AZ-700 Q&As

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

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

https://www.pass4itsure.com/az-700.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure Firewall.

Does this meet the requirement?

A. Yes

B. No

Correct Answer: A

Explanation:

Correct Solution: You implement Azure Firewall.

What is a secured virtual hub?

A virtual hub is a Microsoft-managed virtual network that enables connectivity from other resources. When a virtual hub is created from a Virtual WAN in the Azure portal, a virtual hub VNet and gateways (optional) are created as its

components.

A secured virtual hub is an Azure Virtual WAN Hub with associated security and routing policies configured by Azure Firewall Manager.

Create a secured virtual hub

Using Firewall Manager in the Azure portal, you can either create a new secured virtual hub, or convert an existing virtual hub that you previously created using Azure Virtual WAN.

Reference:

https://learn.microsoft.com/en-us/azure/firewall-manager/secured-virtual-hub

QUESTION 2

You have an Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159ylhjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


You need to ensure that the URL is accessible through the application gateway.

Solution: You add a rewrite rule for the host header.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

https://docs.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url#limitations

QUESTION 3

You need to configure VNET1 to log all events and metrics. The solution must ensure that you can query the events and metrics directly from the Azure portal by using KQL.

To complete this task, sign in to the Azure portal.

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

Plan

Stage 1: Determine the resource group of VNET1

Stage 2: In Azure Monitor set up monitoring with the VNET\\'s Resource Group as source, and Log Analytics workspace as destination

Stage 1: Determine the resource group of VNET1

Step 1: In Azure portal locate VNET1 and detect which resource group it is in (here we use XGroup).

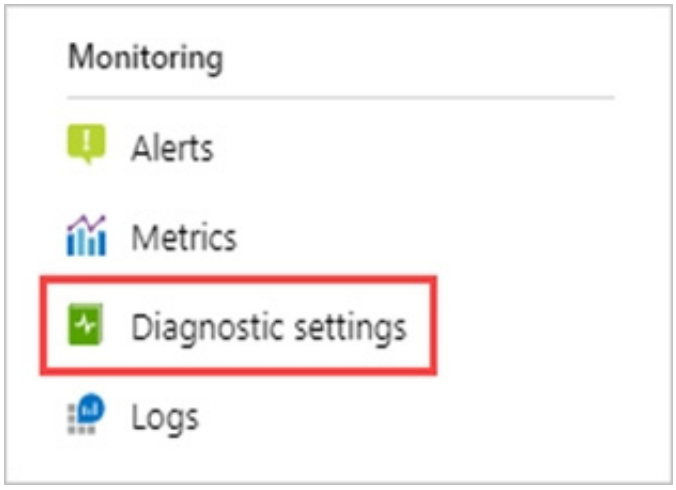
Stage 2: In Azure Monitor set up monitoring with the VNET\\'s Resource Group as source, and Log Analytics workspace as destination

Create diagnostic settings

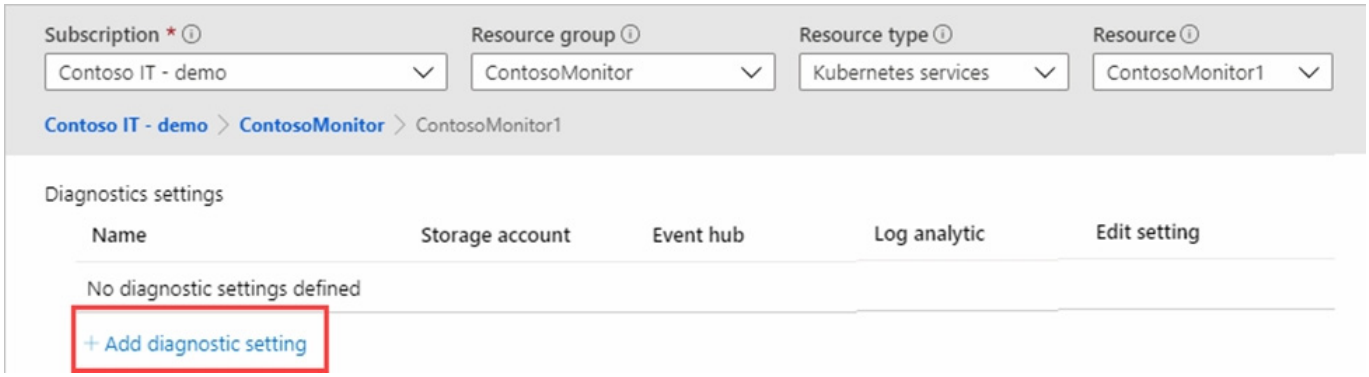
Step 2: You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource (XGroup in our case).

