Prüfungsnummer:AZ-100

Prüfungsname: Microsoft Azure Infrastructure and Deployment

Version:demo

https://www.it-pruefungen.ch/

Achtung: Aktuelle englische Version zu AZ-100 bei uns ist gratis!!

1.Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Sie möchten die Bereitstellung einer Skalierungsgruppe für virtuelle Maschinen (VMs) automatisieren. Die bereitgestellten VMs werden das Windows Server 2016-Datacenter Image verwenden.
Sie müssen sicherstellen, dass bei der Bereitstellung der Skalierungsgruppe für virtuelle Maschinen Webserver-Komponenten installiert werden.
Welche zwei Schritte führen Sie aus?
(Jede richtige Antwort stellt einen Teil der Lösung dar. Sie erhalten für jede richtige Auswahl einen Punkt.)

A.Ändern Sie den Abschnitt extensionProfile der Azure Resource Manager-Vorlage.
B.Erstellen Sie im Azure-Portal eine neue Skalierungsgruppe für virtuelle Maschinen.
C.Erstellen Sie eine Azure-Richtlinie.
D.Erstellen Sie ein Azure Automation-Konto.
E.Laden Sie ein Konfigurationsskript hoch.

Korrekte Antwort: A, E

Erläuterungen:
VM-Skalierungsgruppen können mit dem Erweiterungshandler Azure-Konfiguration des gewünschten Zustands verwendet werden. VM-Skalierungsgruppen bieten eine Möglichkeit, eine große Anzahl von virtuellen Computern bereitzustellen und zu verwalten, und lassen sich je nach Auslastung elastisch hoch- und herunterskalieren. DSC dient zum Konfigurieren der VMs, sobald sie online geschaltet wurden, damit sie in der Produktionssoftware ausgeführt werden.
Die zugrunde liegende Vorlagenstruktur für eine VM-Skalierungsgruppe unterscheidet sich geringfügig von einem einzelnen virtuellen Computer. Ein Punkt ist, dass bei einer einzelnen VM Erweiterungen unter dem Knoten „virtualMachines“ bereitgestellt werden. Es gibt einen Eintrag des Typs „Extensions“. Hier wird DSC der Vorlage hinzugefügt.

Ein Knoten einer VM-Skalierungsgruppe weist den Abschnitt „properties“ mit dem Attribut „VirtualMachineProfile“, „extensionProfile“ auf. DSC wird unter „extensions“ hinzugefügt.

```
"extensionProfile": {
        "extensions": [
            {
                "name": "Microsoft.Powershell.DSC",
                "properties": {
                    "publisher": "Microsoft.Powershell",
                    "type": "DSC",
```

```
                    "typeHandlerVersion": "2.20",
                    "autoUpgradeMinorVersion": false,
                    "forceUpdateTag":
"[parameters('DscExtensionUpdateTagVersion')]",
                    "settings": {
                        "configuration": {
                            "url": "[concat(parameters('_artifactsLocation'), '/',
variables('DscExtensionArchiveFolder'), '/', variables('DscExtensionArchiveFileName'))]",
                            "script": "DscExtension.ps1",
                            "function": "Main"
                        },
                        "configurationArguments": {
                            "nodeName": "localhost"
                        }
                    },
                    "protectedSettings": {
                        "configurationUrlSasToken":
"[parameters('_artifactsLocationSasToken')]"
                    }
                }
            }
        ]
```

Das Verhalten bei einer VM-Skalierungsgruppe entspricht dem Verhalten bei einem einzelnen virtuellen Computer. Beim Erstellen ein neues virtuellen Computers wird er automatisch mit der DSC-Erweiterung bereitgestellt. Wenn eine neuere Version des WMF von der Erweiterung angefordert wird, wird die VM neu gestartet, ehe sie online geschaltet wird. Sobald sie online ist, lädt sie die ZIP-Datei mit der DSC-Konfiguration herunter und stellt sie auf dem virtuellen Computer bereit.
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Verwenden von VM-Skalierungsgruppen mit der Azure DSC-Erweiterung

2.Sie haben ein Azure-Abonnement, das eine virtuelle Maschine mit dem Namen VM1 enthält. VM1 hostet eine Branchenanwendung, die rund um die Uhr verfügbar ist.
VM1 verfügt über eine Netzwerkschnittstelle und eine verwaltete Festplatte. VM1 verwendet die Größe D4s_v3.
Sie möchten die folgenden Änderungen an VM1 vornehmen:
Ändern der Größe in D8s_v3.
Hinzufügen einer verwalteten Festplatte mit 500 GB Kapazität.
Hinzufügen der Erweiterung Puppet Agent.
Hinzufügen einer zusätzlichen Netzwerkschnittstelle.
Welche Änderung führt zu Ausfallzeiten für VM1?

