Azure Storage Explorer
B. AzureのSQLクエリエディター
C. Windowsのファイルエクスプローラー
D. Azureセキュリティセンター
Answer: (解答を表示する**)**
説明
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ストレージクライアント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。
参照：
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2
https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers

最新問題**: 20**
Sub2のVM1、VM2、およびVM3のセキュリティを評価しています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 21**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス：10598168

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。
Answer:
以下の説明を参照してください。
説明
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]を選択してから、次の項目の選択肢を選択します。
3. Log Analytics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 :LogAnalyticsVM拡張機能を有効にする
WindowsおよびLinux用のLogAnalyticsVM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（手順で作成した名前）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

最新問題**: 22**
次の表に示すユーザーを含むAzureActiveDirectory (Azure AD）テナントがあります。

Azure AD Privileged Identity Management（PIM）では、コントリビューターロールのロール設定は、展示に示されているように構成されます。（展示]タブをクリックします。）
次の表に示すように、2019年5月1日にユーザーにコントリビューターの役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

最新問題**: 23**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
Azure AD Privileged Identity Management（PIM）では、コントリビューターロールのロール設定は、展示に示されているように構成されます。（展示]タブをクリックします。）
次の表に示すように、2019年5月1日にユーザーにコントリビューターの役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assig

最新問題**: 24**
注：この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Sub1という名前のAzureサブスクリプションがあります。
RG1という名前のリソースグループにSa1という名前のAzureStorageアカウントがあります。
ユーザーとアプリケーションは、いくつかの共有アクセス署名（SAS）と保存されたアクセスポリシーを使用して、Sa1のblobサービスとファイルサービスにアクセスします。

許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。
Sa1へのすべてのアクセスを取り消す必要があります。
解決策：新しいSASを生成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
代わりに、新しい保存済みアクセスポリシーを作成する必要があります。
保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。
署名された識別子を変更すると、既存の署名と保存されているアクセスポリシーの間の関連付けが解除されます。保存されたアクセスポリシーを削除または名前変更すると、それに関連付けられているすべての共有アクセス署名にすぐに影響します。
参照：
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

最新問題**: 25**
あなたの会社はシアトルとニューヨークに2つのオフィスを持っています。各オフィスは、NATデバイスを使用してインターネットに接続します。次の表に示すIPアドレスを使用します。
同社には、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれています。
MFAサービス設定は、展示に示されているように構成されています。（展示]タブをクリックします。）
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス2：いいえ
MicrosoftAuthenticatorを使用する必要はありません。
注：Microsoft Authenticatorは、2段階認証プロセスで使用される時間ベースのコードを生成するモバイルデバイス用の多要素アプリです。
ボックス3：いいえ
ニューヨークのIPアドレスサブネットは、「リクエストの多要素認証をスキップする」に含まれています。
参照：

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

最新問題**: 26**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。
各ユーザーには、Azure ADPremiumP2ライセンスが割り当てられます。
オンボードで計画し、AzureADID保護を構成します。
Azure AD Identity Protectionをオンボードし、ユーザーを修正し、ポリシーを構成できるユーザーはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります
Answer:

最新問題**: 27**
プラットフォーム保護要件を満たすには、AKS1を展開する必要があります。
順番に実行する必要がある4つのアクションはどれですか？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、正しい順序に並べます。
注：回答の選択肢の複数の順序が正しいです。選択した正しい注文のいずれかに対してクレジットを受け取ります。
Answer:
説明
シナリオ：Azure ADユーザーは、AzureADクレデンシャルを使用してAKS1に対して認証する必要があります。
Litewireは、マネージドAKS（Azure Kubernetes Services）クラスターであるAKS1をデプロイすることを計画しています。
ステップ1：サーバーアプリケーションを作成する
AKSクラスターにAzureAD認証を提供するために、2つのAzureADアプリケーションが作成されます。最初のアプリケーションは、ユーザー認証を提供するサーバーコンポーネントです。
ステップ2：クライアントアプリケーションを作成する
2番目のアプリケーションは、CLIから認証を求められたときに使用されるクライアントコンポーネントです。
このクライアントアプリケーションは、クライアントによって提供された資格情報の実際の認証にサーバーアプリケーションを使用します。
ステップ3：AKSクラスターをデプロイします。
az group createコマンドを使用して、AKSクラスターのリソースグループを作成します。
az aks createコマンドを使用して、AKSクラスターをデプロイします。
手順4：RBACバインディングを作成します。

AKSクラスターでAzureActiveDirectoryアカウントを使用する前に、ロールバインディングまたはクラスターロールバインディングを作成する必要があります。ロールは付与する権限を定義し、バインディングはそれらを目的のユーザーに適用します。これらの割り当ては、特定の名前空間に適用することも、クラスター全体に適用することもできます。
参照：
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration
トピック1、Contoso仮想マシンがロードされるまでお待ちください。一度
ロードされたら、ラボセクションに進むことができます。これには少し時間がかかる場合があります
分、そして待機時間はあなたの全体から差し引かれません
テスト時間。
[次へ]ボタンが使用可能になったら、それをクリックしてラボセクションにアクセスします。このセクションでは、ライブ環境で一連のタスクを実行します。ほとんどの機能はライブ環境と同じように利用できますが、一部の機能 ロピーと貼り付け、外部Webサイトへの移動機能など）は設計上不可能です。
スコアリングは、ラボで説明されているタスクを実行した結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行すると、そのタスクのクレジットを獲得できます。
ラボの時間は個別に設定されていません。この試験には、完了する必要のあるラボが複数ある場合があります。各ラボを完了するのに必要なだけの時間を使用できます。ただし、ラボを完了できるように時間を適切に管理する必要があります。ラボ内の[次へ]ボタンをクリックして作業を送信したら、注意してください。
タスク1：
インターネットからVM1という名前の仮想マシンへのRDP接続を許可するようにAzureを構成する必要があります。
ソリューションは、VM1の攻撃対象領域を最小限に抑える必要があります。
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。
タスク2：
VM1という名前の仮想マシンのネットワークインターフェイスを、ASG1という名前のアプリケーションセキュリティグループに追加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。
タスク3：
Microsoft Antimalware for Virtual Machinesを使用して、VM1という名前の仮想マシンで毎週日曜日の02:00に完全なマルウェアスキャンを実行する必要があります。
タスク4：
あなたの会社の開発者は、App103178O6という名前のWebアプリを作成し、そのアプリをhtlps ://www.contoso.comに公開することを計画しています。
次のタスクを実行する必要があります。
*App10317806がAzureActiveDirectory Azure AD）に登録されていることを確認します。

*App10317806のパスワードを生成します。
タスク5：
管理ユーザーがVNET1という名前の仮想ネットワークを誤って削除しないようにする必要があります。管理ユーザーは、VNET1の設定を変更できるようにする必要があります。
タスク6：
user2103l7806という名前のユーザーが、RG1lod10317806リソースグループ内の仮想マシンのプロパティを管理できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
タスク7：
131.107.0.0/16サブネットに接続されているデバイスのみが、railod10317806 Azureストレージアカウントのデータにアクセスできるようにする必要があります。タスク8：
VM1という名前の仮想マシンの平均CPU使用率が15分間で70%を超える場合は、admin1@contoso.comという名前の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。
タスク9：
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。
タスク10：
rg1lodl03l7806n1AzureStorageアカウントへのHTTP接続を防ぐ必要があります。
タスク11：
KeyVault10317806 Azureキーボールトに格納されているキーを使用して、rg1lod10317806n1Azureストレージアカウントが暗号化されていることを確認する必要があります。
タスク12：
10317806.onmicrosoft.comという名前の新しいAzureActiveDirectory（Azure AD）ディレクトリを作成する必要があります。
新しいディレクトリには、Azure Multi-Factor Authentication（MFA）を使用してサインインするように構成されたuserl103l7806.onmicrosoft.comという名前のユーザーが含まれている必要があります。
これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。提供された時間内にこの試験に含まれるすべての質問を確実に完了することができるように、時間を管理する必要があります。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナ

リオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。各質問は、このケーススタディの他の質問とは無関係です。
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。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、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には
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ます。質問に答える前に、左側のペインのボタンを使用して、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、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。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質問に戻ります。
概要
Contoso、Ltd.は、モントリオールに本社を置き、シアトルとニューヨークに2つの支店を持つコンサルティング会社です。
同社は、サーバーインフラストラクチャ全体をAzureでホストしています。
Contosoには、Sub1とSub2という名前の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）テナントに関連付けられています。
技術要件
Contosoは、次の技術要件を識別します。
*AzureファイアウォールをSub2のVNetWork1にデプロイします。
*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、最小特権の原則を使用してください。
*contoso.comのAzureAD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。
User2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。
サブ2
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は、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。各仮想マシンのファイアウォールは、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ルールがあります。
NSG2には、次の表に示すインバウンドセキュリティルールがあります。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
NSG4には、次の表に示すインバウンドセキュリティルールがあります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示すアウトバウンドセキュリティルールがあります。
Contosoは、次の技術要件を識別します。
*AzureファイアウォールをSub2のVNetwork1にデプロイします。
*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、最小特権の原則を使用してください。
* contoso.comに対してAzureAD特権ID管理（PIM）を有効にします。

最新問題: **28**
次の表に示すリソースを含むSub1という名前のAzureサブスクリプションがあります。
含まれているデータベースユーザーを使用して、VM1にSQL1上のデータベースへの安全なアクセスを提供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？
A. VM1でマネージドサービスIDを有効にします。
B. KV1でシークレットを作成します。
C. SQL1でサービスエンドポイントを構成します。
D. KV1でキーを作成します。
Answer: A (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm

最新問題: **29**
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
2019年1月1日、Vault1は次のシークレットを保存します。
アプリケーションが各シークレットを使用できるのはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

最新問題: **30**

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。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 31**
AzureADアプリケーションの登録と同意の構成がIDとアクセスの要件を満たしていることを確認する必要があります。
Azureポータルで何を使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consentこれはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。提供された時間内にこの試験に含まれるすべての質問を確実に完了することができるように、時間を管理する必要があります。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。各質問は、このケーススタディの他の質問とは無関係です。
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。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、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には
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ます。質問に答える前に、左側のペインのボタンを使用して、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、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタ

ブに表示される情報と同じであることに注意してください。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質問に戻ります。
概要
Contoso、Ltd.は、モントリオールに本社を置き、シアトルとニューヨークに2つの支店を持つコンサルティング会社です。
同社は、サーバーインフラストラクチャ全体をAzureでホストしています。
Contosoには、Sub1とSub2という名前の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）テナントに関連付けられています。
トピック3、Fabrikam Inc
総括
Fabrikam、Inc.は、モントリオールに本社を置き、シアトルとニューヨークに支社を置くコンサルティング会社です。Fabrikamには、IT、人材（HR）、および財務部門があります。
既存の環境
ネットワーク環境
Fabrikamには、Microsoft365サブスクリプションとsubscription1という名前のAzureサブスクリプションがあります。
ネットワークには、Fabrikam.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。ドメインには、OU1およびOU2という名前の2つの組織単位（OU）が含まれています。AzureADConnectクラウド同期はOU1のみを同期します。
次の展示では、Azureリソースの階層を示しています。
Azure Active Directory（Azure AD）テナントには、次の表に示すユーザーが含まれています。
Azure ADには、次の表に示すリソースが含まれています。
Subscription1リソース
Subscription1には、次の表に示す仮想ネットワークが含まれています。
Subscription1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。
Subscription1には、次の表に示す仮想マシンが含まれています。
Subscription1には、次の表に示すAzureキーボールトが含まれています。
Subscription1には、米国西部のAzureリージョンにあるstorage1という名前のストレージアカウントが含まれています。
計画された変更と要件
計画された変更
Fabrikamは、次の変更を実装する予定です。
次の表に示すように、2つのアプリケーションセキュリティグループを作成します。
VM1のネットワークインターフェイスをASG1に関連付けます。
AzureSecurityCenterを使用してSecPol1をデプロイします。

App1という名前のサードパーティアプリをデプロイします。App1のバージョンは、使用可能なすべてのオペレーティングシステムに対応しています。
RG2という名前のリソースグループを作成します。
OU2をAzureADに同期します。
User1をGroup1に追加します。
技術要件
Fabrikamは、次の技術要件を識別します。
財務部門のユーザーは、SharePointOnlineにアクセスする3時間後に再認証する必要があります。
Storage1は、顧客が管理するキーと自動キーローテーションを使用して暗号化する必要があります。
Sentinel1から、次のノートブックを起動できることを確認する必要があります。
エンティティエクスプローラーアカウント
エンティティエクスプローラーWindowsホスト
ガイド付き調査プロセスアラート
VM1、VM2、およびVM3は、AzureDiskEncryptionを使用して暗号化する必要があります。
VM1、VM2、およびVM3のジャストインタイム（JIT）VMアクセスを有効にする必要があります。
App1は、KeyVault1に保存されている安全な接続文字列を使用する必要があります。
KeyVault1トラフィックはインターネット上を移動してはなりません。

最新問題: **32**
User2がPIMを実装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？
A. User2にグローバル管理者の役割を割り当てます。
B. contoso.comの認証方法を構成します。
C. contoso.comのIDセキュア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。
Answer: (解答を表示する**)**
説明
ディレクトリでPIMの使用を開始するには、最初に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。
ディレクトリのPIMを有効にするには、Microsoftアカウント（@ outlook.comなど）ではなく、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。
シナリオ：技術要件は次のとおりです。contoso.comのAzure AD特権ID管理（PIM）を有効にする参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-starte

最新問題: **33**
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？
A. VM3のみ
B. VM1およびVM3のみ
C. VM3およびVM4のみ
D. VM1、VM2、VM3、およびVM4
Answer: D (メーッセージを残す)
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AzureVMと作成された新しいVMでMicrosoftMonitoringAgent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）、および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

最新問題: **34**
LAW1という名前のAzureLogAnalytics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 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。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
参照：

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

最新問題: **35**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
3つのAzureサブスクリプションの集中ポリシー管理にAzureSecurityCenter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？
A. はい
B. いいえ
Answer: (解答を表示する**)**
説明
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-managementgroups/

最新問題: **36**
QUESTION NO: 181次の表に示すAzureInformationProtectionの条件があります
。
AzureInformationProtectionがファイルにラベルを付ける方法を特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

最新問題: **37**

https://www.contoso.comのURLを使用してアクセスするオンプレミスサーバーでホストされているWebアプリがあります。Webアプリをazureに移行することを計画しています。引き続きhttps://www.contoso.comを使用します。AzureWebアプリでHTTPSを有効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. オンプレミスサーバーから公開鍵をエクスポートし、その鍵をP7bファイルとして保存します。
B. オンプレミスサーバーから秘密鍵をエクスポートし、TripleDESを使用して暗号化されたPFXファイルとして鍵を保存します。
C. オンプレミスサーバーから公開鍵をエクスポートし、CERファイルとして保存します。
D. オンプレミスサーバーから秘密鍵をエクスポートし、AES256を使用して暗号化されたPFXファイルとして鍵を保存します。
Answer: B (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

最新問題**: 38**
次の表に示すAzureキーボールトがあります。
KV1は、Secret1という名前のシークレットと、Key1という名前の管理対象ストレージアカウントのキーを格納します。
Secret1とKey1をバックアップします。
各バックアップをどの主要なボールトに復元できますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
バックアップは、同じサブスクリプションおよび同じ地域の主要なボールトにのみ復元できます。同じ地域の別の地域に復元できます。

最新問題**: 39**
Azureサブスクリプションを作成します。
Azure Active Directory（Azure AD）の特権ID管理（PIM）を使用してAzureADの役割を保護できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
ステップ1：PIMへの同意
手順：2多要素認証（MFA）を使用してIDを確認する[IDの確認]をクリックして、AzureMFAでIDを確認します。アカウントを選択するように求められます。

手順3 :AzureADの役割にPIMをサインアップする
ディレクトリに対してPIMを有効にしたら、AzureADの役割を管理するためにPIMにサインアップする必要があります。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

最新問題**: 40**
次の表に示すように、Azureサブスクリプションにリソースを作成します。
VNET1には、Subnet1およびSubnet2という名前の2つのサブネットが含まれています。Subnet1のネットワークIDは10.0.0.0/24です。Subnet2のネットワークIDは10.1.1.0/24です。
Contoso1901は、展示に示されているように構成されています。 [展示]タブをクリックします。）
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :はい
Subnet1からのアクセスが許可されます。
ボックス2 :いいえ
Subnet2からのアクセスは許可されていません。
ボックス3 :はい
IPアドレス193.77.10.2からのアクセスが許可されます。

最新問題**: 41**
AzureサブスクリプションマットにRG1という名前のリソースグループが含まれています。RG1には、storage1という名前のストレージアカウントが含まれています。
RG1をスコープとするRole1とRole2という名前の2つのカスタムAzureロートがあります。
Role1の権限は、次のJSONコードに示されています。
Answer:

最新問題**: 42**
更新管理が有効になっているAzure仮想マシンがあります。仮想マシンは、次の表に示すように構成されています。
Update1とUpdate2という名前の2つの更新デプロイメントをスケジュールします。Update1はVM3を更新します。Update2はVM6を更新します。

Update1とUpdate2を使用して更新できる追加の仮想マシンはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

最新問題**: 43**
Azureサブスクリプションを作成します。
Azure Active Directory（Azure AD）の特権ID管理（PIM）を使用してAzureADの役割を保護できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
ステップ1：PIMへの同意
手順2：多要素認証（MFA）を使用してIDを確認する[IDの確認]をクリックして、AzureMFAでIDを確認します。アカウントを選択するように求められます。
手順3：AzureADの役割にPIMをサインアップする
ディレクトリに対してPIMを有効にしたら、AzureADの役割を管理するためにPIMにサインアップする必要があります。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

最新問題**: 44**
Azure Active Directory（Azure AD）のハイブリッド構成があります。AzureAD認証をサポートするように構成されたAzureSQLデータベースインスタンスがあります。
データベース開発者は、データベースインスタンスに接続し、オンプレミスのActiveDirectoryアカウントを使用して認証する必要があります。
開発者がMicrosoftSQLServerManagementStudioを使用してインスタンスに接続できることを確認する必要があります。ソリューションは、認証プロンプトを最小限に抑える必要があります。
どの認証方法をお勧めしますか？
A. ActiveDirectory-パスワード
B. ActiveDirectory-MFAをサポートするユニバーサル
C. SQLServer認証
D. ActiveDirectory-統合
Answer: (解答を表示する**)**
参照：

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

最新問題**: 45**
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と思われます。
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ために、AzureLogAnalyticsクエリを作成する必要があります。結果には、サインインに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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
次の例では、前日に5回以上ログインに失敗したユーザーアカウントと、最後にログインを試みた日時を特定します。
時間枠=1dとします。
SecurityEvent
| ここでTimeGenerated>ago（1d）
| ここで、AccountType=='User'およびEventID==4625//4625-ログインに失敗しました
| アカウントごとにfailed_login_attempts=count（）、latest_failed_login =
arg_max（TimeGenerated、Account）を要約します
| ここでfailed_login_attempts>5
| プロジェクトアウェイアカウント1
参照：
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