Where you configure diagnostic settings in the Azure portal depends on the resource:

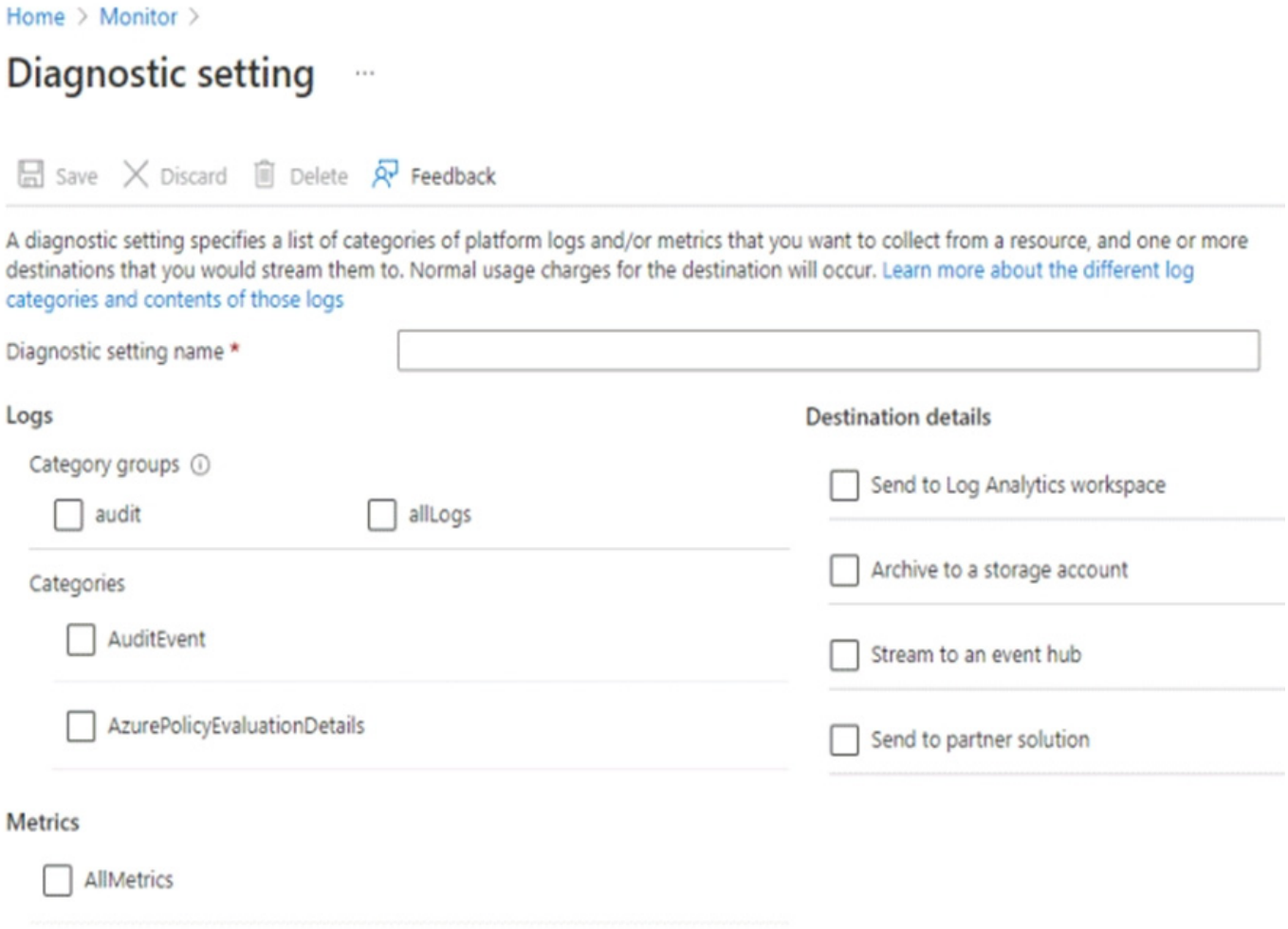
For a single resource, select Diagnostic settings under Monitoring on the resource\\'s menu.



