



Reference Solution for microsoft.pass4sure.az-303.v2020-10- 19.by.lucy.30q.vce AZ-303

AZ-303

Score: 800/1000
Version: 1
Time Limit: 120 Minutes

Implement and Monitor an Azure Infrastructure

(12 questions)

Question 1

You have an Azure subscription that contains 10 virtual machines on a virtual network.

You need to create a graph visualization to display the traffic flow between the virtual machines.

What should you do from Azure Monitor?

- ☐ From Activity log, use quick insights.
- ☐ From Metrics, create a chart.
- ☒ From Logs, create a new query.
- ☐ From Workbooks, create a workbook.

Explanation:

Explanation:

Navigate to Azure Monitor and select Logs to begin querying the data

Reference:

<https://azure.microsoft.com/en-us/blog/analysis-of-network-connection-data-with-azure-monitor-for-virtual-machines/>

Question 2

You have an Azure App Service app.

You need to implement tracing for the app. The tracing information must include the following:

Usage trends

AJAX call responses

Page load speed by browser

Server and browser exceptions

What should you do?

- ☐ Configure IIS logging in Azure Log Analytics.
- ☐ Configure a connection monitor in Azure Network Watcher.
- ☐ Configure custom logs in Azure Log Analytics.
- ☒ Enable the Azure Application Insights site extension.

Explanation:

Explanation:

For web pages, Application Insights JavaScript SDK automatically collects AJAX calls as dependencies.

Note: Some of the things you can track or collect are:

What are the most popular webpages in your application, at what time of day and where is that traffic coming from?

Dependency rates or response times and failure rates to find out if there's an external service that's causing performance issues on your app, maybe a user is using a portal to get through to your application and there are response time issues going through there for instance.

Exceptions for both server and browser information, as well as page views and load performance from the end users' side.

Reference:

<https://azure.microsoft.com/en-us/blog/ajax-collection-in-application-insights/>

<https://blog.pragmaticworks.com/what-is-application-insights>

Question 3

You have an Azure subscription.

You have 100 Azure virtual machines.

You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.

Which blade should you use?

- ☐ Metrics
- ☐ Customer sights
- ☐ Monitor
- ☒ Advisor

Explanation:

Explanation:

Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

Reference:

<https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations>

Question 4

You have an Azure subscription that contains 100 virtual machines.

You have a set of Pester tests in PowerShell that validate the virtual machine environment.

You need to run the tests whenever there is an operating system update on the virtual machines. The solution must minimize implementation time and recurring costs.

Which three resources should you use to implement the tests? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☒ Azure Automation runbook
- ☒ an alert rule
- ☐ an Azure Monitor query
- ☐ a virtual machine that has network access to the 100 virtual machines
- ☒ an alert action group

Explanation:

Explanation:

AE: You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.

B: Alerts are one of the key features of Azure Monitor. They allow us to alert on actions within an Azure subscription

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook>

<https://techsnips.io/snips/how-to-create-and-test-azure-monitor-alerts/?page=13>

Question 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use Synchronization Rules Editor to create a synchronization rule.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

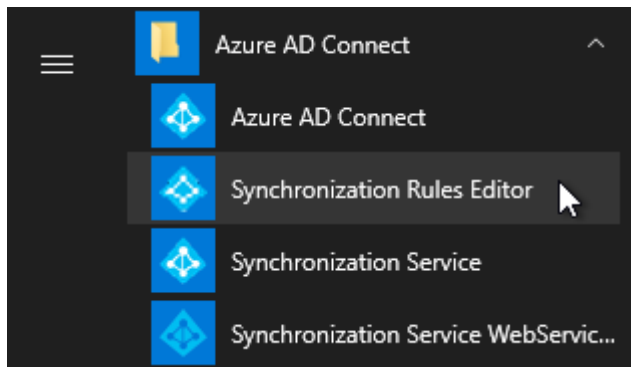
Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI or PowerShell.

Through GUI:

Using The Synchronization Rules Editor

1. Open the Synchronization Rules Editor on the server where Azure AD Connect is installed.



2. Click the Add new rule button on the View and manage your synchronization rules window.
3. Fill out the appropriate fields on the Description tab and click Next >.
4. On the Scoping filter tab, click Add group, then Add clause, add a userPrincipalName attribute filter, and click Next >.

Attribute: userPrincipalName

Operator: ENDSWITH

Value: Your internal UPN suffix prefixed with @ (e.g., @internal.acme.com). Users with this UPN suffix will NOT be synced with Office 365.

Create inbound synchronization rule

Create inbound synchronization rule

Description

Scoping filter

Join rules

Transformations

Add scoping filters, or click next to skip this step

Attribute	Operator	Value
userPrincipalName	ENDSWITH	@ [redacted]

< Add clause Remove clause(s) >

Add group Remove group(s)

< Previous Next > Add Cancel

Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

Question 6

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use Azure AD Connect to customize the synchronization options.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Instead use Synchronization Rules Editor to create a synchronization rule.

Note: Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI (Synchronization Rules Editor) or PowerShell.

Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

Question 7

You have a virtual network named VNet1 as shown in the exhibit. (Click the Exhibit tab.)

 Refresh
  Move
  Delete

Resource group (change) Production	Address space 10.2.0.0/16
Location West US	DNS servers Azure provided DNS service
Subscription (change) Production subscription	
Subscription ID 14d26092-8e42-4ea7-b770-9dcef70fb1ea	
Tags (change) Click here to add tags	

Connected devices

 Search connected devices

DEVICE	TYPE	IP ADDRESS	SUBNET
No results.			

No devices are connected to VNet1.

You plan to peer VNet1 to another virtual network named VNet2. VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

- ☐ Configure a service endpoint on VNet2.
- ☐ Add a gateway subnet to VNet1.
- ☐ Create a subnet on VNet1 and VNet2.
- ☒ Modify the address space of VNet1.

Explanation:

Explanation:

The virtual networks you peer must have non-overlapping IP address spaces. The exhibit indicates that VNet1 has an address space of 10.2.0.0/16, which is the same as VNet2, and thus overlaps. We need to change the address space for VNet1.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

Question 8

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Contains
storagecontoso1	A blob service and a table service
storagecontoso2	A blob service and a file service
storagecontoso3	A queue service
storagecontoso4	A file service and a queue service
storagecontoso5	A table service

You enable Storage Advanced Threat Protection (ATP) for all the storage accounts.

You need to identify which storage accounts will generate Storage ATP alerts.

Which two storage accounts should you identify? Each correct answer presents part of the solution.

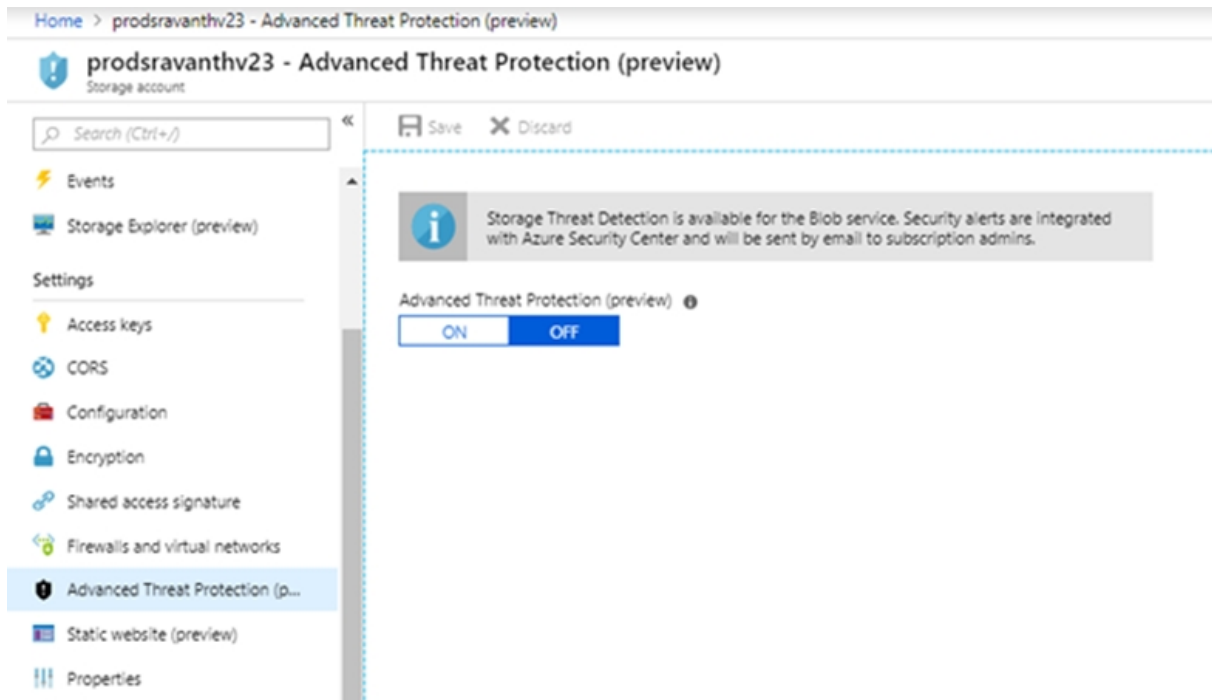
NOTE: Each correct selection is worth one point.

- ☒ storagecontoso1
- ☒ storagecontoso2
- ☐ storagecontoso3
- ☐ storagecontoso4
- ☐ storagecontoso5

Explanation:

Explanation:

Storage Threat Detection is available for the Blob Service.



Reference:

<https://azure.microsoft.com/en-us/blog/advanced-threat-protection-for-azure-storage-now-in-public-preview/>

Question 9

You are designing an Azure solution.

The solution must meet the following requirements:

Distribute traffic to different pools of dedicated virtual machines (VMs) based on rules.
Provide SSL offloading capabilities.

You need to recommend a solution to distribute network traffic.

Which technology should you recommend?

- ☒ Azure Application Gateway
- ☐ Azure Load Balancer
- ☐ Azure Traffic Manager
- ☐ server-level firewall rules

Explanation:

Explanation:

If you require "SSL offloading", application layer treatment, or wish to delegate certificate management to Azure, you should use Azure's layer 7 load balancer Application Gateway instead of the Load Balancer.

Incorrect Answers:

D: Because Load Balancer is agnostic to the TCP payload and TLS offload ("SSL") is not provided.

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

Question 10

You have an Azure subscription that contains an Azure Log Analytics workspace.

You have a resource group that contains 100 virtual machines. The virtual machines run Linux.

You need to collect events from the virtual machines to the Log Analytics workspace.

Which type of data source should you configure in the workspace?

- ☒ Syslog
- ☐ Linux performance counters
- ☐ custom fields

Explanation:

Explanation:

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Log Analytics agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to Azure Monitor where a corresponding record is created.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-custom-logs>

Question 11

You have an Azure virtual machine named VM1 and an Azure Active Directory (Azure AD) tenant named adatum.com.

VM1 has the following settings:

IP address: 10.10.0.10

System-assigned managed identity: On

You need to create a script that will run from within VM1 to retrieve the authentication token of VM1.

Which address should you use in the script?

- ☐ vm1.adatum.com.onmicrosoft.com
- ☒ 169.254.169.254
- ☐ 10.10.0.10
- ☐ vm1.adatum.com

Explanation:

Explanation:

Your code that's running on the VM can request a token from the Azure Instance Metadata Service identity endpoint, accessible only from within the VM:

<http://169.254.169.254/metadata/identity/oauth2/token>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

Question 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use the Synchronization Service Manager to modify the Active Directory Domain Services (AD DS) Connector.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Instead use Synchronization Rules Editor to create a synchronization rule.

Note: Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI (Synchronization Rules Editor) or PowerShell.

Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

Case Study (0 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end

A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

Move all the tiers of App1 to Azure.

Move the existing product blueprint files to Azure Blob storage.

Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

Move all the virtual machines for App1 to Azure.

Minimize the number of open ports between the App1 tiers.

Ensure that all the virtual machines for App1 are protected by backups.

Copy the blueprint files to Azure over the Internet.

Ensure that the blueprint files are stored in the archive storage tier.

Ensure that partner access to the blueprint files is secured and temporary.

Prevent user passwords or hashes of passwords from being stored in Azure.

Use unmanaged standard storage for the hard disks of the virtual machines.

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

Designate a new user named Admin1 as the service admin for the Azure subscription.

Admin1 must receive email alerts regarding service outages.

Ensure that a new user named User3 can create network objects for the Azure subscription.

Implement Management and Security Solutions

(11 questions)

Question 13

An administrator plans to create a function app in Azure that will have the following settings:

Runtime stack: .NET Core

Operating System: Linux

Plan type: Consumption

Enable Application Insights: Yes

You need to ensure that you can back up the function app.

Which settings should you recommend changing before creating the function app?

- ☐ Runtime stack
- ☐ Enable Application Insights
- ☐ Operating System
- ☒ Plan type

Explanation:

Explanation:

The Backup and Restore feature requires the App Service plan to be in the Standard, Premium or Isolated tier.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/manage-backup#requirements-and-restrictions>

Question 14

You have resources in three Azure regions. Each region contains two virtual machines. Each virtual machine has a public IP address assigned to its network interface and a locally installed application named App1.

You plan to implement Azure Front Door-based load balancing across all the virtual machines.

You need to ensure that App1 on the virtual machines will only accept traffic routed from Azure Front Door.

What should you implement?

- ☐ Azure Private Link
- ☐ service endpoints
- ☒ network security groups (NSGs) with service tags
- ☐ network security groups (NSGs) with application security groups

Explanation:

Explanation:

Configure IP ACLing for your backends to accept traffic from Azure Front Door's backend IP address space and Azure's infrastructure services only. Refer the IP details below for ACLing your backend:

Refer AzureFrontDoor.Backend section in Azure IP Ranges and Service Tags for Front Door's IPv4 backend IP address range or you can also use the service tag AzureFrontDoor.Backend in your network security groups.

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq>

Question 15

You are implementing authentication for applications in your company. You plan to implement self-service password reset (SSPR) and multifactor authentication (MFA) in Azure Active Directory (Azure AD).

You need to select authentication mechanisms that can be used for both MFA and SSPR.

Which two authentication methods should you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☒ Authenticator app
- ☐ Email addresses
- ☐ App passwords
- ☒ Short Message Service (SMS) messages
- ☐ Security questions

Explanation:

Explanation:

The following authentication mechanisms can be used for both MFA and SSPR:

Short Message Service (SMS) messages

Azure AD passwords

Microsoft Authenticator app

Voice call

Incorrect Answers:

B, E: The following authentication mechanisms are used for SSPR only:

Email addresses

Security questions

E: App passwords authentication mechanisms can be used for MFA only, but only in certain cases.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

Question 16

You have an Azure key vault named KV1.

You need to ensure that applications can use KV1 to provision certificates automatically from an external certification authority (CA).

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ From KV1, create a certificate issuer resource.
- ☐ Obtain the CA account credentials.
- ☒ Obtain the root CA certificate.
- ☒ From KV1, create a certificate signing request (CSR).
- ☐ From KV1, create a private key,

Explanation:

Explanation:

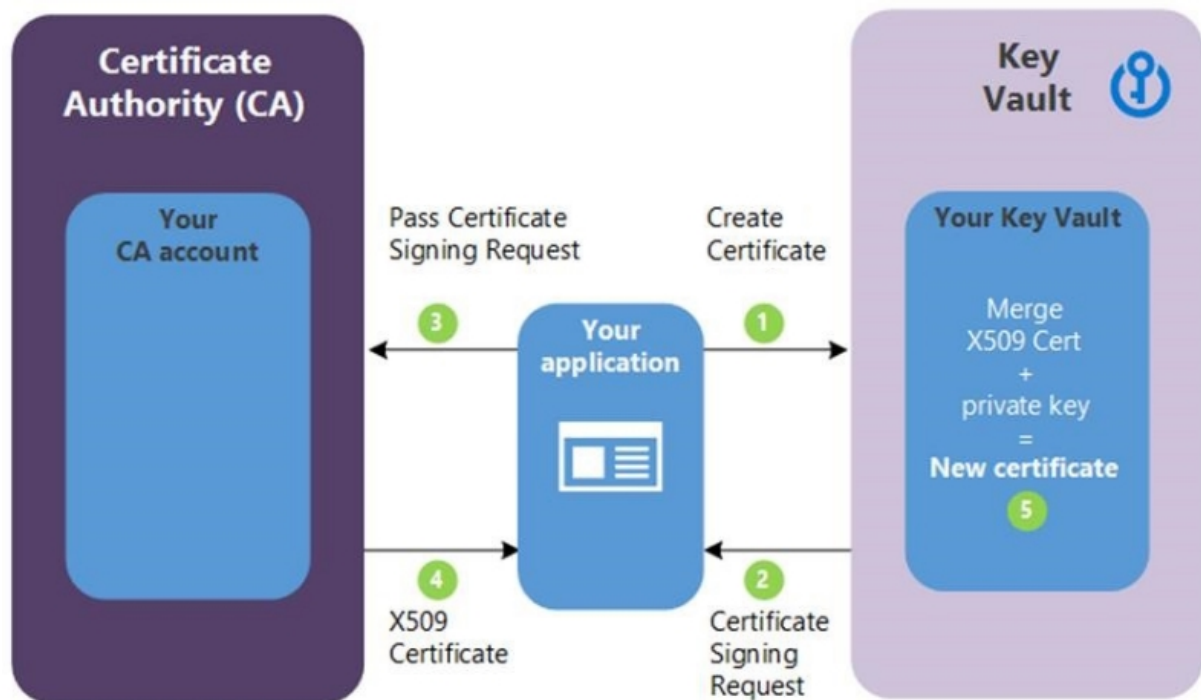
C: Obtain the root CA certificate (step 4 in the picture below)

D: From KV1, create a certificate signing request (CSR) (step 2 in the picture below)

Note:

Creating a certificate with a CA not partnered with Key Vault

This method allows working with other CAs than Key Vault's partnered providers, meaning your organization can work with a CA of its choice.



The following step descriptions correspond to the green lettered steps in the preceding diagram.

In the diagram above, your application is creating a certificate, which internally begins by creating a key in your key vault.

Key Vault returns to your application a Certificate Signing Request (CSR).

Your application passes the CSR to your chosen CA.

Your chosen CA responds with an X509 Certificate.

Your application completes the new certificate creation with a merger of the X509 Certificate from your CA.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/certificates/certificate-scenarios>

Question 17

You create the following Azure role definition.

```
{
  "Name": "Role1",
  "Id": "80808080-8080-8080-8080-808080808080",
  "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": [ ]
}
```

You need to create Role1 by using the role definition.

Which two values should you modify before you create Role1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☒ AssignableScopes
- ☐ Description
- ☐ DataActions
- ☒ IsCustom
- ☐ Id

Explanation:

Explanation:

Part of example:

"IsCustom": true,

```
"AssignableScopes": [
  "/subscriptions/{subscriptionId1}",
  "/subscriptions/{subscriptionId2}",
  "/subscriptions/{subscriptionId3}"
]
```

The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
{
  "Name": "Virtual Machine Operator",
  "Id": "88888888-8888-8888-8888-888888888888",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/{subscriptionId1}",
    "/subscriptions/{subscriptionId2}",
    "/subscriptions/{subscriptionId3}"
  ]
}
```

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

Question 18

Your company has an Azure subscription.

You enable multi-factor authentication (MFA) for all users.

The company's help desk reports an increase in calls from users who receive MFA requests while they work from the company's main office.

You need to prevent the users from receiving MFA requests when they sign in from the main office.

What should you do?

- ☐ From Conditional access in Azure Active Directory (Azure AD), create a named location.
- ☒ From the MFA service settings, create a trusted IP range.
- ☐ From Conditional access in Azure Active Directory (Azure AD), create a custom control.
- ☐ From Azure Active Directory (Azure AD), configure organizational relationships.

Explanation:

Explanation:

The first thing you may want to do, before enabling Multi-Factor Authentication for any users, is to consider configuring some of the available settings. One of the most important features is a trusted IPs list. This will allow you to whitelist a range of IPs for your network. This way, when users are in the office, they will not get prompted with MFA, and when they take their devices elsewhere, they will. Here's how to do it:

Log in to your Azure Portal.

Navigate to Azure AD > Conditional Access > Named locations.

From the top toolbar select Configure MFA trusted IPs.

Reference:

<https://www.kraftkennedy.com/implementing-azure-multi-factor-authentication/>

Question 19

Your company has the groups shown in the following table.

Group	Number of members
Managers	10
Sales	100
Development	15

The company has an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 attempts to enable Enterprise State Roaming for all the users in the Managers groups.

Admin1 reports that the options for Enterprise State Roaming are unavailable from Azure AD.

You verify that Admin1 is assigned the Global administrator role.

You need to ensure that Admin1 can enable Enterprise State Roaming.

What should you do?

- ☐ Assign an Azure AD Privileged Identity Management (PIM) role to Admin1.
- ☐ Purchase an Azure Rights Management (Azure RMS) license for each user in the Managers group.
- ☐ Enforce Azure Multi-Factor Authentication (MFA) for Admin1.
- ☒ Purchase an Azure AD Premium P1 license for each user in the Managers group.

Explanation:

Explanation:

Enterprise State Roaming is available to any organization with an Azure AD Premium or Enterprise Mobility + Security (EMS) license.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/devices/enterprise-state-roaming-enable>

Question 20

You have SQL Server on an Azure virtual machine named SQL1.

You need to automate the backup of the databases on SQL1 by using Automated Backup v2 for the virtual machines. The backups must meet the following requirements:

Meet a recovery point objective (RPO) of 15 minutes.

Retain the backups for 30 days.

Encrypt the backups at rest.

What should you provision as part of the backup solution?

- ☐ Elastic Database jobs
- ☐ Azure Key Vault
- ☒ an Azure Storage account
- ☐ a Recovery Services vault

Explanation:

Explanation:

An Azure storage account is used for storing Automated Backup files in blob storage. A container is created at this location to store all backup files. The backup file naming convention includes the date, time, and database GUID.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup>

Question 21

You have 10 Azure virtual machines on a subnet named Subnet1. Subnet1 is on a virtual network named VNet1.

You plan to deploy a public Azure Standard Load Balancer named LB1 to the same Azure region as the 10 virtual machines.

You need to ensure that traffic from all the virtual machines to the internet flows through LB1. The solution must prevent the virtual machines from being accessible on the internet.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☒ Add health probes to LB1.
- ☒ Add the network interfaces of the virtual machines to the backend pool of LB1.
- ☐ Add an inbound rule to LB1.
- ☒ Add an outbound rule to LB1.
- ☐ Associate a network security group (NSG) to Subnet1.
- ☐ Associate a user-defined route to Subnet1.

Explanation:

Explanation:

A: To allow the Load Balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the Load Balancer rotation based on their response to health checks.

B: To distribute traffic to the VMs, a backend address pool contains the IP addresses of the virtual (NICs) connected to the Load Balancer.

D: A Load Balancer rule is used to define how traffic is distributed to the VMs. Only outbound traffic is allowed.

Reference: <https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal>

Question 22

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Connected to
VM1	VNET1/Subnet1
VM2	VNET1/Subnet2

KeyVault1 has an access policy that provides several users with Create Key permissions.

You need to ensure that the users can only register secrets in KeyVault1 from VM1.

What should you do?

- ☐ Create a network security group (NSG) that is linked to Subnet1.
- ☐ Configure the Firewall and virtual networks settings for KeyVault1.
- ☒ Modify the access policy for KeyVault1.
- ☐ Configure KeyVault1 to use a hardware security module (HSM).

Explanation:

Explanation:

You grant data plane access by setting Key Vault access policies for a key vault.

Note 1: Grant our VM's system-assigned managed identity access to the Key Vault.

Select Access policies and click Add new.

In Configure from template, select Secret Management.

Choose Select Principal, and in the search field enter the name of the VM you created earlier. Select the VM in the result list and click Select.

Click OK to finishing adding the new access policy, and OK to finish access policy selection.

Note 2: Access to a key vault is controlled through two interfaces: the management plane and the data plane. The management plane is where you manage Key Vault itself. Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies. The data plane is where you work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad>

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault2>

Question 23

You have an application named App1 that does not support Azure Active Directory (Azure AD) authentication.

You need to ensure that App1 can send messages to an Azure Service Bus queue. The solution must prevent App1 from listening to the queue.

What should you do?

- ☐ Configure Access control (IAM) for the Service Bus.
- ☒ Add a shared access policy to the queue.
- ☐ Modify the locks of the queue.
- ☐ Configure Access control (IAM) for the queue.

Explanation:

Explanation:

There are two ways to authenticate and authorize access to Azure Service Bus resources: Azure Activity Directory (Azure AD) and Shared Access Signatures (SAS).

Each Service Bus namespace and each Service Bus entity has a Shared Access Authorization policy made up of rules.

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-authentication-and-authorization>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-sas>

Case Study (1 questions)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end

A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

Move all the tiers of App1 to Azure.

Move the existing product blueprint files to Azure Blob storage.

Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

Move all the virtual machines for App1 to Azure.

Minimize the number of open ports between the App1 tiers.

Ensure that all the virtual machines for App1 are protected by backups.

Copy the blueprint files to Azure over the Internet.

Ensure that the blueprint files are stored in the archive storage tier.

Ensure that partner access to the blueprint files is secured and temporary.

Prevent user passwords or hashes of passwords from being stored in Azure.

Use unmanaged standard storage for the hard disks of the virtual machines.

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

Designate a new user named Admin1 as the service admin for the Azure subscription.

Admin1 must receive email alerts regarding service outages.

Ensure that a new user named User3 can create network objects for the Azure subscription.

Question 24

You need to recommend an identity solution that meets the technical requirements.

What should you recommend?

- ☐ password hash synchronization and single sign-on (SSO)
- ☐ federated single sign-on (SSO) and Active Directory Federation Services (AD FS)
- ☒ Pass-through Authentication and single sign-on (SSO)
- ☐ cloud-only user accounts

Explanation:

Explanation:

With Pass-through Authentication the on-premises passwords are never stored in the cloud in any form.

Scenario:

Prevent user passwords or hashes of passwords from being stored in Azure.

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

Implement Solutions for Apps

(6 questions)

Question 25

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Server1 that runs Windows Server 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

```
XCOPY File1.txt C:\Folder1\
```

You then build the container image.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Copy is the correct command to copy a file to the container image. Furthermore, the root directory is specified as '/' and not as 'C:/'.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>

Question 26

You have an Azure subscription that contains the web apps shown in the following table.

Name	Runtime stack
WebApp1	Java SE
WebApp2	Ruby 2.6
WebApp3	Python 3.7
WebApp4	ASP.NET V4.7

For which web app can you configure a WebJob?

- ☐ WebApp1
- ☒ WebApp4
- ☐ WebApp2
- ☐ WebApp3

Explanation:

Explanation:

Publishing a .NET Core WebJob to App Service from Visual Studio uses the same tooling as publishing an ASP.NET Core app.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/webjobs-dotnet-deploy-vs>

Question 27

Your network contains an on-premises Active Directory domain named contoso.com that contains a member server named Server1.

You have the accounts shown in the following table.

Name	Member of
CONTOSO\User1	Domain Admins
CONTOSO\User2	Domain Users
CONTOSO\User3	Enterprise Admin
SERVER1\User4	Users

You are installing Azure AD Connect on Server1.

You need to specify the account for Azure AD Connect synchronization. The solution must use the principle of least privilege.

Which account should you specify?

- ☒ CONTOSO\User2
- ☐ SERVER1\User4
- ☐ CONTOSO\User1
- ☐ CONTOSO\User3

Explanation:

Explanation:

The default Domain User permissions are sufficient

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

Question 28

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Server1 that runs Windows Server 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

```
COPY File1.txt /Folder1/
```

You then build the container image.

Does this meet the goal?

- ☒ Yes
☐ No

Explanation:

Explanation:

Copy is the correct command to copy a file to the container image.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>

Question 29

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You assign the Global administrator role to Admin1.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Question 30

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a server named Server1 that runs Windows Server 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

```
ADD File1.txt C:/Folder1/
```

You then build the container image.

Does this meet the goal?

- ☐ Yes
☒ No

Explanation:

Explanation:

Copy is the correct command to copy a file to the container image. The ADD command can also be used. However, the root directory is specified as '/' and not as 'C:/'.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>