最新問題**: 46**
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、述べられた目標を達成する可能性のある独自のソリューションが含まれています。いくつかの質問セット
正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。
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。結果として、これらは
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AzureStorageアカウントがあります。
ユーザーとアプリケーションは、いくつかの共有アクセスを使用して、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）と保存されたアクセスポリシー。

許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。
Sa1へのすべてのアクセスを取り消す必要があります。
解決策：新しい保存済みアクセスポリシーを作成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: (解答を表示する**)**
説明/参照：
Explanation:
保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。
署名された識別子を変更すると、既存の署名と保存されている署名の間の関連付けが解除されます
アクセスポリシー。保存されたアクセスポリシーを削除または名前変更すると、すべての共有アクセスにすぐに影響します
それに関連付けられた署名。
参照：
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

最新問題**: 47**
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。
実行する必要がある2つのアクションはどれですか？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。
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オンにします。
C. 最小TLSバージョンプロトコル設定を1.2に設定します。
D. AppServiceプランの料金階層を変更します。
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。

Answer: B,E (メーッセージを残す)
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-authを参照してください
トピック1、Litware、inc
既存の環境
Litwareには、サブスクリプションIDが43894a43-17c2-4a39-8cfc-3540c2653ef4のSub1という名前のAzureサブスクリプションがあります。
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。テナントには、すべてのLitware従業員とそのデバイスのユーザー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。各ユーザーには、Azure ADPremiumP2ライセンスが割り当てられます。Azure AD特権ID管理（PIM）がアクティブ化されます。
テナントには、次の表に示すグループが含まれています。
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。
AzureSecurityCenterは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ことを計画しています。
Litwareは、次のID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のメンバーである必要があります。
Group2のメンバーは、永続的な適格な割り当てを使用して、ResourceGroup2にContributorロールを割り当てる必要があります。
ユーザーは、Azure ADにアプリケーションを登録したり、ユーザーに代わって会社の情報にアクセスする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。
プラットフォーム保護要件
Litwareは、次のプラットフォーム保護要件を識別します。
Microsoft Antimalwareは、ResourceGroup1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、AzureKubernetesサービスクラスターの管理者ロールを割り当てる必要があります。
Azure ADユーザーは、AzureADクレデンシャルを使用してAKS1に対して認証する必要があります。
計画された変更の実装後、ITチームはJITVMアクセスを使用してVM0に接続できる必要があります。
リソースグループ1の管理対象ディスクの管理を委任するには、Role1という名前の新しいカスタムRBACロールを使用する必要があります。Role1は、ResourceGroup1でのみ使用可能である必要があります。
セキュリティ運用要件

Litwareは、AzureSecurityCenterの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。

最新問題: **48**
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。
許可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。
何を設定する必要がありますか？
A. Azure Active Directory（Azure AD）特権ID管理（PIM）
B. アプリケーションセキュリティグループ
C. Azure Active Directory（Azure AD）の条件付きアクセス
D. ジャストインタイム（JIT）VMアクセス
Answer: D (メーッセージを残す**)**
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役割ベースのアクセス制御（RBAC）権限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安全なデータとアプリケーションテストレット1これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。提供された時間内にこの試験に含まれるすべての質問を確実に完了することができるように、時間を管理する必要があります。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、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の最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、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には
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ます。質問に答える前に、左側のペインのボタンを使用して、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、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。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質問に戻ります。
概要
Litware、Inc.は、シカゴ地域に500人の従業員を擁し、サンフランシスコ地域に20人の従業員を擁するデジタルメディア企業です。
既存の環境
Litwareには、サブスクリプションIDが43894a43-17c2-4a39-8cfc-のSub1という名前のAzureサブスクリプションがあります。
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。テナントには、すべてのLitware従業員とそのデバイスのユーザー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。各ユーザーには、Azure ADPremiumP2ライセンスが割り当てられます。Azure AD特権ID管理（PIM）がアクティブ化されます。
テナントには、次の表に示すグループが含まれています。
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。
AzureSecurityCenterは標準層に設定されています。
要件
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ことを計画しています。
IDとアクセスの要件
Litwareは、次のID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のメンバーである必要があります。
* Group2のメンバーは、永続的な適格な割り当てを使用して、RG2にコントリビューターの役割を割り当てる必要があります。
*ユーザーは、Azure ADにアプリケーションを登録したり、ユーザーに代わって会社情報にアクセスする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。
プラットフォーム保護要件
* Litwareは、次のプラットフォーム保護要件を識別します。
* Microsoft Antimalwareは、RG1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、AzureKubernetesサービスクラスターの管理者ロールを割り当てる必要があります。
* Azure ADユーザーは、AzureADクレデンシャルを使用してAKS1に対して認証できる必要があります。
*計画された変更の実装後、ITチームはJITVMアクセスを使用してVM0に接続できる必要があります。
* RG1の管理対象ディスクの管理を委任するには、Role1という名前の新しいカスタムRBACロールを使用する必要があります。Role1は、RG1でのみ使用可能である必要があります。
セキュリティ運用要件
Litwareは、AzureSecurityCenterの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。
データとアプリケーションの要件
Litwareは、次のデータとアプリケーションの要件を識別します。
* Group2のユーザーは、AzureADクレデンシャルを使用してSQLDB1に対して認証できる必要があります。
*WebApp1は相互認証を実施する必要があります。
一般要件
Litwareは、次の一般的な要件を識別します。
*可能な限り、管理作業を最小限に抑える必要があります。
*可能な限り、自動化を最大限に活用する必要があります。

最新問題**: 49**
次の表に示すAzureInformationProtectionの条件があります。
AzureInformationProtectionがファイルにラベルを付ける方法を特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

最新問題**: 50**
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。
次の構成を持つAzureキーボールトを作成します。
名前 :Vault5
地域：米国西部
リソースグループ :RG1

VM1でAzureDiskEncryptionを有効にするには、Vault5を使用する必要があります。ソリューションは、AzureBackupを使用したVM1のバックアップをサポートする必要があります。
どの主要なボールト設定を構成する必要がありますか？
A. アクセスポリシー
B. 秘密
C. キー
D. ロック
Answer: A (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

最新問題**: 51**
次の表に示すように、Azureサブスクリプションにリソースを作成します。
VNET1には、Subnet1およびSubnet2という名前の2つのサブネットが含まれています。Subnet1のネットワークIDは10.0.0.0/24です。Subnet2のネットワークIDは10.1.1.0/24です。
Contoso1901は、展示に示されているように構成されています。 [展示]タブをクリックします。）
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :はい
Subnet1からのアクセスが許可されます。
ボックス2 :いいえ
Subnet2からのアクセスは許可されていません。
ボックス3 :はい
IPアドレス193.77.10.2からのアクセスが許可されます。

最新問題**: 52**
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。
実行する必要がある2つのアクションはどれですか？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。
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オンにします。
C. 最小TLSバージョンプロトコル設定を1.2に設定します。

D. AppServiceプランの料金階層を変更します。
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。
Answer: A,C (メーッセージを残す**)**
A：Azure Webサイトアプリケーションで使用する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：時間の経過とともに、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てきました。TLS 1.2は、AzureAppServiceで実行されているアプリで利用できる最新バージョンです。
不正解：
B：httpurlもサポートする必要があります。
ノート：
参照：
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-versions/安全なデータとアプリケーション質問セット2

最新問題**: 53**
シミュレーション
複数のWindowsサーバーをWS11641655AzureLogAnalytics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。
A. Azure Monitorは、WindowsイベントログまたはLinux Syslogからイベントを収集し、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を使用して、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。

B. Azure Monitorは、WindowsイベントログまたはLinux Syslogからイベントを収集し、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を使用して、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。
Answer: A (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

最新問題**: 54**
RG1という名前のリソースグループに15台のAzure仮想マシンがあります。
すべての仮想マシンは同一のアプリケーションを実行します。
不正なアプリケーションやマルウェアが仮想マシンで実行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？
A. AzureポリシーをRG1に適用します。
B. Azure Security Centerから、アダプティブアプリケーションコントロールを構成します。
C. Azure Active Directory (Azure AD)ID保護を構成します。
D. RG1にリソースロックを適用します。
Answer: B (メーッセージを残す**)**
セクション :[なし]
Explanation:
アダプティブアプリケーション制御は、AzureSecurityCenterのインテリジェントな自動化されたエンドツーエンドのアプリケーションホワイトリストソリューションです。これは、AzureおよびAzure以外のVM (WindowsおよびLinux)で実行できるアプリケーションを制御するのに役立ちます。これは、他の利点の中でも、マルウェアに対してVMを強化するのに役立ちます。セキュリティセンターは、機械学習を使用してVMで実行されているアプリケーションを分析し、このインテリジェンスを使用して特定のホワイトリストルールを適用するのに役立ちます。

参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

最新問題**: 55**
sql1という名前のAzureSQLデータベースを含むAzureサブスクリプションがあります。
sql1を監査する予定です。
監査ログの宛先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。
Kustoクエリ言語を使用してイベントのクエリをサポートします。
管理作業を最小限に抑えます。
何を設定する必要がありますか？
A. イベントハブ
B. ストレージアカウント
C. LogAnalyticsワークスペース
Answer: C (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

最新問題**: 56**
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、WindowsServerを実行するAzure仮想マシンが含まれています
2016年。
ポリシーを実装して、各仮想マシンにカスタムのアンチウイルス仮想マシン拡張機能がインストールされていることを確認する必要があります。
ポリシーをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :DeployIfNotExists
DeployIfNotExistsは、条件が満たされたときにテンプレート展開を実行します。
ボックス2 :テンプレート
DeployIfNotExistsエフェクトのdetailsプロパティには、照合する関連リソースと実行するテンプレートデプロイメントを定義するすべてのサブプロパティがあります。
展開[必須]
このプロパティには、Microsoft.Resources /deployationリファレンスに渡される完全なテンプレートデプロイメントが含まれている必要があります。
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

最新問題**: 57**
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は、次の表に示すユーザーを含むAzure Active Directory（Azure AD）テナントにリンクされています。
次の表に示すグループを作成します。
Group1とGroup2のメンバーシップルールは、次の展示に示すように構成されています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

最新問題**: 58**
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にメンバーシップルールを追加します。
B. Group1を削除します。メンバーシップの種類がOffice365であるGroup1という名前の新しいグループを作成します。ユーザーとデバイスをグループに追加します。
C. Group1のメンバーシップルールを変更します。
D. Group1のメンバーシップタイプをAssignedに変更します。動的メンバーシップを持つ2つのグループを作成します。Group1に新しいグループを追加します。
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership説明：
シナリオ：
Litwareは、次のIDと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のメンバーである必要があります。
テナントには現在、次のグループが含まれています。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal
トピック1、Litware、inc
既存の環境
Litwareには、サブスクリプションIDが43894a43-17c2-4a39-8cfc-3540c2653ef4のSub1という名前のAzureサブスクリプションがあります。

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。テナントには、すべてのLitware従業員とそのデバイスのユーザー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。各ユーザーには、Azure ADPremiumP2ライセンスが割り当てられます。Azure AD特権ID管理（PIM）がアクティブ化されます。
テナントには、次の表に示すグループが含まれています。
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。
AzureSecurityCenterは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ことを計画しています。
Litwareは、次のID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のメンバーである必要があります。
Group2のメンバーは、永続的な適格な割り当てを使用して、ResourceGroup2にContributorロールを割り当てる必要があります。
ユーザーは、Azure ADにアプリケーションを登録したり、ユーザーに代わって会社の情報にアクセスする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。
プラットフォーム保護要件
Litwareは、次のプラットフォーム保護要件を識別します。
Microsoft Antimalwareは、ResourceGroup1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、AzureKubernetesサービスクラスターの管理者ロールを割り当てる必要があります。
Azure ADユーザーは、AzureADクレデンシャルを使用してAKS1に対して認証する必要があります。
計画された変更の実装後、ITチームはJITVMアクセスを使用してVM0に接続できる必要があります。
リソースグループ1の管理対象ディスクの管理を委任するには、Role1という名前の新しいカスタムRBACロールを使用する必要があります。Role1は、ResourceGroup1でのみ使用可能である必要があります。
セキュリティ運用要件
Litwareは、AzureSecurityCenterの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。

最新問題**: 59**
Group1とGroup2のメンバーシップは何ですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

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

最新問題: **60**
プラットフォーム保護要件を満たすには、MicrosoftAntimalwareを展開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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **61**
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？
A. Azureイベントハブ
B. AzureStorageアカウント
C. AzureAutomationアカウント
D. AzureLogAnalyticsワークスペース
Answer: (解答を表示する**)**

最新問題: **62**
Azureサブスクリプションを作成します。
Azure Active Directory（Azure AD）の特権ID管理（PIM）を使用してAzureADの役割を保護できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:

Explanation:
ステップ1 :PIMへの同意
手順 :2多要素認証 MFA）を使用してIDを確認する[IDの確認]をクリックして、Azure MFでIDを確認します手順3 :Azure ADロールにPIMをサインアップするディレクトリでPIMを有効にしたら、次のことを行う必要があります。PIMにサインアップして、AzureADの役割を管理します。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

最新問題**: 63**
Contoso.comという名前のAzureActiveDirectory Azure AD）テナントとAzure Kubernetes Service AKS）クラスターAKS1があります。
Contoso.comのアカウントを使用してAKS1にアクセスできないことがわかりました。
Contoso.comのアカウントを使用してAKS1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、管理作業を最小限に抑える必要があります。
あなたは最初に何をすべきですか？
A. AzureからAKS1を再作成します。
B. AKS1から、Kubernetesのバージョンをアップグレードします。
C. Azure ADから、AzureADPremiumを実装します。
D. Azure ADから、ユーザー設定を構成します。
Answer: (解答を表示する**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

最新問題**: 64**
Group1とGroup2のメンバーシップは何ですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :User1、User2、User3、User4
文字列と正規表現の操作では大文字と小文字が区別されないため、モントリオール User1）、MONTREAL User2）、ロンドン User 3）、およびオンタリオ User4）には ON」が含まれます。
ボックス2 :User3のみ
一致 『on」はロンドン User3）にのみ当てはまります。
シナリオ：
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。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

最新問題: **65**
contoso.comという名前のAzureActiveDirectory（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。
次の表に示すリソースで構成されるアプリケーションを実装することを計画しています。
ユーザーは、Azure ADユーザーアカウントを使用して認証し、リソーストークンを使用してCosmosDBアカウントにアクセスします。
CosmosDB1とWebApp1に実装されるタスクを特定する必要があります。
リソースごとにどのタスクを特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
CosmosDB1：データベースユーザーを作成し、リソーストークンを生成します。
Azure Cosmos DBリソーストークンは、クライアントが付与されたアクセス許可に従ってAzure Cosmos DBアカウントの特定のリソースを読み取り、書き込み、および削除できるようにするための安全なメカニズムを提供します。
WebApp1：Azure ADユーザーを認証し、リソーストークンを中継します
リソーストークンを要求、生成、およびモバイルアプリケーションに配信するための一般的なアプローチは、リソーストークンブローカーを使用することです。次の図は、サンプルアプリケーションがリソーストークンブローカーを使用してドキュメントデータベースデータへのアクセスを管理する方法の概要を示しています。
参照：
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

最新問題: **66**
：2ホットスポット
User2が現在の状態で変更および削除できるSub1の仮想ネットワークはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1：VNET4およびVNET1のみ
RG1には削除ロックしかありませんが、RG4にはロックがありません。

RG2とRG3の両方に読み取り専用ロックがあります。
ボックス2 :VNET4のみ
RG4にはロックはありませんが、他のリソースグループには削除または読み取り専用のロックがあります。
注：管理者は、組織内の他のユーザーが重要なリソースを誤って削除または変更しないように、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する必要がある場合があります。ロックレベルをCanNotDeleteまたはReadOnlyに設定できます。ポータルでは、ロックはそれぞれ削除と読み取り専用と呼ばれます。
* CanNotDeleteは、許可されたユーザーが引き続きリソースを読み取って変更できることを意味しますが、リソースを削除することはできません。
* ReadOnlyは、許可されたユーザーはリソースを読み取ることができますが、リソースを削除または更新できないことを意味します。
このロックを適用することは、すべての許可されたユーザーをReaderロールによって付与されたアクセス許可に制限することに似ています。
シナリオ：
User2はセキュリティ管理者です。
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。
User2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。
参照：
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

最新問題**: 67**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれています。
次の展示に示すように、Review1という名前のアクセスレビューを設定します。
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。
Answer:
参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

最新問題**: 68**
Sub1という名前のAzureサブスクリプションがあります。

1つのサブネットを含む仮想ネットワークを作成します。サブネット上で、次の表に示す仮想マシンをプロビジョニングします。
現在、ネットワークセキュリティグループ（NSG）はプロビジョニングされていません。
次の要件を満たすには、ネットワークセキュリティを実装する必要があります。
*VM3からVM4へのトラフィックのみを許可します。
*インターネットからVM1およびVM2へのトラフィックのみを許可します。
*NSGとネットワークセキュリティルールの数を最小限に抑えます。
NSGとネットワークセキュリティルールをいくつ作成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
NSG :2
ネットワークセキュリティルール :3
2以外 :セキュリティルールで複数のサービスタグまたはアプリケーショングループを指定することはできません。
参照：
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

最新問題**: 69**
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。ルールに必要なコンポーネントはどれですか？答えるには、答えの中から適切なオプションを選択してください。注正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 70**
Azure Active Directory（Azure AD）のハイブリッド構成があります。
すべてのユーザーは、Windows 10を実行し、ハイブリッドAzureADに参加しているコンピューターを持っています。
AzureAD認証をサポートするように構成されたAzureSQL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 Studio（SSMS）を使用してSQLデータベースに接続し、オンプレミスのActiveDirectoryアカウントを使用して認証する必要があります。
SSMSからSQLデータベースに接続するために使用する認証方法を開発者に伝える必要があります。ソリューションは、認証プロンプトを最小限に抑える必要があります。
開発者に使用するように指示する必要がある認証方法はどれですか？
A. SQLログイン
B. ActiveDirectory-MFAをサポートするユニバーサル

C. ActiveDirectory-統合
D. ActiveDirectory-パスワード
Answer: C (メーッセージを残す)
Azure ADは、最初のAzureAD管理対象ドメインにすることができます。Azure AD は、AzureADとフェデレーションされているオンプレミスのActiveDirectoryドメインサービスにすることもできます。
AzureADIDを使用してSSMSまたはSSDTを使用して接続する
次の手順は、SQL Server ManagementStudioまたはSQLServerデータベースツールを使用して、AzureADIDでSQLデータベースに接続する方法を示しています。
ActiveDirectory統合認証
フェデレーションドメインからAzureActiveDirectoryクレデンシャルを使用してWindowsにログインしている場合は、この方法を使用します。
1. ManagementStudioまたはDataTools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]）ダイアログボックスの[認証]ボックスで、[ActiveDirectory]-[統合]を選択します。接続には既存のクレデンシャルが表示されるため、パスワードは不要であるか、入力できます。
2. [オプション]ボタンを選択し、[接続のプロパティ]ページの[データベースに接続]ボックスに、接続するユーザーデータベースの名前を入力します。 ADドメイン名またはテナントID "オプションは、MFA接続オプションを備えたユニバーサルでのみサポートされます。それ以外の場合はグレー表示されます。）参照：
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md

