Prüfungsnummer:AZ-303

Prüfungsname:(deutsche Version und englische Version) Microsoft Azure Architect Technologies

Version:demo

https://www.itpruefungsfragen.de/

Achtung: Aktuelle englische Version zu AZ-303 bei uns ist gratis!!

1.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Sie haben eine Azure App Service-App.

Sie müssen die Ablaufverfolgung für die App implementieren. Die Ablaufverfolgungsinformationen müssen Folgendes enthalten:
Nutzungstrends
Antworten auf AJAX-Aufrufe
Geschwindigkeit des Ladens von Seiten per Browser
Server- und Browser-Ausnahmefehler
Wie gehen Sie vor?

A.Konfigurieren Sie die IIS-Protokollierung in Azure Log Analytics.
B.Konfigurieren Sie einen Verbindungsmonitor in Azure Network Watcher.
C.Konfigurieren Sie benutzerdefinierte Protokolle in Azure Log Analytics.
D.Aktivieren Sie die Azure Application Insights-Site-Erweiterung.

Korrekte Antwort: D

Erläuterungen:

Application Insights, ein Feature von Azure Monitor, ist ein erweiterbarer Dienst zur Verwaltung der Anwendungsleistung (Application Performance Management, APM) für Entwickler und DevOps-Profis. Überwachen Sie damit Ihre aktiven Anwendungen. Der Dienst erkennt automatisch Leistungsanomalien und verfügt über leistungsstarke Analysetools, mit denen Sie Probleme diagnostizieren und nachvollziehen können, wie Ihre App von den Benutzern verwendet wird. Der Dienst unterstützt Sie bei der kontinuierlichen Verbesserung der Leistung und Benutzerfreundlichkeit Ihrer App. Er lässt sich für Apps auf einer Vielzahl von Plattformen einsetzen. Dazu zählen unter anderem .NET, Node.js, Java und Python (lokal gehostet, als Hybridmodell oder in einer öffentlichen Cloud). Der Dienst lässt sich in Ihren DevOps-Prozess integrieren und verfügt über Verbindungspunkte mit einer Vielzahl von Entwicklungstools. Sie können Telemetriedaten von mobilen Apps durch die Integration in Visual Studio App Center überwachen und analysieren.

Funktionsweise von Application Insights

Sie installieren ein kleines Instrumentierungspaket (SDK) in Ihrer Anwendung oder aktivieren Application Insights mithilfe des Application Insights-Agents (sofern unterstützt). Die Instrumentierung überwacht Ihre App und leitet die Telemetriedaten an eine Azure Application

Insights-Ressource weiter. Dabei wird eine eindeutige GUID (ein sogenannter Instrumentierungsschlüssel) verwendet.

Sie können nicht nur die Webdienstanwendung instrumentieren, sondern auch Hintergrundkomponenten und den JavaScript-Code in den Webseiten selbst. Die Anwendung und die zugehörigen Komponenten können überall ausgeführt und müssen nicht in Azure gehostet werden.

Die folgenden Artikel enthalten weitere Informationen zum Thema:

Was ist Application Insights?

AJAX Collection in Application Insights

2.Sie haben ein Azure-Abonnement, das die in der folgenden Tabelle aufgeführten Speicherkonten enthält:

Name	Enthält
speichercb1	Einen Blob-Dienst und einen Tabellenspeicherdienst
speichercb2	Einen Blob-Dienst und einen Dateidienst
speichercb3	Einen Warteschlangendienst
speichercb4	Einen Dateidienst und einen Warteschlangendienst
speichercb5	Einen Tabellenspeicherdienst

Sie aktivieren Storage Advanced Threat Protection (ATP) für alle Speicherkonten.

Sie müssen identifizieren, welche Speicherkonten ATP-Warnungen generieren.

Welche drei Speicherkonten generieren ATP-Warnungen?

(Jede korrekte Antwort stellt einen Teil der Lösung dar. Wählen Sie drei Antworten.)

A.speichercb1
B.speichercb2
C.speichercb3
D.speichercb4
E.speichercb5

Korrekte Antwort: A, B, D

Erläuterungen:

Advanced Threat Protection (ATP) für Azure Storage ermöglicht die Nutzung intelligenter Sicherheitsfunktionen zur Erkennung von ungewöhnlichen und möglicherweise schädlichen Versuchen, auf Speicherkonten zuzugreifen oder diese unbefugt zu nutzen. Mithilfe dieser Sicherheitsebene können Sie Ihre Systeme vor potenziellen Bedrohungen für Ihre Speicherkonten schützen und sofort auf diese reagieren, ohne ein Sicherheitsexperte sein zu müssen.

