AZ-101$^{Q\&As}$

Microsoft Azure Integration and Security

Pass Microsoft AZ-101 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-101.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have an Azure subscription named Subscription1 and two Azure Active Directory (Azure AD) tenants named Tenant1 and Tenant2.

Subscription1 is associated to Tenant1. Multi-factor authentication (MFA) is enabled for all the users in Tenant1.

You need to enable MFA for the users in Tenant2. The solution must maintain MFA for Tenant1.

What should you do first?

A. Transfer the administration of Subscription1 to a global administrator of Tenant2

B. Configure the MFA Server setting in Tenant1.

C. Create and link a subscription to Tenant2.

D. Change the directory for Subscription1.

Correct Answer: C

QUESTION 2

You have an Azure subscription.

Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by

using site-to-site VPNs.

You have a line-of-business app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016.

You need to ensure that the connections to App1 are spread across all the virtual machines.

What are two possible Azure services that you can use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a public load balancer

B. Traffic Manager

C. an Azure Content Delivery Network (CDN)

D. an internal load balancer

E. an Azure Application Gateway

Correct Answer: DE

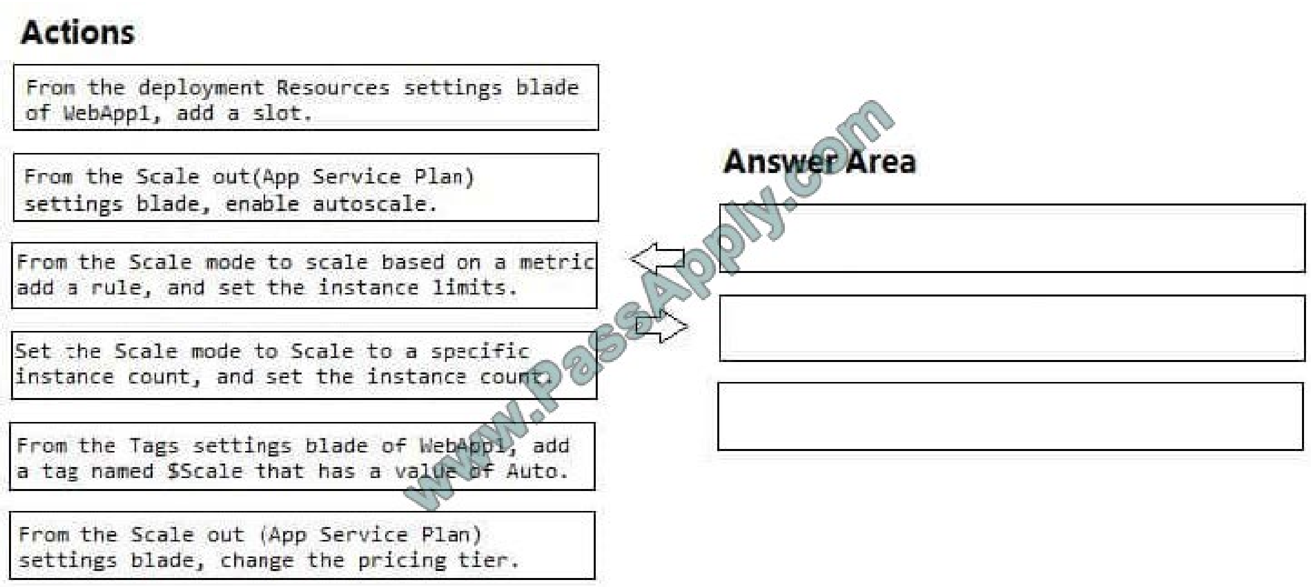
QUESTION 3

You are developing an Azure web app named WebApp1. WebApp1 uses an Azure App Service plan named Plan1 that uses the B1 pricing tier.

You need to configure WebApp1 to add additional instances of the app when CPU usage exceeds 70 percent for 10 minutes.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