最新問題**: 71**
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AzureSecurityCenter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？
A. はい
B. いいえ

Answer: (解答を表示する**)**
説明/参照：
https://docs.microsoft.com/en-us/azure/governance/policy/overview
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

最新問題**: 72**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
次の図に示すように、Azure AD Privileged Identity Management（PIM）から、セキュリティ管理者ロールの設定を構成します。
PIMから、セキュリティ管理者の役割を次のグループに割り当てます。
グループ1 :アクティブな割り当てタイプ、永続的に割り当てられる
Group2：適格な割り当てタイプ、永続的に適格
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

最新問題**: 73**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure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、Windows Server2012R2またはWindowsServer2016を実行する50台の仮想マシンが含まれています。
MicrosoftAntimalwareを仮想マシンに展開する必要があります。
解決策：各仮想マシンに接続し、Windows機能を追加します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
セクション :[なし]
Explanation:

Microsoft Antimalwareは、機能ではなく拡張機能として展開されます。
参照：
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

最新問題: **74**
次のリソースを含むAzureサブスクリプションがあります。
*Subnet1とSubnet2という名前の2つのサブネットを含むVNET1という名前の仮想ネットワーク。
*プライベートIPアドレスのみを持ち、Subnet1に接続するVM1という名前の仮想マシン。
インターネットからVM1へのリモートデスクトップ接続を確立できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序で並べ替えます。
Answer:
説明

最新問題: **75**
Azureサブスクリプションがあります。
S1AppServiceプランを使用するContoso1812という名前のAzureWebアプリを作成します。
Contoso1812を指すwww.contoso.comのCNAMEDNSレコードを作成する予定です。
https://www.contoso.com URLを使用して、ユーザーがContoso1812にアクセスできることを確認する必要があります。
実行する必要がある2つのアクションはどれですか？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。
A. Contoso1812のシステム割り当ての管理対象IDをオンにします。
B. Contoso1812にホスト名を追加します。
C. Contoso1812のAppServiceプランをスケールアウトします。
D. Contoso1812に展開スロットを追加します。
E. Contoso1812のAppServiceプランをスケールアップします。
F. PFXファイルをContoso1812にアップロードします。
Answer: B,F (メーッセージを残す**)**
セクション :[なし]
Explanation:
B :Webアプリのカスタムドメインをホストするようにを構成できます。たとえば、Azure Webアプリを作成し、完全修飾ドメイン名（FQDN）としてwww.contoso.comまたはcontoso.comを使用してユーザーにアクセスさせることができます。
これを行うには、次の3つのレコードを作成する必要があります。

contoso.comを指すルート 'A」レコード
検証用のルート 'TXT」レコード
Aレコードを指すwww名の 'CNAME」レコード
F :HTTPSを使用するには、PFXファイルをAzureWebAppにアップロードする必要があります。PFXファイルには、HTTPSに必要なSSL証明書が含まれています。
参照：
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

最新問題: **76**
Azureサブスクリプションのリソースへのアクセスを保護しています。
新しい会社のポリシーでは、サブスクリプション内のすべてのAzure仮想マシンは管理対象ディスクを使用する必要があると規定されています。
ユーザーがアンマネージディスクを使用する仮想マシンを作成できないようにする必要があります。
何を使うべきですか？
A. Azureモニター
B. Azureポリシー
C. Azureセキュリティセンター
D. Azure Service Health
Answer: (解答を表示する**)**
セクション :[なし]

最新問題: **77**
あなたの会社には、次の表に示すユーザーを含む、Subscription1という名前のAzureサブスクリプションがあります。
会社は新しい所有者に売却されます。
会社はSubscription1の所有権を譲渡する必要があります。
どのユーザーが所有権を譲渡でき、どのツールを使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

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

最新問題**: 78**
Azure Log Analyticsを使用して、WindowsServer2016を実行している200台のサーバーからログを収集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、すべてのサーバーへのMicrosoftMonitoringAgent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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
参照：
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/
Answer:

最新問題**: 79**
プラットフォーム保護要件を満たすには、MicrosoftAntimalwareを展開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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 80**
Azure Active Directory（Azure AD）にリンクされているAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。
パージ保護が無効に設定されているVault1という名前のAzureキーボールトがあります。Vault1には、次の表に示すアクセスポリシーが含まれています。
次の表に示すように、Vault1の役割の割り当てを作成します。
次の各ステートメントについて、ステートメントが真の場合は「はい」、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。
Answer:

最新問題**: 81**
次の表に示す仮想ネットワークを含むAzureサブスクリプションがあります。
サブスクリプションには、次の表に示す仮想マシンが含まれています。

NIC1では、ASG1という名前のアプリケーションセキュリティグループを構成します。
他のどのネットワークインターフェイスでASG1を構成できますか？
A. NIC2のみ
B. NIC2、NIC3、NIC4、およびNIC5
C. NIC2およびNIC3のみ
D. NIC2、NIC3、およびNIC4のみ
Answer: C (メーッセージを残す**)**
アプリケーションセキュリティグループに割り当てられたすべてのネットワークインターフェイスは、アプリケーションセキュリティグループに割り当てられた最初のネットワークインターフェイスと同じ仮想ネットワークに存在する必要があるため、Subnet11とSubnet12で構成されるNVET1のネットワークインターフェイスのみをASG1で構成できます。。
参照：
https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

最新問題**: 82**
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。
次の表に示すAzureポリシーを作成します。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

最新問題**: 83**
AzureSQLデータベースがあります。
AlwaysEncrypted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ことを確認する必要があります。
開発者に提供する必要がある2つの情報はどれですか。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。
A. 保存されたアクセスポリシー
B. 共有アクセス署名 $AS）
C. 列暗号化キー
D. ユーザーの資格情報
E. 列マスターキー
Answer: C,E (メーッセージを残す**)**
セクション :[なし]

Explanation:
Always Encrypted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。列暗号化キーは、暗号化された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、1つ以上の列暗号化キーを暗号化するキー保護キーです。
参照：
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

最新問題: **84**
Azureサブスクリプションがあります。
別のAzureActiveDirectory（Azure AD）テナントを使用するようにサブスクリプションを構成します。
変更による2つの考えられる影響は何ですか？それぞれの正解は完全な解決策を提示します。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. サブスクリプションレベルでの役割の割り当ては失われます。
B. 仮想マシンで管理されているIDは失われます。
C. 仮想マシンのディスクスナップショットが失われます。
D. 既存のAzureリソースが削除されます。
Answer: A,B (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associa

最新問題: **85**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Sub1という名前のAzureサブスクリプションがあります。
RG1という名前のリソースグループにSa1という名前のAzureStorageアカウントがあります。
ユーザーとアプリケーションは、いくつかの共有アクセス署名（SAS）と保存されたアクセスポリシーを使用して、Sa1のblobサービスとファイルサービスにアクセスします。
許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。
Sa1へのすべてのアクセスを取り消す必要があります。
解決策 :Sa1にロックを作成します。

これは目標を達成していますか？
A. はい
B. いいえ
Answer: B (メーッセージを残す)
説明/参照：
Explanation:
保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。
署名された識別子を変更すると、既存の署名と保存されているアクセスポリシーの間の関連付けが解除されます。保存されたアクセスポリシーを削除または名前変更すると、それに関連付けられているすべての共有アクセス署名にすぐに影響します。
参照：
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

最新問題**: 86**
Sub2の仮想マシン間のネットワーク通信に対するアプリケーションセキュリティグループの影響を評価しています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :いいえ。VM4はNSG3が接続されているSubnet13にあります。
VM1はASG1にあります。NSG3は、ASG2からのICMP pingのみを許可し、ASG1は許可しません。ASG1からのTCPトラフィックのみが許可されます。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
ボックス2 :はい。
VM2はASG2にあります。ASG2からのプロトコルはすべて許可されるため、ICMPpingが許可されます。
ボックス3。VM1はASG1にあります。TCPトラフィックはASG1から許可されるため、Webサーバーへの接続はポートTCP80またはTCP443で行われるため、VM1はWebサーバーに接続できます。

最新問題**: 87**
wenアプリApp1とVault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
Vault1にシークレットを保存してアクセスするようにApp1を構成する必要があります。
App1をどのように構成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 88**
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AzureStorage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。
Container1のコンテンツにアクセスして共有するために使用できるツールはどれですか。SASを使用して？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明

最新問題**: 89**
IDという名前の管理されたIDを持ち、Azure Active Directory（Azure AD）テナントにリンクされているAzureサブスクリプションがあります。テナントには、次の表に示すリソースが含まれています。
AUIとAU2に追加できるリソースはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
AU1とAU2に追加できるリソースはどれですか。回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 90**
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AzureStorage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。
Container1のコンテンツにアクセスして共有するために使用できるツールはどれですか。SASを使用して？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 91**
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の各効果を使用するポリシーを割り当てることを計画しています。
割り当てに管理されたIDが必要な効果はどれですか？
A. AuditIfNotExist

B. 追加
C. DeployIfNotExist
D. 拒否
Answer: C (メーッセージを残す**)**
Azureポリシーが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。
参照：
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

最新問題**: 92**
あなたの会社はシアトルとニューヨークに2つのオフィスを持っています。各オフィスは、NATデバイスを使用してインターネットに接続します。次の表に示すIPアドレスを使用します。
同社には、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれています。
MFAサービス設定は、展示に示されているように構成されています。 [展示]タブをクリックします。）
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://www.cayosoft.com/difference-enabling-enforcing-mfa/

最新問題**: 93**
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。
SQL1では透過的データ暗号化（TDE）が無効になっています。
次の表に示すように、リソースグループにポリシーを割り当てます。
Azure Resource Manager（ARM）テンプレートを使用してAzureSQLデータベースを展開することを計画しています。データベースは、次の表に示すように構成されます。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:

最新問題**: 94**
次の表に示すAzure仮想マシンがあります。
どの仮想マシンに対して更新管理を有効にできますか？
A. VM2およびVM3のみ
B. VM2、VM3、およびVM4のみ
C. VM1、VM2、およびVM4のみ
D. VM1、VM2、VM3、およびVM4
E. VM1、VM2、およびVM3のみ
Answer: C (メーッセージを残す**)**
説明
参照：
https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautoma

最新問題**: 95**
次の表に示すストレージアカウントを含むAzureサブスクリプションがあります。
許可アクセスを構成する必要があります。
各ストレージアカウントに使用できる認証タイプはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access

最新問題**: 96**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。
各ユーザーには、Azure ADPremiumP2ライセンスが割り当てられます。
オンボードで計画し、AzureADID保護を構成します。
Azure AD Identity Protectionをオンボードし、ユーザーを修正し、ポリシーを構成できるユーザーはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります
Answer:

最新問題**: 97**
プラットフォーム保護要件を満たすには、Role1を作成する必要があります。

Role1の役割定義をどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 98**
技術的な要件を満たすには、AzureSentinelノートブックのサポートを構成する必要があります。
必要なAzureコンテナーレジストリとAzureMachineLearningワークスペースの最小数はいくつですか？
Answer:
参照：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

最新問題**: 99**
次の表に示すリソースを含むAzureActiveDirectory（Azure AD）テナントがあります。
User2はGroup2の所有者です。
App1のユーザーとグループの設定は、次の図に示すように構成されています。
次の展示に示すように、App1のセルフサービスアプリケーションアクセスを有効にします。
User3は、Applへのアクセスを承認するように構成されています。
Group2の所有者とApplのユーザーを特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

最新問題**: 100**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。

ラボインスタンス :10598168

user21059868という名前のユーザーが、RG1lod10598168リソースグループ内の仮想マシンのプロパティを管理できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。

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。

Answer:

以下の説明を参照してください。

説明

1. Azureポータルで、RG1lod10598168リソースグループを見つけて選択します。
2. [アクセス制御（IAM）]をクリックします。
3. [役割の割り当て]タブをクリックして、このスコープのすべての役割の割り当てを表示します。
4.[追加]>[役割の割り当ての追加]をクリックして、[役割の割り当ての追加]ペインを開きます。
5. [役割]ドロップダウンリストで、[仮想マシンコントリビューター]の役割を選択します。仮想マシンコントリビューターを使用すると、仮想マシンを管理できますが、仮想マシンにアクセスすることはできません。また、接続している仮想ネットワークやストレージアカウントも管理できません。
6. [選択]リストで、ユーザーuser21059868を選択します
7.[保存]をクリックして役割を割り当てます。

参照：

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

最新問題**: 101**

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。実行する必要がある2つのアクションはどれですか？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。

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オンにします。
C. 最小TLSバージョンプロトコル設定を1.2に設定します。
D. AppServiceプランの料金階層を変更します。
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。

Answer: (解答を表示する**)**

説明

A :Azure Webサイトアプリケーションで使用する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：時間の経過とともに、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てきました。TLS 1.2は、AzureAppServiceで実行されているアプリで利用できる最新バージョンです。

最新問題**: 102**
AzureADアプリケーションの登録と同意の構成がIDとアクセスの要件を満たしていることを確認する必要があります。
Azureポータルで何を使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

最新問題**: 103**
App1という名前のWebアプリとVault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
Vault1にシークレットを保存してアクセスするようにApp1を構成する必要があります。
App1をどのように構成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

最新問題**: 104**
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ストレージ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LogAnalytics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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 105**
セキュリティ運用要件を確実に満たす必要があります。
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オンにします。

B. セキュリティセンターとMicrosoft CloudAppSecurityを統合します。
C. 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。
D. セキュリティセンターのワークスペース構成を変更します。
Answer: C (メーッセージを残す**)**
説明
標準層は、無料層の機能をプライベートクラウドやその他のパブリッククラウドで実行されているワークロードに拡張し、ハイブリッドクラウドワークロード全体で統合されたセキュリティ管理と脅威保護を提供します。
標準層には、高度な脅威検出機能も追加されています。これは、組み込みの行動分析と機械学習を使用して攻撃とゼロデイエクスプロイトを識別し、アクセスとアプリケーションの制御を使用してネットワーク攻撃とマルウェアへの露出を減らします。
シナリオ :セキュリティ運用要件
Litwareは、AzureSecurityCenterの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。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

最新問題**: 106**
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。
同社はApp1という名前のアプリケーションを開発しています。App1は、Windows Server 2016を実行するサーバー上のサービスとして実行されます。App1は、contoso.comに対して認証され、MicrosoftGraphにアクセスしてディレクトリデータを再広告します。
最低限必要な権限をApp1に委任する必要があります。
Azureポータルから順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
ステップ1 :アプリ登録を作成する
まず、アプリケーションを作成/登録する必要があります。
手順2 :アプリケーションのアクセス許可を追加する
アプリケーションのアクセス許可は、サインインしたユーザーがいない状態で実行されるアプリによって使用されます。
ステップ3：権限を付与する

最新問題**: 107**
次の内容を含むFile1.yamlという名前のファイルがあります。
File1.yamlを使用して、container1という名前のAzureコンテナーインスタンスを作成します。
Variable1とVariable2の値にアクセスできる場所を特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables

最新問題**: 108**
次の表に示す仮想ネットワークを含むAzureサブスクリプションがあります。
SpokeVNetSubnet0上のAzure仮想マシンは、オンプレミスネットワーク上のコンピューターと通信できます。
AzureファイアウォールをHubVNetにデプロイすることを計画しています。
次の2つのルーティングテーブルを作成します。
* RT1 :Azureファイアウォールのプライベートアドレスをネクストホップアドレスとして指すユーザー定義ルートが含まれます
* RT2 :BGPルートの伝播を無効にし、Azureファイアウォールのプライベートアドレスをデフォルトゲートウェイとして定義します。SpokeVNetSubnet0とオンプレミスネットワーク間のトラフィックがAzureファイアウォールを通過するようにする必要があります。
各ルートテーブルをどのサブネットに関連付ける必要がありますか？答えるには、適切なサブネットを正しいルートテーブルにドラッグします。各サブネットは、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。
Answer:
説明

最新問題**: 109**

User2がPIMを実装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？
A. User2にグローバル管理者の役割を割り当てます。
B. contoso.comの認証方法を構成します。
C. contoso.comのIDセキュア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。
Answer: A (メーッセージを残す**)**
ディレクトリでPIMの使用を開始するには、最初に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。
ディレクトリのPIMを有効にするには、Microsoftアカウント（@ outlook.comなど）ではなく、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。
シナリオ：技術要件は次のとおりです。contoso.comのAzure AD特権ID管理（PIM）を有効にする参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

最新問題**: 110**
SQL1という名前のAzureSQLデータベースサーバーがあります。
Advanced Threat Protection for SQL1をオンにして、すべての脅威検出タイプを検出します。
Advanced Threat Protectionはどのアクションを脅威として検出しますか？
A. ユーザーがテーブル内のレコードの50%以上を更新します。
B. ユーザーがSELECT *FROMtable1としてサインインしようとしました。
C. ユーザーがdb_ownerデータベースロールに追加されます。
D. ユーザーが同じテーブルから100を超えるレコードを削除します。
Answer: B (メーッセージを残す**)**
Advanced Threat Protectionは、潜在的なSQLインジェクションを検出できます。このアラートは、SQLインジェクションに対する特定されたアプリケーションの脆弱性に対してアクティブなエクスプロイトが発生したときにトリガーされます。これは、攻撃者が脆弱なアプリケーションコードまたはストアドプロシージャを使用して悪意のあるSQLステートメントを挿入しようとしていることを意味します。
参照：
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

最新問題**: 111**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
次の設定を持つAzureADIdentityProtectionサインインリスクポリシーを作成して適用します。

割り当て :Group1を含め、Group2を除外します
条件 :サインインリスクレベル：中以上
アクセスアクセスを許可し、多要素認証を要求する
ユーザーがAzureADにサインインしたときに何が発生するかを特定する必要があります。
ユーザーごとに何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

最新問題**: 112**
Azureキーボールトがあります。
次の要件を満たすには、キーボールトへの管理アクセスを委任する必要があります。
* User1という名前のユーザーに、キーボールトの高度なアクセスポリシーを設定する機能を提供します。
* User2という名前のユーザーに、キーボールトで証明書を追加および削除する機能を提供します。
*最小特権の原則を使用します。
各ユーザーにアクセス権を割り当てるには、何を使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ユーザー1 :RBAC
RBACは、管理プレーンのKeyVaultアクセス制御メカニズムとして使用されます。これにより、適切なIDを持つユーザーは次のことが可能になります。
*KeyVaultアクセスポリシーを設定する
*キーボールトの作成、読み取り、更新、および削除
*KeyVaultタグを設定します
注 :ロールベースのアクセス制御（RBAC）は、Azureリソースのきめ細かいアクセス管理を提供するシステムです。RBACを使用すると、チーム内の職務を分離し、ユーザーが職務を遂行するために必要なアクセス量のみをユーザーに許可できます。
User2：主要なボールトアクセスポリシー

