

Microsoft.AZ-500.v2023-08-26.q374

|                                                                                                                                                               |                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 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:                                                                                                                                                        | 374                                   |
| バージョン:                                                                                                                                                        | v2023-08-26                           |
| アクセス数:                                                                                                                                                        | 2387                                  |
| ページビュー数:                                                                                                                                                      | 3740                                  |
| <a href="https://www.jpnpdf.com/Microsoft.AZ-500.v2023-08-26.q374-mondaishu.html">https://www.jpnpdf.com/Microsoft.AZ-500.v2023-08-26.q374-mondaishu.html</a> |                                       |

最新問題: 1

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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。

<https://www.fast2test.com/AZ-500-practice-test.html> 49

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。  
Azure サブスクリプションをお持ちです。サブスクリプションには、Windows Server 2012 R2 または Windows Server 2016 を実行する 50 台の仮想マシンが含まれています。

Microsoft Antimalware 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: ([解答を表示する](#))

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: 2

AU1 と AU2 という 2 つの管理単位を含む Azure Active Directory (Azure AD) テナントがあります。  
ユーザーは、次の表に示すように管理単位に割り当てられます。

| User name | Member of |
|-----------|-----------|
| Admin1    | AU1       |
| Admin2    | AU1       |
| Admin3    | AU2       |
| Admin4    | AU2       |
| User1     | AU1       |

Answer Area

| Statements                               | Yes                   | No                    |
|------------------------------------------|-----------------------|-----------------------|
| Admin1 can reset the password of User1.  | <input type="radio"/> | <input type="radio"/> |
| Admin2 can reset the password of User3.  | <input type="radio"/> | <input type="radio"/> |
| Admin3 can reset the password of Admin4. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                               | Yes                              | No                               |
|------------------------------------------|----------------------------------|----------------------------------|
| Admin1 can reset the password of User1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can reset the password of User3.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin3 can reset the password of Admin4. | <input type="radio"/>            | <input checked="" type="radio"/> |

最新問題: 3

Group1 と Group2 のメンバーシップは何ですか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Group1:

Microsoft

No members  
Only User2  
Only User2 and User4  
User1, User2, User3, and User4

Group2:

No members  
Only User3  
Only User1 and User3  
User1, User2, User3, and User4

Answer:

Group1:

No members  
Only User2  
Only User2 and User4  
**User1, User2, User3, and User4**

Group2:

No members  
**Only User3**  
Only User1 and User3  
User1, User2, User3, and User4

Explanation:

ボックス 1: ユーザー 1、ユーザー 2、ユーザー 3、ユーザー 4

文字列および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、ON を含む」はモントリオール (ユーザー 1)、モントリオール (ユーザー 2)、ロンドン (ユーザー 3)、およびオンタリオ (ユーザー 4) に当てはまります。

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。

| Name  | City     | Role                            |
|-------|----------|---------------------------------|
| User1 | Montreal | Global administrator            |
| User2 | MONTREAL | Security administrator          |
| User3 | London   | Privileged role administrator   |
| User4 | Ontario  | Application administrator       |
| User5 | Seattle  | Cloud application administrator |
| User6 | Seattle  | User administrator              |
| User7 | Sydney   | Reports reader                  |
| User8 | Sydney   | None                            |

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。

| Name   | Membership type | Dynamic membership rule  |
|--------|-----------------|--------------------------|
| Group1 | Dynamic user    | user.city -contains "ON" |
| Group2 | Dynamic user    | user.city -match "*on"   |

参考文献:

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

最新問題: 4

KeyVault1 という名前の Azure Key Vault があり、次の表に示す項目が含まれています。

| Name    | Type          |
|---------|---------------|
| Item1   | Key           |
| Item2   | Secret        |
| Policy1 | Access policy |

KeyVault では、次のイベントが順番に発生します。

※ 項目1は削除されました

\* 管理者が論理的な削除を有効にします

※ Item2とPolicy1は削除されます。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



Statements

Yes

No

You can recover Policy1.

☐

☐

You can add a new key named Item1.

☐

☐

You can add a new secret named Item2.

☐

☐

Answer:



Statements

Yes

No

You can recover Policy1.

☐

☒

You can add a new key named Item1.

☒

☐

You can add a new secret named Item2.

☐

☒

説明

いいえ。ポリシーは回復できません

はい、Item1 は完全に削除されます

いいえ、Item2 が Seoft-deleted ステータスにあるため、同じ名前を使用することはできません

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

最新問題: 5

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



SecurityPolicyInitiative1 という名前の Azure Policy イニシアチブを作成します。  
すべての新しいリソース グループでどの標準的な役割の割り当てを構成する必要があるかを特定します。  
新しいリソース グループの作成時に、SecurityPolicyInitiative1 とロールの割り当てを適用する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Microsoft

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

Create a custom role-based access control (RBAC) role.

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

Answer Area

⏪

⏩

⏴

⏵

Answer:

Answer Area

Create an Azure Blueprints definition

Publish an Azure Blueprints version

Assign an Azure blueprint.

- 1 - Azure Blueprints 定義を作成します。
- 2 - Azure Blueprints バージョンを公開する
- 3 - Azure ブループリントを割り当てます。

参照 :

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

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

sub1 という名前の Azure サブスクリプションがあります。

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

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

権限の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 ([メッセージを残す](#))**

説明

<https://www.fast2test.com/AZ-500-practice-test.html> 15

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

Explanation:

保存されたアクセス ポリシーを取り消すには、アクセス 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。

署名付き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直ちに影響します。

参考文献:

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

最新問題: 7

Azure サブスクリプションを作成します。

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を使用して Azure AD ロールを保護できることを確認する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

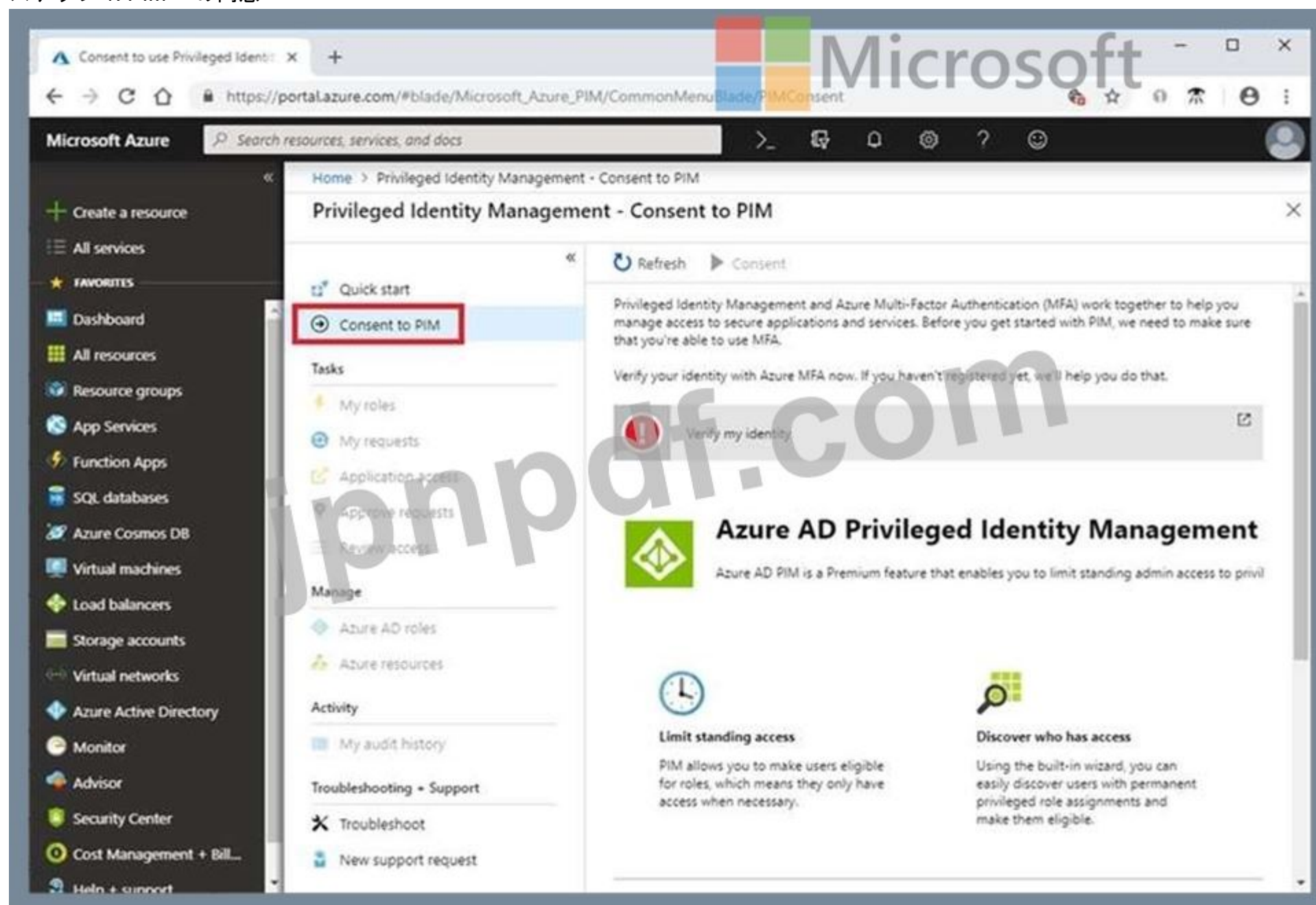


Consent to PIM.

Verify your identity by using multi-factor authentication (MFA).

Sign up PIM for Azure AD roles.

ステップ 1: PIM への同意



ステップ 2 多要素認証 (MFA) を使用して ID を確認する [ID を確認する] をクリックして、Azure MFA 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。

ステップ 3: Azure AD ロールの PIM にサインアップする

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

参考文献:



最新問題: 8

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。  
Contoso.com にはグループ名前付けポリシーが含まれています。このポリシーには、Contoso という単語を含むカスタムの禁止単語リスト  
ルールがあります。  
contoso.com で Contoso Sales という名前のグループを作成できるのはどのユーザーですか? 回答するには、回答領域で適切なオプション  
を選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Users who can create a security group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Answer:

Users who can create a security group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

説明



Users who can create a security group named Contoso Sales:

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

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

最新問題: 9

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。

| Name        | Type                  | Region      |
|-------------|-----------------------|-------------|
| RG1         | Resource group        | West Europe |
| VNET1       | Azure virtual network | West Europe |
| Contoso1901 | Azure Storage account | West Europe |

VNET1 には、Subnet1 と 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、展示に示すように構成されています。クリック

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
ByPass          : Logging, Metrics
DefaultAction    : Deny
IpRules          : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules
Action IPAddressOrRange
-----
Allow  193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules
Action VirtualNetworkResourceId State
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _
```

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

説明

| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

ボックス 1: はい

Subnet1からのアクセスは許可されます。

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からのアクセスを許可します。

最新問題: 10

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

| Name                                 | Type            | In resource group |
|--------------------------------------|-----------------|-------------------|
| 8372f433-2dcd-4361-b5ef-5b188fed87d0 | Subscription ID | Not applicable    |
| RG1                                  | Resource group  | Not applicable    |
| VM1                                  | Virtual machine | RG1               |
| VNET1                                | Virtual network | RG1               |
| storage                              | Storage account | RG1               |
| User1                                | User account    | Not applicable    |

次の JSON ファイルを使用して Azure ロールを作成します。

```
{
  "properties": {
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

RG1 の User1 に、Role1 を割り当てます。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



| Statements                                              | Yes                   | No                    |
|---------------------------------------------------------|-----------------------|-----------------------|
| User1 can create a new virtual machine in RG1.          | <input type="radio"/> | <input type="radio"/> |
| User can modify the properties of storage1.             | <input type="radio"/> | <input type="radio"/> |
| User1 can attach the network interface of VM1 to VNET1. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                              | Yes                   | No                               |
|---------------------------------------------------------|-----------------------|----------------------------------|
| User1 can create a new virtual machine in RG1.          | <input type="radio"/> | <input checked="" type="radio"/> |
| User can modify the properties of storage1.             | <input type="radio"/> | <input checked="" type="radio"/> |
| User1 can attach the network interface of VM1 to VNET1. | <input type="radio"/> | <input checked="" type="radio"/> |

参照：

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

#### 最新問題: 11

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、Group1、Group2、Group3 という 3 つのセキュリティ グループと、次の表に示すユーザーが含まれています。

| Name  | Role                            | Member of |
|-------|---------------------------------|-----------|
| User1 | Application administrator       | Group1    |
| User2 | Application developer           | Group2    |
| User3 | Cloud application administrator | Group3    |

グループ 3 はグループ 2 のメンバーです。

contoso.com で、次の設定を持つ App1 という名前のエンタープライズ アプリケーションを登録します。

所有者: ユーザー1

ユーザーとグループ: Group2

次の例に示すように、App1 のプロパティを構成します。



Enabled for users to sign-in? ☒ Yes ☐ No

Name \*

Homepage URL

Logo 

AP

Select a file

Application ID

Object ID

User assignment required? ☐ Yes ☒ No

Visible to users ☒ Yes ☐ No

Notes 

Microsoft

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| <div><div></div>Statements</div>             | Yes                   | No                    |
|----------------------------------------------|-----------------------|-----------------------|
| User1 has App1 listed on his My Apps portal. | <input type="radio"/> | <input type="radio"/> |
| User2 has App1 listed on her My Apps portal. | <input type="radio"/> | <input type="radio"/> |
| User3 has App1 listed on her My Apps portal. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                   | Yes                              | No                               |
|----------------------------------------------|----------------------------------|----------------------------------|
| User1 has App1 listed on his My Apps portal. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 has App1 listed on her My Apps portal. | <input type="radio"/>            | <input type="radio"/>            |
| User3 has App1 listed on her My Apps portal. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照 :  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

最新問題: 12

次の表に示すように、East US2 リージョンに 2 つの Azure 仮想マシンがあります。

| Name | Operating system       | Type | Tier     |
|------|------------------------|------|----------|
| VM1  | Windows Server 2008 R2 | A3   | Basic    |
| VM2  | Ubuntu 16.04-DAILY-LTS | L4s  | Standard |

Azure Key Vault をデプロイして構成します。  
VM1 と VM2 で Azure Disk Encryption 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、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

VM1:

The operating system version

The tier

The type

VM2:

The operating system version

The tier

The type

Answer:

VM1:

▼

The operating system version

The tier

The type

VM2:

▼

The operating system version

The tier

The type Microsoft

説明

VM1:

▼

The operating system version

The tier

The type

Microsoft

VM2:

▼

The operating system version

The tier

The type

VM1: 階層

階層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 IaaS VM のディスク暗号化は、Standard VM および Azure Premium Storage を備えた VM のすべての Azure パブリック リージョンと Azure Government リージョン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 IaaS VM 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: Ubuntu 16.04 がサポートされています。

参考文献:

<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](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)

最新問題: 13

必要に応じて、次のログイン資格情報を使用します。

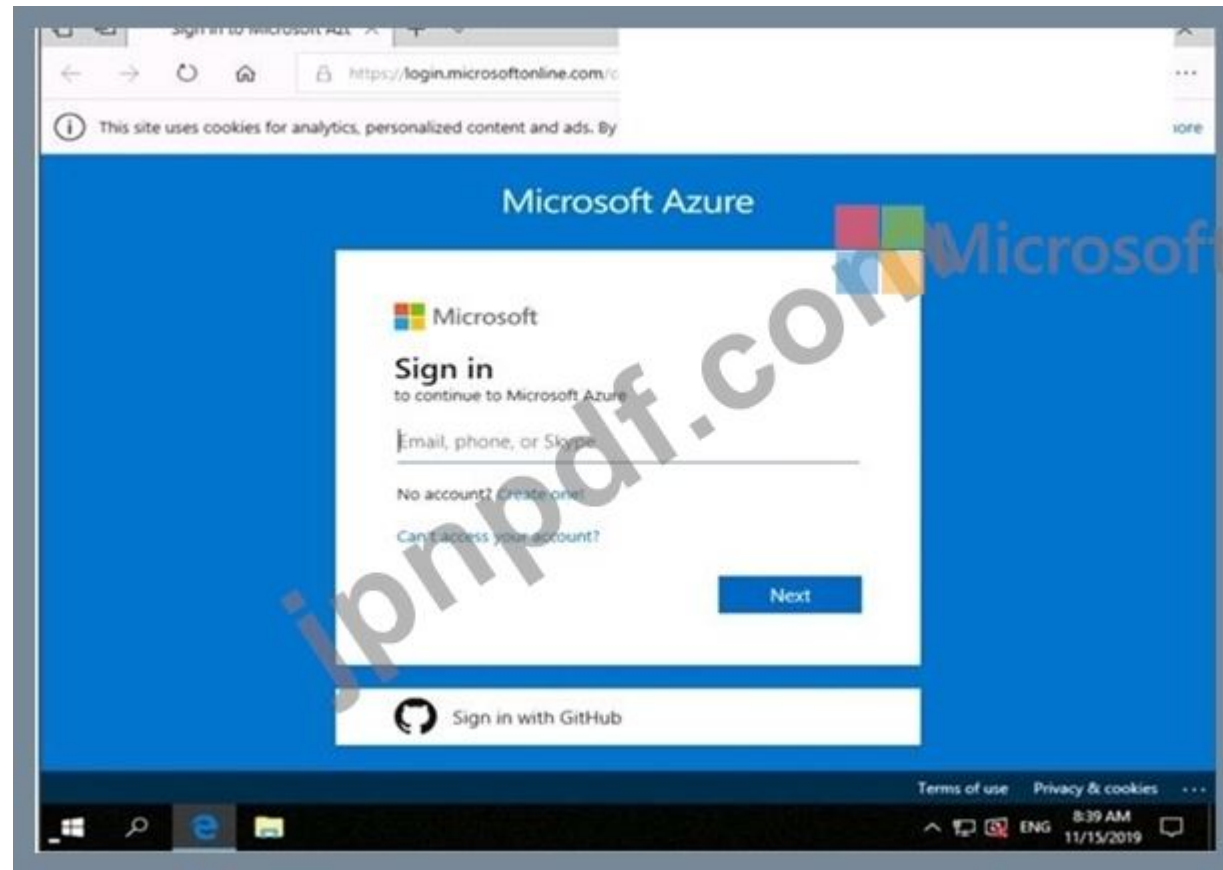
ユーザー名を入力するには、[サインイン] ボックスにカーソルを置き、下のユーザー名をクリックします。  
パスワードを入力するには、「パスワードの入力」ボックスにカーソルを置き、下のパスワードをクリックします。

Azure ユーザー名: User1-10598168@ExamUsers.com

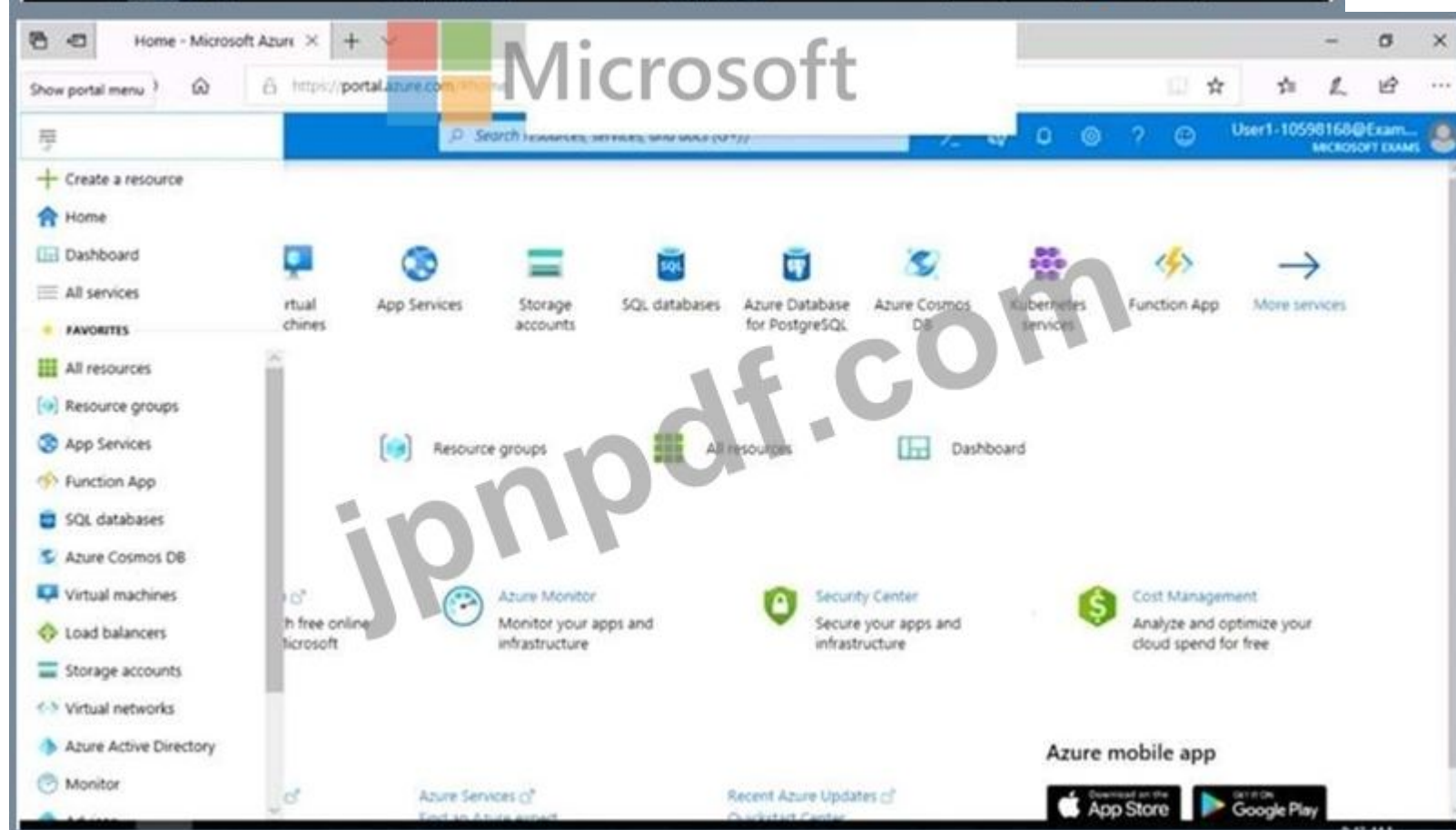
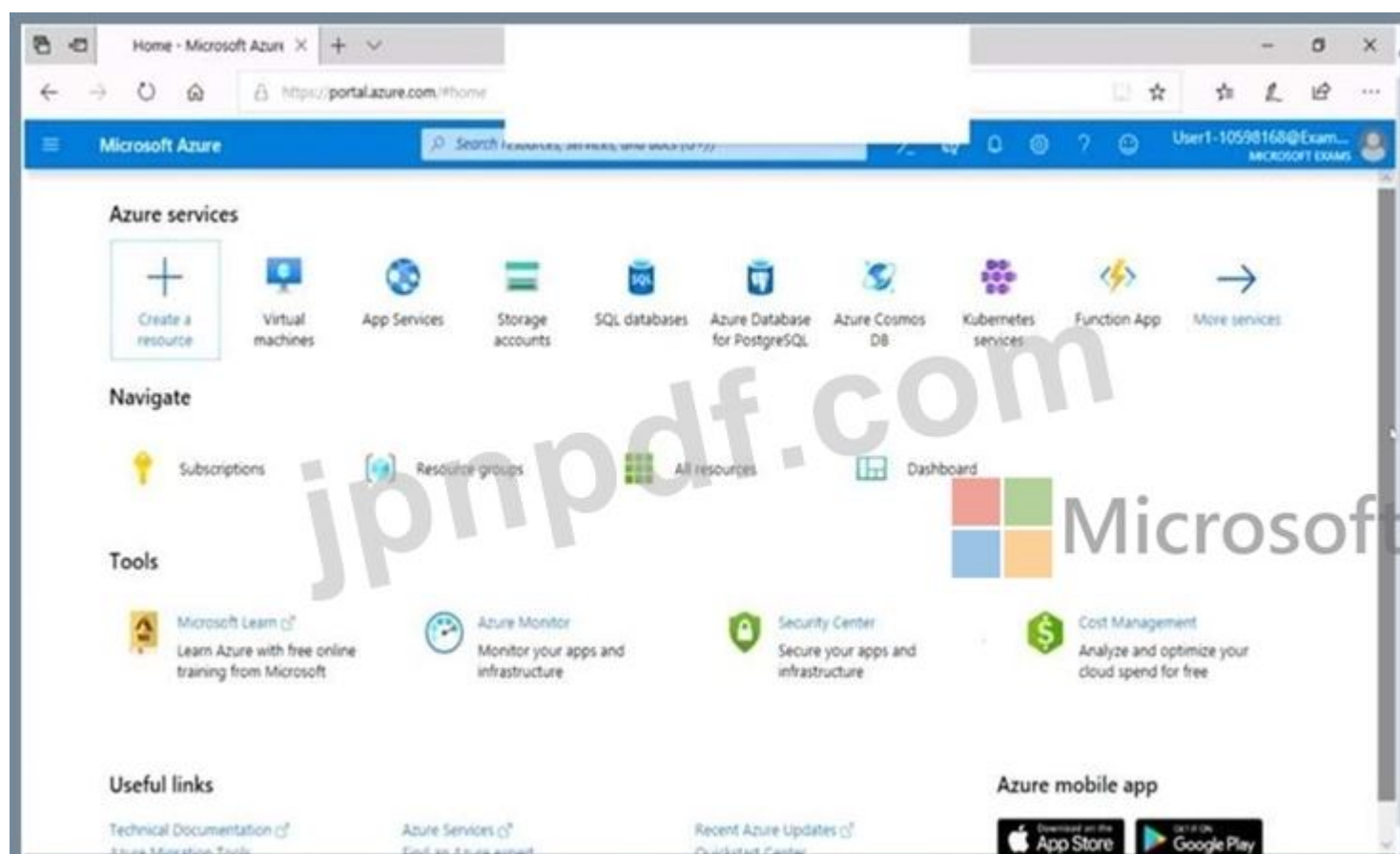
Azure パスワード: Ag1Bh9!#Bd

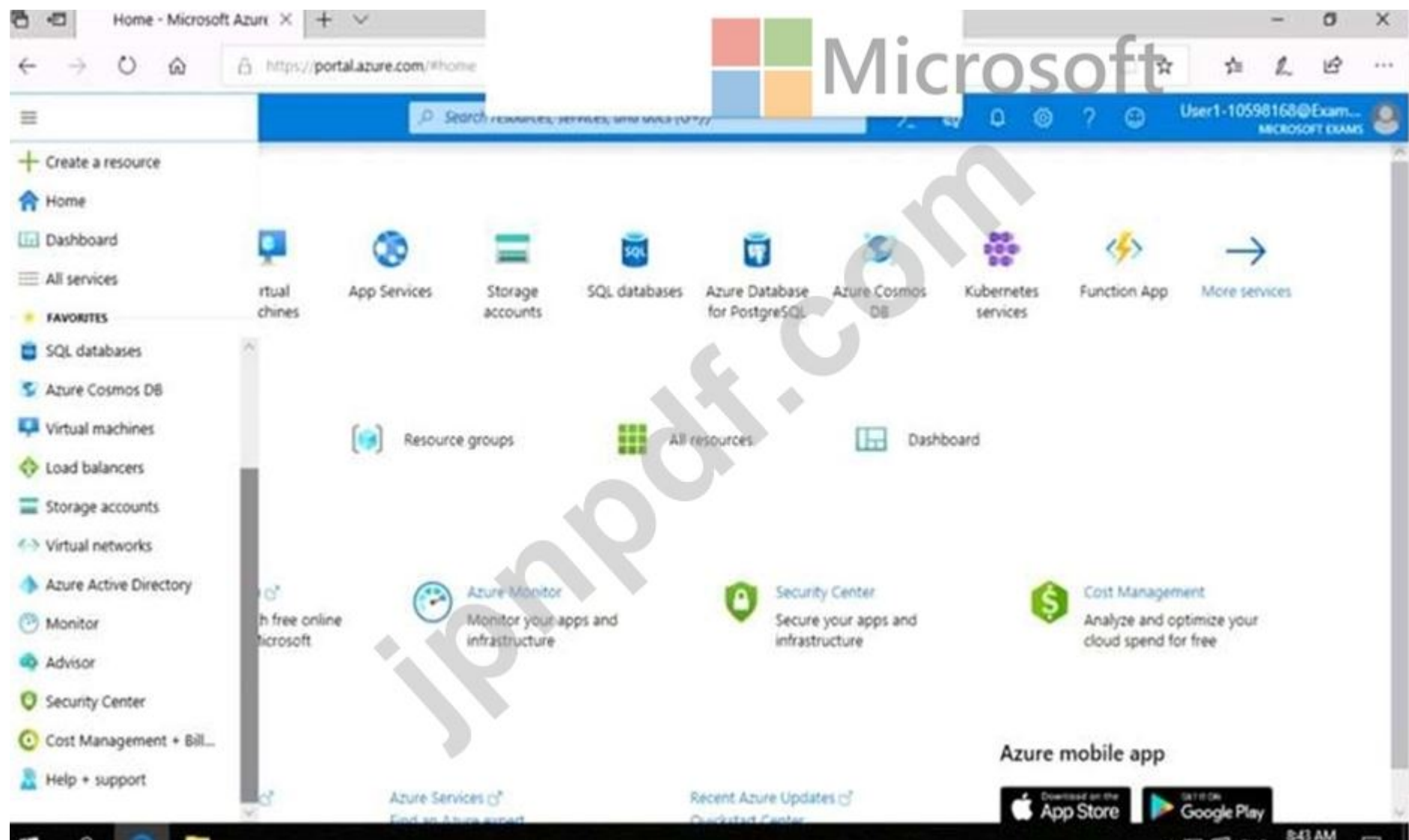
次の情報は、テクニカル サポートのみを目的としています。

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上で毎週日曜日の 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 portal にサインインします。

**Answer:**

単一 VM 展開用の Azure Portal を使用して Microsoft Antimalware Extension を展開する

1. Azure Portal 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。

Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions

# Microsoft

## devrgvm - Extensions

Virtual machine

Search (Ctrl+=/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Disks

Size

Security

Extensions

+ Add

Search to filter items...

| NAME                     | TYPE                              |
|--------------------------|-----------------------------------|
| CustomScriptExtension    | Microsoft.Compute.CustomScriptE   |
| DependencyAgentWindows   | Microsoft.Azure.Monitoring.Deper  |
| enablevmaccess           | Microsoft.Compute.VMAccessAgei    |
| IaaS.Diagnostics         | Microsoft.Azure.Diagnostics.IaaSD |
| MicrosoftMonitoringAgent | Microsoft.EnterpriseCloud.Monitor |
| SiteRecovery-Windows     | Microsoft.Azure.RecoveryServices. |

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。
- スケジュール済み: 有効にする
- スキャンタイプ: フル
- スキャン日: 日曜日

## Install extension



Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ

Enable

Disable

Run a scheduled scan ⓘ

Enable

Disable

Scan type ⓘ

Quick

Full

Scan day ⓘ

Saturday



Scan time ⓘ

120



OK

参照：

<https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/>

#### 最新問題: 14

ユーザーがアクセス権のないリソースにサインインしようとしているのではないかと考えられます。

過去 3 日間に失敗したユーザーのサインイン試行を特定するには、Azure Log Analytics クエリを作成する必要があります。結果には、サインイン試行が 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設定すればよいでしょうか？ 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: 正しく選択するたびに 1 ポイントの価値があります。

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and  ==4625
    ActivityID
    DataType
    EventID
    QuantityUnit

| Summarize failed_login_attempts=
    Count(),
    Countif(),
    Makeset(),
    Split(),

latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

Answer:

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and

```

ActivityID  
 DataType  
 EventID  
 QuantityUnit

==4625

```

| Summarize failed_login_attempts=

```

Count(),  
 Count(),  
 Makeset(),  
 Split(),

```

    latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5

```

参照：

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

#### 最新問題: 15

Azure サブスクリプションをお持ちです。

ストレージ アカウントを作成する予定です。

ストレージ アカウント内のテーブルを暗号化するには、カスタマー マネージド キーを使用する必要があります。

Azure Cloud Shell から、どの 3 つのコマンドレットを順番に実行する必要がありますか？ 回答するには、コマンドレットのリストから適切なコマンドレットを回答領域に移動し、正しい順序で並べます。

**Cmdlets**

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider

**Answer Area**

>
<

^  
v

**Answer:**

Answer Area

New- AzStorageAccount



Microsoft

New- AzStorageAccountKey

New- AzStorageTable

1 - 新しい - AzStorageAccount

2 - 新しい - AzStorageAccountKey

3 - 新しい - AzStorageTable

参照 :

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=powershell>

最新問題: 16

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。

| Name     | Type            |
|----------|-----------------|
| VM1      | Virtual machine |
| VNET1    | Virtual network |
| storage1 | Storage account |
| Vault1   | Key vault       |

<https://www.fast2test.com/AZ-500-practice-test.html> 76

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

サブスクリプションに対して Azure Defender を有効にする予定です。

Azure Defender を使用して保護できるのはどのリソースですか？

A. VM1、VNET1、storage1、および Vault1

B. VM1、VNET1、および storage1 のみ

C. VM1、storage1、および Vault1 のみ

D. VM1 および VNET1 のみ

E. VM1 と storage1 のみ

Answer: [\(解答を表示する\)](#)

説明/参照:

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

<https://www.fast2test.com/AZ-500-practice-test.html> 77

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

データとアプリケーションを保護する

テストレット 1

これはケーススタディです。ケーススタディは個別に時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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、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なら、**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、サンフランシスコ地域に 20 人の従業員を抱え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- である 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 AD Premium P2 ライセンスが割り当てられます。Azure AD Privileged Identity Management (PIM) がアクティブ化されています。

テナントには、次の表に示すグループが含まれています。

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team                                                                              |

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。

<https://www.fast2test.com/AZ-500-practice-test.html> 78

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題



| Name    | Type               | Description                                                                                                                                             |
|---------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| VNet1   | Virtual network    | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0     | Virtual machine    | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.                    |
| VM1     | Virtual machine    | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.                                                                  |
| SQLDB1  | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.                                                                       |
| WebApp1 | Web app            | WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.                                       |
| RG1     | Resource group     | RG1 is a resource group that contains VNet1, VM0, and VM1.                                                                                              |
| RG2     | Resource group     | RG2 is a resource group that contains shared IT resources.                                                                                              |

Azure Security Center は Standard レベル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。

| Name      | Type                           | Description                                                                                                           |
|-----------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Firewall1 | Azure Firewall                 | An Azure firewall on VNet1.                                                                                           |
| RT1       | Route table                    | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1      | Azure Kubernetes Service (AKS) | A managed AKS cluster                                                                                                 |

ID とアクセスの要件

Litware は、次の ID およびアクセス要件を特定します。

- \* すべてのサンフランシスコ 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 のメンバーには、永続的な適格な割り当てを使用して、RG2 への共同作成者ロールを割り当てる必要があります。
- \* ユーザーが 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することを禁止する必要があります。

プラットフォームの保護要件

<https://www.fast2test.com/AZ-500-practice-test.html> 79

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

\* Litware は、次のプラットフォーム保護要件を特定します。

- \* Microsoft Antimalware が RG1 の仮想マシンにインストールされている必要があります。
- \* Group2 のメンバーには、Azure Kubernetes Service Cluster Admin ロールが割り当てられている必要があります。
- \* Azure AD ユーザーは、Azure AD 資格情報を使用して 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 JIT VM アクセスを使用して VM0 に接続できる必要があります。
- \* RG1 のマネージド 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、Azure Security Center でオペレーティング システムのセキュリティ構成をカスタマイズできる必要があります。

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特定します。

- \* Group2 のユーザーは、Azure AD 資格情報を使用して SQLDB1 に対して認証できる必要があります。
- \* WebApp1 は相互認証を強制する必要があります。

一般的な要件

Litware では、次の一般要件が特定されています。

- \* 可能な限り、管理上の労力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。

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> (**51730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 17

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/> | <input type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can connect to the web server on VM4.                | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can connect to the web server on VM4.                | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 18

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 では、次の表に示すアラート ルールを作成します。

| Name  | Resource           | Condition                               |
|-------|--------------------|-----------------------------------------|
| Rule1 | RG1                | All security operations                 |
| Rule2 | RG1                | All administrative operations           |
| Rule3 | Azure subscription | All security operations by Admin1       |
| Rule4 | Azure subscription | All administrative operations by Admin1 |

Admin1 は RG1 で次のアクションを実行します。

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

Admin1 のアクションの結果としてアラートをトリガーするルールはどれですか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Microsoft

Adding VNET1:

▼

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

▼

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

Answer:

Adding VNET1:

▼

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

▼

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

説明



Adding VNET1:

|                                |
|--------------------------------|
| Rule2 only                     |
| Rule4 only                     |
| Rule2 and Rule 4 only          |
| Rule3 and Rule 4 only          |
| Rule1, Rule2, Rule3 and Rule 4 |

Adding Lock1:

|                                |
|--------------------------------|
| Rule2 only                     |
| Rule4 only                     |
| Rule2 and Rule 4 only          |
| Rule3 and Rule 4 only          |
| Rule1, Rule2, Rule3 and Rule 4 |

最新問題: 19

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Sub1 という名前の Azure サブスクリプションがあります。

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

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

権限の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: 20

シングル サインオン (SSO) が有効になっている Azure Active Directory (Azure AD) のハイブリッド構成があります。

Azure AD 認証をサポートするように構成された Azure SQL Database インスタンスがあります。

データベース開発者は、ドメインに参加しているデバイスからデータベース インスタンスに接続し、オンプレミスの Active Directory アカウ

ントを使用して認証する必要があります。  
開発者が Microsoft SQL Server Management Studio を使用してインスタンスに接続できることを確認する必要があります。ソリューションでは、認証プロンプトを最小限に抑える必要があります。  
どの認証方法を推奨しますか？

- A. Active Directory - パスワード
- B. Active Directory - MFA サポートを備えたユニバーサル
- C. SQL サーバー認証
- D. Active Directory - 統合

Answer: D (メッセージを残す)

Active Directory - 統合  
Azure Active Directory 認証は、Azure Active Directory (Azure AD) の ID を使用して Microsoft Azure SQL Database に接続するメカニズムです。フェデレーション ドメインから Azure Active Directory 資格情報を使用して Windows にログインしている場合は、この方法を使用して SQL Database に接続します。

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

最新問題: 21

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 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。  
どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area



Answer:

**Actions**

Configure a network security group (NSG).
Create a network rule collection.
Create a NAT rule collection.
Create a new subnet.
Deploy Azure Application Gateway.
Deploy Azure Firewall.

**Answer Area**

Create a new subnet.
Deploy Azure Firewall.
Create a NAT rule collection.

説明

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

最新問題: 22

Group1 と Group2 のメンバーシップは何ですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Group1:

Microsoft

▼

No members
Only User2
Only User2 and User4
User1, User2, User3, and User4

Group2:

▼

No members
Only User3
Only User1 and User3
User1, User2, User3, and User4

Answer:

Group1: 

No members  
Only User2  
Only User2 and User4  
User1, User2, User3, and User4

Group2: 

No members  
Only User3  
Only User1 and User3  
User1, User2, User3, and User4

Explanation:

ボックス 1: ユーザー 1、ユーザー 2、ユーザー 3、ユーザー 4

文字列および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、ON を含む」はモントリオール (ユーザー 1)、モントリオール (ユーザー 2)、ロンドン (ユーザー 3)、およびオンタリオ (ユーザー 4) に当てはまります。

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。

| Name  | City     | Role                            |
|-------|----------|---------------------------------|
| User1 | Montreal | Global administrator            |
| User2 | MONTREAL | Security administrator          |
| User3 | London   | Privileged role administrator   |
| User4 | Ontario  | Application administrator       |
| User5 | Seattle  | Cloud application administrator |
| User6 | Seattle  | User administrator              |
| User7 | Sydney   | Reports reader                  |
| User8 | Sydney   | None                            |

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。

| Name   | Membership type | Dynamic membership rule  |
|--------|-----------------|--------------------------|
| Group1 | Dynamic user    | user.city -contains "ON" |
| Group2 | Dynamic user    | user.city -match "**on"  |

参考文献:

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

最新問題: 23

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。



| Name      | Region  | Description                                                                                                                                                                           |
|-----------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HubVNet   | East US | HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0. |
| SpokeVNet | East US | SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.                                                        |

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 にデプロイする予定です。

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のルートが含まれます

\* RT2: BGP ルートの伝達を無効にし、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ことを確認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 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります。

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

Answer:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

説明

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

最新問題: 24

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ています。  
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM5. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the private IP address of VM5. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 25

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。

| Name       | Type                          | Region      | Resource group |
|------------|-------------------------------|-------------|----------------|
| SQL1       | Azure SQL database            | East US     | RG1            |
| Analytics1 | Azure Log Analytics workspace | East US     | RG1            |
| Analytics2 | Azure Log Analytics workspace | East US     | RG2            |
| Analytics3 | Azure Log Analytics workspace | West Europe | RG1            |

次の表に示す Azure ストレージ アカウントを作成します。

| Name     | Region      | Resource group | Storage account type | Access tier (default) |
|----------|-------------|----------------|----------------------|-----------------------|
| Storage1 | East US     | RG1            | Blob                 | Cool                  |
| Storage2 | East US     | RG2            | General purpose V1   | Not applicable        |
| Storage3 | West Europe | RG1            | General purpose V2   | Hot                   |

SQL1 の監査を構成する必要があります。

監査ログの保存先として使用できるストレージ アカウントと Log Analytics ワークスペースはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area



Storage accounts that can be used as the audit log destination:

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Answer:  
Answer Area

Storage accounts that can be used as the audit log destination:

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

最新問題: 26

ホットスポット

次の表に示す Azure Key Vault があります。



KV1 には、Secret1 という名前のシークレットと、Key1 という名前のマネージドストレージ アカウントのキーが保存されます。  
Secret1 と Key1 をバックアップします。  
各バックアップをどのキー コンテナーに復元できますか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。  
ホットエリア:



**Answer:**



Explanation:  
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内のキー コンテナーにのみ復元できます。同じ地域内の別のリージョンに復元できません。  
混合質問  
質問セット 1



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

| Name   | Type                   |
|--------|------------------------|
| User1  | User                   |
| User2  | User                   |
| User3  | User                   |
| Group1 | Security group         |
| Group2 | Security group         |
| App1   | Enterprise application |

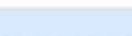
User2 は Group2 の所有者です。

App1 のユーザーとグループの設定は、次のように構成されています。

[+ Add user](#)
[✎ Edit](#)
[🗑 Remove](#)
[🔑 Update Credentials](#)
[☰ Columns](#)
[💡 Got feedback?](#)

📘 The application will appear on the access panel for assigned users. Set "visible to users?" to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

| DISPLAY NAME                                                                                                      | OBJECT TYPE                                                                             | ROLE ASSIGNED  |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/>  Group1 |  Group | Default Access |

Allow users to request access to this application? ⓘ ☒ Yes ☐ No

To which group should assigned users be added? ⓘ

Select group >

Group2

Require approval before granting access to this application? ⓘ ☒ Yes ☐ No

Who is allowed to approve access to this application? ⓘ

Select approvers >

1 users selected

To which role should users be assigned in this application? ⓘ

\*Select a role >

Default Access

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。

何を識別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: 正しく選択するたびに 1 ポイントの価値があります。

Group2 owners:

|                         |
|-------------------------|
| ▼                       |
| User2 only              |
| User3 only              |
| User1 and User2 only    |
| User2 and User3 only    |
| User1, User2, and User3 |

App1 users:

|                                                  |
|--------------------------------------------------|
| ▼                                                |
| Group1 members only                              |
| Group2 members only                              |
| Group1 and Group2 members only                   |
| Group1 and Group2 members and User1 only         |
| Group1 and Group2 members, User1, and User3 only |

Answer:

|                                                  |   |
|--------------------------------------------------|---|
| Group2 owners:                                   | ▼ |
| User2 only                                       |   |
| User3 only                                       |   |
| User1 and User2 only                             |   |
| User2 and User3 only                             |   |
| User1, User2, and User3                          |   |
| App1 users:                                      | ▼ |
| Group1 members only                              |   |
| Group2 members only                              |   |
| Group1 and Group2 members only                   |   |
| Group1 and Group2 members and User1 only         |   |
| Group1 and Group2 members, User1, and User3 only |   |

参照：

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

最新問題: 28

次の表に示すリソースが含まれる Subscription1 という名前の Azure サブスクリプションがあります。

| Name      | Type                            | Description                                                            |
|-----------|---------------------------------|------------------------------------------------------------------------|
| EventHub1 | Azure Event Hubs                | Not applicable                                                         |
| Adf1      | Azure Data Factory              | Not applicable                                                         |
| NVA1      | Network virtual appliance (NVA) | The NVA sends security event messages in the Common Event Format (CEF) |

次のリソースを含む Subscription2 という名前の Azure サブスクリプションがあります。

Azure Sentinel ワークスペース

Azure Event Grid インスタンス

CEF メッセージを NVA から Azure Sentinel に取り込む必要があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Subscription1:

An Azure Log Analytics agent on a Linux virtual machine

A Data Factory pipeline

An Event Hubs namespace

An Azure Service Bus queue

Subscription2:

A new Azure Log Analytics workspace

A new Azure Sentinel data connector

A new Azure Sentinel playbook

A new Event Grid resource provider

Answer:

Answer Area

Subscription1:

An Azure Log Analytics agent on a Linux virtual machine

A Data Factory pipeline

An Event Hubs namespace

An Azure Service Bus queue

Subscription2:

A new Azure Log Analytics workspace

A new Azure Sentinel data connector

A new Azure Sentinel playbook

A new Event Grid resource provider

最新問題: 29

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

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

ポータル ポリシーの条件設定は、条件の説明に示されているように構成されます。( 条件」タブをクリックします。)



Portal Policy

Info

Delete

Name

Portal Policy

Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

1 condition selected

Access controls

Grant

2 controls selected

Session

0 controls selected

Conditions

Info

Device platforms

Not configured

Locations

1 included

Client apps (preview)

Not configured

Device state (preview)

Not configured

Locations

Control user access based on their physical location. [Learn more](#)

Configure

Yes

No

Include

Exclude

Any location

All trusted locations

Selected locations

Select

Contoso

Contoso

...

ポータル ポリシーの付与設定は、「付与」の図に示されているように構成されます。(「付与」タブをクリックします。)

Portal Policy

Info

Delete

Name

Portal Policy

Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

1 condition selected

Access controls

Grant

2 controls selected

Session

0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

See list of approved client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                                                                    | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                                                                    | Yes                   | No                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input checked="" type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input checked="" type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input checked="" type="radio"/> |

参照：

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

最新問題: 30

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 コンテナー
- \* Database1 という名前の Azure SQL データベース
- \* システム割り当てのマネージド ID を使用し、Database1 にアクセスするように構成された AppSrv1 および AppSrv2 という 2 つの Azure App Service Web 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。
- \* Database1 のDiscount という名前の列のデータは、AppSrv1 だけがデータを復号できるように暗号化する必要があります。
- \* AppSrv1 と AppSrv2 は、マネージド ID を使用して暗号化キーを取得することで承認される必要があります。

データベース 1 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: 正しく選択するたびに 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: 31

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Azure サブスクリプションがあります。テナントには、次の表に示すユーザーが含まれます。

| Name  | Subscription role | Azure AD user role    |
|-------|-------------------|-----------------------|
| User1 | Owner             | None                  |
| User2 | Contributor       | None                  |
| User3 | Security Admin    | None                  |
| User4 | None              | Service administrator |

RG1 という名前のリソース グループを作成します。  
どのユーザーが RG1 の権限を変更でき、どのユーザーが RG1 で仮想ネットワークを作成できますか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。



Microsoft

Users who can modify the permissions for RG1:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1, User2 and User3 only    |
| User1, User2, User3, and User4 |

Users who can create virtual networks in RG1:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1, User2 and User3 only    |
| User1, User2, User3, and User4 |

Answer:

Microsoft

Users who can modify the permissions for RG1:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1, User2 and User3 only    |
| User1, User2, User3, and User4 |

Users who can create virtual networks in RG1:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1, User2 and User3 only    |
| User1, User2, User3, and User4 |

説明



Users who can modify the permissions for RG1:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1, User2 and User3 only    |
| User1, User2, User3, and User4 |

Users who can create virtual networks in RG1:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1, User2 and User3 only    |
| User1, User2, User3, and User4 |

ボックス 1: 所有者のみがリソースの権限を変更できます。

ボックス 2: 共同作成者はサブスクリプション内のあらゆるものを作成/変更/削除できますが、権限を変更することはできません。

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> (517**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

#### 最新問題: 32

Azure ストレージ 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 ストレージ エクスプローラー
- 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: A** ([メッセージを残す](#))

セクション: [なし]

Explanation:

メトリクスをダウンロードして長期保存したり、ローカルで分析したりする場合は、ツールを使用するか、テーブルを読み取るコードを作成する必要があります。分析のために分単位のメトリクスをダウンロードする必要があります。ストレージ アカウント内のすべてのテーブル

を一覧表示した場合、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 ブラウズ ツールはこれらのテーブルを認識しているため、これらのテーブルを直接表示できます (利用可能なツールのリストについては、Azure Storage クライアント ツール」を参照してください)。

Microsoft は、Azure Storage アカウント内のデータを操作するためのいくつかのグラフィカル ユーザー インターフェイス (GUI) ツールを提供しています。次の表に示すツールはすべて無料です。

| Azure Storage client tool              | Supported platforms | Block Blob | Page Blob | Append Blob | Tables | Queues | Files |
|----------------------------------------|---------------------|------------|-----------|-------------|--------|--------|-------|
| Azure portal                           | Web                 | Yes        | Yes       | Yes         | Yes    | Yes    | Yes   |
| Azure Storage Explorer                 | Windows, OSX        | Yes        | Yes       | Yes         | Yes    | Yes    | Yes   |
| Microsoft Visual Studio Cloud Explorer | Windows             | Yes        | Yes       | Yes         | Yes    | Yes    | No    |

ノート :

試験ではこの問題にはいくつかのバージョンがあります。試験の問題には 2 つの異なる正解があります。

- 1. Azure ストレージ エクスプローラー
- 2.AZコピー

試験で表示される可能性のあるその他の不正解の選択肢には次のものがあります。

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

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: 33

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。

| Name        | Type                  | Region      |
|-------------|-----------------------|-------------|
| RG1         | Resource group        | West Europe |
| VNET1       | Azure virtual network | West Europe |
| Contoso1901 | Azure Storage account | West Europe |

VNET1 には、Subnet1 と 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、展示に示すように構成されています。( 展示」タブをクリックします。)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass          : Logging, Metrics
DefaultAction    : Deny
IpRules          : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules

Action  IPAddressOrRange
-----  -
Allow   193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action  VirtualNetworkResourceId                                     State
-----  -
Allow   /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\> _
```

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input type="radio"/> | <input type="radio"/> |

Answer:  
説明



| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

ボックス 1: はい

Subnet1からのアクセスは許可されます。

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からのアクセスを許可します。

#### 最新問題: 34

次の表に示すキー コンテナーを含む Azure サブスクリプションがあります。

| Name      | Days to retain deleted vaults | Purge protection | Permission model                             |
|-----------|-------------------------------|------------------|----------------------------------------------|
| KeyVault1 | 10                            | Enabled          | Azure role-based access control (Azure RBAC) |
| KeyVault2 | 15                            | Disabled         | Azure role-based access control (Azure RBAC) |

サブスクリプションには、次の表に示すユーザーが含まれています。

| Name   | Role                      | Assigned to |
|--------|---------------------------|-------------|
| Admin1 | Key Vault Contributor     | KeyVault1   |
| Admin2 | Key Vault Secrets Officer | KeyVault2   |
| Admin3 | Key Vault Administrator   | KeyVault1   |

6 月 1 日に、次のアクションを実行します。

\* KeyVault1 から key1 という名前のキーを削除します。

\* KeyVault2 から Secret 1 という名前のシークレットを削除します。

次の各ステートメントについて、そのステートメントが 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。

| Statements                           | Yes                   | No                    |
|--------------------------------------|-----------------------|-----------------------|
| Admin1 can recover key1 on June 5.   | <input type="radio"/> | <input type="radio"/> |
| Admin2 can purge secret1 on June 12. | <input type="radio"/> | <input type="radio"/> |
| Admin3 can recover key1 on June 17.  | <input type="radio"/> | <input type="radio"/> |



Answer:

| Statements                           | Yes                              | No                               |
|--------------------------------------|----------------------------------|----------------------------------|
| Admin1 can recover key1 on June 5.   | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can purge secret1 on June 12. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin3 can recover key1 on June 17.  | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

はい

はい

いいえ

最新問題: 35

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

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を使用して Azure ロールを保護できることを確認する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                                          | Answer Area |
|------------------------------------------------------------------|-------------|
| Discover privileged roles.                                       |             |
| Sign up PIM for Azure AD roles.                                  |             |
| Consent to PIM.                                                  |             |
| Discover resources.                                              |             |
| Verify your identity by using multi-factor authentication (MFA). |             |

Answer:

Actions

Discover privileged roles.

Sign up PIM for Azure AD roles.

Consent to PIM.

Discover resources.

Verify your identity by using multi-factor authentication (MFA).

Answer Area

Verify your identity by using multi-factor authentication (MFA).

Consent to PIM.

Sign up PIM for Azure AD roles.

- 説明
- 1. MFA で本人確認を行う
  - 2. PIMへの同意
  - 3. AAD ロールの PIM にサインアップする

最新問題: 36

次の表に示すキー コンテナーを含む Azure サブスクリプションがあります。

| Name      | Days to retain deleted vaults | Purge protection | Permission model                             |
|-----------|-------------------------------|------------------|----------------------------------------------|
| KeyVault1 | 10                            | Enabled          | Azure role-based access control (Azure RBAC) |
| KeyVault2 | 15                            | Disabled         | Azure role-based access control (Azure RBAC) |

サブスクリプションには、次の表に示すユーザーが含まれています。

| Name   | Role                      | Assigned to |
|--------|---------------------------|-------------|
| Admin1 | Key Vault Contributor     | KeyVault1   |
| Admin2 | Key Vault Secrets Officer | KeyVault2   |
| Admin3 | Key Vault Administrator   | KeyVault1   |

- 6 月 1 日に、次のアクションを実行します。
- \* KeyVault1 から key1 という名前のキーを削除します。
  - \* KeyVault2 から Secret 1 という名前のシークレットを削除します。
- 次の各ステートメントについて、そのステートメントが 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。

| Statements                           | Yes                   | No                    |
|--------------------------------------|-----------------------|-----------------------|
| Admin1 can recover key1 on June 5.   | <input type="radio"/> | <input type="radio"/> |
| Admin2 can purge secret1 on June 12. | <input type="radio"/> | <input type="radio"/> |
| Admin3 can recover key1 on June 17.  | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                           | Yes                              | No                               |
|--------------------------------------|----------------------------------|----------------------------------|
| Admin1 can recover key1 on June 5.   | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can purge secret1 on June 12. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin3 can recover key1 on June 17.  | <input type="radio"/>            | <input checked="" type="radio"/> |

#### 最新問題: 37

SQL1 という名前の Azure SQL データベースを含む Azure サブスクリプションがあります。

App1 という名前の Web アプリをデプロイする予定です。

App1 に SQL1 への読み取りおよび書き込みアクセスを提供する必要があります。ソリューションは次の要件を満たす必要があります。

パスワードを保存せずに App1 に SQL1 へのアクセスを提供します。

最小特権の原則を使用します。

管理労力を最小限に抑えます。

App1 が SQL1 にアクセスするにはどの種類のアカウントを使用する必要がありますか?また、どのデータベース ロールを App1 に割り当て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: 正しく選択するたびに 1 ポイントの価値があります。

Account type:

Azure Active Directory User

Managed identity

Service Principal

Roles:

db\_datawriter only

db\_datareader and db\_datawriter

db owner only

Answer:

Account type:

Azure Active Directory User

Managed identity

Service Principal

Roles:

db\_datawriter only

db\_datareader and db\_datawriter

db owner only

参照 :

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet>

#### 最新問題: 38

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 と 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、展示に示すように構成されています。(「展示」タブをクリックします。)



```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass          : Logging, Metrics
DefaultAction    : Deny
IpRules          : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules

Action  IPAddressOrRange
-----  -
Allow   193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action  VirtualNetworkResourceId  State
-----  -
Allow   /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\> _
```

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

説明

| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

ボックス 1: はい  
Subnet1からのアクセスは許可されます。  
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からのアクセスを許可します。

最新問題: 39

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

| Name  | Member of      | Mobile phone | Multi-factor authentication (MFA) status |
|-------|----------------|--------------|------------------------------------------|
| User1 | Group1         | 123 555 7890 | Disabled                                 |
| User2 | Group1, Group2 | None         | Enabled                                  |
| User3 | Group1         | 123 555 7891 | Required                                 |

次の設定を持つ Azure AD Identity Protection ユーザー リスク ポリシーを作成して適用します。  
割り当て: グループ 1 を含める、グループ 2 を除外する  
条件: サインインリスクが中以上  
アクセス: アクセスを許可、パスワードの変更が必要  
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                                                      | Yes                   | No                    |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| If User1 signs in from an unfamiliar location, he must change his password.                                                     | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in from an anonymous IP address, she must change her password.                                                   | <input type="radio"/> | <input type="radio"/> |
| If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                                                      | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| If User1 signs in from an unfamiliar location, he must change his password.                                                     | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User2 signs in from an anonymous IP address, she must change her password.                                                   | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照 :

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

最新問題: 40

次の表に示す Azure 仮想マシンがあります。

| Name | Location  | Connected to  |
|------|-----------|---------------|
| VM1  | West US 2 | VNET1/Subnet1 |
| VM2  | West US 2 | VNET1/Subnet1 |
| VM3  | West US 2 | VNET1/Subnet2 |
| VM4  | East US   | VNET2/Subnet3 |
| VM5  | West US 2 | VNET5/Subnet5 |

各仮想マシンには単一のネットワーク インターフェイスがあります。  
VM1 のネットワーク インターフェイスを ASG1 という名前のアプリケーション セキュリティ グループに追加します。  
ASG1 に追加できる仮想マシンのネットワーク インターフェイスを特定する必要があります。  
何を識別する必要がありますか？

- A. VM2、VM3、VM5 のみ
- B. VM2 のみ
- C. VM2、VM3、VM4、VM5
- D. Vm2、Vm3のみ

Answer: D (メッセージを残す)

最新問題: 41



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。RG1 には、Azure Active Directory (Azure AD) 認証を使用する VM1 という名前の仮想マシンが含まれています。

スコープが RG1 である、Role1 と Role2 という名前の 2 つのカスタム Azure ロールがあります。

Role1 の権限は、次の JSON コードに示されています。

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [],
    "notDataActions": []
  }
]
```

Role2 の権限は、次の JSON コードに示されています。

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

次の表に示すユーザーにロールを割り当てます。

| Name  | Role         |
|-------|--------------|
| User1 | Role1        |
| User2 | Role1, Role2 |
| User3 | Role1, Role2 |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

| Statements                                              | Yes                   | No                    |
|---------------------------------------------------------|-----------------------|-----------------------|
| User1 can delete VM1.                                   | <input type="radio"/> | <input type="radio"/> |
| User2 can delete VM1.                                   | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in to VM1 by using Azure AD credentials. | <input type="radio"/> | <input type="radio"/> |

Answer:



Answer Area

| Statements                                              | Yes                              | No                               |
|---------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can delete VM1.                                   | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can delete VM1.                                   | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can sign in to VM1 by using Azure AD credentials. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 42

ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。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 Azure Active Directory (Azure AD) テナントにリンクされた Azure サブスクリプションがあります。テナントには、storage1 という名前の Azure ストレージ 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。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                                                     | Answer Area |
|-----------------------------------------------------------------------------|-------------|
| Create a private link to storage1.                                          |             |
| Enable Active Directory Domain Services (AD DS) authentication on storage1. |             |
| Implement Azure AD Connect.                                                 |             |
| Create a service endpoint to storage1.                                      |             |
| Assign share-level permissions for share1.                                  |             |

Answer:

**Actions**

- Create a private link to storage1.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Implement Azure AD Connect.
- Create a service endpoint to storage1.
- Assign share-level permissions for share1.

**Answer Area**

- Implement Azure AD Connect.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Assign share-level permissions for share1.

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

**最新問題: 43**

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。

| Name        | Type                  | Region      |
|-------------|-----------------------|-------------|
| RG1         | Resource group        | West Europe |
| VNET1       | Azure virtual network | West Europe |
| Contoso1901 | Azure Storage account | West Europe |

VNET1 には、Subnet1 と 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、展示に示すように構成されています。(「展示」タブをクリックします。)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass          : Logging, Metrics
DefaultAction   : Deny
IpRules         : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules

Action  IPAddressOrRange
-----  -
Allow   193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action  VirtualNetworkResourceId                                     State
-----  -
Allow   /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\> _
```

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input type="radio"/> | <input type="radio"/> |

Answer:



| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

説明

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input type="radio"/> | <input type="radio"/> |

ボックス 1: はい  
Subnet1からのアクセスは許可されます。  
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からのアクセスを許可します。

最新問題: 44

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 ルールに設定されたアクション 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  
フィルタ条件: リソース タイプ = "仮想マシン"  
このスコープで定義: 抑制  
抑制設定: これから (常に)  
名前: アクションルール1  
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                      | Yes                   | No                    |
|-------------------------------------------------|-----------------------|-----------------------|
| If you start VM1, an alert is triggered.        | <input type="radio"/> | <input type="radio"/> |
| If you start VM2, an alert is triggered.        | <input type="radio"/> | <input type="radio"/> |
| If you add a tag to RG1, an alert is triggered. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                      | Yes                              | No                               |
|-------------------------------------------------|----------------------------------|----------------------------------|
| If you start VM1, an alert is triggered.        | <input type="radio"/>            | <input checked="" type="radio"/> |
| If you start VM2, an alert is triggered.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| If you add a tag to RG1, an alert is triggered. | <input type="radio"/>            | <input checked="" type="radio"/> |

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: 45

Azure AD 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 ポータルでは何を使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

To configure the registration settings:

|                                         |   |
|-----------------------------------------|---|
|                                         | ▼ |
| Azure AD – User settings                |   |
| Azure AD – App registrations settings   |   |
| Enterprise Applications – User settings |   |

To configure the consent settings:

|                                         |   |
|-----------------------------------------|---|
|                                         | ▼ |
| Azure AD – User settings                |   |
| Azure AD – App registrations settings   |   |
| Enterprise Applications – User settings |   |

Answer:

|                                         |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---|--------------------------|--|---------------------------------------|--|-----------------------------------------|--|
| To configure the registration settings: | <table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Azure AD – User settings</td></tr><tr><td colspan="2">Azure AD – App registrations settings</td></tr><tr><td colspan="2">Enterprise Applications – User settings</td></tr></table> |  | ▼ | Azure AD – User settings |  | Azure AD – App registrations settings |  | Enterprise Applications – User settings |  |
|                                         | ▼                                                                                                                                                                                                                                                    |  |   |                          |  |                                       |  |                                         |  |
| Azure AD – User settings                |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |
| Azure AD – App registrations settings   |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |
| Enterprise Applications – User settings |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |
| To configure the consent settings:      | <table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Azure AD – User settings</td></tr><tr><td colspan="2">Azure AD – App registrations settings</td></tr><tr><td colspan="2">Enterprise Applications – User settings</td></tr></table> |  | ▼ | Azure AD – User settings |  | Azure AD – App registrations settings |  | Enterprise Applications – User settings |  |
|                                         | ▼                                                                                                                                                                                                                                                    |  |   |                          |  |                                       |  |                                         |  |
| Azure AD – User settings                |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |
| Azure AD – App registrations settings   |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |
| Enterprise Applications – User settings |                                                                                                                                                                                                                                                      |  |   |                          |  |                                       |  |                                         |  |

最新問題: 46

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 ルールに設定されたアクション 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。

\* 範囲: VM1

\* フィルタ条件: リソース タイプ = "仮想マシン"

\* このスコープで定義: 抑制

※ 抑制設定 :これから (常時)

\* 名前: アクションルール 1

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                      | Yes                              | No                    |
|-------------------------------------------------|----------------------------------|-----------------------|
| If you start VM1, an alert is triggered.        | <input checked="" type="radio"/> | <input type="radio"/> |
| If you start VM2, an alert is triggered.        | <input type="radio"/>            | <input type="radio"/> |
| If you add a tag to RG1, an alert is triggered. | <input type="radio"/>            | <input type="radio"/> |

Answer:

| Statements                                      | Yes                              | No                               |
|-------------------------------------------------|----------------------------------|----------------------------------|
| If you start VM1, an alert is triggered.        | <input type="radio"/>            | <input checked="" type="radio"/> |
| If you start VM2, an alert is triggered.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| If you add a tag to RG1, an alert is triggered. | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

| Statements                                      | Yes                              | No                               |
|-------------------------------------------------|----------------------------------|----------------------------------|
| If you start VM1, an alert is triggered.        | <input type="radio"/>            | <input checked="" type="radio"/> |
| If you start VM2, an alert is triggered.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| If you add a tag to RG1, an alert is triggered. | <input type="radio"/>            | <input checked="" type="radio"/> |

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ます。

ボックス 2:

アクション ルールのスコープは 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。

参考文献:  
<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>

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> (517**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 47  
次の表に示すように、East US2 リージョンに 2 つの Azure 仮想マシンがあります。  
Azure Key Vault をデプロイして構成します。  
VM1 と VM2 で Azure Disk Encryption 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、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

VM1:

▼

The operating system version

The tier

The type

VM2:

▼

The operating system version

The tier

The type

Answer:



VM1:  ▼

|                              |
|------------------------------|
| The operating system version |
| The tier                     |
| The type                     |

VM2:  ▼

|                              |
|------------------------------|
| The operating system version |
| The tier                     |
| The type                     |

Explanation:

VM1: 階層

階層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 IaaS VM のディスク暗号化は、Standard VM および Azure Premium Storage を備えた VM のすべての Azure パブリック リージョンと Azure Government リージョン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 IaaS VM 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: Ubuntu 16.04 がサポートされています。

参考文献:

<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](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)

最新問題: 48

Group1 と Group2 のメンバーシップは何ですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Group1:  Microsoft ▼

|                                |
|--------------------------------|
| No members                     |
| Only User2                     |
| Only User2 and User4           |
| User1, User2, User3, and User4 |

Group2: ▼

|                                |
|--------------------------------|
| No members                     |
| Only User3                     |
| Only User1 and User3           |
| User1, User2, User3, and User4 |

Answer:

Group1:  Microsoft ▼

|                                |
|--------------------------------|
| No members                     |
| Only User2                     |
| Only User2 and User4           |
| User1, User2, User3, and User4 |

Group2: ▼

|                                |
|--------------------------------|
| No members                     |
| Only User3                     |
| Only User1 and User3           |
| User1, User2, User3, and User4 |

参照：

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

#### 最新問題: 49

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ています。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

### Answer Area

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the public IP address of VM5.  | <input type="radio"/> | <input type="radio"/> |

Answer:

### Answer Area

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the public IP address of VM5.  | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the public IP address of VM5.  | <input type="radio"/>            | <input checked="" type="radio"/> |

ボックス 1: はい

NSG1 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG2 has the inbound security rules shown in the following table.