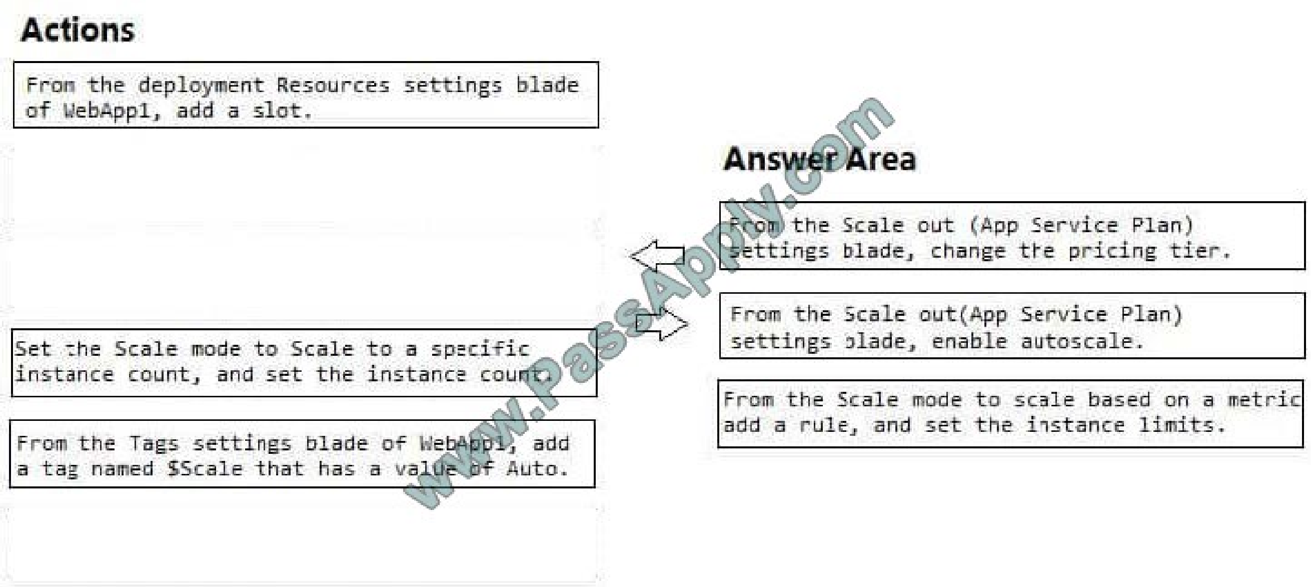


Actions

- From the deployment Resources settings blade of WebApp1, add a slot.
- From the Scale out(App Service Plan) settings blade, enable autoscale.
- From the Scale mode to scale based on a metric add a rule, and set the instance limits.
- Set the Scale mode to Scale to a specific instance count, and set the instance count.
- From the Tags settings blade of WebApp1, add a tag named $Scale that has a value of Auto.
- From the Scale out (App Service Plan) settings blade, change the pricing tier.

Answer Area

Correct Answer:



Actions

- From the deployment Resources settings blade of WebApp1, add a slot.
- Set the Scale mode to Scale to a specific instance count, and set the instance count.
- From the Tags settings blade of WebApp1, add a tag named $Scale that has a value of Auto.

Answer Area

1. From the Scale out (App Service Plan) settings blade, change the pricing tier.
2. From the Scale out(App Service Plan) settings blade, enable autoscale.
3. From the Scale mode to scale based on a metric add a rule, and set the instance limits.

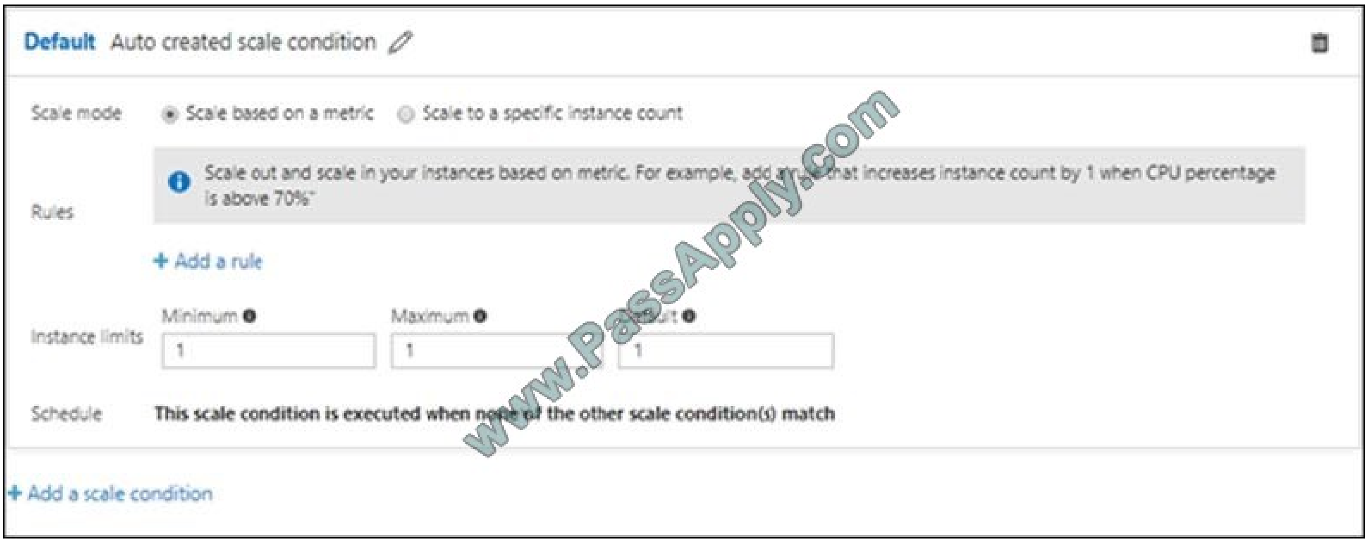
Box 1: From the Scale out (App Service Plan) settings blade, change the pricing tier The B1 pricing tier only allows for 1 core. We must choose another pricing tier. Box 2: From the Scale out (App Service Plan) settings blade, enable autoscale