キーボールトアクセスポリシーは、キーボールトデータプレーンにアクセスするためのアクセス制御メカニズムです。Key Vaultアクセスポリシーは、キー、シークレット、および証明書に個別にアクセス許可を付与します。
参照：
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

最新問題**: 113**
技術的な要件を満たすには、AzureSentinelノートブックのサポートを構成する必要があります。
必要なAzureコンテナーレジストリとAzureMachineLearningワークスペースの最小数はいくつですか？
Answer:
参照：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

最新問題**: 114**
Azureサブスクリプションを作成します。
Azure Active Directory（Azure AD）の特権ID管理（PIM）を使用してAzureADの役割を保護できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
ステップ1：PIMへの同意
手順2：多要素認証（MFA）を使用してIDを確認する[IDの確認]をクリックして、AzureMFAでIDを確認します。アカウントを選択するように求められます。
手順3：AzureADの役割にPIMをサインアップする
ディレクトリに対してPIMを有効にしたら、AzureADの役割を管理するためにPIMにサインアップする必要があります。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

最新問題**: 115**
Azure Log Analyticsを使用して、WindowsServer2016を実行している200台のサーバーからログを収集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、すべてのサーバーへのMicrosoftMonitoringAgent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、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

最新問題**: 116**
Azureキーボールトを作成する必要があります。ソリューションでは、キーボールトから削除されたオブジェクトが90日間保持されるようにする必要があります。
コマンドをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
Explanation:
ボックス1 :-EnablePurgeProtection
指定した場合、このボールトの即時削除に対する保護が有効になります。ソフト削除も有効にする必要があります。
ボックス2 :-EnableSoftDelete
このキーボールトに対してソフト削除機能が有効になっていることを指定します。ソフト削除が有効になっている場合、猶予期間中、削除後にこのキーボールトとその内容を回復できます。
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

最新問題**: 117**
ネットワークには、Azure Active Directory（Azure AD）と同期するadatum.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。
Azure ADテナントには、次の表に示すユーザーが含まれています。
次の展示に示すように、認証方法-adatum.comのパスワード保護設定を構成します。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-sumption-deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

最新問題**: 118**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。
Admin1という名前の管理者は、次のIDにアクセスできます。
*OpenID対応のユーザーアカウント
*Hotmailアカウント
*contoso.comのアカウント
*fabrikam.comという名前のAzureADテナントのアカウント
Azureアカウントセンターを使用して、Sub1の所有権をAdmin1に譲渡する予定です。
Sub1の所有権をどのアカウントに譲渡できますか？
A. contoso.comのみ
B. contoso.com、fabrikam.com、およびHotmailのみ
C. contoso.comおよびfabrikam.comのみ
D. contoso.com、fabrikam.com、Hotmail、およびOpenID対応のユーザーアカウント
Answer: C (メーッセージを残す**)**
説明
サブスクリプションの請求所有権を別のAzureADテナントのアカウントに譲渡する場合、サブスクリプションを新しいアカウントのテナントに移動できます。これを行うと、サブスクリプションとそのリソースを管理するための役割ベースのアクセス（RBAC）を持っていたすべてのユーザー、グループ、またはサービスプリンシパルがアクセスできなくなります。転送リクエストを受け入れる新しいアカウントのユーザーのみが、リソースを管理するためのアクセス権を持ちます。
参照：
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-anaccou

最新問題**: 119**
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
状態 :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
フィルタ基準 :リソースタイプ="仮想マシン"
このスコープで定義する：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。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
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

最新問題**: 120**
次の表に示すリソースを含むazureアクティブディレクトリ（Azure AD）テナントがあります。
User2はGroup2の所有者です。
App1のユーザーとグループの設定は、次の図に示すように構成されています。
Answer:

最新問題**: 121**
プラットフォーム保護要件を満たすには、AKS1を展開する必要があります。
順番に実行する必要がある4つのアクションはどれですか？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、正しい順序に並べます。
注：回答の選択肢の複数の順序が正しいです。選択した正しい注文のいずれかに対してクレジットを受け取ります。
Answer:
Explanation:
シナリオ：Azure ADユーザーは、AzureADクレデンシャルを使用してAKS1に対して認証する必要があります。
Litewireは、マネージドAKS（Azure Kubernetes Services）クラスターであるAKS1をデプロイすることを計画しています。
ステップ1：サーバーアプリケーションを作成する
AKSクラスターにAzureAD認証を提供するために、2つのAzureADアプリケーションが作成されます。最初のアプリケーションは、ユーザー認証を提供するサーバーコンポーネントです。
ステップ2：クライアントアプリケーションを作成する
2番目のアプリケーションは、CLIから認証を求められたときに使用されるクライアントコンポーネントです。このクライアントアプリケーションは、クライアントによって提供された資格情報の実際の認証にサーバーアプリケーションを使用します。
ステップ3：AKSクラスターをデプロイします。
az group createコマンドを使用して、AKSクラスターのリソースグループを作成します。
az aks createコマンドを使用して、AKSクラスターをデプロイします。
手順4：RBACバインディングを作成します。

AKSクラスターでAzureActiveDirectoryアカウントを使用する前に、ロールバインディングまたはクラスターロールバインディングを作成する必要があります。ロールは付与する権限を定義し、バインディングはそれらを目的のユーザーに適用します。これらの割り当ては、特定の名前空間に適用することも、クラスター全体に適用することもできます。
参照：
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

最新問題**: 122**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
10598168.onmicrosoft.comという名前の新しいAzureActiveDirectory（Azure AD）ディレクトリを作成する必要があります。
新しいディレクトリには、Azure Multi-Factor Authentication（MFA）を使用してサインインするように構成されたuser1@10598168.onmicrosoft.comという名前のユーザーが含まれている必要があります。
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。
Answer:
以下の説明を参照してください。
説明
手順1 :AzureActiveDirectoryテナントを作成する
1. Azureポータルを参照し、Azureサブスクリプションを持つアカウントでサインインします。
2.プラスアイコン（+）を選択し、AzureActiveDirectoryを検索します。
3.検索結果で[AzureActiveDirectory]を選択します。

4.[作成]を選択します。
5.組織名と初期ドメイン名（10598168）を入力します。次に、[作成]を選択します。あなたのディレクトリ
創造された。
6.ディレクトリの作成が完了したら、情報ボックスを選択して新しいディレクトリを管理します。次に、テナントユーザーを追加します。
手順2：AzureActiveDirectoryテナントユーザーを作成する
7. Azureポータルで、AzureActiveDirectoryフライアウトを使用していることを確認します。
8. [管理]で、[ユーザー]を選択します。
9. [すべてのユーザー]を選択してから、[+新しいユーザー]を選択します。
10.通常のユーザーテナントの名前とユーザー名（user1）を指定します。一時パスワードを表示することもできます。完了したら、[作成]を選択します。
名前：user1
ユーザー名：user1@10598168.onmicrosoft.com
参照：
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

最新問題: **123**
シミュレーション
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス：10598168
10598168.onmicrosoft.comという名前の新しいAzureActiveDirectory（Azure AD）ディレクトリを作成する必要があります。新しいディレクトリには、Azure Multi-Factor Authentication（MFA）を使用してサインインするように構成されたuser1@10598168.onmicrosoft.comという名前のユーザーが含まれている必要があります。
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。
A. ステップ1：AzureActiveDirectoryテナントを作成する
1. Azureポータルを参照し、Azureサブスクリプションを持つアカウントでサインインします。

3.検索結果で[AzureActiveDirectory]を選択します。
4.[作成]を選択します。
6.ディレクトリの作成が完了したら、情報ボックスを選択して新しいディレクトリを管理します。次に、テナントユーザーを追加します。
手順2：AzureActiveDirectoryテナントユーザーを作成する
8. [管理]で、[ユーザー]を選択します。
9. [すべてのユーザー]を選択してから、[+新しいユーザー]を選択します。
10.通常のユーザーテナントの名前とユーザー名（user1）を指定します。一時パスワードを表示することもできます。完了したら、[作成]を選択します。
名前：user1
ユーザー名：user1@10598168.onmicrosoft.com
B. ステップ1：AzureActiveDirectoryテナントを作成する
1. Azureポータルを参照し、Azureサブスクリプションを持つアカウントでサインインします。
3.検索結果で[AzureActiveDirectory]を選択します。
4.[作成]を選択します。
6.ディレクトリの作成が完了したら、情報ボックスを選択して新しいディレクトリを管理します。次に、テナントユーザーを追加します。
手順2：AzureActiveDirectoryテナントユーザーを作成する
7. Azureポータルで、AzureActiveDirectoryフライアウトを使用していることを確認します。
8. [管理]で、[ユーザー]を選択します。
9. [すべてのユーザー]を選択してから、[+新しいユーザー]を選択します。
10.通常のユーザーテナントの名前とユーザー名（user1）を指定します。一時パスワードを表示することもできます。完了したら、[作成]を選択します。
名前：user1
ユーザー名：user1@10598168.onmicrosoft.com
Answer: B (メーッセージを残す)
参照：
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

最新問題**: 124**
次の表に示すカスタムロールを含むAzureサブスクリプションがあります。
Azureポータルでは、既存のロールのクローンを作成して、新しいカスタムロールを作成することを計画しています。新しい役割は、次の表に示すように構成されます。
それぞれの新しい役割を作成するために、どの役割を複製できますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:
説明
グラフィカルユーザーインターフェイス、テキスト、アプリケーション、電子メール説明が自動的に生成されます
参照：
https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

最新問題**: 125**
ネットワークには、contoso.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。ドメインには、User1という名前のユーザーが含まれています。
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントにリンクされているAzureサブスクリプションがあります。テナントには、storage1という名前のAzureStorageアカウントが含まれています。Storage1には、share1という名前のAzureファイル共有が含まれています。
現在、ドメインとテナントは統合されていません。
User1がドメイン資格情報を使用してshare1にアクセスできることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

最新問題**: 126**
Sub2の仮想マシン間のネットワーク通信に対するアプリケーションセキュリティグループの影響を評価しています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1：いいえ。VM4はNSG3が接続されているSubnet13にあります。
VM1はASG1にあります。NSG3は、ASG2からのICMP pingのみを許可し、ASG1は許可しません。ASG1からのTCPトラフィックのみが許可されます。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
ボックス2：はい。

VM2はASG2にあります。ASG2からのプロトコルはすべて許可されるため、ICMPpingが許可されます。
ボックス3。VM1はASG1にあります。TCPトラフィックはASG1から許可されるため、Webサーバーへの接続はポートTCP80またはTCP443で行われるため、VM1はWebサーバーに接続できます。

最新問題**: 127**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
user21059868という名前のユーザーが、RG1lod10598168リソースグループ内の仮想マシンのプロパティを管理できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
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。
以下の説明を参照してください。
Answer:
説明
1. Azureポータルで、RG1lod10598168リソースグループを見つけて選択します。
2. [アクセス制御（IAM）]をクリックします。
3. [役割の割り当て]タブをクリックして、このスコープのすべての役割の割り当てを表示します。
4.[追加]>[役割の割り当ての追加]をクリックして、[役割の割り当ての追加]ペインを開きます。
5. [役割]ドロップダウンリストで、[仮想マシンコントリビューター]の役割を選択します。仮想マシンコントリビューターを使用すると、仮想マシンを管理できますが、仮想マシンにアクセスすることはできません。また、接続している仮想ネットワークやストレージアカウントも管理できません。
6. [選択]リストで、ユーザーuser21059868を選択します
7.[保存]をクリックして役割を割り当てます。
参照：
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

最新問題: **128**
あなたの会社は、部門ごとに個別のサブスクリプションを作成することを計画しています。各サブスクリプションは、同じAzure Active Directory（Azure AD）テナントに関連付けられます。
同じ役割が割り当てられるように各サブスクリプションを構成する必要があります。
何を使うべきですか？
A. Azureセキュリティセンター
B. Azureポリシー
C. Azure ADの特権ID管理（PIM）
D. Azureブループリント
Answer: (解答を表示する**)**
説明
ブループリントによってエンジニアまたはアーキテクトがプロジェクトの設計パラメーターをスケッチできるように、Azureブループリントを使用すると、クラウドアーキテクトと中央情報技術グループは、組織の標準、パターン、および要件を実装および準拠する反復可能な一連のAzureリソースを定義できます。
ブループリントは、さまざまなリソーステンプレートや、次のようなその他の成果物の展開を調整するための宣言型の方法です。
*役割の割り当て
*ポリシーの割り当て
* AzureResourceManagerテンプレート
*リソースグループ
参照：
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

最新問題: **129**
Registry1という名前のAzureContainerRegistryがあります。
次の表に示すように、Registry1の役割の割り当てを追加します。
どのユーザーがRegistry1に画像をアップロードし、Registry1から画像をダウンロードできますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
Explanation:
ボックス1：User1とUser4のみ
所有者、寄稿者、およびAcrPushは画像をプッシュできます。
ボックス2：User1、User2、およびUser4
AcrImagineSignerを除くすべてのユーザーが、画像をダウンロード/プルできます。
参照：
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

最新問題**: 130**
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。
同社はApp1という名前のアプリケーションを開発しています。App1は、Windows Server 2016を実行するサーバー上のサービスとして実行されます。App1は、contoso.comに対して認証され、MicrosoftGraphにアクセスしてディレクトリデータを読み取ります。
最低限必要な権限をApp1に委任する必要があります。
Azureポータルから順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
ステップ1 :アプリ登録を作成する
まず、アプリケーションを作成/登録する必要があります。
手順2 :アプリケーションのアクセス許可を追加する
アプリケーションのアクセス許可は、サインインしたユーザーがいない状態で実行されるアプリによって使用されます。
ステップ3：権限を付与する

最新問題**: 131**
container1という名前のBLOBコンテナーとApp1という名前のクライアントアプリケーションを含むAzureStorageアカウントがあります。
Azure Active Directory（Azure AD）認証を使用して、container1へのApp1アクセスを有効に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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md

最新問題**: 132**
次の表に示すように、東US2リージョンに2つのAzure仮想マシンがあります。
AzureKeyVaultをデプロイして構成します。
VM1とVM2でAzureDiskEncryptionを有効にできることを確認する必要があります。

各仮想マシンで何を変更する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
VM1 :ティア
Tierを標準にアップグレードする必要があります。
WindowsおよびLinuxのディスク暗号化IaaSVMは、すべてのAzureパブリックリージョンおよびAzure Governmentリージョンで、標準VMおよびAzureプレミアムストレージを備えたVMで一般提供されています。
VM2 :タイプ
VMtypeをA、D、DS、G、GS、Fなどのシリーズ IaaSVMのいずれかに変更する必要があります。
オペレーティングシステムのバージョンではありません :Ubuntu16.04がサポートされています。
参照：
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport

最新問題**: 133**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
次の図に示すように、Azure AD Privileged Identity Management（PIM）から、セキュリティ管理者ロールの設定を構成します。
PIMから、セキュリティ管理者の役割を次のグループに割り当てます。
*グループ1 :アクティブな割り当てタイプ、永続的に割り当てられる
*グループ2：適格な割り当てタイプ、永続的に適格
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
Explanation:
ボックス1 :はい
適格なタイプ :ユーザーが役割を使用するために1つ以上のアクションを実行する必要がある役割の割り当て。ユーザーがロールの対象になっている場合は、特権タスクを実行する必要があるときにロールをアクティブ化できることを意味します。永続的な役割と適格な役割が割り当てられている人に与えられるアクセスに違いはありません。唯一の違いは、一部の人々は常にそのアクセスを必要としないということです。

役割の設定を構成するときに、割り当てタイプ（適格およびアクティブ）ごとに2つの割り当て期間オプションから選択できます。これらのオプションは、ユーザーが特権ID管理のロールに割り当てられている場合のデフォルトの最大期間になります。
[アクティブ化の最大期間]スライダーを使用して、役割が期限切れになる前にアクティブのままでいる最大時間を時間単位で設定します。この値は1～24時間です。
ボックス2 :はい
アクティブタイプ :ユーザーがロールを使用するためにアクションを実行する必要のないロール割り当て。アクティブとして割り当てられたユーザーには、ロールに割り当てられた特権があります。ボックス3 :はいUser3はGroup2のメンバーです。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

最新問題**: 134**
Sub1という名前のAzureサブスクリプションがあります。
ITチームのすべてのメンバーを含むGroup1という名前のAzureActiveDirectory（Azure AD）グループがあります。
Group1のメンバーが、Sub1のAzure仮想マシンを停止、起動、および再起動できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
参照：
https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

最新問題**: 135**
次の表に示すユーザーを含むcontoso.comという名前のAzureActiveDirectory（Azure AD）テナントがあります。
テナントに対してAzureAD特権ID管理（PIM）が有効になっています。
PIMでは、パスワード管理者の役割には次の設定があります。
*最大アクティベーション期間（時間）2：
*アクティベーションを管理者に通知するメールを送信する：無効にする
*アクティベーション中にインシデント/リクエストチケット番号を要求する：無効にする
*アクティベーションにAzureMulti-Factor認証が必要：有効にする
*この役割をアクティブ化するには承認が必要です：有効にする
*選択された承認者 :Group1
次の表に示すように、ユーザーにパスワード管理者の役割を割り当てます。

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-

最新問題: **136**
次の表に示すユーザーを含む、contoso1812.onmicrosoft.comという名前のAzure Active Directory（Azure AD）テナントがあります。
Label1という名前のAzureInformationProtectionラベルを作成します。Label1の保護設定は、展示に示されているように構成されています。（展示]タブをクリックします。）
Label1は、File1という名前のファイルに適用されます。
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、そうでない場合は[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。
Answer:
説明

最新問題: **137**
20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のメンバーには、所有者の役割が割り当てられます。
RG1へのアクセス許可の変更は防止されます。

あなたは何をするべきか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **138**
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に対して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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **139**
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AzureStorageアカウントに記録する必要があります。
実行する必要がある2つのアクションはどれですか？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。
A. 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。
B. AzureNetworkWatcherを有効にします。
C. NSGの診断ログを有効にします。
D. NSGフローログを有効にします。
E. AzureLogAnalyticsワークスペースを作成します。
Answer: B,D (メーッセージを残す**)**
セクション :[なし]
Explanation:
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。
*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
* Network Watcherを有効にして、Microsoft.Insightsプロバイダーを登録します

* Network Watcher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します
*ログに記録されたデータをダウンロードする
*ログに記録されたデータを表示する
参照：
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

最新問題: **140**
更新管理が有効になっているAzure仮想マシンがあります。仮想マシンは、次の表に示すように構成されています。
Update1とUpdate2という名前の2つの更新デプロイメントをスケジュールします。Update1はVM3を更新します。Update2はVM6を更新します。
Update1とUpdate2を使用して更新できる追加の仮想マシンはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