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | 80   | TCP      | Internet          | VirtualNetwork | Allow  |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

ボックス 2: はい

ボックス 3: いいえ

ノート :

Sub2 には、次の表に示す仮想マシンが含まれています。

| Name | Network interface | Application security group | Connected to |
|------|-------------------|----------------------------|--------------|
| VM1  | NIC1              | ASG1                       | Subnet1.1    |
| VM2  | NIC2              | ASG2                       | Subnet1.1    |
| VM3  | NIC3              | None                       | Subnet1.2    |
| VM4  | NIC4              | ASG1                       | Subnet1.3    |
| VM5  | NIC5              | None                       | Subnet2.1    |

| Name      | Subnet                             |
|-----------|------------------------------------|
| VNetwork1 | Subnet1.1, Subnet1.2 and Subnet1.3 |
| VNetwork2 | Subnet2.1                          |

Sub2 contains the network security groups (NSGs) shown in the following table.

| Name | Associated to |
|------|---------------|
| NSG1 | NIC2          |
| NSG2 | Subnet1.1     |
| NSG3 | Subnet1.3     |
| NSG4 | Subnet2.1     |

最新問題: 50

条件付きアクセス ポリシーを実装しています。

ポリシーを構成して実装するには、既存の Azure Active Directory (Azure AD) 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。

認証情報が漏洩したユーザー

特殊な場所への旅行は不可能



不審なアクティビティのある IP アドレスからのサインイン  
各リスクイベントについて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: 正しく選択するたびに 1 ポイントの価値があります。

| Levels | Answer Area                                                               |
|--------|---------------------------------------------------------------------------|
| High   | Impossible travel to atypical locations: <input type="text"/>             |
| Low    | Users with leaked credentials: <input type="text"/>                       |
| Medium | Sign ins from IP addresses with suspicious activity: <input type="text"/> |

Answer:

| Levels | Answer Area                                          | Microsoft |
|--------|------------------------------------------------------|-----------|
| High   | Impossible travel to atypical locations:             | Medium    |
| Low    | Users with leaked credentials:                       | High      |
| Medium | Sign ins from IP addresses with suspicious activity: | Medium    |

- 最新問題: 51
- VM1 という名前の Azure 仮想マシンがあります。
- Azure Security Center から、仮想マシンにエンドポイント保護ソリューションをインストールする」という重要度の高い推奨事項が表示されます。
- 重大度の高い推奨事項の原因となっている問題を解決する必要があります。
- あなたは何をすべきか？
- A. Microsoft マルウェア対策拡張機能を VM1 に追加します。
  - B. VM1 に Endpoint Protection 用の Microsoft System Center Security Management Pack をインストールします。
  - C. Windows 拡張機能用 Network Watcher Agent を VM1 に追加します。
  - D. VM1 を Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) にオンボードします。

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/security-center/security-center-endpoint-protection>

最新問題: 52

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。

| Name | Operating system        |
|------|-------------------------|
| VM1  | Windows Server 2016     |
| VM2  | Ubuntu Server 18.04 LTS |

Azure Security Center から、自動プロビジョニングを有効にします。

次の表に示す仮想マシンをデプロイします。

| Name | Operating system        |
|------|-------------------------|
| VM3  | Windows Server 2016     |
| VM4  | Ubuntu Server 18.04 LTS |

Microsoft 監視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 と VM3 のみ
- C. VM3 および VM4 のみ
- D. VM1、VM2、VM3、および VM4

Answer: D ([メッセージを残す](#))

セクション: [なし]

Explanation:

自動プロビジョニングが有効になっている場合、Security Center は、サポートされているすべての Azure VM および作成された新しい VM に Microsoft Monitoring Agent をプロビジョニングします。

サポートされているオペレーティング システムには、Ubuntu 14.04 LTS (x86/x64)、16.04 LTS (x86/x64)、および 18.04 LTS (x64)、および Windows Server 2008 R2、2012、2012 R2、2016、バージョン 1709 および 1803 が含まれます。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-faq> 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時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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る場合があります。このケーススタディに関する各質問は、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、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に関する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、サンフランシスコ地域に 20 人の従業員を抱えるデジタル 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- である 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 AD Premium P2 ライセンスが割り当てられます。Azure AD Privileged Identity Management (PIM) がアクティブ化されています。

テナントには、次の表に示すグループが含まれています。

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team                                                                              |

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。

| Name            | Type               | Description                                                                                                                                             |
|-----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| VNet1           | Virtual network    | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0             | Virtual machine    | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.                    |
| VM1             | Virtual machine    | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.                                                                  |
| SQLDB1          | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.                                                                       |
| WebApp1         | Web app            | WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.                                           |
| Resource Group1 | Resource group     | Resource Group1 is a resource group that contains VNet1, VM0, and VM1.                                                                                  |
| Resource Group2 | Resource group     | Resource Group2 is a resource group that contains shared IT resources.                                                                                  |

Azure Security Center は無料レベル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。

| Name      | Type                           | Description                                                                                                           |
|-----------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Firewall1 | Azure Firewall                 | An Azure firewall on VNet1.                                                                                           |
| RT1       | Route table                    | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1      | Azure Kubernetes Service (AKS) | A managed AKS cluster                                                                                                 |

## ID とアクセスの要件

Litware は、次の ID およびアクセス要件を特定します。

- \* すべてのサンフランシスコ 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 のメンバーには、永続的な適格な割り当てを使用して、リソース グループ 2 への共同作成者ロールを割り当てる必要があります。
- \* ユーザーが 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することを禁止する必要があります。

## プラットフォームの保護要件

Litware は、次のプラットフォーム保護要件を特定します。

- \* Microsoft Antimalware は、リソース グループ 1 の仮想マシンにインストールする必要があります。
- \* Group2 のメンバーには、Azure Kubernetes Service Cluster Admin ロールが割り当てられている必要があります。
- \* Azure AD ユーザーは、Azure AD 資格情報を使用して 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 JIT VM アクセスを使用して VM0 に接続できる必要があります。
- \* Resource Group1 のマネージド 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。役割 1 は、リソース グループ 1 に対して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、Azure Security Center でオペレーティング システムのセキュリティ構成をカスタマイズできる必要があります。

## 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特定します。

- \* Group2 のユーザーは、Azure AD 資格情報を使用して SQLDB1 に対して認証できる必要があります。
- \* WebApp1 は相互認証を強制する必要があります。

## 一般的な要件

Litware では、次の一般要件が特定されています。

- \* 可能な限り、管理上の労力を最小限に抑える必要があります。
- \* 可能な限り、自動化の使用を最小限に抑える必要があります。

## 最新問題: 53

Group1 と Group2 のメンバーシップは何ですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Group1:  Microsoft ▼

|                                |
|--------------------------------|
| No members                     |
| Only User2                     |
| Only User2 and User4           |
| User1, User2, User3, and User4 |

Group2: ▼

|                                |
|--------------------------------|
| No members                     |
| Only User3                     |
| Only User1 and User3           |
| User1, User2, User3, and User4 |

Answer:

Group1: ▼

|                                |
|--------------------------------|
| No members                     |
| Only User2                     |
| Only User2 and User4           |
| User1, User2, User3, and User4 |

Group2: ▼

|                                |
|--------------------------------|
| No members                     |
| Only User3                     |
| Only User1 and User3           |
| User1, User2, User3, and User4 |

参照 :

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

最新問題: 54

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。

| Name    | Type                         | Attached to    | NSG            |
|---------|------------------------------|----------------|----------------|
| NSG1    | Network security group (NSG) | VM5            | Not applicable |
| NSG2    | Network security group (NSG) | Subnet1        | Not applicable |
| Subnet1 | Subnet                       | Not applicable | Not applicable |
| VM5     | Virtual machine              | Subnet1        | NSG1           |

IP アドレス 10.1.0.4 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。

### JIT VM access configuration

VM5

+ Add   Save   Discard

Configure the ports for which the just-in-time VM access will be applicable

| Port | Protocol | Allowed source IPs | IP range | Time range (hours) |
|------|----------|--------------------|----------|--------------------|
| 3389 | Any      | Per request        | N/A      | 3 hours            |

VM5 の JIT VM アクセスを有効にします。  
NSG1 には、次の図に示す受信ルールがあります。

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action |
|----------|-------------------------------|------|----------|-------------------|----------------|--------|
| 100      | SecurityCenter-JITRule-...    | 3389 | Any      | Any               | 10.1.0.4       | Allow  |
| 1000     | SecurityCenter-JITRule_341... | 3389 | Any      | Any               | 10.1.0.4       | Deny   |
| 1001     | RDP                           | 3389 | TCP      | Any               | Any            | Allow  |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | AllowAzureLoadBalancerIn...   | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | Deny   |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                         | Yes                   | No                    |
|----------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input type="radio"/> | <input type="radio"/> |
| Remote Desktop access to VM5 is blocked.                                                           | <input type="radio"/> | <input type="radio"/> |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.                  | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                         | Yes                                 | No                                  |
|----------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| Remote Desktop access to VM5 is blocked.                                                           | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.                  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

最新問題: 55

ユーザーがアクセス権のないリソースにサインインしようとしているのではないかと考えられます。  
過去 3 日間に失敗したユーザーのサインイン試行を特定するには、Azure Log Analytics クエリを作成する必要があります。結果には、サインイン試行が 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設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and 

▼ ==4625
  ActivityID
  DataType
  EventID
  QuantityUnit


| Summarize failed_login_attempts=

▼
  Count(),
  Countif(),
  Makeset(),
  Split(),


latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

Answer:



Microsoft

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
| Summarize failed_login_attempts=
latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

▼ ==4625

ActivityID  
Data Type  
EventID  
QuantityUnit

▼

Count(),  
Countif(),  
Makeset(),  
Split(),

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

最新問題: 56

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。)

|                             |                            |
|-----------------------------|----------------------------|
| BASICS                      |                            |
| Subscription                | Microsoft Azure Sponsorshi |
| Resource group              | AzureBackupRG_eastus2_     |
| Region                      | East US                    |
| Kubernetes cluster name     | akscluster2                |
| Kubernetes version          | 1.1 1.5                    |
| DNS name prefix             | akscluster2                |
| Node count                  | 3                          |
| Node size                   | Standard_DS2_v2            |
| Virtual nodes (preview)     | Disabled                   |
| AUTHENTICATION              |                            |
| Enable RBAC                 | No                         |
| NETWORKING                  |                            |
| HTTP application routing    | Yes                        |
| Network configuration       | Basic                      |
| MONITORING                  |                            |
| Enable container monitoring | No                         |
| TAGS                        |                            |

クラスターを実稼働環境にデプロイする予定です。HTTP アプリケーション ルーティングを無効にします。  
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 終端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。  
あなたは何をすべきか？  
A. AKS Ingress 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 Standard Load Balancer を作成します。
- D. Azure 基本ロード バランサーを作成します。

Answer: A ([メッセージを残す](#))

説明

イングレス コントローラーは、Kubernetes サービスにリバース プロキシ、構成可能なトラフィック ルーティング、TLS 終端を提供するソフトウェアです。

参考文献:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

最新問題: 57

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

| Name  | Member of      | Multi-factor authentication (MFA) status |
|-------|----------------|------------------------------------------|
| User1 | Group1, Group2 | Enabled                                  |
| User2 | Group1         | Disabled                                 |
| User3 | Group1         | Disabled                                 |

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

割り当て: Group1 を含め、Group2 を除外

条件: サインインのリスク レベル: 中以上

アクセス アクセスを許可、多要素認証が必要

ユーザーが Azure AD にサインインするときに何が起こるかを特定する必要があります。

各ユーザーについて何を識別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: 正しく選択するたびに 1 ポイントの価値があります。

When User1 signs in from an anonymous IP address, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

Answer:

When User1 signs in from an anonymous IP address, the user will:



▼

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

▼

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

▼

Be blocked

Be prompted for MFA

Sign in by using a username and password only

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: 58

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が含まれる Storage1 という名前の Azure ストレージ アカウントがあります。

| Name       | Type           |
|------------|----------------|
| Container1 | Blob container |
| Share1     | File share     |

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 と Share1 のコンテンツにアクセスするにはどのツールを使用できますか? SAS を使用することで? 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Tools for Container1:

Robocopy.exe

Azure Storage Explorer

File Explorer

Tools for Share1:



Robocopy.exe

Azure Storage Explorer

File Explorer

Answer:

Answer Area



最新問題: 59

10317806.onmicrosoft.com という名前の新しい Azure Active Directory (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 user10317806 という名前のユーザーが含まれている必要があります。

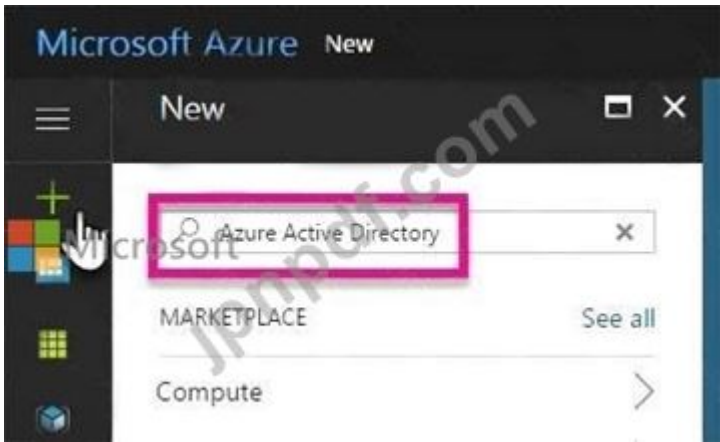
Answer:

以下の説明を参照してください。

説明

新しい Azure AD テナントを作成するには:

1. Azure portal にアクセスし、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、次の項目を検索します。



3. Azure Active Directory」を選択します。



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

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

Create directory

\* Organization name ⓘ  
Contoso Direct ✓  
Microsoft

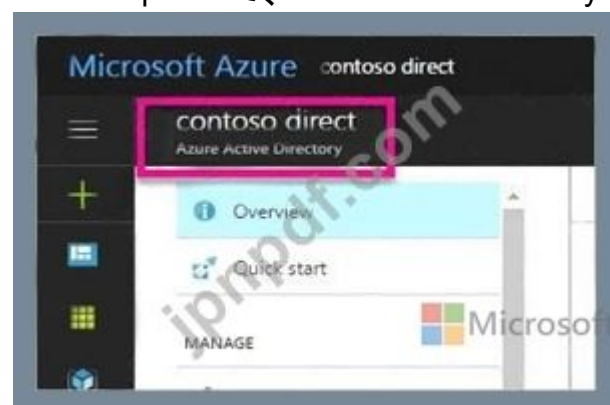
\* Initial domain name ⓘ  
contosodirect ✓  
contosodirect.onmicrosoft.com

Country or region ⓘ  
United States ▼

Directory creation will take about one minute.

6. ディレクトリの作成が完了したら、新しいディレクトリを管理するための情報ボックスを選択します。  
ユーザーを作成するには:

1. Azure portal で、Azure Active Directory フライアウトにいることを確認します。

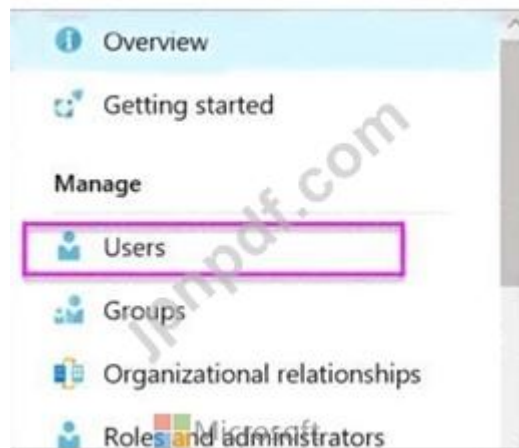


そうでない場合は、左側のサービス ナビゲーションから Azure Active Directory アイコンを選択します。



2. 管理」で ユーザー」を選択します。



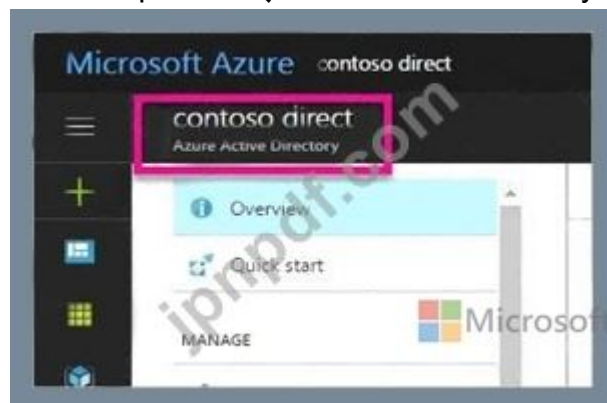


3. [すべてのユーザー] を選択し、

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

MFA を有効にするには:

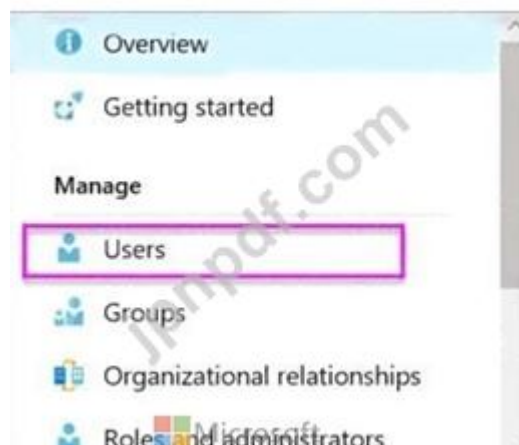
1. Azure portal で、Azure Active Directory フライアウトにいることを確認します。



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



2. [管理] で [ユーザー] を選択します。



3. [多要素認証] をクリックします。

4. ユーザー名の横にあるチェックボックスをオンにして、  
参照：  
<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

最新問題: 60

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、仮想マシンへの PowerShell アクセスをユーザーに許可する必要があります。  
何を設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

Microsoft

Permission that must be granted to users on VM:

Read

Update

View

Write

TCP port that must be allowed:

22

25

3389

5986

Answer:

Answer Area

Microsoft

Permission that must be granted to users on VM:

Read

Update

View

Write

TCP port that must be allowed:

22

25

3389

5986

説明

Permission that must be granted to users on VM:

|        |   |
|--------|---|
|        | ▼ |
| Read   |   |
| Update |   |
| View   |   |
| Write  |   |

TCP port that must be allowed:

|      |   |
|------|---|
|      | ▼ |
| 22   |   |
| 25   |   |
| 3389 |   |
| 5986 |   |

Microsoft

#### 最新問題: 61

ユーザーがアクセス権のないリソースにサインインしようとしているのではないかと考えられます。

過去 3 日間に失敗したユーザーのサインイン試行を特定するには、Azure Log Analytics クエリを作成する必要があります。結果には、サインイン試行が 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設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

Microsoft

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
```

|              |   |
|--------------|---|
|              | ▼ |
| ActivityID   |   |
| DataType     |   |
| EventID      |   |
| QuantityUnit |   |

==4625

```
| Summarize failed_login_attempts=
```

|            |   |
|------------|---|
|            | ▼ |
| Count(),   |   |
| Countif(), |   |
| Makeset(), |   |
| Split(),   |   |

```
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

Answer:

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and

```

▼ ==4625

|              |
|--------------|
| ActivityID   |
| DataType     |
| EventID      |
| QuantityUnit |

```

| Summarize failed_login_attempts=

```

▼

|            |
|------------|
| Count(),   |
| Countif(), |
| Makeset(), |
| Split(),   |

```

latest_failed_login=arg_max(TimeGenerated by Account
where failed_login_attempts > 5

```

説明

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and

```

▼ ==4625

|              |
|--------------|
| ActivityID   |
| DataType     |
| EventID      |
| QuantityUnit |

```

| Summarize failed_login_attempts=

```

▼

|            |
|------------|
| Count(),   |
| Countif(), |
| Makeset(), |
| Split(),   |

```

latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5

```

次の例では、過去 1 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。  
タイムフレーム = 1d とします。

セキュリティイベント

| 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

| アカウント別の failed\_login\_attempts=count()、latest\_failed\_login=arg\_max(TimeGenerated, Account) の要約

| ここで、failed\_login\_attempts > 5

| プロジェクトアウェイアカウント1

参考文献:

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



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> (**51730%OFF**問題集溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: 62

## Basics

|                         |                          |
|-------------------------|--------------------------|
| Subscription            | Azure Pass - Sponsorship |
| Resource group          | RG1                      |
| Region                  | (US) East US             |
| Kubernetes cluster name | AKScluster               |
| Kubernetes version      | 1.12.8                   |
| DNS name prefix         | AKScluster               |
| Node count              | 3                        |
| Node size               | Standard_DS2_v2          |

るように構成されています。



|                         |          |
|-------------------------|----------|
| Virtual nodes           | Disabled |
| VM scale sets (preview) | Disabled |

## Authentication

|             |    |
|-------------|----|
| Enable RBAC | No |
|-------------|----|

## Networking

|                          |       |
|--------------------------|-------|
| HTTP application routing | No    |
| Network configuration    | Basic |

## Monitoring

|                             |    |
|-----------------------------|----|
| Enable container monitoring | No |
|-----------------------------|----|

## Tags

(none)

クラスターを実稼働環境にデプロイする予定です。HTTP アプリケーション ルーティングを無効にします。

AKS サービスにリバース プロキシと TLS 終端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。

<https://www.fast2test.com/AZ-500-practice-test.html> 48

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

単一の IP アドレスを使用して。

あなたは何をすべきか？

- A. AKS Ingress 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 Standard Load Balancer を作成します。
- D. Azure 基本ロード バランサーを作成します。

Answer: (解答を表示する)

イングレス コントローラーは、Kubernetes サービスにリバース プロキシ、構成可能なトラフィック ルーティング、TLS 終端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: 63

次の表に示すように、East US2 リージョンに 2 つの Azure 仮想マシンがあります。

| Name | Operating system       | Type | Tier     |
|------|------------------------|------|----------|
| VM1  | Windows Server 2008 R2 | A3   | Basic    |
| VM2  | Ubuntu 16.04-DAILY-LTS | L4s  | Standard |

Azure Key Vault をデプロイして構成します。

VM1 と VM2 で Azure Disk Encryption 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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

VM1:

▼

The operating system version

The tier

The type

VM2:

▼

The operating system version

The tier

The type

Answer:

VM1:

▼

The operating system version

The tier

The type

VM2:

▼

The operating system version

The tier

The type

説明

VM1:

▼

The operating system version

The tier

The type

Microsoft

VM2:

▼

The operating system version

The tier

The type

VM1: 階層

階層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 IaaS VM のディスク暗号化は、Standard VM および Azure Premium Storage を備えた VM のすべての Azure パブリック リージョンと Azure Government リージョン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 IaaS VM 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: Ubuntu 16.04 がサポートされています。

参考文献:

<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](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)



最新問題: 64

次の表に示す Azure 仮想マシンがあります。

| Name | Operating system             | Region      | Resource group |
|------|------------------------------|-------------|----------------|
| VM1  | Windows Server 2012          | East US     | RG1            |
| VM2  | Windows Server 2012 R2       | West Europe | RG1            |
| VM3  | Windows Server 2016          | West Europe | RG2            |
| VM4  | Red Hat Enterprise Linux 7.4 | East US     | RG2            |

米国東部リージョンの RG1 に Analytics1 という名前の Azure Log Analytics ワークスペースを作成します。

どの仮想マシンを Analytics1 に登録できますか？

- A. VM1のみ
- B. VM1、VM2、VM3 のみ
- C. VM1、VM2、VM3、VM4
- D. VM1 と VM4 のみ

Answer: (解答を表示する)

注: ワークスペースを作成する

Azure portal で、[すべてのサービス] をクリックします。リソースのリストに [Log Analytics] 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ー処理されます。[ログ分析] を選択します。

[作成] をクリックし、次の項目の選択肢を選択します。

新しい Log Analytics ワークスペースの名前を指定します (DefaultLAWorkspace など)。OMS ワークスペースは、Log Analytics ワークスペースと呼ばれるようになりました。

選択されているデフォルトが適切でない場合は、ドロップダウン リストから選択してリンク先のサブスクリプションを選択します。

[リソース グループ] には、1 つ以上の Azure 仮想マシンを含む既存のリソース グループを選択します。

VM がデプロイされる場所を選択します。詳細については、Log Analytics が利用できるリージョンを参照してください。

不正解:

B、C: Log Analytics ワークスペースは、データ ストレージの地理的な場所を提供します。VM2 と VM3 は別の場所にあります。

D: VM4 は別のリソース グループです。

参照 :

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

最新問題: 65

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

| Name  | Role                  |
|-------|-----------------------|
| User1 | Global administrator  |
| User2 | Billing administrator |
| User3 | Owner                 |
| User4 | Account Admin         |

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ますか?そのユーザーはどのツールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

User:

|       |   |
|-------|---|
|       | ▼ |
| User1 |   |
| User2 |   |
| User3 |   |
| User4 |   |

Tool:

|                       |   |
|-----------------------|---|
|                       | ▼ |
| Azure Account Center  |   |
| Azure Cloud Shell     |   |
| Azure PowerShell      |   |
| Azure Security Center |   |

Answer:

User:

|       |   |
|-------|---|
|       | ▼ |
| User1 |   |
| User2 |   |
| User3 |   |
| User4 |   |

Tool:

|                       |   |
|-----------------------|---|
|                       | ▼ |
| Azure Account Center  |   |
| Azure Cloud Shell     |   |
| Azure PowerShell      |   |
| Azure Security Center |   |

参照 :

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

最新問題: 66

単一のネットワーク セキュリティ グループ (NSG) を持つ単一のサブネット上に 10 台の仮想マシンがあります。  
ネットワーク トラフィックを Azure ストレージ アカウントに記録する必要があります。  
どの 2 つのアクションを実行する必要がありますか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 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. Azure Network Watcher 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. Azure Log Analytics ワークスペースを作成します。

Answer: B,D (メッセージを残す)

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) への受信トラフィックと仮想マシンからの送信トラフィックをフィルターできます。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。手順には次のものが含まれます。

- \* 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、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 ログを有効にする
- \* ログデータをダウンロード
- \* ログデータの表示

参照：

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

最新問題: 67

Microsoft Defender for Cloud を使用する Azure サブスクリプションがあります。

Azure CIS 1.4,0 標準への法規制への準拠を確認するには、Defender for Cloud を使用する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。

まず何をすべきでしょうか？

- A. Azure ポリシーを割り当てます。
- B. すぐに使える標準の 1 つを無効にします。
- C. Azure CIS 1.4.0 標準を手動で追加します。
- D. カスタム イニシアチブを追加します。

Answer: (解答を表示する)

最新問題: 68

Update Management 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。

| Name | Operating system             | Region  | Resource group |
|------|------------------------------|---------|----------------|
| VM1  | Windows Server 2012          | East US | RG1            |
| VM2  | Windows Server 2012 R2       | West US | RG1            |
| VM3  | Windows Server 2016          | West US | RG2            |
| VM4  | Ubuntu Server 18.04 LTS      | West US | RG2            |
| VM5  | Red Hat Enterprise Linux 7.4 | East US | RG1            |
| VM6  | CentOS 7.5                   | East US | RG1            |

Update1 と Update2 という名前の 2 つの更新プログラムの展開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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Update1:

▼

VM2 only

VM4 only

VM1 and VM2 only

VM1, VM2, VM4, VM5, and VM6

Update2:

▼

VM5 only

VM1 and VM5 only

VM4 and VM5 only

VM1, VM2, and VM5 only

VM1, VM2, VM3, VM4, and VM5

Answer:

Update1:

▼

VM2 only

VM4 only

VM1 and VM2 only

VM1, VM2, VM4, VM5, and VM6

Update2:

▼

VM5 only

VM1 and VM5 only

VM4 and VM5 only

VM1, VM2, and VM5 only

VM1, VM2, VM3, VM4, and VM5

参考文献:  
<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>



Azure サブスクリプションで Azure Kubernetes Service (AKS) クラスターを作成する予定です。

<https://www.fast2test.com/AZ-500-practice-test.html> 54

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

登録されたサーバー アプリケーションのマニフェストを次の図に示します。

The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: [Understanding the Azure Active Directory application manifest](#).

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```



AKS クラスターと Azure Active Directory (Azure AD) が統合されていることを確認する必要があります。

マニフェスト内のどのプロパティを変更する必要がありますか？

A. accessTokenAcceptedVersion

B. keyCredentials

C. groupMembershipClaims

D. acceptMappedClaims

**Answer: C (メッセージを残す)**

説明/参照:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

<https://www.fast2test.com/AZ-500-practice-test.html> 55

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

セキュリティ運用を管理する

テストレット 1

これはケーススタディです。ケーススタディは個別に時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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、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、サンフランシスコ地域に 20 人の従業員を抱えるデジタル 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- である 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 AD Premium P2 ライセンスが割り当てられます。Azure AD Privileged Identity Management (PIM) がアクティブ化されています。

テナントには、次の表に示すグループが含まれています。

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team                                                                              |

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。

<https://www.fast2test.com/AZ-500-practice-test.html> 56

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

| Name    | Type               | Description                                                                                                                                             |
|---------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| VNet1   | Virtual network    | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0     | Virtual machine    | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.                    |
| VM1     | Virtual machine    | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.                                                                  |
| SQLDB1  | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.                                                                       |
| WebApp1 | Web app            | WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.                                       |
| RG1     | Resource group     | RG1 is a resource group that contains VNet1, VM0, and VM1.                                                                                              |
| RG2     | Resource group     | RG2 is a resource group that contains shared IT resources.                                                                                              |

Azure Security Center は Standard レベル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。

| Name      | Type                           | Description                                                                                                           |
|-----------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Firewall1 | Azure Firewall                 | An Azure firewall on VNet1.                                                                                           |
| RT1       | Route table                    | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1      | Azure Kubernetes Service (AKS) | A managed AKS cluster                                                                                                 |

ID とアクセスの要件

Litware は、次の ID およびアクセス要件を特定します。

- \* すべてのサンフランシスコ 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 のメンバーには、永続的な適格な割り当てを使用して、RG2 への共同作成者ロールを割り当てる必要があります。
- \* ユーザーが 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することを禁止する必要があります。

プラットフォームの保護要件

<https://www.fast2test.com/AZ-500-practice-test.html> 57

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

Litware は、次のプラットフォーム保護要件を特定します。

- \* Microsoft Antimalware が RG1 の仮想マシンにインストールされている必要があります。
- \* Group2 のメンバーには、Azure Kubernetes Service Cluster Admin ロールが割り当てられている必要があります。



- \* Azure AD ユーザーは、Azure AD 資格情報を使用して 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 JIT VM アクセスを使用して VM0 に接続できる必要があります。
- \* RG1 のマネージド 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、Azure Security Center でオペレーティング システムのセキュリティ構成をカスタマイズできる必要があります。

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特定します。

- \* Group2 のユーザーは、Azure AD 資格情報を使用して SQLDB1 に対して認証できる必要があります。
- \* WebApp1 は相互認証を強制する必要があります。

一般的な要件

Litware では、次の一般要件が特定されています。

- \* 可能な限り、管理上の労力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: 70

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ています。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM5. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the private IP address of VM5. | <input checked="" type="radio"/> | <input type="radio"/>            |

説明

Q1: いいえ {「インターネット」サービス タグからは TCP 80 のみが許可されているため、許可されるべきではありません。Q2: はい {プライベート IP 上で相互に ping を実行し、NSG が構成されていない同じローカル サブネット内の VM ではそうすべきであるため} Q3 : はい {VM5 は、NSG の最初のルールによって任意の送信元から宛先へのトラフィックが許可されるサブネットにあります}



最新問題: 71

LAW1 という名前の Azure Log Analytics ワークスペースを含む Sub1 という名前の Azure サブスクリプションがあります。  
Windows Server 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。  
システム更新評価ソリューションを LAW1 に追加する予定です。  
システム更新評価関連のログが 100 台の仮想マシンのみから LAW1 にアップロードされるようにする必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                        | Answer Area |
|------------------------------------------------|-------------|
| Create a new workspace.                        |             |
| Apply the scope configuration to the solution. |             |
| Create a scope configuration.                  |             |
| Create a computer group.                       |             |
| Create a data source.                          |             |

Answer:

| Actions                                        | Answer Area                                    |
|------------------------------------------------|------------------------------------------------|
| Create a new workspace.                        | Create a computer group.                       |
| Apply the scope configuration to the solution. | Create a scope configuration.                  |
| Create a scope configuration.                  | Apply the scope configuration to the solution. |
| Create a computer group.                       |                                                |
| Create a data source.                          |                                                |

参考文献:

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

最新問題: 72

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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Virtual networks that User2 can modify:

Microsoft

▼

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

Virtual networks that User2 can delete:

▼

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

Answer:

Virtual networks that User2 can modify:

Microsoft

▼

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

Virtual networks that User2 can delete:

▼

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

Virtual networks that User2 can modify:

Microsoft

VNET4 only  
VNET4 and VNET1 only  
VNET4, VNET3, and VNET1 only  
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only  
VNET4 and VNET1 only  
VNET4, VNET3, and VNET1 only  
VNET4, VNET3, VNET2, and VNET1

ボックス 1: VNET4 と VNET1 のみ  
RG1 には削除ロックのみがありますが、RG4 にはロックがありません。  
RG2 と RG3 は両方とも読み取り専用ロックを持っています。

ボックス 2: VNET4 のみ  
RG4 にはロックがありませんが、他のリソース グループには削除ロックまたは読み取り専用ロックが設定されています。

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および読み取り専用と呼ばれます。

\* CanNotDelete は、許可されたユーザーがリソースの読み取りと変更はできるが、リソースを削除できないことを意味します。

\* ReadOnly は、承認されたユーザーがリソースを読み取ることはできますが、リソースを削除または更新することは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、承認されたすべてのユーザーを閲覧者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と似ています。

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。

| Name  | Resource group |
|-------|----------------|
| VNET1 | RG1            |
| VNET2 | RG2            |
| VNET3 | RG3            |
| VNET4 | RG4            |

Sub1 には、次の表に示すロックが含まれています。

参考文献:

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

最新問題: 73

storage1 という名前の Azure ストレージ 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 マネージド ディスクがあります。



VM1 に対して Azure Disk Encryption を有効にする必要があります。

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

**Actions**

Run the Set-AzVMDiskEncryptionExtension cmdlet.

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment.**

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption.**

Generate a key vault certificate.

Create an Azure key vault.

Configure storage1 to use a customer-managed key.

**Answer Area**

Answer:

**Actions**

Run the Set-AzVMDiskEncryptionExtension cmdlet.

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment.**

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption.**

Generate a key vault certificate.

Create an Azure key vault.

Configure storage1 to use a customer-managed key.

**Answer Area**

Create an Azure key vault.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption.**

Run the Set-AzVMDiskEncryptionExtension cmdlet.

参照：

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

最新問題: 74

プラットフォームの保護要件を満たすには、Microsoft マルウェア対策を導入する必要があります。

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

注: 正しく選択するたびに 1 ポイントの価値があります。



Create a custom policy definition that has effect set to:

Append  
Deny  
DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting  
The exclusion settings  
The scope

Answer:

Create RG2:

Admin3 only  
Admin2 and Admin3 only  
Admin3 and Admin4 only  
Admin2, Admin3, and Admin4 only  
Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:

Admin4 only  
Admin1 and Admin4 only  
Admin2 and Admin3 only  
Admin1, Admin2, and Admin4 only  
Admin1, Admin2, Admin3, and Admin4

- 説明
- 1.存在しない場合のデプロイ
  - 2. 範囲

最新問題: 75

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ています。  
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Answer Area                                                        |                       |                       |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| Statements                                                         | Yes                   | No                    |
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the public IP address of VM5.  | <input type="radio"/> | <input type="radio"/> |

Answer:

| Answer Area                                                        |                                  |                                  |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| Statements                                                         | Yes                              | No                               |
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the public IP address of VM5.  | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 76

LAW1 という名前の Azure Log Analytics ワークスペースを含む Sub1 という名前の Azure サブスクリプションがあります。  
Windows Server 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。  
システム更新評価ソリューションを LAW1 に追加する予定です。  
システム更新評価関連のログが 100 台の仮想マシンのみから LAW1 にアップロードされるようにする必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                                                                                                            | Answer Area |
|------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Create a new workspace.                                                                                                            |             |
|  Apply the scope configuration to the solution. |             |
| Create a scope configuration.                                                                                                      |             |
| Create a computer group.                                                                                                           |             |
| Create a data source.                                                                                                              |             |

Answer:

Actions

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

Answer Area

Create a computer group.

Create a scope configuration.

Apply the scope configuration to the solution.

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

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> (517**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 77  
次の表に示す Azure Information Protection 条件があります。

| Name       | Pattern | Case sensitivity |
|------------|---------|------------------|
| Condition1 | White   | On               |
| Condition2 | Black   | Off              |

You have the Azure Information Protection labels shown in the following table.

| Name    | Applies to     | Use label | Set the default label |
|---------|----------------|-----------|-----------------------|
| Global  | Not applicable | None      | None                  |
| Policy1 | User1          | Label1    | None                  |
| Policy2 | User2          | Label2    | None                  |

Azure Information Protection がファイルにどのようにラベルを付けるかを特定する必要があります。  
何を識別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: 正しく選択するたびに 1 ポイントの価値があります。



If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

|                   |   |
|-------------------|---|
|                   | ▼ |
| No label          |   |
| Label1 only       |   |
| Label2 only       |   |
| Label1 and Label2 |   |

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

|                   |   |
|-------------------|---|
|                   | ▼ |
| No label          |   |
| Label1 only       |   |
| Label2 only       |   |
| Label1 and Label2 |   |

Answer:

|                                                                                                                      |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---|----------|--|-------------|--|-------------|--|-------------------|--|
| <p>If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:</p>   | <table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">No label</td></tr><tr><td colspan="2">Label1 only</td></tr><tr><td colspan="2">Label2 only</td></tr><tr><td colspan="2">Label1 and Label2</td></tr></table> |  | ▼ | No label |  | Label1 only |  | Label2 only |  | Label1 and Label2 |  |
|                                                                                                                      | ▼                                                                                                                                                                                                                             |  |   |          |  |             |  |             |  |                   |  |
| No label                                                                                                             |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| Label1 only                                                                                                          |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| Label2 only                                                                                                          |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| Label1 and Label2                                                                                                    |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| <p>If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:</p> | <table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">No label</td></tr><tr><td colspan="2">Label1 only</td></tr><tr><td colspan="2">Label2 only</td></tr><tr><td colspan="2">Label1 and Label2</td></tr></table> |  | ▼ | No label |  | Label1 only |  | Label2 only |  | Label1 and Label2 |  |
|                                                                                                                      | ▼                                                                                                                                                                                                                             |  |   |          |  |             |  |             |  |                   |  |
| No label                                                                                                             |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| Label1 only                                                                                                          |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| Label2 only                                                                                                          |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |
| Label1 and Label2                                                                                                    |                                                                                                                                                                                                                               |  |   |          |  |             |  |             |  |                   |  |

Explanation:

ボックス 1: ラベル 2 のみ

複数の条件が複数のラベルに適用される場合の評価方法 ラベルは、ポリシーで指定した位置に従って評価の順序付けされます。最初に配置されたラベルの位置が最も低く (機密性が最も低い)、最後に配置されたラベルの位置が最も低くなります。最も高い位置 (最も感度が高い)。最も機密性の高いラベルが適用されます。

最後のサブラベルが適用されます。

ボックス 2: ラベルなし

自動分類は、ドキュメントの保存時に Word、Excel、PowerPoint に適用され、電子メールの送信時に Outlook に適用されます。自動分類は Microsoft メモ帳には適用されません。

参考文献:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

最新問題: 78

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



まず。オフィスは次の表に示す IP アドレスを使用します。

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Seattle  | 10.10.0.0/16     | 190.15.1.0/24      |
| New York | 172.16.0.0/16    | 194.25.2.0/24      |

この会社には、contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。テナントには、次の表に示すユーザーが含まれます。

| Name  | Multi-factor authentication (MFA) status |
|-------|------------------------------------------|
| User1 | Enabled                                  |
| User2 | Enforced                                 |

MFA サービス設定は、図に示す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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

|                                                                                                                                       | Yes                   | No                    |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/> | <input type="radio"/> |

Answer:

|                                                                                                                                       | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

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

#### 最新問題: 79

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ています。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Answer Area                                                        |                       |                       |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| Statements                                                         | Yes                   | No                    |
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the public IP address of VM5.  | <input type="radio"/> | <input type="radio"/> |

Answer:

| Answer Area                                                        |                                  |                                  |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| Statements                                                         | Yes                              | No                               |
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the public IP address of VM5.  | <input checked="" type="radio"/> | <input type="radio"/>            |

#### 最新問題: 80

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が含まれる Group1 という名前の Azure Active Directory (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、再起動できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Answer:

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

参照：  
<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

最新問題: 81

次のデータ コネクタを備えた Azure Sentinel ワークスペースがあります。

Azure Active Directory ID 保護

コモンイベントフォーマット(CEF)

Azure ファイアウォール

データが各コネクタから取り込まれていることを確認する必要があります。

[ログ クエリ] ウィンドウから、各コネクタに対してどのテーブルをクエリ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: 正しく選択するたびに 1 ポイントの価値があります。

Azure Active Directory Identity Protection Microsoft

Azure Firewall:

CEF:

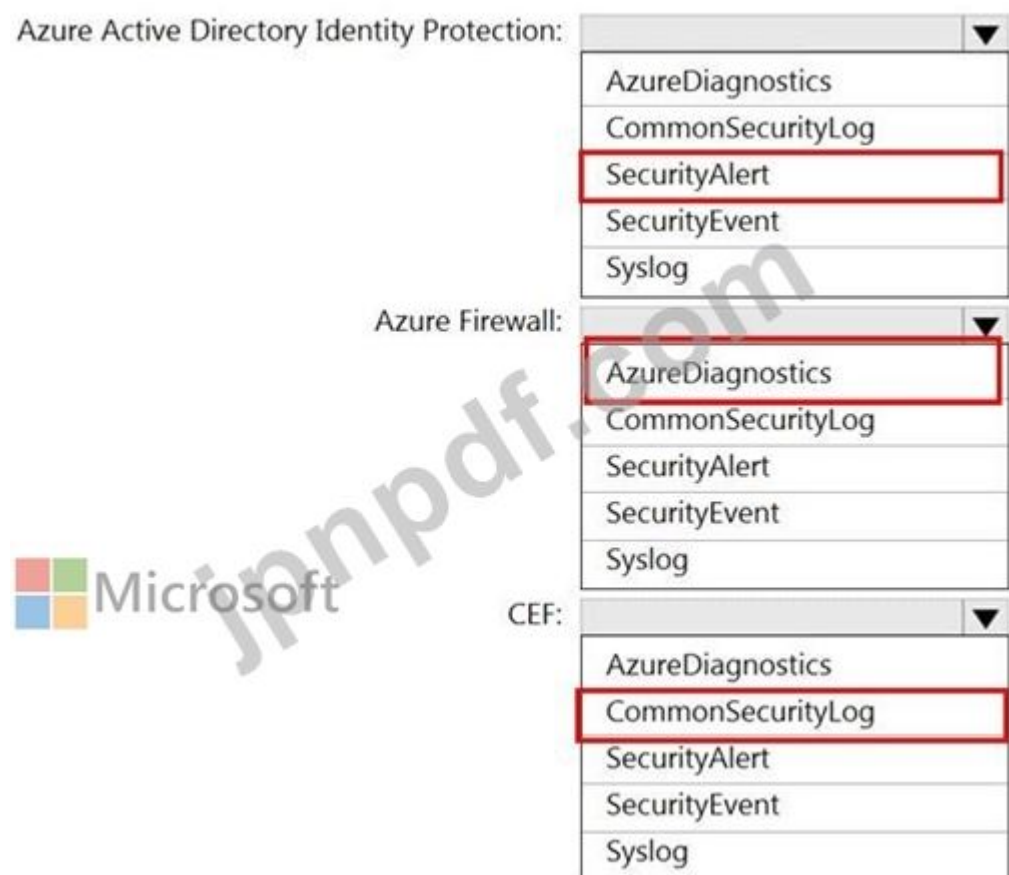
|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

Answer:





#### 最新問題: 82

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、Subnet1 という名前の 1 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が含まれています。

Subnet1 のサービス エンドポイントを作成します。

Subnet1 には、Ubuntu Server 18.04 を実行する VM1 という名前の Azure 仮想マシンが含まれています。

Docker コンテナを VM1 にデプロイする必要があります。コンテナは、サービス エンドポイントを使用して Azure Storage リソースと Azure SQL データベースにアクセスする必要があります。

**A.** アプリケーション セキュリティ グループとネットワーク セキュリティ グループ (NSG) を作成します。

**B.** docker-compose.yml ファイルを編集します。

**C.** 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。

**Answer: C** ([メッセージを残す](#))

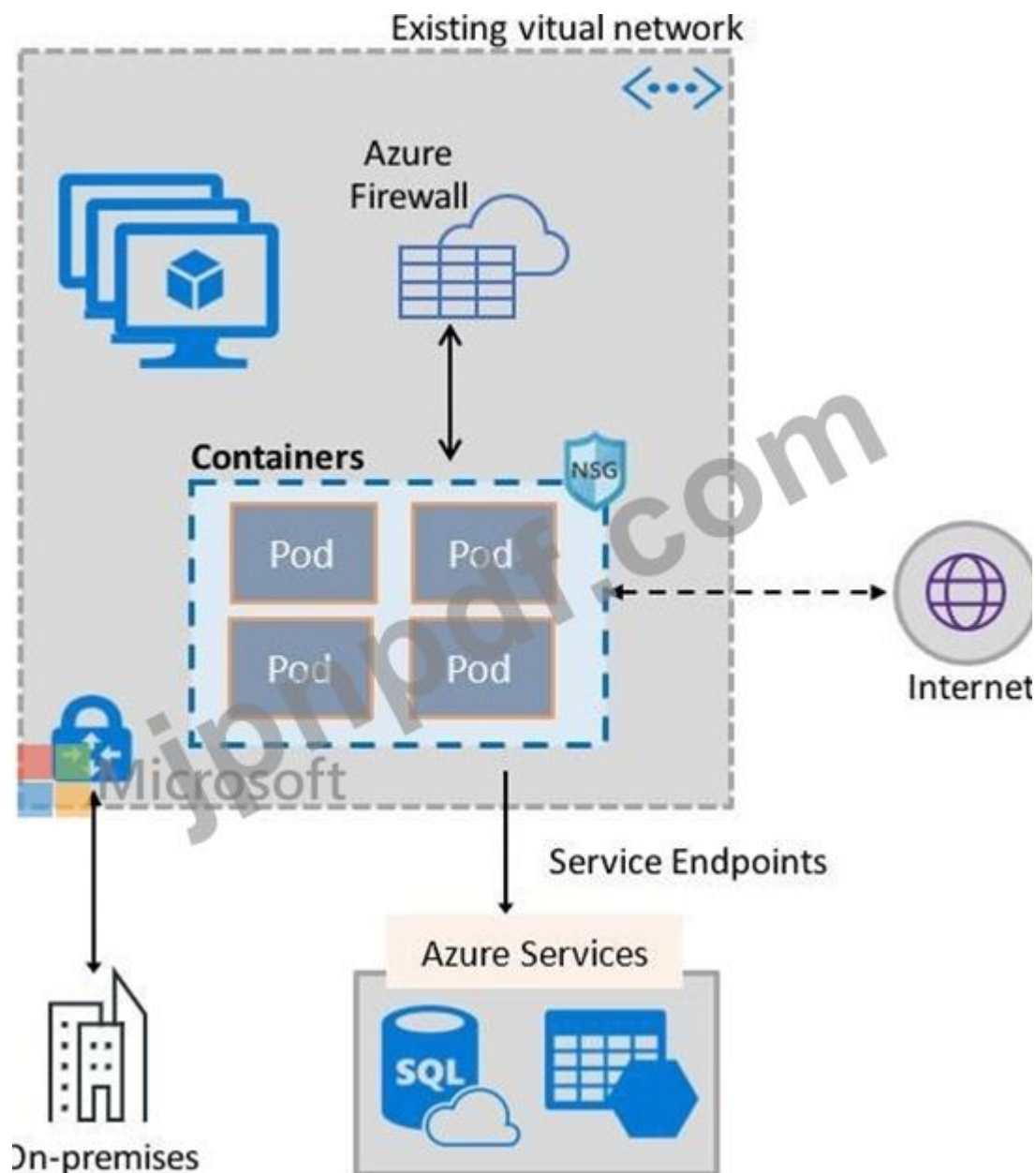
#### 説明

Azure Virtual Network コンテナ ネットワーク インターフェイス (CNI) プラグインは、Azure 仮想マシンにインストールされます。

このプラグインは、Linux と Windows の両方のプラットフォームをサポートします。

プラグインは、仮想ネットワークから仮想マシン内で起動されたコンテナに IP アドレスを割り当て、コンテナを仮想ネットワークに接続し、他のコンテナや仮想ネットワーク リソースに直接接続します。このプラグインは、接続のためにオーバーレイ ネットワークやルートに依存せず、仮想マシンと同じパフォーマンスを提供します。

次の図は、プラグインが Azure 仮想ネットワーク機能をポッドに提供する方法を示しています。



On-premises

参考文献:

<https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview>

最新問題: 83

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。

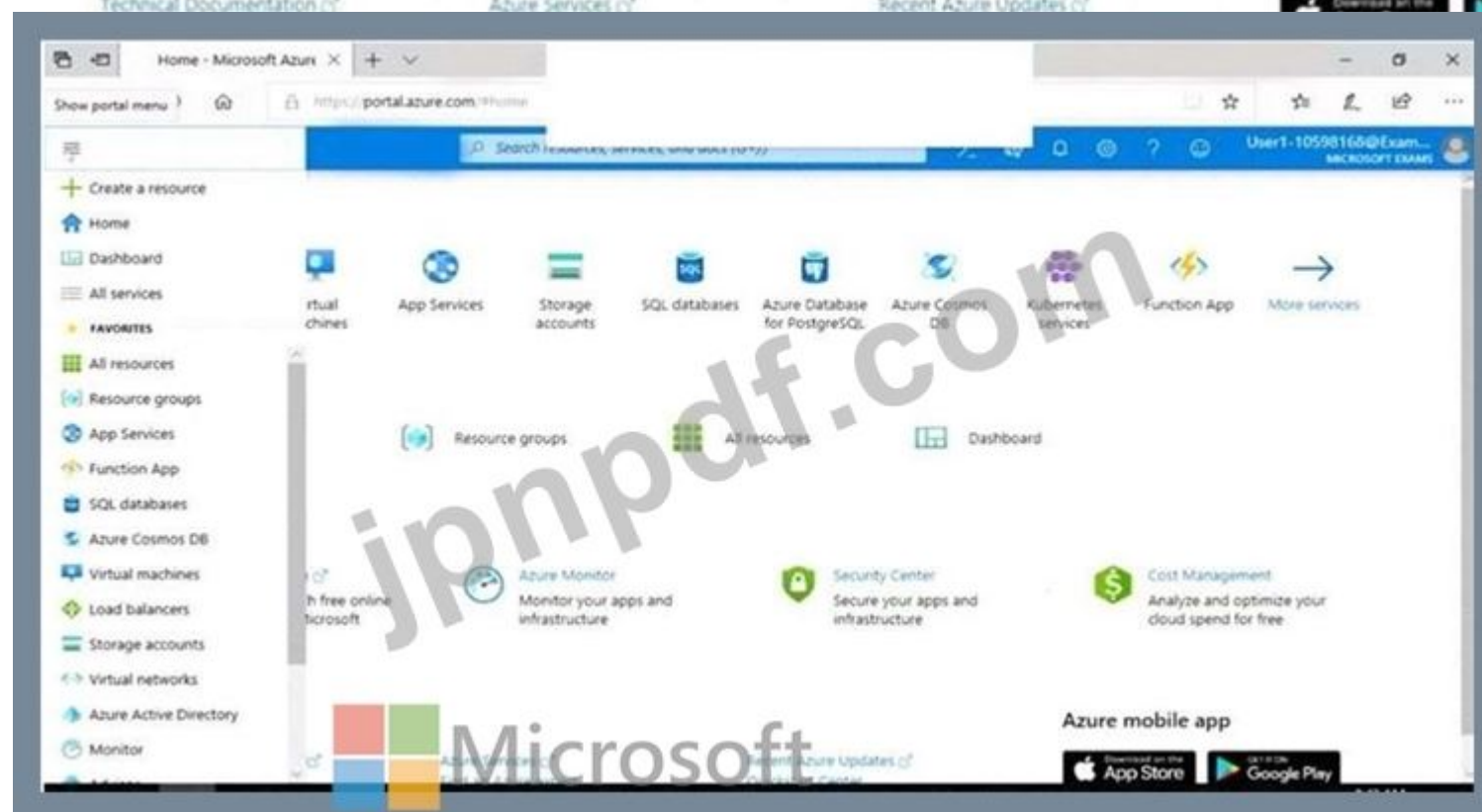
Azure ユーザー名: User1-10598168@ExamUsers.com

Azure パスワード: Ag1Bh9!#Bd

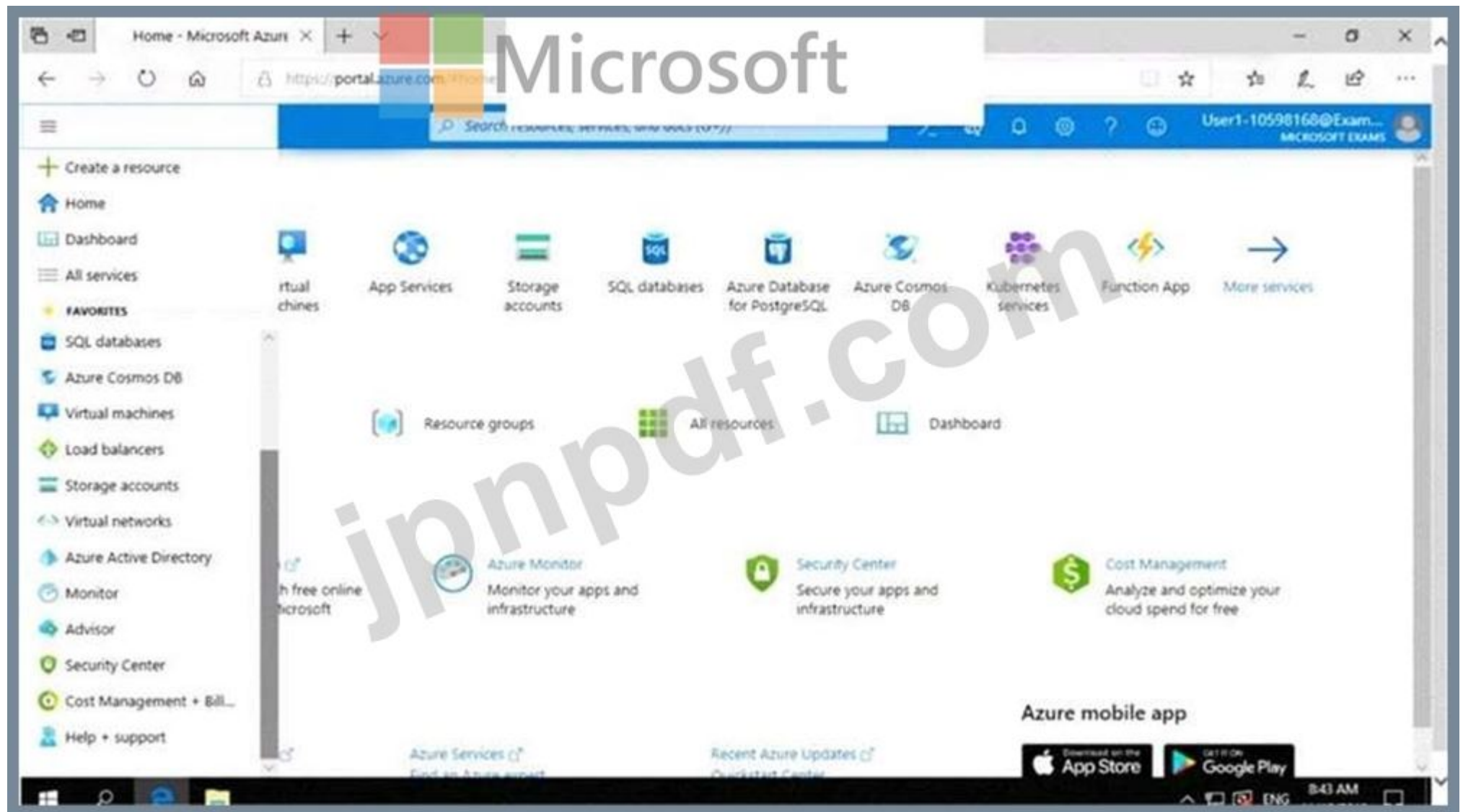
次の情報は、テクニカル サポートのみを目的としています。

ラボインスタンス: 10598168









10598168.onmicrosoft.com という名前の新しい Azure Active Directory (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 portal にサインインします。

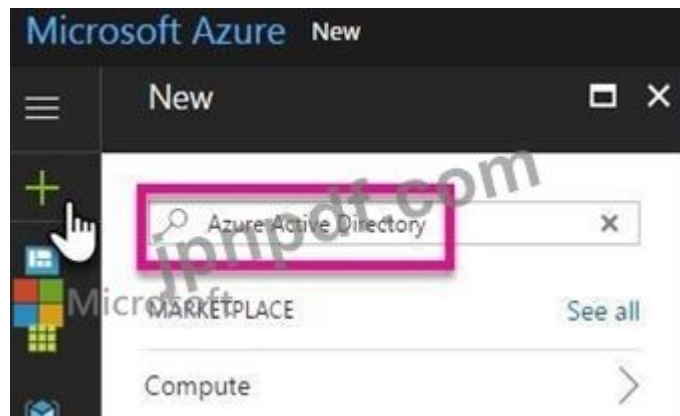
**Answer:**

以下の説明を参照してください。

**説明**

ステップ 1: Azure Active Directory テナントを作成する

1. Azure portal にアクセスし、Azure サブスクリプションを持つアカウントでサインインします。
2. プラス アイコン (+) を選択し、Azure Active Directory を検索します。

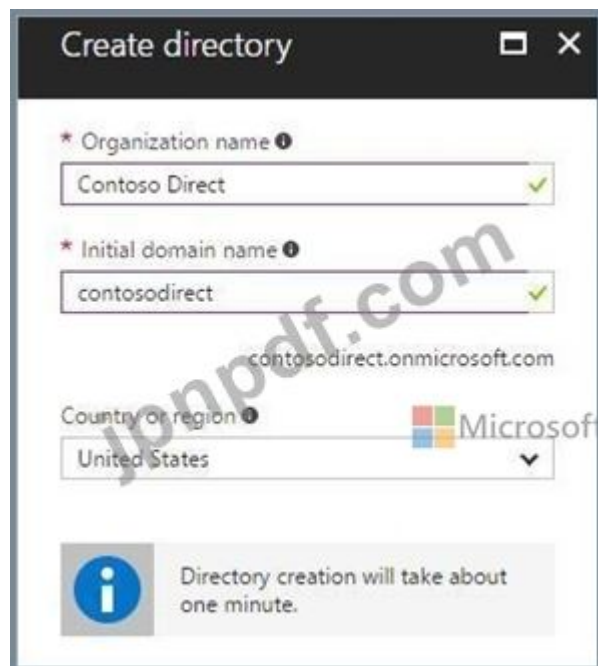


3. 検索結果で「Azure Active Directory」を選択します。



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

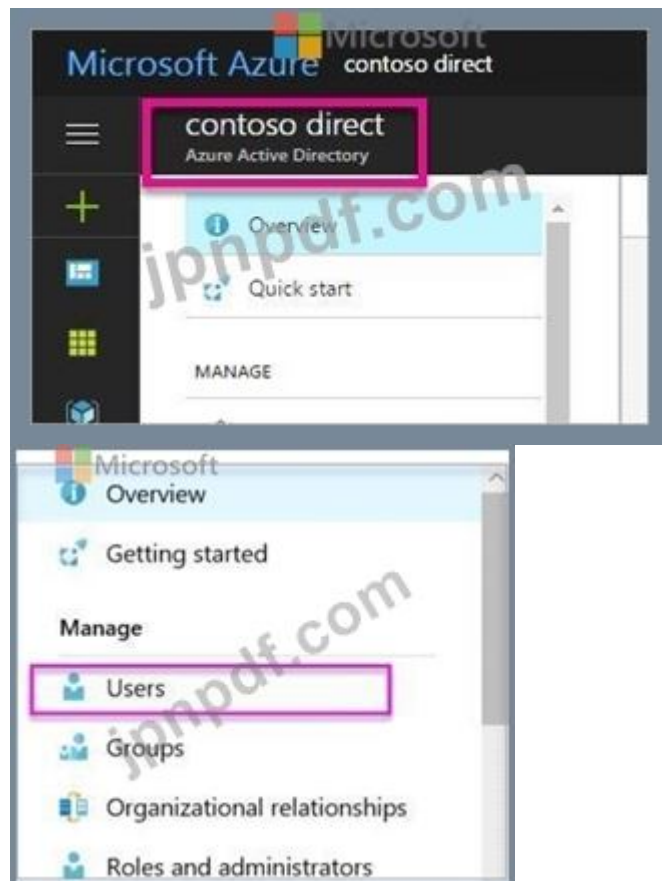


創造された。

6. ディレクトリの作成が完了したら、新しいディレクトリを管理するための情報ボックスを選択します。次に、テナント ユーザーを追加します。

ステップ 2: Azure Active Directory テナント ユーザーを作成する

7. Azure portal で、Azure Active Directory フライアウトに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、[+ 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: ユーザー1
- ユーザー名: user1@10598168.onmicrosoft.com

