Describe Security, Privacy, Compliance and Trust

Completed on 04-February-2021

Attempt	Marks Obtained	Your score	Time Taken	Result
11	0 / 25	0.0%	00 H 01 M 16 S	Failed

Domains wise Quiz Performance Report

No	Domain	Total Question	Correct	Incorrect	Unattempted	Marked as Review
1	Other	5	0	0	5	0
2	Describe identity, governance, privacy, and compliance features	20	0	1	19	0
Total	All Domain	25	0	1	24	0

Review the Answers

Sorting by All

Question 1 **Unattempted**

Domain : Other

A company has created a virtual network and also launched a set of virtual machines in the virtual network. They want to change the way the traffic is routed in the virtual network. Which of the following could be used to fulfil this requirement?

A. User Defined Routes ✓

B. Application Security Groups

C. Network Security Groups

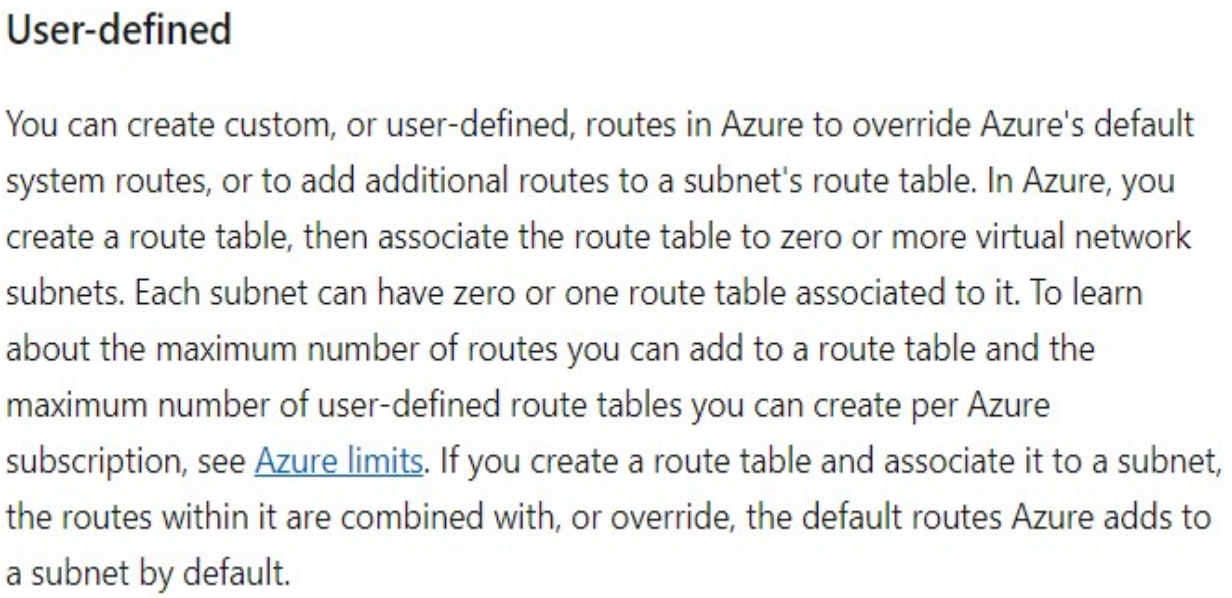
D. Azure DDoS Protection

Explanation:

Answer – A

You can create your network routes using User Defined Routes

The Microsoft documentation mentions the following



User-defined

You can create custom, or user-defined, routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it. To learn about the maximum number of routes you can add to a route table and the maximum number of user-defined route tables you can create per Azure subscription, see Azure limits. If you create a route table and associate it to a subnet, the routes within it are combined with, or override, the default routes Azure adds to a subnet by default.

Options B and C are incorrect since these are used to filter network traffic into and out of virtual networks.

Option D is incorrect since this is used to protect infrastructure against DDoS attacks

For more information on virtual network routing, please visit the below URL

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Ask our Experts Rate this Question?

View Queries open

Question 2 **Unattempted**

Domain : Other

A company currently has an Azure subscription and an Azure tenant. They want to implement Azure Multi-factor authentication. Is it possible to add an SMS as a second means of authentication for a user?

A. Yes ✓

B. No

Explanation:

Answer – A

Azure provides the following authentication methods for both Multi-Factor authentication and self-service password reset. In this, SMS is an authentication method available

Microsoft highly recommends Administrators enable users to select more than the minimum required number of authentication methods in case they do not have access to one.

Authentication Method	Usage
Password	MFA and SSPR
Security questions	SSPR Only
Email address	SSPR Only
Microsoft Authenticator app	MFA and SSPR
OATH Hardware token	Public preview for MFA and SSPR
SMS	MFA and SSPR
Voice call	MFA and SSPR
App passwords	MFA only in certain cases

For more information on authentication methods, please visit the below URL

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

Ask our Experts Rate this Question?

View Queries open

Question 3 **Unattempted**

Domain : Other

A company is planning on using Azure Security Center. They already have a set of resources defined on the Azure platform. Is the company limited to the usage of Azure Security Center to secure its Virtual Machines **ONLY** in Azure Cloud?

A. Yes

B. No

Explanation:

Answer – B

Azure Security Center has support not only for VMs but for other components too like Azure SQL and Storage services etc

The Microsoft documentation mentions the following

For more information on the supported platform for Azure Security Center, please visit the below URL

https://docs.microsoft.com/en-us/azure/security-center/security-center-os-coverage

Ask our Experts Rate this Question?

View Queries open

Question 4 **Unattempted**

Domain : Other

A company wants to have a service that could fulfil the below requirement
"Provide the ability to generate keys in hardware security modules that never leave the hardware security module boundary"
Which of the following service could be used for this requirement?

A. Azure Key vault
B. Azure Security Center
C. Azure Advisor
D. Azure Network Security Groups

Explanation:

Answer – A

You can achieve this requirement with the help of the Azure Key vault service

The Microsoft documentation mentions the following

> Azure Key Vaults may be either software- or hardware-HSM protected. For situations where you require added assurance you can import or generate keys in hardware security modules (HSMs) that never leave the HSM boundary. Microsoft uses nCipher hardware security modules. You can use nCipher tools to move a key from your HSM to Azure Key Vault.

Since this is clear from the documentation, all other options are incorrect

For more information on the Key vault service, please visit the below URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-overview

Ask our Experts

Rate this Question?

View Queries

open

Question 5

Unattempted

Domain : Other

A company is planning on creating several policies in the Azure Policy service. These policies are all meant to achieve a particular goal. Which of the following could be used to organize these policies into one group?

A. Management Groups

B. Initiative Definition

C. Resource Groups

D. Subscriptions

Explanation:

Answer – B

You can club the policy definitions into one Initiative Definition.

The Microsoft documentation mentions the following

Initiative definition

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item. For example, you could create an initiative titled **Enable Monitoring in Azure Security Center**, with a goal to monitor all the available security recommendations in your Azure Security Center.

Under this initiative, you would have policy definitions such as:

- **Monitor unencrypted SQL Database in Security Center** – For monitoring unencrypted SQL databases and servers.
- **Monitor OS vulnerabilities in Security Center** – For monitoring servers that don't satisfy the configured baseline.
- **Monitor missing Endpoint Protection in Security Center** – For monitoring servers without an installed endpoint protection agent.

Since this is clear from the documentation, all other options are incorrect

For more information on Azure Policies, please visit the below URL

https://docs.microsoft.com/en-us/azure/governance/policy/overview

Ask our Experts Rate this Question?