A.Das Hinzufügen der verwalteten 500 GB Festplatte.
B.Das Anschließen der zusätzlichen Netzwerkschnittstelle.
C.Das Hinzufügen der Puppet Agent-Erweiterung.
D.Das Ändern der Größe in D8s_v3.

Korrekte Antwort: D

Erläuterungen:
Einer der großen Vorteile von Azure-VMs ist die Möglichkeit, die Dienstebene Ihrer VM entsprechend den Anforderungen an die CPU-, Netzwerk- oder Festplattenleistung zu ändern.
Wenn eine VM ausgeführt wird, wird sie auf einem physischen Server bereitgestellt. Die physischen Server in Azure-Regionen sind in Clustern gebräuchlicher physischer Hardware zusammengefasst. Eine laufende VM kann problemlos auf jede VM-Größe angepasst werden, die vom aktuellen Hardware-Cluster unterstützt wird, der die VM unterstützt.
Wenn Sie die Größenänderungsaktion auswählen, werden die verfügbaren VM-Größen angezeigt, zu denen die VM geändert werden kann.
Wenn das Resource Manager (ARM)-Bereitstellungsmodell verwendet wurde, kann die Größe der VMs geändert werden, wenn sich die VM und alle anderen VMs im selben Verfügbarkeitssatz in einem angehaltenen Zustand befinden (deallocated).
Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Resize virtual machines

3.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Sie haben ein Azure-Abonnement, das die in der folgenden Tabelle gezeigten Ressourcen enthält.

Name	Typ
ASG1	Anwendungssicherheitsgruppe
NSG1	Netzwerksicherheitsgruppe
Subnet1	Subnetz
VNet1	Virtuelles Netzwerk
NIC1	Netzwerkschnittstelle
VM1	Virtuelle Maschine

Subnet1 ist mit VNet1 verbunden. NIC1 verbindet VM1 mit Subnet1.
Sie müssen ASG1 auf VM1 anwenden.
Wie gehen Sie vor?

A.Ändern Sie die Eigenschaften von NSG1.
B.Ändern Sie die Eigenschaften von ASG1.
C.Verknüpfen Sie NIC1 zu ASG1.
D.Verknüpfen Sie NSG1 mit VM1.