User  
contoso direct

\* Name ⓘ  
PBI Embed ✓ 1

\* User name ⓘ  
pbiembed@contosodirect.onmicrosoft.com ✓ 2

Profile ⓘ  
Not configured

Properties ⓘ  
Default >

Groups ⓘ  
0 groups selected >

Directory role ⓘ  
User > 3

Password Microsoft  
\*\*\*\*\*

☐ Show Password

参照：

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

#### 最新問題: 84

Microsoft Graph を使用して Azure Active Directory (Azure AD) ユーザーのプロパティを変更するアプリを展開する予定です。アプリが Azure AD にアクセスできることを確認する必要があります。最初に何を設定する必要がありますか？

- A. カスタムのロールベースのアクセス制御 (RBAQ ロール)
- B. Azure AD アプリケーション プロキシ
- C. アプリの登録
- D. 外部アイデンティティ

**Answer: D** ([メッセージを残す](#))

#### 最新問題: 85

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

<https://www.fast2test.com/AZ-500-practice-test.html> 61

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

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

※ ログは2年間保存します。

\* Kusto クエリ言語を使用してログをクエリします。

\* 管理労力を最小限に抑えます。



ログはどこに保存すればよいでしょうか？

A. Azure イベント ハブ

B. Azure ストレージ アカウント

C. Azure Log Analytics ワークスペース

**Answer: C** ([メッセージを残す](#))

最新問題: 86

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 Active Directory フォレストがあります。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 Azure AD に同期すると、LAB で始まる GivenName 属性を持つユーザーは Azure AD への同期を許可されないことが通知されます。

次のどのアクションを取る必要がありますか？

A. 属性ベースのフィルタリング ルールを作成するには、同期ルール エディタを使用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を利用して、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** ([メッセージを残す](#))

同期ルール エディタを使用して、属性ベースのフィルタリング ルールを作成します。

参照：

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

最新問題: 87

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 のロール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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

```

{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
    {
      "Microsoft.Compute/":
      {
        "Microsoft.Resources/":
        {
          "Microsoft.Storage/":
          {
            disks/**,
            storageAccounts/**,
            virtualMachines/disks/**
          }
        }
      }
    },
    "NotActions": [
      ],
    "AssignableScopes": [
      {
        "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1",
        "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"
      }
    ]
  ]
}

```

Answer:

| Statements                                                     | Yes                      | No                       |
|----------------------------------------------------------------|--------------------------|--------------------------|
| VM1 can ping VM3 successfully.                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| VM2 can ping VM4 successfully.                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| VM3 can be accessed by using Remote Desktop from the internet. | <input type="checkbox"/> | <input type="checkbox"/> |

説明

1) Microsoft.Compute/

2) ディスク

3) /subscription/{subscriptionId}/resourceGroups/{リソース グループ ID}

Resource Group1 のマネージド 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。役割 1 は、リソース グループ 1 に対してのみ使用可能である必要があります。

最新問題: 88

条件付きアクセス ポリシーを実装しています。

ポリシーを構成して実装するには、既存の Azure Active Directory (Azure AD) 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。

認証情報が漏洩したユーザー

特殊な場所への旅行は不可能

不審なアクティビティのある IP アドレスからのサインイン  
各リスクイベントについて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: 正しく選択するたびに 1 ポイントの価値があります。

| Levels | Answer Area                                                               |
|--------|---------------------------------------------------------------------------|
| High   | Impossible travel to atypical locations: <input type="text"/>             |
| Low    | Users with leaked credentials: <input type="text"/>                       |
| Medium | Sign ins from IP addresses with suspicious activity: <input type="text"/> |

Answer:

| Levels | Answer Area                                                 |
|--------|-------------------------------------------------------------|
| High   | Impossible travel to atypical locations: Medium             |
| Low    | Users with leaked credentials: High                         |
| Medium | Sign ins from IP addresses with suspicious activity: Medium |

最新問題: 89

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。

| Name       | Type                          | Region      | Resource group |
|------------|-------------------------------|-------------|----------------|
| SQL1       | Azure SQL database            | East US     | RG1            |
| Analytics1 | Azure Log Analytics workspace | East US     | RG1            |
| Analytics2 | Azure Log Analytics workspace | East US     | RG2            |
| Analytics3 | Azure Log Analytics workspace | West Europe | RG1            |

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。  
監査ログの保存先として使用できるストレージ アカウントと Log Analytics ワークスペースはどれですか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

Answer:

Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

説明

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

最新問題: 90

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/> | <input type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can connect to the web server on VM4.                | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can connect to the web server on VM4.                | <input checked="" type="radio"/> | <input type="radio"/>            |

#### 最新問題: 91

ユーザーがアクセス権のないリソースにサインインしようとしているのではないかと考えられます。

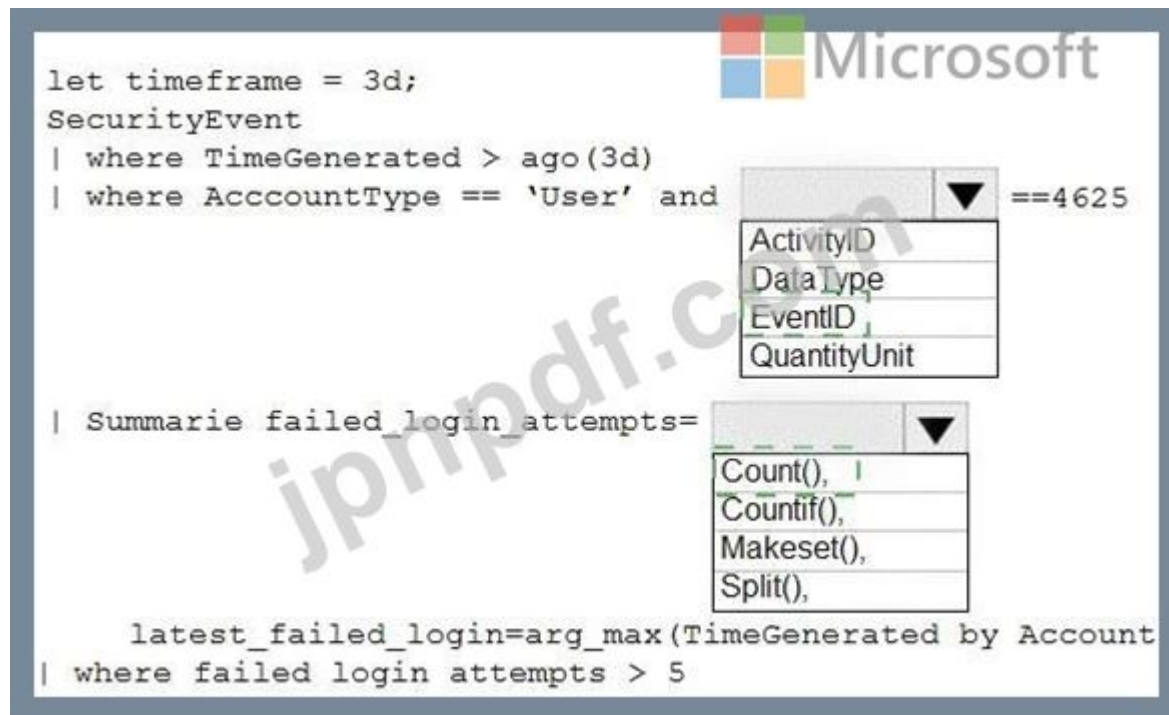
過去 3 日間に失敗したユーザーのサインイン試行を特定するには、Azure Log Analytics クエリを作成する必要があります。結果には、サインイン試行が 5 回以上失敗したユーザーのみが表示される必要があります。

クエリをどのように設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
    ==4625
    ActivityID
    DataType
    EventID
    QuantityUnit
    Summarize failed_login_attempts=
    Count(),
    Countif(),
    Makeset(),
    Split(),
    latest_failed_login=arg_max(TimeGenerated by AccountName)
    where failed_login_attempts > 5
```

Answer:



説明



次の例では、過去 1 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。  
タイムフレーム = 1d とします。

セキュリティイベント

| 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

| アカウント別の failed\_login\_attempts=count(), latest\_failed\_login=arg\_max(TimeGenerated, Account) の要約

| ここで、failed\_login\_attempts > 5

| プロジェクトアウェイアカウント1

参考文献:

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

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> (**51730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 92

次の図に示すように、Azure リソースの階層があります。



次の表に示す Azure Blueprints 定義を作成します。

| Name       | Published at      |
|------------|-------------------|
| Blueprint1 | Tenant Root Group |
| Blueprint2 | Subscription1     |

Blueprint1 と Blueprint2 をどのオブジェクトに割り当てることができますか？ 回答するには、回答領域で適切なオプションを選択してください

Blueprint1:

|                                                             |
|-------------------------------------------------------------|
| ManagementGroup1 only                                       |
| ManagementGroup1, Subscription1, and RG1 only               |
| ManagementGroup1, Subscription1, RG1, and VM1               |
| Subscription1 only                                          |
| Tenant Root Group only                                      |
| Tenant Root Group, ManagementGroup1, and Subscription1 only |

Blueprint2:

|                             |
|-----------------------------|
| ManagementGroup1 only       |
| Subscription1 and RG1 only  |
| Subscription1 only          |
| Subscription1, RG1, and VM1 |

Answer:

Blueprint1:

|                                                             |
|-------------------------------------------------------------|
| ManagementGroup1 only                                       |
| ManagementGroup1, Subscription1, and RG1 only               |
| ManagementGroup1, Subscription1, RG1, and VM1               |
| Subscription1 only                                          |
| Tenant Root Group only                                      |
| Tenant Root Group, ManagementGroup1, and Subscription1 only |

Blueprint2:

|                             |
|-----------------------------|
| ManagementGroup1 only       |
| Subscription1 and RG1 only  |
| Subscription1 only          |
| Subscription1, RG1, and VM1 |

最新問題: 93

Azure AD 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 ポータルでは何を使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。



To configure the registration settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

Answer:

To configure the registration settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

参照：

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

最新問題: 94

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。

| Name | Type               | Resource group |
|------|--------------------|----------------|
| RG1  | Resource group     | Not applicable |
| RG2  | Resource group     | Not applicable |
| RG3  | Resource group     | Not applicable |
| SQL1 | Azure SQL Database | RG3            |

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。

| Name    | Condition   | Effect if condition is false | Assignment |
|---------|-------------|------------------------------|------------|
| Policy1 | TDE enabled | Deny                         | RG1, RG2   |
| Policy2 | TDE enabled | DeployIfNotExists            | RG2, RG3   |
| Policy3 | TDE enabled | Audit                        | RG1        |

Azure Resource Manager (ARM) テンプレートを使用して Azure SQL データベースをデプロイ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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Microsoft

Statements

SQL1 will have TDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

Yes

No

☐

☐

☐

☐

☐

☐

Answer:

Answer Area

Microsoft

Statements

SQL1 will have TDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

Yes

No

☐

☒

☐

☒

☒

☐

最新問題: 95

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ます。

| Name  | Role                                            | Sign in frequency      |
|-------|-------------------------------------------------|------------------------|
| User1 | Password administrator                          | Sign in every work day |
| User2 | Password administrator                          | Sign in bi-weekly      |
| User3 | Global administrator,<br>Password administrator | Signs in every month   |

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

Create an access review

Access reviews enable reviewers to attest to users access.

\* Review name

Description

\* Start date

Frequency

Duration (in days)

End

\* Number of items

\* End date

Users

Scope ☒ Everyone

\* Review role membership

Reviewers

Reviewers

Upon completion settings

Auto apply results to resource

Should reviewer not respond

Microsoft

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成させる回答の選択肢を選択します。  
注: 正しく選択するたびに 1 ポイントの価値があります。

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

User3 only  
User1 and User2 only  
User1, User2, and User3

The Password administrator role will be revoked from User2  
User2 will retain the Password administrator role  
User3 will receive a confirmation request

Answer:

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

User3 only  
User1 and User2 only  
User1, User2, and User3

The Password administrator role will be revoked from User2  
User2 will retain the Password administrator role  
User3 will receive a confirmation request

参考文献:

最新問題: 96

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。

| Name | Type               | Resource group |
|------|--------------------|----------------|
| RG1  | Resource group     | Not applicable |
| RG2  | Resource group     | Not applicable |
| RG3  | Resource group     | Not applicable |
| SQL1 | Azure SQL Database | RG3            |

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。

| Name    | Condition   | Effect if condition is false | Assignment |
|---------|-------------|------------------------------|------------|
| Policy1 | TDE enabled | Deny                         | RG1, RG2   |
| Policy2 | TDE enabled | DeployIfNotExists            | RG2, RG3   |
| Policy3 | TDE enabled | Audit                        | RG1        |

Azure Resource Manager (ARM) テンプレートを使用して Azure SQL データベースをデプロイ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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Microsoft

Statements

SQL1 will have TDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

Yes

No

☐

☐

☐

☐

☐

☐

Answer:

Answer Area

Microsoft

Statements

SQL1 will have TDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

Yes

No

☐

☒

☒

☐

☒

☐

最新問題: 97

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。

| Name | Network interface | Application security group assignment | IP address |
|------|-------------------|---------------------------------------|------------|
| VM1  | NIC1              | AppGroup12                            | 10.0.0.10  |
| VM2  | NIC2              | AppGroup12                            | 10.0.0.11  |
| VM3  | NIC3              | AppGroup3                             | 10.0.0.100 |
| VM4  | NIC4              | AppGroup4                             | 10.0.0.200 |

現在、ネットワーク セキュリティ グループ (NSG) をプロビジョニングしていません。

次の要件を満たすためにネットワーク 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 と 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 ルールはいくつ作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: 正しく選択するたびに 1 ポイントの価値があります。

NSGs:

1

2

3

4

Network security rules:

1

2

3

4

Answer:

NSGs:

1

2

3

4

Network security rules:

1

2

3

4

説明

NSG: 1

ネットワークセキュリティルール: 3

注 2: セキュリティ ルールに複数のサービス 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。

参考文献:

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

**最新問題: 98**

Azure コンテナ インスタンスをデプロイする予定です。

クレジット カードを検証するコンテナ化されたアプリケーションがあります。アプリケーションは、アプリケーション コンテナと検証コンテナの 2 つのコンテナで構成されます。

アプリケーション コンテナは検証コンテナによって監視されます。検証コンテナは、アプリケーション コンテナにリクエストを送信し、トランザクションごとに応答を待つことによってセキュリティ チェックを実行します。

アプリケーション コンテナと検証コンテナと一緒にデプロイされるようにスケジュールされていることを確認する必要があります。コンテナは、外部に公開されていないポート上でのみ相互に通信する必要があります。

導入には何を含める必要がありますか？

- A. アプリケーションセキュリティグループ
- B. ネットワーク セキュリティ グループ (NSG)
- C. 管理グループ
- D. コンテナグループ

**Answer:** ([解答を表示する](#))

説明

Azure Container Instances は、コンテナ グループを使用した単一ホストへの複数のコンテナのデプロイをサポートしています。コンテナ グループは、ログ記録、監視、またはサービスに 2 番目の接続プロセスが必要なその他の構成用のアプリケーション サイドカーを構築するときに役立ちます。

参照 :

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

**最新問題: 99**

App1 という名前の Web アプリと Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。

Vault1 にシークレットを保存してアクセスできるように App1 を構成する必要があります。

App1 をどのように構成すればよいでしょうか？ 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: 正しく選択するたびに 1 ポイントの価値があります。

Configure App1 to authenticate by using a

Key

Certificate

Passphrase

User-assigned managed identity

System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade

General settings tab

TLS/SSL settings blade

Application settings tab

Answer:

Configure App1 to authenticate by using a:

Key

Certificate

Passphrase

User-assigned managed identity

System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade

General settings tab

TLS/SSL settings blade

Application settings tab

参照：

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>

最新問題: 100

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。

| Name      | Region  | Description                                                                                                                                                                           |
|-----------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HubVNet   | East US | HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0. |
| SpokeVNet | East US | SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.                                                        |

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 にデプロイする予定です。  
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のルートが含まれます。  
RT2: BGP ルートの伝達を無効にし、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 ネットワークの間は、Azure ファイアウォールを通過します。  
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 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります。

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:



Answer:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

説明



Answer Area

RT1:

GatewaySubnet

RT2:

HubVNetSubnet0

最新問題: 101

contoso1812.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

| Name  | Username                          | Type   |
|-------|-----------------------------------|--------|
| User1 | User1@contoso1812.onmicrosoft.com | Member |
| User2 | User2@contoso1812.onmicrosoft.com | Member |
| User3 | User3@contoso1812.onmicrosoft.com | Member |
| User4 | User4@outlook.com                 | Guest  |

Label1 という名前の Azure Information Protection ラベルを作成します。Label1 の保護設定は、図に示すように構成されています。(「展示」タブをクリックします。)

Protection

Microsoft

Contoso1812 - Azure Information Protection

Protections settings

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type

☒ Set permissions

☐ Set user-defined permissions (Preview)

USERS

PERMISSIONS

AuthenticatedUsers

Viewer

User1@contoso1812.onmicrosoft.com

Co-Author

User2@contoso1812.onmicrosoft.com

Reviewer

+Add permissions

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、それ以外の場合は [いいえ] を選択します。  
注: 正しく選択するたびに 1 ポイントの価値があります。

| Statements             | Yes                   | No                    |
|------------------------|-----------------------|-----------------------|
| User1 can print File1. | <input type="radio"/> | <input type="radio"/> |
| User3 can read File1.  | <input type="radio"/> | <input type="radio"/> |
| User4 can print File1. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements             | Yes                              | No                               |
|------------------------|----------------------------------|----------------------------------|
| User1 can print File1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can read File1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| User4 can print File1. | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

| Statements             | Yes                              | No                               |
|------------------------|----------------------------------|----------------------------------|
| User1 can print File1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can read File1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| User4 can print File1. | <input type="radio"/>            | <input checked="" type="radio"/> |

10317806.onmicrosoft.com という名前の新しい Azure Active Directory (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 user10317806 という名前のユーザーが含まれている必要があります。

**Answer:**

以下の説明を参照してください。

説明

新しい Azure AD テナントを作成するには:

1. Azure portal にアクセスし、Azure サブスクリプションを持つアカウントでサインインします。
2. プラス アイコン (+) を選択し、Azure Active Directory を検索します。



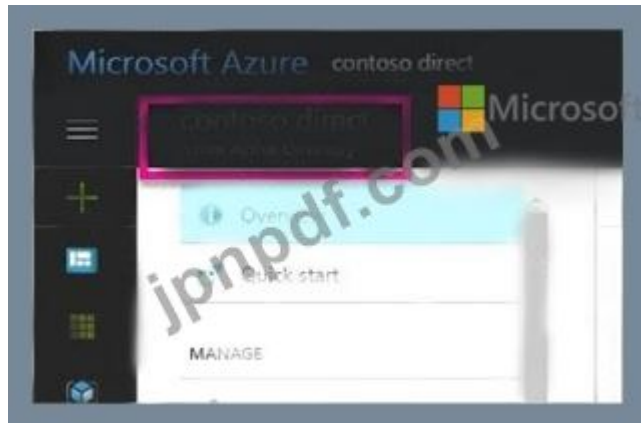
3. Azure Active Directory」を選択します。



4. [作成]を選択します。
5. 組織名 (10317806) と初期ドメイン名 (10317806) を入力します。次に、作成」を選択します。  
これにより、という名前のディレクトリが作成されます  
10317806.onmicrosoft.com。

6. ディレクトリの作成が完了したら、新しいディレクトリを管理するための情報ボックスを選択します。  
ユーザーを作成するには:

1. Azure portal で、Azure Active Directory フライアウトにいることを確認します。

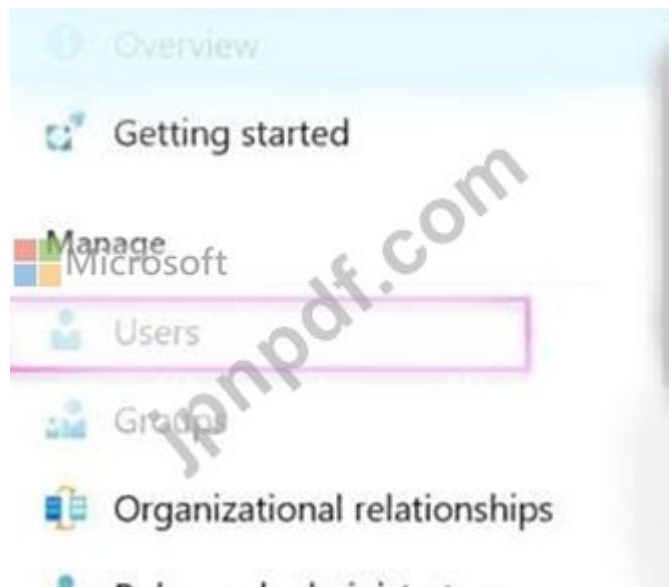


そうでない場合は、左側のサービス ナビゲーションから Azure Active Directory アイコンを選択します。



2. 管理」で ユーザー」を選択します。



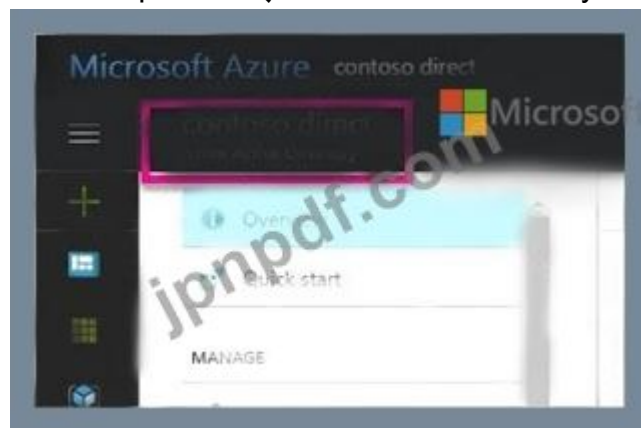


3. [すべてのユーザー] を選択し、

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

MFA を有効にするには:

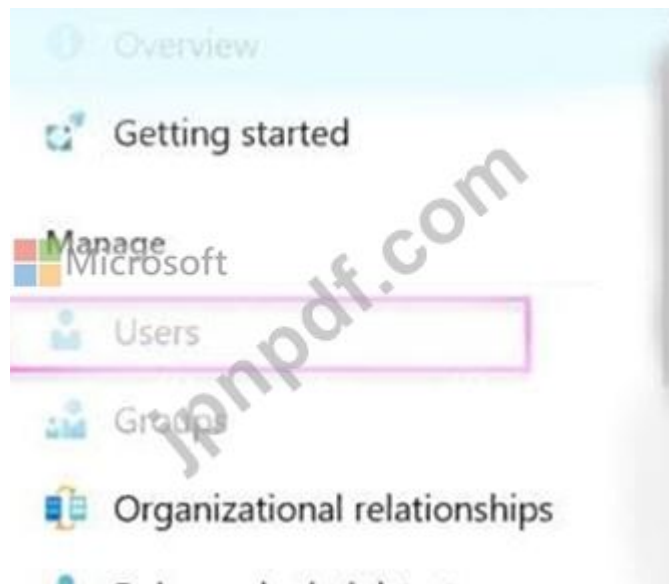
1. Azure portal で、Azure Active Directory フライアウトにいることを確認します。



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



2. [管理] で [ユーザー] を選択します。



3. [多要素認証] をクリックします。

4. ユーザー名の横にあるチェックボックスをオンにして、  
参照：

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

#### 最新問題: 103

Azure 仮想マシンのデプロイに使用する Azure Resource Manager テンプレートがあります。仮想マシンのインスタンスがプロビジョニングされるときに、未使用の Windows 機能を自動的に無効にする必要があります。

何をえばいいのでしょうか？

A. Microsoft Intune のデバイス構成ポリシー

B. Azure Desired State Configuration (DSC) 仮想マシン拡張機能

C. Azure Security Center のセキュリティ ポリシー

D. Azure ロジック アプリ

**Answer: B (メッセージを残す)**

説明

Azure Automation State Configuration を使用して、Azure VM (クラシック マネージャーとリソース マネージャーの両方)、オンプレミス VM、Linux マシン、AWS VM、オンプレミスの物理マシンを管理できます。

注: Azure Automation State Configuration は、Windows 機能 DSC サービスと同様の DSC プル サーバーを提供するため、ターゲット ノードは自動的に構成を受信し、望ましい状態に準拠し、その準拠状況をレポートします。Azure Automation に組み込まれたプル サーバーにより、独自のプル サーバーをセットアップして維持する必要がなくなります。Azure Automation は、クラウドまたはオンプレミスの仮想または物理 Windows マシンまたは Linux マシンをターゲットにできます。

参照：

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

#### 最新問題: 104

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

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

このタスクを完了するには、Azure portal にサインインします。

Azure Monitor でアラート ルールを構成する必要があります。

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

「アラート」をクリックします。

[+新しいアラート ルール] をクリックします。

「スコープ」セクションで、「リソースの選択」リンクをクリックします。

[リソースの種類でフィルター] ボックスに 「locks」と入力し、フィルターされた結果から [管理ロック (ロック)] を選択します。

サブスクリプションを選択し、完了」ボタンをクリックします。

条件」セクションで、条件の選択」リンクをクリックします。

管理ロックの削除」条件を選択し、完了」ボタンをクリックします。

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

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

グループに 「Debbie Mobile App」などの名前を付けて (試験用に入力する名前は関係ありません)、次へ: 通知 >」ボタンをクリックします。

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

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

OK」ボタンをクリックしてウィンドウを閉じます。

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

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

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

D. 通知名ボックスに 「Debbie Mobile App」などの名前を入力します。

**Answer: D (メッセージを残す)**

## 最新問題: 105

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 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。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area



Answer:

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Create a new subnet.

Deploy Azure Firewall.

Create a network rule collection.



最新問題: 106

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。

| Name | Operating system        |
|------|-------------------------|
| VM1  | Windows Server 2016     |
| VM2  | Ubuntu Server 18.04 LTS |

Azure Security Center から、自動プロビジョニングを有効にします。

次の表に示す仮想マシンをデプロイします。

| Name | Operating system        |
|------|-------------------------|
| VM3  | Windows Server 2016     |
| VM4  | Ubuntu Server 18.04 LTS |

- 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 と VM3 のみ
  - C. VM3 および VM4 のみ
  - D. VM1、VM2、VM3、および VM4



**Answer: D (メッセージを残す)**

説明

自動プロビジョニングがオンになっている場合、Security Center は、サポートされているすべての Azure VM と新しく作成された Azure VM に Log Analytics エージェント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)、および 18.04 LTS (x64) および Windows Server 2008 R2、2012、2012 R2、2016、バージョン 1709 および 1803 が含まれます。

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

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> (**51730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 107

Microsoft Antimalware for Virtual Machines を使用して web11597200 がマルウェアから保護されており、毎週金曜日の 01:00 にスキャン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 portal にサインインします。

**Answer:**

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

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

web11597200 のプロパティで、[拡張機能] をクリックします。

追加」ボタンをクリックして拡張機能を追加します。

拡張機能のリストを下にスクロールし、「Microsoft Antimalware」を選択します。

作成」ボタンをクリックします。これにより、Microsoft Antimalware Extension の設定ペインが開きます。

[スキャン日] フィールドで、金曜日を選択します。

スキャン時間」フィールドに「60」と入力します。スキャン時間は午前 0 時からの分単位で測定されるため、60 は 01:00、120 は 02:00 になります。

[OK] ボタンをクリックして構成を保存し、拡張機能をインストールします。

最新問題: 108

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

| Name       | Location | Description            |
|------------|----------|------------------------|
| Workspace1 | East US  | Used by Azure Sentinel |
| Workspace2 | West US  | Not applicable         |

次の表に示す仮想マシンを作成します。

| Name | Location | Operating system    | Connected to |
|------|----------|---------------------|--------------|
| VM1  | East US  | Windows Server 2019 | None         |
| VM2  | East US  | Windows Server 2019 | Workspace2   |
| VM3  | West US  | Windows Server 2019 | None         |
| VM4  | West US  | Windows Server 2019 | Workspace2   |

Azure Sentinel を使用して、仮想マシン上の Windows Defender ファイアウォールを監視する予定です。  
Azure Sentinel に接続できる仮想マシンはどれですか？

- A. VM1 と VM2 のみ
- B. VM1、VM2、VM3、VM4
- C. VM1 のみ
- D. VM1 と VM3 のみ

Answer: A (メッセージを残す)

最新問題: 109

次の表に示す Azure Information Protection 条件があります。

| Name       | Pattern | Case sensitivity |
|------------|---------|------------------|
| Condition1 | White   | On               |
| Condition2 | Black   | Off              |

You have the Azure Information Protection labels shown in the following table.

| Name    | Applies to     | Use label | Set the default label |
|---------|----------------|-----------|-----------------------|
| Global  | Not applicable | None      | None                  |
| Policy1 | User1          | Label1    | None                  |
| Policy2 | User2          | Label2    | None                  |

Azure Information Protection がファイルにどのようにラベルを付けるかを特定する必要があります。  
何を識別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: 正しく選択するたびに 1 ポイントの価値があります。

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

No label  
Label1 only  
Label2 only  
Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

No label  
Label1 only  
Label2 only  
Label1 and Label2

Answer:

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

No label  
Label1 only  
Label2 only  
Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

No label  
Label1 only  
Label2 only  
Label1 and Label2

参照：

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

最新問題: 110

次の表に示す Azure 仮想ネットワークがあります。

| Name  | Location | Subnet           | Peered network |
|-------|----------|------------------|----------------|
| VNET1 | East US  | Subnet1          | VNET2          |
| VNET2 | West US  | Subnet2, Subnet3 | VNET1          |
| VNET4 | East US  | Subnet4          | None           |

次の表に示す Azure 仮想マシンがあります。

| Name | Application security group | Network security group (NSG) | Connected to | Public IP address |
|------|----------------------------|------------------------------|--------------|-------------------|
| VM1  | ASG1                       | NSG1                         | Subnet1      | No                |
| VM2  | ASG2                       | NSG1                         | Subnet2      | No                |
| VM3  | ASG2                       | NSG1                         | Subnet3      | Yes               |
| VM4  | ASG4                       | NSG1                         | Subnet4      | Yes               |

すべての仮想マシンのファイアウォールは ping トラフィックを許可します。

NSG1 は次の図に示すように構成されています。

インバウンドセキュリティルール

| Priority | Name                   | Port | Protocol | Source            | Destination    | Action |
|----------|------------------------|------|----------|-------------------|----------------|--------|
| 110      | Allow_RDP              | 3389 | Any      | Any               | Any            | Allow  |
| 130      | Rule1                  | Any  | Any      | ASG1              | Any            | Allow  |
| 140      | Rule2                  | Any  | Any      | ASG2              | Any            | Allow  |
| 150      | Rule3                  | Any  | Any      | ASG4              | Any            | Allow  |
| 160      | Rule4                  | Any  | Any      | Any               | Any            | Deny   |
| 65000    | AllowVnetInBound       | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | AllowAzureLoadBalan... | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | DenyAllInBound         | Any  | Any      | Any               | Any            | Deny   |

アウトバウンドセキュリティルール

| Priority | Name                   | Port | Protocol | Source         | Destination    | Action |
|----------|------------------------|------|----------|----------------|----------------|--------|
| 65000    | AllowVnetOutBound      | Any  | Any      | VirtualNetwork | VirtualNetwork | Allow  |
| 65001    | AllowInternetOutBou... | Any  | Any      | Any            | Internet       | Allow  |
| 65500    | DenyAllOutBound        | Any  | Any      | Any            | Any            | Deny   |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Statements

VM1 can ping VM3 successfully.

VM2 can ping VM4 successfully.

VM3 can be accessed by using Remote Desktop from the internet.

Yes

No

Answer:

Statements

VM1 can ping VM3 successfully.

VM2 can ping VM4 successfully.

VM3 can be accessed by using Remote Desktop from the internet.

Yes

No

Explanation:



| Statements                                                     | Yes                              | No                               |
|----------------------------------------------------------------|----------------------------------|----------------------------------|
| VM1 can ping VM3 successfully.                                 | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM2 can ping VM4 successfully.                                 | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM3 can be accessed by using Remote Desktop from the internet. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 111

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。

| Name      | Region  | Description                                                                                                                                                                           |
|-----------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HubVNet   | East US | HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0. |
| SpokeVNet | East US | SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.                                                        |

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 にデプロイする予定です。

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のルートが含まれます
  - \* RT2: BGP ルートの伝達を無効にし、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ことを確認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 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります。

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

Answer:

## Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

## Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

### 最新問題: 112

Azure Security Center から、Registry1 内のイメージの Azure Container Registry 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。
- どの 2 つのイメージの脆弱性がスキャンされますか? それぞれの正解は完全な解決策を示します。

注: 正しく選択するたびに 1 ポイントの価値があります。

#### A. 画像4

<https://www.fast2test.com/AZ-500-practice-test.html> 46

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

#### B. 画像2

#### C. 画像1

#### D. 画像3

#### E. 画像5

**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: 113

次の表に示す Azure 仮想ネットワークがあります。

| Name  | Location | Subnet           | Peered network |
|-------|----------|------------------|----------------|
| VNET1 | East US  | Subnet1          | VNET2          |
| VNET2 | West US  | Subnet2, Subnet3 | VNET1          |
| VNET4 | East US  | Subnet4          | None           |

次の表に示す Azure 仮想マシンがあります。

| Name | Application security group | Network security group (NSG) | Connected to | Public IP address |
|------|----------------------------|------------------------------|--------------|-------------------|
| VM1  | ASG1                       | NSG1                         | Subnet1      | No                |
| VM2  | ASG2                       | NSG1                         | Subnet2      | No                |
| VM3  | ASG2                       | NSG1                         | Subnet3      | Yes               |
| VM4  | ASG4                       | NSG1                         | Subnet4      | Yes               |

すべての仮想マシンのファイアウォールは ping トラフィックを許可します。  
NSG1 は次の図に示すように構成されています。  
インバウンドセキュリティルール

| Priority | Name                    | Port | Protocol | Source            | Destination    | Action |
|----------|-------------------------|------|----------|-------------------|----------------|--------|
| 110      | Allow_RDP               | 3389 | Any      | Any               | Any            | Allow  |
| 130      | Rule1                   | Any  | Any      | ASG1              | Any            | Allow  |
| 140      | Rule2                   | Any  | Any      | ASG2              | Any            | Allow  |
| 150      | Rule3                   | Any  | Any      | ASG4              | Any            | Allow  |
| 160      | Rule4                   | Any  | Any      | Any               | Any            | Deny   |
| 65000    | AllowVnetInBound        | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | AllowAzureLoadBalanc... | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | DenyAllInBound          | Any  | Any      | Any               | Any            | Deny   |

アウトバウンドセキュリティルール

| Priority | Name                   | Port | Protocol | Source         | Destination    | Action |
|----------|------------------------|------|----------|----------------|----------------|--------|
| 65000    | AllowVnetOutBound      | Any  | Any      | VirtualNetwork | VirtualNetwork | Allow  |
| 65001    | AllowInternetOutBou... | Any  | Any      | Any            | Internet       | Allow  |
| 65500    | DenyAllOutBound        | Any  | Any      | Any            | Any            | Deny   |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                     | Yes                   | No                    |
|----------------------------------------------------------------|-----------------------|-----------------------|
| VM1 can ping VM3 successfully.                                 | <input type="radio"/> | <input type="radio"/> |
| VM2 can ping VM4 successfully.                                 | <input type="radio"/> | <input type="radio"/> |
| VM3 can be accessed by using Remote Desktop from the internet. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                     | Yes                              | No                               |
|----------------------------------------------------------------|----------------------------------|----------------------------------|
| VM1 can ping VM3 successfully.                                 | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM2 can ping VM4 successfully.                                 | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM3 can be accessed by using Remote Desktop from the internet. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 114

3 つの Azure サブスクリプションと User1 という名前のユーザーがあります。

User1 に、3 つのサブスクリプションすべてにわたるリソースのコストを管理および表示する機能を提供する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

注: 回答の選択肢は複数の順序で正解です。選択した正しい注文に対してクレジットを受け取ります。

| Actions                                                                     |
|-----------------------------------------------------------------------------|
| Create a management group.                                                  |
| Add the three subscriptions to the management group.                        |
| Assign User1 the Global administrator role.                                 |
| Assign User1 the Owner role for the management group.                       |
| Assign User1 the Cost Management Contributor role for the management group. |

Answer:



| Actions                                                                     |                                                                             |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Create a management group.                                                  | Assign User1 the Cost Management Contributor role for the management group. |
| Add the three subscriptions to the management group.                        |                                                                             |
| Assign User1 the Global administrator role.                                 | Assign User1 the Global administrator role.                                 |
| Assign User1 the Owner role for the management group.                       |                                                                             |
| Assign User1 the Cost Management Contributor role for the management group. | Add the three subscriptions to the management group.                        |

説明

| Actions                                                                     | Answer Area                                                              |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Create a management group.                                                  | 1 Assign User1 the Cost Management Reader role for the management group. |
| Assign User1 the Owner role for the management group.                       | 2 Assign User1 the Global administrator role.                            |
| Assign User1 the Cost Management Contributor role for the management group. | 3 Add the three subscriptions to the management group.                   |

最新問題: 115

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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

|                                         |                                                                                                                                      |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Virtual networks that User2 can modify: | <div>▼</div> <div> VNET4 only<br/> VNET4 and VNET1 only<br/> VNET4, VNET3, and VNET1 only<br/> VNET4, VNET3, VNET2, and VNET1 </div> |
| Virtual networks that User2 can delete: | <div>▼</div> <div> VNET4 only<br/> VNET4 and VNET1 only<br/> VNET4, VNET3, and VNET1 only<br/> VNET4, VNET3, VNET2, and VNET1 </div> |

Answer:

Virtual networks that User2 can modify:

Microsoft

Virtual networks that User2 can delete:

参考文献:  
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

最新問題: 116  
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。

| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

次の表に示すリソース ロックを作成します。

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                               | Yes                   | No                    |
|------------------------------------------|-----------------------|-----------------------|
| You can start VM1.                       | <input type="radio"/> | <input type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                               | Yes                   | No                               |
|------------------------------------------|-----------------------|----------------------------------|
| You can start VM1.                       | <input type="radio"/> | <input checked="" type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input checked="" type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input checked="" type="radio"/> |

Explanation:

1.) 次のスコープがロックされているため、書き込み操作を実行できません:

「subscriptions/xxxx/resourceGroups/xxx」ロックを解除して、もう一度お試しください。

2.) 読み取り専用ロックを持つリソース グループに VM を作成すると、エラーが表示されます。

「選択されたリソース グループは読み取り専用です」

3.) 読み取り専用ロックのため、マシンの起動後にロックが追加されると、仮想マシンは起動または停止できません。(このユースケースの一部ではありませんが、知っておくと良いでしょう。

回答で参照されている記事は、ブループリントに範囲が限定されているため、異なると述べています。

[リソースのロック] ページには、VM の起動に関して次のことが記載されています。

「仮想マシンを含むリソース グループに対する読み取り専用ロックにより、すべてのユーザーが仮想マシンを起動または再起動できなくなります。これらの操作には POST リクエストが必要です。」

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

最新問題: 117

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、仮想マシンへの PowerShell アクセスをユーザーに許可する必要があります。

何を設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Microsoft

Permission that must be granted to users on VM:

|        |
|--------|
| Read   |
| Update |
| View   |
| Write  |

TCP port that must be allowed:

|      |
|------|
| 22   |
| 25   |
| 3389 |
| 5986 |

Answer:

Answer Area

Microsoft

Permission that must be granted to users on VM:

|        |
|--------|
| Read   |
| Update |
| View   |
| Write  |

TCP port that must be allowed:

|      |
|------|
| 22   |
| 25   |
| 3389 |
| 5986 |

#### 最新問題: 118

Azure コンテナ インスタンスをデプロイする予定です。

クレジット カードを検証するコンテナ化されたアプリケーションがあります。アプリケーションは、アプリケーション コンテナと検証コンテナの 2 つのコンテナで構成されます。

アプリケーション コンテナは検証コンテナによって監視されます。検証コンテナは、アプリケーション コンテナにリクエストを送信し、トランザクションごとに応答を待つことによってセキュリティ チェックを実行します。

アプリケーション コンテナと検証コンテナと一緒にデプロイされるようにスケジュールされていることを確認する必要があります。コンテナは、外部に公開されていないポート上でのみ相互に通信する必要があります。

導入には何を含める必要がありますか？

- A. アプリケーションセキュリティグループ
- B. ネットワーク セキュリティ グループ (NSG)
- C. 管理グループ
- D. コンテナグループ

Answer: D ([メッセージを残す](#))

セクション: [なし]

Explanation:

Azure Container Instances は、コンテナ グループを使用した単一ホストへの複数のコンテナのデプロイをサポートしています。コンテナ グループは、ログ記録、監視、またはサービスに 2 番目の接続プロセスが必要なその他の構成用のアプリケーション サイドカーを構築するときに役立ちます。

参照 :

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

#### 最新問題: 119



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

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

次の要件を満たすように構成する Azure Sentinel コンポーネントを特定する必要があります。

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

Azure Sentinel でインシデントが作成されるとき、チケットはサービス管理プラットフォームに記録される必要があります。

各要件に対してどのコンポーネントを特定する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

When Azure Sentinel identifies a threat, an incident must be created:

Analytics  
Data connectors  
Playbooks  
Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

Analytics  
Data connectors  
Playbooks  
Workbooks

Answer:

When Azure Sentinel identifies a threat, an incident must be created:

Analytics  
Data connectors  
Playbooks  
Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

Analytics  
Data connectors  
Playbooks  
Workbooks

参照 :

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

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

最新問題: 120

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 のロール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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
```

|                       |   |                           |   |
|-----------------------|---|---------------------------|---|
|                       | ▼ |                           | ▼ |
| "Microsoft.Compute/   |   | disks/*",                 |   |
| "Microsoft.Resources/ |   | storageAccounts/*",       |   |
| "Microsoft.Storage/   |   | virtualMachines/disks/*", |   |

```
    ],
  "NotActions": [
    ],
  "AssignableScopes": [
```

|                                                                                      |   |
|--------------------------------------------------------------------------------------|---|
|                                                                                      | ▼ |
| "/*"                                                                                 |   |
| "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1" |   |
| "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"                                |   |

```
    ]
  }
}
```



Answer:


Microsoft

```

{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
    {
      "Microsoft.Compute/",
      "Microsoft.Resources/",
      "Microsoft.Storage/"
    },
    {
      "disks/*",
      "storageAccounts/*",
      "virtualMachines/disks/*"
    }
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    {
      "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
    },
    {
      "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"
    }
  ]
}

```

### 最新問題: 121

OU2 と User1 に対して計画された変更を実行する必要があります。

どのツールを使用する必要がありますか？ 答えるには、適切なツールを正しいリソースにドラッグします。各ツールは 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: 正しく選択するたびに 1 ポイントの価値があります。

| Tools                                | Answer Area |
|--------------------------------------|-------------|
| The Azure portal                     | OU2: Tool   |
| Azure AD Connect                     | User1: Tool |
| The Active Directory admin center    |             |
| Active Directory Sites and Services  |             |
| Active Directory Users and Computers |             |

Answer:

| Tools                                | Answer Area             |
|--------------------------------------|-------------------------|
| The Azure portal                     | OU2: Azure AD Connect   |
| Azure AD Connect                     | User1: The Azure portal |
| The Active Directory admin center    |                         |
| Active Directory Sites and Services  |                         |
| Active Directory Users and Computers |                         |

説明  
テーブルの説明が自動的に生成される

|        |                  |
|--------|------------------|
| OU2:   | Azure AD Connect |
| User1: | The Azure portal |

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> (517**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 122  
LAW1 という名前の Azure Log Analytics ワークスペースを含む Sub1 という名前の Azure サブスクリプションがあります。



Windows Server 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。  
システム更新評価ソリューションを LAW1 に追加する予定です。  
システム更新評価関連のログが 100 台の仮想マシンのみから LAW1 にアップロードされるようにする必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                        | Answer Area |
|------------------------------------------------|-------------|
| Create a new workspace.                        |             |
| Apply the scope configuration to the solution. |             |
| Create a scope configuration.                  |             |
| Create a computer group.                       |             |
| Create a data source.                          |             |

Answer:

| Actions                                        | Answer Area                                    |
|------------------------------------------------|------------------------------------------------|
| Create a new workspace.                        | Create a computer group.                       |
| Apply the scope configuration to the solution. | Create a scope configuration.                  |
| Create a scope configuration.                  | Apply the scope configuration to the solution. |
| Create a computer group.                       |                                                |
| Create a data source.                          |                                                |

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

最新問題: 123  
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の保護要件を満たしている必要があります。

あなたは何をすべきか？

- 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: D (メッセージを残す)

説明

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat>

トピック 1、Litware, Inc

これはケーススタディです。ケーススタディは個別に時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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る場合があります。このケーススタディに関する各質問は、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、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に関する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、サンフランシスコ地域に 20 人の従業員を抱えるデジタル メディア企業です。

既存の環境

Litware には、Sub1 という名前の Azure サブスクリプションがあり、サブスクリプション ID は次のとおりです。

43894a43-17c2-4a39-8cfc-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 AD Premium P2 ライセンスが割り当てられます。Azure AD Privileged Identity Management (PIM) がアクティブ化されています。

テナントには、次の表に示すグループが含まれています。

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team                                                                              |

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。



| Name            | Type               | Description                                                                                                                                             |
|-----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| VNet1           | Virtual network    | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0             | Virtual machine    | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.                    |
| VM1             | Virtual machine    | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.                                                                  |
| SQLDB1          | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.                                                                       |
| WebApp1         | Web app            | WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.                                           |
| Resource Group1 | Resource group     | Resource Group1 is a resource group that contains VNet1, VM0, and VM1.                                                                                  |
| Resource Group2 | Resource group     | Resource Group2 is a resource group that contains shared IT resources.                                                                                  |

Azure Security Center は無料レベル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。

| Name      | Type                           | Description                                                                                                           |
|-----------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Firewall1 | Azure Firewall                 | An Azure firewall on VNet1.                                                                                           |
| RT1       | Route table                    | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1      | Azure Kubernetes Service (AKS) | A managed AKS cluster                                                                                                 |

Litware は、次の ID およびアクセス要件を特定します。

- \* すべてのサンフランシスコ 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 のメンバーには、永続的な適格な割り当てを使用して、リソース グループ 2 への共同作成者ロールを割り当てる必要があります。
- \* ユーザーが Azure AD にアプリケーションを登録したり、アプリケーションに同意したりできないようにする必要があります
- \* ユーザーに代わって企業情報にアクセスします。

プラットフォームの保護要件

Litware は、次のプラットフォーム保護要件を特定します。

- \* Microsoft Antimalware は、リソース グループ 1 の仮想マシンにインストールする必要があります。
- \* Group2 のメンバーには、Azure Kubernetes Service Cluster Admin ロールが割り当てられている必要があります。
- \* Azure AD ユーザーは、Azure AD 資格情報を使用して 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 JIT VM アクセスを使用して VM0 に接続できる必要があります。

\* Resource Group1 のマネージド 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。役割 1 は、リソース グループ 1 に対して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、Azure Security Center でオペレーティング システムのセキュリティ構成をカスタマイズする必要があります。

#### 最新問題: 124

次の表に示す Azure 仮想マシンを含む Azure サブスクリプションがあります。



Profile1 という名前の MDM セキュリティ ベースライン プロファイルを作成します。

Profile1 を適用できる仮想マシンを特定する必要があります。

どの仮想マシンを識別する必要がありますか？

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

**Answer: A** ([メッセージを残す](#))

説明/参照:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

#### 最新問題: 125

Homepage という名前の Azure SQL データベースの毎週のバックアップを構成する必要があります。バックアップは 8 週間保持する必要があります。

このタスクを完了するには、Azure portal にサインインします。

**Answer:**

Azure SQL データベースのバックアップ ポリシーを構成する必要があります。

Azure portal で、検索ボックスに「Azure SQL Database」と入力し、検索結果から [Azure SQL Database] を選択し、[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 ウィンドウで Azure SQL Database を参照します。

ホームページ データベースをホストしているサーバーを選択し、[バックアップの管理] をクリックします。

「ポリシーの構成」をクリックします。

[毎週のバックアップ] オプションにチェックが入っていることを確認します。

[毎週のバックアップをどのくらいの期間保持しますか] オプションを 8 週間に設定します。

「適用」をクリックして変更を保存します。



### 最新問題: 126

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Azure Security Center を使用して、3 つの Azure サブスクリプションの一元的なポリシー管理を行います。

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 3 つのサブスクリプションすべてにグループとして展開する必要があります。

解決策: リソース グループを範囲とするポリシー 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

<https://www.fast2test.com/AZ-500-practice-test.html> 69

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

**Answer: B (メッセージを残す)**

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 ポリシーを適用する必要があるという問題を解決します。

参照 :

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

### 最新問題: 127

Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。

2019 年 1 月 1 日、Vault1 には次のシークレットが保存されます。

Enabled : False  
Expires :  
NotBefore : 5/1/19 12:00:00 AM  
Created : 12/20/18 2:55:00 PM  
Updated : 12/20/18 2:55:00 PM  
ContentType :  
Tags :  
TagTable :  
VaultName : vault1  
Name : Password1  
Version :  
Id : https://vault1.vault.azure.net:443/secrets/Password1

Enabled : True  
Expires : 5/1/19 12:00:00 AM  
NotBefore : 3/1/19 12:00:00 AM  
Created : 12/20/18 3:00:00 PM  
Updated : 12/20/18 3:00:00 PM  
ContentType :  
Tags :  
TagTable :  
VaultName : vault1  
Name : Password2  
Version :  
Id : https://vault1.vault.azure.net:443/secrets/Password2

アプリケーションで利用できる各シークレットはどれですか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Password1:  ▼

Never  
Always  
Only after May 1, 2019

Password2:  ▼

Never  
Always  
Only between March 1, 2019 and May 1, 2019

Answer:

Microsoft

Password1:  ▼

|                        |
|------------------------|
| Never                  |
| Always                 |
| Only after May 1, 2019 |

Password2:  ▼

|                                            |
|--------------------------------------------|
| Never                                      |
| Always                                     |
| Only between March 1, 2019 and May 1, 2019 |

参照 :

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute>

#### 最新問題: 128

##### シミュレーション

管理者が Azure Resource Manager テンプレートを使用してリソースをデプロイするときに、そのデプロイメントが KV11597200 という名前の Azure Key Vault 内のシークレットにアクセスでき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 portal にサインインします。

**A.** キー コンテナの高度なアクセス ポリシーでオプションを構成する必要があります。

\* Azure portal で、検索ボックスに「Azure Key Vault」と入力し、検索結果から [Azure Key Vault] を選択して、KV11597200 という名前のキー コンテナを選択します。

\* キー コンテナのプロパティで、[高度なアクセス ポリシー] をクリックします。

\* テンプレートのデプロイのために Azure Resource Manager へのアクセスを有効にするというチェックボックスをオンにします。

\* [保存] をクリックして変更を保存します。

**B.** キー コンテナの高度なアクセス ポリシーでオプションを構成する必要があります。

\* Azure portal で、検索ボックスに「Azure Key Vault」と入力し、検索結果から [Azure Key Vault] を選択して、KV11597200 という名前のキー コンテナを選択します。または、左側のナビゲーション ウィンドウで Azure Key Vault を参照します。

\* キー コンテナのプロパティで、[高度なアクセス ポリシー] をクリックします。

\* テンプレートのデプロイのために Azure Resource Manager へのアクセスを有効にするというチェックボックスをオンにします。

\* [保存] をクリックして変更を保存します。

**Answer: B** ([メッセージを残す](#))

#### 最新問題: 129

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。

次の要件を満たすために、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。

\* コストは最小限に抑える必要があります。

各仮想ネットワークにはどの VPN ゲートウェイ (SKU) 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 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります

SKUs

Basic

VpnGw1

VpnGw2

VpnGw3

Answer Area

Microsoft

VNET1:SKU

VNET2:SKU

Answer:

SKUs

Basic

VpnGw1

VpnGw2

VpnGw3

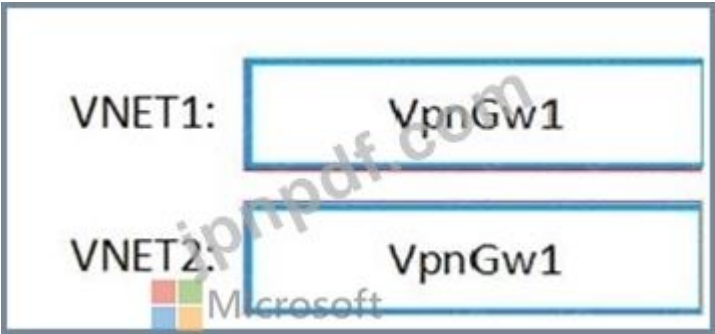
Answer Area

Microsoft

VNET1:VpnGw1

VNET2:VpnGw1

説明



参考文献:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

最新問題: 130

ContosoKey1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。

次の表に示すように、ユーザーを作成し、ロールを割り当てます。

| Name  | Subscription role assignment | ContosoKey1 role assignment |
|-------|------------------------------|-----------------------------|
| User1 | Owner                        | None                        |
| User2 | Security Admin               | None                        |
| User3 | None                         | User Access Administrator   |
| User4 | None                         | Key Vault Contributor       |

どのユーザーが次のアクションを実行できるかを特定する必要があります。

\* ContososKey1 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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Delegate permissions for ContosoKey1: 

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1 and User4 only           |
| User1, User2, and User3 only   |
| User1, User2, User3, and User4 |

Configure network access to ContosoKey1: 

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| User1 and User4 only           |
| User1, User2, and User3 only   |
| User1, User2, User3, and User4 |

Answer:

| Statements                               | Yes                   | No                    |
|------------------------------------------|-----------------------|-----------------------|
| You can start VM1.                       | <input type="radio"/> | <input type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input type="radio"/> |

説明

Delegate permissions for ContosoKey1:

User1 only  
User1 and User2 only  
User1 and User3 only  
User1 and User4 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

Configure network access to ContosoKey1:

User1 only  
User1 and User2 only  
User1 and User3 only  
User1 and User4 only  
User1, User2, and User3 only  
User1, User2, User3, and User4



参照 :  
<https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide>

最新問題: 131

Azure Key Vault を作成する必要があります。このソリューションでは、キー コンテナー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ればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment  
-EnablePurgeProtection  
-Tag

-Confirm  
-DefaultProfile  
-EnableSoftDelete  
-SKU

Answer:

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

 -Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

参照：

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

最新問題: 132

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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、Windows Server 2016 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。

Azure Disk Encryption を使用して VM1 ディスクを暗号化する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area

Answer:

| Actions                                            | Answer Area                                        |
|----------------------------------------------------|----------------------------------------------------|
| Configure secrets for the Azure key vault.         | Create an Azure key vault.                         |
| Create an Azure key vault.                         | Configure access policies for the Azure key vault. |
| Run Set-AzureRmStorageAccount.                     | Run Set-AzureRmVmDiskEncryptionExtension.          |
| Configure access policies for the Azure key vault. |                                                    |
| Run Set-AzureRmVmDiskEncryptionExtension.          |                                                    |

参照：

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

### 最新問題: 133

Azure サブスクリプションをお持ちです。サブスクリプションには、Windows Server 2016 を実行する Azure 仮想マシンが含まれています。各仮想マシンにカスタムのマルウェア対策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ポリシーを実装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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



```

{
  "if" : {
    "allOf": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : " ",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters": {
            " " : {
              "existenceCondition":
              "resources
              template
            }
          }
        }
      }
    }
  }
}

```

Answer:



参考文献:

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

#### 最新問題: 134

contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた 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予定です。

| Name             | Type                    | Description                                                                                                    |
|------------------|-------------------------|----------------------------------------------------------------------------------------------------------------|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database<br>Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1          | Azure web app           | A web app configured to serve as the middle tier of the application                                            |

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 Cosmos DB アカウントにアクセスします。

どのタスクが CosmosDB1 と WebApp1 に実装されるかを特定する必要があります。

各リソースに対してどのタスクを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

CosmosDB1:

▼

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

WebApp1:

▼

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

Answer:

CosmosDB1:

▼

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

WebApp1:

▼

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

参照 :

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

最新問題: 135

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。

各サブスクリプションについて、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。

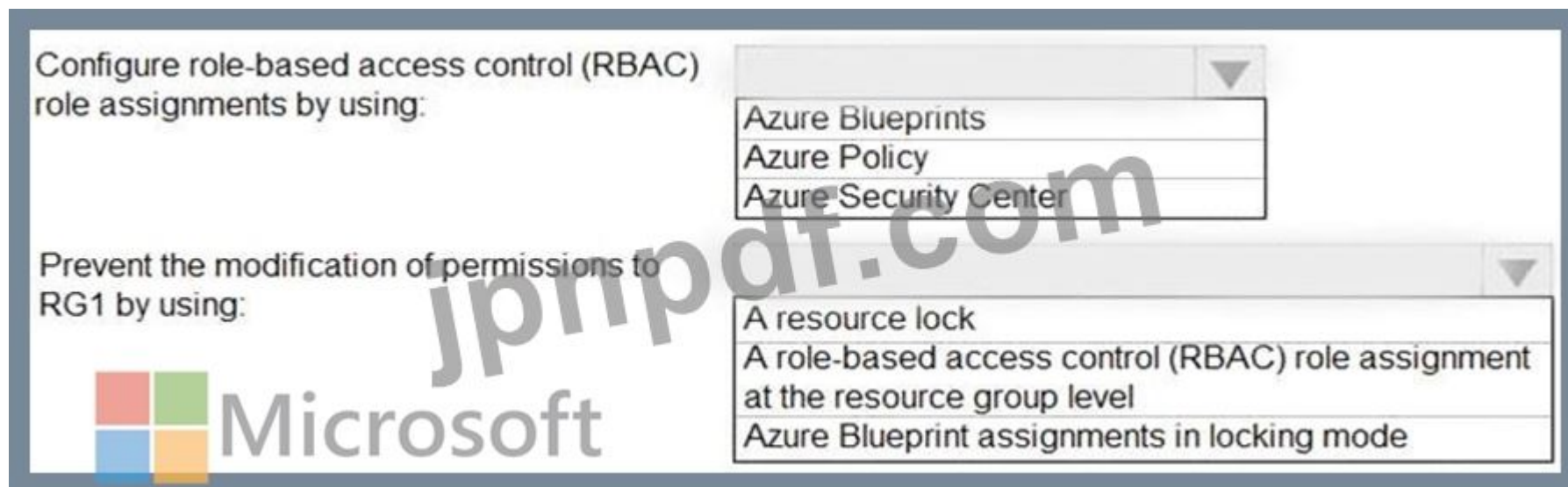
\* Group1 のメンバーには、所有者の役割が割り当てられます。

※RG1に対する権限の変更は禁止されています。

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

注: 正しく選択するたびに 1 ポイントの価値があります。



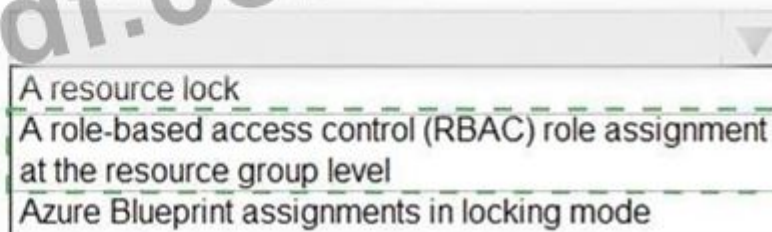


Answer:

Configure role-based access control (RBAC) role assignments by using:



Prevent the modification of permissions to RG1 by using:

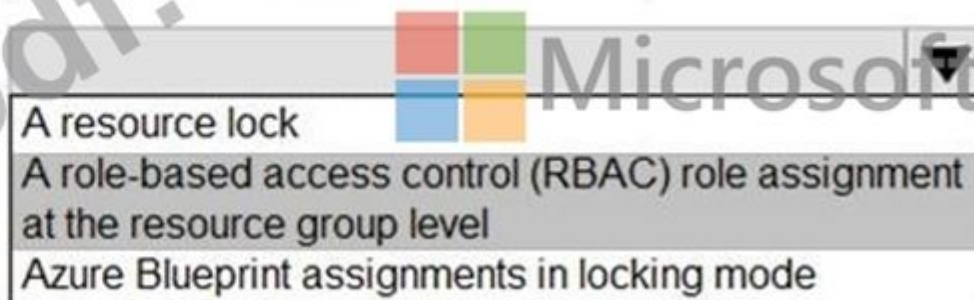


説明

Configure role-based access control (RBAC) role assignments by using:



Prevent the modification of permissions to RG1 by using:



最新問題: 136

cont1 という名前の BLOB コンテナを含む Azure サブスクリプションがあります。Cont1 には、次の図に示すアクセス ポリシーがあります。





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

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

1  
2  
4  
7  
15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

1  
2  
4  
7  
15



Answer:

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

1

2

4

7

15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

1

2

4

7

15

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> (517**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 137