1. Log in to the Azure portal at http://portal.azure.com

2. Navigate to the App Service you would like to autoscale.

3. Select Scale out (App Service plan) from the menu

4. Click on Enable autoscale. This activates the editor for scaling rules.



Default Auto created scale condition

Scale mode ● Scale based on a metric ○ Scale to a specific instance count

Rules: Scale out and scale in your instances based on metric. For example, add a rule that increases instance count by 1 when CPU percentage is above 70%"

+ Add a rule

Instance limits: Minimum 1, Maximum 1, Default 1

Schedule: This scale condition is executed when none of the other scale condition(s) match

+ Add a scale condition

Box 3: From the Scale mode to Scale based on metric, add a rule, and set the instance limits.

Click on Add a rule. This shows a form where you can create a rule and specify details of the scaling.

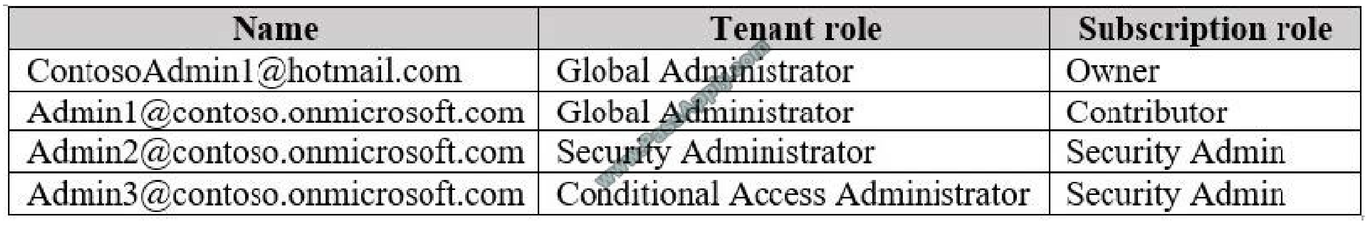
References:

https://azure.microsoft.com/en-us/pricing/details/app-service/windows/

https://blogs.msdn.microsoft.com/hsirtl/2017/07/03/autoscaling-azure-web-apps/

QUESTION 4

You create an Azure subscription named Subscription1 and an associated Azure Active Directory (Azure AD) tenant named Tenant1. Tenant1 contains the users in the following table.



Name	Tenant role	Subscription role
ContosoAdmin1@hotmail.com	Global Administrator	Owner
Admin1@contoso.onmicrosoft.com	Global Administrator	Contributor
Admin2@contoso.onmicrosoft.com	Security Administrator	Security Admin
Admin3@contoso.onmicrosoft.com	Conditional Access Administrator	Security Admin

You need to add an Azure AD Privileged Identity Management application to Tenant1. Which account can you use?

A. Admin3@contoso.onmicrosoft.com

B. Admin1@contoso.onmicrosoft.com

C. Admin2@contoso.onmicrosoft.com

D. ContosoAdmin1@hotmail.com

Correct Answer: B

References: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

QUESTION 5

You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com.

From the Azure Active Directory blade, you assign the Conditional Access Administrator role to a user named Admin1.

You need to ensure that Admin1 has just-in-time access as a conditional access administrator.

What should you do next?

A. Enable Azure AD Multi-Factor Authentication (MFA).

B. Set Admin1 as Eligible for the Privileged Role Administrator role.

C. Set Admin1 as Eligible for the Conditional Access Administrator role.

D. Enable Azure AD Identity Protection.

Correct Answer: A

Require MFA for admins is a baseline policy that requires MFA for the following directory roles: Global administrator

SharePoint administrator

Exchange administrator

Conditional access administrator

Security administrator

References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/baseline-protection

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

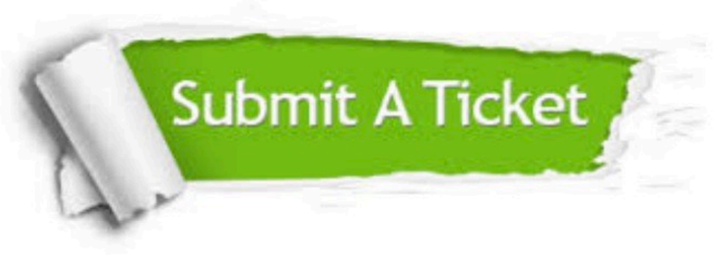
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.passapply.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.