View Queries open

Question 6 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company has deployed a virtual machine in Azure, to enable communication with other resources, a Network Security Group is created while creating the Network Security Group, following text is entered into the Tags Text box:

Tag :

Name:CrossSiteScript
Value:<script>Alert("CrossSiteScript")</script>
What happens while deploying the NSG?

A. Input Validation has to be enabled on the controls to avoid error

B. Throws error during deployment

C. Deploys successfully

D. Input Validation has to be disabled on the controls to avoid error

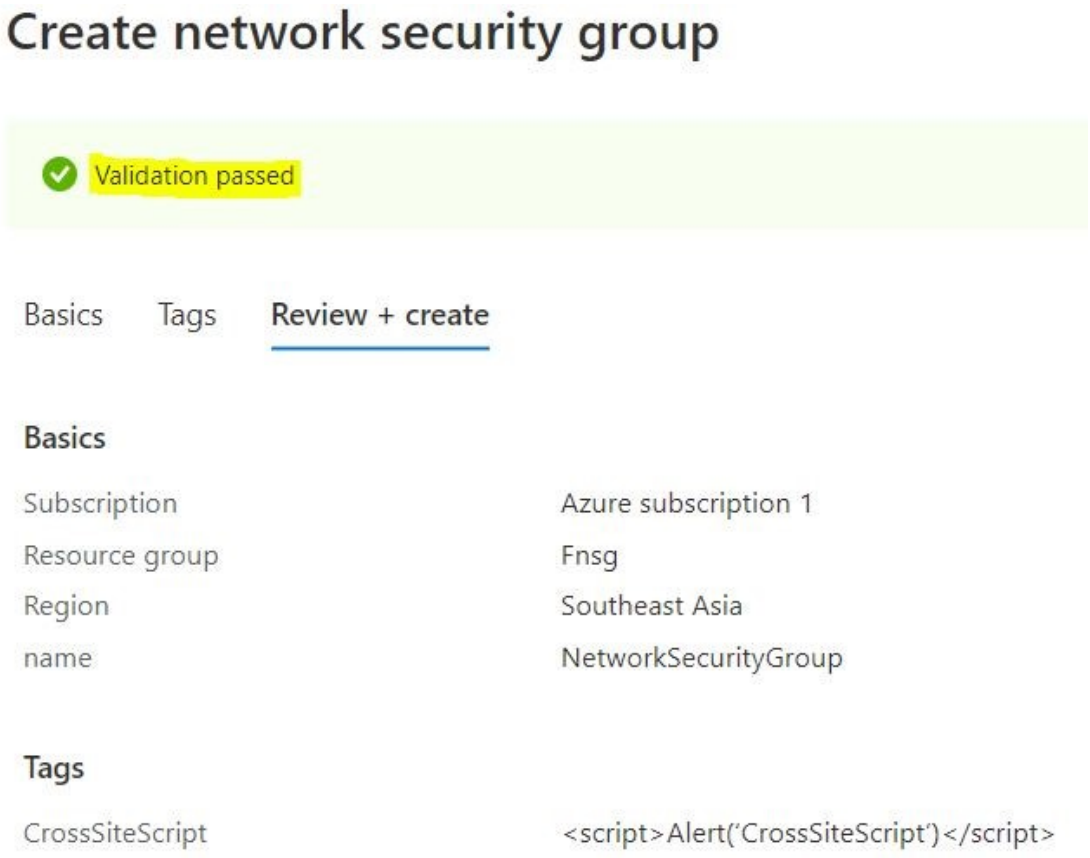
Explanation:

Answer: C

Option A, B, D are incorrect because input validation on controls is taken care in azure

Option C is CORRECT as the input validation is taken care in Azure, the script that is entered in Tags Text Control does not throw any error, it would be treated as a raw text. Please see the screenshot, which shows the validation result while creating the Network Security Group

Diagram:



Reference: https://portal.azure.com

Ask our Experts Rate this Question?

View Queries open

Question 7 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company has deployed a virtual machine in Azure and to filter the network traffic, an Application Security Group is created through CLI using a template.
Which of the following is a valid Application Security Group template?

A.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01
    "contentVersion": "1.0.0.0",
    @parameters@: {
        "applicationSecurityGroupName": {
            "type": "string",
            "metadata": {
                "description": "This is the name of the application se
            }
        },
        @location@: {
            "type": "string",
            "metadata": {
                "description": "Location where the application securit
            }
        }
    },
    @resources@: [
        {
            "apiVersion": "2019-02-01",
            "type": "Microsoft.Network/applicationSecurityGroups",
            "name": "[parameters('applicationSecurityGroupName')]",
            "location": "[parameters('location')]",
            "tags": {}
        }
    ]
}
```

B.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01
    "contentVersion": "1.0.0.0",
    "parameters": {
        "applicationSecurityGroupName": {
            "type": "string",
            "metadata": {
                "description": "This is the name of the application se
            }
        },
        "location": {
            "type": "string",
            "metadata": {
                "description": "Location where the application securit
            }
        }
    },
    "resources": [
        {
            "apiVersion": "2019-02-01",
            "type": "Microsoft.Network/applicationSecurityGroups",
            "name": "[parameters('applicationSecurityGroupName')]",
            "location": "[parameters('location')]",
            "tags": {}
        }
    ]
}
```

C.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01
    "contentVersion": "1.0.0.0",
    #parameters#: {
        "applicationSecurityGroupName": {
            "type": "string",
            "metadata": {
                "description": "This is the name of the application se
            }
        },
        #location#: {
            "type": "string",
            "metadata": {
                "description": "Location where the application securit
            }
        }
    },
    #resources#: [
        {
            "apiVersion": "2019-02-01",
            "type": "Microsoft.Network/applicationSecurityGroups",
            "name": "[parameters('applicationSecurityGroupName')]",
            "location": "[parameters('location')]",
            "tags": {}
        }
    ]
}
```

D.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01
    "contentVersion": "1.0.0.0",
    $parameters$: {
        "applicationSecurityGroupName": {
            "type": "string",
            "metadata": {
                "description": "This is the name of the application se
            }
        },
        $location$: {
            "type": "string",
            "metadata": {
                "description": "Location where the application securit
            }
        }
    },
    $resources$: [
        {
            "apiVersion": "2019-02-01",
            "type": "Microsoft.Network/applicationSecurityGroups",
            "name": "[parameters('applicationSecurityGroupName')]",
            "location": "[parameters('location')]",
            "tags": {}
        }
    ]
}
```

Explanation:

Answer: B

Option A is incorrect because the template is in json format and has an invalid @ character

Option B is CORRECT as it has a valid json

Option C is incorrect because the template is in json format and has an invalid # character

Option D is incorrect because the template is in json format and has an invalid $ character

Reference:

https://docs.microsoft.com/en-us/azure/templates/microsoft.network/applicationsecuritygroups

Ask our Experts

Rate this Question?

View Queries open

Question 8 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company has a Virtual Network and wants to implement the following requirements

To create 2 subnets and 2 VM's in each subnet

To create a user defined route to enable the 2 subnet resources to communicate

Can a user defined route be created without creating Subnet?