次の表に示すリソース グループを含む Sub1 という名前の Azure サブスクリプションがあります。

| Name | Location |
|------|----------|
| RG1  | West US  |
| RG2  | East US  |

次の例に示す Azure Policy 定義を作成します。

```
Microsoft
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourcegroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

ポリシーを Sub1 に割り当てます。  
次の表に示すリソースを作成する予定です。

| Name      | Type              | Location | Resource group |
|-----------|-------------------|----------|----------------|
| IPobject1 | Public IP address | East US  | RG2            |
| obj1      | Resource group    | West US  | Not applicable |
| OBJ3      | Virtual network   | West US  | RG1            |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

| Statements                | Yes                   | No                    |
|---------------------------|-----------------------|-----------------------|
| You can create IPobject1. | <input type="radio"/> | <input type="radio"/> |
| You can create obj1.      | <input type="radio"/> | <input type="radio"/> |
| You can create OBJ3.      | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                | Yes                   | No                                  |
|---------------------------|-----------------------|-------------------------------------|
| You can create IPobject1. | <input type="radio"/> | <input checked="" type="checkbox"/> |
| You can create obj1.      | <input type="radio"/> | <input checked="" type="checkbox"/> |
| You can create OBJ3.      | <input type="radio"/> | <input checked="" type="checkbox"/> |

最新問題: 138

Contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられている、Sub 1 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ます。

| Name  | Role                   |
|-------|------------------------|
| User1 | Global administrator   |
| User2 | Security administrator |
| User3 | Security reader        |
| User4 | License administrator  |

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。

オンボードを計画し、Azure AD ID Protection を構成します。

Azure AD Identity Protection をオンボードし、ユーザーを修復し、ポリシーを構成できるのはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります

ANSWER AREA

Microsoft

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

Answer:

Microsoft

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

説明



Users who can onboard Azure AD Identity Protection:

▼

User1 only  
User1 and User2 only  
User1, User2, and User3 only  
User1, User2, User3, and User4 only

Users who can remediate users and configure policies:

▼

User1 and User2 only  
User1 and User3 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

Microsoft

最新問題: 139

次の表に示すリソースが含まれる Subscription1 という名前の Azure サブスクリプションがあります。

| Name      | Type                            | Description                                                             |
|-----------|---------------------------------|-------------------------------------------------------------------------|
| EventHub1 | Azure Event Hubs                | Not applicable                                                          |
| Adf1      | Azure Data Factory              | Not applicable                                                          |
| NVA1      | Network virtual appliance (NVA) | The NVA sends security event messages in the Common Event Format (CEF). |

次のリソースを含む Subscription2 という名前の Azure サブスクリプションがあります。

Azure Sentinel ワークスペース

Azure Event Grid インスタンス

CEF メッセージを NVA から Azure Sentinel に取り込む必要があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Subscription1: An Azure Log Analytics agent on a Linux virtual machine  
A Data Factory pipeline  
An Event Hubs namespace  
An Azure Service Bus queue

Subscription2: A new Azure Log Analytics workspace  
A new Azure Sentinel data connector  
A new Azure Sentinel playbook  
A new Event Grid resource provider

Answer:

Answer Area

Subscription1: An Azure Log Analytics agent on a Linux virtual machine  
A Data Factory pipeline  
An Event Hubs namespace  
An Azure Service Bus queue

Subscription2: A new Azure Log Analytics workspace  
A new Azure Sentinel data connector  
A new Azure Sentinel playbook  
A new Event Grid resource provider

最新問題: 140

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

Windows Server 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。  
システム更新評価ソリューションを LAW1 に追加する予定です。  
システム更新評価関連のログが 100 台の仮想マシンのみから LAW1 にアップロードされるようにする必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                        | Answer Area |
|------------------------------------------------|-------------|
| Create a new workspace.                        |             |
| Apply the scope configuration to the solution. |             |
| Create a scope configuration.                  |             |
| Create a computer group.                       |             |
| Create a data source.                          |             |

Answer:

| Actions                                        | Answer Area                                    |
|------------------------------------------------|------------------------------------------------|
| Create a new workspace.                        | Create a computer group.                       |
| Apply the scope configuration to the solution. | Create a scope configuration.                  |
| Create a scope configuration.                  | Apply the scope configuration to the solution. |
| Create a computer group.                       |                                                |
| Create a data source.                          |                                                |

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

最新問題: 141

1 つの Azure Active Directory (Azure AD) テナントにリンクされた 5 つの Azure サブスクリプションがあります。  
SecurityPolicyInitiative1 という名前の Azure Policy イニシアチブを作成します。

すべての新しいリソース グループでどの標準的な役割の割り当てを構成する必要があるかを特定します。  
新しいリソース グループの作成時に、SecurityPolicyInitiative1 とロールの割り当てを適用する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

Create a custom role-based access control (RBAC) role.

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

⏪

⏩

Answer Area

⏴

⏵

Answer:

Answer Area

Create an Azure Blueprints definition.

publish an Azure Blueprints version

Assign an Azure blueprint.

- 1 - Azure Blueprints 定義を作成します。
- 2 - Azure Blueprints バージョンを公開する
- 3 - Azure ブループリントを割り当てます。

参照 :

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

最新問題: 142

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。



| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

次の表に示すリソース ロックを作成します。

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Microsoft

Statements

Yes

No

You can start VM1.

☐

☐

You can start VM2.

☐

☐

You can create a virtual machine in RG2.

☐

☐

Answer:

Microsoft

Statements

Yes

No

You can start VM1.

☐

☒

You can start VM2.

☐

☒

You can create a virtual machine in RG2.

☐

☒

説明  
いいえ  
いいえ  
いいえ



1.) 次のスコープがロックされているため、書き込み操作を実行できません:

「subscriptions/xxxx/resourceGroups/xxx」ロックを解除して、もう一度お試しください。

2.) 読み取り専用ロックを持つリソース グループに VM を作成すると、エラーが表示されます。

「選択されたリソース グループは読み取り専用です」

3.) 読み取り専用ロックのため、マシンの起動後にロックが追加されると、仮想マシンは起動または停止できません。(このユースケースの一部ではありませんが、知っておくと良いでしょう。

回答で参照されている記事は、ブループリントに範囲が限定されているため、異なると述べています。

[リソースのロック] ページには、VM の起動に関して次のことが記載されています。

「仮想マシンを含むリソース グループに対する読み取り専用ロックにより、すべてのユーザーが仮想マシンを起動または再起動できなくなります。これらの操作には POST リクエストが必要です。」

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

#### 最新問題: 143

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

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

- \* log を 2 年間保持します。

- \* Kusto クエリ言語を使用してログをクエリする

- \* 管理労力を最小限に抑えます。

ログはどこに保存すればよいでしょうか？

**A.** Azure Log Analytics ワークスペース

**B.** Azure イベント ハブ

**C.** Azure ストレージ アカウント

**Answer: A** ([メッセージを残す](#))

説明

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

#### 最新問題: 144

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

サブスクリプションで Azure サービスの監視を計画しています。

次の詳細を取得する必要があります。

- \* 3 週間前に仮想マシンを削除したユーザーを特定します。

- \* Windows Server 2016 を実行する仮想マシンのセキュリティ イベントをクエリします。

Azure Monitor では何を使用する必要がありますか？ 回答するには、適切な構成設定を正しい詳細にドラッグします。各構成設定は、1 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります。

| Settings       | Answer Area                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------|
| Activity log   |                                                                                                    |
| Logs           | Identify the user who deleted a virtual machine three weeks ago: <input type="text"/>              |
| Metrics        | Query the security events of a virtual machine that runs Windows Server 2016: <input type="text"/> |
| Service Health |                                                                                                    |

Answer:

| Settings       | Answer Area                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| Activity log   |                                                                                                                 |
| Logs           | Identify the user who deleted a virtual machine three weeks ago: <input type="text" value="Activity log"/>      |
| Metrics        | Query the security events of a virtual machine that runs Windows Server 2016: <input type="text" value="Logs"/> |
| Service Health |                                                                                                                 |

Explanation:

ボックス 1: アクティビティ ログ

Azure アクティビティ ログは、サブスクリプション内のリソースに対して実行された操作に関する洞察を提供します。アクティビティ ログは、サブスクリプションのコントロール プレーン イベントを報告するため、以前は「監査ログ」または「操作ログ」と呼ばれていました。アクティビティ ログは、書き込み操作 (つまり、PUT、POST、または DELETE) を「何を、誰が、いつ」行ったかを判断するのに役立ちます。

ボックス 2: ログ

ログ統合は、Windows 仮想マシン、Azure アクティビティ ログ、Azure Security Center アラート、および Azure リソース プロバイダー ログから Azure 診断を収集します。この統合により、オンプレミスかクラウドかに関係なく、すべての資産に統合されたダッシュボードが提供されるため、セキュリティ イベントの集計、関連付け、分析、アラートを行うことができます。

参考文献:

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

最新問題: 145

Sub1 という名前の Azure サブスクリプションがあります。

Azure Security Center には、Play1 という名前のセキュリティ プレイブックがあります。Play1 は、User1 という名前のユーザーに電子メール メッセージを送信するように構成されています。

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

Play1を変更するには何を使用する必要がありますか？

A. Azure DevOps

- B. Azure Application Insights
  - C. Azure モニター
  - D. Azure Logic Apps デザイナー
- Answer: D (メッセージを残す)

説明

Security Center で既存のプレイブックを変更して、アクションまたは条件を追加できます。これを行うには、[プレイブック] タブで変更するプレイブックの名前をクリックするだけで、ロジック アプリ デザイナーが開きます。

参考文献:

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

最新問題: 146

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。

| Name    | Type                         | Attached to    | NSG            |
|---------|------------------------------|----------------|----------------|
| NSG1    | Network security group (NSG) | VM5            | Not applicable |
| NSG2    | Network security group (NSG) | Subnet1        | Not applicable |
| Subnet1 | Subnet                       | Not applicable | Not applicable |
| VM5     | Virtual machine              | Subnet1        | NSG1           |

IP アドレス 10.1.0.4 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。

### JIT VM access configuration

VM5

+ Add

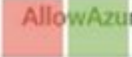
Save

Discard

Configure the ports for which the just-in-time VM access will be applicable

| Port | Protocol | Allowed source IPs | IP range | Time range (hours) |     |
|------|----------|--------------------|----------|--------------------|-----|
| 3389 | Any      | Per request        | N/A      | 3 hours            | ... |

VM5 の JIT VM アクセスを有効にします。  
NSG1 には、次の図に示す受信ルールがあります。

| Priority | Name                                                                                                          | Port | Protocol | Source            | Destination    | Action                                                                                    |
|----------|---------------------------------------------------------------------------------------------------------------|------|----------|-------------------|----------------|-------------------------------------------------------------------------------------------|
| 100      |  SecurityCenter-JITRule-...  | 3389 | Any      | Any               | 10.1.0.4       |  Allow |
| 1000     | SecurityCenter-JITRule_341...                                                                                 | 3389 | Any      | Any               | 10.1.0.4       |  Deny  |
| 1001     | RDP                                                                                                           | 3389 | TCP      | Any               | Any            |  Allow |
| 65000    | AllowVnetInBound                                                                                              | Any  | Any      | VirtualNetwork    | VirtualNetwork |  Allow |
| 65001    |  AllowAzureLoadBalancerIn... | Any  | Any      | AzureLoadBalancer | Any            |  Allow |
| 65500    |  DenyAllInBound              | Any  | Any      | Any               | Any            |  Deny  |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                         | Yes                   | No                    |
|----------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input type="radio"/> | <input type="radio"/> |
| Remote Desktop access to VM5 is blocked.                                                           | <input type="radio"/> | <input type="radio"/> |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.                  | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                         | Yes                              | No                               |
|----------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Remote Desktop access to VM5 is blocked.                                                           | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.                  | <input type="radio"/>            | <input checked="" type="radio"/> |

最新問題: 147

あなたは、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。

| Name    | IP address space |
|---------|------------------|
| Boston  | 180.15.10.0/24   |
| Seattle | 132.32.15.0/24   |

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ます。

| Name  | User device | Last sign-in | During last sign-in, user selected<br>Don't ask again for 14 days |
|-------|-------------|--------------|-------------------------------------------------------------------|
| User1 | Device1     | June 1       | Yes                                                               |
| User2 | Device2     | June 3       | No                                                                |



contoso.com の多要素設定は、次のように構成されています。

multi-factor authentication

users

service settings

app passowrds

[\(learn more\)](#)

☒

Allow users to create app paswords to sign in to non-browser apps

☐

Do not allow users to create app passwords to sign in to non-browser apps

trusted ips

[\(learn more\)](#)

☐

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

verification options

[\(learn more\)](#)

Methods available to users:

☐

call to phone

☒

Text message to phone

☒

Notification through mobile app

☒

Verification code from mobile app or hardware token

remember multi-factor authentication

[\(learn more\)](#)

☒

Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 

14

Microsoft

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                                   | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.        | <input type="radio"/> | <input type="radio"/> |
| When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.          | <input type="radio"/> | <input type="radio"/> |
| When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                                   | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.        | <input type="radio"/>            | <input checked="" type="radio"/> |
| When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.          | <input checked="" type="radio"/> | <input type="radio"/>            |
| When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 148

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

| Name  | Member of      | Multi-factor authentication (MFA) status |
|-------|----------------|------------------------------------------|
| User1 | Group1, Group2 | Disabled                                 |
| User2 | Group2         | Disabled                                 |

テナントには、次の表に示す名前付きの場所が含まれています。

| Name    | IP address range | Trusted location |
|---------|------------------|------------------|
| Seattle | 193.77.10.0/24   | Yes              |
| Boston  | 154.12.18.0/24   | No               |

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

| Name    | Include | Exclude | Condition               | Grant                                             |
|---------|---------|---------|-------------------------|---------------------------------------------------|
| Policy1 | Group1  | Group2  | Locations: Boston       | Block access                                      |
| Policy2 | Group1  | None    | Locations: Any location | Grant access, Require multi-factor authentication |
| Policy3 | Group2  | Group1  | Locations: Boston       | Block access                                      |
| Policy4 | User2   | None    | Locations: Any location | Grant access, Require multi-factor authentication |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Microsoft

Statements

Yes

No

|                                                           |                       |                       |
|-----------------------------------------------------------|-----------------------|-----------------------|
| User1 can access App1 from an IP address of 154.12.18.10. | <input type="radio"/> | <input type="radio"/> |
| User2 can access App1 from an IP address of 193.77.10.15. | <input type="radio"/> | <input type="radio"/> |
| User2 can access App1 from an IP address of 154.12.18.34. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

Microsoft

Statements

Yes

No

|                                                           |                                  |                                  |
|-----------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can access App1 from an IP address of 154.12.18.10. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can access App1 from an IP address of 193.77.10.15. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can access App1 from an IP address of 154.12.18.34. | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

Microsoft

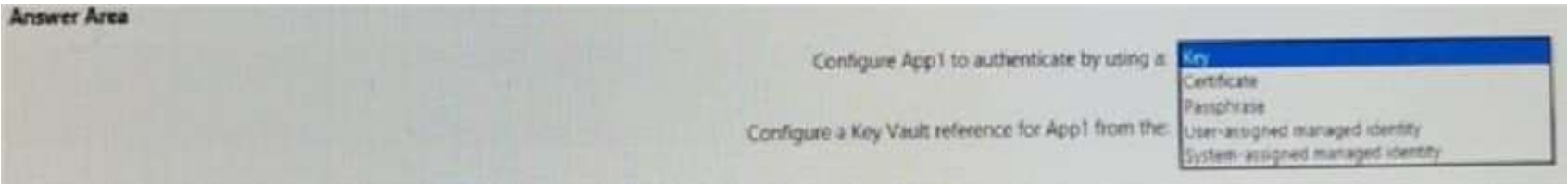
Statements

Yes

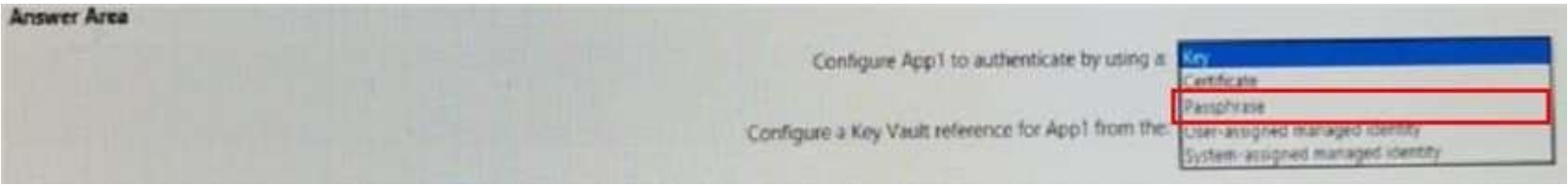
No

|                                                           |                                  |                                  |
|-----------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can access App1 from an IP address of 154.12.18.10. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can access App1 from an IP address of 193.77.10.15. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can access App1 from an IP address of 154.12.18.34. | <input type="radio"/>            | <input checked="" type="radio"/> |

Wen App App1 と Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。  
Vault1 にシークレットを保存してアクセスできるように App1 を構成する必要があります。  
App1 をどのように構成すればよいでしょうか？ 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: 正しく選択するたびに 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 Azure Active Directory (Azure AD) テナントがあります。

| Name  | Member of      | Multi-factor authentication (MFA) status |
|-------|----------------|------------------------------------------|
| User1 | Group1, Group2 | Disabled                                 |
| User2 | Group2         | Disabled                                 |

テナントには、次の表に示す名前付きの場所が含まれています。

| Name    | IP address range | Trusted location |
|---------|------------------|------------------|
| Seattle | 193.77.10.0/24   | Yes              |
| Boston  | 154.12.18.0/24   | No               |

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

| Name    | Include | Exclude | Condition               | Grant                                             |
|---------|---------|---------|-------------------------|---------------------------------------------------|
| Policy1 | Group1  | Group2  | Locations: Boston       | Block access                                      |
| Policy2 | Group1  | None    | Locations: Any location | Grant access, Require multi-factor authentication |
| Policy3 | Group2  | Group1  | Locations: Boston       | Block access                                      |
| Policy4 | User2   | None    | Locations: Any location | Grant access, Require multi-factor authentication |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



Answer Area

Microsoft

Statements

Yes

No

User1 can access App1 from an IP address of 154.12.18.10.

☐

☐

User2 can access App1 from an IP address of 193.77.10.15.

☐

☐

User2 can access App1 from an IP address of 154.12.18.34.

☐

☐

Answer:

Answer Area

Microsoft

Statements

Yes

No

User1 can access App1 from an IP address of 154.12.18.10.

☐

☒

User2 can access App1 from an IP address of 193.77.10.15.

☒

☐

User2 can access App1 from an IP address of 154.12.18.34.

☐

☒

説明

Microsoft

Statements

Yes

No

User1 can access App1 from an IP address of 154.12.18.10.

☐

☒

User2 can access App1 from an IP address of 193.77.10.15.

☒

☐

User2 can access App1 from an IP address of 154.12.18.34.

☐

☒

最新問題: 151

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。

| Name | Connected to  | Private IP address | Public IP address |
|------|---------------|--------------------|-------------------|
| VM1  | VNET1/Subnet1 | 10.1.1.4           | 13.80.73.87       |
| VM2  | VNET2/Subnet2 | 10.2.1.4           | 213.199.133.190   |
| VM3  | VNET2/Subnet2 | 10.2.1.5           | None              |

Subnet1 と Subnet2 には Microsoft.Storage サービス エンドポイントが構成されています。  
storageacc1 という名前の Azure ストレージ アカウントがあり、次のように構成されています。

Save Discard Refresh

Allow access from  

All networks Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks  
Secure your storage account with virtual networks. [+ Add existing virtual network](#)  
[+ Add new virtual network](#)

| VIRTUAL NETWORK      | SUBNET | ADDRESS RANGE | ENDPOINT STATUS | RESOURCE GROUP | SUBSCRIPTION |
|----------------------|--------|---------------|-----------------|----------------|--------------|
| No network selected. |        |               |                 |                |              |

Firewall  
Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87

IP address or CIDR

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ

☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network

次の各ステートメントについて、そのステートメントが 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。

| Statements                                       | Yes                   | No                    |
|--------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can upload a blob to storageacc1.  | <input type="radio"/> | <input type="radio"/> |
| From VM2, you can upload a blob to storageacc1.  | <input type="radio"/> | <input type="radio"/> |
| From VM3 , you can upload a blob to storageacc1. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                       | Yes                              | No                               |
|--------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can upload a blob to storageacc1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM2, you can upload a blob to storageacc1.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM3 , you can upload a blob to storageacc1. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

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> (51730%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 152

次の表に示す Azure 仮想マシンがあります。

| Name | Operating system             | Region      | Resource group |
|------|------------------------------|-------------|----------------|
| VM1  | Windows Server 2012          | East US     | RG1            |
| VM2  | Windows Server 2012 R2       | West Europe | RG1            |
| VM3  | Windows Server 2016          | West Europe | RG2            |
| VM4  | Red Hat Enterprise Linux 7.4 | East US     | RG2            |

米国東部リージョンの RG1 に Analytics1 という名前の Azure Log Analytics ワークスペースを作成します。どの仮想マシンを Analytics1 に登録できますか？

- A. VM1のみ
- B. VM1、VM2、VM3 のみ
- C. VM1、VM2、VM3、VM4
- D. VM1 と VM4 のみ

**Answer: A** ([メッセージを残す](#))

注: ワークスペースを作成する

\* Azure portal で、[すべてのサービス] をクリックします。リソースのリストに [Log Analytics]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ー処理されます。[ログ分析] を選択します。

\* [作成] をクリックし、次の項目の選択肢を選択します。

新しい Log Analytics ワークスペースの名前を指定します (DefaultLAWorkspace など)。OMS ワークスペースは、Log Analytics ワークスペースと呼ばれるようになりました。

選択されているデフォルトが適切でない場合は、ドロップダウン リストから選択してリンク先のサブスクリプションを選択します。

[リソース グループ] には、1 つ以上の Azure 仮想マシンを含む既存のリソース グループを選択します。

VM がデプロイされる場所を選択します。詳細については、「Log Analytics がどのリージョンであるか」を参照してください。

<https://www.fast2test.com/AZ-500-practice-test.html> 47

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題  
で利用可能です。

不正解:

B、C: Log Analytics ワークスペースは、データ ストレージの地理的な場所を提供します。VM2 と VM3 は別の場所にあります。

D: VM4 は別のリソース グループです。

参考文献:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

最新問題: 153

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. グループ1を削除します。グループ タイプが Office 365 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 [割り当て済み] 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。

新しいグループを Group1 に追加します。

Answer: ([解答を表示する](#))

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については、個別のメンバーのみを追加できます。

シナリオ :

Litware は、次の ID およびアクセス要件を特定します。すべてのサンフランシスコ 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:

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |

参考文献:

<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> ID とアクセスの管理

Testlet 2 のケース 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時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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、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なら、**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 つの支社を構える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。どちらのサブスクリプションも、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。

| Name  | City     | Role                            |
|-------|----------|---------------------------------|
| User1 | Montreal | Global administrator            |
| User2 | MONTREAL | Security administrator          |
| User3 | London   | Privileged role administrator   |
| User4 | Ontario  | Application administrator       |
| User5 | Seattle  | Cloud application administrator |
| User6 | Seattle  | User administrator              |
| User7 | Sydney   | Reports reader                  |
| User8 | Sydney   | None                            |
| User9 | Sydney   | Owner                           |

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。

| Name   | Membership type | Dynamic membership rule  |
|--------|-----------------|--------------------------|
| Group1 | Dynamic user    | user.city -contains "ON" |
| Group2 | Dynamic user    | user.city -match "*on"   |

サブ1

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。

| Name  | Resource group |
|-------|----------------|
| VNET1 | RG1            |
| VNET2 | RG2            |
| VNET3 | RG3            |
| VNET4 | RG4            |

Sub1 には、次の表に示すロックが含まれています。

| Name  | Set on | Lock type |
|-------|--------|-----------|
| Lock1 | RG1    | Delete    |
| Lock2 | RG2    | Read-only |
| Lock3 | RG3    | Delete    |
| Lock4 | RG3    | Read-only |

Sub1 には、次の表に示す Azure ポリシーが含まれています。

| Policy definition          | Resource type                          | Scope |
|----------------------------|----------------------------------------|-------|
| Allowed resource types     | networkSecurityGroups                  | RG4   |
| Not allowed resource types | virtualNetworks/subnets                | RG5   |
| Not allowed resource types | networkSecurityGroups                  | RG5   |
| Not allowed resource types | virtualNetworks/virtualNetworkPeerings | RG6   |

サブ2

Sub2 には、次の表に示す仮想ネットワークが含まれます。

| Name      | Subnet                           |
|-----------|----------------------------------|
| VNetwork1 | Subnet11, Subnet12, and Subnet13 |
| VNetwork2 | Subnet21                         |

Sub2 には、次の表に示す仮想マシンが含まれています。

| Name | Network interface | Application security group | Connected to |
|------|-------------------|----------------------------|--------------|
| VM1  | NIC1              | ASG1                       | Subnet11     |
| VM2  | NIC2              | ASG2                       | Subnet11     |
| VM3  | NIC3              | None                       | Subnet12     |
| VM4  | NIC4              | ASG1                       | Subnet13     |
| VM5  | NIC5              | None                       | Subnet21     |

すべての仮想マシンにはパブリック IP アドレスがあり、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では、ping リクエストと Web リクエストが許可されます。

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。



| Name | Associated to |
|------|---------------|
| NSG1 | NIC2          |
| NSG2 | Subnet11      |
| NSG3 | Subnet13      |
| NSG4 | Subnet21      |

NSG1 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG2 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | 80   | TCP      | Internet          | VirtualNetwork | Allow  |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG3 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | Any  | TCP      | ASG1              | ASG1           | Allow  |
| 150      | Any  | Any      | ASG2              | VirtualNetwork | Allow  |
| 200      | Any  | Any      | Any               | Any            | Deny   |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG4 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | Any  | Any      | Any               | Any            | Allow  |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG1、NSG2、NSG3、および NSG4 には、次の表に示す送信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source         | Destination    | Action |
|----------|------|----------|----------------|----------------|--------|
| 65000    | Any  | Any      | VirtualNetwork | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | Any            | Internet       | Allow  |
| 65500    | Any  | Any      | Any            | Any            | Deny   |

技術的要件

Contoso は次の技術要件を特定します。

- \* Azure Firewall を Sub2 の VNetwork1 にデプロイします。
- \* App2 という名前のアプリケーションを contoso.com に登録します。

\* 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 Azure AD Privileged Identity Management (PIM) を有効にします。

#### 最新問題: 154

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。

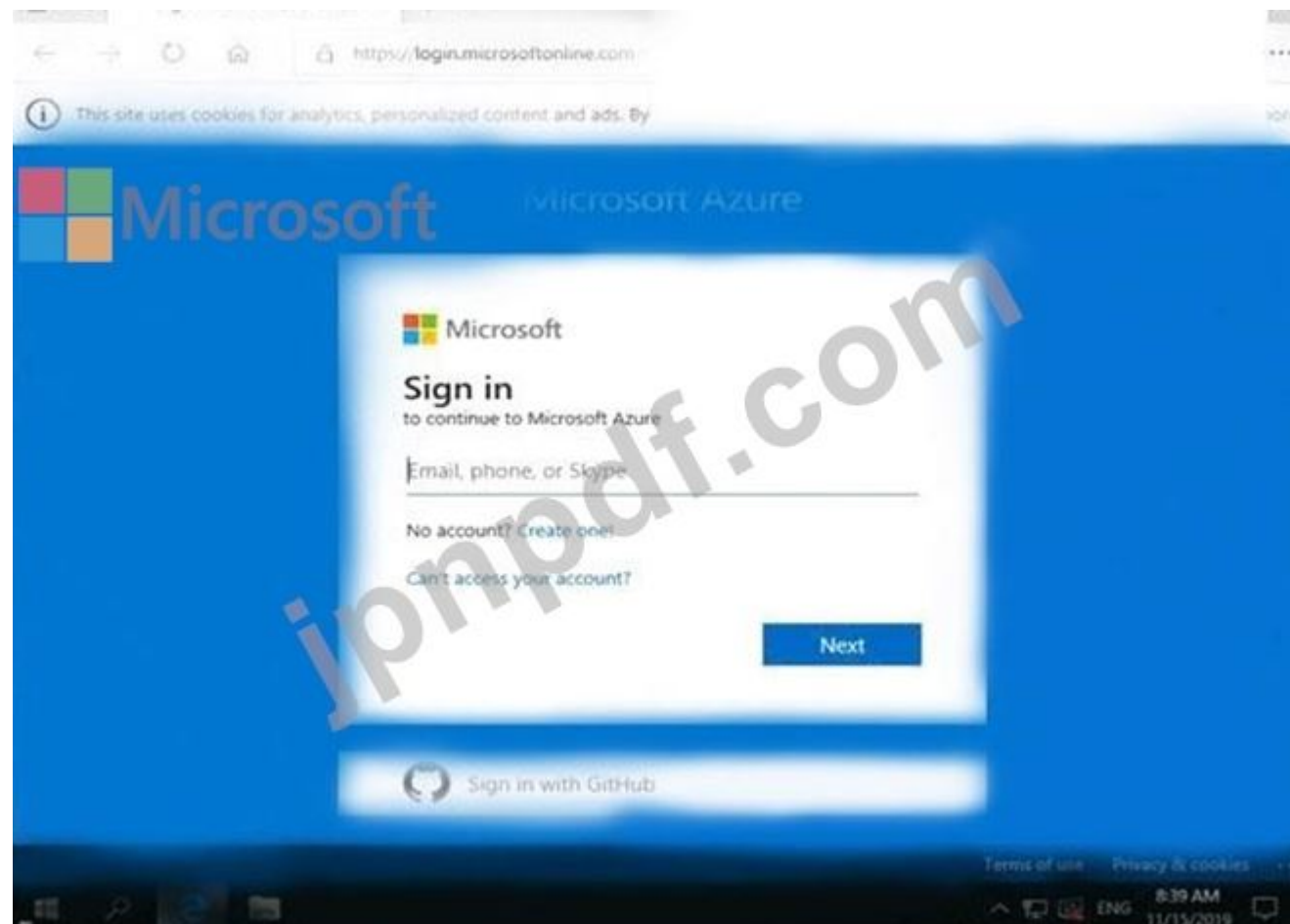
パスワードを入力するには、「パスワードの入力」ボックスにカーソルを置き、下のパスワードをクリックします。

Azure ユーザー名: User1-10598168@ExamUsers.com

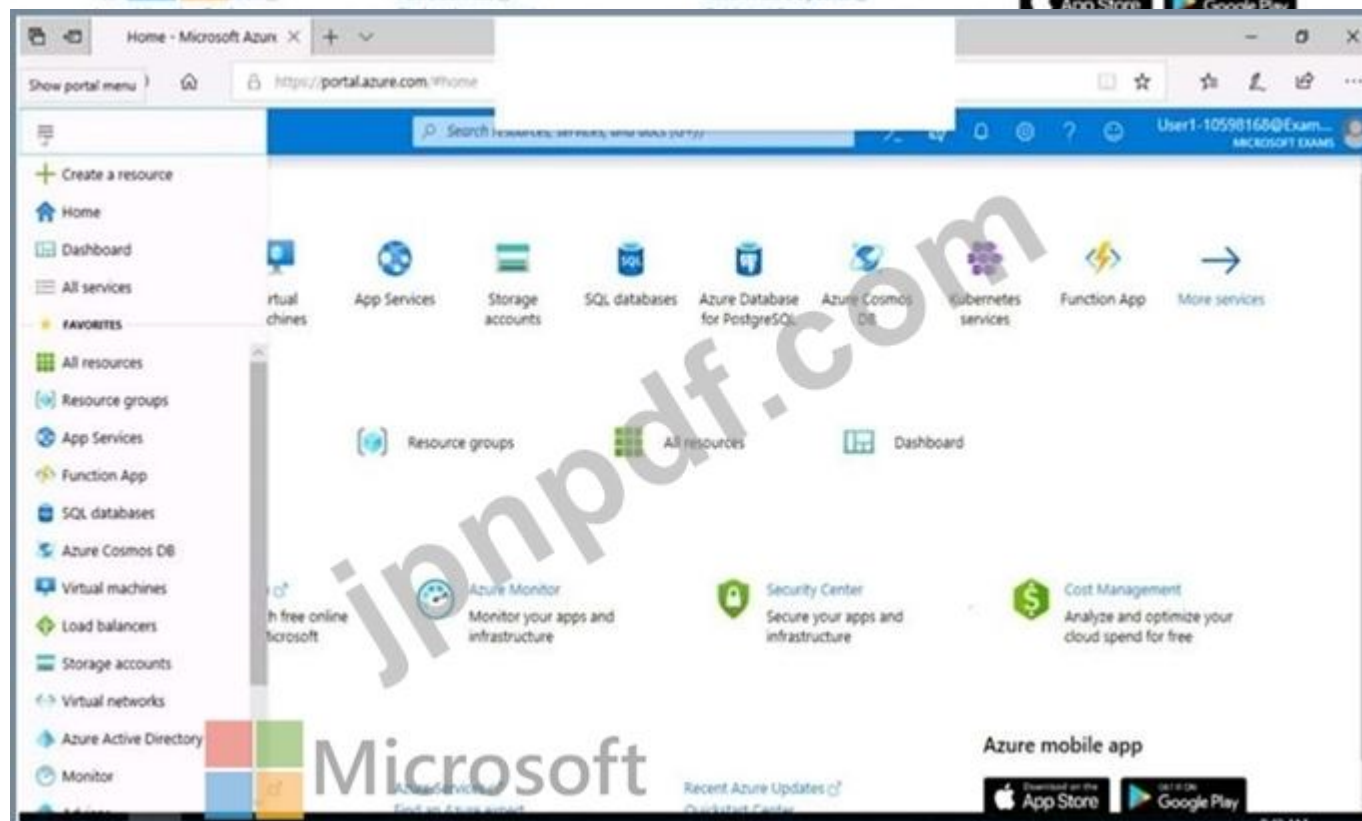
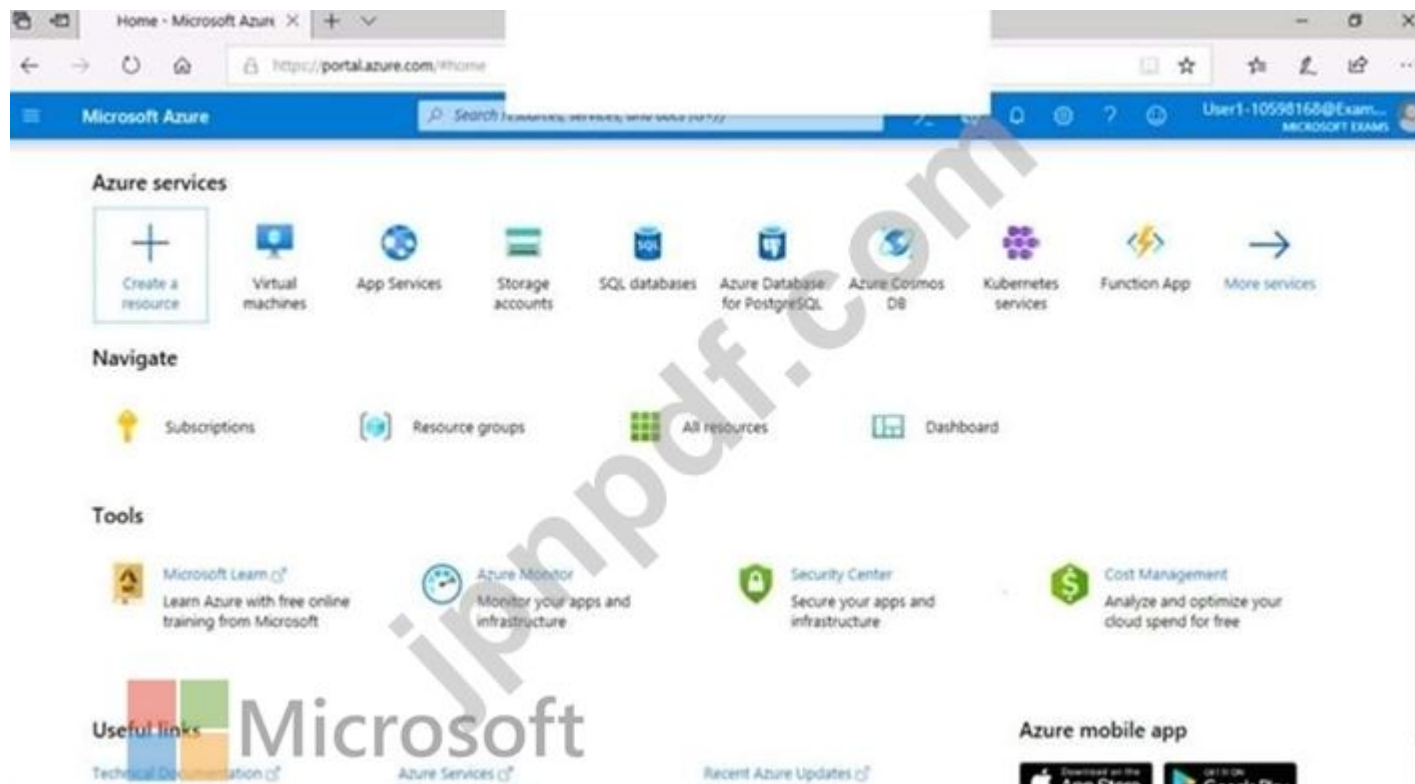
Azure パスワード: Ag1Bh9!#Bd

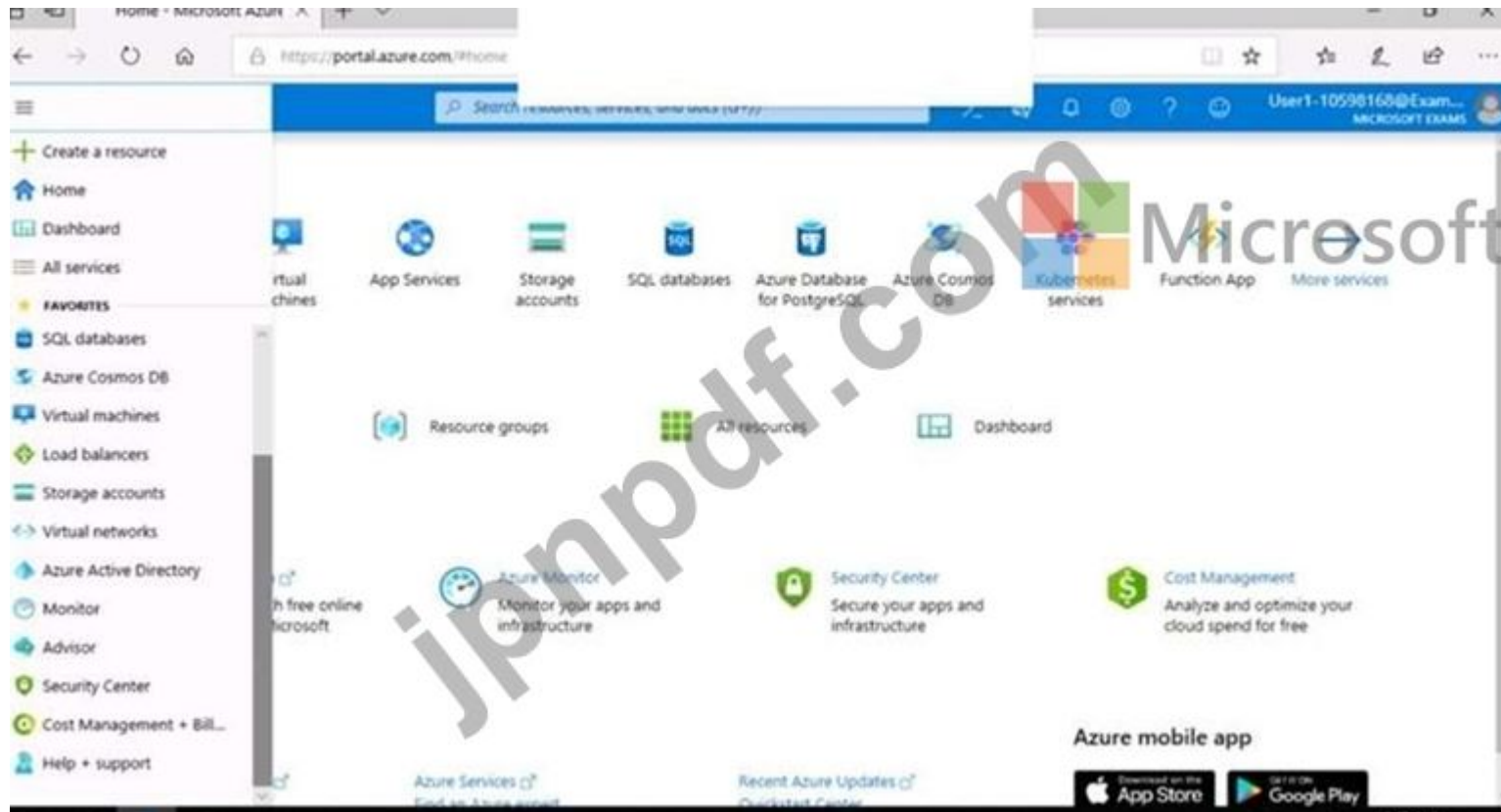
次の情報は、テクニカル サポートのみを目的としています。

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% を超えた場合は、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 portal 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 portal を使用してメトリックに対するアラート 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ごとに若干異なる場合があります。
3. [メトリック アラートの追加 (クラシック)] ボタンを選択し、以下のようにフィールドに入力し、[OK] をクリックします。

メトリック: CPU の割合

条件: 以上

期間: 最後の 15 分以上

通知方法: 電子メール

追加の管理者の電子メール: admin1@contoso.com

Condition

Greater than

\* Threshold

60

Period

Over the last 5 minutes

Notify via

Email owners, contributors, and readers

Additional administrator email(s)

admin@contoso.com

Webhook

http://www.contoso.com/dowork?param

参照：

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

### 最新問題: 155

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                 | Yes                   | No                    |
|----------------------------------------------------------------------------|-----------------------|-----------------------|
| From the Internet, you can connect to the web server on VM1 by using HTTP. | <input type="radio"/> | <input type="radio"/> |
| From the Internet, you can connect to the web server on VM2 by using HTTP. | <input type="radio"/> | <input type="radio"/> |
| From the Internet, you can connect to the web server on VM3 by using HTTP. | <input type="radio"/> | <input type="radio"/> |

Answer:



Microsoft

Statements

From the Internet, you can connect to the web server on VM1 by using HTTP.

From the Internet, you can connect to the web server on VM2 by using HTTP.

From the Internet, you can connect to the web server on VM3 by using HTTP.

Yes

☒

No

☐☐☒☒☐

最新問題: 156

次の表に示すように、East US2 リージョンに 2 つの Azure 仮想マシンがあります。

| Name | Operating system       | Type | Tier     |
|------|------------------------|------|----------|
| VM1  | Windows Server 2008 R2 | A3   | Basic    |
| VM2  | Ubuntu 16.04-DAILY-LTS | L4s  | Standard |

Azure Key Vault をデプロイして構成します。

VM1 と VM2 で Azure Disk Encryption 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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

VM1:

▼

The operating system version

The tier

The type

VM2:

▼

The operating system version

The tier

The type

Answer:



VM1:

▼

The operating system version

The tier

The type

Microsoft

VM2:

▼

The operating system version

The tier

The type

説明

VM1:

▼

The operating system version

The tier

The type

Microsoft

VM2:

▼

The operating system version

The tier

The type

VM1: 階層

階層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 IaaS VM のディスク暗号化は、Standard VM および Azure Premium Storage を備えた VM のすべての Azure パブリック リージョンと Azure Government リージョン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 IaaS VM 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: Ubuntu 16.04 がサポートされています。

参考文献:

<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](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)

最新問題: 157

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。

| Name     | Type                |
|----------|---------------------|
| storage1 | Azure Blob storage  |
| storage2 | Azure Files SMB     |
| storage3 | Azure Table storage |

認証アクセスを構成する必要があります。

各ストレージ アカウントにどの承認の種類を使用できますか? 回答するには、回答エリアで適切な選択肢を選択してください。注 正しい選択肢はそれぞれ 1 ポイントの価値があります。

Answer:

storage1:

Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

Shared Key only

storage3:

Shared access signature (SAS) only

最新問題: 158

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/> | <input type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can connect to the web server on VM4.                | <input type="radio"/> | <input type="radio"/> |

| Statements                                                 | Yes                   | No                    |
|------------------------------------------------------------|-----------------------|-----------------------|
| On May 15, 2019, User1 can activate the Contributor role.  | <input type="radio"/> | <input type="radio"/> |
| On May 15, 2019, User2 can use the Contributor role.       | <input type="radio"/> | <input type="radio"/> |
| On June 15, 2019, User3 can activate the Contributor role. | <input type="radio"/> | <input type="radio"/> |

説明

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can connect to the web server on VM4.                | <input checked="" type="radio"/> | <input type="radio"/>            |

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 のみを許可しますが、ASG1 からの ICMP ping は許可しません。ASG1 からは TCP トラフィックのみが許可されます。

NSG3 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | Any  | TCP      | ASG1              | ASG1           | Allow  |
| 150      | Any  | Any      | ASG2              | VirtualNetwork | Allow  |
| 200      | Any  | Any      | Any               | Any            | Deny   |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

ボックス 2: はい。

VM2 は ASG2 にあります。ASG2 からは任意のプロトコルが許可されるため、ICMP ping が許可されます。

ボックス3。VM1 は ASG1 にあります。ASG1 からの TCP トラフィックが許可されるため、Web サーバーへの接続はポート TCP 80 または TCP 443 上で行われるため、VM1 は Web サーバーに接続できます。

#### 最新問題: 159

Azure Key Vault を作成する必要があります。このソリューションでは、キー コンテナー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ればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

Answer:

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

参照 :

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

最新問題: 160

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

| Name  | Member of      | Multi-factor authentication (MFA) status |
|-------|----------------|------------------------------------------|
| User1 | Group1, Group2 | Enabled                                  |
| User2 | Group1         | Disabled                                 |
| User3 | Group1         | Disabled                                 |

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

\* 割り当て: Group1 を含み、Group2 を除く

※条件 :サインイン危険度 : 中以上

\* アクセス アクセスを許可、多要素認証が必要

ユーザーが Azure AD にサインインするときに何が起きるかを特定する必要があります。

各ユーザーについて何を識別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: 正しく選択するたびに 1 ポイントの価値があります。



|                                                                  |                                                                                                                            |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| When User1 signs in from an anonymous IP address, the user will: | <div>▼</div> <div>Be blocked</div> <div>Be prompted for MFA</div> <div>Sign in by using a username and password only</div> |
| When User2 signs in from an unfamiliar location, the user will:  | <div>▼</div> <div>Be blocked</div> <div>Be prompted for MFA</div> <div>Sign in by using a username and password only</div> |
| When User3 signs in from an infected device, the user will:      | <div>▼</div> <div>Be blocked</div> <div>Be prompted for MFA</div> <div>Sign in by using a username and password only</div> |

Answer:

|                                                                  |                                                                                                                            |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| When User1 signs in from an anonymous IP address, the user will: | <div>▼</div> <div>Be blocked</div> <div>Be prompted for MFA</div> <div>Sign in by using a username and password only</div> |
| When User2 signs in from an unfamiliar location, the user will:  | <div>▼</div> <div>Be blocked</div> <div>Be prompted for MFA</div> <div>Sign in by using a username and password only</div> |
| When User3 signs in from an infected device, the user will:      | <div>▼</div> <div>Be blocked</div> <div>Be prompted for MFA</div> <div>Sign in by using a username and password only</div> |

説明

When User1 signs in from an anonymous IP address, the user will:

When User2 signs in from an unfamiliar location, the user will:

When User3 signs in from an infected device, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

Be blocked

Be prompted for MFA

Sign in by using a username and password only

Be blocked

Be prompted for MFA

Sign in by using a username and password only

参考文献:

<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: 161

ネットワークには、Azure Active Directory (Azure AD) と同期する adatum.com という名前のオンプレミスの Active Directory ドメインが含まれています。

Azure AD テナントには、次の表に示すユーザーが含まれています。

| Name  | Source                       | Password          |
|-------|------------------------------|-------------------|
| User1 | Azure AD                     | Adatum123         |
| User2 | Azure AD                     | N3w3rT0Gue33      |
| User3 | On-premises Active Directory | ComplexPassword33 |

次の図に示すように、adatum.com の認証方法 - パスワード保護設定を構成します。

**Custom smart lockout**

Lockout threshold ⓘ  ✓

Lockout duration in seconds ⓘ  ✓

**Custom banned passwords**

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ 

Adatum ✓

**Password protection for Windows Server Active Directory**

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/> | <input type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input type="radio"/> | <input type="radio"/> |
| User3 can change the password to Adatum123!.                       | <input type="radio"/> | <input type="radio"/> |

**Answer:**

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can change the password to Adatum123!.                       | <input checked="" type="radio"/> | <input type="radio"/>            |

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

最新問題: 162

SQL という名前の Azure SQL Database ロジック サーバーを含む Azure サブスクリプションがあります。そして VM1 という名前の Azure 仮想マシン。VM1 はプライベート IP アドレスのみを使用します。

SQL1 のファイアウォールと仮想ネットワークの設定を次の図に示します。

Save X Discard + Add client IP

Deny public network access ⓘ  
Yes No

Click here to create a new private endpoint.  
Create Private Endpoint

Minimum TLS Version ⓘ  
1.0 1.1 1.2

Connection Policy ⓘ  
Default Proxy Redirect

Allow Azure services and resources to access this server ⓘ  
Yes No

Client IP address 89.212.25.106

| Rule name | Start IP | End IP |
|-----------|----------|--------|
|           |          | ...    |

No firewall rules configured.

Virtual networks  
+ Add existing virtual network + Create new virtual network

| Rule name                      | Virtual network | Subnet |
|--------------------------------|-----------------|--------|
| No vnet rules for this server. |                 |        |

VM1 が SQL1 に接続できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。あなたは何をすべきか？

- A. 新しいファイアウォール ルールを作成します。
- B. 既存の仮想ネットワークを追加します。
- C. Azure サービスとリソースによるこのサーバーへのアクセスを許可するを [はい] に設定します。
- D. 接続ポリシーをプロキシに設定します。

Answer: A ([メッセージを残す](#))

最新問題: 163

Azure Security Center 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、セキュリティ閲覧者役割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 ([メッセージを残す](#))

説明/参照:

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

最新問題: 164

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。

| Name | Resource group |
|------|----------------|
| VM1  | RG1            |
| VM2  | RG2            |
| VM3  | RG1            |
| VM4  | RG2            |

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

何を設定すればよいでしょうか？

- A. Azure Active Directory (Azure AD) Privileged Identity Management (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) 条件付きアクセス

<https://www.fast2test.com/AZ-500-practice-test.html> 75

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

- D. ジャストインタイム (JIT) VM アクセス

Answer: ([解答を表示する](#))

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 への受信トラフィックをロックダウンし、攻撃にさらされるリスクを軽減しながら、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、Security Center は NSG ルールを作成することによって、Azure VM への受信トラフィックをロックダウンします。受信トラフィックをロックダウンする 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、Security Center は、ユーザーが VM へのアクセスを正常に要求できる役割ベースのアクセス制御 (RBAC) アクセス許可を持っているかどうかを確認します。要求が承認されると、Security Center は、指定された期間、選択されたポートおよび要求された送信元 IP アドレスまたは範囲への受信トラフィックを許可するように、ネットワーク セキュリティ グループ (NSG) と Azure Firewall を自動的に構成します。時間が経過すると、Security Center 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ません。

参照 :

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

最新問題: 165

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ます。

| Name  | Role                                            | Sign in frequency      |
|-------|-------------------------------------------------|------------------------|
| User1 | Password administrator                          | Sign in every work day |
| User2 | Password administrator                          | Sign in bi-weekly      |
| User3 | Global administrator,<br>Password administrator | Signs in every month   |

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

Create an access review

Access reviews enable reviewers to attest to users access.

Review name

Review1

Description

Start date

2019-03-01

Frequency

One time

Duration (in days)

1

End

Never

Number of times

1

End date

2019-03-20

Users

Microsoft

Scope

Everyone

Review role membership

Password administrator

Reviewers

Members(self)

Upon completion settings

Auto apply results to resource

Enable

Disable

Should reviewer not respond

Take recommendations

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成させる回答の選択肢を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

Answer:

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

説明

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

ボックス 1: User3 のみ

ユーザーに自分の役割の割り当てを確認させるには、[メンバー (自分)] オプションを使用します。

ボックス 2: User3 は確認リクエストを受信します

「レビュー担当者は応答すべきではない」リストを使用して、レビュー期間内にレビュー担当者がレビューしなかったユーザーに何が起こるか指定します。この設定は、レビュー担当者によって手動でレビューされたユーザーには影響しません。最終レビュー担当者の決定が「拒否」の場合、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権を変更しないままにします

アクセス権の削除 - ユーザーのアクセス権を削除します

アクセスを承認 - ユーザーのアクセスを承認します

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

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

最新問題: 166

App1 という名前の Web アプリと Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。

Vault1 にシークレットを保存してアクセスできるように App1 を構成する必要があります。

App1 をどのように構成すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

Answer:

Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

参照 :

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>



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> (517**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 167

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。

| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

次の表に示すリソース ロックを作成します。

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                               | Yes                              | No                    |
|------------------------------------------|----------------------------------|-----------------------|
| You can start VM1.                       | <input checked="" type="radio"/> | <input type="radio"/> |
| You can start VM2.                       | <input type="radio"/>            | <input type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/>            | <input type="radio"/> |

| Statements                               | Yes                   | No                               |
|------------------------------------------|-----------------------|----------------------------------|
| You can start VM1.                       | <input type="radio"/> | <input checked="" type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input checked="" type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input checked="" type="radio"/> |

最新問題: 168

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

| Name       | Location | Description            |
|------------|----------|------------------------|
| Workspace1 | East US  | Used by Azure Sentinel |
| Workspace2 | West US  | Not applicable         |

次の表に示す仮想マシンを作成します。

| Name | Location | Operating system    | Connected to |
|------|----------|---------------------|--------------|
| VM1  | East US  | Windows Server 2019 | None         |
| VM2  | East US  | Windows Server 2019 | Workspace2   |
| VM3  | West US  | Windows Server 2019 | None         |
| VM4  | West US  | Windows Server 2019 | Workspace2   |

Azure Sentinel を使用して、仮想マシン上の Windows Defender ファイアウォールを監視する予定です。

Azure Sentinel に接続できる仮想マシンはどれですか？

- A. VM1のみ
- B. VM1 と VM3 のみ
- C. VM1、VM2、VM3、VM4
- D. VM1 と VM2 のみ

Answer: C (メッセージを残す)

セクション: [なし]

説明/参照:

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

最新問題: 169

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。

| Name       | Type                          | Region      | Resource group |
|------------|-------------------------------|-------------|----------------|
| SQL1       | Azure SQL database            | East US     | RG1            |
| Analytics1 | Azure Log Analytics workspace | East US     | RG1            |
| Analytics2 | Azure Log Analytics workspace | East US     | RG2            |
| Analytics3 | Azure Log Analytics workspace | West Europe | RG1            |

次の表に示す Azure ストレージ アカウントを作成します。

| Name     | Region      | Resource group | Storage account type | Access tier (default) |
|----------|-------------|----------------|----------------------|-----------------------|
| Storage1 | East US     | RG1            | Blob                 | Cool                  |
| Storage2 | East US     | RG2            | General purpose V1   | Not applicable        |
| Storage3 | West Europe | RG1            | General purpose V2   | Hot                   |

SQL1 の監査を構成する必要があります。  
監査ログの保存先として使用できるストレージ アカウントと Log Analytics ワークスペースはどれですか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

Answer:

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

最新問題: 170

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。

| Name | Connected to  | Private IP address | Public IP address |
|------|---------------|--------------------|-------------------|
| VM1  | VNET1/Subnet1 | 10.1.1.4           | 13.80.73.87       |
| VM2  | VNET2/Subnet2 | 10.2.1.4           | 213.199.133.190   |
| VM3  | VNET2/Subnet2 | 10.2.1.5           | None              |

Subnet1 と Subnet2 には Microsoft.Storage サービス エンドポイントが構成されています。  
storageacc1 という名前の Azure ストレージ アカウントがあり、次のように構成されています。



SaveDiscardRefresh

Allow access from

All networksSelected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)  
[+ Add new virtual network](#)

| VIRTUAL NETWORK      | SUBNET | ADDRESS RANGE | ENDPOINT STATUS | RESOURCE GROUP | SUBSCRIPTION |
|----------------------|--------|---------------|-----------------|----------------|--------------|
| No network selected. |        |               |                 |                |              |

Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87

IP address or CIDR

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ  
☐ Allow read access to storage logging from any network  
☐ Allow read access to storage metrics from any network

次の各ステートメントについて、そのステートメントが 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。

| Statements                                       | Yes                   | No                    |
|--------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can upload a blob to storageacc1.  | <input type="radio"/> | <input type="radio"/> |
| From VM2, you can upload a blob to storageacc1.  | <input type="radio"/> | <input type="radio"/> |
| From VM3 , you can upload a blob to storageacc1. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                       | Yes                              | No                               |
|--------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can upload a blob to storageacc1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM2, you can upload a blob to storageacc1.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM3 , you can upload a blob to storageacc1. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照 :  
<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>  
最新問題: 171



次の表に示すリソースが含まれる Subscription1 という名前の Azure サブスクリプションがあります。

| Name      | Type                            | Description                                                             |
|-----------|---------------------------------|-------------------------------------------------------------------------|
| EventHub1 | Azure Event Hubs                | Not applicable                                                          |
| Adf1      | Azure Data Factory              | Not applicable                                                          |
| NVA1      | Network virtual appliance (NVA) | The NVA sends security event messages in the Common Event Format (CEF). |

次のリソースを含む Subscription2 という名前の Azure サブスクリプションがあります。

Azure Sentinel ワークスペース

Azure Event Grid インスタンス

CEF メッセージを NVA から Azure Sentinel に取り込む必要があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Subscription1:

An Azure Log Analytics agent on a Linux virtual machine

A Data Factory pipeline

An Event Hubs namespace

An Azure Service Bus queue

Subscription2:

A new Azure Log Analytics workspace

A new Azure Sentinel data connector

A new Azure Sentinel playbook

A new Event Grid resource provider

Answer:

Answer Area

Subscription1:

A Data Factory pipeline

An Event Hubs namespace

An Azure Service Bus queue

Subscription2:

A new Azure Log Analytics workspace

A new Azure Sentinel data connector

A new Azure Sentinel playbook

A new Event Grid resource provider

最新問題: 172

Container1 という名前の BLOB コンテナと App1 という名前のクライアント アプリケーションを含む Azure ストレージ アカウントがあります。

Azure Active Directory (Azure AD) 認証を使用して、App1 の Container1 への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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Answer:

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

参照 :

<https://azure.microsoft.com/en-in/blog/payment-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: 173

次の図に示す役割の割り当てがあります。



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

注: 正しく選択するたびに 1 ポイントの価値があります。

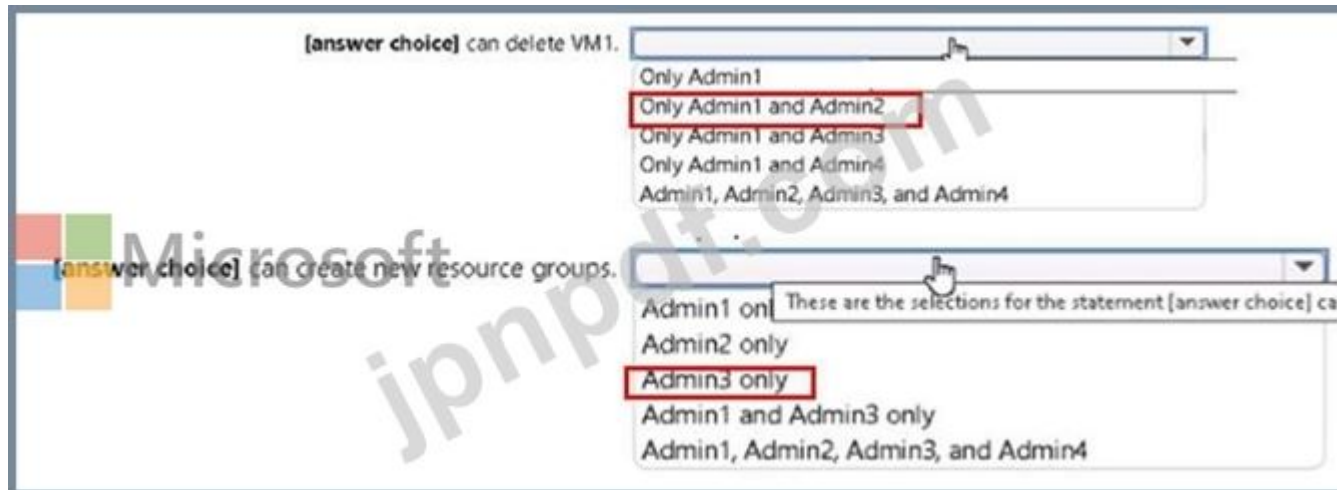
[answer choice] can delete VM1.

Only Admin1  
Only Admin1 and Admin2  
Only Admin1 and Admin3  
Only Admin1 and Admin4  
Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 only  
Admin2 only  
Admin3 only  
Admin1 and Admin3 only  
Admin1, Admin2, Admin3, and Admin4

Answer:



最新問題: 174

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

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

どの Azure ポリシーまたはイニシアチブ定義を確認する必要がありますか？

- A. 監査診断設定ポリシー定義
- B. Azure Security Center での監視の有効化イニシアチブの定義
- C. Azure Monitor for VMs の有効化イニシアチブの定義
- D. Azure Monitor ソリューションの「セキュリティと監査」ポリシー定義をデプロイする必要があります

Answer: B (メッセージを残す)

参照：

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

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

最新問題: 175

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



サブスクリプションで Azure サービスの監視を計画しています。  
次の詳細を取得する必要があります。  
3 週間前に仮想マシンを削除したユーザーを特定します。  
Windows Server 2016 を実行する仮想マシンのセキュリティ イベントをクエリします。  
Azure Monitor では何を使用する必要がありますか? 回答するには、適切な構成設定を正しい詳細にドラッグします。各構成設定は、1 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります。

Settings

Activity log

Logs

Metrics

Service Health

Answer Area

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:

Answer:

Settings

Activity log

Logs

Metrics

Service Health

Answer Area

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:

Activity log

Logs

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

最新問題: 176

OU2 と User1 に対して計画された変更を実行する必要があります。  
どのツールを使用する必要がありますか? 答えるには、適切なツールを正しいリソースにドラッグします。各ツールは 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: 正しく選択するたびに 1 ポイントの価値があります。



| Tools                                | Answer Area |
|--------------------------------------|-------------|
| The Azure portal                     | OU2: Tool   |
| Azure AD Connect                     | User1: Tool |
| The Active Directory admin center    |             |
| Active Directory Sites and Services  |             |
| Active Directory Users and Computers |             |

Answer:

| Tools                                | Answer Area             |
|--------------------------------------|-------------------------|
| The Azure portal                     | OU2: Azure AD Connect   |
| Azure AD Connect                     | User1: The Azure portal |
| The Active Directory admin center    |                         |
| Active Directory Sites and Services  |                         |
| Active Directory Users and Computers |                         |

#### 最新問題: 177

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Sub1 という名前の Azure サブスクリプションがあります。

RG1 という名前のリソース グループに Sa1 という名前の Azure ストレージ アカウントがあります。

ユーザーとアプリケーションは、いくつかの共有アクセス署名 (SAS) と保存されたアクセス ポリシーを使用して、Sa1 の BLOB サービスとファイル サービスにアクセスします。

権限の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: 新しい保存されたアクセス 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

共有アクセス署名は、ブログなどの特定のリソースへのアクセスを提供します。保存されたアクセス ポリシーは、Shared Access Signature (SAS) のグループです。SAS へのアクセスを取り消すには、次のいずれかを実行できます。

1. Key1 または Key 2、つまり SAS への署名に使用されるアクセス キーをローテーションします。SAS の署名に使用されたアクセス キーをローテーションすると、以前に署名された SAS が無効になるため、以前に使用されていた SAS が取り消されます。
2. SAS がリンクされている保存されたアクセス ポリシーを削除します。ストアド アクセス ポリシーが削除されると、そのストアド アクセス ポリシーに関連付けられている SAS も無効になります。

最新問題: 178

ID という名前のマネージド 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 および AU2 にはどのリソースを追加できますか? 回答するには、回答領域で適切なオプションを選択してください。

| Name   | Type                | Assigned object |
|--------|---------------------|-----------------|
| AU1    | Administrative unit | User1, Group1   |
| AU2    | Administrative unit | None            |
| User1  | User                | Not applicable  |
| Group1 | Security group      | Not applicable  |
| Group2 | Microsoft 365 group | Not applicable  |

AU1 と AU2 にはどのリソースを追加できますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

AU1:

AU2 only

Group2 only

Identity1 only

AU2 and Group2 only

Group2 and Identity1 only

AU2:

Identity1 only

AU1 and Identity1 only

Group1 and Group2 only

AU1, Group1 and Identity1 only

Group1, Group2 and Identity1 only

Answer:

Answer Area

AU1:

AU2 only

Group2 only

Identity1 only

AU2 and Group2 only

Group2 and Identity1 only

AU2:

Identity1 only

AU1 and Identity1 only

Group1 and Group2 only

AU1, Group1 and Identity1 only

Group1, Group2 and User1 only

最新問題: 179

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 のロール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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