最新問題: **141**
sub1という名前のAzureサブスクリプションを含むGroup1という名前の管理グループがあります。Sub1のサブスクリプションIDは11111111-1234-1234-1234-1111111111です。
Group1内のすべてのオブジェクトのタグを管理するためのアクセス許可を委任するカスタムAzureロールベースアクセス制御（RBAC）ロールを作成する必要があります。
Role1の役割定義に何を含める必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
注：管理グループレベルとしてのカスタムRBACロールの割り当ては、現在プレビューのみです。したがって、今のところ、割り当て可能なスコープに対する答えはサブスクリプションレベルです。
参照：
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

最新問題: **142**

注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Sub1という名前のAzureサブスクリプションがあります。Sub1には、WindowsServer2016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。
AzureDiskEncryptionを使用してVM1ディスクを暗号化する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

最新問題**: 143**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
user21059868という名前のユーザーが、RG1lod10598168リソースグループ内の仮想マシンのプロパティを管理できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
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。
Answer:
以下の説明を参照してください。
説明
1. Azureポータルで、RG1lod10598168リソースグループを見つけて選択します。
2. [アクセス制御（IAM）]をクリックします。
3. [役割の割り当て]タブをクリックして、このスコープのすべての役割の割り当てを表示します。
4.[追加]>[役割の割り当ての追加]をクリックして、[役割の割り当ての追加]ペインを開きます。

5. [役割]ドロップダウンリストで、[仮想マシンコントリビューター]の役割を選択します。仮想マシンコントリビューターを使用すると、仮想マシンを管理できますが、仮想マシンにアクセスすることはできません。また、接続している仮想ネットワークやストレージアカウントも管理できません。
6. [選択]リストで、ユーザーuser21059868を選択します
7.[保存]をクリックして役割を割り当てます。
参照：
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

最新問題**: 144**
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はメールを送信するように構成されています
User1という名前のユーザーへのメッセージ。
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？
A. Azure DevOps
B. Azure Application Insights
C. Azureモニター
D. Azure Logic Apps Designer
Answer: (解答を表示する**)**
説明/参照：
Explanation:
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。それをするためにあなたはただ
[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必要があります。ロジックアプリ
Designerが開きます。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

最新問題**: 145**
VNET1という名前の仮想ネットワークとVNET2という名前の仮想ネットワークの間のネットワーク接続を構成する必要があります。このソリューションでは、VNET1に接続された仮想マシンがVNET2に接続された仮想マシンと通信でき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。

Answer:
2つのネットワーク間でVNetピアリングを構成する必要があります。質問には、「ソリューションでは、VNET1に接続された仮想マシンがVNET2に接続された仮想マシンと通信できるようにする必要があります」と記載されています。VNET2上のVMがVNET1上のVMと通信できる必要があるとは言っていません。したがって、一方向の通信のみを許可するようにピアリン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「仮想ネットワーク」と入力し、検索結果から[仮想ネットワーク]を選択してから、[VNET1]を選択します。または、左側のナビゲーションペインで[仮想ネットワーク]を参照します。
2. VNET1のプロパティで、[ピアリング]をクリックします。
3. [ピアリング]ブレードで、[追加]をクリックして新しいピアリングを追加します。
4. [VNET1からリモート仮想ネットワークへのピアリングの名前]ボックスに、VNET1-VNET2などの名前を入力します（これは、VNET1のようにピアリングが表示される名前です）。
5. [仮想ネットワーク]ボックスで、[VNET2]を選択します。
6. [リモート仮想ネットワークからVNET1へのピアリングの名前]ボックスに、VNET2-VNET1などの名前を入力します（これは、VNET2のようにピアリングが表示される名前です）。
VNETからリモート仮想ネットワークへの仮想ネットワークアクセスを許可するオプションがあります。これは有効のままにしておく必要があります。
7. [リモートネットワークからVNET1への仮想ネットワークアクセスを許可する]オプションの場合は、スライダーボタンをクリックして[無効]にします。
8. [OK]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/virtual-network/virtual-network-manage-peering

最新問題**: 146**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス：10598168
管理ユーザーがVNET1という名前の仮想ネットワークを誤って削除しないようにする必要があります。管理ユーザーは、VNET1の設定を変更でき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。

Answer:
以下の説明を参照してください。
説明
ロックすると、組織内の他のユーザーが、Azureサブスクリプション、リソースグループ、リソースなどの重要なリソースを誤って削除または変更するのを防ぐことができます。
注：Azureでは、リソースという用語はAzureによって管理されるエンティティを指します。たとえば、仮想マシン、仮想ネットワーク、およびストレージアカウントはすべてAzureリソースと呼ばれます。
1.仮想ネットワークVNETの[設定]ブレードで、[ロック]を選択します。
2.ロックを追加するには、[追加]を選択します。
3. [ロックの種類]で[ロックの削除]を選択し、[OK]をクリックします
参照：
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

最新問題**: 147**
User2がPIMを実装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？
A. User2にグローバル管理者の役割を割り当てます。
B. contoso.comの認証方法を構成します。
C. contoso.comのIDセキュア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。
Answer: A (メーッセージを残す**)**
セクション：[なし]
Explanation:
ディレクトリでPIMの使用を開始するには、最初に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。
ディレクトリのPIMを有効にするには、Microsoftアカウント（@ outlook.comなど）ではなく、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。
シナリオ：技術要件は次のとおりです。contoso.comのAzure AD特権ID管理（PIM）を有効にする参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started質問セット3

最新問題**: 148**
次の表に示すユーザーを含むcontoso.comという名前のAzureActiveDirectory（Azure AD）テナントがあります。
テナントに対してAzureAD特権ID管理（PIM）が有効になっています。
PIMでは、パスワード管理者の役割には次の設定があります。

最大アクティベーション期間（時間）2：
管理者にアクティベーションを通知するメールを送信する：無効にする
アクティベーション中にインシデント/リクエストチケット番号を要求する：無効にする
アクティベーションにAzureMulti-Factor認証を要求する：有効にする
この役割をアクティブ化するには承認が必要です：有効にする
選択された承認者：Group1
次の表に示すように、ユーザーにパスワード管理者の役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 149**
KeyVault1という名前のAzureキーボールトと次の表に示す仮想マシンを含むAzureサブスクリプションがあります。
Key Vaultアクセスポリシーを、ボリューム暗号化のためにAzureDiskEncryptionへのアクセスを有効にするように設定します。
KeyVault1は、次の展示に示すように構成されています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 150**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
Azure AD Privileged Identity Management（PIM）では、コントリビューターロールのロール設定は、展示に示されているように構成されます。（[展示]タブをクリックします。）
次の表に示すように、2019年5月1日にユーザーにコントリビューターの役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
Explanation:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

最新問題**: 151**

次の表に示すオフィスを持つContoso、Ltd.という会社で働いています。
Contosoには、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。すべてのcontoso.comユーザーは、Azure Multi-Factor Authentication（MFA）を有効にしています。テナントには、次の表に示すユーザーが含まれています。
contoso.comの多要素設定は、次の展示に示すように構成されています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 152**
Azureキーボールトを作成する必要があります。ソリューションでは、キーボールトから削除されたオブジェクトが90日間保持されるようにする必要があります。
コマンドをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

最新問題**: 153**
あなたの会社には、次の表に示すユーザーを含む、Subscription1という名前のAzureサブスクリプションがあります。
会社は新しい所有者に売却されます。
会社はSubscription1の所有権を譲渡する必要があります。
どのユーザーが所有権を譲渡でき、どのツールを使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

説明
ボックス1; User2
請求管理者
譲渡するサブスクリプションの[請求所有権の譲渡]を選択します。
サブスクリプションの新しい所有者となるアカウントの課金管理者であるユーザーの電子メールアドレスを入力します。
ボックス2 :Azureアカウントセンター
Azureアカウントセンターを使用できます。
参照：
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azu

最新問題**: 154**
sub1という名前のAzureサブスクリプションを含むGroup1という名前の管理グループがあります。Sub1のサブスクリプションIDは11111111-1234-1234-1234-1111111111です。
Group1内のすべてのオブジェクトのタグを管理するためのアクセス許可を委任するカスタムAzureロールベースアクセス制御（RBAC）ロールを作成する必要があります。
Role1の役割定義に何を含める必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

最新問題**: 155**
Azure Active Directory（Azure AD）テナントとUser1という名前のユーザーを含むAzureサブスクリプションがあります。
テナントのアプリ登録設定は、以下の展示のように構成されています。
App1という名前のアプリをデプロイする予定です。
User1がApp1をAzureADに登録できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
User1にどの役割を割り当てる必要がありますか？
A. サブスクリプションのアプリ構成データ所有者
B. サブスクリプションのマネージドアプリケーションコントリビューター
C. AzureADのクラウドアプリケーション管理者
D. AzureADのアプリケーション開発者。

Answer: (解答を表示する**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

最新問題**: 156**
次の表に示すように、東US2リージョンに2つのAzure仮想マシンがあります。
AzureKeyVaultをデプロイして構成します。
VM1とVM2でAzureDiskEncryptionを有効にできることを確認する必要があります。
各仮想マシンで何を変更する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-capabilities

最新問題**: 157**
Sub1という名前のAzureサブスクリプションがあります。
1つのサブネットを含む仮想ネットワークを作成します。サブネット上で、次の表に示す仮想マシンをプロビジョニングします。
現在、ネットワークセキュリティグループ（NSG）はプロビジョニングされていません。
次の要件を満たすには、ネットワークセキュリティを実装する必要があります。
VM3からのみVM4へのトラフィックを許可します。
インターネットからVM1およびVM2へのトラフィックのみを許可します。
NSGとネットワークセキュリティルールの数を最小限に抑えます。
NSGとネットワークセキュリティルールをいくつ作成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

最新問題**: 158**
Azure Securityから、カスタムアラートルールを作成します。
アラートがトリガーされたときに電子メールメッセージを受信するユーザーを構成する必要があります。
あなたは何をするべきか？
A. Azure Monitorから、アクショングループを作成します。
B. セキュリティセンターから、Azureサブスクリプションのセキュリティポリシー設定を変更します。

C. Azure Active Directory（Azure AD）から、セキュリティリーダーロールグループのメンバーを変更します。
D. セキュリティセンターから、アラートルールを変更します。
Answer: A (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

最新問題**: 159**
シミュレーション
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス：10598168

user21059868という名前のユーザーが、RG1lod10598168リソースグループ内の仮想マシンのプロパティを管理できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
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。
A. 1. Azureポータルで、RG1lod10598168リソースグループを見つけて選択します。
2. [アクセス制御（IAM）]をクリックします。
3. [役割の割り当て]タブをクリックして、このスコープのすべての役割の割り当てを表示します。
4.[追加]>[役割の割り当ての追加]をクリックして、[役割の割り当ての追加]ペインを開きます。
5. [役割]ドロップダウンリストで、仮想マシンコントリビューターの役割を選択します。Virtual Machine Contributorを使用すると、仮想マシンを管理できますが、仮想マシンにアクセスすることはできません。また、仮想マシンが接続されている仮想ネットワークやストレージアカウントも管理できません。
6. [選択]リストで、ユーザーuser21059868を選択します
7.[保存]をクリックして役割を割り当てます。
B. 1. Azureポータルで、RG1lod10598168リソースグループを見つけて選択します。
2. [アクセス制御（IAM）]をクリックします。
3. [役割の割り当て]タブをクリックして、このスコープのすべての役割の割り当てを表示します。

4.[追加]>[役割の割り当ての追加]をクリックして、[役割の割り当ての追加]ペインを開きます。
5. [役割]ドロップダウンリストで、仮想マシンコントリビューターの役割を選択します。6. [選択]リストで、ユーザーuser21059888を選択します
7.[保存]をクリックして役割を割り当てます。
Answer: (解答を表示する**)**
参照：
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

最新問題**: 160**
ネットワークには、Azure Active Directory（Azure AD）と同期するadatum.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。Azure AD Connectは、Server1という名前のドメインメンバーサーバーにインストールされます。
adatum.comドメインのドメイン管理者が同期オプションを変更できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
ドメイン管理者に割り当てる必要があるAzureADの役割はどれですか。
A. セキュリティ管理者
B. グローバル管理者
C. ユーザー管理者
Answer: B (メーッセージを残す**)**
説明/参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

最新問題**: 161**
あなたの会社はシアトルとニューヨークに2つのオフィスを持っています。各オフィスは、NATデバイスを使用してインターネットに接続します。次の表に示すIPアドレスを使用します。
同社には、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれています。
MFAサービス設定は、展示に示されているように構成されています。 [展示]タブをクリックします。）
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://www.cayosoft.com/difference-enabling-enforcing-mfa/

最新問題: **162**
次の表に示すユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
Azure AD Privileged Identity Management（PIM）では、コントリビューターロールのロール設定は、展示に示されているように構成されます。（展示]タブをクリックします。）
次の表に示すように、2019年5月1日にユーザーにコントリビューターの役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assig

最新問題: **163**
User1という名前のユーザーを含むcontoso.comという名前のAzureActiveDin-dory（Azure AD）テナントがあります。
テナントで複数のアプリを公開する予定です。
User1が公開されたアプリの管理者同意を付与できることを確認する必要があります。
ユーザーに割り当てることができる2つの可能なユーザーロールはどれですか。この目標を達成するには？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。
A. アプリケーション開発者
B. セキュリティ管理者
C. アプリケーション管理者
D. ユーザー管理者
E. クラウドアプリケーション管理者
Answer: C,E (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

最新問題: **164**
Azure Security Centerから、Registry1のイメージのAzureContainerRegistry脆弱性スキャンを有効にします。
次のアクションを実行します。
*Image1という名前のWindowsイメージをRegistry1にプッシュします。
*Image2という名前のLinuxイメージをRegistry1にプッシュします。
*Image3という名前のWindowsイメージをRegistry1にプッシュします。

* Image1を変更し、新しいイメージをImage4としてRegistry1にプッシュします。
* Image2を変更し、新しいイメージをImage5としてRegistry1にプッシュします。
脆弱性についてスキャンされる2つの画像はどれですか？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。
A. Image4
https://www.fast2test.com/AZ-500-practice-test.html 46
有効なFast2testAZ-500試験PDFダンプ新しいAZ-500実際の試験問題
B. Image2
C. Image1
D. Image3
E. Image5
Answer: (解答を表示する**)**
Linuxイメージのみがスキャンされます。Windowsイメージはスキャンされません。
参照：
https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration

最新問題**: 165**
条件付きアクセスポリシーを実装しています。
ポリシーを構成および実装するには、既存のAzure Active Directory（Azure AD）のリスクイベントとリスクレベルを評価する必要があります。
次のリスクイベントのリスクレベルを特定する必要があります。
クレデンシャルが漏洩したユーザー
非定型の場所への不可能な旅行
疑わしいアクティビティのあるIPアドレスからのサインイン
リスクイベントごとにどのレベルを特定する必要がありますか？答えるには、適切なレベルを正しいリスクイベントにドラッグします。各レベルは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、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。
Answer:

最新問題**: 166**
User8に、RG4、RG5、およびRG6の所有者の役割を割り当てます。
User8はどのリソースグループで仮想ネットワークとNSGを作成できますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/governance/policy/overview

最新問題**: 167**
AzureADアプリケーションの登録と同意の構成がIDとアクセスの要件を満たしていることを確認する必要があります。
Azureポータルで何を使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 168**
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？
A. Windowsのファイルエクスプローラー
B. セキュリティおよびコンプライアンス管理センター
C. AzCopy
D. AzureのSQLクエリエディター
Answer: B (メーッセージを残す**)**

最新問題**: 169**
次の表に示すように、東US2リージョンに2つのAzure仮想マシンがあります。
AzureKeyVaultをデプロイして構成します。
VM1とVM2でAzureDiskEncryptionを有効にできることを確認する必要があります。
各仮想マシンで何を変更する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-capabilities

最新問題: **170**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Sub1という名前のAzureサブスクリプションがあります。
RG1という名前のリソースグループにsa1という名前のAzureStorageアカウントがあります。
ユーザーとアプリケーションは、いくつかの共有アクセス署名 (SAS) と保存されたアクセスポリシーを使用して、sa1のblobサービスとファイルサービスにアクセスします。
許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。
sa1へのすべてのアクセスを取り消す必要があります。
解決策 :Azureストレージアカウントのアクセスキーを再生成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: A (メーッセージを残す)
セクション :[なし]
Explanation:
新しいストレージアカウントキーを生成すると、以前のキーに基づいていたすべてのSASが無効になります。

最新問題: **171**
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？
A. Azure Storage Explorer
B. AzureのSQLクエリエディター
C. Windowsのファイルエクスプローラー
D. Azureセキュリティセンター
Answer: (解答を表示する)
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ストレージクライアント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。
参照：
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

最新問題**: 172**
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と思われます。
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ために、AzureLogAnalyticsクエリを作成する必要があります。結果には、サインインに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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

最新問題**: 173**
条件付きアクセスポリシーを実装しています。
ポリシーを構成および実装するには、既存のAzure Active Directory（Azure AD）のリスクイベントとリスクレベルを評価する必要があります。
次のリスクイベントのリスクレベルを特定する必要があります。
クレデンシャルが漏洩したユーザー
非定型の場所への不可能な旅行
疑わしいアクティビティのあるIPアドレスからのサインイン
リスクイベントごとにどのレベルを特定する必要がありますか？答えるには、適切なレベルを正しいリスクイベントにドラッグします。各レベルは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、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。
Answer:

最新問題**: 174**
仮想ネットワークを含むAzureサブスクリプションがあります。仮想ネットワークには、次の表に示すサブネットが含まれています。

サブスクリプションには、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対してジャストインタイム（JIT）VMアクセスを有効にします。
JITによって保護されている仮想マシンを特定する必要があります。
どの仮想マシンを特定する必要がありますか？
A. VM4のみ
B. VM1およびVM3のみ
https://www.fast2test.com/AZ-500-practice-test.html 45
有効なFast2testAZ-500試験PDFダンプ新しいAZ-500実際の試験問題
C. VM1、VM3、VM4のみ
D. VM1、VM2、VM3、およびVM4
Answer: (解答を表示する**)**
NSGは、VMレベルまたはサブネットレベルのいずれかで有効にする必要があります。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

最新問題**: 175**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス：10598168
VM1という名前の仮想マシンの平均CPU使用率が15分間で70％を超える場合は、admin1@contoso.comという名前の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。
Answer:
以下の説明を参照してください。
説明
Azureポータルを使用してメトリックにアラートルールを作成する
1.ポータルで、監視対象のリソース（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（クラシック）の追加]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
状態：より大きい

期間：過去5分間
通知 :メール
追加の管理者メール :admin1@contoso.com
参照：
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

最新問題**: 176**
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。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 177**
次の内容を含むFile1.yamlという名前のファイルがあります。
File1.yamlを使用して、container1という名前のAzureコンテナーインスタンスを作成します。
Variable1とVariable2の値にアクセスできる場所を特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
参照：
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables

最新問題**: 178**
次の表に示すAzureキーボールトがあります。
KV1は、Secret1という名前のシークレットと、Key1という名前の管理対象ストレージアカウントのキーを格納します。
Secret1とKey1をバックアップします。