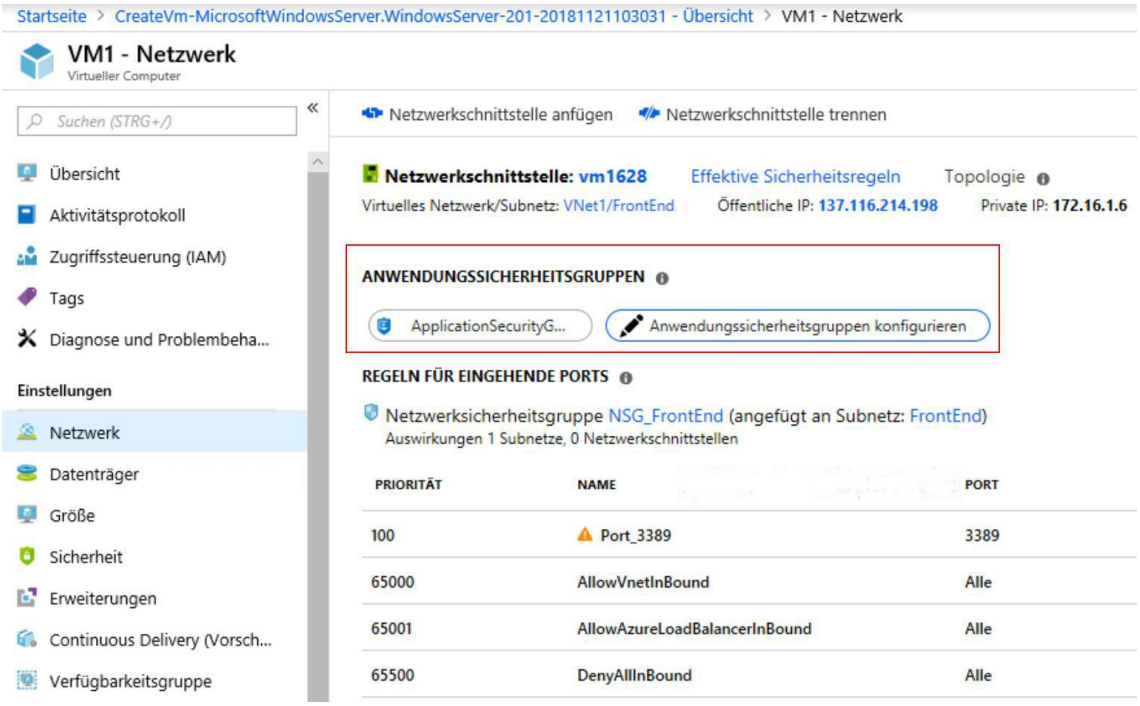
Korrekte Antwort: C

Erläuterungen:
Mithilfe von ASGs können Sie differenzierte Netzwerksicherheitsrichtlinien auf der Grundlage von Workloads definieren, die zentral für Anwendungen anstelle von expliziten IP-Adressen festgelegt werden. ASGs bieten die Möglichkeit, VMs mit Monikern und sicheren Anwendungen zu gruppieren, indem der Verkehr aus vertrauenswürdigen Segmenten Ihres Netzwerks gefiltert wird.

Durch die Implementierung differenzierter Sicherheitsverkehrskontrollen wird die Isolation von Workloads verbessert und einzeln geschützt. Wenn ein Verstoß auftritt, begrenzt diese Technik die möglichen Auswirkungen auf Ihre Netzwerke durch Hacker.

Mit ASGs wird das Filtern von Verkehr basierend auf Anwendungsmustern mit den folgenden Schritten vereinfacht:

Definieren Sie Ihre Anwendungsgruppen und geben Sie einen beschreibenden Moniker-Namen an, der zu Ihrer Architektur passt. Sie können es für Anwendungen, Workload-Typen, Systeme, Ebenen, Umgebungen oder beliebige Rollen verwenden.
Definieren Sie eine einzelne Sammlung von Regeln mit ASGs und Network Security Groups (NSG). Sie können eine einzelne NSG auf Ihr gesamtes virtuelles Netzwerk in allen Subnetzen anwenden. Eine einzelne NSG bietet Ihnen vollständige Transparenz Ihrer Richtlinien und eine zentrale Stelle für die Verwaltung.
Skalieren Sie in Ihrem eigenen Tempo. Wenn Sie VMs bereitstellen, fügen Sie sie zu den entsprechenden ASGs hinzu. Wenn Ihre VM mehrere Workloads ausführt, weisen Sie einfach mehrere ASGs zu. Der Zugriff wird basierend auf Ihren Workloads gewährt. Sie müssen sich nicht mehr um die Sicherheitsdefinition kümmern. Noch wichtiger ist jedoch, dass Sie ein Zero-Trust-Modell implementieren können, das den Zugriff auf die explizit zulässigen Anwendungsflüsse einschränkt.
Anwendungssicherheitsgruppen werden der Netzwerkschnittstelle der VM zugewiesen:



4.Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Sie haben zwei Abonnements mit den Namen Abonnement1 und Abonnement2. Jedes Abonnement ist einem anderen Azure AD-Mandanten zugeordnet.
Abonnement1 enthält ein virtuelles Netzwerk mit dem Namen VNet1. VNet1 enthält eine Azure virtuelle Maschine mit dem Namen VM1 und verwendet den IP-Adressraum 10.0.0.0/16.
Das Abonnement2 enthält ein virtuelles Netzwerk mit dem Namen VNet2. VNet2 enthält eine Azure virtuelle Maschine mit dem Namen VM2 und verwendet den IP-Adressraum 10.10.0.0/24.
Sie müssen VNet1 mit VNet2 verbinden.
Welchen Schritt führen Sie als erstes aus?