```

{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
    {
      "Microsoft.Compute/disk/*",
      "Microsoft.Resources/storageAccounts/*",
      "Microsoft.Storage/virtualMachines/disk/*"
    },
    {
      "NotActions": [
      ],
      "AssignableScopes": [
        {
          "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
        },
        {
          "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"
        }
      ]
    }
  ]
}

```

Answer:

User:

User1

User2

User3

User4

Tool:

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

説明

1) Microsoft.Compute/

2) ディスク

3) /subscription/{subscriptionId}/resourceGroups/{リソース グループ ID}

Resource Group1 のマネージド 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

す。役割 1 は、リソース グループ 1 に対してのみ使用可能である必要があります。

最新問題: 180

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。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、Windows Server 2016 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。

Azure Disk Encryption を使用して VM1 ディスクを暗号化する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area



Answer:

Actions

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area

Create an Azure key vault.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Explanation:

参考文献:

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

最新問題: 181



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。

| Name | Type                  | Region    | Resource group |
|------|-----------------------|-----------|----------------|
| Sa1  | Azure Storage account | East US   | RG1            |
| VM1  | Azure virtual machine | East US   | RG2            |
| KV1  | Azure key vault       | East US 2 | RG1            |
| SQL1 | Azure SQL database    | East US 2 | RG2            |

包含データベース ユーザーを使用して、SQL1 上のデータベースへの安全なアクセスを VM1 に提供できることを確認する必要があります。  
あなたは何をすべきか？

- A. KV1 にシークレットを作成します。
- B. SQL1 でサービス エンドポイントを構成します。
- C. KV1にキーを作成します。
- D. VM1 でマネージド サービス ID を有効にします。

Answer: A (メッセージを残す)

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> (517**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 182

Azure コンテナに接続する Azure Kubernetes Service (AKS) クラスターを構成しています。  
レジストリ。

Azure Container Registry に対する認証には、自動生成されたサービス プリンシパルを使用する必要があります。  
何を作成する必要がありますか？

- A. Azure Active Directory (Azure AD) グループ
- B. Azure Active Directory (Azure AD) のロールの割り当て
- C. Azure Active Directory (Azure AD) ユーザー
- D. Azure Key Vault のシークレット

Answer: B (メッセージを残す)

AKS クラスターを作成すると、Azure は他のクラスターとのクラスターの操作性をサポートするサービス プリンシパルも作成します。  
Azure のリソース。この自動生成されたサービス プリンシパルを ACR レジストリでの認証に使用できます。に  
そのためには、クラスターのサービス プリンシパルにクラスターへのアクセスを許可する Azure AD ロール割り当てを作成する必要があります。

参考: レジストリ。  
<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks>

### 最新問題: 183

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。

無許可のアプリケーションやマルウェアが仮想マシン上で実行されるのを防ぐ必要があります。

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、適応型アプリケーション 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:** ([解答を表示する](#))

セクション: [なし]

Explanation:

アダプティブ アプリケーション コントロールは、Azure Security Center が提供するインテリジェントで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 および非 Azure VM (Windows および Linux) でどのアプリケーションを実行できるかを制御するのに役立ちます。これにより、マルウェアに対して VM を強化することができます。Security Center は、機械学習を使用して VM 上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: 184

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

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

Playbook1 をトリガーする Query1 に基づいて Azure Sentinel 分析ルールを作成する予定です。

Playbook1 を新しいルールに追加できることを確認する必要があります。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

Create the rule and set the type to:

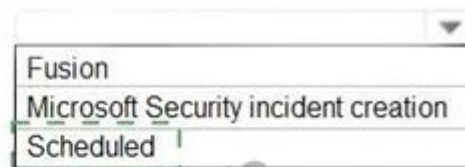
|                                      |
|--------------------------------------|
| Fusion                               |
| Microsoft Security incident creation |
| Scheduled                            |

Configure the playbook to include:

|                                    |
|------------------------------------|
| A managed connector                |
| A system-assigned managed identity |
| A trigger                          |
| D diagnostic settings              |

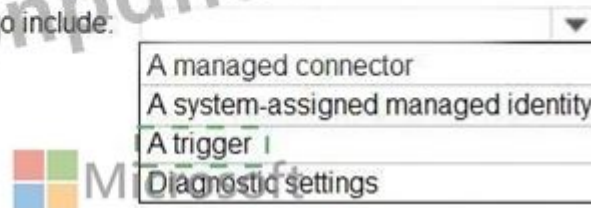
## Answer:

Create the rule and set the type to:



|                                      |
|--------------------------------------|
| Fusion                               |
| Microsoft Security incident creation |
| Scheduled                            |

Configure the playbook to include:



|                                    |
|------------------------------------|
| A managed connector                |
| A system-assigned managed identity |
| A trigger                          |
| Diagnostic settings                |

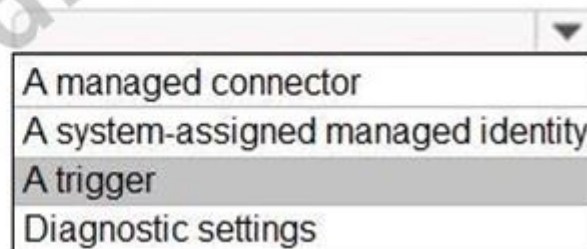
## 説明

Create the rule and set the type to:



|                                      |
|--------------------------------------|
| Fusion                               |
| Microsoft Security incident creation |
| Scheduled                            |

Configure the playbook to include:



|                                    |
|------------------------------------|
| A managed connector                |
| A system-assigned managed identity |
| A trigger                          |
| Diagnostic settings                |

## 参照 :

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

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

## 最新問題: 185

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。

次の要件を満たすために、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。
- \* コストは最小限に抑える必要があります。

各仮想ネットワークにはどの VPN ゲートウェイ (SKU) 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 回だけ使用することも、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: 正しく選択するたびに 1 ポイントの価値があります

SKUs

Basic

VpnGw1

VpnGw2

VpnGw3

Answer Area

Microsoft

VNET1:SKU

VNET2:SKU

Answer:

SKUs

Basic

VpnGw1

VpnGw2

VpnGw3

Answer Area

Microsoft

VNET1:VpnGw1

VNET2:VpnGw1

Explanation:

参考文献:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

最新問題: 186

LAW1 という名前の Azure Log Analytics ワークスペースを含む Sub1 という名前の Azure サブスクリプションがあります。Windows Server 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。システム更新評価ソリューションを LAW1 に追加する予定です。システム更新評価関連のログが 100 台の仮想マシンのみから LAW1 にアップロードされるようにする必要があります。どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a new workspace.

Apply

 the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

Answer Area

Answer:



| Actions                                        | Answer Area                                    |
|------------------------------------------------|------------------------------------------------|
| Create a new workspace.                        | Create a computer group.                       |
| Apply the scope configuration to the solution. | Create a scope configuration.                  |
| Create a scope configuration.                  | Apply the scope configuration to the solution. |
| Create a computer group.                       |                                                |
| Create a data source.                          |                                                |

参考文献:

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

### 最新問題: 187

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、仮想マシンへの PowerShell アクセスをユーザーに許可する必要があります。  
 何を設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

| Answer Area                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>  <div> <p>Permission that must be granted to users on VM:</p> <p>Read<br/>Update<br/>View<br/>Write</p> </div> </div> <div> <p>TCP port that must be allowed:</p> <p>22<br/>25<br/>3389<br/>5986</p> </div> |

Answer:

| Answer Area                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>  <div> <p>Permission that must be granted to users on VM:</p> <p>Read<br/>Update<br/>View<br/>Write</p> </div> </div> <div> <p>TCP port that must be allowed:</p> <p>22<br/>25<br/>3389<br/>5986</p> </div> |

### 最新問題: 188

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。  
 各サブスクリプションについて、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 に対する権限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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Configure role-based access control (RBAC) role assignments by using:

Azure Blueprints

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

A resource lock

A role-based access control (RBAC) role assignment at the resource group level

Azure Blueprint assignments in locking mode

Answer:

Configure role-based access control (RBAC) role assignments by using:

Azure Blueprints

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

A resource lock

A role-based access control (RBAC) role assignment at the resource group level

Azure Blueprint assignments in locking mode

最新問題: 189

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。

| Name | Operating system        |
|------|-------------------------|
| VM1  | Windows Server 2016     |
| VM2  | Ubuntu Server 18.04 LTS |

Azure Security Center から、自動プロビジョニングを有効にします。

次の表に示す仮想マシンをデプロイします。

| Name | Operating system        |
|------|-------------------------|
| VM3  | Windows Server 2016     |
| VM4  | Ubuntu Server 18.04 LTS |

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 と VM3 のみ
- C. VM3 および VM4 のみ
- D. VM1、VM2、VM3、および VM4

Answer: D (メッセージを残す)

説明

自動プロビジョニングがオンになっている場合、Security Center は、サポートされているすべての Azure VM と新しく作成された Azure VM に Log Analytics エージェント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)、および 18.04 LTS (x64) および Windows Server 2008 R2、2012、2012 R2、2016、バージョン 1709 および 1803 が含まれます。

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

最新問題: 190

新しい Azure Active Directory (Azure AD) テナントに関連付けられた新しい Azure サブスクリプションを作成します。  
ポータル ポリシーという名前のアクティブな条件付きアクセス ポリシーを 1 つ作成します。ポータル ポリシーは、Microsoft Azure 管理クラウド アプリへのアクセスを提供するために使用されます。

ポータル ポリシーの条件設定は、条件の説明に示されているように構成されます。( 条件」タブをクリックします。)

Portal Policy

InfoDelete

Name

Portal Policy

Assignments

Users and groups1

All users

Cloud apps1

1 app included

Conditions1

1 condition selected

Access controls

Grant1

2 controls selected

Session1

0 controls selected

Conditions

Info

Device platforms1

Not configured

Locations1

1 included

Client apps (preview)1

Not configured

Device state (preview)1

Not configured

Locations

Control user access based on their physical location. Learn more

Configure1

YesNo

IncludeExclude

Any location

All trusted locations

Selected locations

Select

Contoso

Contoso...

ポータル ポリシーの付与設定は、付与」の図に示されているように構成されます。( 付与」タブをクリックします。)

Portal Policy

Info

Delete

\* Name

Portal Policy

Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

1 condition selected

Access controls

Grant

2 controls selected

Session

0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

See list of approved client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                                                                    | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input type="radio"/> |

Answer:



| Statements                                                                                                                                    | Yes                   | No                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input checked="" type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input checked="" type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input checked="" type="radio"/> |

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

最新問題: 191

Azure Active Directory (Azure AD) Privileged Identity Management (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 アクセス管理者ロールが割り当てられている PIM ユーザーは、ロール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信すると報告します。この問題を解決するには、PIM サービス プリンシパルにサブスクリプションに対する正しいアクセス許可があることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。PIM サービス原則にはどの役割を割り当てる必要がありますか？

- A. 投稿者
- B. ユーザーアクセス管理者
- C. リソース ポリシーの貢献者
- D. マネージド アプリケーション オペレーター

Answer: B (メッセージを残す)

最新問題: 192

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Azure サブスクリプションがあります。テナントには、次の表に示すユーザーが含まれます。

| Name  | Subscription role | Azure AD user role    |
|-------|-------------------|-----------------------|
| User1 | Owner             | None                  |
| User2 | Contributor       | None                  |
| User3 | Security Admin    | None                  |
| User4 | None              | Service administrator |

RG1 という名前のリソース グループを作成します。どのユーザーが RG1 の権限を変更でき、どのユーザーが RG1 で仮想ネットワークを作成できますか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Answer:

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

最新問題: 193  
Update Management 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。

| Name | Operating system             | Region  | Resource group |
|------|------------------------------|---------|----------------|
| VM1  | Windows Server 2012          | East US | RG1            |
| VM2  | Windows Server 2012 R2       | West US | RG1            |
| VM3  | Windows Server 2016          | West US | RG2            |
| VM4  | Ubuntu Server 18.04 LTS      | West US | RG2            |
| VM5  | Red Hat Enterprise Linux 7.4 | East US | RG1            |
| VM6  | CentOS 7.5                   | East US | RG1            |

Update1 と Update2 という名前の 2 つの更新プログラムの展開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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Update1:

▼

VM2 only

VM4 only

VM1 and VM2 only

VM1, VM2, VM4, VM5, and VM6

Update2:

▼

VM5 only

VM1 and VM5 only

VM4 and VM5 only

VM1, VM2, and VM5 only

VM1, VM2, VM3, VM4, and VM5

Answer:

Update1: 

▼

VM2 only

VM4 only

VM1 and VM2 only

VM1, VM2, VM4, VM5, and VM6

Update2: 

▼

VM5 only

VM1 and VM5 only

VM4 and VM5 only

VM1, VM2, and VM5 only

VM1, VM2, VM3, VM4, and VM5

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

最新問題: 194

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が含まれる Storage1 という名前の Azure ストレージ アカウントがあります。

| Name       | Type           |
|------------|----------------|
| Container1 | Blob container |
| Share1     | File share     |

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 と Share! のコンテンツにアクセスするにはどのツールを使用できますか? SAS を使用することで? 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Tools for Container1:

Robocopy.exe

Azure Storage Explorer

File Explorer

Tools for Share1:

Robocopy.exe

Azure Storage Explorer

File Explorer

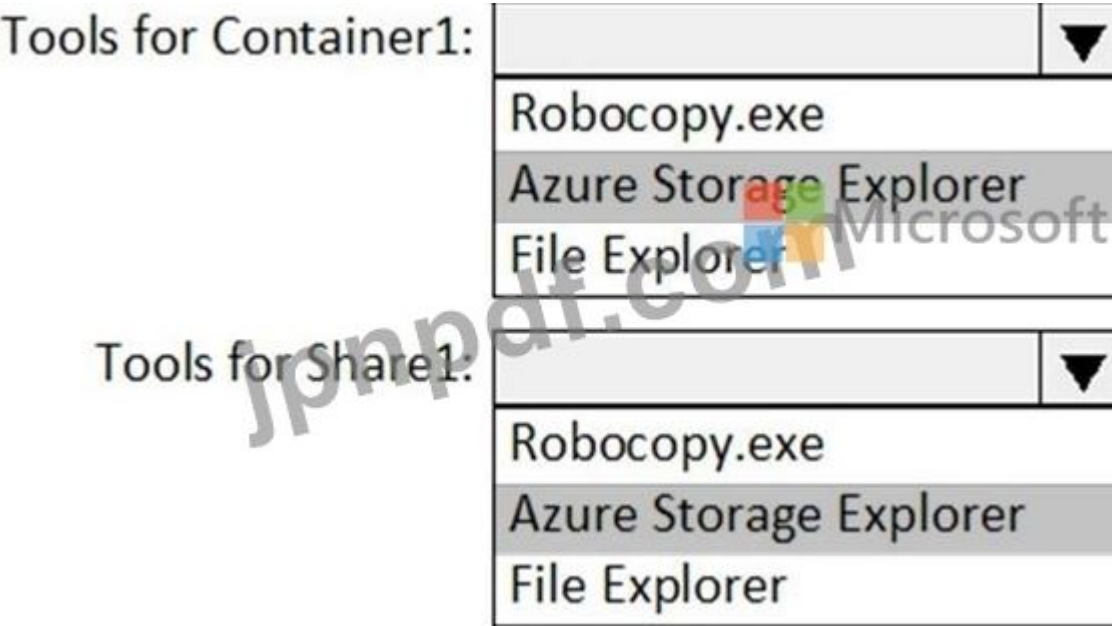
Answer:



Answer Area



説明



最新問題: 195

次の図に示すように、Azure リソースの階層があります。



次の表に示す Azure Blueprints 定義を作成します。

| Name       | Published at      |
|------------|-------------------|
| Blueprint1 | Tenant Root Group |
| Blueprint2 | Subscription1     |

Blueprint1 と Blueprint2 をどのオブジェクトに割り当てることができますか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Blueprint1:

ManagementGroup1 only

ManagementGroup1, Subscription1, and RG1 only

ManagementGroup1, Subscription1, RG1, and VM1

Subscription1 only

Tenant Root Group only

Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only

Subscription1 and RG1 only

Subscription1 only

Subscription1, RG1, and VM1

Answer:

Blueprint1:

Microsoft

ManagementGroup1 only

ManagementGroup1, Subscription1, and RG1 only

ManagementGroup1, Subscription1, RG1, and VM1

Subscription1 only

Tenant Root Group only

Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only

Subscription1 and RG1 only

Subscription1 only

Subscription1, RG1, and VM1

説明

Blueprint1:

Microsoft

ManagementGroup1 only

ManagementGroup1, Subscription1, and RG1 only

ManagementGroup1, Subscription1, RG1, and VM1

Subscription1 only

Tenant Root Group only

Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only

Subscription1 and RG1 only

Subscription1 only

Subscription1, RG1, and VM1

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: 196

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、次のような出力が表示されます。

|                                      |                     |
|--------------------------------------|---------------------|
| Name                                 | : DenyStorageAccess |
| Description                          |                     |
| Protocol                             | : *                 |
| SourcePortRange                      | : {*}               |
| DestinationPortRange                 | : {*}               |
| SourceAddressPrefix                  | : {*}               |
| DestinationAddressPrefix             | : {Storage}         |
| SourceApplicationSecurityGroups      | : []                |
| DestinationApplicationSecurityGroups | : []                |
| Access                               | : Deny              |
| Priority                             | : 105               |
| Direction                            | : Outbound          |
| Name                                 | : StorageEA2Allow   |
| ProvisioningState                    | : Succeeded         |
| Description                          |                     |
| Protocol                             | : *                 |
| SourcePortRange                      | : {*}               |
| DestinationPortRange                 | : {443}             |
| SourceAddressPrefix                  | : {*}               |
| DestinationAddressPrefix             | : {Storage/EastUS2} |
| SourceApplicationSecurityGroups      | : []                |
| DestinationApplicationSecurityGroups | : []                |
| Access                               | : Allow             |
| Priority                             | : 104               |
| Direction                            | : Outbound          |
| Name                                 | : Contoso_FTP       |
| Description                          |                     |
| Protocol                             | : TCP               |
| SourcePortRange                      | : {*}               |
| DestinationPortRange                 | : {21}              |
| SourceAddressPrefix                  | : {1.2.3.4/32}      |
| DestinationAddressPrefix             | : {10.0.0.5/32}     |
| SourceApplicationSecurityGroups      | : []                |
| DestinationApplicationSecurityGroups | : []                |
| Access                               | : Allow             |
| Priority                             | : 504               |
| Direction                            | : Inbound           |

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成させる回答の選択肢を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。



Traffic destined for an Azure Storage account is [answer choice].

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

Answer:

Traffic destined for an Azure Storage account is [answer choice].

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

説明

ボックス 1: 米国東部 2 に接続可能

StorageEA2Allow には DestinationAddressPrefix {Storage/EastUS2} があります

ボックス 2: ドロップされました

参照 :

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

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> (517**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 197

Azure サブスクリプションをお持ちです。

次の要件を満たす Azure ポリシーを作成してデプロイする必要があります。

新しい仮想マシンがデプロイされると、カスタム セキュリティ拡張機能が自動的にインストールされます。

非準拠の仮想マシンに対して自動生成された修復タスクをトリガーして、拡張機能をインストールします。  
ポリシーには何を含めるべきですか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Definition effect:

▼

Append  
DeployIfNotExists  
EnforceOPAConstraint  
EnforceRegoPolicy  
Modify

Assignment remediation task:

▼

A managed identity that has the Contributor role  
A managed identity that has the User Access Administrator role  
A service principal that has the Contributor role  
A service principal that has the User Access Administrator role

Answer:

Definition effect:

▼

Append  
DeployIfNotExists  
EnforceOPAConstraint  
EnforceRegoPolicy  
Modify

Assignment remediation task:

▼

A managed identity that has the Contributor role  
A managed identity that has the User Access Administrator role  
A service principal that has the Contributor role  
A service principal that has the User Access Administrator role

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

最新問題: 198

contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた 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予定です。

| Name             | Type                    | Description                                                                                                    |
|------------------|-------------------------|----------------------------------------------------------------------------------------------------------------|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database<br>Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1          | Azure web app           | A web app configured to serve as the middle tier of the application                                            |

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 Cosmos DB アカウントにアクセスします。  
どのタスクが CosmosDB1 と WebApp1 に実装されるかを特定する必要があります。  
各リソースに対してどのタスクを特定する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

CosmosDB1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

WebApp1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

Answer:

CosmosDB1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

WebApp1:

Authenticate Azure AD users and generate resource tokens.

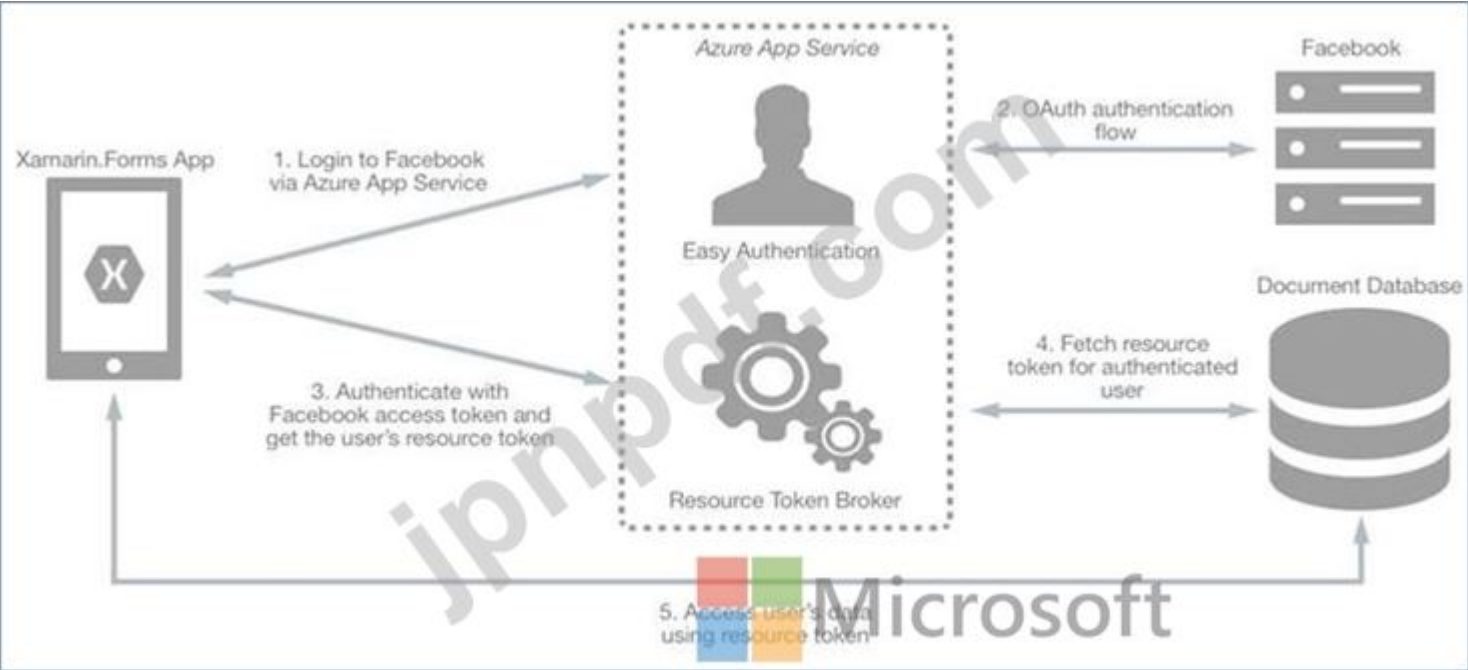
Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

Explanation:  
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、付与されたアクセス許可に従って、クライアントが Azure Cosmos DB アカウント内の特定のリソースを読み取り、書き込み、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 トークンを中継する  
リソース トークンを要求、生成し、モバイル アプリケーションに配信する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。



参考文献:

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

最新問題: 199

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。オフィスは次の表に示すIPアドレスを使用します。

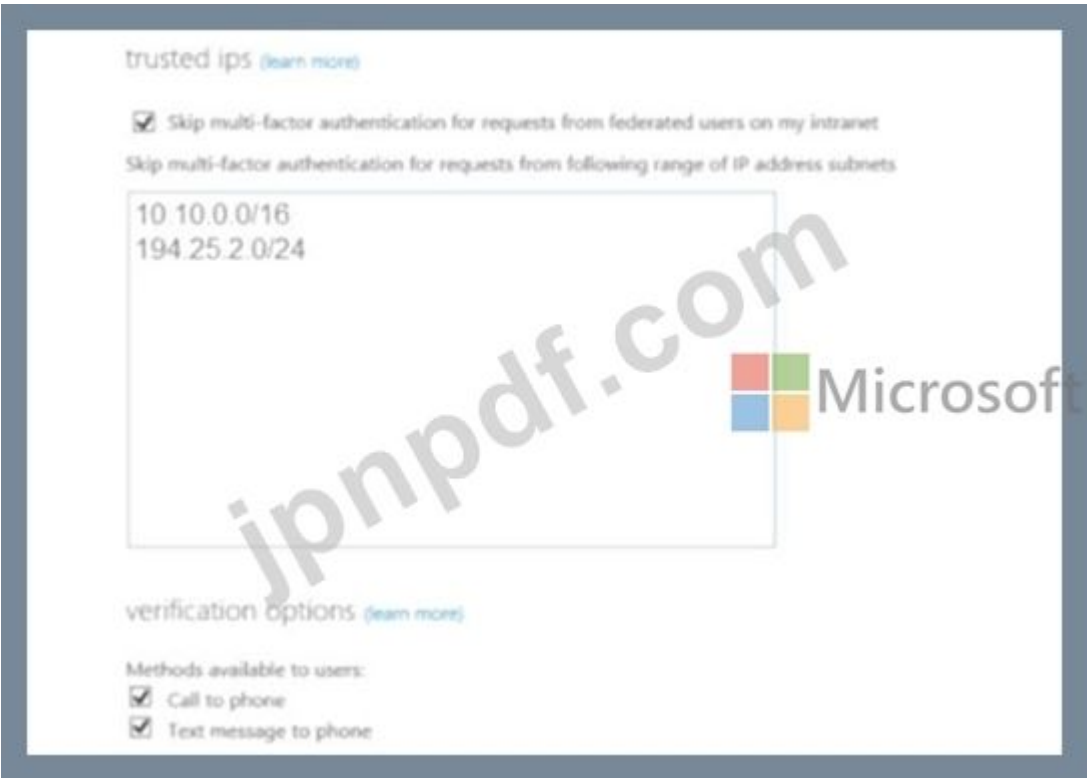
| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Seattle  | 10.10.0.0/16     | 190.15.1.0/24      |
| New York | 172.16.0.0/16    | 194.25.2.0/24      |

この会社には、contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。テナントには、次の表に示すユーザーが含まれます。

| Name  | Multi-factor authentication (MFA) status |
|-------|------------------------------------------|
| User1 | Enabled                                  |
| User2 | Enforced                                 |

MFA サービス設定は、図に示す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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

|                                                                                                                                       | Yes                   | No                    |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/> | <input type="radio"/> |

Answer:

|                                                                                                                                       | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

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

最新問題: 200

注: この質問は、同じシナリオを示す一連の質問の一部です。それぞれの質問  
このシリーズには、指定された目標を達成でき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。いくつかの問題集  
複数の正しい解決策がある場合もあれば、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すると、その質問に戻ることはできません。その結果、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 Azure HDInsight クラスターがあります。  
ユーザーがオンプレミスの Active Directory を使用してクラスターに対して認証できるようにする予定です。  
資格。  
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 ([メッセージを残す](#))

説明/参照:

Explanation:

代わりに、Azure Virtual Networks と VPN を使用して、HDInsight をオンプレミス ネットワークに接続します。  
ゲートウェイ。

注: HDInsight と参加ネットワーク内のリソースが名前で通信できるようにするには、次の手順を実行する必要があります。  
次のアクション:

- Azure仮想ネットワークを作成します。
- Azure Virtual Network にカスタム DNS サーバーを作成します。
- デフォルトの Azure Recursive の代わりにカスタム DNS サーバーを使用するように仮想ネットワークを構成する
- 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。

参考文献:

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

最新問題: 201

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。

| Name         | Type           | Description                     |
|--------------|----------------|---------------------------------|
| RG1          | Resource group | Used to store virtual machines  |
| RG2          | Resource group | Used to store virtual networks  |
| ServerAdmins | Security group | Used to manage virtual machines |

ServerAdmins が次のタスクを実行できることを確認する必要があります。  
RG2 の既存の仮想ネットワークにのみ仮想マシンを作成します。  
ソリューションでは、最小特権の原則を使用する必要があります。  
ServerAdmins に割り当てべき 2 つのロールベースのアクセス制御 (RBAC) ロールはどれですか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

- A. サブスクリプションの共同作成者の役割
- B. RG1 の仮想マシン共同作成者ロール。
- C. RG2 のカスタム RBAC ロール
- D. RG2 のネットワーク共同作成者の役割
- E. RG1 のネットワーク共同作成者の役割。
- F. サブスクリプションのカスタム RBAC ロール

Answer: [\(解答を表示する\)](#)

最新問題: 202

QUESTION NO: 275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。

| Name     | Type             | Resource group | Location |
|----------|------------------|----------------|----------|
| RG1      | Resource group   | Not applicable | West US  |
| Managed1 | Managed identity | RG1            | West US  |

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。

| Name  | Usage location |
|-------|----------------|
| User1 | United States  |
| User2 | Germany        |

次の表に示すグループを作成します。

| Name   | Type          | Membership type |
|--------|---------------|-----------------|
| Group1 | Security      | Dynamic User    |
| Group2 | Microsoft 365 | Dynamic User    |

Group1 と Group2 のメンバーシップ ルールは次のように構成されています。

Dynamic membership rules

...

×

 Save

 Discard

|

 Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule.  [Learn more](#)

| And/Or | Property       | Operator | Value |  |
|--------|----------------|----------|-------|--|
|        | accountEnabled | Equals   | true  |  |
| Or     | usageLocation  | Equals   | US    |  |

+

 Add expression

+

 Get custom extension properties 

Rule syntax  Edit

(user.accountEnabled -eq true) or (user.usageLocation - eq "US")

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                 | Yes                   | No                    |
|--------------------------------------------|-----------------------|-----------------------|
| User1 is a member of Group1 and Group2.    | <input type="radio"/> | <input type="radio"/> |
| User2 is a member of Group2 only.          | <input type="radio"/> | <input type="radio"/> |
| Managed1 is a member of Group1 and Group2. | <input type="radio"/> | <input type="radio"/> |

Answer:



| Statements                                 | Yes                              | No                               |
|--------------------------------------------|----------------------------------|----------------------------------|
| User1 is a member of Group1 and Group2.    | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 is a member of Group2 only.          | <input type="radio"/>            | <input checked="" type="radio"/> |
| Managed1 is a member of Group1 and Group2. | <input type="radio"/>            | <input checked="" type="radio"/> |

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

最新問題: 203

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。  
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、Windows Server 2016 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。

Azure Disk Encryption を使用して VM1 ディスクを暗号化する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                            | Answer Area |
|----------------------------------------------------|-------------|
| Configure secrets for the Azure key vault.         |             |
| Create an Azure key vault.                         |             |
| Run Set-AzureRmStorageAccount.                     |             |
| Configure access policies for the Azure key vault. |             |
| Run Set-AzureRmVmDiskEncryptionExtension.          |             |

Answer:

Actions

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area

Create an Azure key vault.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Explanation:

参考文献:

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

最新問題: 204

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ます。

| Name  | Role                                            | Sign in frequency      |
|-------|-------------------------------------------------|------------------------|
| User1 | Password administrator                          | Sign in every work day |
| User2 | Password administrator                          | Sign in bi-weekly      |
| User3 | Global administrator,<br>Password administrator | Signs in every month   |

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

**Create an access review**

Access reviews enable reviewers to attest to users access.

\* Review name

Description

\* Start date

Frequency

Duration (in days)

Cost

\* Number of times

\* End date

Users

Scope ☒

\* Review role membership

Reviewers

Upset completion settings

Auto apply results to resource ☒

Should reviewer not respond ☒

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成させる回答の選択肢を選択します。  
注: 正しく選択するたびに 1 ポイントの価値があります。

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

User2 will retain the Password administrator role

User3 will receive a confirmation request

**Answer:**

User3 can perform Review1 for

User3 only

User1 and User2 only

User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

The Password administrator role will be revoked from User2

User2 will retain the Password administrator role

User3 will receive a confirmation request

説明

User3 can perform Review1 for

User3 only

User1 and User2 only

User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

The Password administrator role will be revoked from User2

User2 will retain the Password administrator role

User3 will receive a confirmation request

ボックス 1: User3 のみ

ユーザーに自分の役割の割り当てを確認させるには、メンバー (自分) オプションを使用します。

ボックス 2: User3 は確認リクエストを受信します

レビュー担当者は応答すべきではない」リストを使用して、レビュー期間内にレビュー担当者がレビューし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、レビュー担当者によって手動でレビューされたユーザーには影響しません。最終レビュー担当者の決定が「拒否」の場合、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権を変更しないままにします

アクセス権の削除 - ユーザーのアクセス権を削除します

アクセスを承認 - ユーザーのアクセスを承認します

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

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

最新問題: 205

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

| Name   | Role                 |
|--------|----------------------|
| Admin1 | Global administrator |
| Admin2 | Group administrator  |
| Admin3 | User administrator   |

Contoso.com にはグループ名前付けポリシーが含まれています。このポリシーには、Contoso という単語を含むカスタムの禁止単語リストルールがあります。

contoso.com で Contoso Sales という名前のグループを作成できるのはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。



注: 正しく選択するたびに 1 ポイントの価値があります。

Users who can create a security group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

**Answer:**

Users who can create a security group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

参照 :

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

#### 最新問題: 206

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

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

次の要件を満たすように構成する Azure Sentinel コンポーネントを特定する必要があります。

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

Azure Sentinel でインシデントが作成されるとき、チケットはサービス管理プラットフォームに記録される必要があります。

各要件に対してどのコンポーネントを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

When Azure Sentinel identifies a threat, an incident must be created:

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:



▼

Analytics

Data connectors

Playbooks

Workbooks

Answer:

When Azure Sentinel identifies a threat, an incident must be created:

▼

Analytics

Data connectors

Playbooks

Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

▼

Analytics

Data connectors

Playbooks

Workbooks

参照 :

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

最新問題: 207

Azure 環境があります。  
ISO 27001 に準拠していない Azure 構成とワークロードを特定する必要があります。  
規格。何をえばいいのでしょうか？

- A. アズールセンチネル
- B. Azure Active Directory (Azure AD) ID 保護
- C. Azure セキュリティ センター
- D. Azure Advanced Threat Protection (ATP)

Answer: C (メッセージを残す)

参照 :

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

最新問題: 208

contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた 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予定です。

| Name             | Type                    | Description                                                                                                    |
|------------------|-------------------------|----------------------------------------------------------------------------------------------------------------|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database<br>Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1          | Azure web app           | A web app configured to serve as the middle tier of the application                                            |

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 Cosmos DB アカウントにアクセスします。  
どのタスクが CosmosDB1 と WebApp1 に実装されるかを特定する必要があります。  
各リソースに対してどのタスクを特定する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

CosmosDB1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

WebApp1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

Answer:

CosmosDB1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

WebApp1:

Authenticate Azure AD users and generate resource tokens.

Authenticate Azure AD users and relay resource tokens.

Create database users and generate resource tokens.

説明



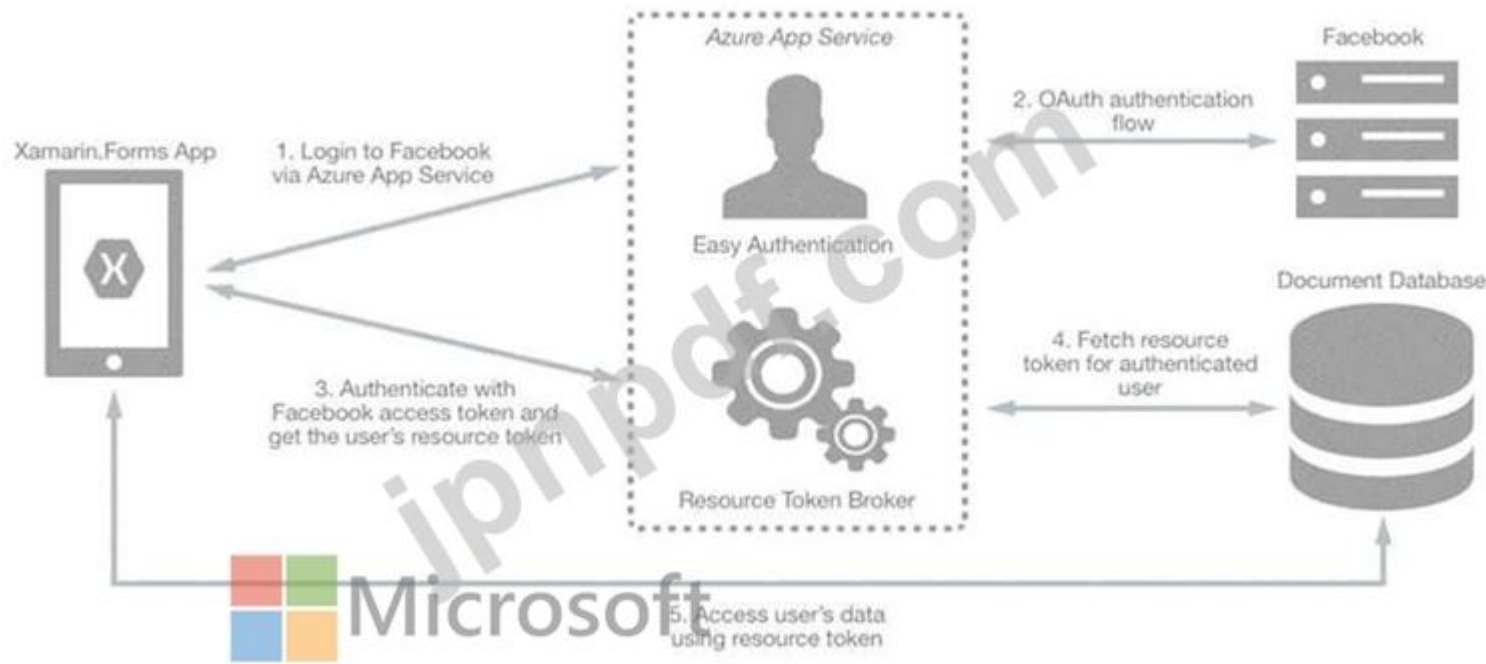
|            |                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CosmosDB1: | <div>▼</div> <div>Authenticate Azure AD users and generate resource tokens.<br/>Authenticate Azure AD users and relay resource tokens.<br/>Create database users and generate resource tokens.</div> |
| WebApp1:   | <div>▼</div> <div>Authenticate Azure AD users and generate resource tokens.<br/>Authenticate Azure AD users and relay resource tokens.<br/>Create database users and generate resource tokens.</div> |

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、付与されたアクセス許可に従って、クライアントが Azure Cosmos DB アカウント内の特定のリソースを読み取り、書き込み、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 トークンを中継する

リソース トークンを要求、生成し、モバイル アプリケーションに配信する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。



参考文献:

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

最新問題: 209

Vault という名前の Azure Key Vault があります。次の表に示すリソースが格納されます。



| Name    | Type        |
|---------|-------------|
| Key1    | Key         |
| Secret1 | Secret      |
| Cert1   | Certificate |

ローテーション ポリシーの作成をサポートするリソースはどれですか？

- A. Key1 と Cert1 のみ
- B. Key1 と Secret1 のみ
- C. Cert1 のみ
- D. キー 1 のみ
- E. Secret1 と Cert1 のみ
- F. Key1、Secret1、Cert1

Answer: [\(解答を表示する\)](#)

最新問題: 210

Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。

2019 年 1 月 1 日、Vault1 には次のシークレットが保存されます。

|             |                                                        |
|-------------|--------------------------------------------------------|
| Enabled     | : False                                                |
| Expires     | :                                                      |
| NotBefore   | : 5/1/19 12:00:00 AM                                   |
| Created     | : 12/20/18 2:55:00 PM                                  |
| Updated     | : 12/20/18 2:55:00 PM                                  |
| ContentType | :                                                      |
| Tags        | :                                                      |
| TagTable    | :                                                      |
| VaultName   | : vault1                                               |
| Name        | : Password1                                            |
| Version     | :                                                      |
| Id          | : https://vault1.vault.azure.net:443/secrets/Password1 |
| Enabled     | : True                                                 |
| Expires     | : 5/1/19 12:00:00 AM                                   |
| NotBefore   | : 3/1/19 12:00:00 AM                                   |
| Created     | : 12/20/18 3:00:00 PM                                  |
| Updated     | : 12/20/18 3:00:00 PM                                  |
| ContentType | :                                                      |
| Tags        | :                                                      |
| TagTable    | :                                                      |
| VaultName   | : vault1                                               |
| Name        | : Password2                                            |
| Version     | :                                                      |
| Id          | : https://vault1.vault.azure.net:443/secrets/Password2 |

アプリケーションで利用できる各シークレットはどれですか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Password1:  ▼  
Never  
Always  
Only after May 1, 2019

Password2:  ▼  
Never  
Always  
Only between March 1, 2019 and May 1, 2019

Answer:

Password1:  ▼  
Never  
Always  
Only after May 1, 2019

Password2:  ▼  
Never  
Always  
Only between March 1, 2019 and May 1, 2019

参照 :

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute>

#### 最新問題: 211

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

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

どの 2 つのアクションを実行する必要がありますか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 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. Azure Network Watcher 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. Azure Log Analytics ワークスペースを作成します。

Answer: ([解答を表示する](#))

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) への受信トラフィックと仮想マシンからの送信トラフィックをフィルターできます。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。手順には次のものが含まれます。

- \* 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、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 ログを有効にする
- \* ログデータをダウンロード
- \* ログデータの表示

参照：

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

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> (**51730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 212

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

| Name | Private IP address | Public IP address | Connected to  |
|------|--------------------|-------------------|---------------|
| VM1  | 10.7.0.4           | 51.144.245.152    | VNET1/Default |
| VM2  | 10.8.0.4           | 104.45.9.227      | VNET2/Default |

Key Vault アクセス ポリシーを、ボリューム暗号化のための Azure Disk Encryption へのアクセスを有効にするように設定します。KeyVault1 は次のように構成されています。

Save Discard

Allow access from:

☐ All networks ☒ Selected networks

**i** Configure network access control for your key vault. [Learn More](#)

Virtual networks: **i**

+ Add existing virtual networks

+ Add new virtual network

VIRTUAL NETWORK

SUBNET

RESOURCE GROUP

SUBSCRIPTION

VNET1

default

RG1

...



Microsoft

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall? **i**

☒ Yes ☐ No

**i** This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



Statements

Yes

No

From VM1, users can manage the keys and secrets stored in KeyVault1.

☐☐

From VM2, users can manage the keys and secrets stored in KeyVault1.

☐☐

VM2 can use KeyVault for Azure Disk Encryption

☐☐

Answer:





### Statements

Yes

No

From VM1, users can manage the keys and secrets stored in KeyVault1.

☒☐

From VM2, users can manage the keys and secrets stored in KeyVault1.

☒☐

VM2 can use KeyVault for Azure Disk Encryption

☒☐

### 最新問題: 213

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

| Name   | Role                 |
|--------|----------------------|
| Admin1 | Global administrator |
| Admin2 | Group administrator  |
| Admin3 | User administrator   |

Contoso.com にはグループ名前付けポリシーが含まれています。このポリシーには、Contoso という単語を含むカスタムの禁止単語リストルールがあります。

contoso.com で Contoso Sales という名前のグループを作成できるのはどのユーザーですか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Users who can create a security group named Contoso Sales:

▼

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

▼

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Answer:

Users who can create a security group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
**Admin1 and Admin3 only**  
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
**Admin1 and Admin3 only**  
Admin1, Admin2, and Admin3

参照：

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

最新問題: 214

LAW1 という名前の Azure Log Analytics ワークスペースを含む Sub1 という名前の Azure サブスクリプションがあります。Windows Server 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。システム更新評価ソリューションを LAW1 に追加する予定です。システム更新評価関連のログが 100 台の仮想マシンのみから LAW1 にアップロードされるようにする必要があります。どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                               | Answer Area |
|-------------------------------------------------------|-------------|
| Create a new workspace.                               |             |
| <b>Apply</b> the scope configuration to the solution. |             |
| Create a scope configuration.                         |             |
| Create a computer group.                              |             |
| Create a data source.                                 |             |

Answer:

Actions

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

Answer Area

Create a computer group.

Create a scope configuration.

Apply the scope configuration to the solution.



Microsoft

:

参照 :

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

### 最新問題: 215

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. グループ1を削除します。Office 365 のメンバーシップ タイプを持つ 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 [割り当て済み] 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。新しいグループを Group1 に追加します。

**Answer: B** ([メッセージを残す](#))

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については、個別のメンバーのみを追加できます。

シナリオ :

Litware は、次の ID およびアクセス要件を特定します。すべてのサンフランシスコ 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:

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |

参考文献:

<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>

### 最新問題: 216

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。

| Name      | Type            |
|-----------|-----------------|
| storage1  | Storage account |
| KeyVault1 | Azure key vault |

90 日ごとにキーを自動的に再生成するように storage1 を構成する必要があります。どのコマンドレットを実行すればよいでしょうか？

- A. セット -A=ストレージアカウント
- B. Add-AsKeyVaultmanageStorageAccount
- C. セット A;ストレージアカウント管理ポリシー
- D. 追加-A:StorogcAccountmanagementPolicyAction

Answer: ([解答を表示する](#))

最新問題: 217

オンプレミス ネットワークには、次のサーバーが含まれています。

| Name    | Operating system                    | Description                                                             |
|---------|-------------------------------------|-------------------------------------------------------------------------|
| Server1 | Windows Server 2019                 | Hyper-V host hosting four virtual machines that run Windows Server 2022 |
| Server2 | Windows Server 2019                 | File server that has the Azure Arc agent installed                      |
| Server3 | SUSE Linux Enterprise Server (SLES) | Database server that has the Azure Arc agent installed                  |

Windows Server 2019 または SLES のいずれかを実行する複数の仮想マシンを含む Azure サブスクリプションがあります。Microsoft Defender for Cloud に適応型アプリケーション コントロールを実装する予定です。どのオペレーティング システムとプラットフォームを監視できますか？ 回答するには、回答領域で適切なオプションを選択してください。

Operating systems:

SLES only

Windows Server only

SLES and Windows Server

Platforms:

Azure virtual machines only

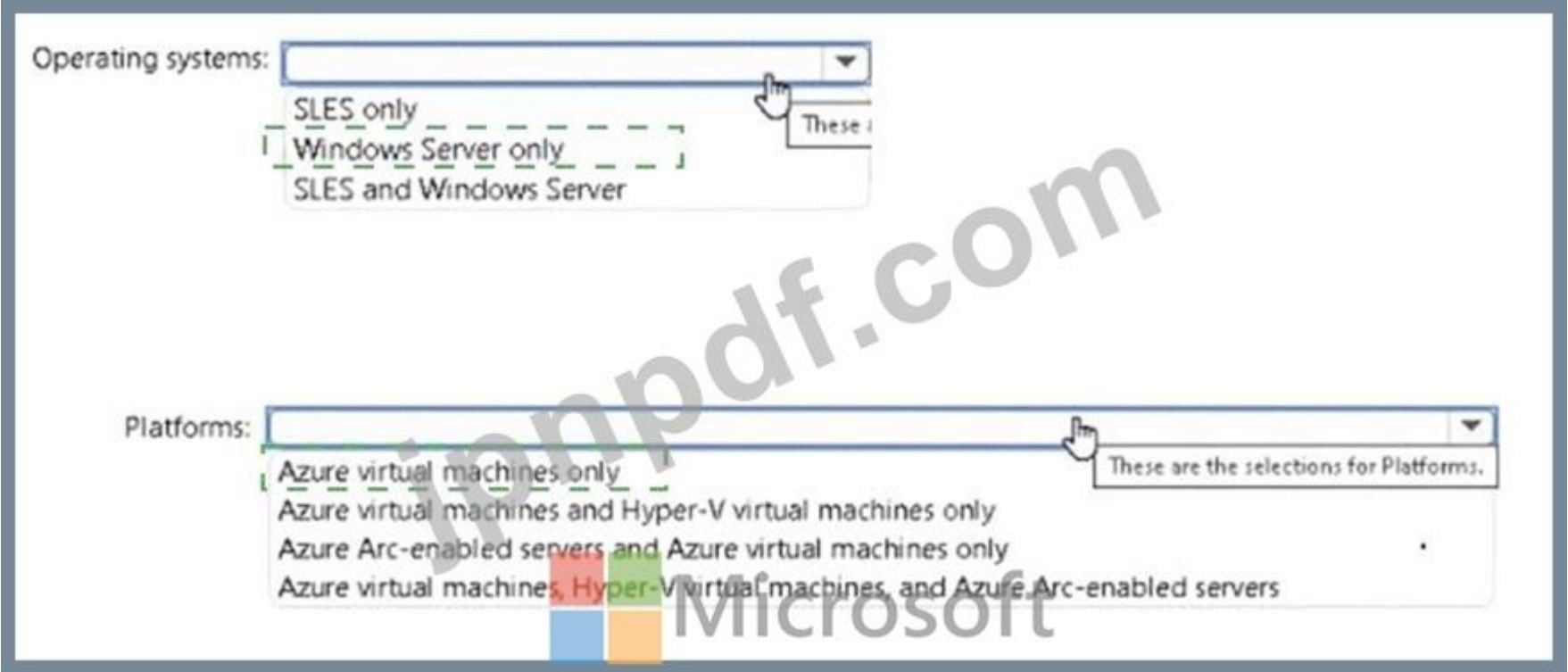
Azure virtual machines and Hyper-V virtual machines only

Azure Arc-enabled servers and Azure virtual machines only

Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

Answer:





最新問題: 218

ネットワークには、Azure Active Directory (Azure AD) と同期する adatum.com という名前のオンプレミスの Active Directory ドメインが含まれています。

Azure AD テナントには、次の表に示すユーザーが含まれています。

| Name  | Source                       | Password          |
|-------|------------------------------|-------------------|
| User1 | Azure AD                     | Adatum123         |
| User2 | Azure AD                     | N3w3rT0Gue33      |
| User3 | On-premises Active Directory | ComplexPassword33 |

次の図に示すように、adatum.com の認証方法 - パスワード保護設定を構成します。

Custom smart lockout

Lockout threshold ⓘ 10 ✓

Lockout duration in seconds ⓘ 60 ✓

Custom banned passwords

Enforce custom list ⓘ ☒ Yes ☐ No

Custom banned password list ⓘ

Adatum ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ ☒ Yes ☐ No

Mode ⓘ ☐ Enforced ☒ Audit

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/> | <input type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input type="radio"/> | <input type="radio"/> |
| User3 can change the password to Adatum123!.                       | <input type="radio"/> | <input type="radio"/> |

Answer:  
説明  
自動生成されるテキスト説明

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can change the password to Adatum123!.                       | <input checked="" type="radio"/> | <input type="radio"/>            |

参照 :  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-de>

最新問題: 219

Azure 仮想マシンのデプロイに使用する Azure Resource Manager テンプレートがあります。  
仮想マシンのインスタンスがプロビジョニングされるときに、未使用の Windows 機能を自動的に無効にする必要があります。  
何を使えばいいのでしょうか？

- A. Azure Desired State Configuration (DSC) 仮想マシン拡張機能
- B. Azure ロジック アプリ
- C. Azure Security Center のセキュリティ ポリシー
- D. Azure アドバイザ

Answer: A (メッセージを残す)

トピック 1、Litware, Inc

これはケーススタディです。ケーススタディは個別に時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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る場合があります。このケーススタディに関する各質問は、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、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に関する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なら、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、サンフランシスコ地域に 20 人の従業員を抱えるデジタル メディア企業です。

既存の環境

Litware には、Sub1 という名前の Azure サブスクリプションがあり、サブスクリプション ID は次のとおりです。

43894a43-17c2-4a39-8cfc-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 AD Premium P2 ライセンスが割り当てられます。Azure AD Privileged Identity Management (PIM) がアクティブ化されています。

テナントには、次の表に示すグループが含まれています。

| Name   | Type           | Description                                                                                                                                                     |
|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team                                                                              |



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。

| Name            | Type               | Description                                                                                                                                             |
|-----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| VNet1           | Virtual network    | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0             | Virtual machine    | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.                    |
| VM1             | Virtual machine    | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.                                                                  |
| SQLDB1          | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.                                                                       |
| WebApp1         | Web app            | WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.                                           |
| Resource Group1 | Resource group     | Resource Group1 is a resource group that contains VNet1, VM0, and VM1.                                                                                  |
| Resource Group2 | Resource group     | Resource Group2 is a resource group that contains shared IT resources.                                                                                  |

Azure Security Center は無料レベル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。

| Name      | Type                           | Description                                                                                                           |
|-----------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Firewall1 | Azure Firewall                 | An Azure firewall on VNet1.                                                                                           |
| RT1       | Route table                    | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1      | Azure Kubernetes Service (AKS) | A managed AKS cluster                                                                                                 |

Litware は、次の ID およびアクセス要件を特定します。

- \* すべてのサンフランシスコ 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 のメンバーには、永続的な適格な割り当てを使用して、リソース グループ 2 への共同作成者ロールを割り当てる必要があります。
- \* ユーザーが Azure AD にアプリケーションを登録したり、アプリケーションに同意したりできないようにする必要があります
- \* ユーザーに代わって企業情報にアクセスします。

プラットフォームの保護要件

Litware は、次のプラットフォーム保護要件を特定します。

- \* Microsoft Antimalware は、リソース グループ 1 の仮想マシンにインストールする必要があります。
- \* Group2 のメンバーには、Azure Kubernetes Service Cluster Admin ロールが割り当てられている必要があります。
- \* Azure AD ユーザーは、Azure AD 資格情報を使用して 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 JIT VM アクセスを使用して VM0 に接続できる必要があります。
- \* Resource Group1 のマネージド 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



まず、役割 1 は、リソース グループ 1 に対して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、Azure Security Center でオペレーティング システムのセキュリティ構成をカスタマイズする必要があります。

最新問題: 220

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

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

ポータル ポリシーの条件設定は、条件の説明に示されているように構成されます。( 条件」タブをクリックします。)

Portal Policy

InfoDelete

Name

Portal Policy

Assignments

Users and groups1

All users

Cloud apps1

1 app included

Conditions1

1 condition selected

Access controls

Grant1

2 controls selected

Session1

0 controls selected

Conditions

Info

Device platforms1

Not configured

Locations1

1 included

Client apps (preview)1

Not configured

Device state (preview)1

Not configured

Locations

Close

Control user access based on their physical location. Learn more

Configure1

YesNo

IncludeExclude

Any location

All trusted locations

Selected locations

Select

Contoso

Contoso

...

ポータル ポリシーの付与設定は、付与」の図に示されているように構成されます。( 付与」タブをクリックします。)

## Portal Policy

Info

Delete

\* Name

Portal Policy

### Assignments

Users and groups ⓘ

All users

Cloud apps ⓘ

1 app included

Conditions ⓘ

1 condition selected

### Access controls

Grant ⓘ

2 controls selected

Session ⓘ

0 controls selected

## Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ

See list of approved client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                                                                    | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input type="radio"/> |

Answer:

説明

ボックス 1: いいえ

Contoso の場所は除外されます

ボックス 2: いいえ

ボックス 3: いいえ

参照 :

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

最新問題: 221

Subscription1 という名前の Azure サブスクリプションがあり、これには RG1 という名前のリソース グループと User1 という名前のユーザーが含まれています。User1 には、RG1 の所有者の役割が割り当てられます。

次の図に示すように、RG2 という名前のリソース グループを含む Blueprint1 という名前の Azure Blueprints 定義を作成します。



次の設定を使用して、Blueprint1 を Subscription1 に割り当てます。

\* ロックの割り当て: 読み取り専用

\* マネージド ID: システム割り当て

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                  | Yes                   | No                    |
|-------------------------------------------------------------|-----------------------|-----------------------|
| A locking mode of Read Only will be assigned to RG1.        | <input type="radio"/> | <input type="radio"/> |
| User1 can add tags to RG2.                                  | <input type="radio"/> | <input type="radio"/> |
| You can remove User1 from the Tag Contributor role for RG2. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                  | Yes                              | No                               |
|-------------------------------------------------------------|----------------------------------|----------------------------------|
| A locking mode of Read Only will be assigned to RG1.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| User1 can add tags to RG2.                                  | <input checked="" type="radio"/> | <input type="radio"/>            |
| You can remove User1 from the Tag Contributor role for RG2. | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーションの説明が自動生成される

| Statements                                                  | Yes                   | No                    |
|-------------------------------------------------------------|-----------------------|-----------------------|
| A locking mode of Read Only will be assigned to RG1.        | <input type="radio"/> | <input type="radio"/> |
| User1 can add tags to RG2.                                  | <input type="radio"/> | <input type="radio"/> |
| You can remove User1 from the Tag Contributor role for RG2. | <input type="radio"/> | <input type="radio"/> |

参照：

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

最新問題: 222

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。

| Name       | Type                          | Region      | Resource group |
|------------|-------------------------------|-------------|----------------|
| SQL1       | Azure SQL database            | East US     | RG1            |
| Analytics1 | Azure Log Analytics workspace | East US     | RG1            |
| Analytics2 | Azure Log Analytics workspace | East US     | RG2            |
| Analytics3 | Azure Log Analytics workspace | West Europe | RG1            |

次の表に示す Azure ストレージ アカウントを作成します。



| Name     | Region      | Resource group | Storage account type | Access tier (default) |
|----------|-------------|----------------|----------------------|-----------------------|
| Storage1 | East US     | RG1            | Blob                 | Cool                  |
| Storage2 | East US     | RG2            | General purpose V1   | Not applicable        |
| Storage3 | West Europe | RG1            | General purpose V2   | Hot                   |

SQL1 の監査を構成する必要があります。

監査ログの保存先として使用できるストレージ アカウントと Log Analytics ワークスペースはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

**Answer Area**

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

**Answer:**

Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

最新問題: 223

Azure Key Vault と Azure Storage アカウントを含む Azure サブスクリプションを持っています。Key Vault 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 コンテナーに保存されているカスタマー マネージド 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予定です。

- \* Azure ファイル
- \* Azure Blob ストレージ
- \* Azure ログ分析
- \* Azure テーブル ストレージ
- \* Azure キュー ストレージ

Key Vault に保存されているキーを使用してデータ暗号化を行う 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示します。

注: 正しく選択するたびに 1 ポイントの価値があります。

- A. キューストレージ
- B. テーブル収納
- C. Azure ファイル
- D. BLOB ストレージ

**Answer: A,C** ([メッセージを残す](#))

<https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal>

最新問題: 224

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

Azure Sentinel でのインシデントの軽減を自動化する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。何を作成する必要がありますか？

- A. アラート ルール
- B. ランブック
- C. 関数アプリ
- D. プレイブック

**Answer: C** ([メッセージを残す](#))

最新問題: 225

Azure Sentinel を使用して、疑わしい脅威を検出し、対応を自動化する分析ルールを作成する予定です。

ルールにはどのコンポーネントが必要ですか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Detect suspicious threats:

|                              |
|------------------------------|
| A Kusto query language query |
| A Transact-SQL query         |
| An Azure PowerShell query    |
| An Azure Sentinel playbook   |

Automate responses:

|                            |
|----------------------------|
| An Azure Functions app     |
| An Azure PowerShell script |
| An Azure Sentinel playbook |
| An Azure Sentinel workbook |

**Answer:**



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

最新問題: 226

あなたの会社には、Subscription1 という名前の Azure サブスクリプションがあります。Subscription1 は、次の表に示すユーザーを含む Azure Active Directory テナントに関連付けられています。

| Name  | Role                  |
|-------|-----------------------|
| User1 | Global administrator  |
| User2 | Billing administrator |
| User3 | Owner                 |
| User4 | Account Admin         |

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ますか?そのユーザーはどのツールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

User: 

|       |
|-------|
| User1 |
| User2 |
| User3 |
| User4 |

Tool: 

|                       |
|-----------------------|
| Azure Account Center  |
| Azure Cloud Shell     |
| Azure PowerShell      |
| Azure Security Center |

Answer:

User: 

|       |
|-------|
| User1 |
| User2 |
| User3 |
| User4 |

Tool: 

|                       |
|-----------------------|
| Azure Account Center  |
| Azure Cloud Shell     |
| Azure PowerShell      |
| Azure Security Center |

参照：



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> (**51730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 227

Contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられている、Sub 1 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ます。

| Name  | Role                   |
|-------|------------------------|
| User1 | Global administrator   |
| User2 | Security administrator |
| User3 | Security reader        |
| User4 | License administrator  |

各ユーザーには Azure AD Premium P2 ライセンスが割り当てられます。  
オンボードを計画し、Azure AD ID Protection を構成します。  
Azure AD Identity Protection をオンボードし、ユーザーを修復し、ポリシーを構成できるのはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

Answer:

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only  
User1 and User2 only  
User1, User 2, and User3 only  
User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only  
User1 and User3 only  
User1, User 2, and User3 only  
User1, User 2, User3, and User 4

最新問題: 228

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 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。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area



Answer:

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

最新問題: 229

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。

| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

You create the resource locks shown in the following table.

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



### Statements

Yes

No

You can start VM1.

☐☐

You can start VM2.

☐☐

You can create a virtual machine in RG2.

☐☐

Answer:

### Answer Area



### Statements

Yes

No

You can start VM1.

☐☒

You can start VM2.

☒☐

You can create a virtual machine in RG2.

☒☐

説明



Answer Area

Microsoft

| Statements                               | Yes                              | No                               |
|------------------------------------------|----------------------------------|----------------------------------|
| You can start VM1.                       | <input type="radio"/>            | <input checked="" type="radio"/> |
| You can start VM2.                       | <input checked="" type="radio"/> | <input type="radio"/>            |
| You can create a virtual machine in RG2. | <input checked="" type="radio"/> | <input type="radio"/>            |

参考文献:  
<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

最新問題: 230

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。

| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

You create the resource locks shown in the following table.

Microsoft

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

| Statements                               | Yes                   | No                    |
|------------------------------------------|-----------------------|-----------------------|
| You can start VM1.                       | <input type="radio"/> | <input type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input type="radio"/> |

Answer:

When Azure Sentinel identifies a threat, an incident must be created:

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

Analytics  
Data connectors  
Playbooks  
Workbooks

Analytics  
Data connectors  
Playbooks  
Workbooks

説明

Answer Area

| Statements                               | Yes                              | No                               |
|------------------------------------------|----------------------------------|----------------------------------|
| You can start VM1.                       | <input type="radio"/>            | <input checked="" type="radio"/> |
| You can start VM2.                       | <input checked="" type="radio"/> | <input type="radio"/>            |
| You can create a virtual machine in RG2. | <input checked="" type="radio"/> | <input type="radio"/>            |

参考文献:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

最新問題: 231

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

| Name  | Type               | In resource group |
|-------|--------------------|-------------------|
| cont1 | Container instance | RG1               |
| VNET1 | Virtual network    | RG1               |
| App1  | App Service app    | RG1               |
| VM1   | Virtual machine    | RG1               |
| User1 | User               | Not applicable    |

次の JSON ファイルを使用して、Subscription1 にカスタム RBAC ロールを作成します。

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

RG1 で、Role1 を User1 に割り当てます。  
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                      | Yes                   | No                    |
|---------------------------------|-----------------------|-----------------------|
| User1 can add VM1 to VNET1.     | <input type="radio"/> | <input type="radio"/> |
| User1 can start and stop App1.  | <input type="radio"/> | <input type="radio"/> |
| User1 can start and stop cont1. | <input type="radio"/> | <input type="radio"/> |

Answer:



Yes

No

User1 can add VM1 to VNET1.

☐☒

User1 can start and stop App1.

☐☒

User1 can start and stop cont1.

☐☒

参照 :

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute>

#### 最新問題: 232

cotoso.com という名前の Azure Active Director (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。Contoso.com にはグループ名前付けポリシーが含まれています。このポリシーには、Contoso という単語を含むカスタムの禁止単語リストルールがあります。

注: 正しい選択はそれぞれポイントの価値があります。

| Answer Area                                                   |                                                                                                                                                                                                   |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Users who can create a security group named Contoso Sales:    | <input type="checkbox"/> Admin1 only<br><input type="checkbox"/> Admin1 and Admin2 only<br><input type="checkbox"/> Admin1 and Admin3 only<br><input type="checkbox"/> Admin1, Admin2, and Admin3 |
| Users who can create an Office 365 group named Contoso Sales: | <input type="checkbox"/> Admin1 only<br><input type="checkbox"/> Admin1 and Admin2 only<br><input type="checkbox"/> Admin1 and Admin3 only<br><input type="checkbox"/> Admin1, Admin2, and Admin3 |

Answer:

| Answer Area                                                   |                                                                                                                                                                                                              |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Users who can create a security group named Contoso Sales:    | <input checked="" type="checkbox"/> Admin1 only<br><input type="checkbox"/> Admin1 and Admin2 only<br><input type="checkbox"/> Admin1 and Admin3 only<br><input type="checkbox"/> Admin1, Admin2, and Admin3 |
| Users who can create an Office 365 group named Contoso Sales: | <input checked="" type="checkbox"/> Admin1 only<br><input type="checkbox"/> Admin1 and Admin2 only<br><input type="checkbox"/> Admin1 and Admin3 only<br><input type="checkbox"/> Admin1, Admin2, and Admin3 |

#### 最新問題: 233

OU2 と User1 に対して計画された変更を実行する必要があります。

どのツールを使用する必要がありますか? 答えるには、適切なツールを正しいリソースにドラッグします。各ツールは 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: 正しく選択するたびに 1 ポイントの価値があります。



Tools

The Azure portal

Azure AD Connect

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

Answer Area

OU2:

Tool

User1:

Tool

Answer:

Tools

The Azure portal

Azure AD Connect

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

Answer Area

OU2:

Azure AD Connect

User1:

The Azure portal

最新問題: 234

ID という名前のマネージド 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 および AU2 にはどのリソースを追加できますか? 回答するには、回答領域で適切なオプションを選択してください。

| Name   | Type                | Assigned object |
|--------|---------------------|-----------------|
| AU1    | Administrative unit | User1, Group1   |
| AU2    | Administrative unit | None            |
| User1  | User                | Not applicable  |
| Group1 | Security group      | Not applicable  |
| Group2 | Microsoft 365 group | Not applicable  |

AU1 と AU2 にはどのリソースを追加できますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

AU1:

- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:

- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and Identity1 only

Answer:

Answer Area

AU1:

- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:

- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and Identity1 only

最新問題: 235

Azure Key Vault を作成する必要があります。このソリューションでは、キー コンテナー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ればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

Answer:

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

参照 :

**最新問題: 236**

コンテナ化されたアプリケーション インスタンス用の新しいストレージ アカウントを作成する Function1 という名前の Azure 関数を実装する予定です。

ストレージ アカウントを作成するために、Function1 に最低限必要な権限を付与する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

Assign role to:

|                                    |
|------------------------------------|
| A group account                    |
| A system-assigned managed identity |
| A user account                     |
| A user-assigned managed identity   |

Role assignment to create:

|                                                         |
|---------------------------------------------------------|
| Built-in role assignment                                |
| Classic administrator role assignment                   |
| Custom role-based access control (RBAC) role assignment |

**Answer:**

Assign role to:

|                                    |
|------------------------------------|
| A group account                    |
| A system-assigned managed identity |
| A user account                     |
| A user-assigned managed identity   |

Role assignment to create:

|                                                         |
|---------------------------------------------------------|
| Built-in role assignment                                |
| Classic administrator role assignment                   |
| Custom role-based access control (RBAC) role assignment |

参照 :

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

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



最新問題: 237

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。

各サブスクリプションについて、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 に対する権限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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Configure role-based access control (RBAC) role assignments by using:

Azure Blueprints

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

A resource lock

A role-based access control (RBAC) role assignment at the resource group level

Azure Blueprint assignments in locking mode

Answer:

Configure role-based access control (RBAC) role assignments by using:

Azure Blueprints

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

A resource lock

A role-based access control (RBAC) role assignment at the resource group level

Azure Blueprint assignments in locking mode

最新問題: 238

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

次の表に示すように、Registry1 の役割の割り当てを追加します。

| User  | Role           |
|-------|----------------|
| User1 | AcrPush        |
| User2 | AcrPull        |
| User3 | AcrImageSigner |
| User4 | Contributor    |

Registry1 にイメージをアップロードしたり、Registry1 からイメージをダウンロードしたりできるのはどのユーザーですか？ 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: 正しく選択するたびに 1 ポイントの価値があります。



Upload images:

User1 only

User1 and User4 only

User1, User3, and User4

User1, User2, User3, and User4

Download images:

User2 only

User1 and User2 only

User2 ad User4 only

User1, User2, and User4

User1, User2, User3, and User4

Answer:



Upload images:

User1 only

User1 and User4 only

User1, User3, and User4

User1, User2, User3, and User4

Download images:

User2 only

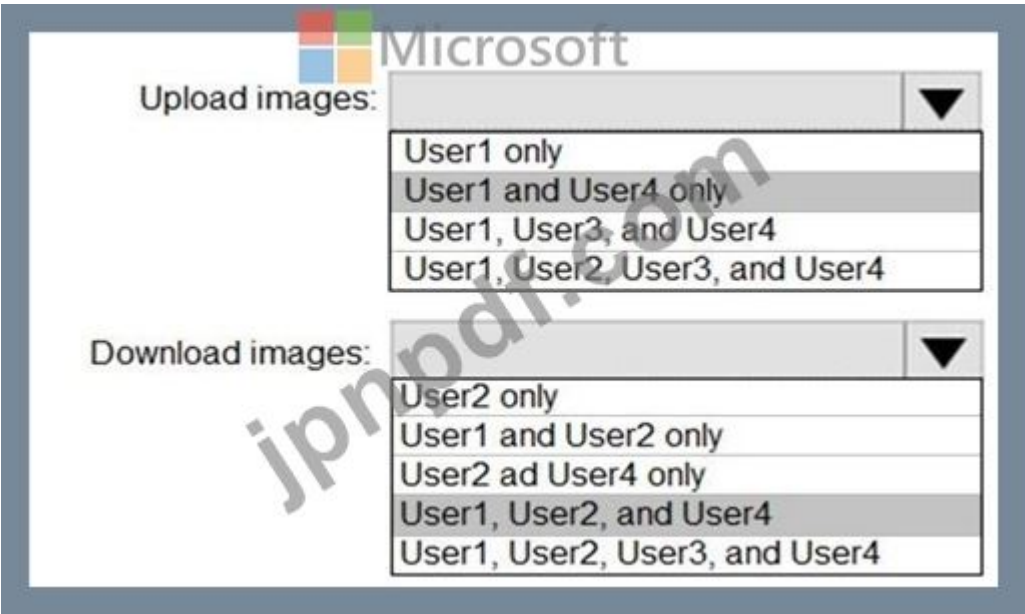
User1 and User2 only

User2 ad User4 only

User1, User2, and User4

User1, User2, User3, and User4

説明



ボックス 1: User1 と User4 のみ

所有者、投稿者、および AcrPush は画像をプッシュできます。

ボックス 2: ユーザー 1、ユーザー 2、およびユーザー 4

AcrImagineSigner を除くすべてのツールは、イメージをダウンロード/プルできます。

| Role/Permission | Access Resource Manager | Create/delete registry | Push image | Pull image | Delete image data | Change policies | Sign images |
|-----------------|-------------------------|------------------------|------------|------------|-------------------|-----------------|-------------|
| Owner           | X                       | X                      | X          | X          | X                 | X               |             |
| Contributor     | X                       | X                      | X          | X          | X                 | X               |             |
| Reader          | X                       |                        |            | X          |                   |                 |             |
| AcrPush         |                         |                        | X          | X          |                   |                 |             |
| AcrPull         |                         |                        |            | X          |                   |                 |             |
| AcrDelete       |                         |                        |            |            | X                 |                 |             |
| AcrImageSigner  |                         |                        |            |            |                   |                 | X           |

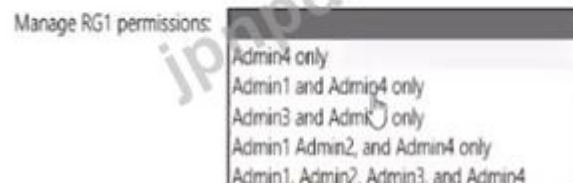
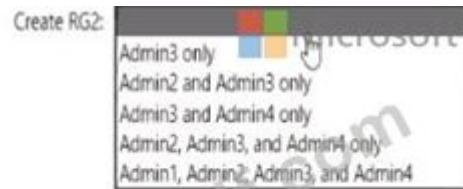
参考文献:

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

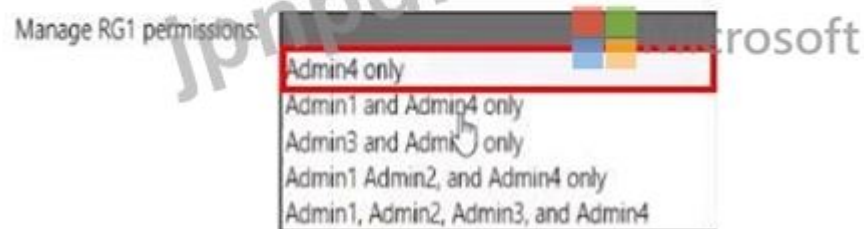
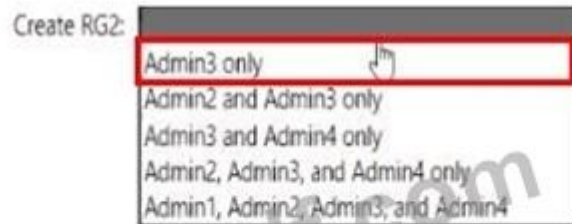
最新問題: 239

RG2 の作成と RG1 の権限の管理を委任する必要があります。各タスクを実行できるのはどのユーザーですか? 回答するには、回答内の適切なオプションを選択してください。

a. 注正しく選択するたびに 1 ポイントの価値があります



**Answer:**



#### 最新問題: 240

Azure サブスクリプションをお持ちです。サブスクリプションには、Windows Server を実行する Azure 仮想マシンが含まれています  
2016年。

各仮想マシンにカスタムのマルウェア対策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ポリシーを実装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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