Azure Defender für Storage ist derzeit für Blob Storage, Azure Files und Azure Data Lake Storage Gen2 verfügbar. Zu den Kontotypen, die Azure Defender unterstützen, gehören Konten vom Typ "Allgemein v2" sowie Blockblob- und Blob Storage-Konten. Azure Defender für Storage ist in allen öffentlichen Clouds und Clouds der US-Regierungsbehörden verfügbar, nicht aber in anderen Sovereign Cloud- oder Azure Government-Cloudregionen.

Info: Advanced Threat Protection (ATP) for Azure Storage wurde in Azure Defender für Storage umbenannt.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Konfigurieren von Azure Defender für Storage

3.Sie haben in Microsoft Azure eine virtuelle Maschine mit dem Namen VM1 und einen Azure Active Directory-Mandanten (Azure AD) mit dem Namen it-pruefungen.de.

VM1 hat die folgenden Einstellungen:
IP-Adresse: 10.10.0.10
Vom System zugewiesene verwaltete Identität: Ein
Sie müssen ein Skript erstellen, das in VM1 ausgeführt wird, um das Authentifizierungstoken von VM1 abzurufen.

Welche Adresse sollten Sie im Skript verwenden?

A.vm1.it-pruefungen.de.onmicrosoft.com
B.169.254.169.254
C.10.10.0.10
D.vm1.it-pruefungen.de

Korrekte Antwort: B

Erläuterungen:

Die Verwaltung von Geheimnissen und Anmeldeinformationen für eine sichere Kommunikation zwischen verschiedenen Diensten stellt für Entwickler eine häufige Herausforderung dar.In Azure brauchen Entwickler dank verwalteter Identitäten keine Anmeldeinformationen mehr zu verwalten. Für die Azure-Ressource in Azure AD wird eine Identität bereitgestellt, mit der Azure Active Directory (Azure AD)-Token abgerufen werden.Das erleichtert auch den Zugriff auf Azure Key Vault. In diesem Schlüsseltresor können Entwickler Anmeldeinformationen auf sichere Art und Weise speichern.Verwaltete Identitäten für Azure-Ressourcen sorgen für eine Lösung des Problems, indem für Azure-Dienste eine automatisch verwaltete Identität in Azure AD bereitgestellt wird.

Es gibt zwei Arten von verwalteten Identitäten:

Systemseitig zugewiesen: Bei einigen Azure-Diensten können Sie eine verwaltete Identität direkt in einer Dienstinstanz aktivieren. Wenn Sie eine systemseitig zugewiesene verwaltete Identität aktivieren, wird in Azure AD eine Identität erstellt, die an den Lebenszyklus der jeweiligen Dienstinstanz gebunden ist. Daher löscht Azure automatisch die Identität, wenn die Ressource gelöscht wird. Entwurfsbedingt kann nur diese Azure-Ressource diese Identität zum Anfordern von Token von Azure AD verwenden.

Benutzerseitig zugewiesen: Sie können eine verwaltete Identität auch als eigenständige Azure-Ressource erstellen. Sie können eine benutzerseitig zugewiesene verwaltete Identität erstellen und diese einer oder mehreren Instanzen eines Azure-Diensts zuweisen. Bei benutzerseitig zugewiesenen verwalteten Identitäten wird die Identität getrennt von den Ressourcen verwaltet, für die sie verwendet wird.

Das folgende Beispiel zeigt, wie Sie mithilfe des Cmdlets „ Invoke-WebRequest “ eine Anforderung an den lokalen Endpunkt für die verwaltete Identität für Azure-Ressourcen, um ein Zugriffstoken für Azure Resource Manager zu erhalten.

$response = Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://management.azure.com/' -Method GET -Headers @{Metadata="true"}

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Abrufen eines Zugriffstokens mithilfe der systemseitig zugewiesenen verwalteten Identität eines virtuellen Computers und Verwenden dieses Zugriffstokens zum Aufrufen von Azure Resource Manager

4.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Das Unternehmen hat ein Azure-Abonnement, das einen Azure-Schlüsseltresor mit dem Namen KeyVault1 und die in der folgenden Tabelle aufgeführten virtuellen Maschinen enthält:

Name	Verbunden mit
VM1	VNet1\Subnetz1
VM2	VNet2\Subnetz2

KeyVault1 verfügt über eine Zugriffsrichtlinie, die mehreren Benutzern die Berechtigung zum Erstellen von Schlüsseln bietet.

Sie müssen sicherstellen, dass die Benutzer nur von VM1 aus Geheimnisse in KeyVault1 registrieren können.

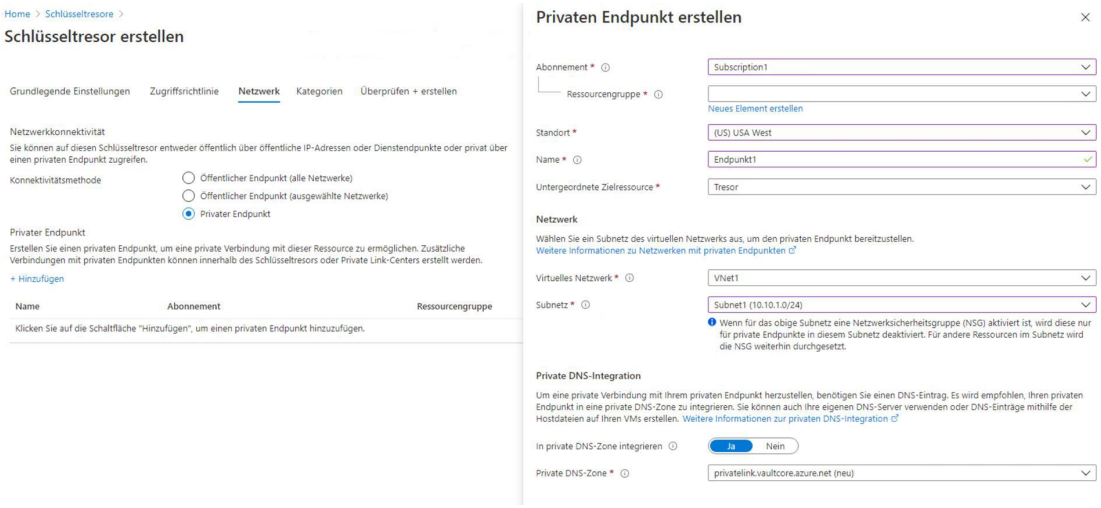
Wie gehen Sie vor?

A.Erstellen Sie eine Netzwerksicherheitsgruppe (NSG), die mit Subnetz1 verknüpft ist.
B.Konfigurieren Sie die Einstellungen für die Firewall und die virtuellen Netzwerke für KeyVault1.
C.Ändern Sie die Zugriffsrichtlinie für KeyVault1.
D.Konfigurieren Sie KeyVault1 für die Verwendung eines Hardware-Sicherheitsmoduls (HSM).

Korrekte Antwort: C

Erläuterungen:

Wir sollten die Zugriffsrichtlinie mit einem privaten Endpunkt konfigurieren und den Zugriff so auf VNet1\Subnetz1 beschränken.



Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Integrieren von Key Vault in Azure Private Link

5.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Sie erstellen die folgende Azure-Rollendefinition.

```
{
  "Name": "Rolle1",
  "Id": "80808080-8080-8080-8080-8080808080808",
  "IsCustom": false,
  "Description": "",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read" ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": []
}
```

Sie müssen Rolle1 mithilfe der Rollendefinition erstellen.

Welche zwei Werte sollten Sie ändern, bevor Sie Rolle1 erstellen?

(Jede korrekte Antwort stellt einen Teil der Lösung dar. Wählen Sie zwei Antworten.)

A.AssignableScopes
B.Description
C.DataActions
D.IsCustom
E.Id

Korrekte Antwort: A, D

Erläuterungen:

Wenn die integrierten Azure-Rollen die Anforderungen Ihrer Organisation nicht erfüllen, können Sie Ihre eigenen benutzerdefinierten Rollen erstellen. Genauso wie integrierte Rollen können auch benutzerdefinierte Rollen Benutzern, Gruppen und Dienstprinzipalen im Verwaltungsgruppen-, Abonnement- und Ressourcengruppenbereich zugewiesen werden. Benutzerdefinierte Rollen können von Abonnements, die demselben Azure AD-Verzeichnis vertrauen, gemeinsam genutzt werden. Es gilt ein Limit von 5.000 benutzerdefinierte Rollen pro Verzeichnis. (Für Azure

Deutschland und Azure China 21ViaNet beträgt das Limit 2.000 benutzerdefinierte Rollen.) Benutzerdefinierte Rollen können über das Azure-Portal, mit Azure PowerShell, über die Azure CLI oder mithilfe der REST-API erstellt werden.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

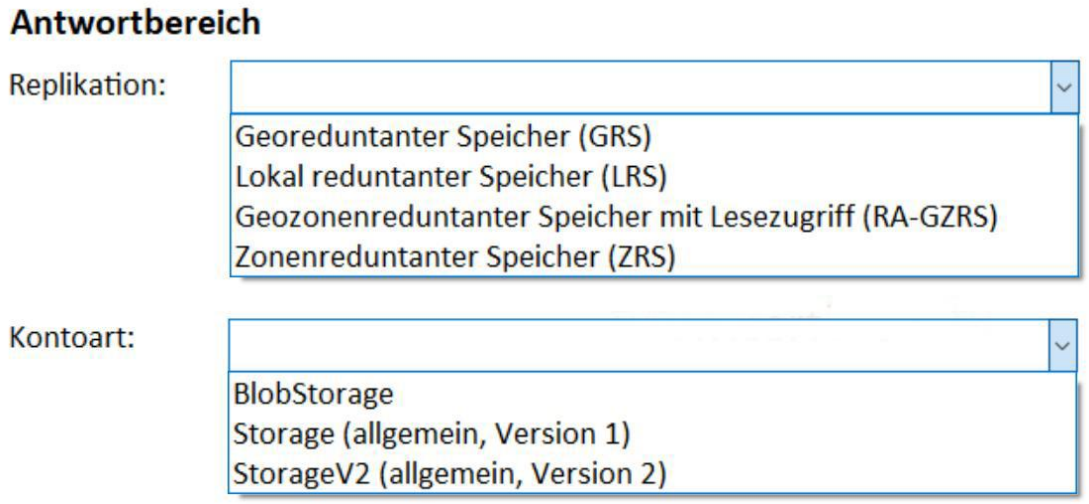
Benutzerdefinierte Azure-Rollen

6.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Sie planen, ein Azure Speicherkonto in der Azure Region USA, Osten 2 zu erstellen.

Sie müssen ein Speicherkonto erstellen, das die folgenden Anforderungen erfüllt:
Repliziert synchron.
Bleibt verfügbar, wenn ein einzelnes Rechenzentrum in der Region ausfällt.
Wie konfigurieren Sie das Speicherkonto?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung



A.Replikation: Lokal reduntanter Speicher (LRS)
Kontoart: BlobStorage
B.Replikation: Georeduntanter Speicher (GRS)
Kontoart: BlobStorage
C.Replikation: Geozonenreduntanter Speicher mit Lesezugriff (RA-GZRS)
Kontoart: Storage (allgemein, Version 1)
D.Replikation: Zonenreduntanter Speicher (ZRS)
Kontoart: Storage (allgemein, Version 1)
E.Replikation: Zonenreduntanter Speicher (ZRS)
Kontoart: StorageV2 (allgemein, Version 2)

F.Replikation: Georeduntanter Speicher (GRS)
Kontoart: StorageV2 (allgemein, Version 2)

Korrekte Antwort: E

Erläuterungen:

Azure Storage speichert immer mehrere Kopien Ihrer Daten, damit sie vor geplanten und ungeplanten Ereignissen geschützt sind – von vorübergehend auftretenden Hardwarefehlern und Netzwerk- oder Stromausfällen bis zu schweren Naturkatastrophen usw. Redundanz stellt sicher, dass Ihr Speicherkonto seine Ziele für Verfügbarkeit und Dauerhaftigkeit selbst bei Ausfällen erfüllt.

Daten in einem Azure Storage-Konto werden immer dreimal in der primären Region repliziert. Azure Storage bietet zwei Optionen für die Replikation Ihrer Daten in der primären Region:

Lokal redundanter Speicher (LRS): Die Daten werden synchron innerhalb eines einzelnen physischen Standorts in der primären Region kopiert. LRS ist die kostengünstigste Replikationsoption, wird jedoch nicht für Anwendungen empfohlen, die Hochverfügbarkeit erfordern.

Zonenredundanter Speicher (ZRS): Die Daten werden synchron über drei Azure-Verfügbarkeitszonen hinweg in der primären Region kopiert. Für Anwendungen, die Hochverfügbarkeit erfordern, empfiehlt Microsoft die Verwendung von ZRS in der primären Region und auch das Replizieren in eine sekundäre Region.

Für die Unterstützung von zonenreduntantem Speicher wird ein Speicherkonto vom Typ StorageV2 (allgemein, Version 2) benötigt.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:

Azure Storage-Redundanz

7.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Sie planen die Bereitstellung einer virtuellen Maschine mit dem Namen VM1 in Microsoft Azure. Für die Bereitstellung soll eine Azure Resource Manager (ARM)-Vorlage verwendet werden.

Sie müssen die Vorlage vervollständigen.

Was sollten Sie in die Vorlage aufnehmen?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

Antwortbereich

```
{
  "type": "Microsoft.Compute/virtualMachines",
  "apiVersion": "2019-07-01",
  "name": "VM1",
  "location": "[parameters('location')]",
  "dependsOn": [
    "resourceId('Microsoft.Storage/storagAccounts/', variables('Name3'))",
    "resourceId(                                    , variables('Name4'))]"
  ],
{
  "type": "Microsoft.Network/networkInterfaces",
  "apiVersion": "2019-07-01",
  "name": "NIC1",
  "location": "[parameters('location')]",
  "dependsOn": [
    "resourceId('Microsoft.Network/publicIPAddresses/', variables('Name1'))",
    "resourceId(                                    , variables('Name2'))]"
  ],
```

P1

'Microsoft.Network/publicIPAddresses/'
'Microsoft.Network/virtualNetworks/'
'Microsoft.Network/networkInterfaces/'
'Microsoft.Network/virtualNetworks/subnets'
'Microsoft.Storage/storageAccounts/'

P2

'Microsoft.Network/publicIPAddresses/'
'Microsoft.Network/virtualNetworks/'
'Microsoft.Network/networkInterfaces/'
'Microsoft.Network/virtualNetworks/subnets'
'Microsoft.Storage/storageAccounts/'

A.P1: 'Microsoft.Network/publicIPAddresses/'
P2: 'Microsoft.Storage/storageAccounts/'
B.P1: 'Microsoft.Storage/storageAccounts/'
P2: 'Microsoft.Network/virtualNetworks/'
C.P1: "Microsoft.Storage/storageAccounts/'
P2: 'Microsoft.Network/networkInterfaces/'
D.P1: 'Microsoft.Network/virtualNetworks/'
P2: 'Microsoft.Network/virtualNetworks/subnets'
E.P1: 'Microsoft.Network/virtualNetworks/'
P2: 'Microsoft.Network/publicIPAddresses/'
F.P1: 'Microsoft.Network/networkInterfaces/'
P2: 'Microsoft.Network/virtualNetworks/'

Korrekte Antwort: F

Erläuterungen:

Innerhalb Ihrer Vorlage bietet das „dependsOn“-Element die Möglichkeit, eine Ressource als von einer oder mehreren Ressourcen abhängig zu definieren. Sein Wert ist ein JSON-Array von Zeichenfolgen, die jeweils einen Ressourcennamen oder eine ID darstellen.

Resource Manager wertet die Abhängigkeiten zwischen den Ressourcen aus und stellt sie in der Reihenfolge ihrer Abhängigkeiten bereit. Wenn Ressourcen nicht voneinander abhängig sind, stellt Resource Manager sie parallel bereit. Sie müssen nur Abhängigkeiten für Ressourcen definieren, die in der gleichen Vorlage bereitgestellt werden.

ie erste in der Vorlage definierte Ressource ist eine virtuelle Maschine. Diese hängt von den folgenden zwei anderen Ressourcen ab:

Microsoft.Storage/storageAccounts
Microsoft.Network/networkInterfaces

Sie können die virtuelle Maschine erst erstellen, wenn das Speicherkonto und die Netzwerkschnittstelle vorhanden sind.

Die zweite in der Vorlage definierte Ressource ist eine Netzwerkschnittstelle. Sie hängt von den folgenden zwei anderen Ressourcen ab:

Microsoft.Network/publicIPAddresses
Microsoft.Network/virtualNetworks

Die folgenden Technet-Artikel enthalten weitere Informationen zum Thema:

Definieren der Reihenfolge für die Bereitstellung von Ressourcen in ARM-Vorlagen

Tutorial: Erstellen von ARM-Vorlagen mit abhängigen Ressourcen