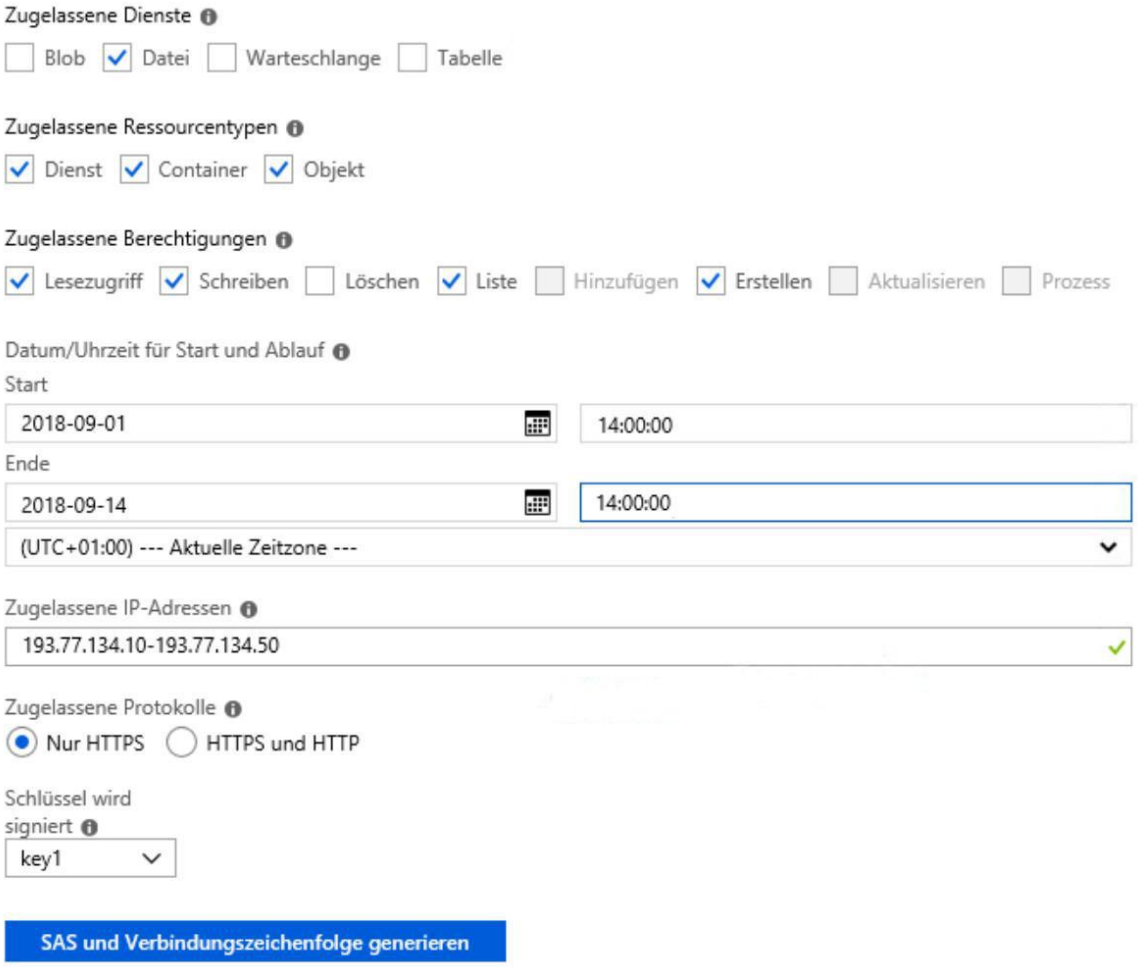
A.Verschieben Sie VNet1 in Abonnement2.
B.Ändern Sie den IP-Adressraum von VNet2.
C.Stellen Sie virtuelle Netzwerkgateways bereit.
D.Verschieben Sie VM1 in Abonnement2.

Korrekte Antwort: C

Erläuterungen:
Wir können die beiden virtuellen Netzwerke über ein VNet-to-VNet-VPN verbinden.
Die virtuellen Netzwerke können sich in derselben oder in unterschiedlichen Regionen befinden und aus denselben oder verschiedenen Abonnements stammen. Beim Verbinden von VNets aus verschiedenen Abonnements müssen die Abonnements nicht demselben Active Directory-Mandanten zugeordnet werden.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Konfigurieren einer VNET-zu-VNET-VPN-Gatewayverbindung über das Azure-Portal