```

{
  "if" : {
    "allof": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      }
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : "
    Append
    Deny
    DeployIfNotExists
    ",
    "details": {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            "
            existenceCondition
            resources
            template
            ": {
          }
        }
      }
    }
  }
}

```

Answer:





# Microsoft

```

{
  "if" : {
    "allOf" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      },
      {
        "field" : "Microsoft.Compute/imagesSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : " ",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            " ",
            " ": {
              "existenceCondition",
              "resources",
              "template"
            }
          }
        }
      }
    }
  }
}

```

説明



# Microsoft

```

"then" : {
  "effect" : " ",
  "details" : {
    "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
    "roleDefinitionsIds" : [
      "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
    ],
    "name" : "customExtension",
    "deployment" : {
      "properties" : {
        "mode": "incremental",
        "parameters" : {
          " ",
          " ": {
            "existenceCondition",
            "resources",
            "template"
          }
        }
      }
    }
  }
}

```

ボックス 1: DeployIfNotExists

DeployIfNotExists は、条件が満たされた場合にテンプレートのデプロイメントを実行します。

ボックス 2: テンプレート

DeployIfNotExists エフェクトの詳細プロパティには、一致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。

導入 [必須]

このプロパティには、Microsoft.Resources/deployment References 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: 241

Azure サブスクリプションをお持ちです。

別の Azure Active Directory (Azure AD) テナントを使用するようにサブスクリプションを構成します。

この変更により考えられる 2 つの影響は何ですか? それぞれの正解は完全な解決策を示します。

注: 正しく選択するたびに 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が失われます。
- B. 仮想マシンの管理対象 ID が失われます。
- 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: ([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/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

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> (**51730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 242

Azure Active Directory (Azure AD) にリンクされた 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ます。

| Name  | Role                   | Member of      |
|-------|------------------------|----------------|
| User1 | Security administrator | Group1         |
| User2 | Network Contributor    | Group2         |
| User3 | Key Vault Contributor  | Group1, Group2 |

Vault1 という名前の Azure Key Vault があり、ページ保護が無効に設定されています。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。

| Name   | Key permission | Secret permission | Certificate permission |
|--------|----------------|-------------------|------------------------|
| Group1 | Purge          | Purge             | Purge                  |
| Group2 | Select all     | Select all        | Select all             |

次の表に示すように、Vault1 のロール割り当てを作成します。

| Name  | Role                      |
|-------|---------------------------|
| User1 | None                      |
| User2 | Key Vault Reader          |
| User3 | User Access Administrator |

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、それ以外の場合は [いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area



Statements

User1 can set Purge protection to Enable for Vault1.

User2 can configure firewalls and virtual networks for Vault1.

User3 can add access policies to Vault1.

Yes

No

Answer:

Answer Area



Statements

User1 can set Purge protection to Enable for Vault1.

User2 can configure firewalls and virtual networks for Vault1.

User3 can add access policies to Vault1.

Yes

No

最新問題: 243

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。

| Name        | Type                  | Region      |
|-------------|-----------------------|-------------|
| RG1         | Resource group        | West Europe |
| VNET1       | Azure virtual network | West Europe |
| Contoso1901 | Azure Storage account | West Europe |

VNET1 には、Subnet1 と 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、展示に示すように構成されています。(「展示」タブをクリックします。)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
ByPass      : Logging, Metrics
DefaultAction : Deny
IpRules      : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules
Action IPAddressOrRange
-----
Allow  193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules
Action VirtualNetworkResourceId
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1
State
-----
Succeeded
```

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/> | <input type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input type="radio"/> | <input type="radio"/> |

| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| An Azure virtual machine on Subnet1 can access data in Contoso1901.                              | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure virtual machine on Subnet2 can access data in Contoso1901.                              | <input type="radio"/>            | <input checked="" type="radio"/> |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 244  
Contosos.com という名前の Azure Active Directory (Azure AD) テナントと RG1 という名前のリソース グループを含む、Subscription1 という



う名前の Azure サブスクリプションがあります。  
contoso.com に対して、Role1 という名前のカスタム ロールを作成します。  
権限の委任にRole1をどこで利用できるかを特定する必要があります。  
何を識別する必要がありますか？

- A. contoso.com のみ
- B. contoso.com および RGT のみ
- C. contoso.com、RG1、および Subscription1
- D. contoso.com および Subscription1 のみ

Answer: B (メッセージを残す)

最新問題: 245

月曜日に、ユーザー user1@contoso.com に通知するように Azure Security Center で電子メール通知を構成します。  
火曜日に、セキュリティ センターは次の表に示すセキュリティ アラートを生成します。

| Time  | Description                                             | Severity |
|-------|---------------------------------------------------------|----------|
| 01:00 | Failed RDP brute force attack                           | Medium   |
| 01:01 | Successful RDP brute force attack                       | High     |
| 06:10 | Suspicious process executed                             | High     |
| 09:00 | Malicious SQL activity                                  | High     |
| 11:15 | Network communication with a malicious machine detected | Low      |
| 13:30 | Suspicious process executed                             | High     |
| 14:00 | Failed RDP brute force attack                           | Medium   |
| 16:01 | Successful RDP brute force attack                       | High     |
| 23:20 | Possible outgoing spam activity detected                | Low      |
| 23:25 | Modified system binary discovered in dump file          | High     |
| 23:30 | Malicious SQL activity                                  | High     |

user1@contoso.com は火曜日に何件の電子メール通知を受け取りますか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

|   |
|---|
| ▼ |
| 1 |
| 2 |
| 3 |
| 4 |

Total number of Security Center email notifications on Tuesday:

|    |
|----|
| ▼  |
| 3  |
| 4  |
| 6  |
| 9  |
| 11 |

Answer:

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

|   |
|---|
| ▼ |
| 1 |
| 2 |
| 3 |
| 4 |

Total number of Security Center email notifications on Tuesday:

|    |
|----|
| ▼  |
| 3  |
| 4  |
| 6  |
| 9  |
| 11 |

参照 :

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

最新問題: 246

Azure Key Vault を作成する必要があります。このソリューションでは、キー コンテナー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ればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
-Location 'East US'
```

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

Answer:

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
-Location 'East US'
```

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

説明

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
-Location 'East US'
```

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

ボックス 1: -EnablePurgeProtection

指定した場合、このコンテナに対して即時削除に対する保護が有効になります。論理的な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 コンテナに対して論理的な削除機能が有効であることを指定します。論理的な削除が有効になっている場合、削除後に猶予期間の間、このキー コンテナとその内容を回復できます。

参考文献:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

最新問題: 247

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



## Statements

Yes

No

From VM1, you can successfully ping the private IP address of VM4.

☐☐

From VM2, you can successfully ping the private IP address of VM4.

☐☐

From VM1, you can connect to the web server on VM4.

☐☐

Answer:

Container registries:

|   | ▼ |
|---|---|
| 0 |   |
| 1 |   |
| 2 |   |
| 3 |   |

Workspaces:

|   | ▼ |
|---|---|
| 0 |   |
| 1 |   |
| 2 |   |
| 3 |   |

説明



Microsoft

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the private IP address of VM4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM2, you can successfully ping the private IP address of VM4. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can connect to the web server on VM4.                | <input checked="" type="radio"/> | <input type="radio"/>            |

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 のみを許可しますが、ASG1 からの ICMP ping は許可しません。ASG1 からは TCP トラフィックのみが許可されます。  
NSG3 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | Any  | TCP      | ASG1              | ASG1           | Allow  |
| 150      | Any  | Any      | ASG2              | VirtualNetwork | Allow  |
| 200      | Any  | Any      | Any               | Any            | Deny   |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

ボックス 2: はい。  
VM2 は ASG2 にあります。ASG2 からは任意のプロトコルが許可されるため、ICMP ping が許可されます。  
ボックス3。VM1 は ASG1 にあります。ASG1 からの TCP トラフィックが許可されるため、Web サーバーへの接続はポート TCP 80 または TCP 443 上で行われるため、VM1 は Web サーバーに接続できます。

最新問題: 248

Sub1 という名前の Azure サブスクリプションがあります。  
Azure Security Center には、WF1 という名前のワークフロー自動化があります。WF1 は、User1 という名前のユーザーに電子メール メッセージを送信するように構成されています。  
Alerts という名前の配布グループに電子メール メッセージを送信するには、WF1 を変更する必要があります。  
WF1 を変更するには何を使用する必要がありますか？

- A. Azure Application Insights
- B. Azure モニター
- C. Azure Logic Apps デザイナー
- D. Azure DevOps

Answer: (解答を表示する)

参照 :  
<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>  
<https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure->  
最新問題: 249

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

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

このタスクを完了するには、Azure portal にサインインします。

Azure Monitor でアラート ルールを構成する必要があります。

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

「アラート」をクリックします。

[+新しいアラート ルール] をクリックします。

「スコープ」セクションで、「リソースの選択」リンクをクリックします。

[リソースの種類でフィルター] ボックスに 「locks」と入力し、フィルターされた結果から [管理ロック (ロック)] を選択します。

サブスクリプションを選択し、完了」ボタンをクリックします。

「条件」セクションで、条件の選択」リンクをクリックします。

「管理ロックの削除」条件を選択し、完了」ボタンをクリックします。

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

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

グループに Debbie Mobile App」などの名前を付けて (試験用に入力する名前は関係ありません)、次へ: 通知 >」ボタンをクリックします。

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

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

OK」ボタンをクリックしてウィンドウを閉じます。

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

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

C. 通知名ボックスに Debbie Mobile App」などの名前を入力します。

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

Answer: A ([メッセージを残す](#))

最新問題: 250

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。

| Name    | Type                         | Attached to    | NSG            |
|---------|------------------------------|----------------|----------------|
| NSG1    | Network security group (NSG) | VM5            | Not applicable |
| NSG2    | Network security group (NSG) | Subnet1        | Not applicable |
| Subnet1 | Subnet                       | Not applicable | Not applicable |
| VM5     | Virtual machine              | Subnet1        | NSG1           |

IP アドレス 10.1.0.4 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

+ Add  Save  Discard

Configure the ports for which the just-in-time VM access will be applicable

| Port | Protocol | Allowed source IPs | IP range | Time range (hours) |     |
|------|----------|--------------------|----------|--------------------|-----|
| 3389 | Any      | Per request        | N/A      | 3 hours            | ... |

VM5 の JIT VM アクセスを有効にします。  
NSG1 には、次の図に示す受信ルールがあります。

| Priority | Name                                                                                                            | Port | Protocol | Source            | Destination    | Action                                                                                      |
|----------|-----------------------------------------------------------------------------------------------------------------|------|----------|-------------------|----------------|---------------------------------------------------------------------------------------------|
| 100      |  SecurityCenter-JITRule-...    | 3389 | Any      | Any               | 10.1.0.4       |  Allow   |
| 1000     | SecurityCenter-JITRule_341...                                                                                   | 3389 | Any      | Any               | 10.1.0.4       |  Deny    |
| 1001     | RDP                                                                                                             | 3389 | TCP      | Any               | Any            |  Allow  |
| 65000    | AllowVnetInBound                                                                                                | Any  | Any      | VirtualNetwork    | VirtualNetwork |  Allow |
| 65001    |  AllowAzureLoadBalancerIn... | Any  | Any      | AzureLoadBalancer | Any            |  Allow |
| 65500    |  DenyAllInBound              | Any  | Any      | Any               | Any            |  Deny  |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                         | Yes                   | No                    |
|----------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input type="radio"/> | <input type="radio"/> |
| Remote Desktop access to VM5 is blocked.                                                           | <input type="radio"/> | <input type="radio"/> |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.                  | <input type="radio"/> | <input type="radio"/> |

Answer:



| Statements                                                                                         | Yes                              | No                               |
|----------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Remote Desktop access to VM5 is blocked.                                                           | <input checked="" type="radio"/> | <input type="radio"/>            |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.                  | <input type="radio"/>            | <input checked="" type="radio"/> |

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が含まれる Group1 という名前の Azure Active Directory (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、再起動できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Answer:

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area



参照 :  
<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

最新問題: 252

Azure AD Premium P2 を使用して Azure サブスクリプションを作成します。  
Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を使用して Azure ロールを保護できることを確認する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                                          | Answer Area |
|------------------------------------------------------------------|-------------|
| Discover privileged roles.                                       |             |
| Sign up PIM for Azure AD roles.                                  |             |
| Consent to PIM.                                                  |             |
| Discover resources.                                              |             |
| Verify your identity by using multi-factor authentication (MFA). |             |

Answer:

| Actions                                                          | Answer Area                                                      |
|------------------------------------------------------------------|------------------------------------------------------------------|
| Discover privileged roles.                                       | Verify your identity by using multi-factor authentication (MFA). |
| Sign up PIM for Azure AD roles.                                  | Consent to PIM.                                                  |
| Consent to PIM.                                                  | Sign up PIM for Azure AD roles.                                  |
| Discover resources.                                              |                                                                  |
| Verify your identity by using multi-factor authentication (MFA). |                                                                  |

説明  
1. MFA で本人確認を行う

- 2. PIMへの同意
- 3. AAD ロールの PIM にサインアップする

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。  
IT チームのすべてのメンバーが含まれる Group1 という名前の Azure Active Directory (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、再起動できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Answer:

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

参照 :  
<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

最新問題: 254

3 つのストレージ アカウント、SQL という名前の Azure SQL マネージド インスタンス、および 3 つの Azure SQL データベースを含む Azure サブスクリプションがあります。ストレージ アカウントは次の表に示すように構成されています。  
SQ11 には次の設定があります。

- \* 監査: オン
- \* 監査宛先: storage1

Azure SQL データベースは、次の表に示すように構成されています。

Answer Area

| Statements                                                 | Yes                   | No                    |
|------------------------------------------------------------|-----------------------|-----------------------|
| Audit events for DB1 are written to storage1.              | <input type="radio"/> | <input type="radio"/> |
| Audit events for DB2 are written to storage1 and storage2. | <input type="radio"/> | <input type="radio"/> |
| Storage3 can be used as an audit log destination for DB3.  | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                                 | Yes                              | No                               |
|------------------------------------------------------------|----------------------------------|----------------------------------|
| Audit events for DB1 are written to storage1.              | <input checked="" type="radio"/> | <input type="radio"/>            |
| Audit events for DB2 are written to storage1 and storage2. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Storage3 can be used as an audit log destination for DB3.  | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

Answer Area

|                                                            |                                  |                                  |
|------------------------------------------------------------|----------------------------------|----------------------------------|
| Audit events for DB1 are written to storage1.              | <input checked="" type="radio"/> | <input type="radio"/>            |
| Audit events for DB2 are written to storage1 and storage2. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Storage3 can be used as an audit log destination for DB3.  | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure>

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview>

最新問題: 255

新しい Azure Active Directory (Azure AD) テナントに関連付けられた新しい Azure サブスクリプションを作成します。  
ポータル ポリシーという名前のアクティブな条件付きアクセス ポリシーを 1 つ作成します。ポータル ポリシーは、Microsoft Azure 管理クラウド アプリへのアクセスを提供するために使用されます。  
ポータル ポリシーの条件設定は、条件の説明に示されているように構成されます。( 条件」タブをクリックします。)



Portal Policy

InfoDelete

Name

Portal Policy

Assignments

Users and groups1

All users

Cloud apps1

1 app included

Conditions1

1 condition selected

Access controls

Grant1

2 controls selected

Session1

0 controls selected

Conditions

Info

Device platforms1

Not configured

Locations1

1 included

Client apps (preview)1

Not configured

Device state (preview)1

Not configured

Locations

Control user access based on their physical location. Learn more

Configure1

YesNo

IncludeExclude

Any location

All trusted locations

Selected locations

Select

Contoso

Contoso...

ポータル ポリシーの付与設定は、「付与」の図に示されているように構成されます。(「付与」タブをクリックします。)

Portal Policy

InfoDelete

Name

Portal Policy

Assignments

Users and groups1

All users

Cloud apps1

1 app included

Conditions1

1 condition selected

Access controls

Grant1

2 controls selected

Session1

0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication1

Require device to be marked as compliant1

Require Hybrid Azure AD joined device1

Require approved client app1

See list of approved client apps

For multiple controls

Require all the selected controls

Require one of the selected controls



次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                                                                    | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                                                                    | Yes                   | No                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------------|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                                  | <input type="radio"/> | <input checked="" type="radio"/> |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | <input type="radio"/> | <input checked="" type="radio"/> |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.                           | <input type="radio"/> | <input checked="" type="radio"/> |

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

最新問題: 256

User1 という名前のユーザーと storage 1 という名前のストレージ アカウントを含む Azure サブスクリプションがあります。storage1 アカウントには、次の表に示すリソースが含まれています。

| Name       | Type       |
|------------|------------|
| container1 | Container  |
| folder1    | File share |
| table1     | Table      |

- User1 には、storage1 に対して次のロールが割り当てられます。
- \* ストレージ BLOB データ リーダー
  - \* ストレージ テーブルのデータ提供者
  - \* ストレージ ファイル データ SMB 共有リーダー

| Statements                                                                                                                                                   | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.                                                             | <input type="radio"/> | <input type="radio"/> |
| On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1. | <input type="radio"/> | <input type="radio"/> |
| On October 1, 2022, User1 can delete the rows in table1 by using SAS1.                                                                                       | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                                                                                   | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.                                                             | <input type="radio"/>            | <input checked="" type="radio"/> |
| On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| On October 1, 2022, User1 can delete the rows in table1 by using SAS1.                                                                                       | <input type="radio"/>            | <input checked="" type="radio"/> |

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> (517**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

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。

| Name | Connected to  | Private IP address | Public IP address |
|------|---------------|--------------------|-------------------|
| VM1  | VNET1/Subnet1 | 10.1.1.4           | 13.80.73.87       |
| VM2  | VNET2/Subnet2 | 10.2.1.4           | 213.199.133.190   |
| VM3  | VNET2/Subnet2 | 10.2.1.5           | None              |

Subnet1 と Subnet2 には Microsoft.Storage サービス エンドポイントが構成されています。  
storageacc1 という名前の Azure ストレージ アカウントがあり、次のように構成されています。

SaveDiscardRefresh

Allow access from

All networksSelected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)  
[+ Add new virtual network](#)

| VIRTUAL NETWORK      | SUBNET | ADDRESS RANGE | ENDPOINT STATUS | RESOURCE GROUP | SUBSCRIPTION |
|----------------------|--------|---------------|-----------------|----------------|--------------|
| No network selected. |        |               |                 |                |              |

Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87

IP address or CIDR

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ  
☐ Allow read access to storage logging from any network  
☐ Allow read access to storage metrics from any network

次の各ステートメントについて、そのステートメントが 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。

| Statements                                       | Yes                   | No                    |
|--------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can upload a blob to storageacc1.  | <input type="radio"/> | <input type="radio"/> |
| From VM2, you can upload a blob to storageacc1.  | <input type="radio"/> | <input type="radio"/> |
| From VM3 , you can upload a blob to storageacc1. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                       | Yes                              | No                               |
|--------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can upload a blob to storageacc1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM2, you can upload a blob to storageacc1.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM3 , you can upload a blob to storageacc1. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照 :

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>



### 最新問題: 258

VNetwork1 の技術要件を満たす必要があります。  
まず何をすべきでしょうか?

- A. VNetwork1 に新しいサブネットを作成します。
- B. Subnet11 と Subnet13 から NSG を削除します。
- C. NSG を Subnet12 に関連付けます。
- D. VNetwork1 の DDoS 保護を構成します。

**Answer: A (メッセージを残す)**

シナリオより: Azure Firewall を Sub2 の VNetwork1 にデプロイします。

Azure ファイアウォールには、AzureFirewallSubnet という名前の専用サブネットが必要です。

参照 :

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

### 最新問題: 259

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 コンテナー

\* Database1 という名前の Azure SQL データベース

\* システム割り当てのマネージド ID を使用し、Database1 にアクセスするように構成された AppSrv1 および AppSrv2 という 2 つの Azure App Service Web 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。

\* Database1 のDiscount という名前の列のデータは、AppSrv1 だけがデータを復号できるように暗号化する必要があります。

\* AppSrv1 と AppSrv2 は、マネージド ID を使用して暗号化キーを取得することで承認される必要があります。

データベース 1 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: 正しく選択するたびに 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: 260

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。

| Name         | Type           | Description                     |
|--------------|----------------|---------------------------------|
| RG1          | Resource group | Used to store virtual machines  |
| RG2          | Resource group | Used to store virtual networks  |
| ServerAdmins | Security group | Used to manage virtual machines |

ServerAdmins が次のタスクを実行できることを確認する必要があります。

RG2 の既存の仮想ネットワークにのみ仮想マシンを作成します。

ソリューションでは、最小特権の原則を使用する必要があります。

ServerAdmins に割り当てるべき 2 つのロールベースのアクセス制御 (RBAC) ロールはどれですか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

- A. RG2 のネットワーク共同作成者の役割
- B. RG2 のカスタム RBAC ロール
- C. RG1 のネットワーク共同作成者の役割。
- D. サブスクリプションのカスタム RBAC ロール
- E. RG1 の仮想マシン共同作成者ロール。
- F. サブスクリプションの共同作成者の役割

Answer: A,E (メッセージを残す)

最新問題: 261

OU2 と User1 に対して計画された変更を実行する必要があります。

どのツールを使用する必要がありますか? 答えるには、適切なツールを正しいリソースにドラッグします。各ツールは 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: 正しく選択するたびに 1 ポイントの価値があります。

Tools

The Azure portal

Azure AD Connect

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

Answer Area

OU2:

Tool

User1:

Tool



Answer:

The screenshot shows a Microsoft exam interface. On the left, under the heading 'Tools', there is a list of five items, each in a green-bordered box: 'The Azure portal', 'Azure AD Connect', 'The Active Directory admin center', 'Active Directory Sites and Services', and 'Active Directory Users and Computers'. On the right, under the heading 'Answer Area', there are two input fields. The first is labeled 'OU2:' and contains the text 'Azure AD Connect'. The second is labeled 'User1:' and contains the text 'The Azure portal'. A large, semi-transparent watermark 'Microsoft.com' is visible across the center of the image.

**最新問題: 262**

Azure Container Registry に接続する Azure Kubernetes Service (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 クラスターに対して自動的に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. Azure Key Vault のシークレット
- 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** ([メッセージを残す](#))

説明/参照:

参考文献:

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

**最新問題: 263**

次の図に示すように、Azure リソースの階層があります。



次の表に示す Azure Blueprints 定義を作成します。

| Name       | Published at      |
|------------|-------------------|
| Blueprint1 | Tenant Root Group |
| Blueprint2 | Subscription1     |

Blueprint1 と Blueprint2 をどのオブジェクトに割り当てることができますか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Blueprint1:

ManagementGroup1 only

ManagementGroup1, Subscription1, and RG1 only

ManagementGroup1, Subscription1, RG1, and VM1

Subscription1 only

Tenant Root Group only

Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only

Subscription1 and RG1 only

Subscription1 only

Subscription1, RG1, and VM1

Answer:

Blueprint1:

- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- Subscription1 only
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

- ManagementGroup1 only
- Subscription1 and RG1 only
- Subscription1 only
- Subscription1, RG1, and VM1

最新問題: 264

contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた 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予定です。

| Name             | Type                    | Description                                                                                                 |
|------------------|-------------------------|-------------------------------------------------------------------------------------------------------------|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1          | Azure web app           | A web app configured to serve as the middle tier of the application                                         |

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 Cosmos DB アカウントにアクセスします。どのタスクが CosmosDB1 と WebApp1 に実装されるかを特定する必要があります。

各リソースに対してどのタスクを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

CosmosDB1:

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

WebApp1:

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

Answer:



|            |                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CosmosDB1: | <div>▼</div> <div>Authenticate Azure AD users and generate resource tokens.<br/>Authenticate Azure AD users and relay resource tokens.<br/>Create database users and generate resource tokens.</div> |
| WebApp1:   | <div>▼</div> <div>Authenticate Azure AD users and generate resource tokens.<br/>Authenticate Azure AD users and relay resource tokens.<br/>Create database users and generate resource tokens.</div> |

説明

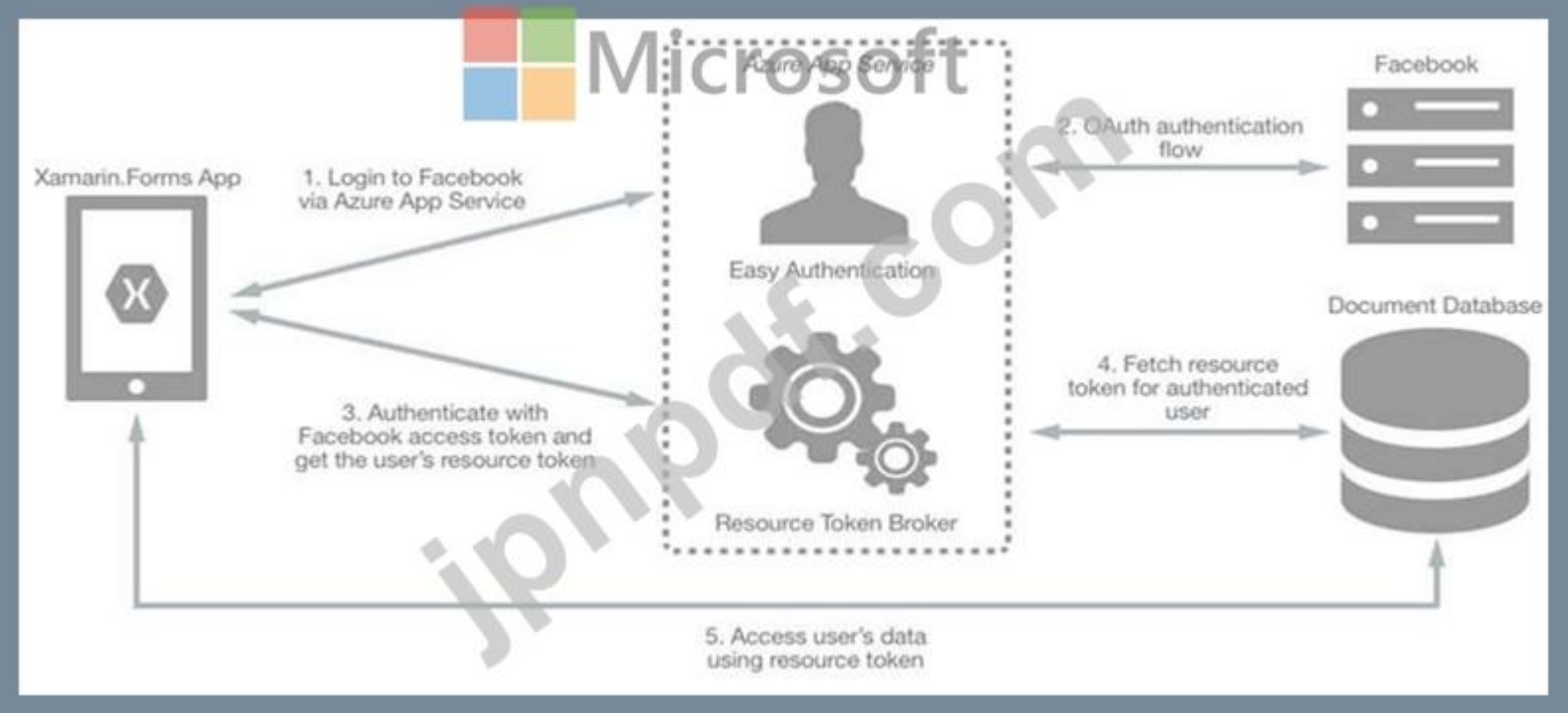
|            |                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CosmosDB1: | <div>▼</div> <div>Authenticate Azure AD users and generate resource tokens.<br/>Authenticate Azure AD users and relay resource tokens.<br/>Create database users and generate resource tokens.</div> |
| WebApp1:   | <div>▼</div> <div>Authenticate Azure AD users and generate resource tokens.<br/>Authenticate Azure AD users and relay resource tokens.<br/>Create database users and generate resource tokens.</div> |

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、付与されたアクセス許可に従って、クライアントが Azure Cosmos DB アカウント内の特定のリソースを読み取り、書き込み、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 トークンを中継する

リソース トークンを要求、生成し、モバイル アプリケーションに配信する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。



参考文献:  
<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

最新問題: 265

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

| Name  | Type               | In resource group |
|-------|--------------------|-------------------|
| cont1 | Container instance | RG1               |
| VNET1 | Virtual network    | RG1               |
| App1  | App Service app    | RG1               |
| VM1   | Virtual machine    | RG1               |
| User1 | User               | Not applicable    |

次の JSON ファイルを使用して、Subscription1 にカスタム RBAC ロールを作成します。

```

{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}

```

RG1 で、Role1 を User1 に割り当てます。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                      | Yes                   | No                    |
|---------------------------------|-----------------------|-----------------------|
| User1 can add VM1 to VNET1.     | <input type="radio"/> | <input type="radio"/> |
| User1 can start and stop App1.  | <input type="radio"/> | <input type="radio"/> |
| User1 can start and stop cont1. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                      | Yes                   | No                               |
|---------------------------------|-----------------------|----------------------------------|
| User1 can add VM1 to VNET1.     | <input type="radio"/> | <input checked="" type="radio"/> |
| User1 can start and stop App1.  | <input type="radio"/> | <input checked="" type="radio"/> |
| User1 can start and stop cont1. | <input type="radio"/> | <input checked="" type="radio"/> |

参照 :

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute>

最新問題: 266

データとアプリケーションの要件を満たすように WebApp1 を構成する必要があります。  
どの 2 つのアクションを実行する必要がありますか? それぞれの正解は、解決策の一部を示しています。  
注: 正しく選択するたびに 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. App Service プランの価格レベルを変更します。
- 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 (メッセージを残す)

説明

<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。

最新問題: 267

Registry1 という名前の Azure Container Registry があります。  
次の表に示すように、Registry1 の役割の割り当てを追加します。

| User  | Role           |
|-------|----------------|
| User1 | AcrPush        |
| User2 | AcrPull        |
| User3 | AcrImageSigner |
| User4 | Contributor    |

Registry1 にイメージをアップロードしたり、Registry1 からイメージをダウンロードしたりできるのはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Upload images:

User1 only

User1 and User4 only

User1, User3, and User4

User1, User2, User3, and User4

Download images:

User2 only

User1 and User2 only

User2 ad User4 only

User1, User2, and User4

User1, User2, User3, and User4

Answer:



Upload images:

User1 only

User1 and User4 only

User1, User3, and User4

User1, User2, User3, and User4

Download images:

User2 only

User1 and User2 only

User2 ad User4 only

User1, User2, and User4

User1, User2, User3, and User4

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

最新問題: 268

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。

| Name     | Type             | Resource group | Location |
|----------|------------------|----------------|----------|
| RG1      | Resource group   | Not applicable | West US  |
| Managed1 | Managed identity | RG1            | West US  |

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。

| Name  | Usage location |
|-------|----------------|
| User1 | United States  |
| User2 | Germany        |

次の表に示すグループを作成します。

| Name   | Type          | Membership type |
|--------|---------------|-----------------|
| Group1 | Security      | Dynamic User    |
| Group2 | Microsoft 365 | Dynamic User    |

Group1 と Group2 のメンバーシップ ルールは次のように構成されています。

Dynamic membership rules

...

×

 Save

 Discard

|

 Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule.  [Learn more](#)

| And/Or | Property       | Operator | Value |  |
|--------|----------------|----------|-------|--|
|        | accountEnabled | Equals   | true  |  |
| Or     | usageLocation  | Equals   | US    |  |

+

 Add expression

+

 Get custom extension properties 

Rule syntax  Edit

(user.accountEnabled -eq true) or (user.usageLocation - eq "US")

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                 | Yes                   | No                    |
|--------------------------------------------|-----------------------|-----------------------|
| User1 is a member of Group1 and Group2.    | <input type="radio"/> | <input type="radio"/> |
| User2 is a member of Group2 only.          | <input type="radio"/> | <input type="radio"/> |
| Managed1 is a member of Group1 and Group2. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                 | Yes                              | No                               |
|--------------------------------------------|----------------------------------|----------------------------------|
| User1 is a member of Group1 and Group2.    | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 is a member of Group2 only.          | <input type="radio"/>            | <input checked="" type="radio"/> |
| Managed1 is a member of Group1 and Group2. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

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

最新問題: 269

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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Virtual networks that User2 can modify:

▼

VNET4 only  
VNET4 and VNET1 only  
VNET4, VNET3, and VNET1 only  
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

▼

VNET4 only  
VNET4 and VNET1 only  
VNET4, VNET3, and VNET1 only  
VNET4, VNET3, VNET2, and VNET1

Answer:

Virtual networks that User2 can modify:

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |



Microsoft

Virtual networks that User2 can delete:

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

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、人事 (HR)、財務の部門があります。

既存の環境

ネットワーク環境

Fabrikam には、Microsoft 365 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 Active Directory ドメインが含まれています。ドメインには、OU1 と OU2 という 2 つの組織単位 (OU) が含まれています。Azure AD Connect クラウド同期は OU1 のみを同期します。

Azure リソースの階層を次の図に示します。





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。

| Name   | Type  | Directory-synced | Role                      | Delegated to      |
|--------|-------|------------------|---------------------------|-------------------|
| User1  | User  | Yes              | User                      | None              |
| Admin1 | User  | No               | User Access Administrator | Tenant Root Group |
| Admin2 | User  | No               | Security administrator    | MG1               |
| Admin3 | User  | No               | Contributor               | Subscription1     |
| Admin4 | User  | No               | Owner                     | RG1               |
| Group1 | Group | No               | Not applicable            | None              |

Azure AD には、次の表に示すリソースが含まれています。

| Name      | Type                      | Setting                                                                                                               |
|-----------|---------------------------|-----------------------------------------------------------------------------------------------------------------------|
| CAPolicy1 | Conditional access policy | Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online |
| Sentinel1 | Azure Sentinel workspace  | Not applicable                                                                                                        |
| SecPol1   | Azure Policy definition   | Security configuration for virtual machines                                                                           |

サブスクリプション 1 のリソース

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。

| Name  | Subnet           | Location   | Peer         |
|-------|------------------|------------|--------------|
| VNET1 | Subnet1, Subnet2 | West US    | VNET2, VNET3 |
| VNET2 | Subnet1          | Central US | VNET1, VNET3 |
| VNET3 | Subnet1          | West US    | VNET1, VNET2 |

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。

| Name | Location   |
|------|------------|
| NSG2 | West US    |
| NSG3 | Central US |
| NSG4 | West US    |

Subscription1 には、次の表に示す仮想マシンが含まれています。

| Name | Operating system        | Location   | Connected tor | Associated NSG |
|------|-------------------------|------------|---------------|----------------|
| VM1  | Windows Server 2019     | West US    | VNET1/Subnet1 | None           |
| VM2  | CentOS-based 8.2        | West US    | VNET1/Subnet2 | NSG2           |
| VM3  | Windows Server 2016     | Central US | VNET2/Subnet1 | NSG3           |
| VM4  | Ubuntu Server 18.04 LTS | West US    | VNET3/Subnet1 | NSG4           |

Subscription1 には、次の表に示す Azure Key Vault が含まれています。

| Name      | Location   | Pricing tier | Private endpoint                            |
|-----------|------------|--------------|---------------------------------------------|
| KeyVault1 | West US    | Standard     | VNET1/Subnet1                               |
| KeyVault2 | Central US | Premium      | None                                        |
| KeyVault3 | East US    | Premium      | VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1 |

Subscription1 には、米国西部 Azure リージョンの 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。

| Name | Location   |
|------|------------|
| ASG1 | West US    |
| ASG2 | Central US |

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。

Azure Security Center 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、利用可能なすべてのオペレーティング システムに存在

します。  
RG2 という名前のリソース グループを作成します。  
OU2 を Azure AD に同期します。  
User1 を Group1 に追加します。

技術的要件  
Fabrikam は次の技術要件を特定します。  
財務部門のユーザーは、SharePoint Online にアクセスするときに 3 時間後に再認証する必要があります。  
Storage1 は、顧客管理のキーと自動キー 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のアラート  
VM1、VM2、および VM3 は、Azure Disk Encryption 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経由で移動してはなりません。

最新問題: 270

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。オフィスは次の表に示す IP アドレスを使用します。

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Seattle  | 10.10.0.0/16     | 190.15.1.0/24      |
| New York | 172.16.0.0/16    | 194.25.2.0/24      |

この会社には、contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。テナントには、次の表に示すユーザーが含まれます。

| Name  | Multi-factor authentication (MFA) status |
|-------|------------------------------------------|
| User1 | Enabled                                  |
| User2 | Enforced                                 |

MFA サービス設定は、図に示すように構成されています。( 展示」タブをクリックします。)



Learn more

☒ Skip multi-factor authentication for requests from federated users on my intranet  
Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16  
194.25.2.0/24



verification options [learn more](#)

Methods available to users:

☒ Call to phone

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

|                                                                                                                                       | Yes                   | No                    |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/> | <input type="radio"/> |

Answer:

|                                                                                                                                       | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/>            | <input checked="" type="radio"/> |

説明

|                                                                                                                                       | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.       | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone                         | <input type="radio"/>            | <input checked="" type="radio"/> |



ボックス 2: いいえ

Microsoft Authenticator の使用は必要ありません。

注: Microsoft Authenticator は、2 段階認証プロセス中に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」に含まれています。

参考文献:

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

最新問題: 271

あなたの会社には、Subscription1 という名前の Azure サブスクリプションがあります。Subscription1 は、次の表に示すユーザーを含む Azure Active Directory テナントに関連付けられています。

| Name  | Role                  |
|-------|-----------------------|
| User1 | Global administrator  |
| User2 | Billing administrator |
| User3 | Owner                 |
| User4 | Account Admin         |

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ますか?そのユーザーはどのツールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

User:  ▼

|       |
|-------|
| User1 |
| User2 |
| User3 |
| User4 |

Tool:  ▼

|                       |
|-----------------------|
| Azure Account Center  |
| Azure Cloud Shell     |
| Azure PowerShell      |
| Azure Security Center |

Answer:

User:  ▼

|       |
|-------|
| User1 |
| User2 |
| User3 |
| User4 |

Tool:  ▼

|                       |
|-----------------------|
| Azure Account Center  |
| Azure Cloud Shell     |
| Azure PowerShell      |
| Azure Security Center |

参照：

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

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> (**51730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **272**

Azure portal から、Azure ポリシーを構成します。

DeployIfNotExist、AuditIfNotExist、Append、および Deny 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。

割り当てにマネージド ID が必要なのはどの効果ですか？

存在しない場合の監査

A.

B. 追加

<https://www.fast2test.com/AZ-500-practice-test.html> 84

有効な Fast2test AZ-500 試験 PDF 問題集 - 新しい AZ-500 本当の試験問題

存在しない場合のデプロイ

C.

D. 拒否

**Answer:** ([解答を表示する](#))

Azure Policy は、deployIfNotExists ポリシー定義内のテンプレートを実行するときに、マネージド 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: **273**

OU2 と User1 に対して計画された変更を実行する必要があります。

どのツールを使用する必要がありますか？ 答えるには、適切なツールを正しいリソースにドラッグします。各ツールは 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: 正しく選択するたびに 1 ポイントの価値があります。

| Tools                                | Answer Area |
|--------------------------------------|-------------|
| The Azure portal                     | OU2: Tool   |
| Azure AD Connect                     | User1: Tool |
| The Active Directory admin center    |             |
| Active Directory Sites and Services  |             |
| Active Directory Users and Computers |             |

**Answer:**

| Tools                                | Answer Area             |
|--------------------------------------|-------------------------|
| The Azure portal                     | OU2: Azure AD Connect   |
| Azure AD Connect                     | User1: The Azure portal |
| The Active Directory admin center    |                         |
| Active Directory Sites and Services  |                         |
| Active Directory Users and Computers |                         |

**最新問題: 274**

Azure Container Registry に接続する Azure Kubernetes Service (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 クラスターの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. Azure Key Vault のシークレット
- 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:** ([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/kubernetes-service-principal>

**最新問題: 275**

You plan to use Azure Disk Encryption for several virtual machine disks.

You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault.

To complete this task, sign in to the Azure portal and modify the Azure resources.

**Answer:**



See the explanation below.

Explanation

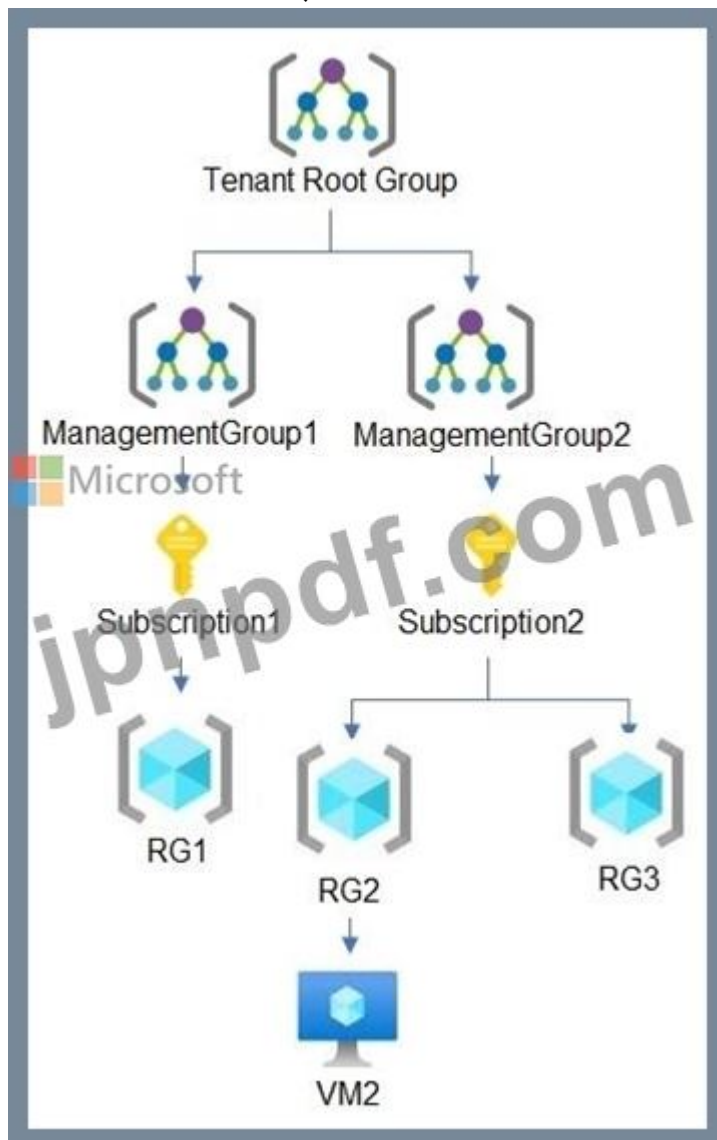
1. In the Azure portal, type Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to in the left navigation pane.
2. In the Key Vault properties, scroll down to the Access Policies.
3. Select the Azure Disk Encryption for volume encryption



4. Click Save to save the changes.

最新問題: 276

次の図に示すように、Azure リソースの階層があります。



RG1、RG2、RG3 はリソース グループです。

RG2 には VM1 という名前の仮想マシンが含まれています。  
次の表に示すユーザーに、ロールベースのアクセス制御 (RBAC) の役割を割り当てます。

| Name  | Role                                | Added to resource |
|-------|-------------------------------------|-------------------|
| User1 | Contributor                         | Tenant Root Group |
| User2 | Virtual Machine Contributor         | Subscription2     |
| User3 | Virtual Machine Administrator Login | RG2               |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                 | Yes                   | No                    |
|----------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 can deploy virtual machines to RG1.                                  | <input type="radio"/> | <input type="radio"/> |
| User2 can delete VM2.                                                      | <input type="radio"/> | <input type="radio"/> |
| User3 can reset the password of the built-in Administrator account of VM2. | <input type="radio"/> | <input type="radio"/> |

Answer:  
説明

| Statements                                                                 | Yes                              | No                               |
|----------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can deploy virtual machines to RG1.                                  | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can delete VM2.                                                      | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can reset the password of the built-in Administrator account of VM2. | <input type="radio"/>            | <input checked="" type="radio"/> |

最新問題: 277

User2 が PIM を実装できることを確認する必要があります。  
まず何をすべきでしょうか？

- A. User2 に全体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 セキュリティ 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: D (メッセージを残す)

ディレクトリで PIM の使用を開始するには、まず PIM を有効にする必要があります。

1. ディレクトリの全体管理者として Azure portal にサインインします。

ディレクトリに対して 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) を持つ全体管理者である必要があります。

シナリオ: 技術要件には次のものが含まれます: contoso.com に対して Azure AD Privileged Identity Management (PIM) を有効にする 参照:

最新問題: 278

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が含まれる Group1 という名前の Azure Active Directory (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、再起動できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。  
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Answer:

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Explanation:

参考文献:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

最新問題: 279

contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた Sub1 という名前の Azure サブスクリプションが

あります。

あなたには、テナントの全体管理者の役割が割り当てられています。Azure Security Center の設定を管理するのはお客様の責任です。

カスタム機密ラベルを作成する必要があります。

まず何をすべきでしょうか？

- A. カスタムの機密情報の種類を作成します。
- B. Azure AD のグローバル管理者のアクセス権を昇格します。
- C. セキュリティ センターの価格レベルを標準にアップグレードします。
- D. Microsoft Cloud App Security との統合を有効にします。

Answer: (解答を表示する)

まず、デフォルトのルールを直接変更できないため、新しい機密情報の種類を作成する必要があります。

参照：

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

最新問題: 280

次の表に示す Azure Active Directory (Azure AD) リソースを含む Azure サブスクリプションがあります。

| Name     | Description                                                 |
|----------|-------------------------------------------------------------|
| User1    | User                                                        |
| Group1   | Security group that has a Membership type of Dynamic Device |
| Managed1 | Managed identity                                            |
| App1     | Enterprise application                                      |

次の表に示すグループを作成します。

| Name   | Description                                                |
|--------|------------------------------------------------------------|
| Group5 | Security group that has a Membership type of Assigned      |
| Group6 | Microsoft 365 group that has a Membership type of Assigned |

どのリソースを Group5 と Group6 に追加できますか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



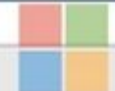
Group5:  ▼

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6: ▼

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Answer:

Group5:  ▼

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6: ▼

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

最新問題: 281

Azure Key Vault を作成する必要があります。このソリューションでは、キー コンテナー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ればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

|                        |                   |
|------------------------|-------------------|
| -EnabledForDeployment  | -Confirm          |
| -EnablePurgeProtection | -DefaultProfile   |
| -Tag                   | -EnableSoftDelete |
|                        | -SKU              |

Answer:

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

|                        |                   |
|------------------------|-------------------|
| -EnabledForDeployment  | -Confirm          |
| -EnablePurgeProtection | -DefaultProfile   |
| -Tag                   | -EnableSoftDelete |
|                        | -SKU              |

参考文献:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

最新問題: 282

Azure Key Vault を持っています。

次の要件を満たすには、キー コンテナー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 コンテナーの高度なアクセス ポリシーを設定する権限を与えます。

User2 という名前のユーザーに、キー コンテナー内の証明書を追加および削除する権限を与えます。

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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

User1:  ▼

|                                        |
|----------------------------------------|
| A key vault access policy              |
| Azure Information Protection           |
| Azure Policy                           |
| Managed identities for Azure resources |
| RBAC                                   |

User2:  ▼

|                                        |
|----------------------------------------|
| A key vault access policy              |
| Azure Information Protection           |
| Azure Policy                           |
| Managed identities for Azure resources |
| RBAC                                   |

Answer:

User1:  ▼

|                                        |
|----------------------------------------|
| A key vault access policy              |
| Azure Information Protection           |
| Azure Policy                           |
| Managed identities for Azure resources |
| RBAC                                   |

User2:  ▼

|                                        |
|----------------------------------------|
| A key vault access policy              |
| Azure Information Protection           |
| Azure Policy                           |
| Managed identities for Azure resources |
| RBAC                                   |

Explanation:

ユーザー1: RBAC

RBAC は、管理プレーンの Key Vault 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。

Key Vault アクセス ポリシーを設定する

キー コンテナの作成、読み取り、更新、および削除

Key Vault タグを設定する

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、職務の実行に必要な量のアクセスのみをユーザーに付与できます。

User2: キー コンテナのアクセス ポリシー

キー コンテナのアクセス ポリシーは、キー コンテナのデータ 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、証明書に個別にアクセス許可を付与します。

参考文献:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

#### 最新問題: 283

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。

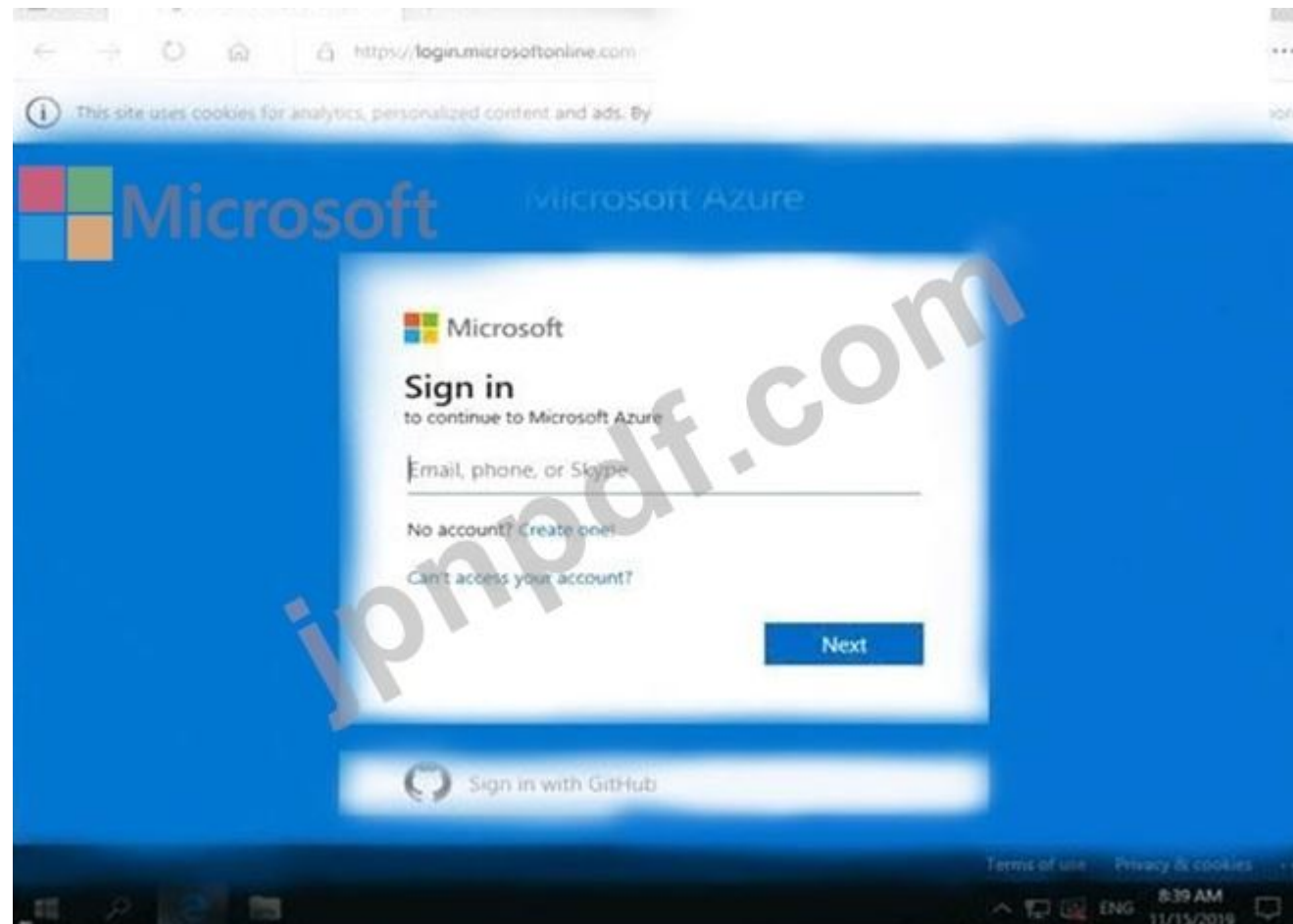
パスワードを入力するには、「パスワードの入力」ボックスにカーソルを置き、下のパスワードをクリックします。

Azure ユーザー名: User1-10598168@ExamUsers.com

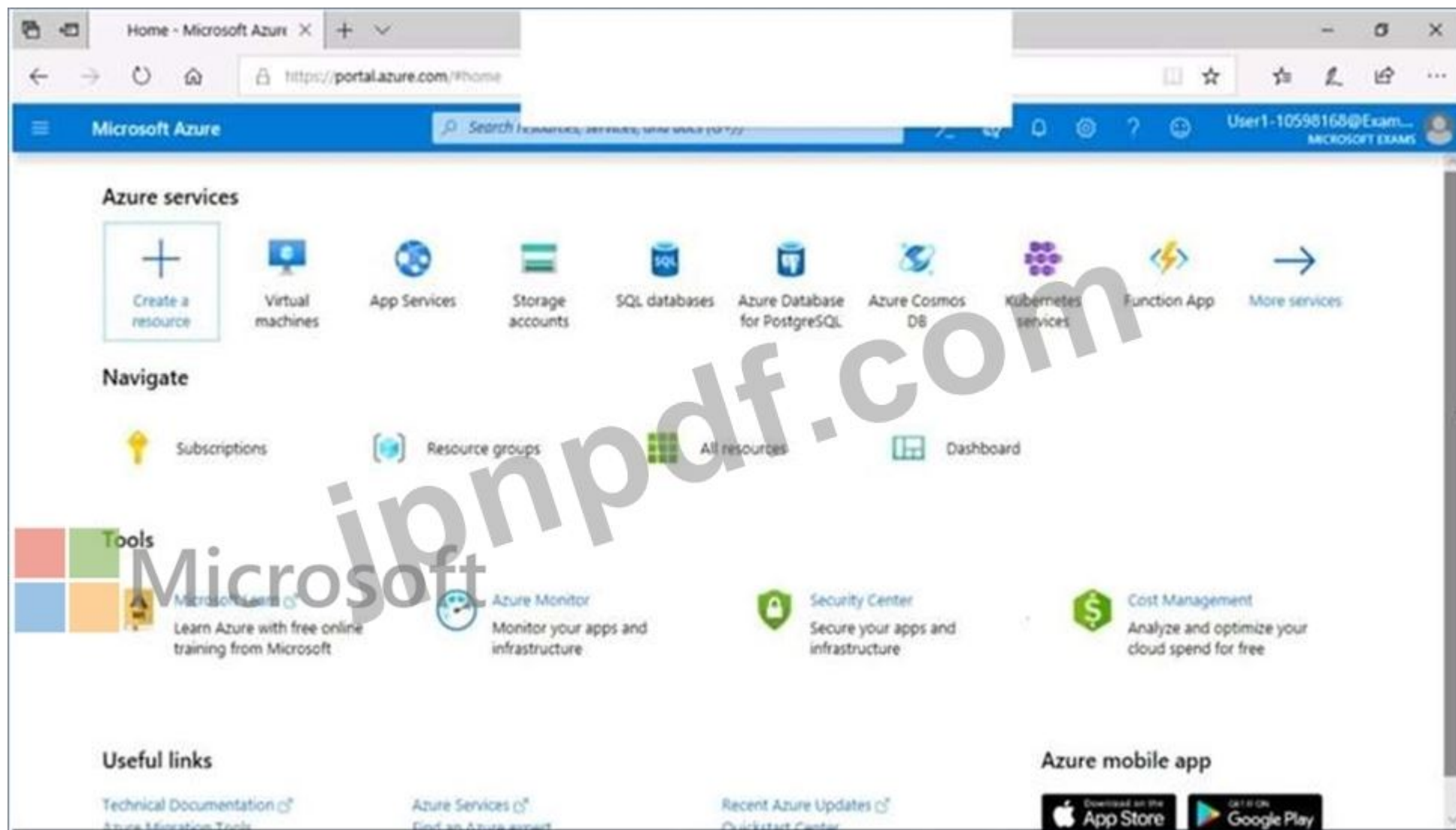
Azure パスワード: Ag1Bh9!#Bd

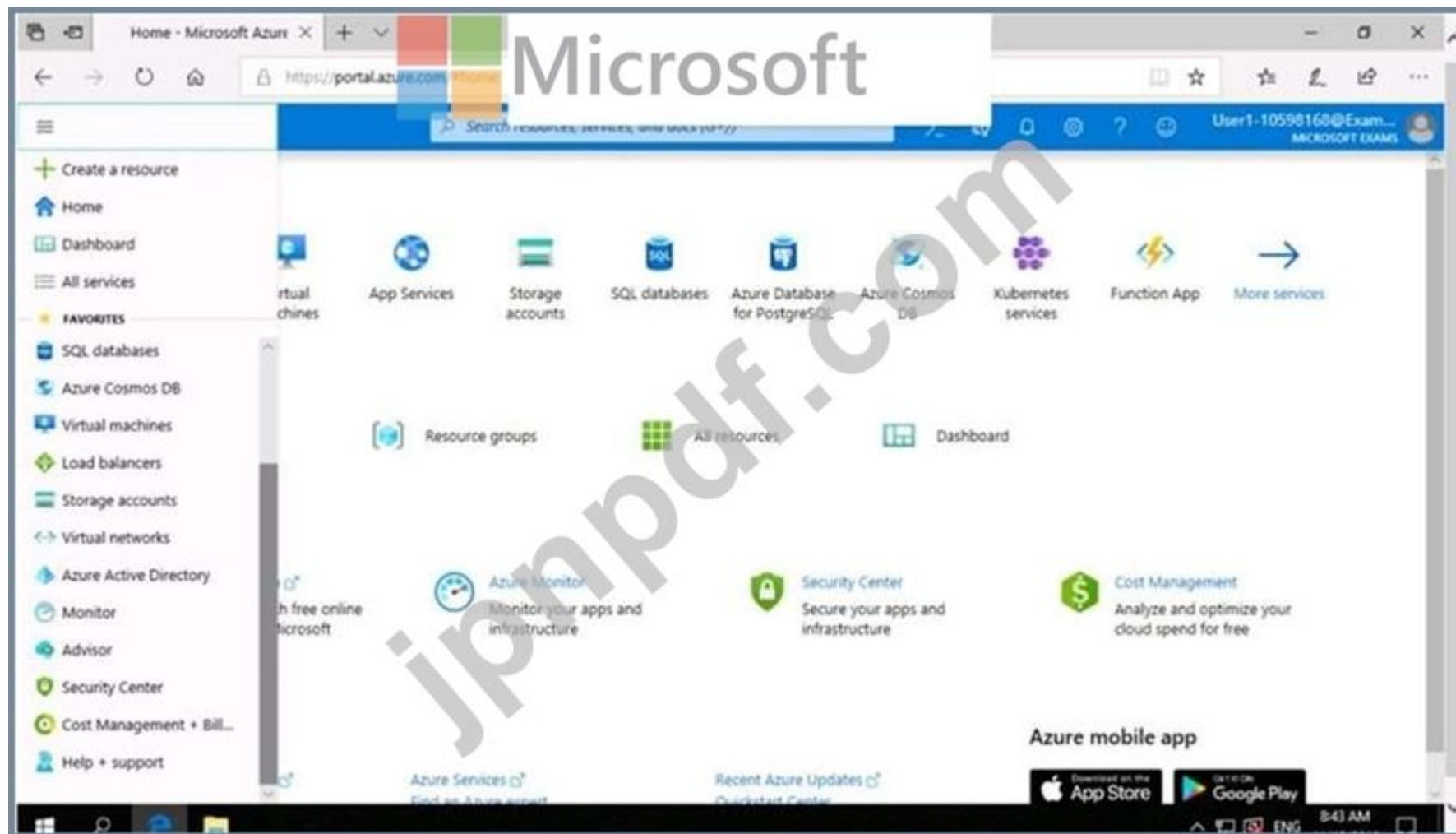
次の情報は、テクニカル サポートのみを目的としています。

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。ソリューションでは、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 portal 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 portal 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] > [役割割り当ての追加] をクリックして、[役割割り当ての追加] ペインを開きます。



5. [ロール] ドロップダウン リストで、ロール [仮想マシン共同作成者] を選択します。仮想マシン共同作成者を使用すると、仮想マシンを管理できますが、仮想マシンへのアクセスや、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 アカウントへのアクセスはできません。

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: 284

ID という名前のマネージド 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 および AU2 にはどのリソースを追加できますか? 回答するには、回答領域で適切なオプションを選択してください。

| Name   | Type                | Assigned object |
|--------|---------------------|-----------------|
| AU1    | Administrative unit | User1, Group1   |
| AU2    | Administrative unit | None            |
| User1  | User                | Not applicable  |
| Group1 | Security group      | Not applicable  |
| Group2 | Microsoft 365 group | Not applicable  |

AU1 と AU2 にはどのリソースを追加できますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



#### 最新問題: 285

Active Directory ドメイン サービス (AD DS) ドメインと同期する Azure Active Directory テナントがあります。

フォルダーとファイルを含む Azure ファイル共有を作成する予定です。

Azure ファイル共有と共有内のフォルダーにアクセス許可を割り当てるには、どのアイデンティティ ストアを使用できますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Azure files share:

Folders in the file share:

Answer:

答えは下の画像の通りです。

Answer Area

Azure files share: AD DS only

Folders in the file share: AD DS and Azure AD

#### 最新問題: 286

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

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を使用して Azure ロールを保護できることを確認する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。



| Actions                                                          | Answer Area |
|------------------------------------------------------------------|-------------|
| Discover privileged roles.                                       |             |
| Sign up PIM for Azure AD roles.                                  |             |
| Consent to PIM.                                                  |             |
| Discover resources.                                              |             |
| Verify your identity by using multi-factor authentication (MFA). |             |

Answer:

| Actions                                                          | Answer Area                                                      |
|------------------------------------------------------------------|------------------------------------------------------------------|
| Discover privileged roles.                                       | Verify your identity by using multi-factor authentication (MFA). |
| Sign up PIM for Azure AD roles.                                  | Consent to PIM.                                                  |
| Consent to PIM.                                                  | Sign up PIM for Azure AD roles.                                  |
| Discover resources.                                              |                                                                  |
| Verify your identity by using multi-factor authentication (MFA). |                                                                  |

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> (517**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

Contosostorage1 という名前の Azure Storage アカウントと Contosokeyvault1 という名前の Azure Key Vault 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 に保存する Azure Automation Runbook を作成する予定です。

Runbook を確実に実装するには、前提条件を実装する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

⬅

➡

⬆

⬆

Answer:

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

## 説明

Create an Azure Automation account.

 Microsoft  
Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

ステップ 1: Azure Automation アカウントを作成する

Runbook は Azure Automation アカウント内に存在し、PowerShell スクリプトを実行できます。

ステップ 2: PowerShell モジュールを Azure Automation 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 [資産] で、[Runbook にモジュールを追加する] を選択します。Runbook で Key Vault コマンドレットを実行するには、AzureRM.profile と AzureRM.key Vault を追加する必要があります。

ステップ 3: Azure Automation 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、実行アカウントを使用して認証し、Runbook で Resource Manager リソースを管理できます。AzureRunAsConnection は、上記の「実行アカウント」を作成したときに自動的に作成される接続アセットです。

これは、[資産] -> [接続] にあります。認証コードの後に、上記と同じコードを実行して、ポータル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...」  
AzureRmAccount の追加`  
-サービスプリンシパル`  
-TenantId $servicePrincipalConnection.TenantId`  
-ApplicationId $servicePrincipalConnection.ApplicationId`  
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint  
}
```

参考文献:

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

最新問題: 288

cont1 という名前の BLOB コンテナを含む Azure サブスクリプションがあります。Cont1 には、次の図に示すアクセス ポリシーがありま

す。

Save

Stored access policies

| Identifier | Start time | Expiry time | Permissions |
|------------|------------|-------------|-------------|
| Policy1    |            |             | r ***       |

+ Add policy

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成させる回答の選択肢を選択します。

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

▼

1

2

4

7

15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

▼

1

2

4

7

15

Answer:



The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

1

2

4

7

15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

1

2

4

7

15

説明

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

最新問題: 289

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。

| Name   | Type                                    |
|--------|-----------------------------------------|
| User1  | Azure Active Directory (Azure AD) user  |
| User2  | Azure Active Directory (Azure AD) user  |
| Group1 | Azure Active Directory (Azure AD) group |
| Vault1 | Azure key vault                         |

User1 は Group1 のメンバーです。Group1 と User2 には、Vault1 の Key Vault 共同作成者ロールが割り当てられます。2019 年 1 月 1 日に、Vault1 にシークレットを作成します。秘密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。)

## Create a secret

### Upload options

Manual

\* Name ⓘ

Password1

\* Value

• • • • • • • • • •

Content type (optional)

Set activation date? ⓘ ☒

Activation Date

2019-03-01  12:00:00 AM

(UTC+02:00)  Current Time Zone ---

Set expiration Date? ⓘ ☒

Expiration Date

2020-03-01  12:00:00 AM

(UTC+02:00)  Current Time Zone ---

Enabled?



User2 には Vault1 へのアクセス ポリシーが割り当てられます。ポリシーには次の構成があります。

キー管理操作: 取得、リスト、および復元

暗号化操作: キーの復号化とラップ解除

シークレット管理操作: 取得、リスト、および復元

Group1 には Vault1 へのアクセスが割り当てられます。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、および復元

次の各ステートメントについて、そのステートメントが 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。

| Statements                                                 | Yes                   | No                    |
|------------------------------------------------------------|-----------------------|-----------------------|
| On January 1, 2019, User1 can view the value of Password1. | <input type="radio"/> | <input type="radio"/> |
| On June 1, 2019, User2 can view the value of Password1.    | <input type="radio"/> | <input type="radio"/> |
| On June 1, 2019, User1 can view the value of Password1.    | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                 | Yes                              | No                               |
|------------------------------------------------------------|----------------------------------|----------------------------------|
| On January 1, 2019, User1 can view the value of Password1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| On June 1, 2019, User2 can view the value of Password1.    | <input checked="" type="radio"/> | <input type="radio"/>            |
| On June 1, 2019, User1 can view the value of Password1.    | <input type="radio"/>            | <input checked="" type="radio"/> |

最新問題: 290

あなたの会社には、Sub1 という名前の Azure サブスクリプションがあります。Sub1 には、Azure Application Insights を使用する WebApp1 という名前の Azure Web アプリが含まれています。WebApp1 では、ユーザーは OAuth 2.0 クライアント シークレットを使用して認証する必要があります。

同社の開発者は、Web App1 へのユーザー トラフィックをエミュレートする合成トランザクションを実行する、複数ステップの Web テスト アプリを作成することを計画しています。

Web テストが無人で実行できることを確認する必要があります。

まず何をすべきでしょうか？

- A. Microsoft Visual Studio で、.webtest ファイルを変更します。
- B. .webtest ファイルを Application Insights にアップロードします。
- C. Web テスト アプリを Azure AD に登録します。
- D. Web テスト アプリにプラグインを追加します。

Answer: B ([メッセージを残す](#))

説明

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep>

最新問題: 291

Azure Key Vault を含む Azure サブスクリプションを持っています。キー コンテナの役割の割り当てを次の図に示します。

```
[
  {
    "RoleAssignmentId": "3336fcbf-43db-4e8a-b5b6-d8edd964762b",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
    "DisplayName": "User1",
    "SignInName": "User1@contoso.com",
    "RoleDefinitionName": "Owner",
    ...
  },
  {
    "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User2",
    "SignInName": "User2@contoso.com",
    "RoleDefinitionName": "Key Vault Crypto Officer",
    "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
    "DisplayName": "User4",
    "SignInName": "User4@contoso.com",
    "RoleDefinitionName": "Key Vault Administrator",
    ...
  },
  {
    "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
    "DisplayName": "User4",
    "SignInName": "User4@contoso.com",
    "RoleDefinitionName": "Key Vault Administrator",
    ...
  }
]
```

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成させる回答の選択肢を選択します。注: 正しく選択するたびに 1 ポイントの価値があります。

#### Answer Area

[Answer choice] can create keys in the key vault. 

[Answer choice] can create secrets in the key vault. 

#### Answer:

答えは下の画像の通りです。

**Answer Area**

[Answer choice] can create keys in the key vault. 

[Answer choice] can create secrets in the key vault.

#### 最新問題: 292

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 グループに仮想ネットワークと NSG を作成できますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



User8 can create virtual networks in:

|                   |   |
|-------------------|---|
|                   | ▼ |
| RG4 only          |   |
| RG6 only          |   |
| RG4 and RG6 only  |   |
| RG4, RG5, and RG6 |   |

User8 can create NSGs in:

|                   |   |
|-------------------|---|
|                   | ▼ |
| RG4 only          |   |
| RG4 and RG5 only  |   |
| RG4 and RG6 only  |   |
| RG4, RG5, and RG6 |   |

Answer:

User8 can create virtual networks in:

|                   |   |
|-------------------|---|
|                   | ▼ |
| RG4 only          |   |
| RG6 only          |   |
| RG4 and RG6 only  |   |
| RG4, RG5, and RG6 |   |

User8 can create NSGs in:

|                   |   |
|-------------------|---|
|                   | ▼ |
| RG4 only          |   |
| RG4 and RG5 only  |   |
| RG4 and RG6 only  |   |
| RG4, RG5, and RG6 |   |

説明

User8 can create virtual networks in:

▼

RG4 only

RG6 only

RG4 and RG6 only

RG4, RG5, and RG6

User8 can create NSGs in:

▼

RG4 only

RG4 and RG5 only

RG4 and RG6 only

RG4, RG5, and RG6

ボックス 1: RG4 のみ

Rg5 および Rg6 では仮想ネットワークは許可されません。

ボックス 2: Rg4、Rg5、および Rg6

シナリオ :

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。

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。

User8 に RG4、RG5、および RG6 の所有者の役割を割り当てます。

User8 都市シドニー、役割:なし

注: ネットワーク セキュリティ グループ (NSG) には、Azure Virtual Network (VNet) に接続されているリソースへのネットワーク トラフィックを許可または拒否するセキュリティ ルールのリストが含まれています。NSG は、サブネット、個々の VM (クラシック)、または VM に接続された個々のネットワーク インターフェイス (NIC) (リソース マネージャー) に関連付けることができます。

参考文献:

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

最新問題: 293

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

| Name  | Member of      | Multi-factor authentication (MFA) status |
|-------|----------------|------------------------------------------|
| User1 | Group1, Group2 | Enabled                                  |
| User2 | Group1         | Disabled                                 |
| User3 | Group1         | Disabled                                 |

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

\* 割り当て: Group1 を含み、Group2 を除く

※条件 :サインイン危険度 : 中以上

\* アクセス :アクセスを許可、多要素認証が必要

ユーザーが Azure AD にサインインするときに何が起きるかを特定する必要があります。

各ユーザーについて何を識別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: 正しく選択するたびに 1 ポイントの価値があります。

When User1 signs in from an anonymous IP address, the user will:

|                                               |   |
|-----------------------------------------------|---|
|                                               | ▼ |
| Be blocked                                    |   |
| Be prompted for MFA                           |   |
| Sign in by using a username and password only |   |

When User2 signs in from an unfamiliar location, the user will:

|                                               |   |
|-----------------------------------------------|---|
|                                               | ▼ |
| Be blocked                                    |   |
| Be prompted for MFA                           |   |
| Sign in by using a username and password only |   |

When User3 signs in from an infected device, the user will:

|                                               |   |
|-----------------------------------------------|---|
|                                               | ▼ |
| Be blocked                                    |   |
| Be prompted for MFA                           |   |
| Sign in by using a username and password only |   |

Answer:

When User1 signs in from an anonymous IP address, the user will:

|                                               |   |
|-----------------------------------------------|---|
|                                               | ▼ |
| Be blocked                                    |   |
| Be prompted for MFA                           |   |
| Sign in by using a username and password only |   |

When User2 signs in from an unfamiliar location, the user will:

|                                               |   |
|-----------------------------------------------|---|
|                                               | ▼ |
| Be blocked                                    |   |
| Be prompted for MFA                           |   |
| Sign in by using a username and password only |   |

When User3 signs in from an infected device, the user will:

|                                               |   |
|-----------------------------------------------|---|
|                                               | ▼ |
| Be blocked                                    |   |
| Be prompted for MFA                           |   |
| Sign in by using a username and password only |   |

Explanation:

参考文献:

<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: 294**

管理者が Azure Resource Manager テンプレートを使用してリソースをデプロイするときに、そのデプロイメントが KV11597200 という名前の Azure Key Vault 内のシークレットにアクセスでき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 portal 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

キー コンテナの高度なアクセス ポリシーでオプションを構成する必要があります。

\* Azure portal で、検索ボックスに Azure Key Vault」と入力し、検索結果から [Azure Key Vault] を選択して、KV11597200 という名前のキー コンテナを選択します。または、左側のナビゲーション ウィンドウで Azure Key Vault を参照します。

\* キー コンテナのプロパティで、[高度なアクセス ポリシー] をクリックします。

\* テンプレートのデプロイのために Azure Resource Manager へのアクセスを有効にするというチェックボックスをオンにします。

\* [保存] をクリックして変更を保存します。

**最新問題: 295**

あなたの会社には、contoso.com という名前の Azure Active Directory Azure (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。

会社は App1 という名前のモバイル アプリケーションを開発しています。App1 は、OAuth 2 暗黙的付与タイプを使用して Azure AD アクセス トークンを取得します。

App1 を Azure AD に登録する必要があります。

アプリケーションを登録するには開発者からどのような情報を取得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: A ([メッセージを残す](#))**

セクション: [なし]

Explanation:

ネイティブ アプリケーションの場合は、Azure AD がトークン応答を返すために使用するリダイレクト URI を指定する必要があります。

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

**最新問題: 296**

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。Azure Security Center を使用して、3 つの Azure サブスクリプションの一元的なポリシー管理を行います。



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 3 つのサブスクリプションすべてにグループとして展開する必要があります。  
解決策: リソース グラフと、管理グループを範囲とする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](#))

参考文献:

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

最新問題: 297

Azure サブスクリプションで Azure Kubernetes Service (AKS) クラスターを作成する予定です。

登録されたサーバー アプリケーションのマニフェストを次の図に示します。

Save Discard Upload Download

The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: [Understanding the Azure Active Directory application manifest](#).

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```



AKS クラスターと Azure Active Directory (Azure AD) が統合されていることを確認する必要があります。  
マニフェスト内のどのプロパティを変更する必要がありますか？

- A. accessTokenAcceptedVersion
- B. keyCredentials
- C. groupMembershipClaims
- D. acceptMappedClaims

Answer: (解答を表示する)

参照：

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

最新問題: 298

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

| Name  | Member of | Multi-factor authentication (MFA) status |
|-------|-----------|------------------------------------------|
| User1 | None      | Disabled                                 |
| User2 | Group1    | Disabled                                 |
| user3 | Group1    | Enforced                                 |

Azure AD Privileged Identity Management (PIM) がテナントに対して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電子メールを送信する: 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 チケット番号が必要: 無効にする

アクティブ化に Azure Multi-Factor Authentication が必要: 有効にする

このロール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。

| Name  | Assignment type |
|-------|-----------------|
| User1 | Active          |
| User2 | Eligible        |
| user3 | Eligible        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                          | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| When User1 signs in, the user is assigned the Password Administrator role automatically.            | <input type="radio"/> | <input type="radio"/> |
| User2 can request to activate the Password Administrator role.                                      | <input type="radio"/> | <input type="radio"/> |
| If User3 wants to activate the Password Administrator role, the user can approve their own request. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                          | Yes                              | No                               |
|-----------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| When User1 signs in, the user is assigned the Password Administrator role automatically.            | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can request to activate the Password Administrator role.                                      | <input checked="" type="radio"/> | <input type="radio"/>            |
| If User3 wants to activate the Password Administrator role, the user can approve their own request. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

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

#### 最新問題: 299

次のデータ コネクタを備えた Azure Sentinel ワークスペースがあります。

- \* Azure Active Directory ID 保護
- \* コモンイベントフォーマット(CEF)
- \* Azureファイアウォール

データが各コネクタから取り込まれていることを確認する必要があります。

[ログ クエリ] ウィンドウから、各コネクタに対してどのテーブルをクエリ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: 正しく選択するたびに 1 ポイントの価値があります。

Azure Active Directory Identity Protection:

Azure Firewall:

CEF:

Microsoft

Answer:



Azure Active Directory Identity Protection:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

Azure Firewall:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

CEF:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

説明

グラフィカル ユーザー インターフェイス、アプリケーション、テーブルの説明が自動的に生成される

Azure Active Directory Identity Protection:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

Azure Firewall:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

CEF:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |



#### 最新問題: 300

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

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

次の要件を満たすように構成する Azure Sentinel コンポーネントを特定する必要があります。

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

Azure Sentinel でインシデントが作成されるとき、チケットはサービス管理プラットフォームに記録される必要があります。

各要件に対してどのコンポーネントを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

When Azure Sentinel identifies a threat, an incident must be created:

|                 |
|-----------------|
| Analytics       |
| Data connectors |
| Playbooks       |
| Workbooks       |

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

|                 |
|-----------------|
| Analytics       |
| Data connectors |
| Playbooks       |
| Workbooks       |



Answer:



参照：

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

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

#### 最新問題: 301

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Sub1 という名前の Azure サブスクリプションがあります。

RG1 という名前のリソース グループに Sa1 という名前の Azure ストレージ アカウントがあります。

ユーザーとアプリケーションは、いくつかの共有アクセス署名 (SAS) と保存されたアクセス ポリシーを使用して、Sa1 の BLOB サービスとファイル サービスにアクセスします。

権限の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: 新しい保存されたアクセス 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: A ([メッセージを残す](#))

説明

共有アクセス署名は、ブログなどの特定のリソースへのアクセスを提供します。保存されたアクセス ポリシーは、Shared Access Signature (SAS) のグループです。SAS へのアクセスを取り消すには、次のいずれかを実行できます。

1. Key1 または Key 2、つまり SAS への署名に使用されるアクセス キーをローテーションします。SAS の署名に使用されたアクセス キーをローテーションすると、以前に署名された SAS が無効になるため、以前に使用されていた SAS が取り消されます。
2. SAS がリンクされている保存されたアクセス ポリシーを削除します。ストアド アクセス ポリシーが削除されると、そのストアド アクセ

ス ポリシーに関連付けられている SAS も無効になります。

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> (517**30%OFF**問題集溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: 302

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area



Statements

From the Internet, you can connect to the web server on VM1 by using HTTP.

From the Internet, you can connect to the web server on VM2 by using HTTP.

From the Internet, you can connect to the web server on VM3 by using HTTP.

Yes

No

Answer:

Answer Area



Statements

From the Internet, you can connect to the web server on VM1 by using HTTP.

From the Internet, you can connect to the web server on VM2 by using HTTP.

From the Internet, you can connect to the web server on VM3 by using HTTP.

Yes

No

最新問題: 303

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。

| Name | Resource group |
|------|----------------|
| VM1  | RG1            |
| VM2  | RG2            |
| VM3  | RG1            |
| VM4  | RG2            |



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

何を設定すればよいでしょうか？

- A. Azure Active Directory (Azure AD) Privileged Identity Management (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) 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 への受信トラフィックをロックダウンし、攻撃にさらされるリスクを軽減しながら、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、Security Center は NSG ルールを作成することによって、Azure VM への受信トラフィックをロックダウンします。受信トラフィックをロックダウンする 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、Security Center は、ユーザーが VM へのアクセスを正常に要求できる役割ベースのアクセス制御 (RBAC) アクセス許可を持っているかどうかを確認します。要求が承認されると、Security Center は、指定された期間、選択されたポートおよび要求された送信元 IP アドレスまたは範囲への受信トラフィックを許可するように、ネットワーク セキュリティ グループ (NSG) と Azure Firewall を自動的に構成します。時間が経過すると、Security Center 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ません。

参照：

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

最新問題: 304

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

| Name       | Location | Description            |
|------------|----------|------------------------|
| Workspace1 | East US  | Used by Azure Sentinel |
| Workspace2 | West US  | Not applicable         |

次の表に示す仮想マシンを作成します。

| Name | Location | Operating system    | Connected to |
|------|----------|---------------------|--------------|
| VM1  | East US  | Windows Server 2019 | None         |
| VM2  | East US  | Windows Server 2019 | Workspace2   |
| VM3  | West US  | Windows Server 2019 | None         |
| VM4  | West US  | Windows Server 2019 | Workspace2   |

Azure Sentinel を使用して、仮想マシン上の Windows Defender ファイアウォールを監視する予定です。

Azure Sentinel に接続できる仮想マシンはどれですか？

- A. VM1のみ
- B. VM1 と VM3 のみ
- C. VM1、VM2、VM3、VM4
- D. VM1 と VM2 のみ

Answer: C (メッセージを残す)

説明/参照:

最新問題: 305

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area



Statements

From the Internet, you can connect to the web server on VM1 by using HTTP.

From the Internet, you can connect to the web server on VM2 by using HTTP.

From the Internet, you can connect to the web server on VM3 by using HTTP.

Yes

No

☐

☐

☐

☐

☐

☐

Answer:

Answer Area



Statements

From the Internet, you can connect to the web server on VM1 by using HTTP.

From the Internet, you can connect to the web server on VM2 by using HTTP.

From the Internet, you can connect to the web server on VM3 by using HTTP.

Yes

No

☒

☐

☐

☒

☒

☐

最新問題: 306

AU1 と AU2 という 2 つの管理単位を含む Azure Active Directory (Azure AD) テナントがあります。  
ユーザーは、次の表に示すように管理単位に割り当てられます。

| User name | Member of |
|-----------|-----------|
| Admin1    | AU1       |
| Admin2    | AU1       |
| Admin3    | AU2       |
| Admin4    | AU2       |
| User1     | AU1       |

Answer Area

| Statements                               | Yes                   | No                    |
|------------------------------------------|-----------------------|-----------------------|
| Admin1 can reset the password of User1.  | <input type="radio"/> | <input type="radio"/> |
| Admin2 can reset the password of User3.  | <input type="radio"/> | <input type="radio"/> |
| Admin3 can reset the password of Admin4. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                               | Yes                              | No                               |
|------------------------------------------|----------------------------------|----------------------------------|
| Admin1 can reset the password of User1.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can reset the password of User3.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin3 can reset the password of Admin4. | <input type="radio"/>            | <input checked="" type="radio"/> |

最新問題: 307

プラットフォームの保護要件を満たすには、Microsoft マルウェア対策を導入する必要があります。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

Create a custom policy definition that has effect set to:

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting

The exclusion settings

The scope

Answer:

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists |

Create a policy assignment and modify:



Microsoft

▼

The Create a Managed Identify setting |

The exclusion settings

The scope

説明

Create a custom policy definition that has effect set to:



Microsoft

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

シナリオ:Microsoft Antimalware を RG1 の仮想マシンにインストールする必要があります。

RG1 は、Vnet1、VM0、および VM1 を含むリソース グループです。

ボックス 1: DeployIfNotExists

DeployIfNotExists は、条件が満たされた場合にテンプレートのデプロイメントを実行します。

Azure ポリシー定義マルウェア対策

参照 :

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

最新問題: 308

Contosostorage1 という名前の Azure Storage アカウントと Contosokeyvault1 という名前の Azure Key Vault 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 に保存する Azure Automation Runbook を作成する予定です。

Runbook を確実に実装するには、前提条件を実装する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。



Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

←

→

↑

↓

Microsoft

Answer:

Answer Area

Microsoft

Create an Azure Automation account

Import PowerShell modules to the Azure Automation account

Create a connection resource in the Azure Automation account

- 1 - Azure Automation アカウントを作成する
- 2 - PowerShell モジュールを Azure Automation アカウントにインポートする
- 3 - Azure Automation アカウントで接続リソースを作成する

参照 :

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

#### 最新問題: 309

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ています。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input type="radio"/> | <input type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM5. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| From VM1, you can successfully ping the public IP address of VM2.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM1, you can successfully ping the private IP address of VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can successfully ping the private IP address of VM5. | <input checked="" type="radio"/> | <input type="radio"/>            |

最新問題: 310

あなたは、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。

| Name    | IP address space |
|---------|------------------|
| Boston  | 180.15.10.0/24   |
| Seattle | 132.32.15.0/24   |

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ます。

| Name  | User device | Last sign-in | During last sign-in, user selected<br>Don't ask again for 14 days |
|-------|-------------|--------------|-------------------------------------------------------------------|
| User1 | Device1     | June 1       | Yes                                                               |
| User2 | Device2     | June 3       | No                                                                |

contoso.com の多要素設定は、次のように構成されています。

multi-factor authentication

users service settings

app passowrds [\(learn more\)](#)

☒ Allow users to create app passwords to sign in to non-browser apps

☐ Do not allow users to create app passwords to sign in to non-browser apps

## trusted ips [\(learn more\)](#)

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

## verification options [\(learn more\)](#)

Methods available to users:

- ☐ call to phone
- ☒ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

## remember multi-factor authentication [\(learn more\)](#)

☒ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60):

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

|                                                                                   | Statements                                                                                                   | Yes                   | No                    |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
|  | When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.        | <input type="radio"/> | <input type="radio"/> |
|                                                                                   | When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.          | <input type="radio"/> | <input type="radio"/> |
|                                                                                   | When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |

**Answer:**

#### 最新問題: 311

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Sub1 という名前の Azure サブスクリプションがあります。

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

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

権限の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: 新しい保存されたアクセス 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](#))

セクション: [なし]

Explanation:

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

保存されたアクセス ポリシーを取り消すには、アクセス 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。

署名付き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が即座に影響を受けます。

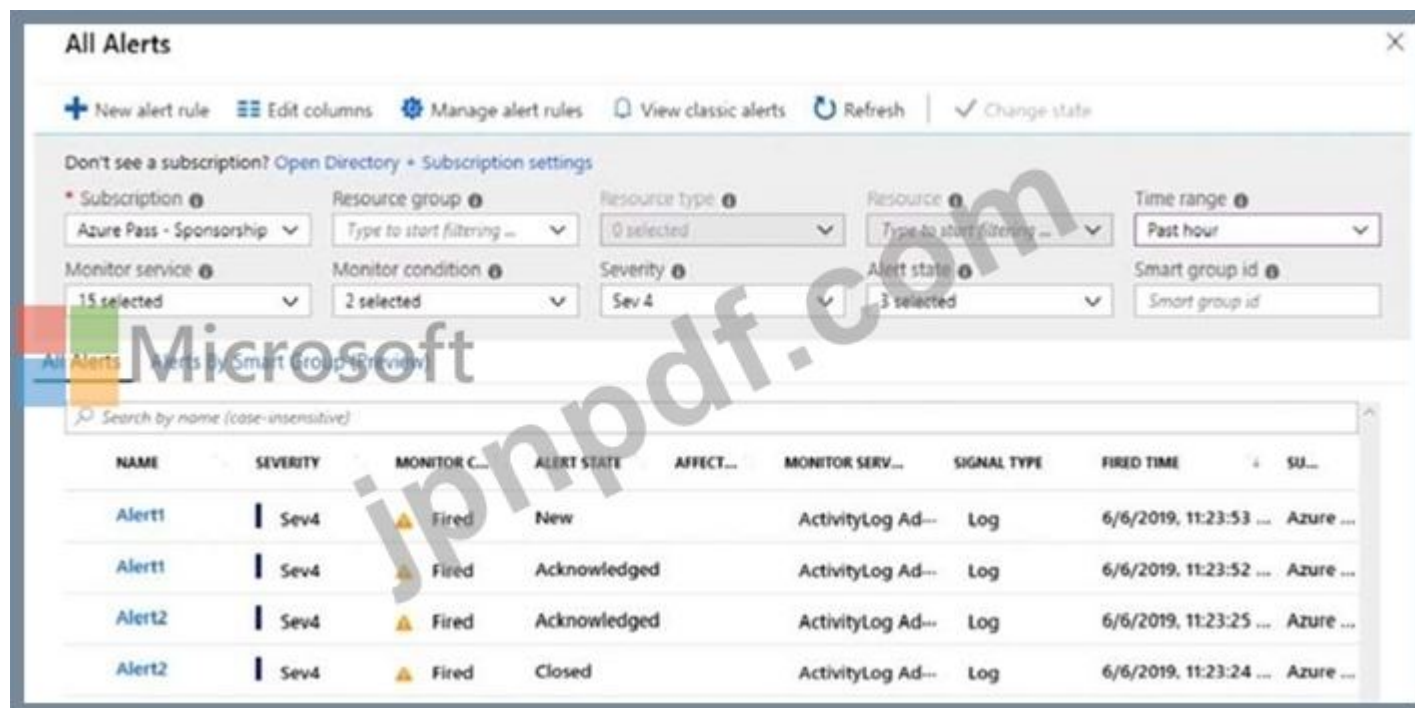
参照 :

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

#### 最新問題: 312

次の図に示すアラートを含む Azure サブスクリプションがあります。





ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。  
 注: 正しく選択するたびに 1 ポイントの価値があります。

The state of Alert1 that was fired at 11:23:52

▼

cannot be changed

can be changed to Closed only

can be changed to New only

can be changed to New or Closed

The state of Alert2 that was fired at 11:23:24

▼

cannot be changed

can be changed to Acknowledged only

can be changed to New only

can be changed to New or Acknowledged

Answer:

The state of Alert1 that was fired at 11:23:52

Microsoft

▼

cannot be changed

can be changed to Closed only

can be changed to New only

can be changed to New or Closed

The state of Alert2 that was fired at 11:23:24

▼

cannot be changed

can be changed to Acknowledged only

can be changed to New only

can be changed to New or Acknowledged

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

最新問題: 313

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。

| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

次の表に示すリソース ロックを作成します。

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                               | Yes                   | No                    |
|------------------------------------------|-----------------------|-----------------------|
| You can start VM1.                       | <input type="radio"/> | <input type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                               | Yes                   | No                               |
|------------------------------------------|-----------------------|----------------------------------|
| You can start VM1.                       | <input type="radio"/> | <input checked="" type="radio"/> |
| You can start VM2.                       | <input type="radio"/> | <input checked="" type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/> | <input checked="" type="radio"/> |

Explanation:

- 1.) 次のスコープがロックされているため、書き込み操作を実行できません:  
「subscriptions/xxxx/resourceGroups/xxx」ロックを解除して、もう一度お試しください。
- 2.) 読み取り専用ロックを持つリソース グループに VM を作成すると、エラーが表示されます。  
「選択されたリソース グループは読み取り専用です」
- 3.) 読み取り専用ロックのため、マシンの起動後にロックが追加されると、仮想マシンは起動または停止できません。(このユースケースの一部ではありませんが、知っておくと良いでしょう。  
回答で参照されている記事は、ブループリントに範囲が限定されているため、異なると述べています。  
[リソースのロック] ページには、VM の起動に関して次のことが記載されています。  
「仮想マシンを含むリソース グループに対する読み取り専用ロックにより、すべてのユーザーが仮想マシンを起動または再起動できなくなります。これらの操作には POST リクエストが必要です。」

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

最新問題: 314

データとアプリケーションの要件を満たすように SQLDB1 を構成する必要があります。  
順番に実行することをお勧めする 3 つのアクションはどれですか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。



## Actions

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

In SQLDB1, create contained database users.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, create a system-assigned managed identity.

In Azure AD, create a user-assigned managed identity.

## Answer Area



Answer:

## Actions

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

In SQLDB1, create contained database users.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, create a system-assigned managed identity.

In Azure AD, create a user-assigned managed identity.

## Answer Area

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In SQLDB1, create contained database users.





Explanation:

<https://www.youtube.com/watch?v=pEPyPsGEevw>

トピック 2、Contoso

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[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。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行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できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では完了する必要があるラボが複数ある場合があります。各ラボを完了したいただけ時間を費やすことができます。ただし、ラボを確実に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。作業を送信した後は、ラボ内の [次へ] ボタンをクリックしてください。

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。ソリューションでは、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 portal 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 portal 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上で毎週日曜日の 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、App10317806 という名前の Web アプリを作成し、そのアプリを <https://www.contoso.com> に公開することを計画しています。

次のタスクを実行する必要があります。

\* App10317806 が Azure Active Directory (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。管理ユーザーには、VNET1 の設定の変更を許可する必要があります。

タスク 6:

user210317806 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。ソリューションでは、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% を超えた場合は、admin1@contoso.com という名前のユーザーにアラ-

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、すべての監査失敗データを Azure ストレージ アカウントに収集する必要があります。

このタスクを完了するには、Azure portal にサインインします。

このタスクが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:

rg1lodl03l7806n1 Azure ストレージ アカウントへの HTTP 接続を禁止する必要があります。

タスク 11:

rg1lod103l7806n1 Azure Storage アカウントが、KeyVault103l7806 Azure Key Vault に保存されているキーを使用して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:

103l7806.onmicrosoft.com という名前の新しい Azure Active Directory (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時間が設定されるわけではありません。各ケースを完了しただけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了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る質問に答えるには、ケーススタディで提供され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る場合があります。このケーススタディに関する各質問は、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、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に関する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を注意してください。質問に答える準備ができたなら、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 つの支社を構える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。どちらのサブスクリプションも、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。

技術的要件

Contoso は次の技術要件を特定します。

\* Azure Firewall を Sub2 の VNetWork1 にデプロイします。

\* App2 という名前のアプリケーションを contoso.com に登録します。

\* 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 Azure AD Privileged Identity Management (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。

| Name  | City     | Role                            |
|-------|----------|---------------------------------|
| User1 | Montreal | Global administrator            |
| User2 | MONTREAL | Security administrator          |
| User3 | London   | Privileged role administrator   |
| User4 | Ontario  | Application administrator       |
| User5 | Seattle  | Cloud application administrator |
| User6 | Seattle  | User administrator              |
| User7 | Sydney   | Reports reader                  |
| User8 | Sydney   | None                            |

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。

| Name   | Membership type | Dynamic membership rule  |
|--------|-----------------|--------------------------|
| Group1 | Dynamic user    | user.city -contains "ON" |
| Group2 | Dynamic user    | user.city -match "*on"   |

サブ1

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。

| Name  | Resource group |
|-------|----------------|
| VNET1 | RG1            |
| VNET2 | RG2            |
| VNET3 | RG3            |
| VNET4 | RG4            |

Sub1 には、次の表に示すロックが含まれています。

| Name  | Set on | Lock type |
|-------|--------|-----------|
| Lock1 | RG1    | Delete    |
| Lock2 | RG2    | Read-only |
| Lock3 | RG3    | Delete    |
| Lock4 | RG3    | Read-only |

Sub1 には、次の表に示す Azure ポリシーが含まれています。

| Policy definition          | Resource type                          | Scope |
|----------------------------|----------------------------------------|-------|
| Allowed resource types     | networkSecurityGroups                  | RG4   |
| Not allowed resource types | virtualNetworks/subnets                | RG5   |
| Not allowed resource types | networksSecurityGroups                 | RG5   |
| Not allowed resource types | virtualNetworks/virtualNetworkPeerings | RG6   |

サブ2

| Name      | Subnet                             |
|-----------|------------------------------------|
| VNetwork1 | Subnet1.1, Subnet1.2 and Subent1.3 |
| VNetwork2 | Subnet2.1                          |



Sub2 には、次の表に示す仮想マシンが含まれています。

| Name | Network interface | Application security group | Connected to |
|------|-------------------|----------------------------|--------------|
| VM1  | NIC1              | ASG1                       | Subnet1.1    |
| VM2  | NIC2              | ASG2                       | Subnet1.1    |
| VM3  | NIC3              | None                       | Subnet1.2    |
| VM4  | NIC4              | ASG1                       | Subnet1.3    |
| VM5  | NIC5              | None                       | Subnet2.1    |

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では、ping リクエストと Web リクエストが許可されます。

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。

| Name | Associated to |
|------|---------------|
| NSG1 | NIC2          |
| NSG2 | Subnet1.1     |
| NSG3 | Subnet1.3     |
| NSG4 | Subnet2.1     |

NSG1 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG2 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | 80   | TCP      | Internet          | VirtualNetwork | Allow  |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG3 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | Any  | TCP      | ASG1              | ASG1           | Allow  |
| 150      | Any  | Any      | ASG2              | VirtualNetwork | Allow  |
| 200      | Any  | Any      | Any               | Any            | Deny   |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |

NSG4 には、次の表に示す受信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source            | Destination    | Action |
|----------|------|----------|-------------------|----------------|--------|
| 100      | Any  | Any      | Any               | Any            | Allow  |
| 65000    | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | Any  | Any      | Any               | Any            | Deny   |



NSG1、NSG2、NSG3、および NSG4 には、次の表に示す送信セキュリティ ルールがあります。

| Priority | Port | Protocol | Source         | Destination    | Action |
|----------|------|----------|----------------|----------------|--------|
| 65000    | Any  | Any      | VirtualNetwork | VirtualNetwork | Allow  |
| 65001    | Any  | Any      | Any            | Internet       | Allow  |
| 65500    | Any  | Any      | Any            | Any            | Deny   |

Contoso は次の技術要件を特定します。

- \* Azure Firewall を Sub2 の VNetwork1 にデプロイします。
- \* App2 という名前のアプリケーションを contoso.com に登録します。
- \* 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 Azure AD Privileged Identity Management (PIM) を有効にします。

最新問題: 315

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。

| Name     | Type             | Resource group | Location |
|----------|------------------|----------------|----------|
| RG1      | Resource group   | Not applicable | West US  |
| Managed1 | Managed identity | RG1            | West US  |

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。

| Name  | Usage location |
|-------|----------------|
| User1 | United States  |
| User2 | Germany        |

次の表に示すグループを作成します。

| Name   | Type          | Membership type |
|--------|---------------|-----------------|
| Group1 | Security      | Dynamic User    |
| Group2 | Microsoft 365 | Dynamic User    |

Group1 と Group2 のメンバーシップ ルールは次のように構成されています。

Dynamic membership rules

...

×

 Save

 Discard

|

 Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule.  [Learn more](#)

| And/Or | Property       | Operator | Value |                                                                                     |
|--------|----------------|----------|-------|-------------------------------------------------------------------------------------|
|        | accountEnabled | Equals   | true  |  |
| Or     | usageLocation  | Equals   | US    |  |

+

 Add expression

+

 Get custom extension properties 

Rule syntax  Edit

(user.accountEnabled -eq true) or (user.usageLocation - eq "US")

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

|  Statements | Yes                   | No                    |
|------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 is a member of Group1 and Group2.                                                        | <input type="radio"/> | <input type="radio"/> |
| User2 is a member of Group2 only.                                                              | <input type="radio"/> | <input type="radio"/> |
| Managed1 is a member of Group1 and Group2.                                                     | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                 | Yes                              | No                               |
|--------------------------------------------|----------------------------------|----------------------------------|
| User1 is a member of Group1 and Group2.    | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 is a member of Group2 only.          | <input type="radio"/>            | <input checked="" type="radio"/> |
| Managed1 is a member of Group1 and Group2. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

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

#### 最新問題: 316

Azure Active Directory Premium Plan 1 テナントにリンクされた Azure サブスクリプションがあります。

Azure Active Directory (Azure AD) Identity Protection を実装する予定です。

ユーザー リスク ポリシーとサインイン リスク ポリシーを構成できることを確認する必要があります。

まず何をすべきでしょうか？

A. すべてのユーザーに対して Azure Active Directory Premium Plan 2 ライセンスを購入します。

B. すべてのユーザーを Azure Multi-Factor Authentication (MFA) に登録します。

C. Azure AD のセキュリティのデフォルトを有効にします。

D. Azure Security Center を標準レベルにアップグレードします。

**Answer: A (メッセージを残す)**

参照：

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

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> (51730%OFF問題集溶と正解付きで 30%w 特別割引コード:

**Freepdfdumps**)

#### 最新問題: 317

Container1 という名前の BLOB コンテナと App1 という名前のクライアント アプリケーションを含む Azure ストレージ アカウントがあります。

Azure Active Directory (Azure AD) 認証を使用して、App1 の Container1 への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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

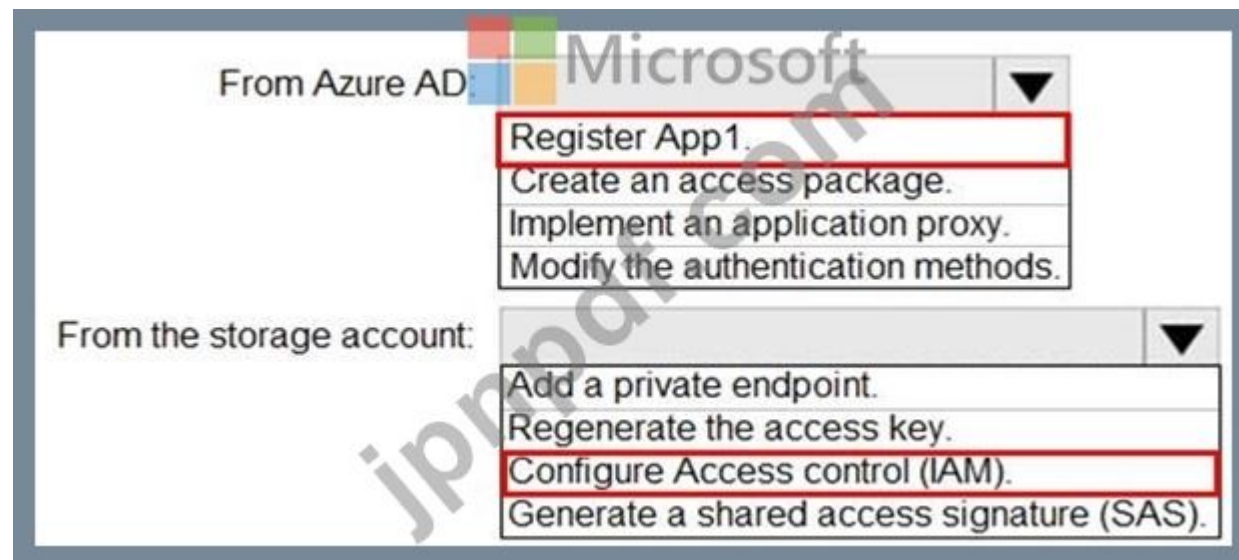
From Azure AD:

Register App1.  
Create an access package.  
Implement an application proxy.  
Modify the authentication methods.

From the storage account:

Add a private endpoint.  
Regenerate the access key.  
Configure Access control (IAM).  
Generate a shared access signature (SAS).

Answer:



参照 :

<https://azure.microsoft.com/en-in/blog/payment-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: 318

Azure サブスクリプションをお持ちです。

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

Contoso1812 の IP アドレスを指す www.contoso.com の DNS レコードを作成します。

ユーザーが <https://www.contoso.com> URL を使用して Contoso1812 にアクセスできることを確認する必要があります。

どの 2 つのアクションを実行する必要がありますか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

A. Contoso1812 のシステム割り当てマネージド ID を有効にします。

B. ホスト名を Contoso1812 に追加します。

C. Contoso1812 の App Service プランをスケールアウトします。

D. Contoso1812 にデプロイ スロットを追加します。



E. Contoso1812 の App Service 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 Azure DNS を構成できます。たとえば、Azure Web アプリを作成し、www.contoso.com または contoso.com を完全修飾ドメイン名 (FQDN) として使用してユーザーにアクセスさせることができます。これを行うには、次の 3 つのレコードを作成する必要があります。

contoso.com を指すルート A」レコード

検証用のルート 「TXT」レコード

A レコードを指す www 名の CNAME」レコード

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

参考資料: <https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-> ドメイン

最新問題: 319

条件付きアクセス ポリシーを実装しています。

ポリシーを構成して実装するには、既存の Azure Active Directory (Azure AD) 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。

認証情報が漏洩したユーザー

特殊な場所への旅行は不可能

不審なアクティビティのある IP アドレスからのサインイン

各リスクイベントについて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: 正しく選択するたびに 1 ポイントの価値があります。

| Levels | Answer Area                                                               |
|--------|---------------------------------------------------------------------------|
| High   | Impossible travel to atypical locations: <input type="text"/>             |
| Low    | Users with leaked credentials: <input type="text"/>                       |
| Medium | Sign ins from IP addresses with suspicious activity: <input type="text"/> |

Answer:

| Levels | Answer Area                                          |        |
|--------|------------------------------------------------------|--------|
| High   | Impossible travel to atypical locations:             | Medium |
| Low    | Users with leaked credentials:                       | High   |
| Medium | Sign ins from IP addresses with suspicious activity: | Medium |

説明

中くらい

高い

中くらい

参照

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-i>

最新問題: 320

あなたは、新しいレビューのコレクションに割り当てる予定のアクセス レビューを構成する任務を負っています。また、リソース所有者がレビューを確認できるようにする必要があります。

まず、アクセス レビュー プログラムとアクセス レビュー コントロールを作成します。

次に、レビュー担当者を構成する必要があります。

レビュー担当者を次のどれに設定する必要がありますか？

- A. 選択されたユーザー。
- B. メンバー (自分)。
- C. グループの所有者。
- D. 誰でも。

Answer: (解答を表示する)

説明

「レビュー担当者」セクションで、範囲内のすべてのユーザーをレビューする 1 人以上のユーザーを選択します。または、メンバーに自分のアクセス権をレビューさせるように選択することもできます。リソースがグループの場合は、グループの所有者にレビューを依頼できます。グラフィカル ユーザー インターフェイス、アプリケーションの説明が中程度の信頼度で自動的に生成される



参照：

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

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

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

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

**Answer:**

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

2- クエリ結果を選択します。

3- ブックマークを追加し、エンティティをマップする

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

最新問題: 322

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ています。  
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Statements

Yes

No

From VM1, you can successfully ping the public IP address of VM2.

From VM1, you can successfully ping the private IP address of VM3.

From VM1, you can successfully ping the private IP address of VM5.

Answer:

Answer Area

Statements

Yes

No

From VM1, you can successfully ping the public IP address of VM2.

From VM1, you can successfully ping the private IP address of VM3.

From VM1, you can successfully ping the private IP address of VM5.

最新問題: 323

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。

| Name  | Type                              |
|-------|-----------------------------------|
| Role1 | Azure Active Directory (Azure AD) |
| Role2 | Azure subscription                |

Azure portal で、既存のロールを複製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。新しいロールは、次の表に示すように構成されます。

| Name  | Type               |
|-------|--------------------|
| Role3 | Azure AD           |
| Role4 | Azure subscription |

新しい役割をそれぞれ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、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。



Role3:   
Role1 only  
Built-in Azure AD roles only  
Role1 and built-in Azure AD roles only  
Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:   
Role2 only  
Built-in Azure AD roles only  
Role2 and built-in Azure subscription roles only  
Role2, built-in Azure subscription roles, and built-in Azure AD roles

Answer:

Role3:   
Role1 only  
Built-in Azure AD roles only  
Role1 and built-in Azure AD roles only  
Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:   
Role2 only  
Built-in Azure AD roles only  
Role2 and built-in Azure subscription roles only  
Role2, built-in Azure subscription roles, and built-in Azure AD roles

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: 324

ネットワークには、Azure Active Directory (Azure AD) と同期する adatum.com という名前のオンプレミスの Active Directory ドメインが含まれています。Azure AD Connect は、Server1 という名前のドメイン メンバー サーバーにインストールされます。

adatum.com ドメインのドメイン管理者が同期オプションを変更できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。

どの Azure AD ロールをドメイン管理者に割り当てる必要がありますか？

- A. セキュリティ管理者
- B. 全体管理者
- C. ユーザー管理者

Answer: ([解答を表示する](#))

説明/参照:

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

#### 最新問題: 325

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

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を使用して Azure ロールを保護できることを確認する必要があります。

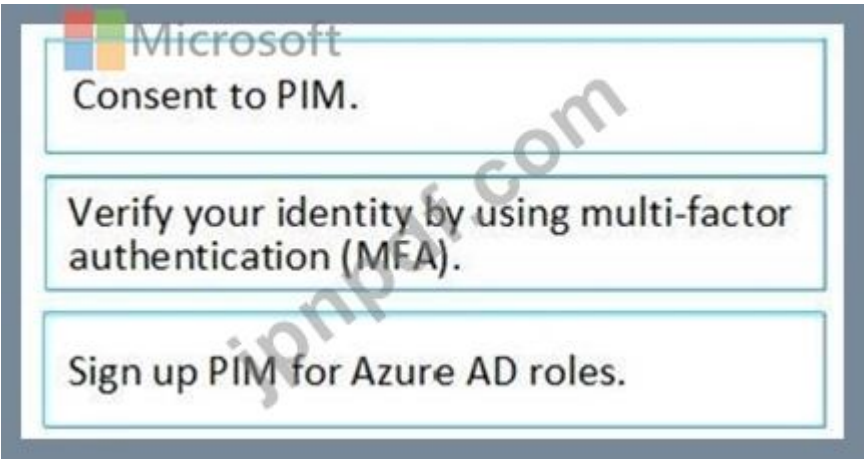
どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                                          | Answer Area |
|------------------------------------------------------------------|-------------|
| Discover privileged roles.                                       |             |
| Sign up PIM for Azure AD roles.                                  |             |
| Consent to PIM.                                                  |             |
| Discover resources.                                              |             |
| Verify your identity by using multi-factor authentication (MFA). |             |

Answer:

| Actions                                                          | Answer Area                                                      |
|------------------------------------------------------------------|------------------------------------------------------------------|
| Discover privileged roles.                                       | Consent to PIM.                                                  |
| Sign up PIM for Azure AD roles.                                  | Verify your identity by using multi-factor authentication (MFA). |
| Consent to PIM.                                                  | Sign up PIM for Azure AD roles.                                  |
| Discover resources.                                              |                                                                  |
| Verify your identity by using multi-factor authentication (MFA). |                                                                  |

説明



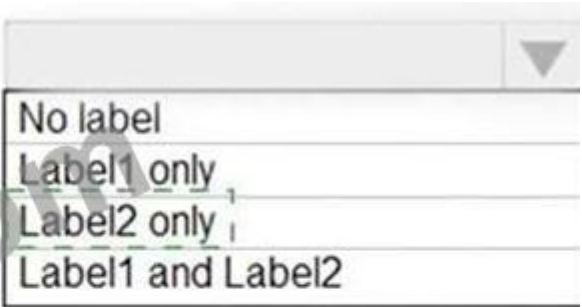
最新問題: 326

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、仮想マシンへの PowerShell アクセスをユーザーに許可する必要があります。  
何を設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:



If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:



Permission that must be granted to users on VM:

|        |   |
|--------|---|
|        | ▼ |
| Read   |   |
| Update |   |
| View   |   |
| Write  |   |

TCP port that must be allowed:

|      |   |
|------|---|
|      | ▼ |
| 22   |   |
| 25   |   |
| 3389 |   |
| 5986 |   |

 Microsoft

最新問題: 327

技術要件を満たすには、Azure Sentinel ノートブックのサポートを構成する必要があります。

Azure コンテナ レジストリと Azure Machine Learning ワークスペースの最小数はどれくらい必要ですか？

Container registries:

|   |   |
|---|---|
|   | ▼ |
| 0 |   |
| 1 |   |
| 2 |   |
| 3 |   |

 Microsoft

Workspaces:

|   |   |
|---|---|
|   | ▼ |
| 0 |   |
| 1 |   |
| 2 |   |
| 3 |   |

Answer:



Container registries:

▼

|   |
|---|
| 0 |
| 1 |
| 2 |
| 3 |

▼

|   |
|---|
| 0 |
| 1 |
| 2 |
| 3 |

Workspaces:

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

最新問題: 328

OU2 と User1 に対して計画された変更を実行する必要があります。

どのツールを使用する必要がありますか? 答えるには、適切なツールを正しいリソースにドラッグします。各ツールは 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: 正しく選択するたびに 1 ポイントの価値があります。

Tools

The Azure portal

Azure AD Connect

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

Answer Area

OU2:

Tool

User1:

Tool

Answer:

Tools

The Azure portal

Azure AD Connect

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

Answer Area

OU2: Azure AD Connect

User1: The Azure portal

最新問題: 329

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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Virtual networks that User2 can modify:

VNET4 only

VNET4 and VNET1 only

VNET4, VNET3, and VNET1 only

VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only

VNET4 and VNET1 only

VNET4, VNET3, and VNET1 only

VNET4, VNET3, VNET2, and VNET1

Answer:

Virtual networks that User2 can modify:

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

Virtual networks that User2 can delete:

|                                |
|--------------------------------|
| VNET4 only                     |
| VNET4 and VNET1 only           |
| VNET4, VNET3, and VNET1 only   |
| VNET4, VNET3, VNET2, and VNET1 |

Explanation:

ボックス 1: VNET4 と VNET1 のみ

RG1 には削除ロックのみがありますが、RG4 にはロックがありません。

RG2 と RG3 は両方とも読み取り専用ロックを持っています。

ボックス 2: VNET4 のみ

RG4 にはロックがありませんが、他のリソース グループには削除ロックまたは読み取り専用ロックが設定されています。

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および読み取り専用と呼ばれます。

CanNotDelete は、許可されたユーザーがリソースの読み取りと変更はできるが、リソースを削除できないことを意味します。

ReadOnly は、承認されたユーザーがリソースを読み取ることはできますが、リソースを削除または更新することは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、承認されたすべてのユーザーを閲覧者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と似ています。

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。

| Name  | Resource group |
|-------|----------------|
| VNET1 | RG1            |
| VNET2 | RG2            |
| VNET3 | RG3            |
| VNET4 | RG4            |

Sub1 には、次の表に示すロックが含まれています。

| Name  | Set on | Lock type |
|-------|--------|-----------|
| Lock1 | RG1    | Delete    |
| Lock2 | RG2    | Read-only |
| Lock3 | RG3    | Delete    |
| Lock4 | RG3    | Read-only |

参考文献:

最新問題: 330

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。

| Name | Operating system        |
|------|-------------------------|
| VM1  | Windows Server 2016     |
| VM2  | Ubuntu Server 18.04 LTS |

Azure Security Center から、自動プロビジョニングを有効にします。

次の表に示す仮想マシンをデプロイします。

| Name | Operating system        |
|------|-------------------------|
| VM3  | Windows Server 2016     |
| VM4  | Ubuntu Server 18.04 LTS |

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 と VM3 のみ
- C. VM3 および VM4 のみ
- D. VM1、VM2、VM3、および VM4

Answer: (解答を表示する)

自動プロビジョニングがオンになっている場合、Security Center は、サポートされているすべての Azure VM と新しく作成された Azure VM に Log Analytics エージェント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)、および 18.04 LTS (x64) および Windows Server 2008 R2、2012、2012 R2、2016、バージョン 1709 および 1803 が含まれます。

最新問題: 331

KeyVault1 という名前の Azure Key Vault があり、次の表に示す項目が含まれています。

| Name    | Type          |
|---------|---------------|
| Item1   | Key           |
| Item2   | Secret        |
| Policy1 | Access policy |

KeyVault では、次のイベントが順番に発生します。

- ※ 項目は削除されました
- \* 管理者は論理的な削除を有効にします。
- ※ Item2とPolicy1は削除されます。

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。



Answer Area

Microsoft

Statements

You can recover Policy1.

You can add a new key named Item1.

You can add a new secret named Item2.

Yes No

Answer:

Answer Area

Microsoft

Statements

You can recover Policy1.

You can add a new key named Item1.

You can add a new secret named Item2.

Yes No

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> (517**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 332

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 では、次の表に示すアラート ルールを作成します。

| Name  | Resource           | Condition                               |
|-------|--------------------|-----------------------------------------|
| Rule1 | RG1                | All security operations                 |
| Rule2 | RG1                | All administrative operations           |
| Rule3 | Azure subscription | All security operations by Admin1       |
| Rule4 | Azure subscription | All administrative operations by Admin1 |

Admin1 は RG1 で次のアクションを実行します。  
VNET1 という名前の仮想ネットワークを追加します  
Lock1 という名前の削除ロックを追加します  
Admin1 のアクションの結果としてアラートをトリガーするルールはどれですか？ 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Adding VNET1:

|                                |
|--------------------------------|
| Rule2 only                     |
| Rule4 only                     |
| Rule2 and Rule 4 only          |
| Rule3 and Rule 4 only          |
| Rule1, Rule2, Rule3 and Rule 4 |

Adding Lock1:

|                                |
|--------------------------------|
| Rule2 only                     |
| Rule4 only                     |
| Rule2 and Rule 4 only          |
| Rule3 and Rule 4 only          |
| Rule1, Rule2, Rule3 and Rule 4 |

Answer:

Adding VNET1:

|                                |
|--------------------------------|
| Rule2 only                     |
| Rule4 only                     |
| Rule2 and Rule 4 only          |
| Rule3 and Rule 4 only          |
| Rule1, Rule2, Rule3 and Rule 4 |

Adding Lock1:

|                                |
|--------------------------------|
| Rule2 only                     |
| Rule4 only                     |
| Rule2 and Rule 4 only          |
| Rule3 and Rule 4 only          |
| Rule1, Rule2, Rule3 and Rule 4 |

### 最新問題: 333

Windows Server1 および Server2 を実行し、内部ネットワーク上に配置されている Server1、Server2、および Server3 という名前の 3 つの オンプレミス サーバーがあります。Server3 はオンプレミス ネットワーク上にあります。すべてのサーバーが Azure にアクセスできます。Azure Sentinel から、Windows ファイアウォール データ コネクタをインストールします。

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

あなたは何をすべきか？

- A. Microsoft エージェントを Server1 にインストールし、Server2 がオンプレミス データ ゲートウェイを Server3 にインストールします。
- B. 各サーバーに Microsoft Agent をインストールします。

- C. Server1、Server2、および Server3 からイベント サブスクリプションを作成します。
- D. オンプレミス データ ゲートウェイを各サーバーにインストールします。

**Answer:** ([解答を表示する](#))

**最新問題: 334**

あなたの会社では Azure DevOps を使用しています。

コードが会社の品質基準とコードレビュー基準を満たしているかどうかを検証する方法を推奨する必要があります。

Azure DevOps に実装することを推奨するものは何ですか？

- A. ブランチフォルダ
- B. ブランチ権限
- C. ブランチポリシー
- D. 分岐ロック

**Answer: C** ([メッセージを残す](#))

セクション: [なし]

Explanation:

ブランチ ポリシーは、チームが開発の重要なブランチを保護するのに役立ちます。ポリシーは、チームのコード品質と変更管理基準を強制します。

参照 :

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts>

**最新問題: 335**

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

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

Answer Area

⬅

➡

⬆

⬆

Answer:

Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

Answer Area

Create an access review program.