Step 3: If no settings exist on the resource you\\'ve selected, you\\'re prompted to create a setting. Select Add diagnostic setting.



Step 4: Give your setting a name if it doesn\\'t already have one.



Step 5: Logs and metrics to route: For logs, either choose a category group or select the individual checkboxes for each category of data you want to send to the destinations specified later. The list of categories varies for each Azure service.

Select AllMetrics if you want to store metrics in Azure Monitor Logs too.

We do the following:

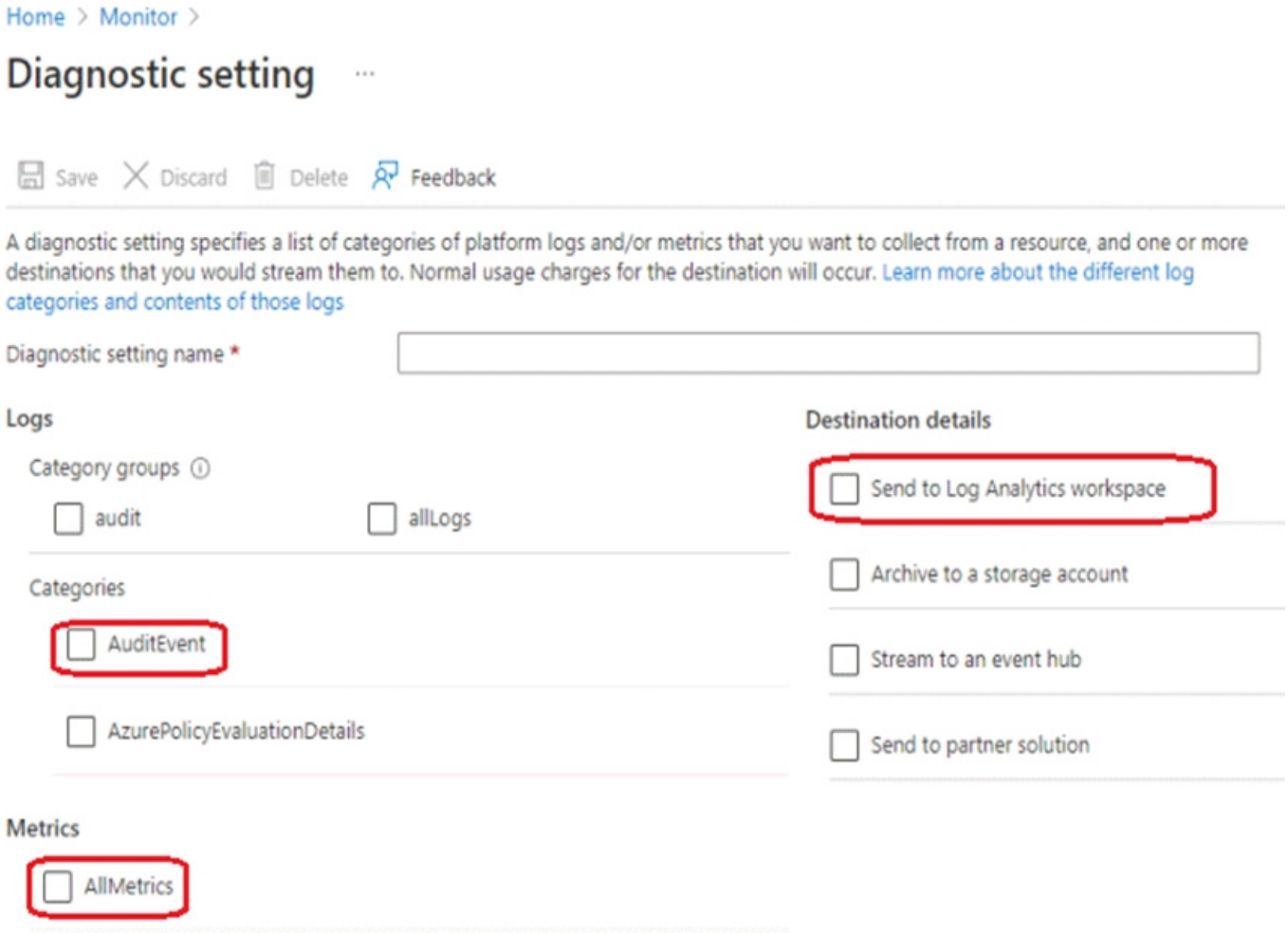
Categories: Select AuditEvent

Metrics: Select AllMetrics

(to log all events and metrics)