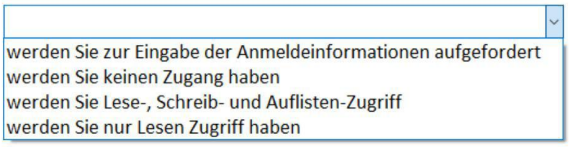
5.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Sie haben ein Azure-Abonnement mit dem Namen Abonnement1. Sie erstellen eine Azure-Dateifreigabe mit dem Namen Freigabe1.
Sie erstellen eine Shared Access Signature (SAS) mit dem Namen SAS1. Die Einstellungen der SAS werden nachstehend gezeigt:



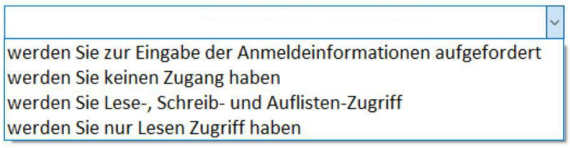
Welche Aussagen treffen zu?
(In der Abbildung werden Auswahlmöglichkeiten gezeigt. Klicken Sie auf die Schaltfläche Zeichnung und vervollständigen Sie die Aussagen so, dass sie zutreffend sind.)
Abbildung

Antwortbereich

Wenn Sie am 2. September 2018 Microsoft Azure Storage Explorer auf einem Computer mit der IP-Adresse 193.77.134.1 ausführen und SAS1 verwenden, um eine Verbindung zum Speicherkonto herzustellen, [Antwortauswahl 1].



Wenn Sie am 10. September 2008 den Befehl net use auf einem Computer mit der IP-Adresse 193.77.134.50 ausführen und SAS1 als Kennwort für die Verbindung mit Freigabe1 verwenden, [Antwortauswahl 1].



A.Antwortauswahl 1: werden Sie keinen Zugang haben
Antwortauswahl 2: werden Sie Lese-, Schreib- und Auflisten-Zugriff
B.Antwortauswahl 1: werden Sie zur Eingabe der Anmeldeinformationen aufgefordert
Antwortauswahl 2: werden Sie keinen Zugang haben
C.Antwortauswahl 1: werden Sie keinen Zugang haben
Antwortauswahl 2: werden Sie nur Lesen Zugriff haben
D.Antwortauswahl 1: werden Sie nur Lesen Zugriff haben
Antwortauswahl 2: werden Sie zur Eingabe der Anmeldeinformationen aufgefordert
E.Antwortauswahl 1: werden Sie Lese-, Schreib- und Auflisten-Zugriff
Antwortauswahl 2: werden Sie Lese-, Schreib- und Auflisten-Zugriff
F.Antwortauswahl 1: werden Sie keinen Zugang haben
Antwortauswahl 2: werden Sie keinen Zugang haben

Korrekte Antwort: F

Erläuterungen:
Die IP-Adresse des verwendeten Computers in Aussage1 ist nicht Teil der zulässigen IP-Adressen der SAS. Unter Verwendung der SAS ist mit dem Azure Storage Explorer von dieser IP-Adresse aus, kein Zugriffmöglich.

Die IP-Adresse des Computers in Aussage2 ist Teil der zulässigen IP-Adressen der SAS. Für das Einbinden der Azure-Dateifreigabe in den Datei-Explorer, ist zu diesem Zeitpunkt (10.09.2018) jedoch entweder der primäre oder der sekundäre Schlüssel des Speicherkontos erforderlich. SAS-Schlüssel können zu diesem Zeitpunkt (noch) nicht für den ZUgriff auf die Dateifreigabe genutzt werden.

Voraussetzungen für das Einbinden einer Azure-Dateifreigabe in den Datei-Explorer

Name des Speicherkontos: Zum Einbinden einer Azure-Dateifreigabe benötigen Sie den Namen des Speicherkontos.

Speicherkontoschlüssel: Zum Einbinden einer Azure-Dateifreigabe benötigen Sie den primären (oder sekundären) Speicherschlüssel. SAS-Schlüssel können derzeit nicht zum Einbinden verwendet werden.

Stellen Sie sicher, dass Port 445 geöffnet ist: Das SMB-Protokoll erfordert dass TCP-Port 445 geöffnet ist. Wenn Port 445 gesperrt ist, sind keine Verbindungen möglich. Mithilfe des Cmdlets Test-NetConnection können Sie überprüfen, ob Ihre Firewall Port 445 blockiert. Denken Sie daran, your-storage-account-name durch den entsprechenden Namen für Ihr Speicherkonto zu ersetzen.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Verwenden einer Azure-Dateifreigabe mit Windows