Create an access review control.

Set Reviewers to Group owners.

⬅

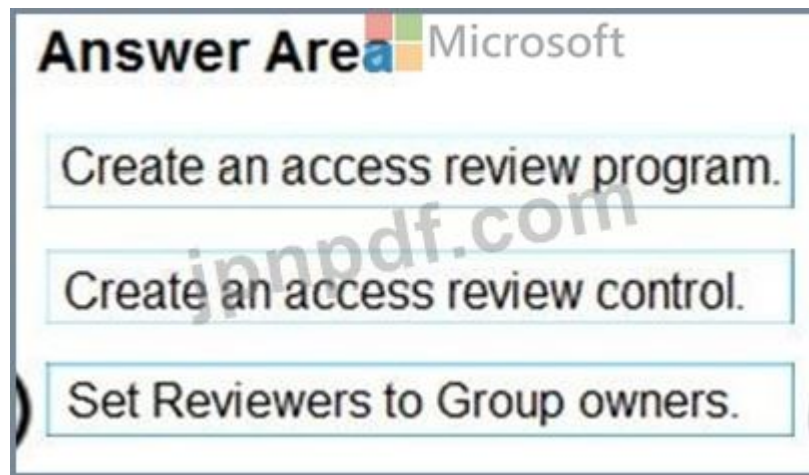
➡

⬆

⬆

説明





ステップ 1: アクセスレビュープログラムを作成する

ステップ 2: アクセス レビュー コントロールを作成する

ステップ 3: レビュー担当者をグループ所有者に設定する

「レビュー担当者」セクションで、範囲内のすべてのユーザーをレビューする 1 人以上のユーザーを選択します。または、メンバーに自分のアクセス権をレビューさせるように選択することもできます。リソースがグループの場合は、グループの所有者にレビューを依頼できます。



参考文献:

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

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

最新問題: 336

Azure サブスクリプションをお持ちです。サブスクリプションには、Windows Server 2016 を実行する Azure 仮想マシンが含まれています。各仮想マシンにカスタムのマルウェア対策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ポリシーを実装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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

```

{
  "if" : {
    "allOf": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : " ",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters": {
            " " : {
              "existenceCondition":
              "resources
              template
            }
          }
        }
      }
    }
  }
}

```

Answer:

```

{
  "if" : {
    "allof" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      },
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : "
    Append
    Deny
    DeployIfNotExists
    ",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            "
            existenceCondition
            resources
            template
            ": {
  }
}
}
}
}

```

参照：

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

#### 最新問題: 337

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が含まれる Group1 という名前の Azure Active Directory (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、再起動できることを確認する必要があります。

ソリューションでは、最小特権の原則を使用する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Answer:

説明

Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

参考文献:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

最新問題: 338

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

| Name  | Multi-factor authentication (MFA) status |
|-------|------------------------------------------|
| User1 | Disabled                                 |
| User2 | Disabled                                 |
| User3 | Enforced                                 |

Azure AD Privileged Identity Management (PIM) では、共同作成者ロールのロール設定が図に示すように構成されています。(「展示」タブをクリックします。)



Role settings

Assignment

☐ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☐ Allow permanent active assignment

Expire active assignments after

1 Month

☒ Require Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

Activation

Activation maximum duration (hours)

8

☒ Require Multi-Factor Authentication on activation

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approvers

No member or group selected

次の表に示すように、2019 年 5 月 1 日にユーザーに共同作成者のロールを割り当てます。

| Name  | Assignment type |
|-------|-----------------|
| User1 | Eligible        |
| User2 | Active          |
| User3 | Active          |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                 | Yes                   | No                    |
|------------------------------------------------------------|-----------------------|-----------------------|
| On May 15, 2019, User1 can activate the Contributor role.  | <input type="radio"/> | <input type="radio"/> |
| On May 15, 2019, User2 can use the Contributor role.       | <input type="radio"/> | <input type="radio"/> |
| On June 15, 2019, User3 can activate the Contributor role. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                 | Yes                              | No                    |
|------------------------------------------------------------|----------------------------------|-----------------------|
| On May 15, 2019, User1 can activate the Contributor role.  | <input checked="" type="radio"/> | <input type="radio"/> |
| On May 15, 2019, User2 can use the Contributor role.       | <input checked="" type="radio"/> | <input type="radio"/> |
| On June 15, 2019, User3 can activate the Contributor role. | <input checked="" type="radio"/> | <input type="radio"/> |

参照：

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

#### 最新問題: 339

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

securityPolicyinitiative1 という名前の Azure Policy イニシアチブを作成します。

すべての新しいリソース グループでどの標準的な役割の割り当てを構成する必要があるかを特定します。

新しいリソース グループの作成時に、SecurityPolicyinitiative1 とロールの割り当てを適用する必要があります。どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

| Actions                                                | Answer Area |
|--------------------------------------------------------|-------------|
| Publish an Azure Blueprint version.                    |             |
| Assign an Azure blueprint.                             |             |
| Create a policy assignment.                            |             |
| Create a custom role-based access control (RBAC) role. |             |
| Create a dedicated management subscription.            |             |
| Create an Azure Blueprints definition.                 |             |
| Create an initiative assignment.                       |             |

Answer:

| Answer Area                                           |                                                                                   |
|-------------------------------------------------------|-----------------------------------------------------------------------------------|
| Assign an Azure blueprint                             |  |
| Create a policy assignment                            |                                                                                   |
| Create a custom role-based access control (RBAC) role |                                                                                   |

- 1 - Azure ブループリントを割り当てる
- 2 - ポリシー割り当てを作成する
- 3 - カスタムのロールベースのアクセス制御 (RBAC) ロールを作成する

最新問題: 340

あなたの会社には、contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた Sub1 という名前の Azure サブスクリプションがあります。

会社は 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 Azure AD に登録されています。

App1 がアプリケーション ユーザーに代わって Azure Key Vault のシークレットにアクセスできることを確認する必要があります。

何を設定すればよいでしょうか？

- A. 管理者の同意のないアプリケーションの許可
- B. 管理者の同意のない委任されたアクセス許可
- C. 管理者の同意が必要な委任されたアクセス許可
- D. 管理者の同意が必要なアプリケーション権限

Answer: B ([メッセージを残す](#))

委任されたアクセス許可 - クライアント アプリケーションはサインイン ユーザーとして Web API にアクセスする必要がありますが、アクセスは選択したアクセス許可によって制限されます。このタイプの権限は、権限に管理者の同意が必要でない限り、ユーザーが付与できます。

不正解:

A、D: アプリケーションのアクセス許可 - クライアント アプリケーションは、それ自体として (ユーザー コンテキストなしで) Web API に直接アクセスする必要があります。このタイプの権限には管理者の同意が必要であり、パブリック (デスクトップおよびモバイル) クライアント アプリケーションでも使用できません。

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

最新問題: 341

Azure Active Directory (Azure AD) に関連付けられた 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。

Admin1 という名前の管理者は、次の ID にアクセスできます。

OpenID が有効なユーザー 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 Azure AD 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、Hotmail のみ  
C. contoso.com と fabrikam.com のみ  
D. contoso.com、fabrikam.com、Hotmail、および OpenID が有効なユーザー アカウント

**Answer: C (メッセージを残す)**  
サブスクリプションの請求所有権を別の Azure AD テナントのアカウントに譲渡すると、サブスクリプションを新しいアカウントのテナントに移動できます。これを行うと、サブスクリプションとそのリソースを管理するためのロールベースのアクセス (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 プリンシパルはアクセス権を失います。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: 342  
次の表に示す Azure 仮想マシンがあります。

| Name | Operating system                            | State   |
|------|---------------------------------------------|---------|
| VM1  | Windows Server 2008 R2 Service Pack 1 (SP1) | Running |
| VM2  | Windows Server 2012R2                       | Running |
| VM3  | Windows Server 2016                         | Stopped |
| VM4  | Ubuntu Server 18.04 LTS                     | Running |

どの仮想マシンに対して Update Management を有効にできますか？  
A. VM2 および VM3 のみ  
B. VM2、VM3、VM4 のみ  
C. VM1、VM2、VM4 のみ  
D. VM1、VM2、VM3、および VM4  
E. VM1、VM2、VM3 のみ

**Answer: C (メッセージを残す)**  
参考文献:  
<https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json>

最新問題: 343  
あなたの会社には、次の表に示すユーザーが含まれる Subscription1 という名前の Azure サブスクリプションがあります。



| Name  | Role                  |
|-------|-----------------------|
| User1 | Global administrator  |
| User2 | Billing administrator |
| User3 | Owner                 |
| User4 | Account Admin         |

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ますか?そのユーザーはどのツールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

User:

▼

User1User2User3User4

Tool:

▼

Azure Account CenterAzure Cloud ShellAzure PowerShellAzure Security Center

Answer:

User:

|       |   |
|-------|---|
|       | ▼ |
| User1 |   |
| User2 |   |
| User3 |   |
| User4 |   |



Tool:

|                       |   |
|-----------------------|---|
|                       | ▼ |
| Azure Account Center  |   |
| Azure Cloud Shell     |   |
| Azure PowerShell      |   |
| Azure Security Center |   |

参照 :

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

最新問題: 344

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、次のような出力が表示されます。

```

Name : DenyStorageAccess
Description :
Protocol : *
SourcePortRange : {*}
DestinationPortRange : {*}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Deny
Priority : 105
Direction : Outbound

Name : StorageEA2Allow
ProvisioningState : Succeeded
Description :
Protocol : *
SourcePortRange : {*}
DestinationPortRange : {443}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage/EastUS2}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 104
Direction : Outbound

Name : Contoso_FTP
Description :
Protocol : TCP
SourcePortRange : {*}
DestinationPortRange : {21}
SourceAddressPrefix : {1.2.3.4/32}
DestinationAddressPrefix : {10.0.0.5/32}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 504
Direction : Inbound

```

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成させる回答の選択肢を選択します。  
 注: 正しく選択するたびに 1 ポイントの価値があります。

Traffic destined for an Azure Storage account is [answer choice].

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

Answer:

Traffic destined for an Azure Storage account is [answer choice].

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

説明

ボックス 1: 米国東部 2 に接続可能

StorageEA2Allow には DestinationAddressPrefix {Storage/EastUS2} があります

ボックス 2: ドロップされました

参照 :

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

最新問題: 345

あなたの会社には、Subscription1 という名前の Azure サブスクリプションがあります。Subscription1 は、次の表に示すユーザーを含む Azure Active Directory テナントに関連付けられています。

| Name  | Role                  |
|-------|-----------------------|
| User1 | Global administrator  |
| User2 | Billing administrator |
| User3 | Owner                 |
| User4 | Account Admin         |

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ますか?そのユーザーはどのツールを使用する必要がありますか? 回答するには、回答領域で適切なオプ



ションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

User: 

User1

User2

User3

User4

Tool: 

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

Answer:

User:

Tool:

参照 :

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

最新問題: 346

ASG1 と ASG2 に対して計画された変更を実装します。

ASG1 を使用できる NSG はどれですか。また、どの仮想マシンのネットワーク インターフェイスを ASG2 に割り当てることができますか？

Answer Area

NSGs:

- NSG2 only
- NSG2 and NSG4 only
- NSG2, NSG3, and NSG4

Virtual machines:

- VM3 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM2, VM3, and VM4 only
- VM1, VM2, VM3, and VM4

Answer:

Answer Area

NSGs:

- NSG2 only
- NSG2 and NSG4 only
- NSG2, NSG3, and NSG4

Virtual machines:

- VM3 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM2, VM3, and VM4 only
- VM1, VM2, VM3, and VM4

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> (517**30%OFF**問題集溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: 347

ユーザーがアクセス権のないリソースにサインインしようとしているのではないかと考えられます。過去 3 日間に失敗したユーザーのサインイン試行を特定するには、Azure Log Analytics クエリを作成する必要があります。結果には、サインイン試行が 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設定すればよいでしょうか? 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: 正しく選択するたびに 1 ポイントの価値があります。

let timeframe = 3d;  
SecurityEvent  
| where TimeGenerated > ago(3d)  
| where AccountType == 'User' and

▼

ActivityID  
DataType  
EventID  
QuantityUnit

==4625

| Summarize failed\_login\_attempts=

▼

Count(),  
Countif(),  
Makeset(),  
Split(),

latest\_failed\_login=arg\_max(TimeGenerated by Account  
| where failed\_login\_attempts > 5

let timeframe = 3d;  
SecurityEvent  
| where TimeGenerated > ago(3d)  
| where AccountType == 'User' and  
  
| Summarize failed\_login\_attempts=  
  
latest\_failed\_login=arg\_max(TimeGenerated by Account  
| where failed login attempts > 5

▼

ActivityID  
DataType  
EventID  
QuantityUnit

==4625

▼

Count(),  
Countif(),  
Makeset(),  
Split(),

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

最新問題: 348

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

| Name  | Member of      |
|-------|----------------|
| User1 | Group1         |
| User2 | Group2         |
| User3 | Group1, Group2 |

Azure AD Privileged Identity Management (PIM) から、次の例に示すようにセキュリティ管理者ロールの設定を構成します。



**Assignment**☒ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☒ Allow permanent active assignment

Expire active assignments after

1 Month

☐ Require Azure Multi-Factor Authentication on active assignment☒ Require justification on active assignment**Activation**

Activation maximum duration (hours)



5

☐ Require Azure Multi-Factor Authentication on activation☐ Require justification on activation☐ Require ticket information on activation☐ Require approval to activate Select approvers

No member or group selected



PIM から、次のグループにセキュリティ管理者の役割を割り当てます。  
Group1: アクティブな割り当てタイプ、永続的に割り当てられています  
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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                                          | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 can only activate the Security Administrator role in five hours.                              | <input type="radio"/> | <input type="radio"/> |
| If User2 activates the Security Administrator role, the user will be assigned the role immediately. | <input type="radio"/> | <input type="radio"/> |
| User3 can activate the Security Administrator role.                                                 | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                          | Yes                              | No                    |
|-----------------------------------------------------------------------------------------------------|----------------------------------|-----------------------|
| User1 can only activate the Security Administrator role in five hours.                              | <input checked="" type="radio"/> | <input type="radio"/> |
| If User2 activates the Security Administrator role, the user will be assigned the role immediately. | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 can activate the Security Administrator role.                                                 | <input checked="" type="radio"/> | <input type="radio"/> |

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: 349

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、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                                 | Yes                   | No                    |
|----------------------------------------------------------------------------|-----------------------|-----------------------|
| From the Internet, you can connect to the web server on VM1 by using HTTP. | <input type="radio"/> | <input type="radio"/> |
| From the Internet, you can connect to the web server on VM2 by using HTTP. | <input type="radio"/> | <input type="radio"/> |
| From the Internet, you can connect to the web server on VM3 by using HTTP. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Answer Area                                                                |                                  |                                  |
|----------------------------------------------------------------------------|----------------------------------|----------------------------------|
| Statements                                                                 | Yes                              | No                               |
| From the Internet, you can connect to the web server on VM1 by using HTTP. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From the Internet, you can connect to the web server on VM2 by using HTTP. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From the Internet, you can connect to the web server on VM3 by using HTTP. | <input checked="" type="radio"/> | <input type="radio"/>            |



最新問題: 350

EASM1 という名前の Microsoft Defender 外部攻撃対象領域管理 (Defender EASM) リソースを含む Azure サブスクリプションがあります。EASM1 では検出が有効になっており、いくつかのインベントリ資産が含まれています。

どのインベントリ資産が最も重大な Web アプリのセキュリティ リスクに対して脆弱かを特定する必要があります。

どの Defender EASM ダッシュボードを使用する必要がありますか？

- A. 攻撃対象領域の概要
- B. OWASPTopIO
- C. GDPR への準拠
- D. 警備体制

Answer: ([解答を表示する](#))

最新問題: 351

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が含まれる Group1 という名前の Azure Active Directory (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、再起動できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Answer:

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

参考文献:  
<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

最新問題: 352

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Azure サブスクリプションがあります。テナントには、次の表に示すユーザーが含まれます。

| Name  | Subscription role | Azure AD user role    |
|-------|-------------------|-----------------------|
| User1 | Owner             | None                  |
| User2 | Contributor       | None                  |
| User3 | Security Admin    | None                  |
| User4 | None              | Service administrator |

RG1 という名前のリソース グループを作成します。  
どのユーザーが RG1 の権限を変更でき、どのユーザーが RG1 で仮想ネットワークを作成できますか? 回答するには、回答領域で適切なオブ



ションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Answer:

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Explanation:  
ボックス 1: 所有者のみがリソースの権限を変更できます。  
ボックス 2: 共同作成者はサブスクリプション内のあらゆるものを作成/変更/削除できますが、権限を変更することはできません。

最新問題: 353  
次の表に示すリソースが含まれる Subscription1 という名前の Azure サブスクリプションがあります。

| Name      | Type                            | Description                                                             |
|-----------|---------------------------------|-------------------------------------------------------------------------|
| EventHub1 | Azure Event Hubs                | Not applicable                                                          |
| Adf1      | Azure Data Factory              | Not applicable                                                          |
| NVA1      | Network virtual appliance (NVA) | The NVA sends security event messages in the Common Event Format (CEF). |

次のリソースを含む Subscription2 という名前の Azure サブスクリプションがあります。

- \* Azure Sentinel ワークスペース
- \* Azure Event Grid インスタンス

CEF メッセージを NVA から Azure Sentinel に取り込む必要があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Subscription1:

Subscription2:

Subscription2:

An Azure Log Analytics agent on a Linux virtual machine  
A Data Factory pipeline  
An Event Hubs namespace  
An Azure Service Bus queue

A new Azure Log Analytics workspace  
A new Azure Sentinel data connector  
A new Azure Sentinel playbook  
A new Event Grid resource provider

Answer:

Answer Area

Subscription1:

Subscription2:

Subscription2:

An Azure Log Analytics agent on a Linux virtual machine  
A Data Factory pipeline  
An Event Hubs namespace  
An Azure Service Bus queue

A new Azure Log Analytics workspace  
A new Azure Sentinel data connector  
A new Azure Sentinel playbook  
A new Event Grid resource provider

最新問題: 354

storage1 という名前のストレージ アカウントと複数の仮想マシンを含む Azure サブスクリプションがあります。  
ストレージ アカウントと仮想マシンは同じ Azure リージョンにあります。仮想マシンのネットワーク構成を次の表に示します。

| Name | Public IP address | Connected to  |
|------|-------------------|---------------|
| VM1  | 52.232.128.194    | VNET1/Subnet1 |
| VM2  | 52.233.129.82     | VNET2/Subnet2 |
| VM3  | 52.233.130.11     | VNET3/Subnet3 |

仮想ネットワーク サブネットには、次の表に示すように定義されたサービス エンドポイントがあります。

| Name          | Service endpoint   |
|---------------|--------------------|
| VNET1/Subnet1 | Microsoft.Storage  |
| VNET2/Subnet2 | None               |
| VNET3/Subnet3 | Microsoft.KeyVault |

storage1 に対して次のファイアウォールと仮想ネットワーク設定を構成します。

- \* からのアクセスを許可: 選択したネットワーク

\* 仮想ネットワーク: VNET3\Subnet3  
\* ファイアウォール - アドレス範囲: 52.233.129.0/24

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                   | Yes                   | No                    |
|------------------------------|-----------------------|-----------------------|
| VM1 can connect to storage1. | <input type="radio"/> | <input type="radio"/> |
| VM2 can connect to storage1. | <input type="radio"/> | <input type="radio"/> |
| VM3 can connect to storage1. | <input type="radio"/> | <input type="radio"/> |

Answer:

説明

| Statements                   | Yes                              | No                               |
|------------------------------|----------------------------------|----------------------------------|
| VM1 can connect to storage1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM2 can connect to storage1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM3 can connect to storage1. | <input type="radio"/>            | <input checked="" type="radio"/> |

ボックス 1: いいえ

VNet1 には、Azure Storage 用に構成されたサービス エンドポイントがあります。ただし、Azure ストレージでは、VNet1 または VM1 のパブリック IP アドレスからのアクセスは許可されません。

ボックス 2: はい

VNet2 にはサービス エンドポイントが構成されていません。ただし、Azure ストレージでは VM2 のパブリック IP アドレスからのアクセスが許可されます。

ボックス 3: いいえ

Azure ストレージでは VNet3 からのアクセスが可能です。ただし、VNet3 には Azure ストレージのサービス エンドポイントがありません。Azure ストレージでは、VM3 のパブリック IP からのアクセスも許可されません。

最新問題: 355

Contosostorage1 という名前の Azure Storage アカウントと Contosokeyvault1 という名前の Azure Key Vault 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 に保存する Azure Automation Runbook を作成する予定です。

Runbook を確実に実装するには、前提条件を実装する必要があります。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。



| Actions                                                       | Answer Area |
|---------------------------------------------------------------|-------------|
| Run Set-AzureRmKeyVaultAccessPolicy                           |             |
| Create an Azure Automation account.                           |             |
| Import PowerShell modules to the Azure Automation account.    |             |
| Create a user-assigned managed identity.                      |             |
| Create a connection resource in the Azure Automation account. |             |

Navigation icons: Left arrow, Right arrow, Up arrow, Down arrow.

Answer:

| Actions                                                       | Answer Area                                                   |
|---------------------------------------------------------------|---------------------------------------------------------------|
| Run Set-AzureRmKeyVaultAccessPolicy                           |                                                               |
| Create an Azure Automation account.                           | Create an Azure Automation account.                           |
| Import PowerShell modules to the Azure Automation account.    | Import PowerShell modules to the Azure Automation account.    |
| Create a user-assigned managed identity.                      |                                                               |
| Create a connection resource in the Azure Automation account. | Create a connection resource in the Azure Automation account. |

Navigation icons: Left arrow, Right arrow, Up arrow, Down arrow.

説明



Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

ステップ 1: Azure Automation アカウントを作成する

Runbook は Azure Automation アカウント内に存在し、PowerShell スクリプトを実行できます。

ステップ 2: PowerShell モジュールを Azure Automation 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 [資産] で、[Runbook にモジュールを追加する] を選択します。Runbook で Key Vault コマンドレットを実行するには、AzureRM.profile と AzureRM.key Vault を追加する必要があります。

ステップ 3: Azure Automation 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、実行アカウントを使用して認証し、Runbook で Resource Manager リソースを管理できます。AzureRunAsConnection は、上記の「実行アカウント」を作成したときに自動的に作成される接続アセットです。

これは、[資産] -> [接続] にあります。認証コードの後に、上記と同じコードを実行して、ボールド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...」  
AzureRmAccount の追加`  
-サービスプリンシパル`  
-TenantId $servicePrincipalConnection.TenantId`  
-ApplicationId $servicePrincipalConnection.ApplicationId`  
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint  
}
```

参考文献:

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

最新問題: 356

プラットフォームの保護要件を満たすには、Microsoft マルウェア対策を導入する必要があります。  
あなたは何をすべきか？回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:



▼

The Create a Managed Identify setting

The exclusion settings

The scope

Answer:

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:



▼

The Create a Managed Identify setting

The exclusion settings

The scope

説明

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists



Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

シナリオ:Microsoft Antimalware を RG1 の仮想マシンにインストールする必要があります。

RG1 は、Vnet1、VM0、および VM1 を含むリソース グループです。

ボックス 1: DeployIfNotExists

DeployIfNotExists は、条件が満たされた場合にテンプレートのデプロイメントを実行します。

Azure ポリシー定義マルウェア対策

参照：

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

#### 最新問題: 357

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。

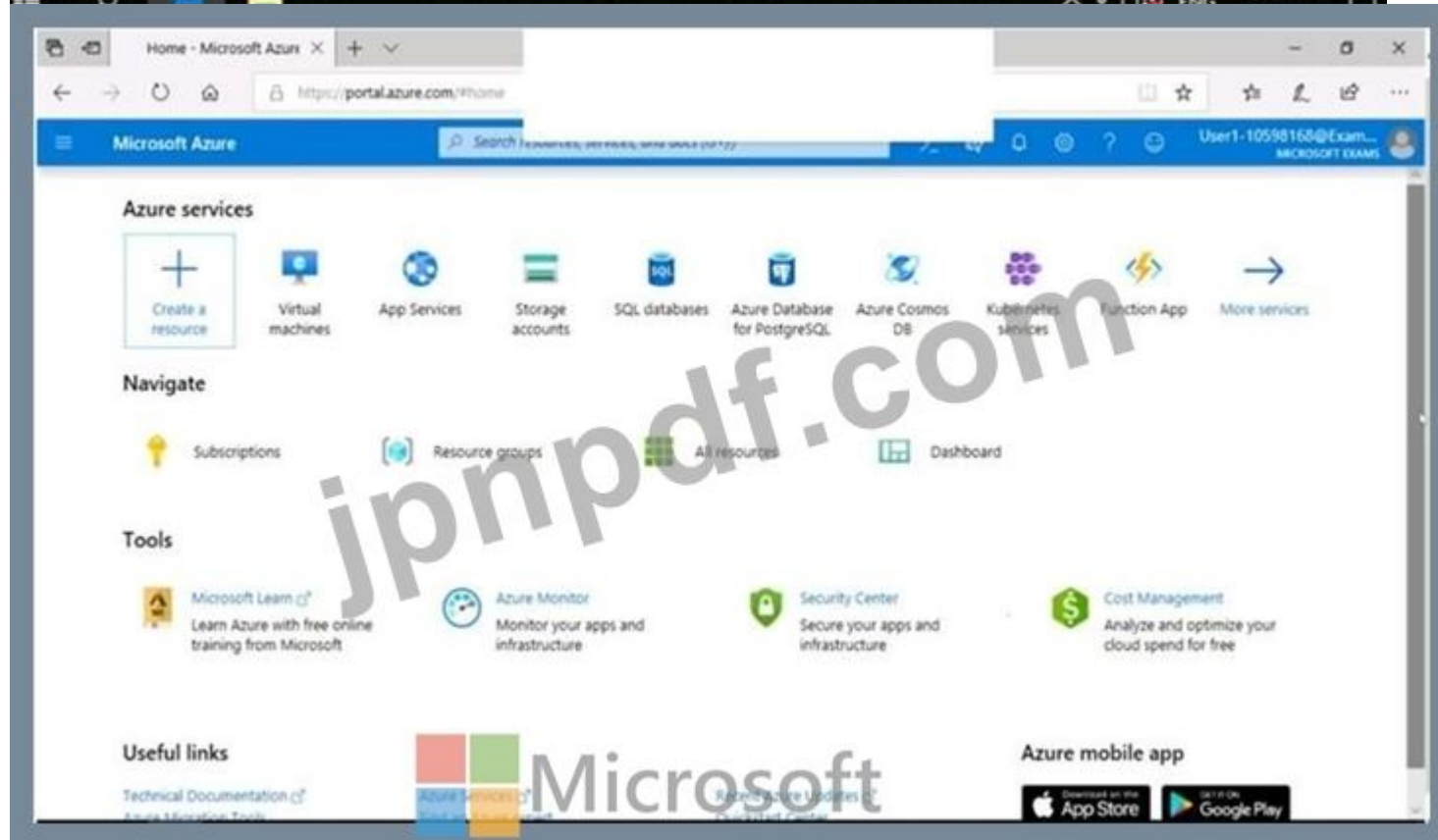
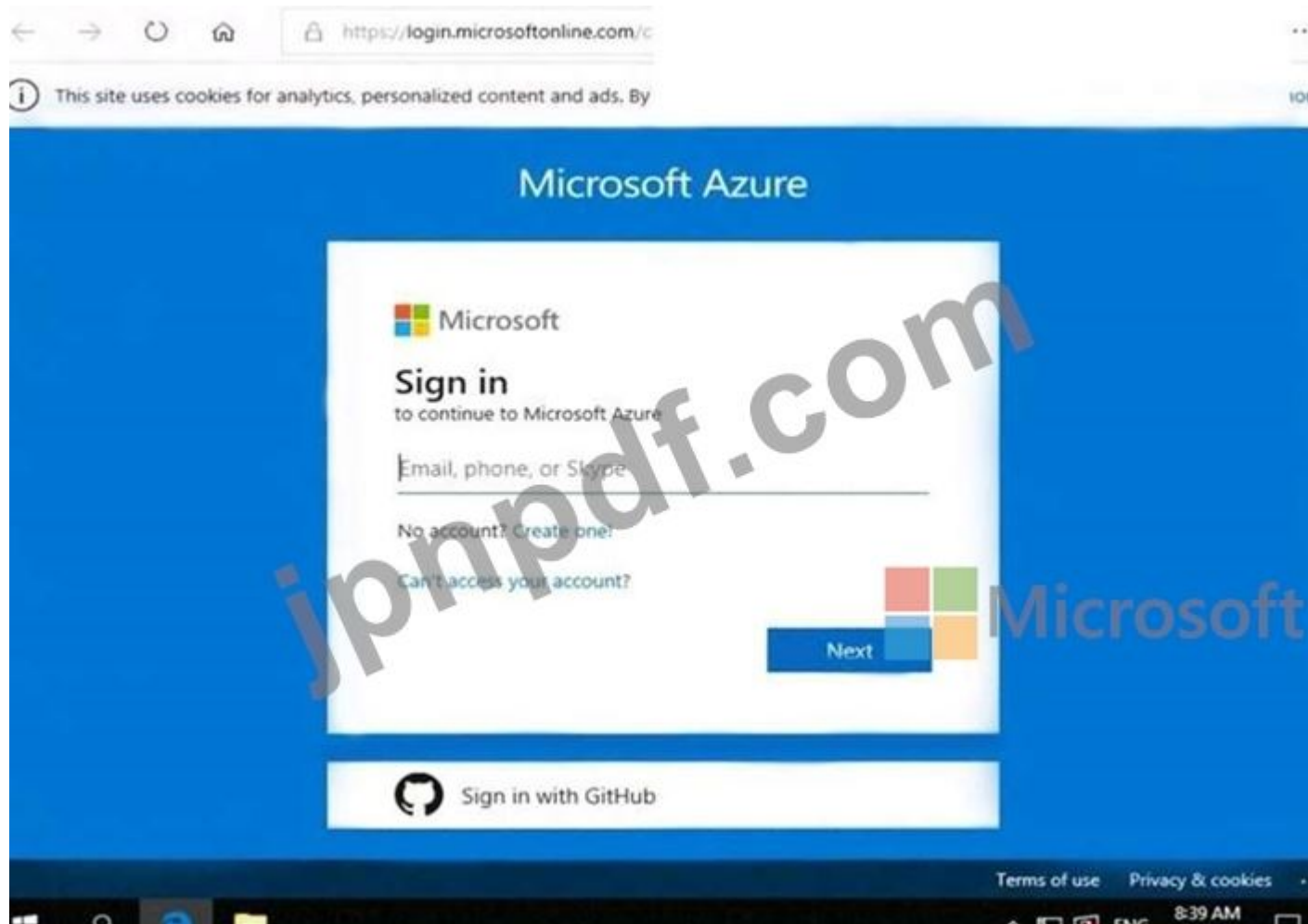
パスワードを入力するには、「パスワードの入力」ボックスにカーソルを置き、下のパスワードをクリックします。

Azure ユーザー名: User1-10598168@ExamUsers.com

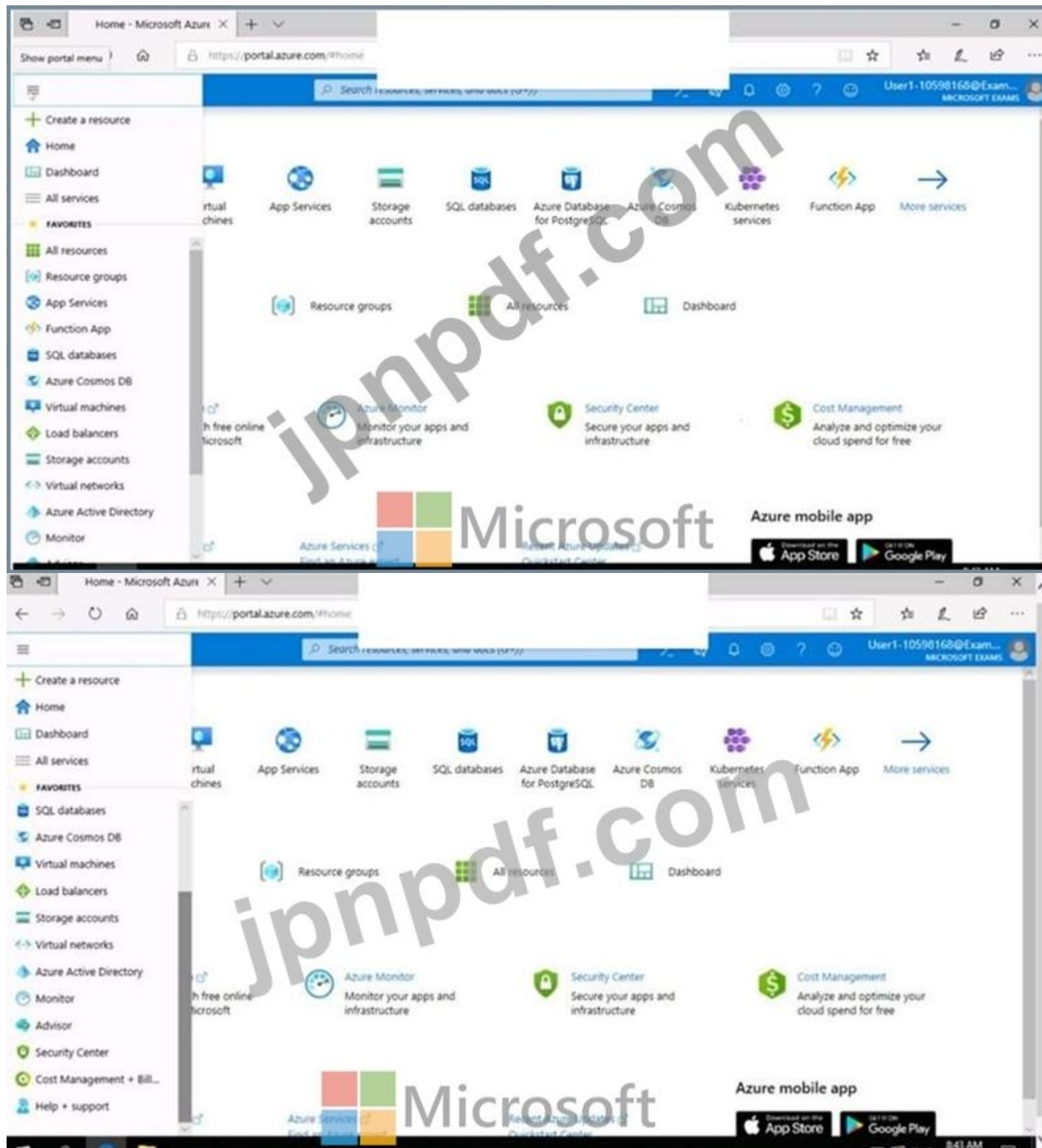
Azure パスワード: Ag1Bh9!#Bd

次の情報は、テクニカル 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 Azure Active Directory (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 portal にサインインします。

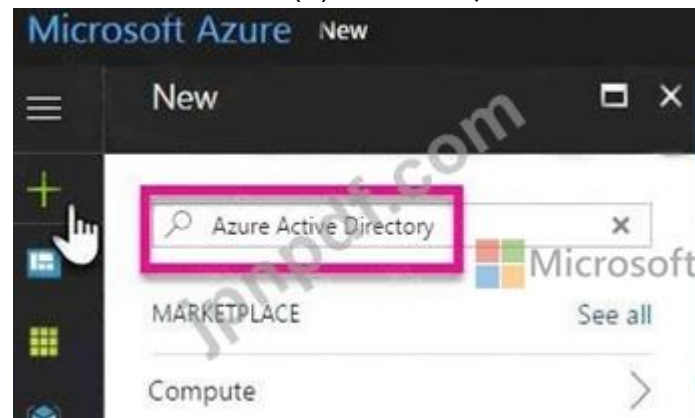
**Answer:**

以下の説明を参照してください。

#### 説明

##### ステップ 1: Azure Active Directory テナントを作成する

1. Azure portal にアクセスし、Azure サブスクリプションを持つアカウントでサインインします。
2. プラス アイコン (+) を選択し、Azure Active Directory を検索します。



3. 検索結果で「Azure Active Directory」を選択します。



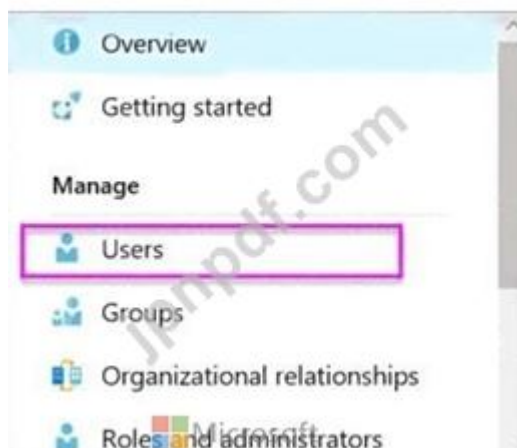
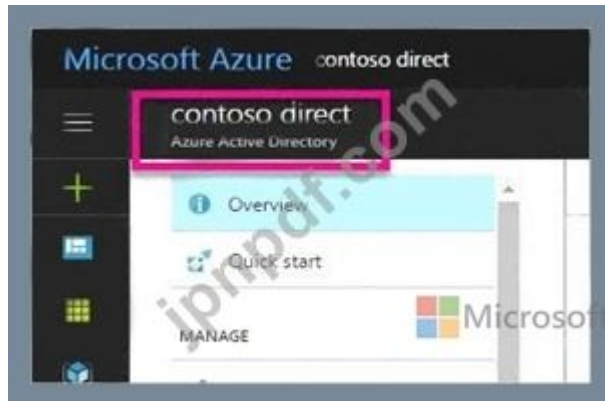
4. [作成]を選択します。
5. 組織名と初期ドメイン名 (10598168) を入力します。次に、「作成」を選択します。あなたのディレクトリ

創造された。

6. ディレクトリの作成が完了したら、新しいディレクトリを管理するための情報ボックスを選択します。次に、テナント ユーザーを追加します。

## ステップ 2: Azure Active Directory テナント ユーザーを作成する

7. Azure portal で、Azure Active Directory フライアウトに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、[+ 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: ユーザー1

ユーザー名: user1@10598168.onmicrosoft.com

User  
contoso direct

\* Name ⓘ  
PBI Embed ✓

\* User name ⓘ  
pbiembed@contosodirect.onmicrosoft.com ✓

Profile ⓘ  
Not configured >

Properties ⓘ  
Default >

Groups ⓘ  
0 groups selected >

Directory role ⓘ  
User >

Password  
\*\*\*\*\*  
☐ Show Password

参照：

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

#### 最新問題: 358

プラットフォームの保護要件を満たすには、AKS1 をデプロイする必要があります。

どの 4 つのアクションを順番に実行する必要がありますか？ 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

注: 回答の選択肢は複数の順序で正解です。選択した正しい注文に対してクレジットを受け取ります。



## Actions

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

## Answer Area

Answer:

## Actions

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

## Answer Area

Create a server application.

Create a client application.

Deploy an AKS cluster.

Create an RBAC binding.

参照 :

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration>

トピック 3、Fabrikam Inc.

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。

| Name | Location   |
|------|------------|
| ASG1 | West US    |
| ASG2 | Central US |

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。

Azure Security Center 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、利用可能なすべてのオペレーティング システムに存在します。

RG2 という名前のリソース グループを作成します。

OU2 を Azure AD に同期します。

User1 を Group1 に追加します。

技術的要件

Fabrikam は次の技術要件を特定します。

財務部門のユーザーは、SharePoint Online にアクセスするときに 3 時間後に再認証する必要があります。

Storage1 は、顧客管理のキーと自動キー 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のアラート

VM1、VM2、および VM3 は、Azure Disk Encryption 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経由で移動してはなりません。

最新問題: 359

ネットワークには、Azure Active Directory (Azure AD) と同期する adatum.com という名前のオンプレミスの Active Directory ドメインが含まれています。

Azure AD テナントには、次の表に示すユーザーが含まれています。

| Name  | Source                       | Password          |
|-------|------------------------------|-------------------|
| User1 | Azure AD                     | Adatum123         |
| User2 | Azure AD                     | N3w3rT0Gue33      |
| User3 | On-premises Active Directory | ComplexPassword33 |

次の図に示すように、adatum.com の認証方法 - パスワード保護設定を構成します。

Custom smart lockout

Lockout threshold ⓘ 10 ✓

Lockout duration in seconds ⓘ 60 ✓

Custom banned passwords

Enforce custom list ⓘ ☒ Yes ☐ No

Custom banned password list ⓘ

Adatum ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ ☒ Yes ☐ No

Mode ⓘ ☐ Enforced ☒ Audit

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                         | Yes                   | No                    |
|--------------------------------------------------------------------|-----------------------|-----------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/> | <input type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input type="radio"/> | <input type="radio"/> |
| User3 can change the password to Adatum123!.                       | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can change the password to Adatum123!.                       | <input checked="" type="radio"/> | <input type="radio"/>            |

説明  
自動生成されるテキスト説明

| Statements                                                         | Yes                              | No                               |
|--------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 will be prompted to change the password on the next sign-in. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can change the password to @d@tum_C0mpleX123.                | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can change the password to Adatum123!.                       | <input checked="" type="radio"/> | <input type="radio"/>            |

参照 :  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-de>  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

最新問題: 360

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。

| Name | Resource group | Status                |
|------|----------------|-----------------------|
| VM1  | RG1            | Stopped (Deallocated) |
| VM2  | RG2            | Stopped (Deallocated) |

次の表に示す Azure ポリシーを作成します。

| Policy definition          | Resource type   | Scope |
|----------------------------|-----------------|-------|
| Not allowed resource types | virtualMachines | RG1   |
| Allowed resource types     | virtualMachines | RG2   |

次の表に示すリソース ロックを作成します。

| Name  | Type      | Created on |
|-------|-----------|------------|
| Lock1 | Read-only | VM1        |
| Lock2 | Read-only | RG2        |

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                               | Yes                              | No                    |
|------------------------------------------|----------------------------------|-----------------------|
| You can start VM1.                       | <input checked="" type="radio"/> | <input type="radio"/> |
| You can start VM2.                       | <input type="radio"/>            | <input type="radio"/> |
| You can create a virtual machine in RG2. | <input type="radio"/>            | <input type="radio"/> |

Answer:

最新問題: 361



Subscription1 という名前の Azure サブスクリプションがあり、これには RG1 という名前のリソース グループと User1 という名前のユーザーが含まれています。User1 には、RG1 の所有者の役割が割り当てられます。

次の図に示すように、RG2 という名前のリソース グループを含む Blueprint1 という名前の Azure Blueprints 定義を作成します。

Edit blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

| NAME                                                           | ARTIFACT TYPE   | PARAMETERS                      |
|----------------------------------------------------------------|-----------------|---------------------------------|
| ▼ Subscription                                                 |                 |                                 |
| + Add artifact...                                              |                 |                                 |
| ▼ RG2                                                          | Resource group  | 2 out of 2 parameters populated |
| User1 (User1@sk200628outlookonmicrosoft.com) : Tag Contributor | Role assignment | 1 out of 1 parameters populated |
| + Add artifact...                                              |                 |                                 |

次の設定を使用して、Blueprint1 を Subscription1 に割り当てます。

ロックの割り当て: 読み取り専用

マネージド ID: システム割り当て

次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

| Statements                                                  | Yes                   | No                    |
|-------------------------------------------------------------|-----------------------|-----------------------|
| A locking mode of Read Only will be assigned to RG1.        | <input type="radio"/> | <input type="radio"/> |
| User1 can add tags to RG2.                                  | <input type="radio"/> | <input type="radio"/> |
| You can remove User1 from the Tag Contributor role for RG2. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                  | Yes                              | No                               |
|-------------------------------------------------------------|----------------------------------|----------------------------------|
| A locking mode of Read Only will be assigned to RG1.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| User1 can add tags to RG2.                                  | <input checked="" type="radio"/> | <input type="radio"/>            |
| You can remove User1 from the Tag Contributor role for RG2. | <input type="radio"/>            | <input checked="" type="radio"/> |

参照：

次の表に示す Azure Key Vault があります。

KV1 には、Secret1 という名前のシークレットと、Key1 という名前のマネージドストレージ アカウントのキーが保存されます。Secret1 と Key1 をバックアップします。

各バックアップをどのキー コンテナに復元できますか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

- ☐ KV1 only
- ☐ KV1 and KV2 only
- ☐ KV1, KV2 and KV3 only
- ☐ KV1, KV2 and KV4 only
- ☐ KV1, KV2, KV3, KV4, and KV5

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

**Answer:**

You can restore the Secret1 backup to:

You can restore the Key1 backup to:

Microsoft

最新問題: 363

複数の仮想マシン ディスクに Azure Disk Encryption を使用する予定です。

Azure Disk Encryption が KeyVault11641655 Azure Key Vault からシークレットを取得でき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 portal にサインインし、Azure リソースを変更します。

以下の説明を参照してください。

**Answer:**

説明

1. Azure portal で、検索結果から「Key Vault」と入力し、KeyVault11641655 を選択します。または、左側のナビゲーション ペインで を参照します。
2. Key Vault のプロパティで、[アクセス ポリシー] まで下にスクロールします。
3. ボリューム暗号化に Azure Disk Encryption を選択します

Enable Access to:

- ☐ Azure Virtual Machines for deployment ⓘ
- ☐ Azure Resource Manager for template deployment ⓘ
- ☒ Azure Disk Encryption for volume encryption ⓘ

4. 「保存」をクリックして変更を保存します。

最新問題: 364

contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた 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 が有効なユーザー 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 Azure AD 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、Hotmail のみ
- C. contoso.com と fabrikam.com のみ
- D. contoso.com、fabrikam.com、Hotmail、および OpenID が有効なユーザー アカウント

**Answer: C** ([メッセージを残す](#))

セクション: [なし]

Explanation:

サブスクリプションの請求所有権を別の Azure AD テナントのアカウントに譲渡すると、サブスクリプションを新しいアカウントのテナントに移動できます。これを行うと、サブスクリプションとそのリソースを管理するためのロール ベースのアクセス (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 プリンシパルはアクセス権を失います。転送リクエストを受け入れる新しいアカウントのユーザーのみが、リソースを管理するためのアクセス権を持ちます。

参照 :

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

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

#### 最新問題: 365

次のデータ コネクタを備えた Azure Sentinel ワークスペースがあります。

Azure Active Directory ID 保護

コモンイベントフォーマット(CEF)

Azure ファイアウォール

データが各コネクタから取り込まれていることを確認する必要があります。

[ログ クエリ] ウィンドウから、各コネクタに対してどのテーブルをクエリ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: 正しく選択するたびに 1 ポイントの価値があります。



Azure Active Directory Identity Protection Microsoft

Azure Firewall:

CEF:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

Answer:

Azure Active Directory Identity Protection:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

Azure Firewall:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

CEF:

|                   |
|-------------------|
| AzureDiagnostics  |
| CommonSecurityLog |
| SecurityAlert     |
| SecurityEvent     |
| Syslog            |

 Microsoft

**最新問題: 366**

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。

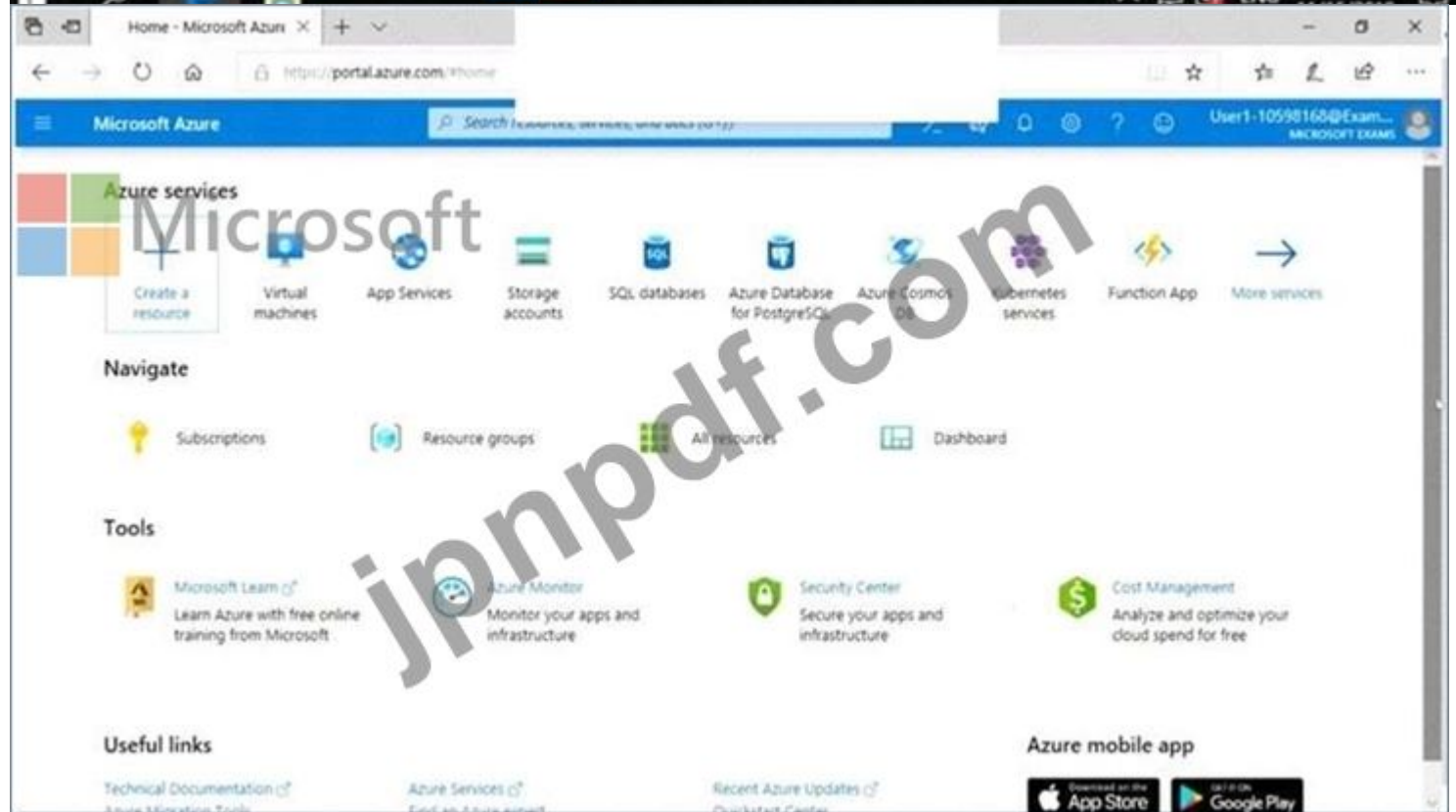
パスワードを入力するには、「パスワードの入力」ボックスにカーソルを置き、下のパスワードをクリックします。

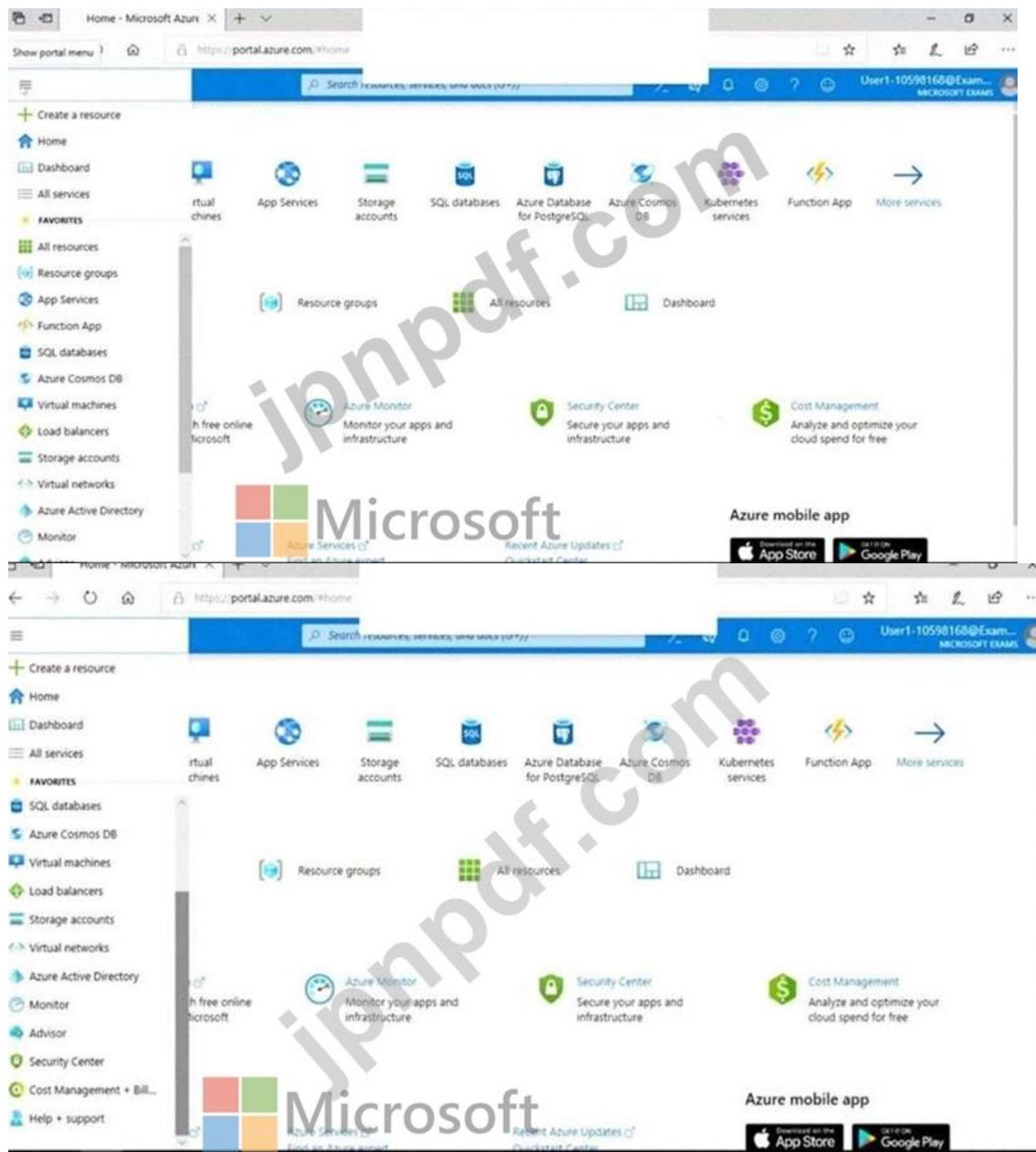
Azure ユーザー名: User1-10598168@ExamUsers.com

Azure パスワード: Ag1Bh9!#Bd

次の情報は、テクニカル 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。ソリューションでは、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 portal 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 portal 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] > [役割割り当ての追加] をクリックして、[役割割り当ての追加] ペインを開きます。



5. [ロール] ドロップダウン リストで、ロール [仮想マシン共同作成者] を選択します。仮想マシン共同作成者を使用すると、仮想マシンを管理できますが、仮想マシンへのアクセスや、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 アカウントへのアクセスはできません。
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: 367**

Azure サブスクリプションをお持ちです。

次の要件を満たす Azure ポリシーを作成してデプロイする必要があります。

新しい仮想マシンがデプロイされると、カスタム セキュリティ拡張機能が自動的にインストールされます。

非標準の仮想マシンに対して自動生成された修復タスクをトリガーして、拡張機能をインストールします。

ポリシーには何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Definition effect:

|                      |
|----------------------|
| ▼                    |
| Append               |
| DeployIfNotExists    |
| EnforceOPAConstraint |
| EnforceRegoPolicy    |
| Modify               |

Assignment remediation task:

|                                                                 |
|-----------------------------------------------------------------|
| ▼                                                               |
| A managed identity that has the Contributor role                |
| A managed identity that has the User Access Administrator role  |
| A service principal that has the Contributor role               |
| A service principal that has the User Access Administrator role |

Answer:

Definition effect:

|                      |
|----------------------|
| ▼                    |
| Append               |
| DeployIfNotExists    |
| EnforceOPAConstraint |
| EnforceRegoPolicy    |
| Modify               |

Assignment remediation task:

|                                                                 |
|-----------------------------------------------------------------|
| ▼                                                               |
| A managed identity that has the Contributor role                |
| A managed identity that has the User Access Administrator role  |
| A service principal that has the Contributor role               |
| A service principal that has the User Access Administrator role |

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

最新問題: 368

Update Management 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。

| Name | Operating system             | Region  | Resource group |
|------|------------------------------|---------|----------------|
| VM1  | Windows Server 2012          | East US | RG1            |
| VM2  | Windows Server 2012 R2       | West US | RG1            |
| VM3  | Windows Server 2016          | West US | RG2            |
| VM4  | Ubuntu Server 18.04 LTS      | West US | RG2            |
| VM5  | Red Hat Enterprise Linux 7.4 | East US | RG1            |
| VM6  | CentOS 7.5                   | East US | RG1            |

Update1 と Update2 という名前の 2 つの更新プログラムの展開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、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Update1:  ▼

|                             |
|-----------------------------|
| VM2 only                    |
| VM4 only                    |
| VM1 and VM2 only            |
| VM1, VM2, VM4, VM5, and VM6 |

Update2:  ▼

|                             |
|-----------------------------|
| VM5 only                    |
| VM1 and VM5 only            |
| VM4 and VM5 only            |
| VM1, VM2, and VM5 only      |
| VM1, VM2, VM3, VM4, and VM5 |

Answer:

Update1:  ▼

|                             |
|-----------------------------|
| VM2 only                    |
| VM4 only                    |
| VM1 and VM2 only            |
| VM1, VM2, VM4, VM5, and VM6 |

Update2:  ▼

|                             |
|-----------------------------|
| VM5 only                    |
| VM1 and VM5 only            |
| VM4 and VM5 only            |
| VM1, VM2, and VM5 only      |
| VM1, VM2, VM3, VM4, and VM5 |

Explanation:

更新 1: VM1 と VM2 のみ

VM3: Windows Server 2016 米国西部 RG2

更新 2: VM4 および VM5 のみ

VM6: CentOS 7.5 米国東部 RG1

Linux の場合、マシンはアップデート リポジトリにアクセスできる必要があります。更新リポジトリはプライベートまたはパブリックにすることができます。

参考文献:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

最新問題: 369

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

| Name  | Member of      | Multi-factor authentication (MFA) status |
|-------|----------------|------------------------------------------|
| User1 | Group1, Group2 | Enabled                                  |
| User2 | Group1         | Disabled                                 |
| User3 | Group1         | Disabled                                 |

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

\* 割り当て: Group1 を含み、Group2 を除く

※ 条件 :サインイン危険度 : 中以上

\* アクセス :アクセスを許可、多要素認証が必要

ユーザーが Azure AD にサインインするときに何が起きるかを特定する必要があります。

各ユーザーについて何を識別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: 正しく選択するたびに 1 ポイントの価値があります。

When User1 signs in from an anonymous IP address, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

Answer:



When User1 signs in from an anonymous IP address,  
the user will:

Be blocked  
Be prompted for MFA  
Sign in by using a username and password only

When User2 signs in from an unfamiliar location,  
the user will:

Be blocked  
Be prompted for MFA  
Sign in by using a username and password only

When User3 signs in from an infected device,  
the user will:

Be blocked  
Be prompted for MFA  
Sign in by using a username and password only

説明

When User1 signs in from an anonymous IP address,  
the user will:

Be blocked  
Be prompted for MFA  
Sign in by using a username and password only

When User2 signs in from an unfamiliar location,  
the user will:

Be blocked  
Be prompted for MFA  
Sign in by using a username and password only

When User3 signs in from an infected device,  
the user will:

Be blocked  
Be prompted for MFA  
Sign in by using a username and password only

参考文献:

<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: 370

次の表に示すリソースを保存する Vault1 という名前の Azure Key Vault があります。

| Name    | Type        |
|---------|-------------|
| Key1    | Key         |
| Secret1 | Secret      |
| Cert1   | Certificate |

ローテーション ポリシーの作成をサポートするリソースはどれですか?

- A. キー1のみ
  - B. Key1 と Secret1 のみ
  - C. Key1、Secret1、Cert1
  - D. Key1 と Cert1 のみ
  - E. Cert1 のみ
  - F. Secret1 と Cert1 のみ
- Answer: A ([メッセージを残す](#))

最新問題: 371

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

| Name  | Role                  |
|-------|-----------------------|
| User1 | Global administrator  |
| User2 | Billing administrator |
| User3 | Owner                 |
| User4 | Account Admin         |

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ますか?そのユーザーはどのツールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。  
注: 正しく選択するたびに 1 ポイントの価値があります。

User:

▼

User1User2User3User4

Tool:

▼

Azure Account CenterAzure Cloud ShellAzure PowerShellAzure Security Center

Answer:

User:  Microsoft ▼

|       |
|-------|
| User1 |
| User2 |
| User3 |
| User4 |

Tool: ▼

|                       |
|-----------------------|
| Azure Account Center  |
| Azure Cloud Shell     |
| Azure PowerShell      |
| Azure Security Center |

Explanation:

ボックス 1; ユーザー2

請求管理者

譲渡するサブスクリプションの請求所有権を譲渡するを選択します。

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が利用可能です。

参照 :

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

#### 最新問題: 372

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 に接続されている仮想マシンが VNET2 に接続されている仮想マシンと通信できることを保証する必要があります。

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

以下の説明を参照してください。

#### Answer:

説明

2 つのネットワーク間に 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 に接続されている仮想マシンが VNET2 に接続されている仮想マシンと通信できることを保証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ない。したがって、一方向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 portal 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、[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、ピアリングが VNET1 で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、ピアリングが VNET2 で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] オプションで、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: 373

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成でき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含まれ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すると、その質問に戻ることはできません。その結果、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 Azure HDInsight クラスタがあります。

ユーザーがオンプレミスの Active Directory 資格情報を使用してクラスタに対して認証できるようにする予定です。

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 (メッセージを残す)**

Azure Virtual Network 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も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 Virtual Network にカスタム DNS サーバーを作成します。

デフォルトの Azure Recursive の代わりにカスタム DNS サーバーを使用するように仮想ネットワークを構成するリゾルバ。

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-premises-network>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>



最新問題: 374

Azure Container Registry に接続する Azure Kubernetes Service (AKS) クラスターを構成しています。  
Azure Container Registry に対する認証には、自動生成されたサービス プリンシパルを使用する必要があります。  
何を作成する必要がありますか？

- A. Azure Active Directory (Azure AD) グループ
- B. Azure Active Directory (Azure AD) のロールの割り当て
- C. Azure Active Directory (Azure AD) ユーザー
- D. Azure Key Vault のシークレット

**Answer: B** ([メッセージを残す](#))

AKS クラスターを作成すると、Azure は他の Azure リソースとのクラスターの操作性をサポートするサービス プリンシパルも作成します。  
この自動生成されたサービス プリンシパルを ACR レジストリでの認証に使用できます。これを行うには、クラスターのサービス プリンシパルにコンテナ レジストリへのアクセスを許可する Azure AD ロール割り当てを作成する必要があります。

参考文献:

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

**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> (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)