A. **UDR cannot be created without creating Subnet**

B. **UDR can be created without creating Subnet** ✓

C. **At-least one UDR is required to create a Subnet**

D. **There is no relation between Route and Subnet**

Explanation:

Answer: B

Option A is incorrect because there is no mandatory validation to have a subnet while creating an UDR

Option B is CORRECT because UDR can be created prior to creation of the Subnet. But it would be effective only once the route is associated with Subnet. Please refer to the reference url

Option C is incorrect because though UDR is required to associate with Subnet, it is not required during creation

Option D is incorrect because UDR is relevant when resources of the subnets communicate with each other

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 9 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company has a Virtual Network with 2 subnets; Subnet1, Subnet2. A Virtual Machine with Web Server is created in Subnet1 and another Virtual Machine with Database Server is created in Subnet2. A Firewall is created in the Virtual Network. The company's Firewall policy is set to get Alert for the Threat Intelligence mode.
Does the Threat Intelligence mode of the newly created Firewall overrides the parent Policy?

A. **Parent policy cannot be overridden**

B. **Parent policy can be overridden**

C. **Parent policy is overridden with stricter setting** ✓

D. **Parent policy is overridden and threat intelligence can be turned off**

Explanation:

Answer: C

Option A is incorrect because Thread Intelligence mode can be overridden for the Parent policy

Option B is incorrect because the new policy cannot be completely overridden, it is overridden with stricter setting only

Option C is CORRECT because the newly created Firewall policy can be overridden with stricter setting, Please refer to the reference url

Option D is incorrect because the Threat Intelligence for the newly created Firewall policy cannot be turned off

Reference:

https://docs.microsoft.com/en-us/azure/firewall-manager/policy-overview

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 10 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company plans to implement an Azure DDoS. Below are the key requirements

Company has multiple subscriptions

The total number of resources across subscriptions are 75

Does the DDoS Protection Standard Plan meet the above requirements?

A. **DDoS Protection Standard Plan does not meet the first requirement**

B. **DDoS Protection Standard Plan does not meet the second requirement**

C. **Multiple DDoS Protection Standard Plans are required, one for each requirement**

D. **DDoS Protection Standard Plan meets both the requirements** ✓

Explanation:

Answer: D

Option A is incorrect because DDoS Protection Standard Plan can be used across multiple subscriptions

Option B is incorrect because DDoS Protection Standard Plan includes protection for 100 resources

Option C is incorrect as a single DDoS Protection Standard Plan meet both the requirements

Option D is CORRECT because by default DDoS Protection Standard Plan meet both the requirements. Please refer to the reference url.

Reference:

https://azure.microsoft.com/en-us/pricing/details/ddos-protection/

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 11 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to know how well the security best practices are implemented in Azure. Which security feature would help to identify the current Identity practices and advice improvements?

A. **Azure Information Protection**

B. **Azure AD Identity Protection**

C. **Azure AD Identity Secure Score** ✓

D. **Security Center**

Explanation:

Answer: C

Option A is incorrect because AIP is used primarily for classifying and protecting documents and emails

Option B is incorrect because Azure AD Identity Protection helps in identifying the vulnerabilities related to identity

Option C is CORRECT because Azure AD Identity Secure Score helps in identifying the identity secure score to provide the recommendations

Option D is incorrect because Security Center primarily assesses the environment and workloads and provides recommendations for threat prevention.

Diagram:

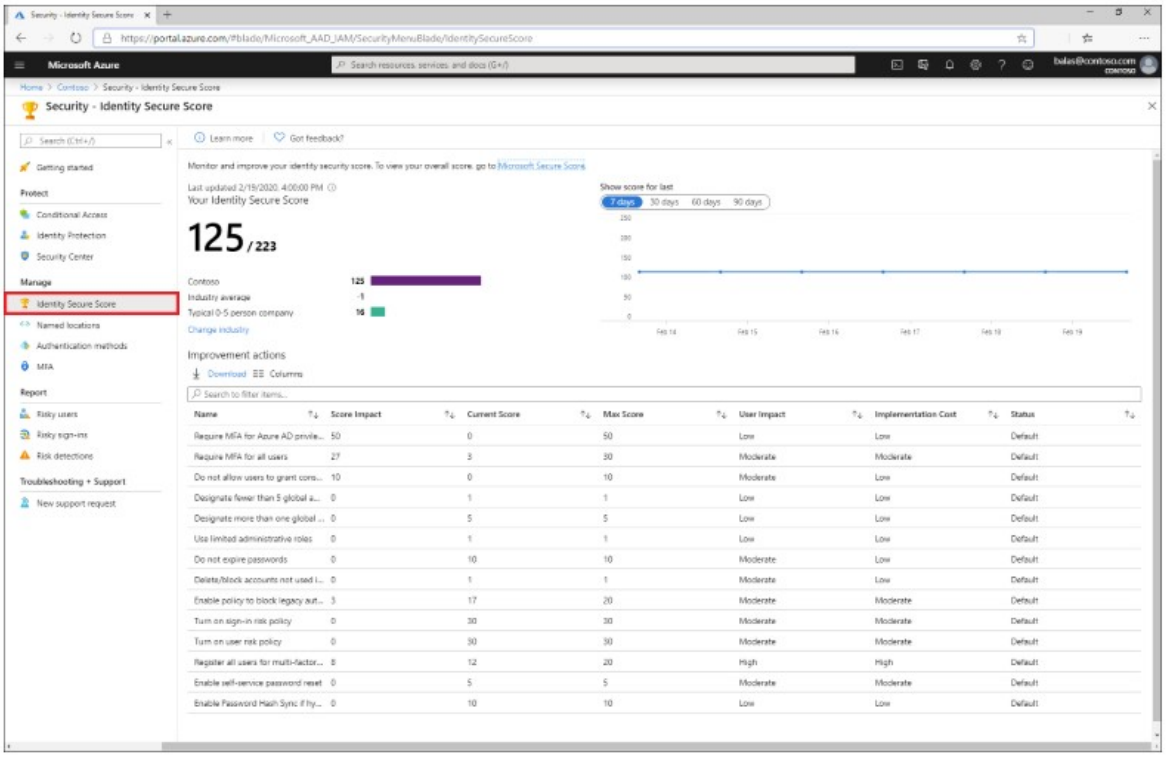
What is the identity secure score in Azure Active Directory?

02/20/2020 • 4 minutes to read • +1

How secure is your Azure AD tenant? If you don't know how to answer this question, this article explains how the identity secure score helps you to monitor and improve your identity security posture.

What is an identity secure score?

The identity secure score is number between 1 and 223 that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security. Each improvement action in identity secure score is tailored to your specific configuration.



The score helps you to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score?branch=pr-en-us-52761

Ask our Experts

Rate this Question?

View Queries open

Question 12 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to implement Azure AD Identity Protection. Following are the key requirements:

Prompt users if the credentials are compromised

Identify suspicious login attempts

Which of the following policies implement the above requirements?
Choose two answers.

A. **User risk policy** ✓

B. **Azure policy**

C. **Sign in risk policy** ✓

D. **MFA registration policy**

Explanation:

Answer: A, C

Option A is CORRECT, it is used if the credentials are compromised

Option B is incorrect as it is a Service to create policies in Azure

Option C is CORRECT, it is considered for any suspicious sign-ins like multiple incorrect login attempts

Option D is incorrect, it ensures that user registers for MFA

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 13 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to move all its employees to Azure Active Directory. What is the initial domain where the tenant is created?

A. onmicrosoft.com

B. portal.azure.com

C. azurewebsites.com

D. microsoft.com

Explanation:

Answer: B

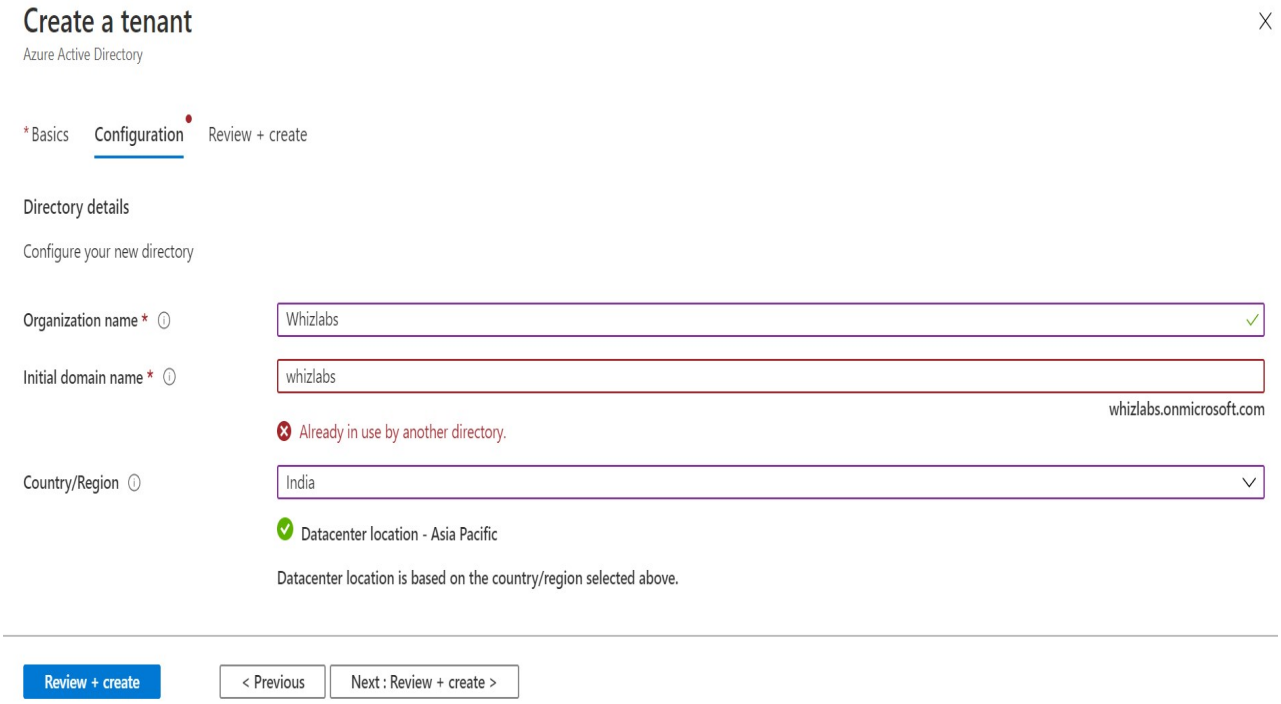
Option A is incorrect as is used for Microsoft products and services—including images, text, and software downloads (the "content")—are owned either by Microsoft Corporation or by third parties who have granted Microsoft permission to use the content.

Option B is correct as portal.azure.com is the default domain where the tenant is created.

Option C is incorrect as azurewebsites.com is used to host the web application in azure.

Option D is incorrect as microsoft.com is Microsoft's public site

Diagram:



Reference: https://portal.azure.com to create a tenant

Ask our Experts Rate this Question?

View Queries open

Question 14 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to implement Azure Multi-Factor Authentication. Which of the following is the recommended policy?

A. Enable per-user

B. Enable per-session

C. Enable Conditional Access

D. Enable Security Defaults

Explanation:

Answer: C

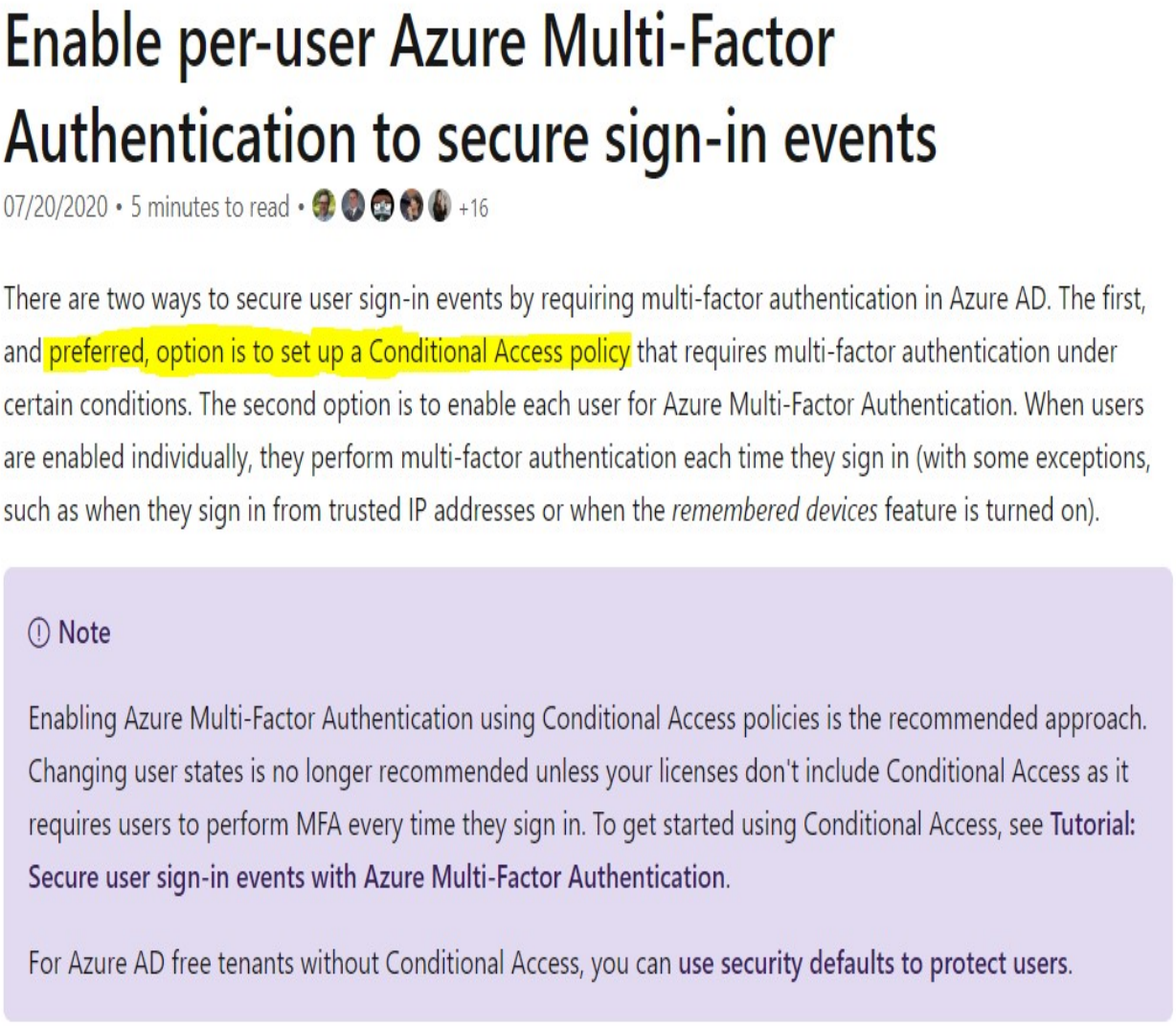
Option A is incorrect as it is not advised per user, as it would be time consuming and difficult to maintain for large number of users

Option B is incorrect because session is per user login and policy is not applied on user session

Option C is CORRECT because it would help to provide the access for group of users and helps in managing efficiently

Option D is incorrect because it is applicable for free tier by default

Diagram:



Enable per-user Azure Multi-Factor Authentication to secure sign-in events

07/20/2020 • 5 minutes to read • +16

There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi-factor authentication under certain conditions. The second option is to enable each user for Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the *remembered devices* feature is turned on).

Note

Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in. To get started using Conditional Access, see **Tutorial: Secure user sign-in events with Azure Multi-Factor Authentication**.

For Azure AD free tenants without Conditional Access, you can **use security defaults to protect users**.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

Ask our Experts Rate this Question?

View Queries open

Question 15 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to create an IP Group to configure with an Azure Firewall. The company has 3 branches, each in a different region.
Which of the following is the right option to create an IP Group?

A. **IP Group has to be created in each region**

B. **IP Group has to be created for each branch**

C. **IP Group has to be created for each subscription**

D. **IP Group can be created in any region**

Explanation:

Answer: D

Option A is incorrect because IP Groups are available in all public regions and not specific to a region

Option B is incorrect because IP address which are part of IP Groups are not tagged at Branch level

Option C is incorrect because IP Group can be used across subscriptions

Option D is CORRECT because IP Groups are used to manage IP addresses for Azure Fire Wall rules and can be created and reused across regions and subscriptions

Diagram:

IP Groups in Azure Firewall

06/23/2020 • 2 minutes to read •

IP Groups allow you to group and manage IP addresses for Azure Firewall rules in the following ways:

- As a source address in DNAT rules
- As a source or destination address in network rules
- As a source address in application rules

An IP Group can have a single IP address, multiple IP addresses, or one or more IP address ranges.

IP Groups can be reused in Azure Firewall DNAT, network, and application rules for multiple firewalls across regions and subscriptions in Azure. Group names must be unique. You can configure an IP Group in the Azure portal, Azure CLI, or REST API. A sample template is provided to help you get started.

Reference:

https://docs.microsoft.com/en-us/azure/firewall/ip-groups

Ask our Experts Rate this Question?

View Queries open

Question 16 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

Your Company has multiple subscriptions and wants to implement a custom Dashboard which would display the Secure Score for each subscription.
Which of the following is a valid option?

A. **Not possible to implement Secure Score on to a custom Dashboard**

B. **Can be implemented for only single subscription**

C. **Can be implemented using Secure Score REST API** ✓

D. **Not possible, Secure score is only accessible through the Azure Portal**

Explanation:

Answer: C

Option A is incorrect because Secure Score can be accessed using REST API

Option B is incorrect because using REST API, Secure Score can be retrieved for multiple subscriptions

Option C is CORRECT, please see the reference url, accessing your secure score section

Option D is incorrect because Secure score can be accessed through REST API

Reference:

https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 17 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to create an automation workflow to send notification for specific Threats. While creating the workflow, is it mandatory to use a Logic App?

A. **No, to create automation workflow, Logic App is not mandatory**

B. Yes, it is mandatory to use a Logic App while creating an automation workflow

C. No, there is no relation between Automation Workflow and Logic App

D. No, the Logic App has to be created after creating Automation Workflow

Explanation:

Answer: B

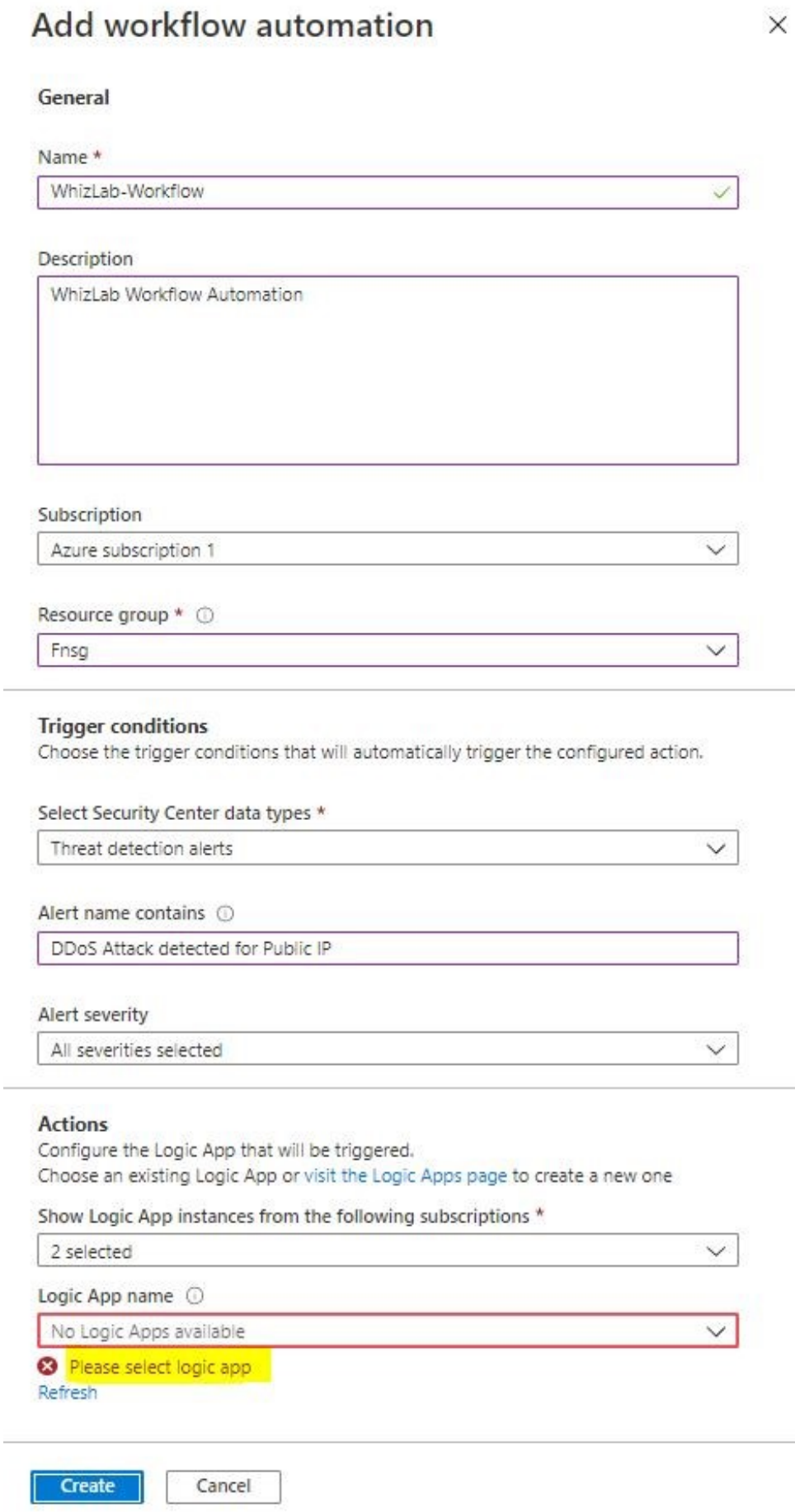
Option A is incorrect because while creating the Automation Workflow, an existing Logic App has to be selected

Option B is CORRECT as Logic App has to be selected while creating an Automation Workflow, please view the diagram below

Option C is incorrect because Logic App is required during automation workflow creation

Option D is incorrect because the Logic App has to be created prior creating automation workflow

Diagram:


Add workflow automation
General
Name *
WhizLab-Workflow
Description
WhizLab Workflow Automation
Subscription
Azure subscription 1
Resource group *
Fnsg
Trigger conditions
Choose the trigger conditions that will automatically trigger the configured action.
Select Security Center data types *
Threat detection alerts
Alert name contains
DDoS Attack detected for Public IP
Alert severity
All severities selected
Actions
Configure the Logic App that will be triggered.
Choose an existing Logic App or visit the Logic Apps page to create a new one
Show Logic App instances from the following subscriptions *
2 selected
Logic App name
No Logic Apps available
Please select logic app
Refresh
Create
Cancel

Reference:

https://portal.azure.com

Ask our Experts

Rate this Question?

View Queries

open

Question 18

Unattempted

Domain :Describe identity, governance, privacy, and compliance features

A company has multiple subscriptions and many resources assigned to each subscription, Administrator wants to know the count of Key Vaults across all the subscriptions, what is the quick way of getting the result?

A. Open Key Vault and Count manually

B. Use Manage view option of Key Vault

C. Use Azure Resource Graph Explorer Query feature

D. Open Key Vault and Apply Filters

Explanation:

Answer: C

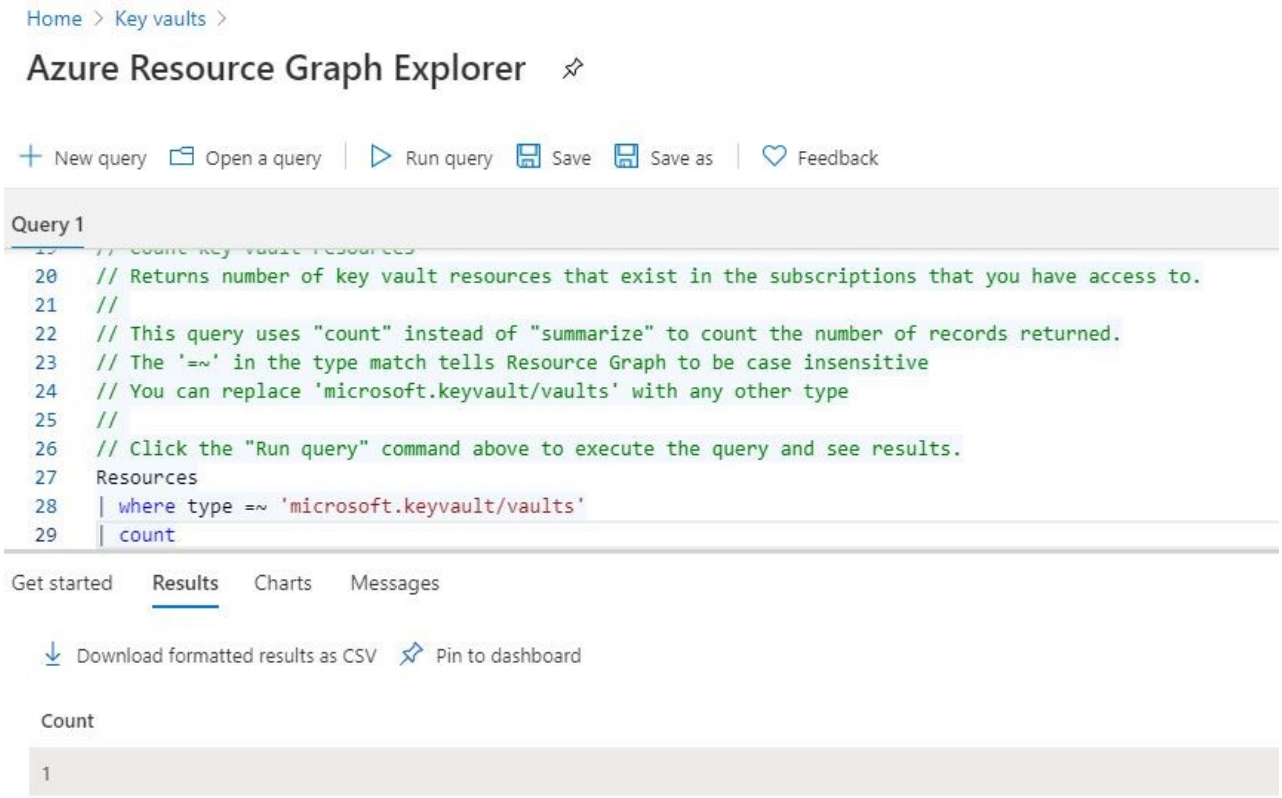
Option A is incorrect because if there are multiple subscriptions, manual counting is not efficient

Option B is incorrect because even for Manage view, manual counting is required

Option C is CORRECT because using Azure Resource Graph total count can be retrieved

Option D is incorrect because Applying Filters would again leads to manual count

Diagram:



Reference:

https://portal.azure.com

Ask our Experts

Rate this Question?

View Queries

open

Question 19

Unattempted

Domain :Describe identity, governance, privacy, and compliance features

A company has implemented Azure Information Protection, a newly joined user is unable to access Azure Information Protection.
Which of the following two roles would enable Azure Information Protection access to the user?

A. **Information Protection Administrator** ✓

B. **Cloud Application Administrator**

C. **Security Administrator** ✓

D. **Group Administrator**

Explanation:

Answer: A, C

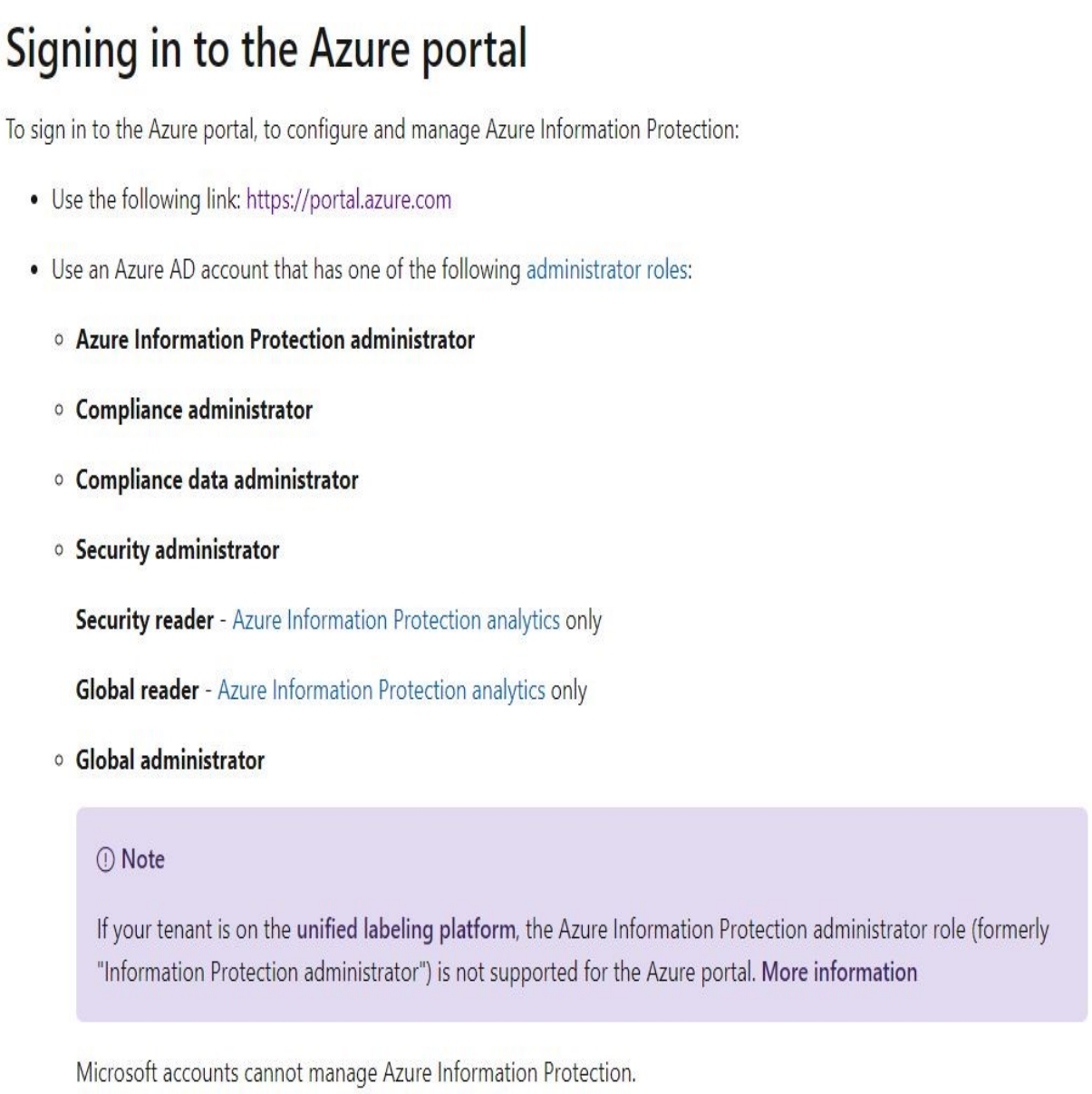
Option A is CORRECT because please see the reference url for the AIP roles list

Option B is incorrect because Cloud Application Administrator is part of Application Administrators

Option C is CORRECT because please see the reference url for the AIP roles list

Option D is incorrect because Group Administrator has access to Administrative features

Diagram:



Signing in to the Azure portal

To sign in to the Azure portal, to configure and manage Azure Information Protection:

- Use the following link: https://portal.azure.com
- Use an Azure AD account that has one of the following administrator roles:
  - **Azure Information Protection administrator**
  - **Compliance administrator**
  - **Compliance data administrator**
  - **Security administrator**

    Security reader - Azure Information Protection analytics only

    Global reader - Azure Information Protection analytics only
  - **Global administrator**

    ⓘ Note

    If your tenant is on the **unified labeling platform**, the Azure Information Protection administrator role (formerly "Information Protection administrator") is not supported for the Azure portal. **More information**

    Microsoft accounts cannot manage Azure Information Protection.

Reference:

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 20 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

Your Company wants to implement a security solution for the users who are on on-premises Active directory, and has following requirement:

Monitor User login/logout

Monitor Active Directory User account changes

Monitor Machine Account

Which is the best option to implement the above requirements?

A. **Azure Advanced Threat Protection**

B. **Azure AD Password Protection**

C. **Azure AD Identity Protection**

D. **Azure AD Privileged Identity Management**

Explanation:

Answer: A

Option A is CORRECT because all the 3 requirements can be implemented using Monitored activities

Option B is incorrect because only Password Protections options are available

Option C is incorrect because it is used for Identity Protections only

Option D is incorrect because it is used only for the important resources

Reference:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/monitored-activities

Ask our Experts Rate this Question?

View Queries open

Question 21 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to implement Azure policy to monitor the virtual machines whose disk encryption is not enabled. What are the ways of creating the policy assignment?
Please select three options.

A. Azure Portal, ARM Template ✓

B. Python, REST ✓

C. Azure CLI, Azure PowerShell ✓

D. Azure Monitor

Explanation:

Answer: A, B, C

Option A is CORRECT because please view the reference url for the ways of creation of policy assignment

Option B is CORRECT because please view the reference url for the ways of creation of policy assignment

Option C is CORRECT because please view the reference url for the ways of creation of policy assignment

Option D is incorrect because Azure Monitor is primarily used to analyze the telemetry data

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/assign-policy-portal

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 22 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company has a health care application, a newly joined user has been added to the Application Developer role. When does the user role take effect?

A. The role will be effective immediately

B. For the role to be effective, it might take up to 15 minutes ✓

C. For the role to be effective, it might take up to 1 hour

D. For the role to be effective, it might take up to 2 hours

Explanation:

Answer: B

Option A is incorrect because it would be effective immediately only on logout\login

Option B is CORRECT because please view the reference url, Active Directory limits section

Option C is incorrect because please view the reference url, Active Directory limits section

Option D is incorrect because please view the reference url, Active Directory limits section

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits#role-based-access-control-limits

Ask our Experts Rate this Question?

View Queries open

Question 23 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company hosts a web application which is load balanced (2 Web Servers and 2 App Servers).The application uses Azure SQL Database, to avoid accidental deletion of the Database, a ReadOnly lock is applied on the Database. An application user wants to update a transaction through the Web application, which following is a valid action?

A. An update transaction is not allowed since ReadOnly lock is applied on the Database

B. An update transaction is a valid action

C. Only Select statements are valid, Update\Delete actions are invalid

D. Only Select/Delete statements are valid, Update action is invalid

Explanation:

Answer: B

Option A is incorrect because transactions are allowed, locks apply only to operations in the management plane

Option B is CORRECT because transactions are allowed though locks are applied, please refer the url below

Option C is incorrect because SELECT\UPDATE\DELETE statements are valid

Option D is incorrect because SELECT\UPDATE\DELETE statements are valid

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Ask our Experts Rate this Question?

View Queries open

Question 24 **Unattempted**

Domain :Describe identity, governance, privacy, and compliance features

A company wants to integrate their ITSM tool Service Now with Azure and create incidents automatically for the Azure Advisor recommendations, what is the best way of achieving this in Azure?

A. **Cannot integrate Azure Advisor with ITSM Tool**

B. **Integrate with ITSM tool using Logic App**

C. **Integrate with ITSM tool using Azure Function**

D. **Integrate with ITSM tool using ITSM Connector**

Explanation:

Answer: D

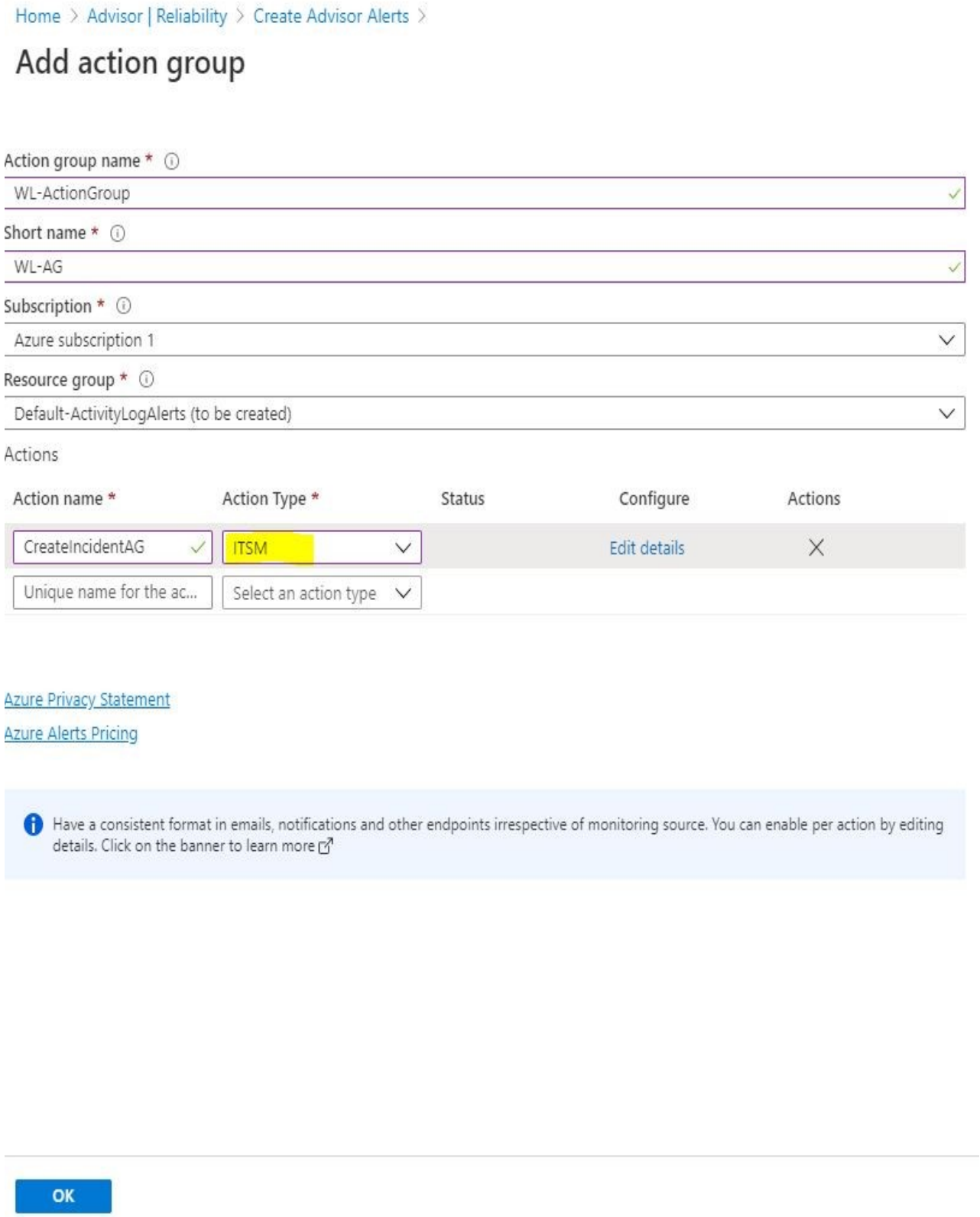
Option A is incorrect because connector exists for integration between Azure and specific ITSM tools

Option B is incorrect because it requires custom development to achieve the integration

Option C is incorrect because it requires custom development to achieve the integration

Option D is CORRECT because ITSM Connector exists to integrate Azure with Service Now

Diagram:



Reference:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/Microsoft.ITSMConnector?tab=Overview

Ask our Experts Rate this Question?

View Queries open

Question 25 **Incorrect**

Domain :Describe identity, governance, privacy, and compliance features

A company plans to deploy multiple resources using Azure Blueprints. While creation of the BluePrint by the administrator, what are the Lock Assignment options available when assigning a BluePrint?

A. **Don't Lock; Do Not Delete; Read Only**

B. **Not Locked; Cannot Edit/Delete; Read Only; Cannot Delete**

✓ C. **Delete; ReadOnly**

D. **Update; ReadOnly**

Explanation:

Answer: A

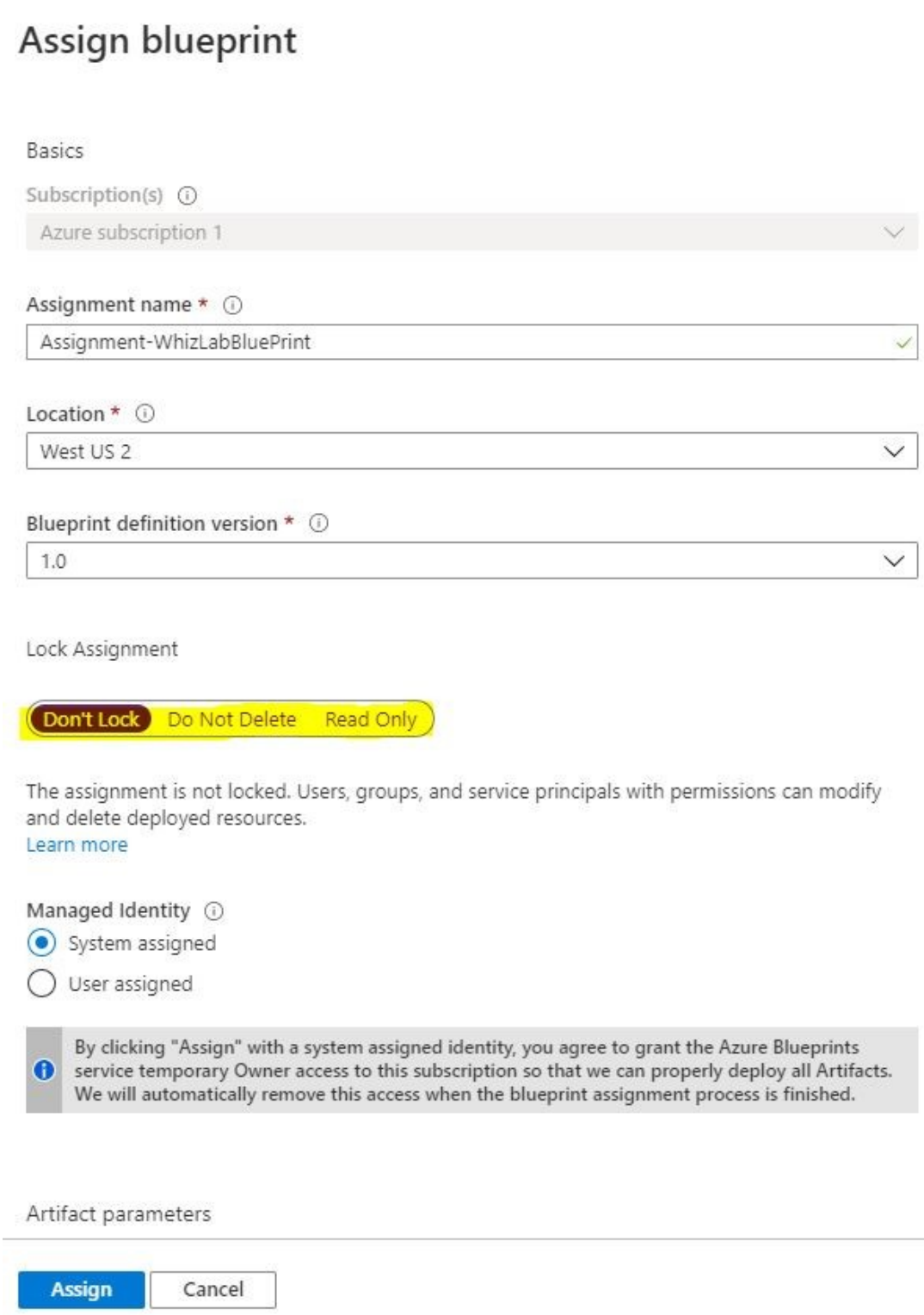
Option A is CORRECT because please see the diagram below

Option B is incorrect because these are the states of the resources and not modes

Option C is incorrect because these are the locks for the resources and not modes

Option D is incorrect because "Update" is an invalid lock option and ReadOnly is a lock on resource

Diagram:



Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

Ask our Experts

Rate this Question?

View Queries open

Finish Review