各バックアップをどの主要なボールトに復元できますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **179**
次の表に示すアイテムを含むKeyVault1という名前のAzureキーボールトがあります。
KeyVaultでは、次のイベントが順番に発生します。
Item1が削除されます
管理者がソフト削除を有効にする
Item2とPolicy1が削除されます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **180**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。
Admin1という名前の管理者は、次のIDにアクセスできます。
*OpenID対応のユーザーアカウント
*Hotmailアカウント
*contoso.comのアカウント
*fabrikam.comという名前のAzureADテナントのアカウント
Azureアカウントセンターを使用して、Sub1の所有権をAdmin1に譲渡する予定です。
Sub1の所有権をどのアカウントに譲渡できますか？
A. contoso.comのみ
B. contoso.com、fabrikam.com、およびHotmailのみ
C. contoso.comおよびfabrikam.comのみ
D. contoso.com、fabrikam.com、Hotmail、およびOpenID対応のユーザーアカウント
Answer: C (メーッセージを残す**)**
サブスクリプションの請求所有権を別のAzureADテナントのアカウントに譲渡する場合、サブスクリプションを新しいアカウントのテナントに移動できます。これを行うと、サブスクリプションとそのリソースを管理するための役割ベースのアクセス（RBAC）を持っていたすべてのユーザー、グループ、またはサービスプリンシパルがアクセスできなくなります。転送リクエストを受け入れる新しいアカウントのユーザーのみが、リソースを管理するためのアクセス権を持ちます。
参照：
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer

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

最新問題: **181**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれています。
次の展示に示すように、Review1という名前のアクセスレビューを設定します。
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。
Answer:
説明
ボックス1：User3のみ
メンバー（自己）オプションを使用して、ユーザーに自分の役割の割り当てを確認してもらいます。
ボックス2：User3は確認リクエストを受け取ります
レビュー担当者が応答しないリストを使用して、レビュー期間内にレビュー担当者によってレビューされなかったユーザーに何が起こるかを指定します。この設定は、レビュー担当者が手動でレビューしたユーザーには影響しません。最終的なレビューアの決定が拒否である場合、ユーザーのアクセスは削除されます。
変更なし：ユーザーのアクセスは変更しないでください
アクセスの削除：ユーザーのアクセスを削除します
アクセスを承認する：ユーザーのアクセスを承認する
推奨事項を取得する：ユーザーの継続的なアクセスの拒否または承認に関するシステムの推奨事項を取得します。参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-se

最新問題: **182**
注：この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セッ

トには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Active Directory（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AzureHDInsightクラスターがあります。
オンプレミスのActiveDirectory資格情報を使用して、ユーザーがクラスターに対して認証できるようにすることを計画しています。
計画された認証をサポートするように環境を構成する必要があります。
解決策：仮想ネットワークとオンプレミスネットワークの間にサイト間VPNを作成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: A (メーッセージを残す**)**
説明
Azure Virtual NetworksとVPNゲートウェイを使用して、HDInsightをオンプレミスネットワークに接続できます。
注：参加しているネットワーク内のHDInsightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。
Azure仮想ネットワークを作成します。
Azure仮想ネットワークにカスタムDNSサーバーを作成します。
デフォルトのAzureRecursiveResolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。
参照：
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

最新問題**: 183**
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にメンバーシップルールを追加します。
B. Group1を削除します。グループタイプがOffice365のGroup1という名前の新しいグループを作成します。ユーザーとデバイスをグループに追加します。
C. Group1のメンバーシップルールを変更します。
D. Group1のメンバーシップタイプをAssignedに変更します。動的メンバーシップを持つ2つのグループを作成します。
Group1に新しいグループを追加します。
Answer: B (メーッセージを残す**)**

不正解：
A、C :デバイスまたはユーザーの動的グループを作成できますが、ユーザーとデバイスの両方を含むルールを作成することはできません。
D：割り当てられたグループの場合、追加できるのは個々のメンバーのみです。
シナリオ：
Litwareは、次のIDと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のメンバーである必要があります。
テナントには現在、次のグループが含まれています。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portalIDの管理とテストレット2へのアクセスケーススタディこれはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。提供された時間内にこの試験に含まれるすべての質問を確実に完了することができるように、時間を管理する必要があります。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、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の最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、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には
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ます。質問に答える前に、左側のペインのボタンを使用して、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、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。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質問に戻ります。
概要
Contoso、Ltd.は、モントリオールに本社を置き、シアトルとニューヨークに2つの支店を持つコンサルティング会社です。
同社は、サーバーインフラストラクチャ全体をAzureでホストしています。
Contosoには、Sub1とSub2という名前の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）テナントに関連付けられています。
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。
User9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。
サブ2
Sub2には、次の表に示す仮想ネットワークが含まれています。
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は、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。各仮想マシンのファイアウォールは、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ルールがあります。
NSG2には、次の表に示すインバウンドセキュリティルールがあります。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
NSG4には、次の表に示すインバウンドセキュリティルールがあります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示すアウトバウンドセキュリティルールがあります。
技術要件
Contosoは、次の技術要件を識別します。
*AzureファイアウォールをSub2のVNetwork1にデプロイします。
*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、最小特権の原則を使用してください。
* contoso.comに対してAzureAD特権ID管理（PIM）を有効にします。

最新問題: **184**
image1という名前のコンテナーイメージを含むContReg1という名前のAzureコンテナーレジストリがあります。
ContReg1のコンテンツ信頼を有効にします。
コンテンツの信頼を有効にした後、次の表に示すように、2つのイメージをContReg1にプッシュします。
どの画像が信頼できる画像ですか？
A. image1とimage2のみ
B. image2のみ
C. image1、image2、およびimage3
Answer: (解答を表示する**)**

Azure Container Registryは、Dockerのコンテンツ信頼モデルを実装し、署名されたイメージのプッシュとプルを可能にします。
信頼できるイメージタグをコンテナレジストリにプッシュするには、コンテンツの信頼を有効にして、Dockerプッシュでイメージをプッシュします。
信頼できるイメージを操作するには、イメージの発行者と使用者の両方がDockerクライアントのコンテンツの信頼を有効にする必要があります。サイト運営者は、コンテンツの信頼が有効なレジストリにプッシュする画像に署名できます。
参照：
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

最新問題**: 185**
Azureキーボールトがあります。
次の要件を満たすには、キーボールトへの管理アクセスを委任する必要があります。
* User1という名前のユーザーに、キーボールトの高度なアクセスポリシーを設定する機能を提供します。
* User2という名前のユーザーに、キーボールトで証明書を追加および削除する機能を提供します。
*最小特権の原則を使用します。
各ユーザーにアクセス権を割り当てるには、何を使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ユーザー1 :RBAC
RBACは、管理プレーンのKeyVaultアクセス制御メカニズムとして使用されます。これにより、適切なIDを持つユーザーは次のことが可能になります。
*KeyVaultアクセスポリシーを設定する
*キーボールトの作成、読み取り、更新、および削除
*KeyVaultタグを設定します
注 :ロールベースのアクセス制御（RBAC）は、Azureリソースのきめ細かいアクセス管理を提供するシステムです。RBACを使用すると、チーム内の職務を分離し、ユーザーが職務を遂行するために必要なアクセス量のみをユーザーに許可できます。
User2：主要なボールトアクセスポリシー
キーボールトアクセスポリシーは、キーボールトデータプレーンにアクセスするためのアクセス制御メカニズムです。Key Vaultアクセスポリシーは、キー、シークレット、および証明書に個別にアクセス許可を付与します。
参照：
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

最新問題: **186**
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の各効果を使用するポリシーを割り当てることを計画しています。
割り当てに管理されたIDが必要な効果はどれですか？
AuditIfNotExist
A.
B. 追加
DeployIfNotExist
C.
D. 拒否
Answer: (解答を表示する**)**
セクション :[なし]
Explanation:
Azureポリシーが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。
参照：
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

最新問題: **187**
あなたの会社には、weylandindustries.comという名前の単一ドメインを持つActiveDirectoryフォレストがあります。また、同じ名前のAzure Active Directory（Azure AD）テナントもあります。
すべてのオンプレミスIDをAzureADに同期した後、LABで始まるgivenName属性を持つユーザーがAzureADに同期することを許可しないようにする必要があることが通知されます。
次のアクションのどれを実行する必要がありますか？
A. 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する必要があります。
B. ファイアウォールでDNATルールを構成する必要があります。
C. 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構成する必要があります。
D. Active Directoryユーザーとコンピューターを使用して、属性ベースのフィルタリングルールを作成する必要があります。
Answer: A (メーッセージを残す**)**
説明
同期ルールエディタを使用して、属性ベースのフィルタリングルールを記述します。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

最新問題**: 188**
あなたの会社には、次の表に示すユーザーを含む、Subscription1という名前のAzureサブスクリプションがあります。
会社は新しい所有者に売却されます。
会社はSubscription1の所有権を譲渡する必要があります。
どのユーザーが所有権を譲渡でき、どのツールを使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription

最新問題**: 189**
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。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 190**
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ストレージ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LogAnalytics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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明

最新問題**: 191**

ネットワークには、contoso.comという名前のActiveDirectoryフォレストが含まれています。フォレストには単一のドメインが含まれています。
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。
Azure AD Connectを展開し、ActiveDirectoryとAzureADテナントを統合することを計画しています。
次の要件を満たす統合ソリューションを推奨する必要があります。
*テナントに同期されるユーザーアカウントにパスワードポリシーとユーザーログオン制限が適用されるようにします
*ソリューションに必要なサーバーの数を最小限に抑えます。
どの認証方法を推奨に含める必要がありますか？
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. シームレスなシングルサインオン（SSO）を使用したパスワードハッシュ同期
C. シームレスなシングルサインオン（SSO）を使用したパススルー認証
Answer: (解答を表示する**)**
パスワードハッシュの同期には、展開、保守、およびインフラストラクチャに関する最小限の労力が必要です。このレベルの作業は通常、ユーザーがOfficeにサインインするだけでよい組織に適用されます。
365、SaaSアプリ、およびその他のAzureAD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同期プロセスの一部であり、2分ごとに実行されます。
不正解：
A :フェデレーション認証システムは、外部の信頼できるシステムに依存してユーザーを認証します。一部の企業は、既存の連合システムへの投資をAzureADハイブリッドIDソリューションで再利用したいと考えています。連合システムの保守と管理は、AzureADの制御の範囲外です。フェデレーションシステムを使用して、システムが安全に展開され、認証の負荷を処理できることを確認するのは、組織の責任です。
C :パススルー認証の場合、既存のサーバーに1つ以上（3つを推奨）の軽量エージェントをインストールする必要があります。これらのエージェントは、オンプレミスのADドメインコントローラーを含む、オンプレミスのActiveDirectoryドメインサービスにアクセスできる必要があります。インターネットへのアウトバウンドアクセスとドメインコントローラーへのアクセスが必要です。このため、境界ネットワークにエージェントを展開することはサポートされていません。
パススルー認証には、ドメインコントローラーへの制約のないネットワークアクセスが必要です。すべてのネットワークトラフィックは暗号化され、認証要求に制限されます。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

最新問題**: 192**
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にメンバーシップルールを追加します。
B. Group1を削除します。メンバーシップの種類がOffice365であるGroup1という名前の新しいグループを作成します。追加
グループへのユーザーとデバイス。
C. Group1のメンバーシップルールを変更します。
D. Group1のメンバーシップタイプをAssignedに変更します。動的な2つのグループを作成する
メンバーシップ。Group1に新しいグループを追加します。
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
不正解：
A、C :デバイスまたはユーザーの動的グループを作成できますが、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の場合、追加できるのは個々のメンバーのみです。
シナリオ：
Litwareは、次のIDと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
Group1のメンバーである必要があります。
テナントには現在、次のグループが含まれています。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/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。ケーススタディは個別にタイミングが調整されていません。あなたはあなたがするのと同じくらい多くの試験時間を使うことができます
それぞれのケースを完了するのが好きです。ただし、この試験には追加のケーススタディとセクションがある場合があります。君は
あなたがこの試験に含まれるすべての質問を完了することができることを保証するためにあなたの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、より多くの情報を提供する展示やその他のリソースが含まれている場合があります

ケーススタディで説明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。この画面では、回答を確認できます
試験の次のセクションに進む前に変更を加えます。新しいセクションを開始した後、
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には
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ます。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、問題の説明などの情報。場合は
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あることに注意してください。
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を置き、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。
とニューヨーク。
同社は、サーバーインフラストラクチャ全体をAzureでホストしています。
Contosoには、Sub1とSub2という名前の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に関連付けられています
contoso.comという名前のAzureActiveDirectory（Azure AD）テナント。
技術要件
Contosoは、次の技術要件を識別します。
Sub2のVNetWork1にAzureファイアウォールをデプロイします。
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、最小特権の原則を使用してください。
contoso.comのAzureAD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。
User2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。
サブ2
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は、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ルールがあります。
NSG2には、次の表に示すインバウンドセキュリティルールがあります。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
NSG4には、次の表に示すインバウンドセキュリティルールがあります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示すアウトバウンドセキュリティルールがあります。
Contosoは、次の技術要件を識別します。
Sub2のVNetwork1にAzureファイアウォールをデプロイします。
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、最小特権の原則を使用してください。
contoso.comに対してAzureAD特権ID管理（PIM）を有効にします。

最新問題**: 193**
VNET1とVNET2という名前の2つのAzure仮想ネットワークのネットワーク接続を構成しています。
次の要件を満たすには、仮想ネットワークにVPNゲートウェイを実装する必要があります。
* VNET1には、BGPを使用する6つのサイト間接続が必要です。
* VNET2には、BGPを使用する12のサイト間接続が必要です。
*コストを最小限に抑える必要があります。
各仮想ネットワークにどのVPNゲートウェイSKI）を使用する必要がありますか？回答するには、適切なSKUを正しいネットワークにドラッグします。各SKU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
Answer:
参照：
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

最新問題**: 194**

AzureキーボールトとAzureストレージアカウントを含むAzureサブスクリプションがあります。キーボールトには、顧客が管理するキーが含まれています。ストレージアカウントは、キーボールトに保存されている顧客管理のキーを使用するように構成されています。
次のサービスを使用して、Azureにデータを保存することを計画しています。
*Azureファイル
*AzureBlobストレージ
* Azure Log Analytics
*Azureテーブルストレージ
*Azureキューストレージ
キーボールトに保存されているキーを使用してデータを暗号化する2つのサービスはどれですか？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。
A. キューストレージ
B. テーブルストレージ
C. Azureファイル
D. BLOBストレージ
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal

最新問題**: 195**
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
要件。
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構成します。
C. RT1をAzureFirewallSubnetに割り当てます。
D. ファイアウォールで、DNATルールを構成します。
Answer: A (メーッセージを残す**)**
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Just-in-Time（JIT）機能との競合。
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、ASCJIT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を介して着信します（JITがアクセスを開始しました）が、リターンパスはファイアウォールを経由します。

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、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
ファイアウォールへのユーザー定義のルート。
シナリオ：
計画された変更の実装後、ITチームは次の方法でVM0に接続できる必要があります。
JITVMアクセスを使用します。
参照：
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。ケーススタディは個別にタイミングが調整されていません。
あなたはあなたがするのと同じくらい多くの試験時間を使うことができます
それぞれのケースを完了するのが好きです。ただし、この試験には追加のケーススタディ
とセクションがある場合があります。君は
あなたがこの試験に含まれるすべての質問を完了することができることを保証するために
あなたの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、より多くの情報を提供する展示やその他のリソースが含まれている場合があります
ケーススタディで説明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。この画面では、回答を確認できます
試験の次のセクションに進む前に変更を加えます。新しいセクションを開始した後、
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には
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ます。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、問題の説明などの情報。場合は
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あることに注意してください。
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を置き、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。

とニューヨーク。
同社は、サーバーインフラストラクチャ全体をAzureでホストしています。
Contosoには、Sub1とSub2という名前の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に関連付けられています
contoso.comという名前のAzureActiveDirectory（Azure AD）テナント。
技術要件
Contosoは、次の技術要件を識別します。
Sub2のVNetWork1にAzureファイアウォールをデプロイします。
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、最小特権の原則を使用してください。
contoso.comのAzureAD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。
User2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。
サブ2
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ルールがあります。
NSG2には、次の表に示すインバウンドセキュリティルールがあります。
NSG3には、次の表に示すインバウンドセキュリティルールがあります。
NSG4には、次の表に示すインバウンドセキュリティルールがあります。
NSG1、NSG2、NSG3、およびNSG4には、次の表に示すアウトバウンドセキュリティルールがあります。
Contosoは、次の技術要件を識別します。
Sub2のVNetwork1にAzureファイアウォールをデプロイします。
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、最小特権の原則を使用してください。
contoso.comに対してAzureAD特権ID管理（PIM）を有効にします。
質問セット3

最新問題: **196**
VNET1とVNET2という名前の2つのAzure仮想ネットワークのネットワーク接続を構成しています。

次の要件を満たすには、仮想ネットワークにVPNゲートウェイを実装する必要があります。
* VNET1には、BGPを使用する6つのサイト間接続が必要です。
* VNET2には、BGPを使用する12のサイト間接続が必要です。
*コストを最小限に抑える必要があります。
各仮想ネットワークにどのVPNゲートウェイSKI）を使用する必要がありますか？回答するには、適切なSKUを正しいネットワークにドラッグします。各SKU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：丌しい選択はそれぞれ1ポイントの価値があります
Answer:
Explanation:
参照：
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

最新問題**: 197**
LAW1という名前のAzureLogAnalytics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 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。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
参照：
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

最新問題: **198**
Azureキーボールトを作成する必要があります。ソリューションでは、キーボールトから削除されたオブジェクトが90日間保持されるようにする必要があります。
コマンドをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

最新問題: **199**
Azure Kubernetes Service（AKS）クラスターをテストしています。クラスターは、展示に示されているように構成されています。
[展示]タブをクリックします。）
クラスターを実稼働環境にデプロイすることを計画しています。HTTPアプリケーションルーティングを無効にします。
単一のIPアドレスを使用して、AKSサービスにリバースプロキシとTLSターミネーション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。
あなたは何をするべきか？
A. AKSIngressコントローラーを作成します。
B. コンテナネットワークインターフェイス（CNI）プラグインをインストールします。
C. Azure標準ロードバランサーを作成します。
D. Azure BasicLoadBalancerを作成します。
Answer: A (メーッセージを残す**)**
説明
入力コントローラーは、リバースプロキシ、構成可能なトラフィックルーティング、およびKubernetesサービスのTLSターミネーションを提供するソフトウェアです。
参照：
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

最新問題: **200**
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。
User1はGroup1のメンバーです。Group1とUser2には、Vault1のKeyVaultContributorロールが割り当てられています。
2019年1月1日に、Vault1でシークレットを作成します。シークレットは展示に示されているように構成されています。 [展示]タブをクリックします。）
User2には、Vault1へのアクセスポリシーが割り当てられています。ポリシーには次の構成があります。

*主要な管理操作：取得、一覧表示、および復元
*暗号化操作：キーの復号化とアンラップ
*秘密の管理操作：取得、一覧表示、および復元
Group1にはVault1へのアクセスが割り当てられています。ポリシーには次の構成があります。
*キー管理操作：取得と回復
*シークレット管理操作：リスト、バックアップ、およびリカバリ
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。
Answer:

最新問題**: 201**
仮想マシンを含むAzureサブスクリプションがあります。
すべての仮想マシンへのジャストインタイム（JIT）VMアクセスを有効にします。
リモートデスクトップを使用して仮想マシンに接続する必要があります。
あなたは最初に何をすべきですか？
A. Azure Directory（Azure AD）の特権ID管理（PIM）から、セキュリティ管理者のユーザーロールをアクティブ化します。
B. Azure Active Directory（Azure AD）の特権ID管理（PIM）から、仮想マシンの所有者の役割をアクティブ化します。
C. Azureポータルから、仮想マシンを選択し、[接続]を選択してから、[アクセスの要求]を選択します。
D. Azureポータルから仮想マシンを選択し、NetworkWatcherAgent仮想マシン拡張機能を追加します。
Answer: C (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

最新問題**: 202**
AzureContainerRegistryに接続するAzureKubernetesService（AKS）クラスターがあります。
Azure Container Registryに対して認証するには、AKSクラスター用に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。
何を作成する必要がありますか？
A. AzureKeyVaultの秘密
B. 役割の割り当て
C. Azure Active Directory（Azure AD）ユーザー
D. Azure Active Directory（Azure AD）グループ
Answer: B (メーッセージを残す**)**
参照：

https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

最新問題**: 203**
新しいAzureサブスクリプションを作成します。
AzureSecurityCenter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。
実行する必要がある2つのアクションはどれですか？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。
A. オンボードAzure Active Directory（Azure AD）ID保護。
B. AzureStorageアカウントを作成します。
C. AzureAdvisorの推奨事項を実装します。
D. AzureLogAnalytics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料金階層を標準にアップグレードします。
Answer: B,D (メーッセージを残す**)**
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。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

最新問題**: 204**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
sub1という名前のAzureサブスクリプションがあります。
RG1という名前のリソースグループにsa1という名前のAzureStorageアカウントがあります。
ユーザーとアプリケーションは、いくつかの共有アクセス署名（SAS）と保存されたアクセスポリシーを使用して、sa1のblobサービスとファイルサービスにアクセスします。
許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。
sa1へのすべてのアクセスを取り消す必要があります。
解決策 :sa1にロックを作成します。
これは目標を達成していますか？
A. はい

B. いいえ
Answer: B (メーッセージを残す**)**
説明
https://www.fast2test.com/AZ-500-practice-test.html 15
有効なFast2testAZ-500試験PDFダンプ新しいAZ-500実際の試験問題
Explanation:
保存されたアクセスポリシーを取り消すには、ポリシーを削除するか、署名付き識別子を変更して名前を変更します。
署名された識別子を変更すると、既存の署名と保存されているアクセスポリシーの間の関連付けが解除されます。保存されたアクセスポリシーを削除または名前変更すると、それに関連付けられているすべての共有アクセス署名にすぐに影響します。
参照：
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

最新問題**: 205**
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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 206**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
KeyVault10598168 Azureキーボールトに格納されているキーを使用して、rg1lod10598168n1Azureストレージアカウントが暗号化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。
Answer:
手順1 :Azureポータルで顧客が管理するキーを有効にするには、次の手順に従います。

1.ストレージアカウントrg1lod10598168n1に移動します
2.ストレージアカウントの[設定]ブレードで、[暗号化]をクリックします。次の図に示すように、[独自のキーを使用する]オプションを選択します。
手順2 :キーボールトからキーを指定する
キーボールトからキーを指定するには、最初に、キーを含むキーボールトがあることを確認します。キーボールトからキーを指定するには、次の手順に従います。
4.[キーボールトから選択]オプションを選択します。
5.使用するキーを含むキーボールトKeyVault10598168を選択します。
6.キーボールトからキーを選択します。
参照：
https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal

最新問題**: 207**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Active Directory（Azure AD）のハイブリッド構成があります。
仮想ネットワーク上にAzureHDInsightクラスターがあります。
オンプレミスのActiveDirectory資格情報を使用して、ユーザーがクラスターに対して認証できるようにすることを計画しています。
計画された認証をサポートするように環境を構成する必要があります。
解決策 :AzureADアプリケーションプロキシをデプロイします。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: (解答を表示する**)**
説明
代わりに、Azure Virtual NetworksとVPNゲートウェイを使用して、HDInsightをオンプレミスネットワークに接続します。
注：参加しているネットワーク内のHDInsightとリソースが名前で通信できるようにするには、次のアクションを実行する必要があります。
*Azure仮想ネットワークを作成します。
*Azure仮想ネットワークにカスタムDNSサーバーを作成します。
*デフォルトのAzureRecursiveResolverの代わりにカスタムDNSサーバーを使用するように仮想ネットワークを構成します。
*カスタムDNSサーバーとオンプレミスDNSサーバー間の転送を構成します。
参照：

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

最新問題: **208**
User2が現在の状態で変更および削除できるSub1の仮想ネットワークはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources
トピック3、Fabrikam Inc
総括
Fabrikam、Inc.は、モントリオールに本社を置き、シアトルとニューヨークに支社を置くコンサルティング会社です。Fabrikamには、IT、人材（HR）、および財務部門があります。
既存の環境
ネットワーク環境
Fabrikamには、Microsoft365サブスクリプションとsubscription1という名前のAzureサブスクリプションがあります。
ネットワークには、Fabrikam.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。ドメインには、OU1およびOU2という名前の2つの組織単位（OU）が含まれています。AzureADConnectクラウド同期はOU1のみを同期します。
次の展示では、Azureリソースの階層を示しています。
Azure Active Directory（Azure AD）テナントには、次の表に示すユーザーが含まれています。
Azure ADには、次の表に示すリソースが含まれています。
Subscription1リソース
Subscription1には、次の表に示す仮想ネットワークが含まれています。
Subscription1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。
Subscription1には、次の表に示す仮想マシンが含まれています。
Subscription1には、次の表に示すAzureキーボールトが含まれています。
Subscription1には、米国西部のAzureリージョンにあるstorage1という名前のストレージアカウントが含まれています。
計画された変更と要件
計画された変更
Fabrikamは、次の変更を実装する予定です。
次の表に示すように、2つのアプリケーションセキュリティグループを作成します。
VM1のネットワークインターフェイスをASG1に関連付けます。
AzureSecurityCenterを使用してSecPol1をデプロイします。

App1という名前のサードパーティアプリをデプロイします。App1のバージョンは、使用可能なすべてのオペレーティングシステムに対応しています。
RG2という名前のリソースグループを作成します。
OU2をAzureADに同期します。
User1をGroup1に追加します。
技術要件
Fabrikamは、次の技術要件を識別します。
財務部門のユーザーは、SharePointOnlineにアクセスする3時間後に再認証する必要があります。
Storage1は、顧客が管理するキーと自動キーローテーションを使用して暗号化する必要があります。
Sentinel1から、次のノートブックを起動できることを確認する必要があります。
エンティティエクスプローラーアカウント
エンティティエクスプローラー-Windowsホスト
ガイド付き調査プロセスアラート
VM1、VM2、およびVM3は、AzureDiskEncryptionを使用して暗号化する必要があります。
VM1、VM2、およびVM3のジャストインタイム (JIT)VMアクセスを有効にする必要があります。
App1は、KeyVault1に保存されている安全な接続文字列を使用する必要があります。
KeyVault1トラフィックはインターネット上を移動してはなりません。

最新問題**: 209**
Vault1RecoveryServicesボールトのAzureBackupReportログがWS11641655AzureLogAnalyticsワークスペース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、Azureリソースを変更します。
Answer:
以下の説明を参照してください。
説明
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RecoveryServicesVault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.[診断設定の名前]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. WS11641655 AzureLogAnalytics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

最新問題: **210**
IDという名前の管理されたIDを持ち、Azure Active Directory（Azure AD）テナントにリンクされているAzureサブスクリプションがあります。テナントには、次の表に示すリソースが含まれています。
AUIとAU2に追加できるリソースはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
AU1とAU2に追加できるリソースはどれですか。回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **211**
次の表に示すオフィスを持つContoso、Ltd.という会社で働いています。
Contosoには、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。すべてのcontoso.comユーザーは、Azure Multi-Factor Authentication（MFA）を有効にしています。テナントには、次の表に示すユーザーが含まれています。
contoso.comの多要素設定は、次の展示に示すように構成されています。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題: **212**
Azureサブスクリプションを含むMG1という名前の管理グループと、RG1という名前のリソースグループがあります。RG1には、VM1という名前の仮想マシンが含まれています。次の表に示すカスタムAzureロールがあります。

Role1の権限は、次の役割定義ファイルに示されています。
次の表に示すユーザーに役割を割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 213**
Sub1という名前のAzureサブスクリプションがあります。
ITチームのすべてのメンバーを含むGroup1という名前のAzureActiveDirectory（Azure AD）グループがあります。
Group1のメンバーが、Sub1のAzure仮想マシンを停止、起動、および再起動できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
Explanation:
参照：
https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

最新問題**: 214**
次のリソースを含むAzureサブスクリプションがあります。
Subnet1とSubnet2という名前の2つのサブネットを含むVNET1という名前の仮想ネットワーク。
プライベートIPアドレスのみを持ち、Subnet1に接続するVM1という名前の仮想マシン。
インターネットからVM1へのリモートデスクトップ接続を確立できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序で並べ替えます。
Answer:

最新問題**: 215**
次の表に示すリソースを含むAzureActiveDirectory（Azure AD）テナントがあります。
User2はGroup2の所有者です。
App1のユーザーとグループの設定は、次の図に示すように構成されています。
次の展示に示すように、App1のセルフサービスアプリケーションアクセスを有効にします。
User3は、Applへのアクセスを承認するように構成されています。
Group2の所有者とApplのユーザーを特定する必要があります。

何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

最新問題: **216**
プラットフォーム保護要件を満たすには、AKS1を展開する必要があります。
順番に実行する必要がある4つのアクションはどれですか？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、正しい順序に並べます。
注：回答の選択肢の複数の順序が正しいです。選択した正しい注文のいずれかに対してクレジットを受け取ります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

最新問題: **217**
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。
すべての仮想ネットワークがピアリングされます。
AzureBastionをVNET2にデプロイします。
要塞ホストで保護できる仮想マシンはどれですか？
A. VM1、VM2、VM3、およびVM4
B. VM1、VM2、およびVM3のみ
C. VM2およびVM4のみ
D. VM2のみ
Answer: A (メーッセージを残す**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

最新問題: **218**
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。
許可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。
何を設定する必要がありますか？
A. Azure Active Directory（Azure AD）特権ID管理（PIM）
B. アプリケーションセキュリティグループ

C. Azure Active Directory（Azure AD）の条件付きアクセス
D. ジャストインタイム（JIT）VMアクセス
Answer: D (メーッセージを残す)
説明
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役割ベースのアクセス制御（RBAC）権限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

最新問題**: 219**
新しいAzureサブスクリプションを作成します。
AzureSecurityCenter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。
実行する必要がある2つのアクションはどれですか？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。
A. オンボードAzure Active Directory（Azure AD）ID保護。
B. AzureStorageアカウントを作成します。
C. AzureAdvisorの推奨事項を実装します。
D. AzureLogAnalytics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料金階層を標準にアップグレードします。
Answer: D,E (メーッセージを残す)
説明
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

最新問題: **220**
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
2019年1月1日、Vault1は次のシークレットを保存します。
アプリケーションが各シークレットを使用できるのはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1：決して
Password1は無効になっています。
ボックス2：2019年3月1日から5月1日までのみ
Password2：
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

最新問題: **221**
App1という名前のアプリを含むAzureサブスクリプションがあります。App1には、次の表に示すアプリ登録があります。
App1がすべてのユーザーカレンダーを読み取り、予定を作成できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
あなたは何をするべきか？
A. Microsoft.GraphCalendars.ReadWrite.Sharedの新しい委任API権限を追加します。
B. Microsoft.GraphCalendars.ReadWriteの新しい委任API権限を追加します。
C. [管理者の同意を付与する]を選択します。
D. Microsoft.GraphCalendars.ReadWriteの新しいアプリケーションAPI権限を追加します。
Answer: B (メーッセージを残す**)**

最新問題: **222**
Azureサブネットにバインドされたネットワークセキュリティグループ（NSG）があります。
Get-AzureRmNetworkSecurityRuleConfigを実行すると、次の展示に示す出力が表示されます。
ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1：米国東部に接続可能

StorageEA2AllowにはDestinationAddressPrefix{Storage/EastUS2}があります
ボックス2 :ドロップ
参照：
https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

最新問題**: 223**
Group1とGroup2のメンバーシップは何ですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :User1、User2、User3、User4
文字列と正規表現の操作では大文字と小文字が区別されないため、モントリオール（User1）、MONTREAL（User2）、ロンドン（User 3）、およびオンタリオ（User4）には「ON」が含まれます。
ボックス2 :User3のみ
一致「on」はロンドン（User3）にのみ当てはまります。
シナリオ：
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。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

最新問題**: 224**
次のリソースを含むAzureサブスクリプションがあります。
Subnet1とSubnet2という名前の2つのサブネットを含むVNET1という名前の仮想ネットワーク。
プライベートIPアドレスのみを持ち、Subnet1に接続するVM1という名前の仮想マシン。
インターネットからVM1へのリモートデスクトップ接続を確立できることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序で並べ替えます。
Answer:

最新問題**: 225**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。

パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
VM1という名前の仮想マシンの平均CPU使用率が15分間で70%を超える場合は、admin1@contoso.comという名前の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。
以下の説明を参照してください。
Answer:
説明
Azureポータルを使用してメトリックにアラートルールを作成する
1.ポータルで、監視対象のリソース（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（クラシック）の追加]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
状態 :より大きい
期間：過去5分間
通知 :メール
追加の管理者メール :admin1@contoso.com
参照：
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

最新問題**: 226**
次の表に示すユーザーを含むcontoso.comという名前のAzureActiveDirectory（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ContosoSales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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
参照：
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy

最新問題**: 227**
VNET1とVNET2という名前の2つのAzure仮想ネットワークのネットワーク接続を構成しています。
次の要件を満たすには、仮想ネットワークにVPNゲートウェイを実装する必要があります。
* VNET1には、BGPを使用する6つのサイト間接続が必要です。
* VNET2には、BGPを使用する12のサイト間接続が必要です。
*コストを最小限に抑える必要があります。
各仮想ネットワークにどのVPNゲートウェイSKI）を使用する必要がありますか？回答するには、適切なSKUを正しいネットワークにドラッグします。各SKU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
Answer:
参照：
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

最新問題**: 228**
ネットワークには、contoso.comという名前のActiveDirectoryフォレストが含まれています。フォレストには単一のドメインが含まれています。
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、ActiveDirectoryとAzureAD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に同期されるユーザーアカウントに適用されることを確認します
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必要がありますか？
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. シームレスなシングルサインオン（SSO）を使用したパスワードハッシュ同期
C. シームレスなシングルサインオン（SSO）を使用したパススルー認証
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
パスワードハッシュの同期には、展開、メンテナンス、および
インフラストラクチャー。このレベルの取り組みは通常、ユーザーが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AzureAD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AzureADConnect同期プロセスの一部であり、2分ごとに実行されます。
不正解：
A :フェデレーション認証システムは、外部の信頼できるシステムに依存してユーザーを認証します。いくつか
企業は、既存の連合システムへの投資をAzureADハイブリッドIDで再利用したいと考えています
解決。連合システムの保守と管理は、AzureADの制御の範囲外です。
連合システムを使用して安全に展開され、次のことができるかどうかは、組織次第です。
認証の負荷を処理します。
C :パススルー認証には、1つ以上（3つをお勧めします）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ます。これらのエージェントは、オンプレミスのActiveDirectory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ー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ーへのアクセス。このため、エージェントを
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ーへの制約のないネットワークアクセスが必要です。すべてのネットワーク
トラフィックは暗号化され、認証要求に制限されます。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

最新問題**: 229**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。

パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
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。
Answer:
以下の説明を参照してください。
説明
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]を選択してから、次の項目の選択肢を選択します。
3. Log Analytics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 :LogAnalyticsVM拡張機能を有効にする
WindowsおよびLinux用のLogAnalyticsVM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（手順で作成した名前）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

最新問題**: 230**
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、WindowsServerを実行するAzure仮想マシンが含まれています
2016年。
ポリシーを実装して、各仮想マシンにカスタムのアンチウイルス仮想マシン拡張機能がインストールされていることを確認する必要があります。
ポリシーをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1 :DeployIfNotExists
DeployIfNotExistsは、条件が満たされたときにテンプレート展開を実行します。
ボックス2 :テンプレート
DeployIfNotExistsエフェクトのdetailsプロパティには、照合する関連リソースと実行するテンプレートデプロイメントを定義するすべてのサブプロパティがあります。
展開[必須]
このプロパティには、Microsoft.Resources /deployationリファレンスに渡される完全なテンプレートデプロイメントが含まれている必要があります。
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

最新問題**: 231**
RG2の作成とRG1の権限の管理を委任する必要があります。どのユーザーが各タスクを実行できますか？答えるには、答えの中から適切なオプションを選択してください。注：正しい選択はそれぞれ1ポイントの価値があります
Answer:

最新問題**: 232**
更新管理が有効になっているAzure仮想マシンがあります。仮想マシンは、次の表に示すように構成されています。
Update1とUpdate2という名前の2つの更新デプロイメントをスケジュールします。Update1はVM3を更新します。Update2はVM6を更新します。
Update1とUpdate2を使用して更新できる追加の仮想マシンはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:
参照：
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

最新問題**: 233**
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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
Explanation:
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。

最新問題**: 234**
次の表に示す仮想ネットワークを含むAzureサブスクリプションがあります。
SpokeVNetSubnet0上のAzure仮想マシンは、オンプレミスネットワーク上のコンピューターと通信できます。
AzureファイアウォールをHubVNetにデプロイすることを計画しています。
次の2つのルーティングテーブルを作成します。
* RT1 :AzureファイアウォールのプライベートIPアドレスをネクストホップアドレスとして指すユーザー定義ルートが含まれます
* RT2 :BGPルートの伝播を無効にし、Azureファイアウォールのプライベート IPアドレスをデフォルトゲートウェイとして定義します。SpokeVNetSubnet0とオンプレミスネットワーク間のトラフィックがAzureファイアウォールを通過するようにする必要があります。
各ルートテーブルをどのサブネットに関連付ける必要がありますか？答えるには、適切なサブネットを正しいルートテーブルにドラッグします。各サブネットは、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。
Answer:
説明

最新問題**: 235**
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AzureStorage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。

Container1のコンテンツにアクセスして共有するために使用できるツールはどれですか。SASを使用して？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 236**
次の表に示すリソースを含むSubcription1という名前のAzureサブスクリプションがあります。
次のJSONファイルを使用してAzureロールを作成します。
Role1をRG1のUser1に割り当てます。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:

最新問題**: 237**
ネットワークには、Azure Active Directory（Azure AD）と同期するadatum.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。
Azure ADテナントには、次の表に示すユーザーが含まれています。
次の展示に示すように、認証方法-adatum.comのパスワード保護設定を構成します。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-sumption-deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

最新問題**: 238**
次の表に示すAzureキーボールトを含むSub1という名前のAzureサブスクリプションがあります。
Sub1では、次の構成を持つ仮想マシンを作成します。
*名前 :VM1
*サイズ :DS2v2
*リソースグループ :RG1
*地域：西ヨーロッパ
*オペレーティングシステム :Windows Server 2016

VM1でAzureDiskEncryptionを有効にする予定です。
VM1の暗号化キーを保存できるキーボールトはどれですか？
A. Vault1またはVault2のみ
B. Vault1、Vault2、Vault3、またはVault4
C. Vault1またはVault3のみ
D. Vault1のみ
Answer: A (メーッセージを残す**)**

最新問題**: 239**
Azure Active Directory（Azure AD）のハイブリッド構成があります。AzureAD認証をサポートするように構成されたAzureSQLデータベースインスタンスがあります。
データベース開発者は、データベースインスタンスに接続し、オンプレミスのActiveDirectoryアカウントを使用して認証する必要があります。
開発者がMicrosoftSQLServerManagementStudioを使用してインスタンスに接続できることを確認する必要があります。ソリューションは、認証プロンプトを最小限に抑える必要があります。
どの認証方法をお勧めしますか？
A. ActiveDirectory-パスワード
B. ActiveDirectory-MFAをサポートするユニバーサル
C. SQLServer認証
D. ActiveDirectory-統合
Answer: A (メーッセージを残す**)**
説明
AzureAD管理対象ドメインを使用してAzureADプリンシパル名に接続する場合は、ActiveDirectoryパスワード認証を使用します。
この方法を使用して、ネイティブまたはフェデレーションAzureADユーザーのAzureADでSQLDB/DWを認証します。ネイティブユーザーは、Azure ADで明示的に作成され、ユーザー名とパスワードを使用して認証されるユーザーです。一方、フェデレーションユーザーは、ドメインがAzureADとフェデレーションされているWindowsユーザーです。後者の方法（ユーザーとパスワードを使用）は、ユーザーがWindowsクレデンシャルを使用したいが、ローカルマシンがドメインに参加していない場合（たとえば、リモートアクセスを使用）に使用できます。この場合、Windowsユーザーは自分のドメインアカウントとパスワードを指定し、フェデレーション資格情報を使用してSQL DB/DWに対して認証できます。

最新問題**: 240**
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
2019年1月1日、Vault1は次のシークレットを保存します。
アプリケーションが各シークレットを使用できるのはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:
説明
ボックス1：決して
Password1は無効になっています。
ボックス2 :2019年3月1日から5月1日までのみ
Password2：
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

最新問題**: 241**
Homepage-AGWという名前のAzureApplicationGatewayを介した接続で、悪意のある要求がないかどうか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。
タスクが完了するのを待つ必要はありません。
Answer:
以下の説明を参照してください。
ApplicationGatewayでWebApplicationFirewallを有効にする必要があります。
Azureポータルで、検索ボックスに 「アプリケーションゲートウェイ」と入力し、検索結果から[アプリケーションゲートウェイ]を選択してから、[ホームページ-AGW] という名前のゲートウェイを選択します。または、左側のナビゲーションペインで[アプリケーションゲートウェイ]を参照します。
アプリケーションゲートウェイのプロパティで、をクリックします
Tier設定には、WAFV2を選択します。
[ファイアウォールステータス]セクションで、スライダーをクリックして切り替えます
[ファイアウォールモード]セクションで、スライダーをクリックして切り替えます
[保存]をクリックして変更を保存します。

最新問題**: 242**
App1という名前のアプリを含むAzureサブスクリプションがあります。App1には、次の表に示すアプリ登録があります。

App1がすべてのユーザーカレンダーを読み取り、予定を作成できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
あなたは何をするべきか？
A. Microsoft.GraphCalendars.ReadWriteの新しい委任API権限を追加します。
B. Microsoft.GraphCalendars.ReadWriteの新しいアプリケーションAPI権限を追加します。
C. [管理者の同意を付与する]を選択します。
D. Microsoft.GraphCalendars.ReadWrite.Sharedの新しい委任API権限を追加します。
Answer: A (メーッセージを残す)
参照：
https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

最新問題**: 243**
Azure Active Directory（Azure AD）テナントがあります。
次の表に示すように、削除されたオブジェクトがあります。
2020年5月4日に、AzureActiveDirectory管理センターを使用して削除されたオブジェクトを復元しようとしました。
どの2つのオブジェクトを復元できますか？それぞれの正解は完全な解決策を提示します。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. グループ1
B. グループ2
C. User2
D. User1
Answer: B,C (メーッセージを残す)
セクション :[なし]
Explanation:
削除されたユーザーと削除されたOffice365グループは、30日間復元できます。
削除したセキュリティグループを復元することはできません。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

最新問題**: 244**
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
2019年1月1日、Vault1は次のシークレットを保存します。
アプリケーションが各シークレットを使用できるのはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1：決して

Password1は無効になっています。
ボックス2 :2019年3月1日から5月1日までのみ
Password2：
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

最新問題**: 245**
次の表に示すリソースを含むAzureActiveDirectory（Azure AD）テナントがあります。
User2はGroup2の所有者です。
App1のユーザーとグループの設定は、次の図に示すように構成されています。
次の展示に示すように、App1のセルフサービスアプリケーションアクセスを有効にします。
User3は、Applへのアクセスを承認するように構成されています。
Group2の所有者とApplのユーザーを特定する必要があります。
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

最新問題**: 246**
会社には、AzureActiveDirectory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、OAuth2の暗黙的な付与タイプを使用して
AzureADアクセストークンを取得します。
App1をAzureAD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には、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
Answer: (解答を表示する**)**
説明/参照：
Explanation:

ネイティブアプリケーションの場合、AzureAD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。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

最新問題**: 247**
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
2019年1月1日、Vault1は次のシークレットを保存します。
アプリケーションが各シークレットを使用できるのはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

最新問題**: 248**
ContosoKey1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
次の表に示すように、ユーザーを作成してロールを割り当てます。
次のアクションを実行できるユーザーを特定する必要があります。
ContsosKey1の権限を委任します。
ContosoKey1へのネットワークアクセスを構成します。
どのユーザーを特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

最新問題**: 249**
VNET1とVNET2という名前の2つのAzure仮想ネットワークのネットワーク接続を構成しています。
次の要件を満たすには、仮想ネットワークにVPNゲートウェイを実装する必要があります。
* VNET1には、BGPを使用する6つのサイト間接続が必要です。
* VNET2には、BGPを使用する12のサイト間接続が必要です。
*コストを最小限に抑える必要があります。

各仮想ネットワークにどのVPNゲートウェイSKI）を使用する必要がありますか？回答するには、適切なSKUを正しいネットワークにドラッグします。各SKU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
Answer:
参照：
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

最新問題**: 250**
技術的な要件を満たすには、AzureSentinelノートブックのサポートを構成する必要があります。
必要なAzureコンテナーレジストリとAzureMachineLearningワークスペースの最小数はいくつですか？
Answer:
参照：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

最新問題**: 251**
Sub1という名前のAzureサブスクリプションがあります。
ITチームのすべてのメンバーを含むGroup1という名前のAzureActiveDirectory（Azure AD）グループがあります。
Group1のメンバーが、Sub1のAzure仮想マシンを停止、起動、および再起動できることを確認する必要があります。
ソリューションは、最小特権の原則を使用する必要があります。
順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
参照：
https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

最新問題**: 252**
Sub2の仮想マシン間のネットワーク通信のセキュリティを評価しました。
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明

最新問題: **253**
Sub1という名前のAzureサブスクリプションがあります。
1つのサブネットを含む仮想ネットワークを作成します。サブネット上で、次の表に示す仮想マシンをプロビジョニングします。
現在、ネットワークセキュリティグループ (NSG)はプロビジョニングされていません。
次の要件を満たすには、ネットワークセキュリティを実装する必要があります。
*VM3からVM4へのトラフィックのみを許可します。
*インターネットからVM1およびVM2へのトラフィックのみを許可します。
*NSGとネットワークセキュリティルールの数を最小限に抑えます。
NSGとネットワークセキュリティルールをいくつ作成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
NSG :2
ネットワークセキュリティルール :3
2以外 :セキュリティルールで複数のサービスタグまたはアプリケーショングループを指定することはできません。
参照：
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

最新問題: **254**
複数のWindowsサーバーをWS11641655AzureLogAnalytics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。
Answer:
以下の説明を参照してください。
説明
Azure Monitorは、WindowsイベントログまたはLinux Syslogからイベントを収集し、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を使用して、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

最新問題: **255**
User2がPIMを実装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？
A. User2にグローバル管理者の役割を割り当てます。
B. contoso.comの認証方法を構成します。
C. contoso.comのIDセキュア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。
Answer: (解答を表示する**)**
説明
ディレクトリでPIMの使用を開始するには、最初に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。
ディレクトリのPIMを有効にするには、Microsoftアカウント（@ outlook.comなど）ではなく、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。
シナリオ：技術要件は次のとおりです。contoso.comのAzure AD特権ID管理（PIM）を有効にする参照：
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

最新問題: **256**
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。の各質問
このシリーズには、定められた目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには
複数の正しい解決策がありますが、他の人は正しい解決策を持っていない可能性があります。
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。結果として、これらは
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AzureHDInsightクラスターがあります。

オンプレミスのActiveDirectory資格情報を使用して、ユーザーがクラスターに対して認証できるようにすることを計画しています。
計画された認証をサポートするように環境を構成する必要があります。
解決策：仮想ネットワークとオンプレミスネットワークの間にサイト間VPNを作成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: A (メーッセージを残す**)**
Azure Virtual NetworksとVPNゲートウェイを使用して、HDInsightをオンプレミスネットワークに接続できます。
注：参加しているネットワーク内のHDInsightとリソースが名前で通信できるようにするには、次の手順を実行する必要があります。
次のアクション：
*Azure仮想ネットワークを作成します。
*Azure仮想ネットワークにカスタムDNSサーバーを作成します。
*デフォルトのAzureRecursive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する
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。
参照：
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-sumption-network

最新問題**: 257**
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エージェントはどの仮想マシンにインストールされていますか？
A. VM3のみ
B. VM1およびVM3のみ
C. VM3およびVM4のみ
D. VM1、VM2、VM3、およびVM4

Answer: D (メーッセージを残す)
自動プロビジョニングがオンの場合、セキュリティセンターは、サポートされているすべてのAzureVMと作成された新しいVMでLogAnalyticsAgent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）、および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-enable-data-collection

最新問題**: 258**
シミュレーション
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名：User1-10598168@ExamUsers.com
Azureパスワード：Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス：10598168
管理ユーザーがVNET1という名前の仮想ネットワークを誤って削除しないようにする必要があります。管理ユーザーは、VNET1の設定を変更でき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。
A. ロックすると、組織内の他のユーザーが、Azureサブスクリプション、リソースグループ、リソースなどの重要なリソースを誤って削除または変更するのを防ぐことができます。
注：Azureでは、リソースという用語はAzureによって管理されるエンティティを指します。たとえば、仮想マシン、仮想ネットワーク、およびストレージアカウントはすべてAzureリソースと呼ばれます。
1.仮想ネットワークVNETの[設定]ブレードで、[ロック]を選択します。
2.ロックを追加するには、[追加]を選択します。
3. [ロックの種類]で[ロックの削除]を選択し、[OK]をクリックします
B. ロックすると、組織内の他のユーザーが、Azureサブスクリプション、リソースグループ、リソースなどの重要なリソースを誤って削除または変更するのを防ぐことができます。
注：Azureでは、リソースという用語はAzureによって管理されるエンティティを指します。たとえば、仮想マシン、仮想ネットワーク、およびストレージアカウントはすべてAzureリソースと呼ばれます。
1.仮想ネットワークVNETの[設定]ブレードで、[ロック]を選択します。
2.ロックを追加するには、[追加]を選択します。

3. [ロックの種類]で[ロックの削除]を選択し、[OK]をクリックします
Answer: B (メーッセージを残す)
参照：
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

最新問題**: 259**
Vault1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
2019年1月1日、Vault1は次のシークレットを保存します。
アプリケーションが各シークレットを使用できるのはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
ボックス1：決して
Password1は無効になっています。
ボックス2 :2019年3月1日から5月1日までのみ
Password2：
参照：
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

最新問題**: 260**
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。
同社はApp1という名前のアプリケーションを開発しています。App1は、Windows Server 2016を実行するサーバー上のサービスとして実行されます。App1は、contoso.comに対して認証され、MicrosoftGraphにアクセスしてディレクトリデータを読み取ります。
最低限必要な権限をApp1に委任する必要があります。
Azureポータルから順番に実行する必要がある3つのアクションはどれですか？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、正しい順序に並べます。
Answer:
説明
ステップ1 :アプリ登録を作成する
まず、アプリケーションを作成/登録する必要があります。
手順2 :アプリケーションのアクセス許可を追加する
アプリケーションのアクセス許可は、サインインしたユーザーがいない状態で実行されるアプリによって使用されます。
ステップ3：権限を付与する

最新問題: **261**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。
各ユーザーには、Azure AD Premium？2ライセンスが割り当てられます。
オンボードで計画し、AzureADID保護を構成します。
Azure AD Identity Protectionをオンボードし、ユーザーを修正し、ポリシーを構成できるユーザーはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります
Answer:
説明

最新問題: **262**
User1という名前のユーザーとConReg1という名前のAzureContainerRegistryを含むAzureサブスクリプションがあります。
ContReg1のコンテンツ信頼を有効にします。
User1がContReg1で信頼できるイメージを作成できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
User1に割り当てる必要がある2つの役割はどれですか？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。
A. AcrQuarantineReader
B. 寄稿者
C. AcrPush
D. AcrImageSigner
E. AcrQuarantineWriter
Answer: (解答を表示する**)**
説明/参照：
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles
https://www.fast2test.com/AZ-500-practice-test.html 39
有効なFast2testAZ-500試験PDFダンプ新しいAZ-500実際の試験問題

最新問題: **263**
AzureSQLデータベースがあります。
https://www.fast2test.com/AZ-500-practice-test.html 85
有効なFast2testAZ-500試験PDFダンプ新しいAZ-500実際の試験問題
AlwaysEncrypted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ことを確認する必要があります。
開発者に提供する必要がある2つの情報はどれですか。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。
A. 保存されたアクセスポリシー
B. 共有アクセス署名（SAS）
C. 列暗号化キー
D. ユーザーの資格情報
E. 列マスターキー
Answer: (解答を表示する**)**
Always Encrypted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。列暗号化キーは、暗号化された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、1つ以上の列暗号化キーを暗号化するキー保護キーです。
参照：
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

最新問題**: 264**
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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明

最新問題**: 265**
contoso.comという名前のAzureActiveDirectory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。
各ユーザーには、Azure AD Premium？2ライセンスが割り当てられます。
オンボードで計画し、AzureADID保護を構成します。
Azure AD Identity Protectionをオンボードし、ユーザーを修正し、ポリシーを構成できるユーザーはどれですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります
Answer:

最新問題: **266**
ContosoKey1という名前のAzureキーボールトを含むAzureサブスクリプションがあります。
次の表に示すように、ユーザーを作成してロールを割り当てます。
次のアクションを実行できるユーザーを特定する必要があります。
ContsosKey1の権限を委任します。
ContosoKey1へのネットワークアクセスを構成します。
どのユーザーを特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
参照：
https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

最新問題: **267**
Azure Kubernetes Service（AKS）クラスターをテストしています。クラスターは、展示に示されているように構成されています。
[展示]タブをクリックします。）
クラスターを実稼働環境にデプロイすることを計画しています。HTTPアプリケーションルーティングを無効にします。
AKSサービスにリバースプロキシとTLSターミネーション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アドレスを使用します。
あなたは何をするべきか？
A. AKSIngressコントローラーを作成します。
B. コンテナネットワークインターフェイス（CNI）プラグインをインストールします。
C. Azure標準ロードバランサーを作成します。
D. Azure BasicLoadBalancerを作成します。
Answer: (解答を表示する**)**
入力コントローラーは、リバースプロキシ、構成可能なトラフィックルーティング、およびTLSを提供するソフトウェアです。
Kubernetesサービスの終了。
参照：
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

最新問題: **268**
storage1という名前のAzureStorageアカウントと、VM1という名前のAzure仮想マシンがあります。VM1にはプレミアムSSD管理対象ディスクがあります。
VM1に対してAzureDiskEncryptionを有効にする必要があります。

順番に実行する必要がある3つのアクションはどれですか？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、正しい順序で並べ替えます。
Answer:
参照：
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

最新問題**: 269**
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン]ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、[パスワードの入力]ボックスにカーソルを置き、下のパスワードをクリックします。
Azureユーザー名 :User1-10598168@ExamUsers.com
Azureパスワード :Ag1Bh9！#Bd
以下の情報は、技術サポートのみを目的としています。
ラボインスタンス :10598168
Microsoft Antimalware for Virtual Machinesを使用して、VM1という名前の仮想マシンで毎週日曜日の02:00に完全なマルウェアスキャンを実行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。
Answer:
以下の説明を参照してください。
説明
AzurePortalを使用してMicrosoftAntimalwareExtensionをデプロイし、単一のVMをデプロイします
1. Azureポータルで、Azure VM1のブレードに移動し、[拡張機能]セクションに移動して、[追加]を押します。
2. Microsoft Antimalware拡張機能を選択し、[作成]を押します。
3.必要に応じて 拡張機能のインストール」フォームに入力し、 OK」を押します。スケジュール :EnableScanタイプ :FullScan日：
日曜日
参照：
https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

最新問題**: 270**
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。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer:
説明
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

最新問題**: 271**
User1という名前のユーザーを含むcontoso.comという名前のAzureActiveDin-dory（Azure AD）テナントがあります。
テナントで複数のアプリを公開する予定です。
User1が公開されたアプリの管理者同意を付与できることを確認する必要があります。
ユーザーに割り当てることができる2つの可能なユーザーロールはどれですか。この目標を達成するには？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。
A. ユーザー管理者
B. クラウドアプリケーション管理者
C. アプリケーション管理者
D. アプリケーション開発者
E. セキュリティ管理者
Answer: (解答を表示する**)**

有効な **AZ-500** 問題集は GoShiken.com が提供された合格しやすい AZ-500 試験問題集！ GoShiken.com が最新の **AZ-500** 試験問題集を提供しています。GoShiken.com AZ-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com AZ-500 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/AZ-500-mondaishu.html (**497**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード**:** **Freepdfdumps**)

Valid AZ-500 Dumps shared by GoShiken.com for Helping Passing AZ-500 Exam! GoShiken.com now offer the **newest AZ-500 exam dumps**, the GoShiken.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com AZ-500 dumps with Test Engine here: https://www.goshiken.com/Microsoft/AZ-500-mondaishu.html (**497** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)