Destination details: Select Send to Log Analytics workspace

(To be able to query using KQL)



Step 6: Destination details -skip

Step 7: Select Save.

Note: Azure virtual network collects the same kinds of monitoring data as other Azure resources.

Azure virtual network uses Azure Monitor.

Collection and routing

Platform metrics and the Activity log are collected and stored automatically, but can be routed to other locations by using a diagnostic setting.

Each Azure resource requires its own diagnostic setting, which defines the following criteria:

Sources: The type of metric and log data to send to the destinations defined in the setting. The available types vary by resource type.

Destinations: One or more destinations to send to.

Destinations

Platform logs and metrics can be sent to the destinations listed in the following table.

*

Log Analytics workspace Metrics are converted to log form. This option might not be available for all resource types. Sending them to the Azure Monitor Logs store (which is searchable via Log Analytics) helps you to integrate them into queries, alerts, and visualizations with existing log data.

*

Etc.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings
https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network

QUESTION 4

HOTSPOT

You have an Azure subscription that contain a storage account named st1 in the East US Azure region.

You have the virtual networks shown in the following table.

Name	Location	IP address space
Vnet1	UK West	10.1.0.0/16
Vnet2	East US	10.2.0.0/16
Vnet3	West US	10.3.0.0/16

You have the subnets shown in the following table.

Name	Virtual network	IP address range	Subnet resources
Subnet1-1	Vnet1	10.1.1.0/24	Five virtual machines that each has one private IP address
Subnet2-1	Vnet2	10.2.1.0/25	Five virtual machines that each has one private IP address
Subnet3-1	Vnet3	10.3.1.0/26	Five virtual machines that each has one private IP address

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	○	○
You can deploy 100 additional virtual machines to Subnet2-1.	○	○
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	○	○
You can deploy 100 additional virtual machines to Subnet2-1.	○	○
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	○	○

Explanation:

Box 1: No

Azure Bastion subnet

You must create this subnet in the same virtual network that you want to deploy Azure Bastion to. The subnet must have the following configuration: Subnet name must be AzureBastionSubnet. Subnet size must be /26 or larger (/25, /24 etc.).

The subnet can\\'t contain other resources.

Box 2: Yes

Subnet-1 has IP address range 10.2.1.0/25

Total Number of Hosts: 128

Number of Usable Hosts: 126

Box 3: No

Subnet3-1 has an IP address range of 10.3.1.0/26.

Vnet3 has an IP address space of 10.3.0.0/16.

10.3.1.0/6 would not be within the Vnet3 IP address range.

Reference:

https://learn.microsoft.com/en-us/azure/bastion/configuration-settings

https://www.calculator.net/ip-subnet-calculator.html

QUESTION 5

You have the Azure virtual networks shown in the following table.

Name	Resource group	Location
Vnet1	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

You have the Azure resources shown in the following table.

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
St1	Storage account	**Not applicable**	RG5	UK West

You need to check latency between the resources by using connection monitors in Azure Network Watcher.

What is the minimum number of connection monitors that you must create?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: B

As per MS guidelines *Region: Select a region for your connection monitor. You can select only the source VMs that are created in this region. Here you see only VMs or Virtual Machine Scale Sets that are bound to the region that you specified when you created the connection monitor. By default, VMs and Virtual Machine Scale Sets are grouped into the subscription that they belong to

* Destination can be anywhere as per this Destinations: You can monitor connectivity to an Azure VM, an on-premises machine, or any endpoint (a public IP, URL, or FQDN) by specifying it as a destination. In a single test group, you can add Azure VMs, on-premises machines, Office 365 URLs, Dynamics 365 URLs, and custom endpoints. https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal