Microsoft.SC-100-KR.v2026-04-08.q141

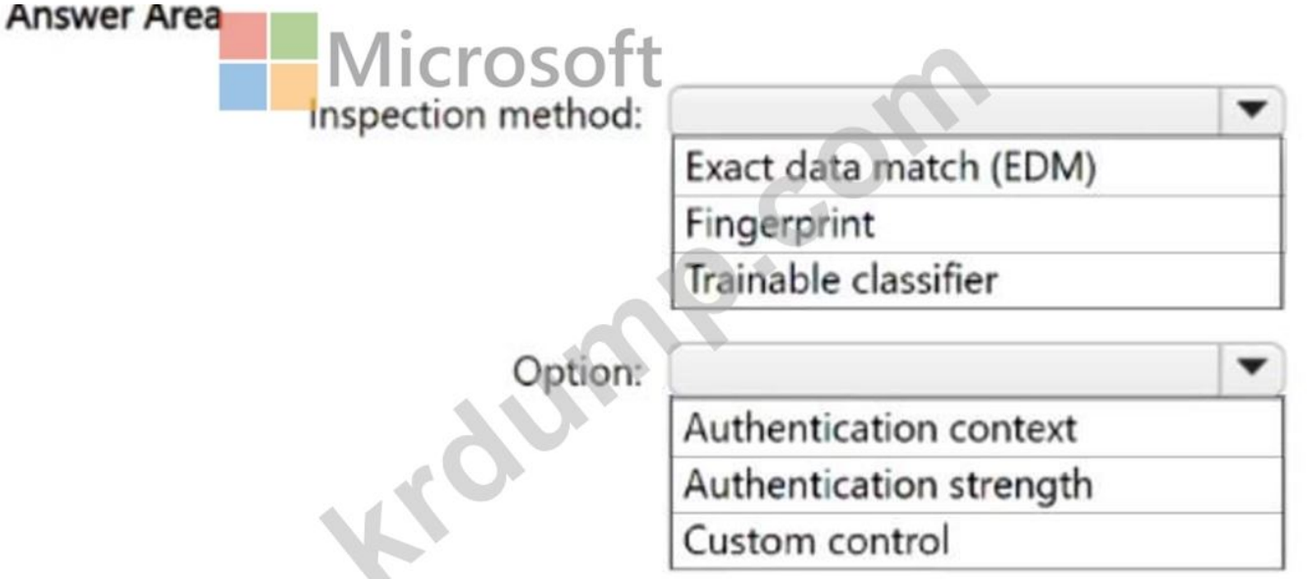
□□□□:	SC-100-KR
□□□□:	Microsoft Cybersecurity Architect (SC-100 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	141
□□:	v2026-04-08
# □□ □:	260
# □□ □□□:	1410
https://www.krdump.com/Microsoft.SC-100-KR.v2026-04-08.q141.html	

NEW QUESTION: 1
Azure □□, Amazon Web Services(AWS) □□, Google Cloud Platform(GCP) □□□ □□□ □□ □□□□ □□□ □□□□.
□□□ □□ □ □□ □□□ □□□ □□□□□.
□□ □□ □□□ □□□□ Compliance Manager □□□□ □□□□ □□□.
- □□□ □□□ □□□□ □□ □□ □□□ □□□□□.
□□ □□
- □□ □□□ □□□□ □□□□□□□.
- □□□ □□□ □□□□□□
□□□□ □□□ □□□□ □□□?
A. □□□□□ Microsoft Defender
B. □□ □□ □□□ □□□
C. □□□□ □□ Microsoft Defender
D. Microsoft Sentinel
Answer: A (LEAVE A REPLY)
Microsoft Purview, Configure cloud settings for use with Compliance Manager Compliance Manager integrates with Microsoft Defender for Cloud to provide multicloud support. Organizations must have at least one subscription within Microsoft Azure and then enable Defender for Cloud so that Compliance Manager can receive the necessary signals to monitor your cloud services. Once you have Defender for Cloud, you need to assign the relevant industry and regulatory standards to your subscriptions.
View available environments
1. In Defender for Cloud, select Environment settings on the left navigation.
2. View the available environments and subscriptions currently visible to MDC for your tenant. You may need to expand your management groups to view subscriptions, which you can do by selecting Expand all below the search bar. In addition to your Azure subscriptions, you'll also see

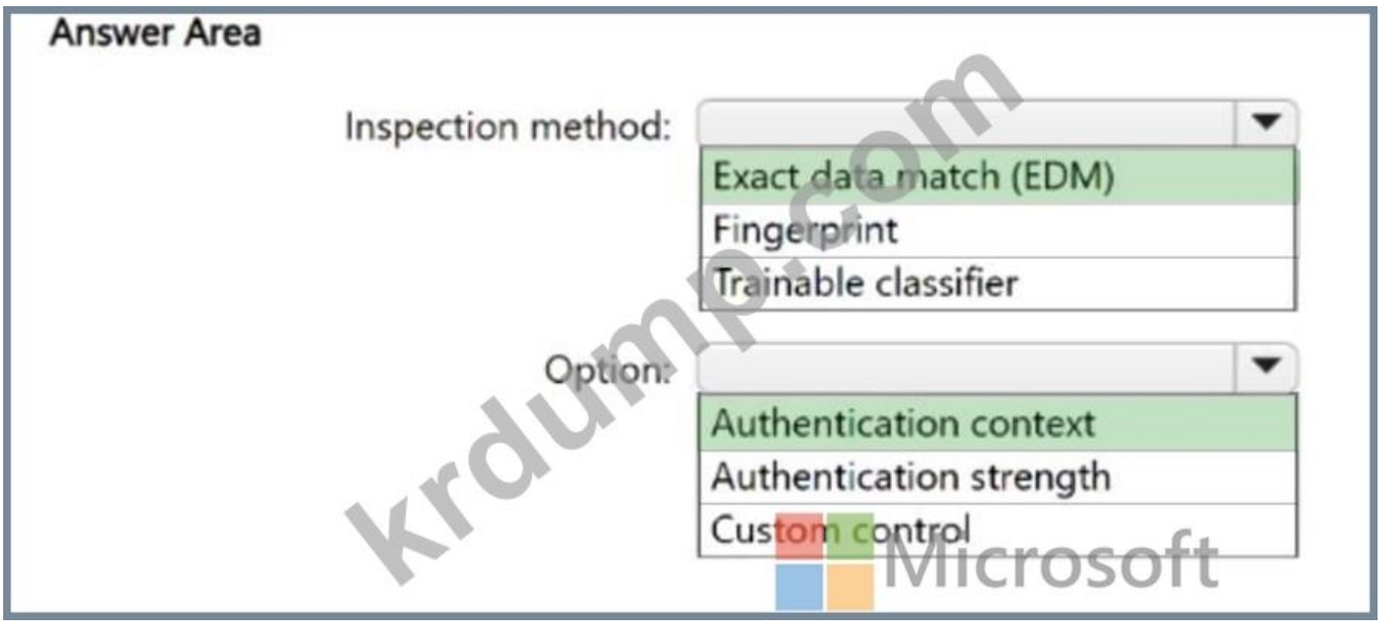
any Google Cloud Platform (GCP) projects or Amazon Web Services (AWS) accounts connected to Defender for Cloud.
Reference:
https://learn.microsoft.com/en-us/purview/compliance-manager-cloud-settings

NEW QUESTION: 2
□□□ □□
Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 □□□ □□□□. Site1□ □□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□ □□□ □□□□□.
Microsoft Defender for Cloud Apps □□ □□□ □□□□ Site1□ □□ □□□□ □□□□□□□.
□□□□ □□ □□□ □□□ □□□□ □□ □□□ □□□□□ □ □□□ □□□ □□□□□ □ □ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□ Microsoft □□□ □□ □□□ □□ □□□ □□□□ □□, □□ □□□ □□ □□□ □□□ □ □□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:



Explanation:

Box 1: Exact data match (EDM)

To trigger a Microsoft Defender for Cloud Apps session policy step-up authentication when a user downloads a document based on a predefined form, use the Data Classification Service (DCS) inspection method and select sensitive information type (SIT) or exact data match (EDM) as the inspection type. These options allow you to specify the type of sensitive information that should trigger the policy and potentially require step-up authentication.

Box 2: Authentication context

You will also need to define the authentication context in Microsoft Entra ID for the step-up authentication.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/dcs-inspection

NEW QUESTION: 3

□□□ □□

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type	Description
VNet1	Virtual network	Contains two subnets named Subnet1 and Subnet2
VM1	Virtual machine	Runs an app named App1 and is connected to Subnet1
DB1	Azure SQL Database	Contains data for App1 and is accessible from the internet

App1□ □□□ □□□□ □□ □□□□ □□□ □□□. □□□□ □□ □□ □□□ □□□□ □□ □.

- Subnet1□ □□□ □□ □□□ □□□□ □□□.

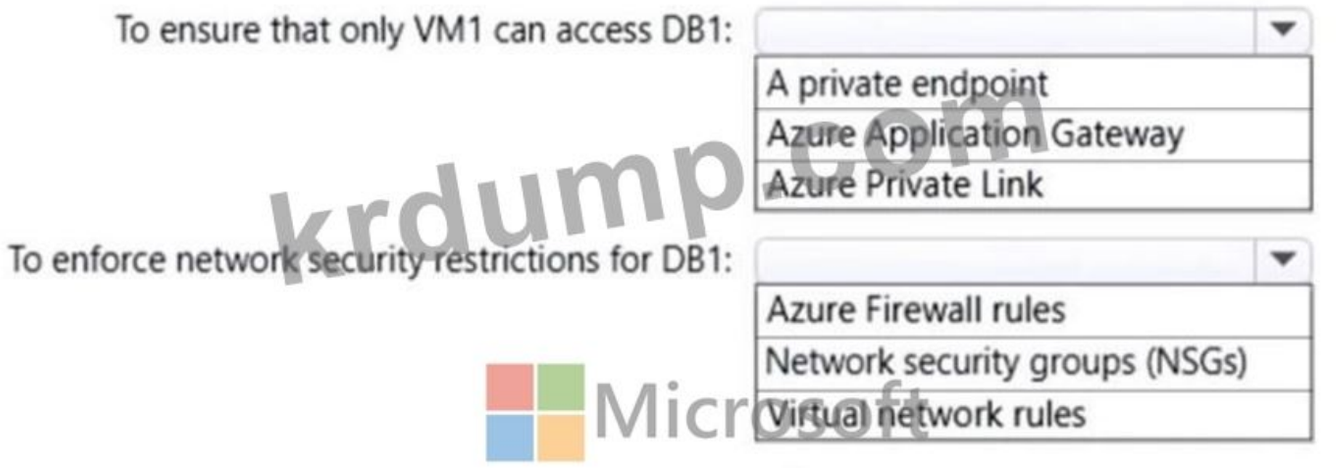
DB1□ □□□□□.

- DB1□ □□□□□ □□□ □ □□□ □□□.
- □□□ □□□□□ □□□.

□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□□□□.

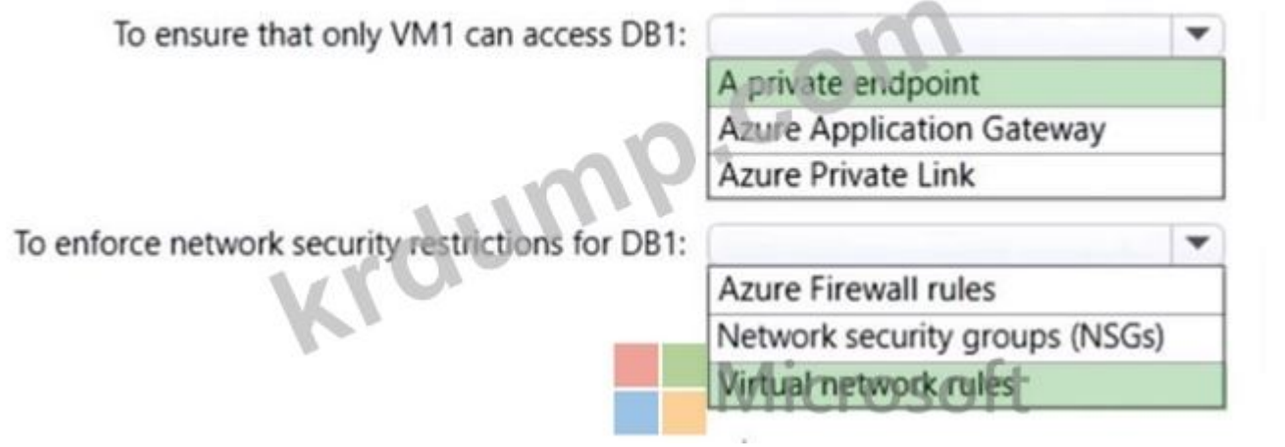
□□: □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:

To ensure that only VM1 can access DB1 - A private endpoint

A private endpoint provides a secure connection to your Azure SQL Database by creating a private IP address that is only accessible from your internal network (i.e., the virtual network connected to Subnet1), ensuring that the database is inaccessible from the internet.

To enforce network security restrictions for DB1 - Virtual network rules Virtual network rules allow you to control access to your Azure SQL Database by setting specific rules for which subnets or IP addresses can access the database. This option ensures that access to DB1 is restricted to VM1, and it prevents access from other machines or the internet.

NEW QUESTION: 4

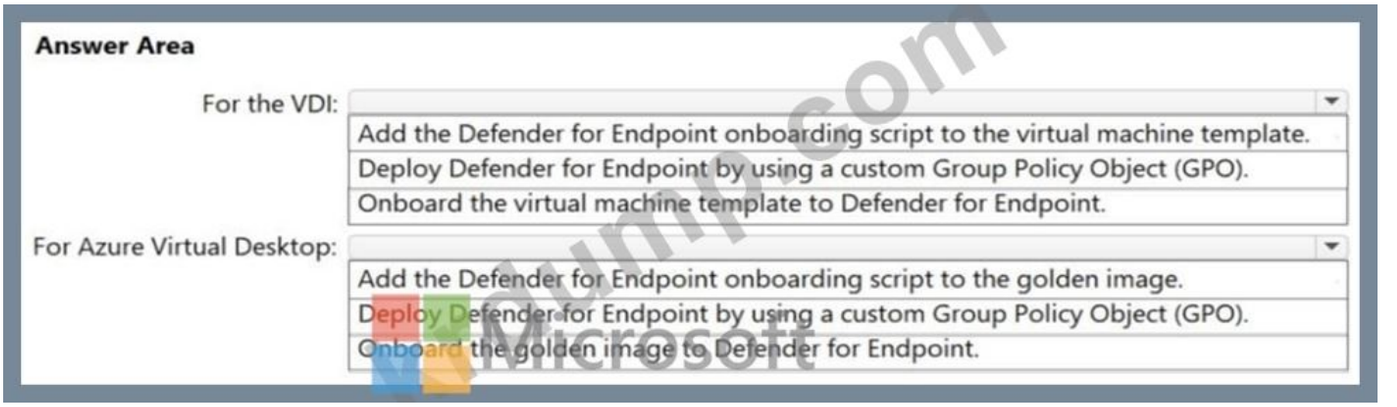
Active Directory □□□ □□□(AD DS) □□□□ □□□□□ Microsoft Entra □□□□ □□□□. □□□□□ □□□□ Windows□ □□□□ Microsoft Entra□ □□□□□□ □□□□ □□□□. □□□□□□□ □□□□□□ □□□□ □□ □□□ □□□□ □□□□. □ □□□ Microsoft □□ □□ □□□ □□□□.

Windows □□□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ Windows □□□□ □□ □□□ □□ □□□ □□□ □□ □□□□ □□□□ □□□□ □□□. □□ □□□□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □□ □□□ □□□ □□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□ □□□ □□□□ □□□(LAPS)
B. Microsoft Entra Identity Protection
C. Microsoft Entra □□ □□ ID □□(PIM)
D. □□ □□□ □□□□□□(PAW)
Answer: A (LEAVE A REPLY)
https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

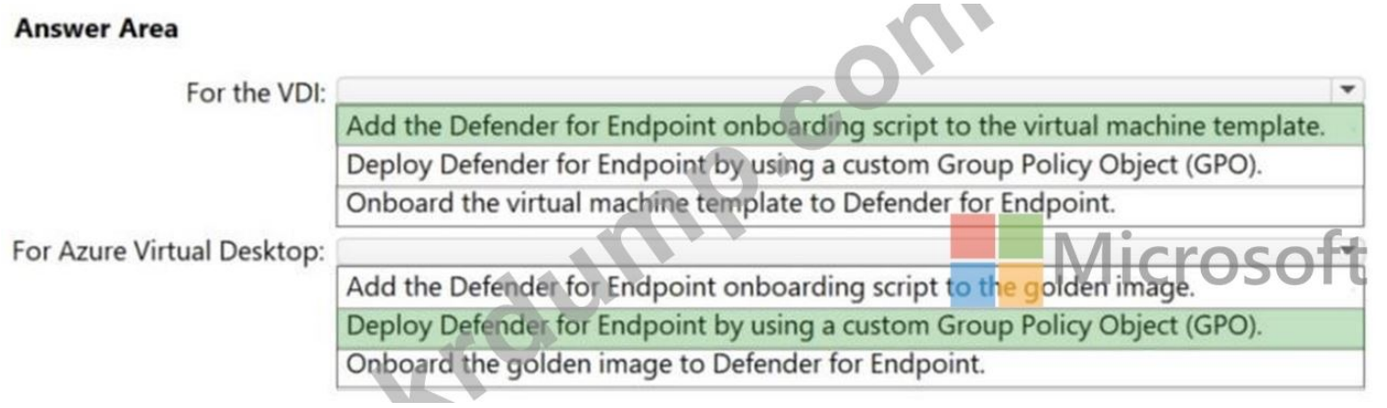
NEW QUESTION: 5
□□□ □□□□ Microsoft Defender for Cloud□ □□ □□□ □□□ □□□□ Azure □□□ □□ □□.
□□ □□□ □□ □□□ □□□ □□□□□□.
NIST 800-53 □□ □□□ □□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Defender for Cloud□□ Defender for Cloud □□□ □□□□□□.
B. Azure Policy□□ □□ □□□ □□ □□ □□ □□ □□□ □□□□□.
C. Azure Policy□□ □□ □□□ □□ □□ □□ □□□□□□ □□□□□.
D. Microsoft Defender for Cloud Apps□□ □□□□ □□□□□□□ □□ □□□ □□□ □□□ □.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
□□□ □□
□□ □□□□ □□□(VDI)□ □□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□.
VDI□ □□□ □□□□ □□□ □□ □□ □□□□ □□□□□.
VDI □□□ □□□□ □□□□□□.
Azure Virtual Desktop □□□ □□□ Azure □□□ □□□□. □ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□ □□ □□□□ □□□□. □□ Azure Virtual Desktop □□□ □□ Microsoft Entra Domain Services □□□□ □□□□□.
□□□□ Microsoft Defender for Endpoint□ □□□□ □□ □□□□ □□□□ □□□. □□ □□ □□ □□ □□ □□□ □□□□ □□□.
- □□□□ Endpoint□ Defender□ □□□□□□□ □□□□□□.
□ □□ □□ □□□.
- Microsoft Defender □□□ □□□ □ VDI □□□□ □□ □□ □□□ □□□□ □□□ □□□□ □.

- □□□ □□□ □□□□□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



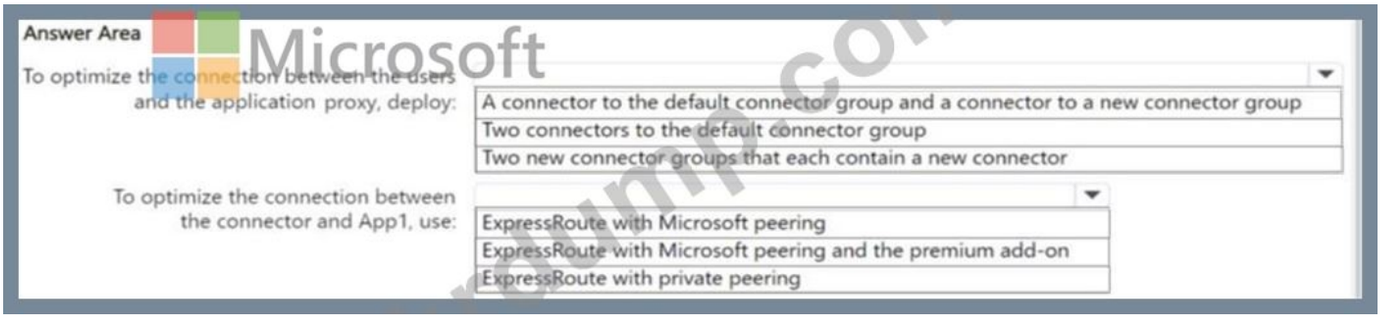
Answer:



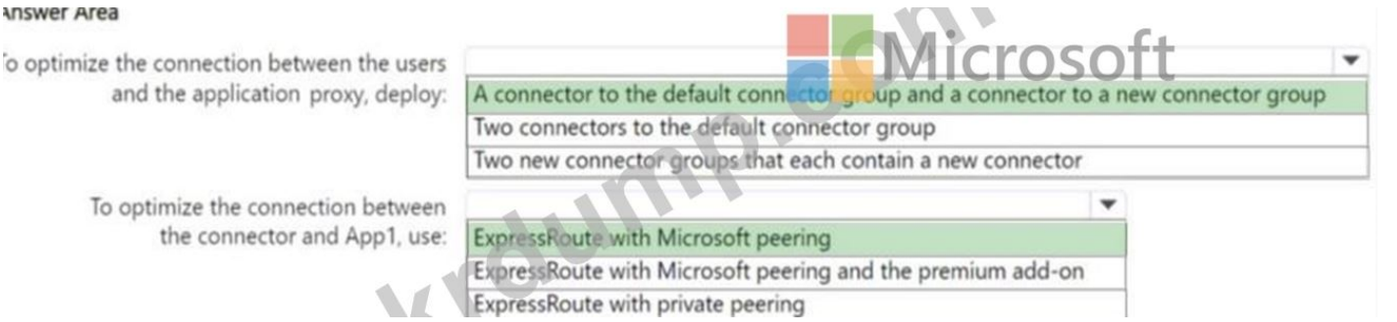
Explanation:
https://learn.microsoft.com/en-us/defender-endpoint/configure-endpoints-vdi

NEW QUESTION: 7
□□□ □□
□□□ □□□□ □□□□□□□ □□□□ □□ □□□□.
□□ □ □□□□□ App1□□□ □□□□□ □□ □□□□.
Azure □□□ □□□□. □ □□□ □□□ □□□□ Microsoft Entra □□□□ □□□□ □□□□.
Microsoft Entra Private Access□ □□□□ □□□□□□ □□□ □□□□ App1 □□□□ □□□ □□□□□. □□ □□□ □□□□ Private Access□ □□□□□.
- □□ □ □□□□□ ExpressRoute □□□ □□□□□.
□□ □□□ □□□ □□.
- □□ □□ Azure□ VNet1□□□ Azure □□ □□□□□ □□□□.
□□.
- VNet1□ Microsoft Entra □□□□□□ □□□ □□□□ □□□□□.
□□□ □□□ □□ □□□□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- App1□ □□ □□□ □□ □□□□ □□□□□□.
- App1□ □□□ □ □□□□ □□□ □□□□□□.
- □□□□ □□□□□□.
- □□□ □□□□□□.

□□□ □□□ □□□□ □□□? □□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: A connector to the default connector group and a connector to a new connector group To optimize the connection between the users and the application proxy, deploy:

Application proxy uses the same connector as Microsoft Entra Private Access. The connector is called Microsoft Entra private network connector.

If you install connectors in different regions, you should optimize traffic by selecting the closest application proxy cloud service region with each connector group.

Box 2: Expressroute with Microsoft peering

To optimize the connection between the connector and App1, use:

Note: For the best performance, connect your organization to Microsoft with Express Route.

General approach to minimize latency

Minimize the latency of end-to-end traffic by optimizing each network connection.

* Reduce the distance between the two ends of the hop.

* Choose the right network to traverse. For example, traversing a private network rather than the public internet could be faster, due to dedicated links.

Consider using a dedicated VPN or ExpressRoute link between Microsoft and your corporate network.

Focus your optimization strategy

There's little that you can do to control the connection between your users and the application proxy service. Users access your apps from a home network, a coffee shop, or a different region. Instead, you can optimize the connections from the application proxy service to the private network connectors to the apps. Consider incorporating the following patterns in your environment.

Reference:

https://learn.microsoft.com/en-us/entra/identity/app-proxy/application-proxy-network-topology

NEW QUESTION: 8

□□□ □□

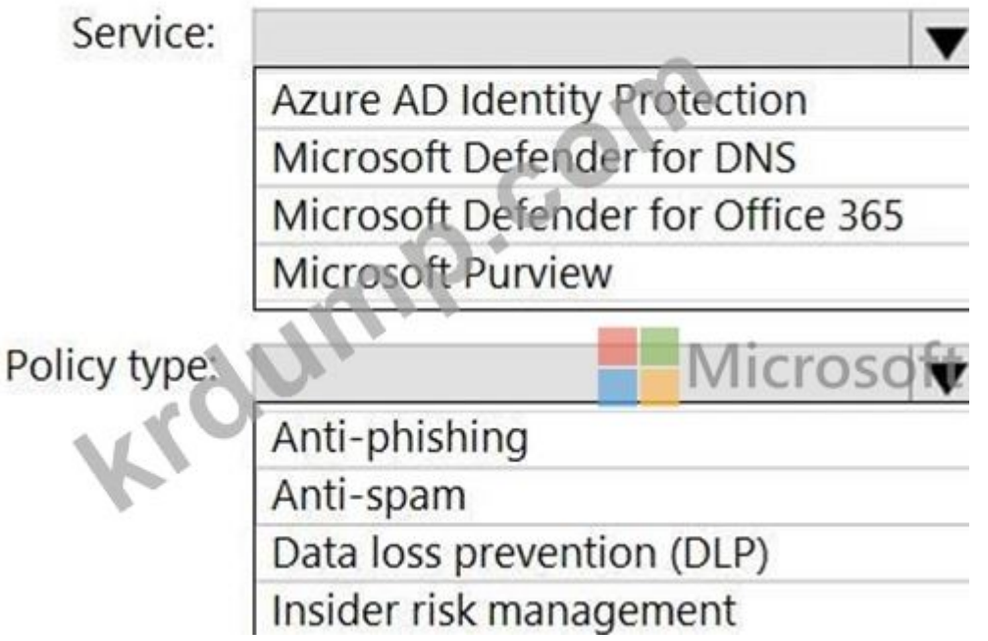
Microsoft Exchange Online□ □□□□ Microsoft 365 E5 □□□ □□□□.

□□□□ □□□□ □□ □□□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□□ □□□□ □□□.

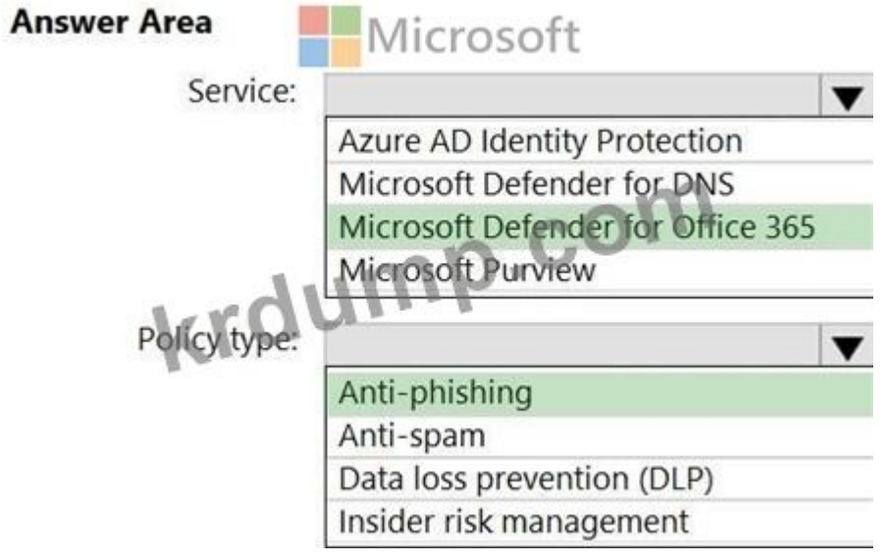
□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area



Answer:



NEW QUESTION: 9

□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□

□□□. □□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□ □□□ □□ □□□ □ □□□□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□ □ □□□□.
Microsoft Defender XDR□ □□□□ Microsoft 365 □□□ □□□□. □ □□□□ Microsoft Intune □ □□□ □□□□ 500□□ □□□□ □□□□. □□, □ □□□□ □□□□□ □□□□ □□ SaaS(Software as a Service) □□ □□□□ □□□ 500□□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□□□ □□□□ □□□.
* Microsoft□□ □□□□□ □□□ SaaS □□ □□ □□□ □□□□ □□□□□.
* Microsoft□□ □□□□□ □□□ SaaS □□ □□ □□□ □□□□ □□□□□.
□□ □□: Intune□□ □ □□ □□□ □□□□ □□□ □□□ □□□ □□□□.
□□□ □□□ □□□□□?

A. □□□

B. □

Answer: (SHOW ANSWER)

NEW QUESTION: 10
□□□ Azure Active Directory(Azure AD)□□ □□□ □□ □□□□□□ □□□□□□□□ □□ □□□ □□ □□□□□□□ □□□□□. □□ □□ □□□ □□ □□□□ □□□□□□□ □□□ □ □□□□ □□ □□□□ □□□□ □□□. □□□ □□□ □□□□ □□□?

A. □□□□ □□ Microsoft Defender□ □□ □□

B. Azure AD Identity Protection□ □□□ □□ □□

C. Microsoft Endpoint Manager□ □□ □□ □□

D. Azure AD □□□ □□□ □□

E. Azure AD Identity Protection□ □□□ □□ □□

Answer: D (LEAVE A REPLY)

You create the app and then set the locations and create a Conditional Access policy based on locations.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location
https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules

NEW QUESTION: 11
□□□ □□
Azure □□□ □□□□.
Azure Synapse Analytics SQL □□ □□ SQL Serverless □□ □□□ □□□□□.
□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□. □ □ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□.

□ □□□ □□□ □□ □□□ □□□□ □□□? □□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Serverless SQL pool:
- Azure Storage infrastructure encryption and Microsoft-managed keys
- Transparent Data Encryption (TDE) and customer-managed keys
- Transparent Data Encryption (TDE) and Microsoft-managed keys

Dedicated SQL pool:
- Azure Storage infrastructure encryption and Microsoft-managed keys
- Transparent Data Encryption (TDE) and customer-managed keys
- Transparent Data Encryption (TDE) and Microsoft-managed keys

Answer:

Answer Area

Serverless SQL pool:
- Azure Storage infrastructure encryption and Microsoft-managed keys
- Transparent Data Encryption (TDE) and customer-managed keys
- Transparent Data Encryption (TDE) and Microsoft-managed keys

Dedicated SQL pool:
- Azure Storage infrastructure encryption and Microsoft-managed keys
- Transparent Data Encryption (TDE) and customer-managed keys
- Transparent Data Encryption (TDE) and Microsoft-managed keys

Explanation:
Box 1: Transparent Data Encryption (TDE and customer-managed keys
SQL serverless pools
Encryption of data at rest
A complete Encryption-at-Rest solution ensures the data is never persisted in unencrypted form. Double encryption of data at rest mitigates threats with two, separate layers of encryption to protect against compromises of any single layer. Azure Synapse Analytics offers a second layer of encryption for the data in your workspace with a customer-managed key. This key is safeguarded in your Azure Key Vault, which allows you to take ownership of key management and rotation.
The data in the following Synapse components is encrypted with the customer-managed key configured at the workspace level:
SQL pools
*-> Dedicated SQL pools
*-> Serverless SQL pools

Data Explorer pools
Apache Spark pools
Azure Data Factory integration runtimes, pipelines, datasets.
Box 2: Transparent Data Encryption (TDE and customer-managed keys
Azure Synapse Analytics SQL dedicated pools
Secure a dedicated SQL pool (formerly SQL DW) in Azure Synapse Analytics Encryption
Transparent Data Encryption (TDE) helps protect against the threat of malicious activity by encrypting and decrypting your data at rest. When you encrypt your database, associated backups and transaction log files are encrypted without requiring any changes to your applications. TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key.
Customer-managed transparent data encryption - Bring Your Own Key
Customer-managed TDE is also referred to as Bring Your Own Key (BYOK) support for TDE. In this scenario, the TDE Protector that encrypts the DEK is a customer-managed asymmetric key, which is stored in a customer-owned and managed Azure Key Vault (Azure's cloud-based external key management system) and never leaves the key vault.
Reference:
https://learn.microsoft.com/en-us/azure/synapse-analytics/security/workspaces-encryption
https://learn.microsoft.com/en-us/azure/synapse-analytics/sql-data-warehouse/sql-data-warehouse-overview-manage-security
https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview

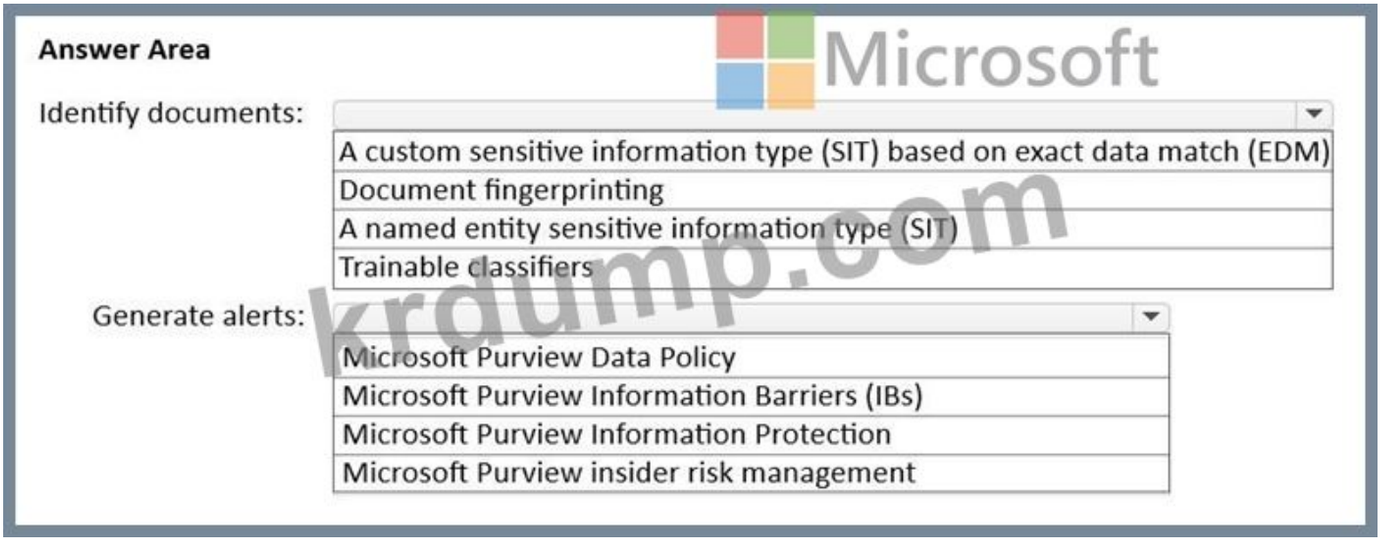
NEW QUESTION: 12
Azure □□□ □□□□.
Azure DevOps□ □□□□ Azure App Services □□ □□□ □□□□□.
□□□ □□ Microsoft □□□□ □□ □□□□(MCSB) □□ □□□ □□□□□ □□□□ □□□ □ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft Defender for Cloud□ DevOps □□
B. □ □□□□ Microsoft Defender
C. Azure □□
D. Azure DevOps□ □□ □□
Answer: (SHOW ANSWER)
This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to App Service. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to App Service. You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud portal page.

When a feature has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance with the Microsoft cloud security benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.
Reference:
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

NEW QUESTION: 13
contoso.com□□□ Microsoft Entra □□□□ □□ Microsoft Intune□ □□□□ □□□□.
contoso.com□ □ □□□□ Microsoft Entra ID P1 □□□□□ Global Secure Access □□□□□ □ □□□ Windows 11 □□□ □□□□ □□□□.
□□ Microsoft Entra Internet Access □□□ □□□ □□□□□.
- □□ □□□□ □□□□□□.
- □□□□□ 300□ Profile1□□□ □□ □□□□ □□□□.
□□□ □□ □ □□□ □□□ □□□ □□□□ □□□□.
WCFPolicy1. □□□ □□ WCFPolicy1□ □□□□□.
- □□□ □□□ □□□□□.
- FQDN(□□□□ □□□ □□)□ □□ □□ □□□ □□□□□.
*.adatum.com□ □□□□□. Profile1□ □□□ □□□□ □□□□□.
CAPolicy1□□□ □□□ □□□ □□ □□□□□ CAPolicy1□ □□□□ □□□ □□□ □□□□ □.
□□□□ □□□ □□□ □□□□ □□ □.
□□□ □□□ □□ □□□□ □□□□ □□□ □□□ □□□□ □□□.
- https://www.adatum.com:8433
- https://www.fabrikam.com
□□ □ □□ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. https://www.fabrikam.com□□□ □□□□ □□ □□□□ □□□□□.
B. https://www.adatum.com:8433□□□ □□□□ □□ □□□□ □□□□□.
C. □□ □□□□ https://www.adatum.com:8433□□□ □□□□ □□□□□.
D. https://www.fabrikam.com□□□ □□□□ □□□ □□□□ □□□□□ □□□□□.
E. https://www.adatum.com:8433□□□ □□□□ □□□ □□□□ □□□□□ □□□□□.
F. https://www.fabrikam.com□□□ □□□□ □□□ □□□□ □□ □□□□□ □□□□□.
Answer: B,D (LEAVE A REPLY)
Traffic to https://www.adatum.com:8433:
In WCFPolicy1, the only rule specifies *.adatum.com as the allowed domain but without specifying a particular port.
Typically, web content filtering applies only to standard HTTP/HTTPS traffic (ports 80 and 443). Since this traffic is over port 8433, which is nonstandard, it would not match the allow rule in WCFPolicy1. Thus, it will be blocked from all devices.

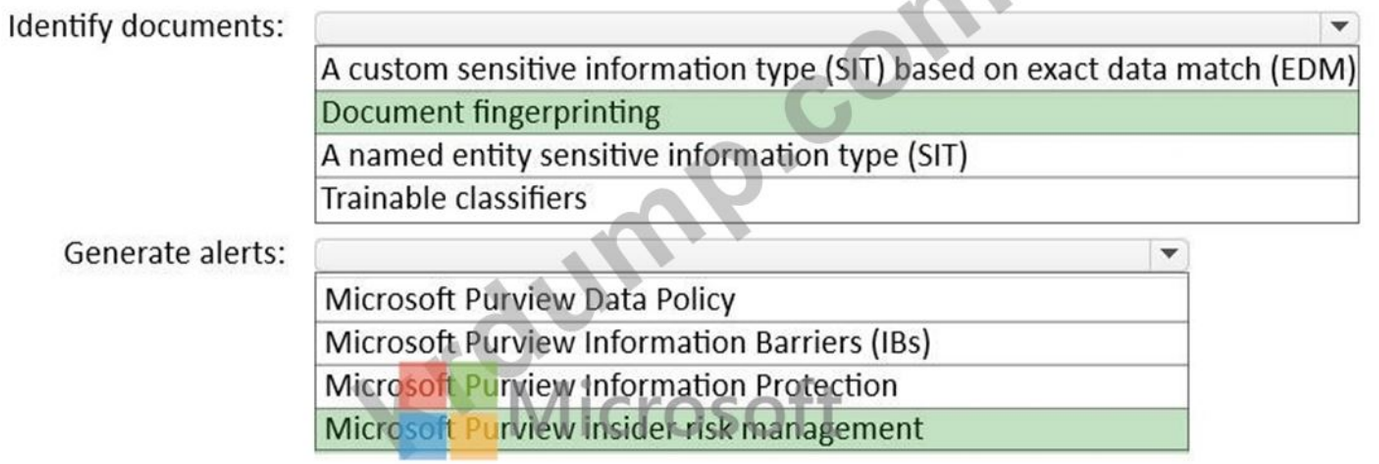
Traffic to https://www.fabrikam.com:
Since there is no rule in WCFPolicy1 to specifically allow or block traffic to fabrikam.com, the Conditional Access policy CAPolicy1 will govern access.
CAPolicy1 is configured to grant access only if a user's device is compliant. Therefore, traffic to https://www.fabrikam.com will be allowed only from compliant devices

NEW QUESTION: 14
□□□ □□
Azure □□□ □□□□. □ □□□□ □□ □□□□ □□□□ DB1□□□ Azure SQL □□□□□ □□ □□□□ □□□□.
Microsoft SharePoint Online, OneDrive □ Teams□ □□□□ Microsoft 365 □□□ □□□□.
□□□□ □□ DB1□ □□□□ □□□ Microsoft Office □□□ □□□□.
□□ □□ □□□ □□□□ Microsoft Purview □□□□ □□□□ □□□.
- DB1□□ □□□□ □□ □□ □ □□□□□ □□□ Office □□□ □□□□□.
- □□□□ □□ □□□ □□ □□□ □□□□□□ □□□ □□□□□.
DB1□ □□□□ □□□ □□
- □□ □□□ □□ □□□□□□.
□ □□ □□□ □□ □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Answer Area



Explanation:

Box 1: Document fingerprinting

Identifies Office documents that contain customer addresses and phone numbers sourced from DB1 Document fingerprinting is a Microsoft Purview feature that takes a standard form that you provide and creates a sensitive information type (SIT) based on that form. Document fingerprinting makes it easier for you to protect sensitive information by identifying standard forms that are used throughout your organization.

Document fingerprinting includes the following benefits:

SITs created from document fingerprinting can be used as a detection method in DLP policies scoped to Exchange, SharePoint, OneDrive, Teams, and Devices.

Etc.

Box 2: Microsoft Purview insider risk management

Generates an alert if a user downloads an above average number of files that contain data from DB1 Microsoft Purview, Configure intelligent detections in insider risk management Use can use the Intelligent detections setting in Microsoft Purview Insider Risk Management to:

* Boost the score for unusual file download activities by entering a minimum number of daily events.

* Etc.

File activity detection

You can use this section to specify the number of daily events required to boost the risk score for download activity that's considered unusual for a user. For example, if you enter "25", if a user downloads 10 files on average over the previous 30 days, but a policy detects that they downloaded 20 files on one day, the score for that activity won't be boosted even though it's unusual for that user because the number of files they downloaded that day was less than 25.

Reference:

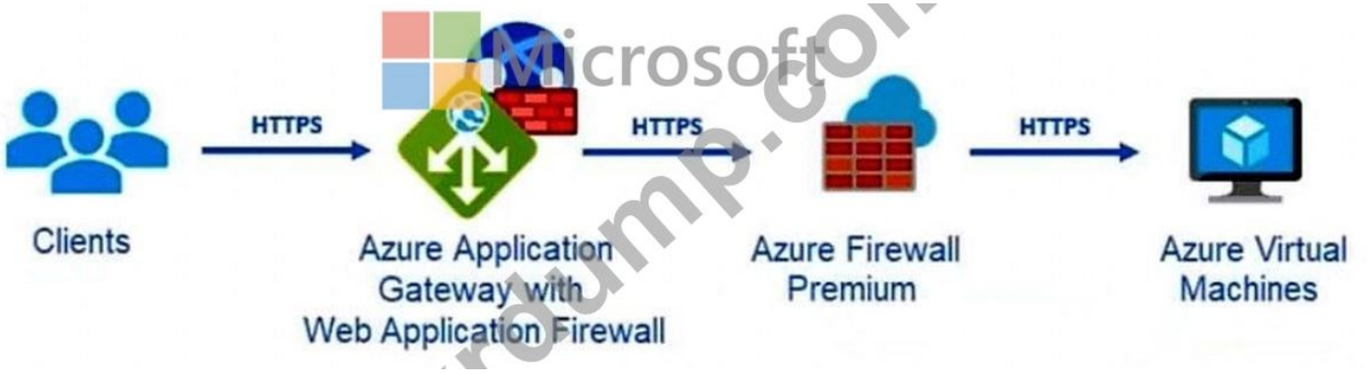
https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting

https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-intelligent-detections

NEW QUESTION: 15

□□□ □□

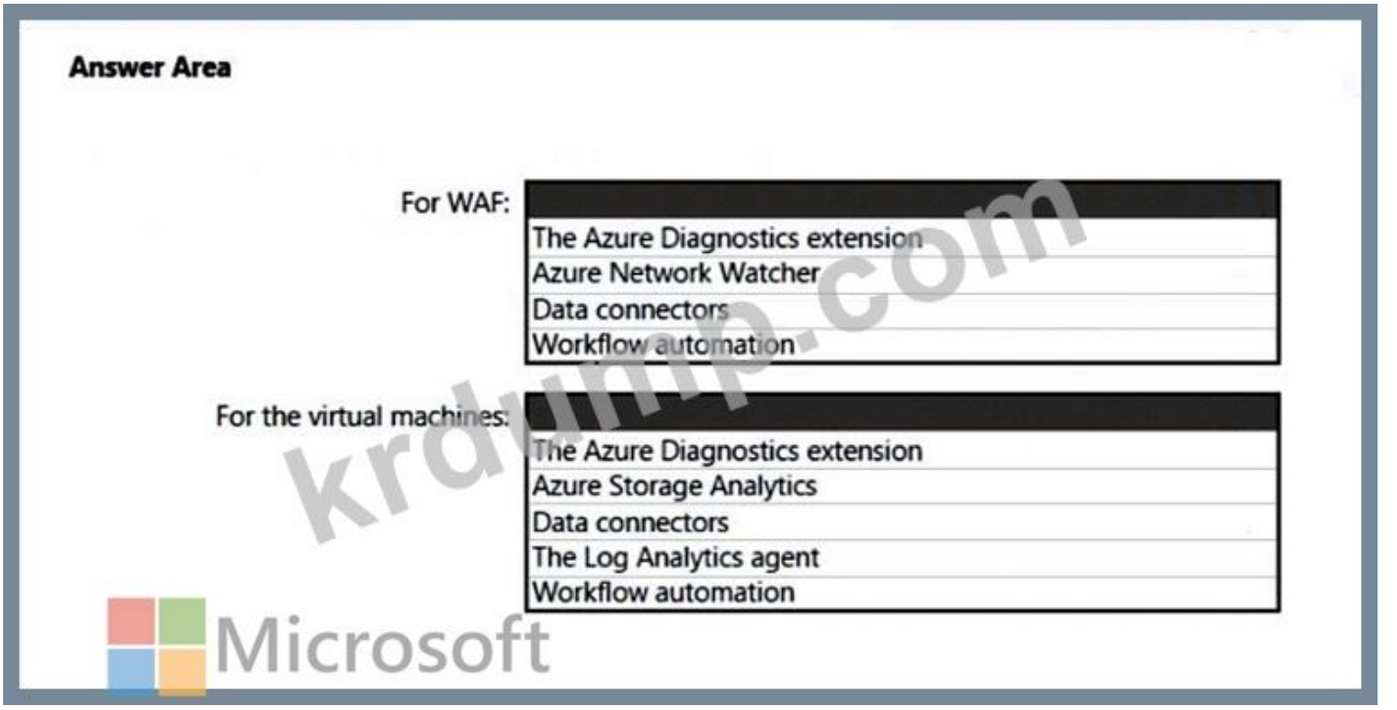
□□□ Microsoft Defender for Cloud□ Microsoft Sentinel□ □□□□ □□□□. □□□ □□ □□ □ □□ □□□□□ □□ □□□□□□□ □□□□ □□□□.



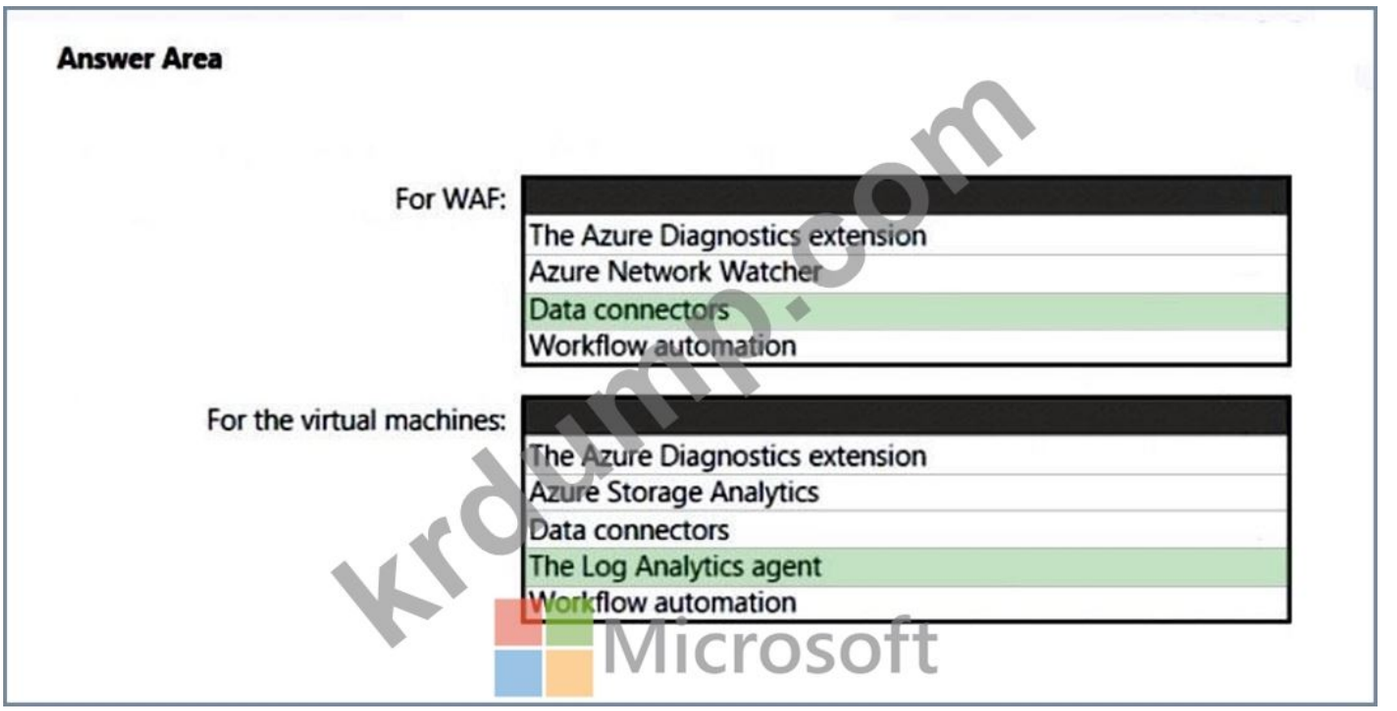
□□□ □□□□□ □□ □□ □ □□ □□□□ □□□□ □□□□. □□□□ □□ □□ □□□ □ □□□ □□□.

- Azure □ □□□□□□ □□□(WAF) □□□ Microsoft□ □□ □□.
- Defender for Cloud□ □□□□ □□ □□□ □□□ □□□□□.

□□□ □□□ □□□□ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Data connectors

Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel.

Launch a WAF workbook (see step 7 below)

The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource.

To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:

1. Select Diagnostic settings.
2. Select + Add diagnostic setting.
3. In the Diagnostic setting page (details skipped)
4. On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.
5. Select an already active workspace or create a new workspace.
6. On the left side panel under Configuration select Data Connectors.
7. Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.
8. Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven't done so previously.
9. Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent

Use the Log Analytics agent to integrate with Microsoft Defender for cloud.

Windows agents

	Azure Monitor agent	Diagnostics extension (WAD)	Log Analytics agent
Environments supported	Azure Other cloud (Azure Arc) On-premises (Azure Arc) Windows Client OS (preview)	Azure	Azure Other cloud On-premises
Agent requirements	None	None	None
Data collected	Event Logs Performance File based logs (preview)	Event Logs ETW events Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs Performance File based logs IIS logs Insights and solutions Other services
Data sent to	Azure Monitor Logs Azure Monitor Metrics[1]	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs
Services and features supported	Log Analytics Metrics explorer Microsoft Sentinel (view scope)	Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel

The Log Analytics agent is required for solutions, VM insights, and other services such as Microsoft Defender for Cloud.

Note: The Log Analytics agent in Azure Monitor can also be used to collect monitoring data from the guest operating system of virtual machines. You may choose to use either or both depending on your requirements.

Azure Log Analytics agent

Use Defender for Cloud to review alerts from the virtual machines.

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends collected data to your Log Analytics workspace in Azure Monitor.

Incorrect:

The Azure Diagnostics extension does not integrate with Microsoft Defender for Cloud.

Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel

https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

NEW QUESTION: 16

□□ □□□□ □□ □□(NSG), □□ □□ □□ □ bastion1□□□ Azure Bastion □□□□ □□□ Azure □□□ □□□□.
□□ NSG□□ bastion1□ □□□□ □□ □□□ □□ □□ RDP □□□□ □□□□ □□□ □□ □□ □□□□.
□□ □□□ bastion1□ □□□□ □□□□ □ □□□ □□ □□□. □□□□ NSG □□□ □□□ □ bastion1□ □□□□ □□ □□□□ □□□.
□□□□ □□□ □□□□ □□□?

A. Azure Virtual Network Manager □□ □□ □□
B. Azure Virtual Network Manager □□ □□
C. Azure Firewall □□□□□□ □□
D. Azure Firewall □□□□ □□

Answer: A (LEAVE A REPLY)

How security admin rules and network security groups (NSGs) are evaluated Security admin rules and network security groups (NSGs) can be used to enforce network security policies in Azure. However, they have different scopes and priorities.# Security admin rules are intended to be used by network admins of a central governance team, thereby delegating NSG rules to individual application or service teams to further specify security as needed. Security admin rules have a higher priority than NSGs and are evaluated before NSG rules.
NSGs, on the other hand, are used to filter network traffic to and from individual subnets or network interfaces. They're intended to be used by individual application or service teams to further specify security as needed. NSGs have a lower priority than security admin rules and are evaluated after security admin rules.
Security admin rules are currently applied at the virtual network level, whereas network security groups can be associated at the subnet and NIC level.
This table shows these differences and similarities:

Rule Type	Target Audience	Applied On	Evaluation Order	Action Types	Parameters
Security admin rules	Network admins, central governance team	Virtual networks	Higher priority	Allow, Deny, Always Allow	Priority, protocol, action, source, destination
Network security group rules	Individual teams	Subnets, NICs	Lower priority, after security admin rules	Allow, Deny	Priority, protocol, action, source, destination

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network-manager/concept-security-admins

NEW QUESTION: 17
Azure □□ □□ □□ □□□ □□□□ □□□□. □□□ □□□ □□ □□ □□ □ □□ □□ □□ □□ □□□ □□□□□.
* □□□□ □□□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□□.
* □□□□ □□□□□ □□□ □□ □□□□ □□ □□ □□□ □□□□□□.
□□ □ □□□ □□ □□ □ □□□□ □□ □□ □□□ □□□□□? □ □□□ □□□□ □□□ □□□□□. □□: □ □□□ 1□□□□.
A. □□□ □□□ □□ □□□□ □□□□ □□ □□ □□□□ Azure Blob □□□□ □□□□□.
B. Azure Key Vault Managed HSM□ □□□ □□ □□□□ □□□□ Azure SQL □□□□□□□ □□ □□□ □□□□ □□□□□.
C. Azure Key Vault □□□ HSM□ □□□□ □□□□ □□ □□ □□□□ Azure Files□ □□□□ □.
D. Microsoft□□ □□□□ □□ □□□□ □□□□ Azure SQL □□□□□□□ □□ □□□ □□ □□ □□□□□.
Answer: (SHOW ANSWER)
Customer provided keys (CPK) enables you to store and manage keys in on-premises or key stores other than Azure Key Vault to meet corporate, contractual, and regulatory compliance requirements for data security.
Reference:
https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service-encryption/

NEW QUESTION: 18
□□ □□□ □□ □□ □□ □□□□□□□ □□□ □, □□ □□ □□□□□ □□□ □□□?
A. □□□ □□□ □□□□□
B. □□ □□□□□□ □□ □□ □□□ □□□□
C. □□□□□ □□□ □□□□□
D. □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
When developing a security operations life cycle for managing threats, 'Stay informed with threat intelligence' is done at the threat analytics stage.

NEW QUESTION: 19
Azure □□□ □□□□.
□ □□□□ □□□□□ □ □□□ Azure Kubernetes Service(AKS) □□□□□ □□□ □□□□ □.
□□□□ □ □□□□ □□□ □□□□ □□□□ □□□□ □□□□ □□□.

□□□□□ □□□ □□□□ □□□?

A. Azure □□ □□ □□

B. Azure □□□□□□ □□□□□

C. Azure □□

D. Azure □□□

Answer: (SHOW ANSWER)

Use Application Gateway Ingress Controller (AGIC) with a multitenant Azure Kubernetes Service. In this solution, Azure Web Application Firewall (WAF) provides centralized protection for web applications deployed on a multi-tenant Azure Kubernetes Service (AKS) cluster from common exploits and vulnerabilities.

Web applications running on Azure Kubernetes Service (AKS) cluster and exposed via the Application Gateway Ingress Controller (AGIC) can be protected from malicious attacks, such as SQL injection and cross-site scripting, by using a WAF Policy on Azure Application Gateway.

WAF policy on Azure Application Gateway comes pre-configured with Open Worldwide Application Security Project (OWASP) core rule sets and can be changed to other supported OWASP Core Rule Set (CRS) versions.

Reference:

https://learn.microsoft.com/en-us/azure/architecture/example-scenario/aks-agic/aks-agic

NEW QUESTION: 20

□□□ □□

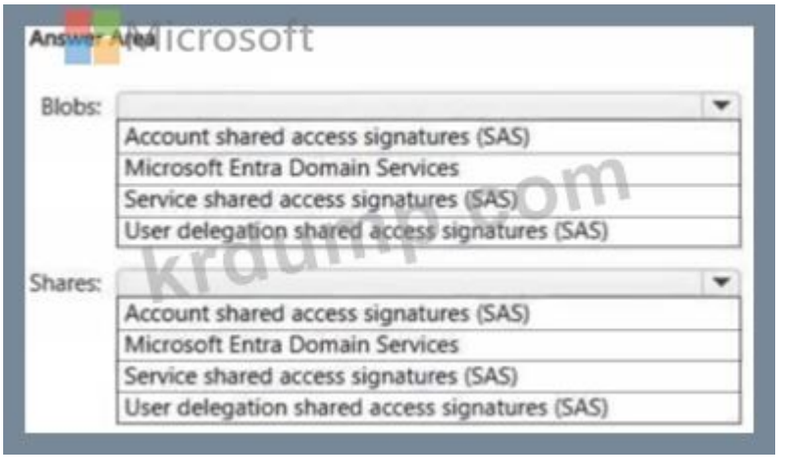
□□ Azure Storage Blob□ Azure Files □□□ □□□ Azure □□□ □□□□.

Blob □ □□ □□□ □□ □□□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□. □□ □□ □□ □□ □□ □□□ □□□□ □□□.

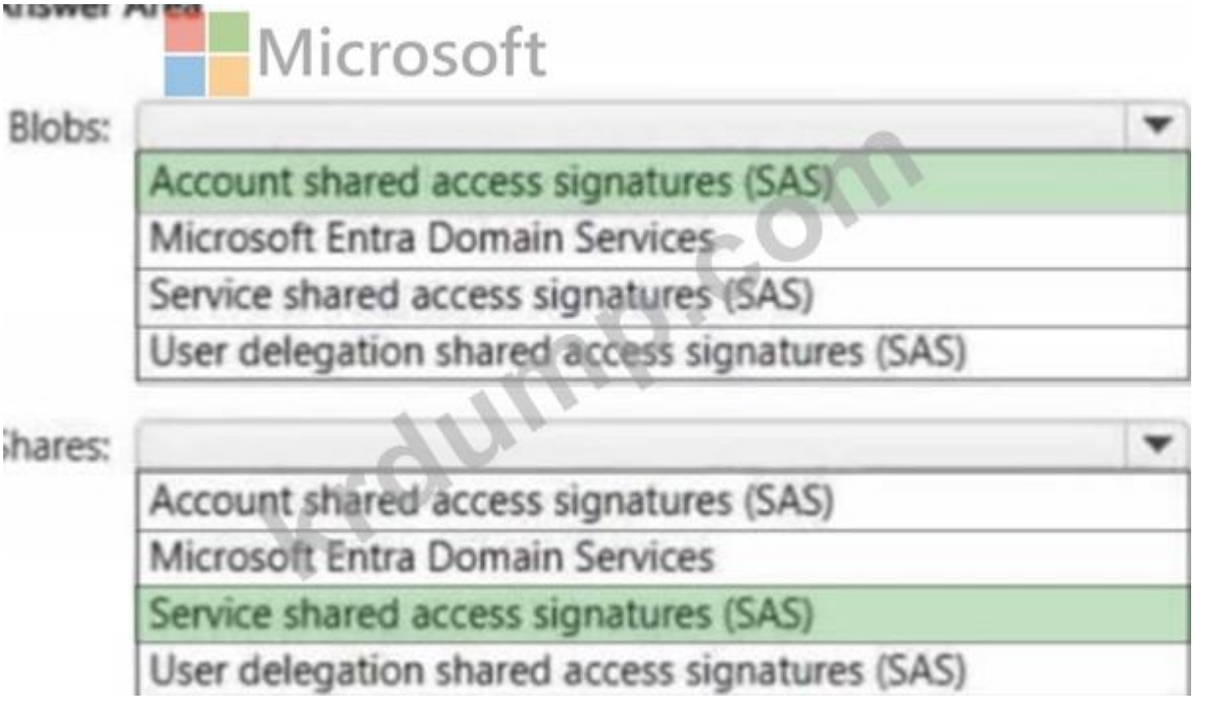
- SMB □□□□□ □□□□ □□□ □□ □□□□ □□□□□.
- □□□ □□ □□□ □□ □□□□ □□□□□.
- □□□□ □□ □□□ □□□□□.

□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Account shared access signature (SAS)

Azure Storage blobs

Limit access to the blobs to specific periods of time

Account SAS

An account SAS is secured with the storage account key. An account SAS delegates access to resources in one or more of the storage services. All of the operations available via a service or user delegation SAS are also available via an account SAS.

Box 2: Service shared access signature (SAS)

Azure Files shares

Support access to the shares by using the SMB protocol.

A shared access signature can take one of the following two forms:

* Ad hoc SAS. When you create an ad hoc SAS, the start time, expiry time, and permissions are specified in the SAS URI. Any type of SAS can be an ad hoc SAS.

*-> Service SAS with stored access policy. A stored access policy is defined on a resource container, which can be a blob container, table, queue, or file share. The stored access policy can be used to manage constraints for one or more service shared access signatures. When you associate a service SAS with a stored access policy, the SAS inherits the constraints--the start time, expiry time, and permissions--defined for the stored access policy.

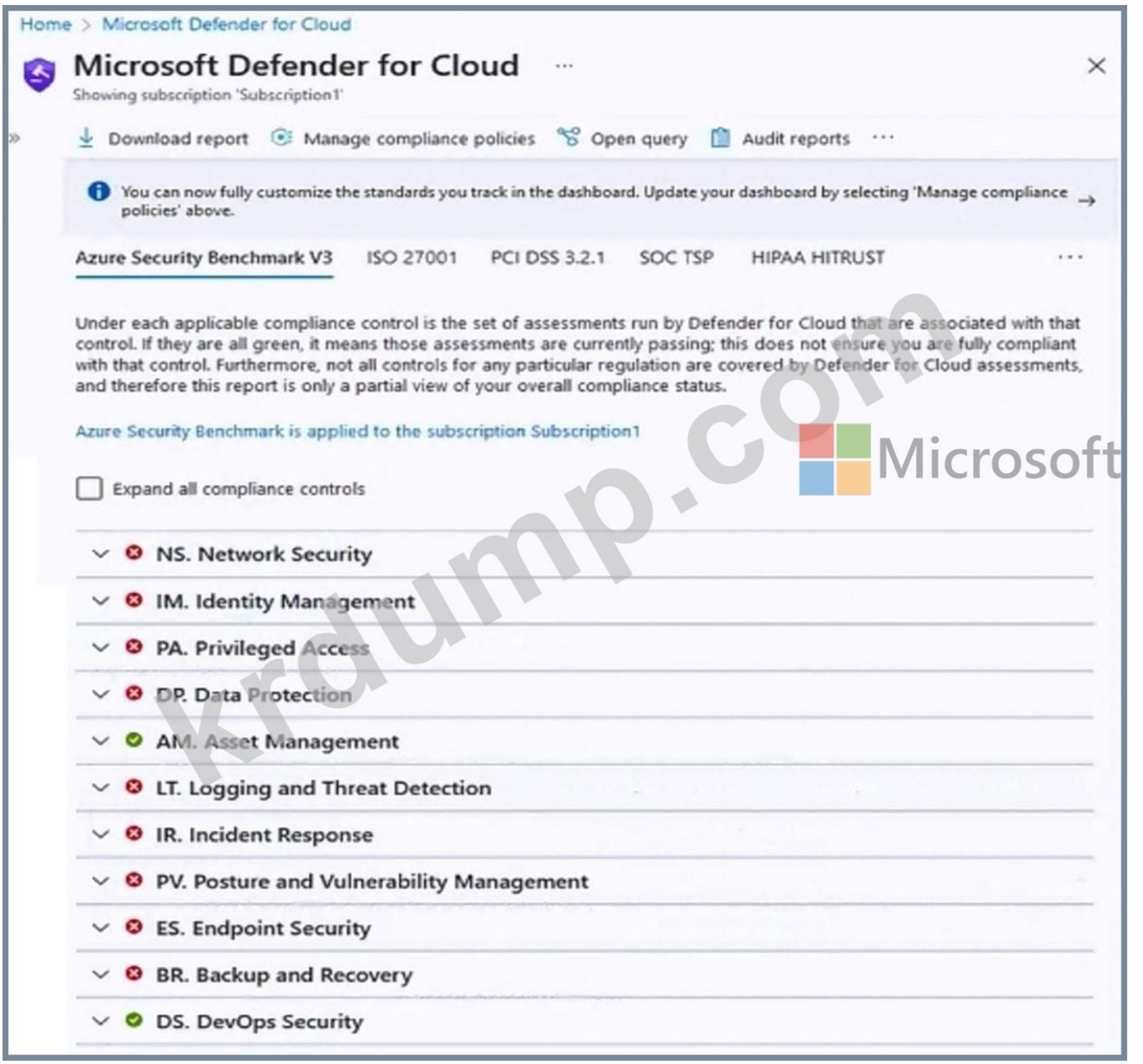
Reference:

https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview

NEW QUESTION: 21

Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□.

□□ □□□ □□□ □□ Azure Security Benchmark V3 □□□□ □□□□ □□□□.



Windows□ □□□□ □□ □□ □□□ Microsoft Defender for server□ □□□□ □□□ □□□□ □□□.

□□ □□ □□ □□□ □□□□ □□□?

A. □□□ □□

B. □□ □□

C. □□ □ □□□ □□

D. □□ □□

E. □□□□□ □□

Answer: (SHOW ANSWER)

Microsoft Defender for servers compliance control installed on Windows

Defender for clout "Endpoint Security" azure security benchmark v3

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.
Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.
Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.
Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

NEW QUESTION: 22
Microsoft Entra □□□□ □□□ Azure □□□ □□□□.
App1□□□ □□□□□□ □□□□□□□ □□□ □□□□□. App1□ Microsoft Entra □□□□ □□□ □□□ □□□□ □□ LDAP□ □□□□□.
LDAP □□ □□□ □□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □ □□ □□□□ □□□ □□ □□□ □□□ □□□ □□□□□.
B. Microsoft Entra Private Access□ □□□□□.
C. Microsoft Entra Domain Services□ □□□□□.
D. □□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
If an enterprise application in Microsoft Entra needs to use LDAP to look up user attributes, Microsoft Entra Domain Services (Microsoft Entra DS) is typically required. Microsoft Entra DS provides a managed domain with LDAP functionality, allowing applications to query for user attributes within the Microsoft Entra environment.
Microsoft Entra ID (formerly Azure AD) does not natively support LDAP lookups for user attributes.
It primarily focuses on cloud-based authentication and authorization using protocols like OAuth 2.0 and OpenID Connect.
Microsoft Entra Domain Services bridges the gap.
It's a managed service that provides a Windows Server Active Directory-compatible environment, including LDAP, Kerberos, and NTLM authentication.
This allows legacy applications that rely on LDAP to integrate with Microsoft Entra.
Organizations can migrate their applications and infrastructure to the cloud without needing to refactor them to use modern authentication protocols.
Reference:
https://learn.microsoft.com/en-us/entra/architecture/auth-ldap

NEW QUESTION: 23
□□ □□ 2 - Litware, inc.
□□

Litware, Inc.□ □□□ □□□□□□□ □□□ □ □□ □□□ □□□□□. Litware□ □□ □□□ 30□□ □□□ □□ □□ □□□ □□ □□□□. □□ □□ □□□ VPN□ □□□□ □□□ □□□ □□.

Litware□ □□ 2□□ □□□□□ □□ □□ □□□□□□. □□ □□□□ □□□□ □□□ □ □ □ □□□ □□□□□.

□□ □□

Litware□□ litware.com□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□□ 20 □□ Azure □□□ □□□ Microsoft Entra □□□□ □□□□. Microsoft Entra Connect□ □□ □ □□ □□□□ □ □□□□□. □□ □□ □□□□ □□□□□□ □□ □□ □□□ □□□□□□. □□ Litware □□□□ Microsoft 365 E5 □□□□□ □□□□□.

□ □□□□ Litware□ □□□□ □□□ □□ AD DS □□□□, Microsoft Entra □□□ □ □□ □ □ Azure □□□ □□□□□.

□□ □□. □□□ □□ □□

Litware□ □□□ □□ □□ □□□ □□□ □□□□□.

- □ Microsoft Entra □□□□ □□ □□ □□ □□ □□□ □□□□.
- Litware□ □□ Azure □□□ □□□□□□ □□ □□ Azure □□□□□ □□□□ □□ □□ □ □□□ □□□□□.
- VPN□ □□□□ □□ □□□□□ □□ □□□□□□□ □□ □□ □□□□ □□□□ □□ Microsoft Entra Application Proxy□ □□□□□.

□□ □□. □□□□ □□ □□

Litware□ □□□ □□ □□□□ □□ □□□ □□□□□.

- □□□□ □□□□□ □□□□ □□□□□□.
- □□□ □□□□□ □□□ □□□□□ □□□□□□.

□□ □□. □□□□□ □□ □□

Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.

- □□□ □□□□ Azure□□ □-□□□□ □□□□ □□□ □ □□□□.

o Azure Policy□ □□□□ □□ □ □□ □□□ □□□□□.

o □□ □□ □□ □ □□ □□□□□ □□□□□.

o □□ □□□ □□□□□.

- □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

□□ □□. Microsoft Sentinel □□ □□

Litware□ Microsoft Sentinel□ □□ □□ □ □□□ □□(SIEM)□ □□ □□□□□□□ □□ □□ (SOAR) □□□ □□□ □□□□□. □□ Microsoft Sentinel□ □□□□ □□ □□ □□(SOC)□ □□ □□□□□□ □□□.

□□□□. □□ □□□□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

- AD DS □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □□ □□ □□□ □□□□□.
- Microsoft Entra □□□ □□□ □□□□ □□ □□□ □□ □□□□ □□ AD DS □□□ □□□ □□□ □□ □□□□□.

- Litware□ Microsoft Entra □□□□□ □□□ □ □□□ □□□ □□□ □□□□□. □□□□ □ □□ □□□□□.
o □□ □□, □□□ □ □□□□ □□
o □□□ □□, □□□□ □ □□□□ □□
o □□□□ □□□ □□ □□
□□ □□. □□ □□ □□ □□
Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.
- □□□ □□□□ □□ □ □□□□ □□□ □□, □□ □□ □ □□□□ □□□ □ □□□ □□ □ □□ □□□□□.
- □□ □□ Azure Policy □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
- □□ □□□ □□□ □□□□□.
□□ □□. Azure Landing Zone □□ □□
Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.
- □□ Azure □□□□ Azure Firewall□ □□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □.
- □□ □□□ □□ □□□ □□□ □□□□□.
- □ □□ □□ Azure □□ □□□ □□ □□□□□□ □□ Microsoft □□ □□□□□ □□ □□□ □□ Azure App Service □□□ □□□□□ □□□□□.
- □□□ □□ □□□□ □□□□□□.
- □□□□ □□□□ □□□□□□.
□□ □ □□□□□□ □□□ □ □□□□□ □□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□. □ □□ □□ □□□ □□ □□□ □□□□.
- □□ □□□□ □□□□□.
- litware.com□ DNS □□□□□□□ □□□□□.
□□ □□. □□□□□□ □□ □□ □□
Litware□ □□□ □□ □□□□□□ □□ □□ □□□ □□□□□.
- Microsoft Entra Application Proxy□ □□□□ SSO(Single Sign-On)□ □□□□ □□ □□□□□ □□ □□□□□.
- Microsoft SharePoint Online □ Exchange Online □□□□ □□ □□□□ □□□□□ □□□□ □□ □□□□□.
□□ □□□ □□□ □□□□ □□□□□ □□ □□□ □□□□ □□□.
□□□□ □□ □□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□ □□□□ □□□?
A. □□□ □□□
B. □□ □□□□ □□□□□
C. □□ □□□
D. VNet-to-VNet □□
Answer: A (LEAVE A REPLY)
Service chaining enables you to direct traffic from one virtual network to a virtual appliance or gateway in a peered network through user-defined routes.

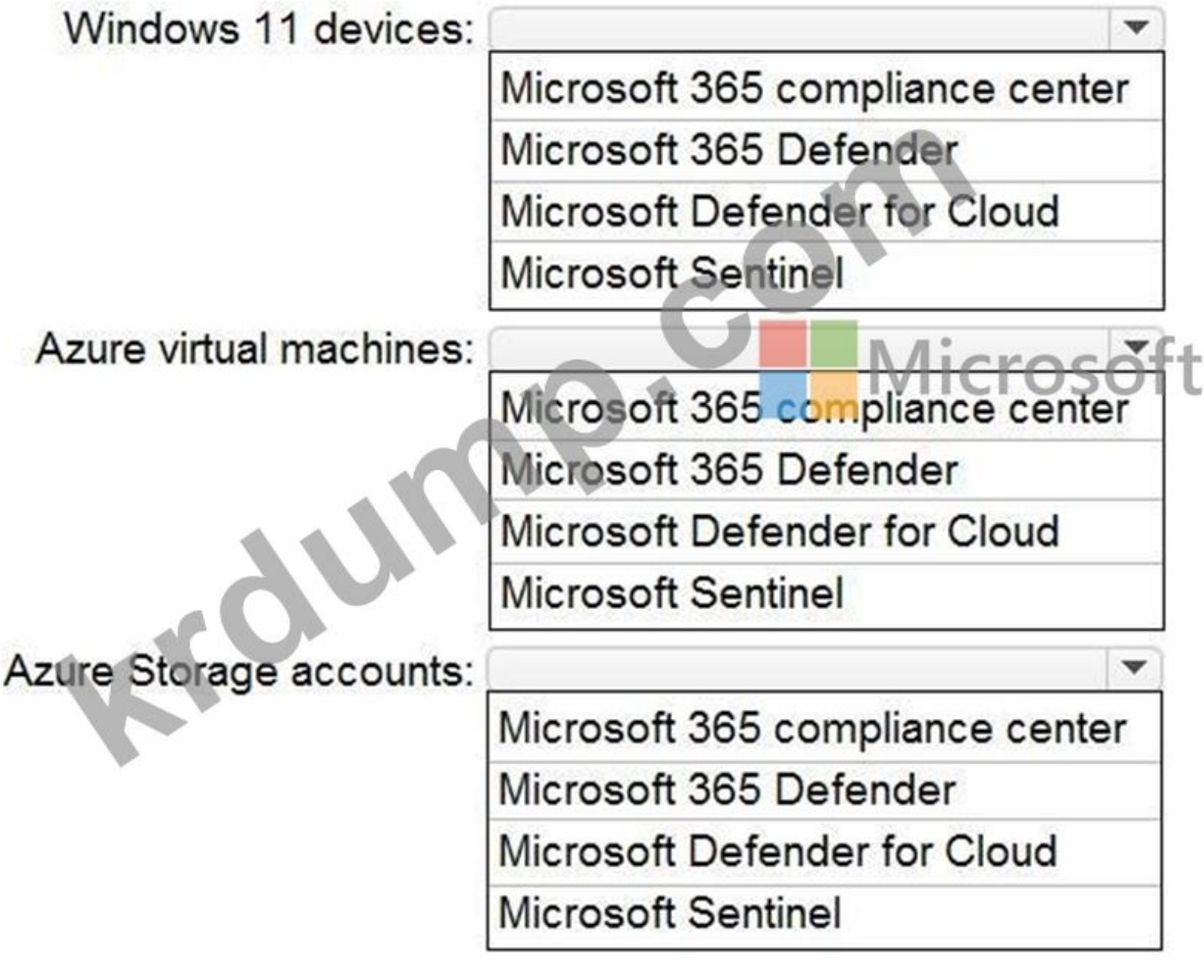
You can deploy hub-and-spoke networks, where the hub virtual network hosts infrastructure components such as a network virtual appliance or VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic flows through network virtual appliances or VPN gateways in the hub virtual network.
Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway.
You can't route between virtual networks with a user-defined route that specifies an Azure ExpressRoute gateway as the next hop type.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview#service-chaining
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

NEW QUESTION: 24
□□□ □□□□ □□□ □□□ □□□□.
□□□□ Windows Server□ □□□□ Microsoft Entra □□□□□□ □□□□ □□□□ □□□□ □□ □□□□□ □□□□□ □□ 20□□ □□□□. □□□□ Windows 11□ □□□□ □□□□ □ □□□ 500□□ □□□□. □□□□ Windows 11□ □□□□ □□□□□ □□□ 100□□ □□ □□.
Intune□ □□□□ □□□□□.
□□ □□ □□□□ Microsoft Intune□ □□□□ □□□□. □□ □□□□ Microsoft 365 ES □□ □ □□□□ □□□□.
Microsoft Entra □□□□ □□□□. Microsoft Entra □□□□ □□□ □□ SaaS(Software as a Service) □□ □□□□.
Global Secure Access□ □□□ □□□□□.
□□□ □□□ □□□□ □□□□ □□ □ □□□ □□□□ □□□ □□□□ □□□□.
□□ □□ □□□□ □□□□ □□□□ □ □□ □□□□□ □□□□□? □ □□□ □□□ □□□ □ □□□□□.
□□: □□□ □□□ □□ 1□□□□.
A. □□ SaaS □□ □□ □□
B. □□ □□□ □□□□□□ □□
C. Microsoft Exchange Online□ □□ □□□□ □□□ □□
D. □□□□□ □□ □□ □□
Answer: A,C (LEAVE A REPLY)
Global Secure Access, Enable compliant network check with Conditional Access A: Organizations who use Conditional Access along with the Global Secure Access, can prevent malicious access to Microsoft apps, third-party SaaS apps, and private line-of-business (LoB) apps using multiple conditions to provide defense-in-depth. These conditions might include device compliance, location, and more to provide protection against user identity or token theft.
Global Secure Access introduces the concept of a compliant network within Microsoft Entra ID Conditional Access. This compliant network check ensures users connect from a verified network

connectivity model for their specific tenant and are compliant with security policies enforced by administrators.
C: Compliant network check data plane enforcement (preview) with Continuous Access Evaluation is supported for SharePoint Online and Exchange Online.
Compliant network check is currently not supported for Private Access applications.
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/reference-current-known-limitations
https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-compliant-network

NEW QUESTION: 25
□□□ □□
Microsoft 365 E5 □□□ Azure □□□ □□□□.
□□ □□ □□□ □□ □□□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□.
- Microsoft Intune□□ □□□□ Windows 11 □□
- Azure Storage □□
- Azure □□ □□
□□ □□□ □□□□ □ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□.

Answer Area



Answer:

Answer Area

Explanation:

Box 1: Microsoft 365 Defender

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Microsoft Defender for Endpoint works with devices that run:

Android -

iOS/iPadOS

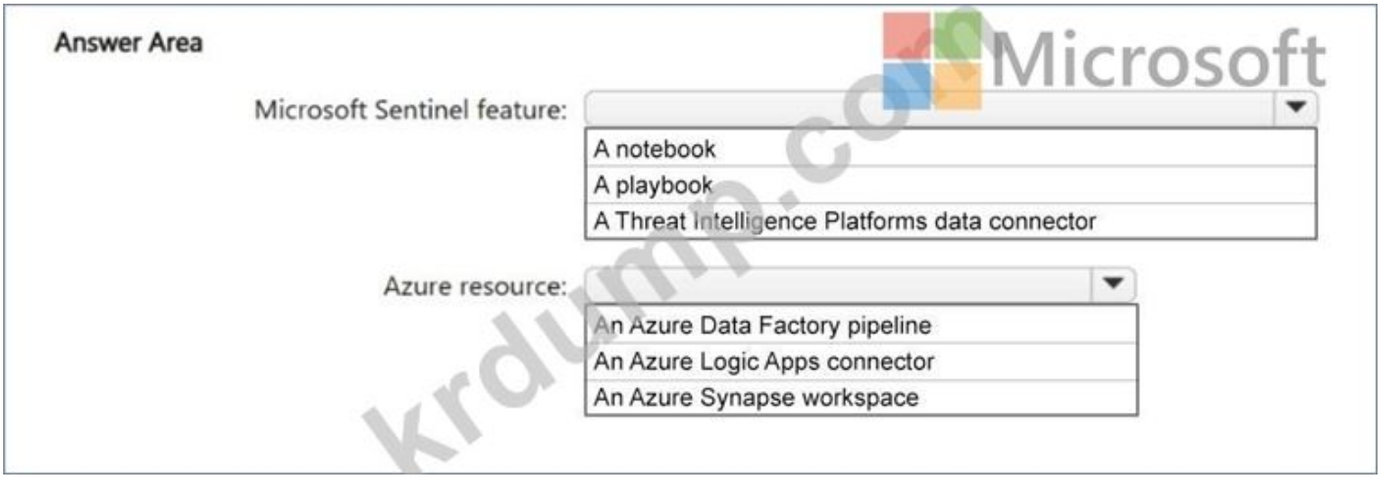
Windows 10 -

Windows 11 -

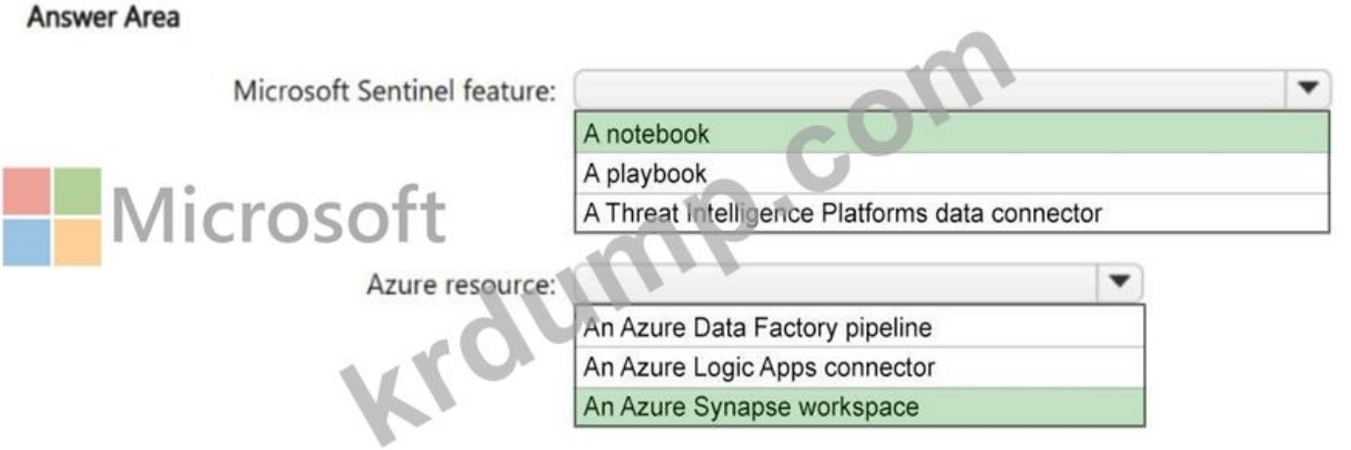
Box 2: Microsoft Defender for Cloud

Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed Instance and Azure Virtual Machines.
Box 3: Microsoft Defender for Cloud
Reference:
https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storag
https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint
https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

NEW QUESTION: 26
□□□ □□
MWS1□□□ Microsoft Sentinel □□ □□□ lake1□□□ Azure Data Lake Storage □□□ □□ □ Azure □□□ □□□□. □□□ □□ □□□□ MWS1□ □□□□□.
MWS1□□ lake1□ □□ □□□ □□ □□□□ □□□□□ □□□.
□□ □□□□ MWS1□□ □□ □□□ □□□ □ □□□ □□ □□□. □□□□ lake1□ □□□ □□□ □□□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:
Box 1: A notebook
To export historical firewall log data from a Microsoft Sentinel workspace to Azure Data Lake Storage (ADLS) for threat hunting, you can utilize the "Export Historical Data" notebook or a scheduled data export using Log Analytics. The notebook approach allows for more granular control over the export process, including the ability to filter and transform data before exporting it to ADLS, while the scheduled data export offers a more automated and continuous approach.
Box 2: An Azure Synapse workspace
The new historical data export notebook uses Azure Synapse to work with data at scale.
Reference:
https://techcommunity.microsoft.com/blog/microsoftsentinelblog/export-historical-log-data-from-microsoft-sentinel/3413418

NEW QUESTION: 27
□□□ □□□□ □□□□□ □□□□□ Azure □□□ □□□□. □□□□□ □□□□□□ □□ □□□□ □□□ □□□□ □□□□.
□ □□□ □□□□ □3□ □□ □□□ □□□ □□ Azure □□□ □□□□ □□ □□□ □□□□ □□□□ □□□□□.
□□ □□□ □□ □□□□ □□□ RDP □□□ □□□□□. □□ □□□□ □□□□ □□□ □□ □□□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ Azure□ □□□□ □□ □□□ □□□ □ □ □□□□. □□ □□□□ □□□□ □□ □□□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□□□ □□ □□□ □□□□□.
Zero Trust □□□ □□□□ □ □□ □□ □□□□ □□□□ □□□. □□□□ □□□□ □□ □□ □ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. IP □□ □□□ □□ □□□ □□□□□ □□□□ □□□□□ □□□□ □□ □□(NSG)□ □□ □□□.
B. □□□ □ □□□□□ □□□□ □□□□ □□ Azure Firewall□ □□□□□.
C. □□ □□ □□(MFA) □ □□□ □□□ □□□□ Azure Active Directory(Azure AD) □□□ □ □□□ □□□□□.
D. □□ □□□□ □□□□ Azure Virtual Desktop□□ □□□□□□□□□.
E. □□□□ □□□ Azure □□□ □□ □□□□ □□□ □□□□□.
Answer: B,C,D (LEAVE A REPLY)
Organizations can use this location for common tasks like:
Requiring multi-factor authentication for users accessing a service when they're off the corporate network.
Blocking access for users accessing a service from specific countries or regions.
The location is determined by the public IP address a client provides to Azure Active Directory or GPS coordinates provided by the Microsoft Authenticator app.
Conditional Access policies by default apply to all IPv4 and IPv6 addresses.

Use Azure Firewall to protect Azure Virtual Desktop deployments.
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
Reference:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

NEW QUESTION: 28
□□□ □□
□□□□ Azure□ □□□□ □□□□□□□□ □□□□. □□□□□ □□ □□ □□(PLL)□ □□ □□ □□□□. □□□ Azure□ PLL □□□ □□□□ Microsoft Information Protection□ □□□ □□□□□.
Azure □□□□□ □□□ □□ PII □□□□ □□□□ □□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□□ 1□□□□.

Answer Area

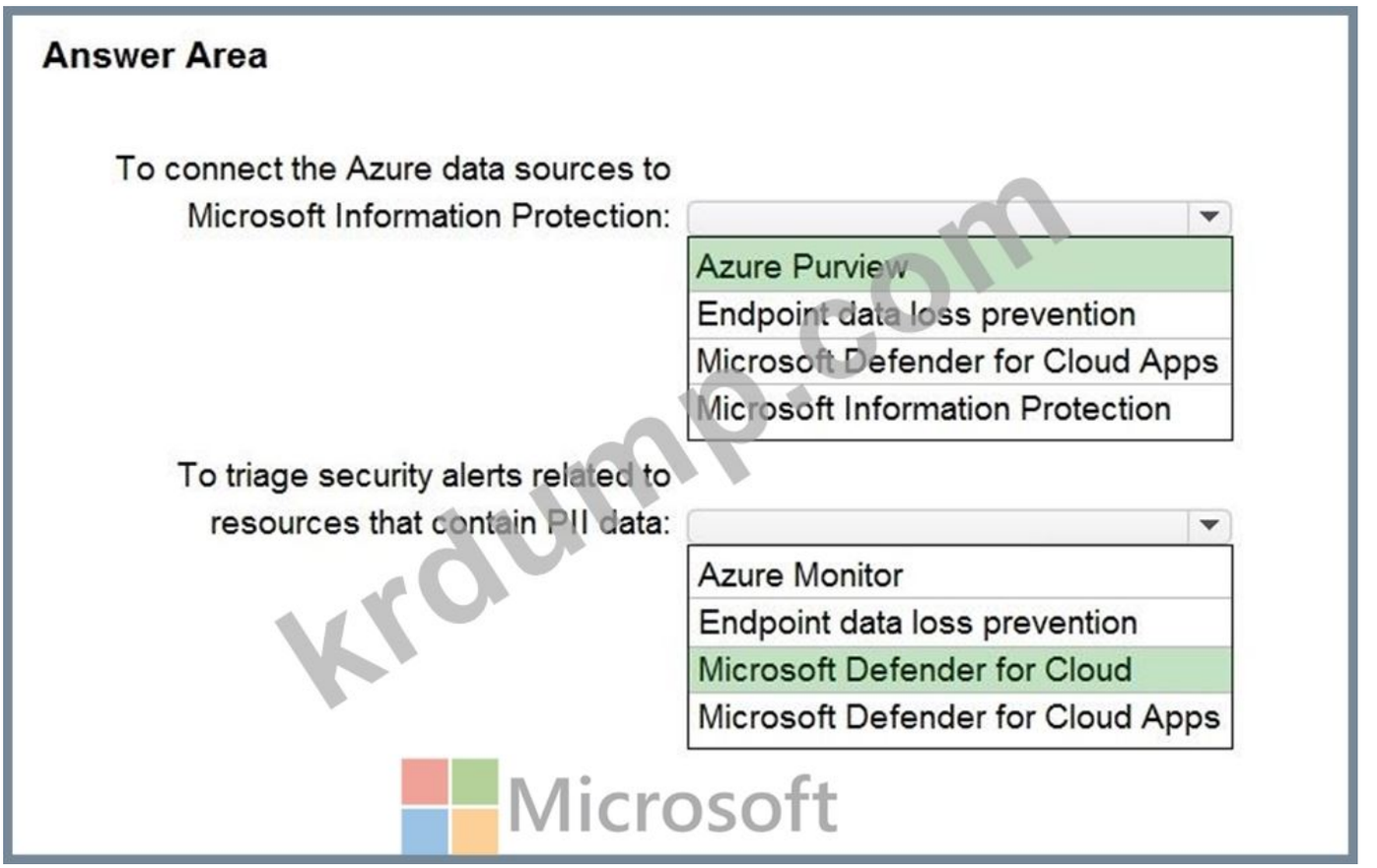
To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer:



Explanation:

Box 1: Azure Purview

Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data.

Microsoft Purview allows you to:

Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

Enable data curators to manage and secure your data estate.

Empower data consumers to find valuable, trustworthy data.

Box 2: Microsoft Defender for Cloud

Microsoft Purview provides rich insights into the sensitivity of your data. This makes it valuable to security teams using Microsoft Defender for Cloud to manage the organization's security posture and protect against threats to their workloads. Data resources remain a popular target for malicious actors, making it crucial for security teams to identify, prioritize, and secure sensitive data resources across their cloud environments. The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.

References:

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

https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

NEW QUESTION: 29

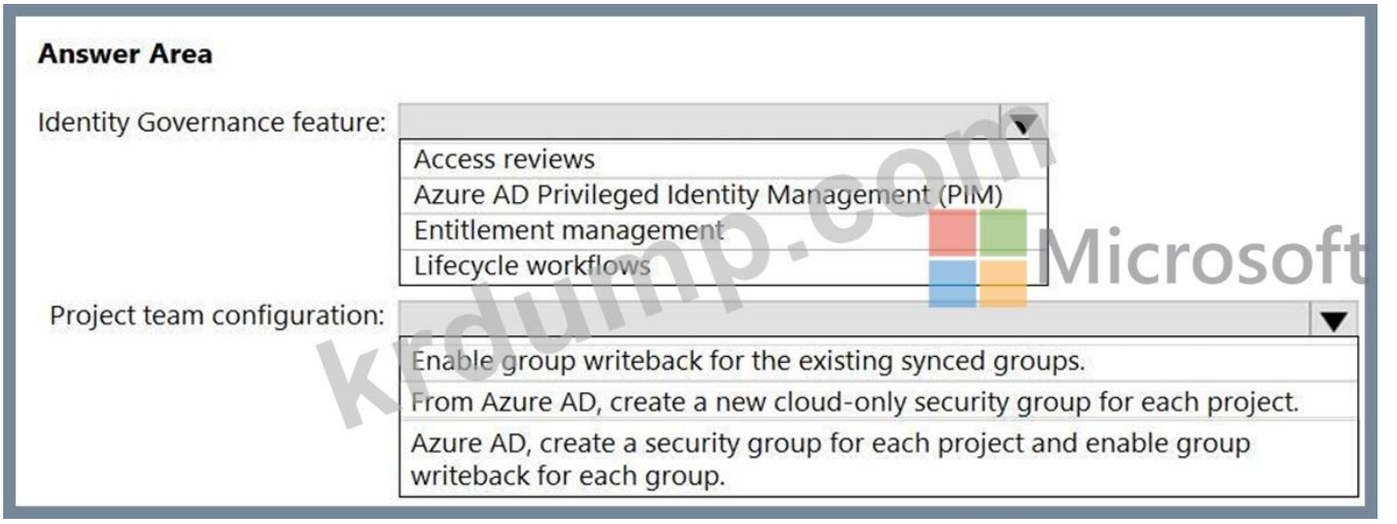
Microsoft Entra □□□□ □□□□. □□□□□ Global Secure Access □□□□□□ □□□ 500 □□ Windows □□□ □□□□.
App1□□□ □□ SaaS(Software as a Service) □□ □□□□.
App1□ □□ □□□□ □□□□ □□ Global Secure Access□ □□□ □□□□□.
App1□ □□ □□□ □□□□ □□□□ □□□□ □□□. □□□□ □□□□ App1□ □□□□ □ □ Microsoft Entra □□ □□□ □□□□ □□□□□ □□ □□□.
□□□□□□ □□□ □□□□ □□□?
A. □□□ □□ □□□ □
B. □□ □□□ □□□ □□ □□□
C. □□□ □□ □□□ □□ □□□
D. □□ □□□ □
Answer: A (LEAVE A REPLY)
Global Secure Access app is the best solution to manage access to a third-party SaaS application, such as App1. By configuring this app within A Microsoft Entra, you can enforce authentication policies that require users to log in with their Microsoft Entra credentials before accessing the SaaS application. This setup provides centralized access management, secure access controls, and ensures consistent user authentication for App1.

NEW QUESTION: 30
Microsoft 365 □□□ □□□□.
Azure □□□ □□□□.
Microsoft Teams □ Yammer□ □□ Microsoft Purview □□□□□□ □□ □□ □□□□ □□□ □ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □□□ □□□□ Microsoft 365 □□□ □□ □□ □□ □□
Microsoft Exchange Online □□.
- □□ □□ □□□ □□ □□□□□□.
- □□□ □□□ □□□□□□.
□□□□ □□□ □□□□ □□□?
A. □□□ □□
B. Microsoft 365 Defender □□□ □□
C. □□ □□
D. Microsoft Purview □□□ □□□
Answer: (SHOW ANSWER)
When you create a communication compliance policy or a policy for retention, you can create or add an adaptive scope for your policy. A single policy can have one or many adaptive scopes. An adaptive scope uses a query that you specify, so you can define the membership of users or groups included in that query. These dynamic queries run daily against the attributes or properties that you specify for the selected scope. You can use one or more adaptive scopes with a single policy.
Reference:
https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

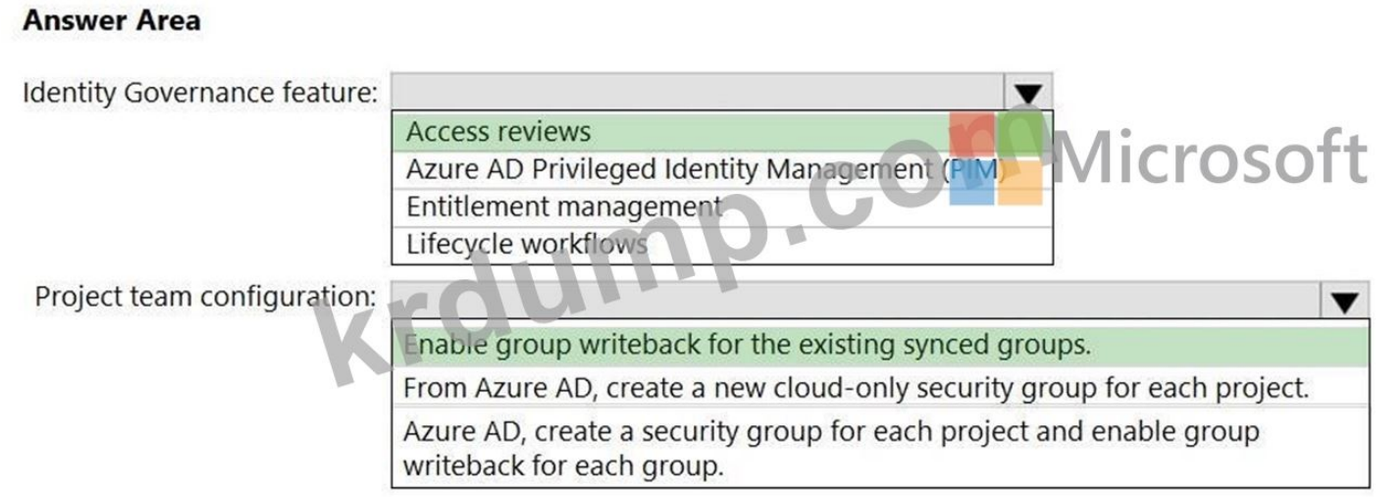
NEW QUESTION: 31
□□□ □□□□□ □□□□, Azure □□, Microsoft 365 E5 □□□ □□□□ □□□□. □□□□ □ □□ □□□ □□□□□.
* Windows 10 □□ Windows 11□ □□□□ □□□
* Android □□ iOS□ □□□□ □□□ □ □□□□
□□□□ □□□ □□□ □□□□ □□□ Microsoft Office 365 □□□□ □□□□ □□□□□ □ □□□ □□□□ □□□. □□□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□ □□
C. □□□□□□ □□□
D. Microsoft □□ □□
Answer: D (LEAVE A REPLY)
Protect your sensitive data with Microsoft Purview.
Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.
Note: You can use Microsoft Information Protection: Microsoft Purview for Auditing and Analytics in Outlook for iOS, Android, and Mac (DoD).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection
https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

NEW QUESTION: 32
□□□ □□
□□□□□ □Ł□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□ □ Windows Server□ □□□□ □□ □□□ □□□□□ □□□ □□□□. □ □□□□ Azure AD Connect□ □□□□ Azure AD□ □□□□□□. Azure AD Connect□□ □□ □□ □□ □□□ □ □□□□ □□□□.
Microsoft SharePoint Online□ □□□□ Microsoft 365 □□□ □□□□.
□□ □□□□ □□ □□□□. □ □□□ Azure AD□ □□□□□ AD DS □□□ □□□□.
□ □□□ □□□ SharePoint Online □□□□ □□ □□□□□ Windows Server □□ □□□ □□ □□□ □□□□. □□□□ □□□□ □ □□ □□□□□ □□□□□.

□□ □□ □□□ □□□□ Azure AD Identity Governance □□□□ □□□□ □□□.
- □□□□ □□□□ □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□.
□□ □□□□ □ □□.
- □ □□□□ □□ □□□ □□□□ □□□□ □ □□□ □□□.
□□□ □□□ □□□□□ □□□□□□.
- □□□□ □□□□ □□□□ □□□□ □□□□□ □□□.
□□□□ □□□□ 30□ □□ □□□ □□□□ □□□□ □□□□□.
- □□□ □□□ □□□□□ □□□.
□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview.

NEW QUESTION: 33
□□□ □□
□□ □□ 100□□ □□□ Azure □□□ □□□□. Azure Bastion□ □□□□ □□ □□□ □□□ □□□.

□□ □□□ □□ □□□□ □□ □□□ □□□□ □ □□□ □□ □□□□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.

- □□ IP□ □□□□ □□ □□□ □□ □□□□ □□□□□.

JIT(Just-In-Time) VM □□□□ □□□□ □□ □□ □□ □□ □□□□ □□ □□.

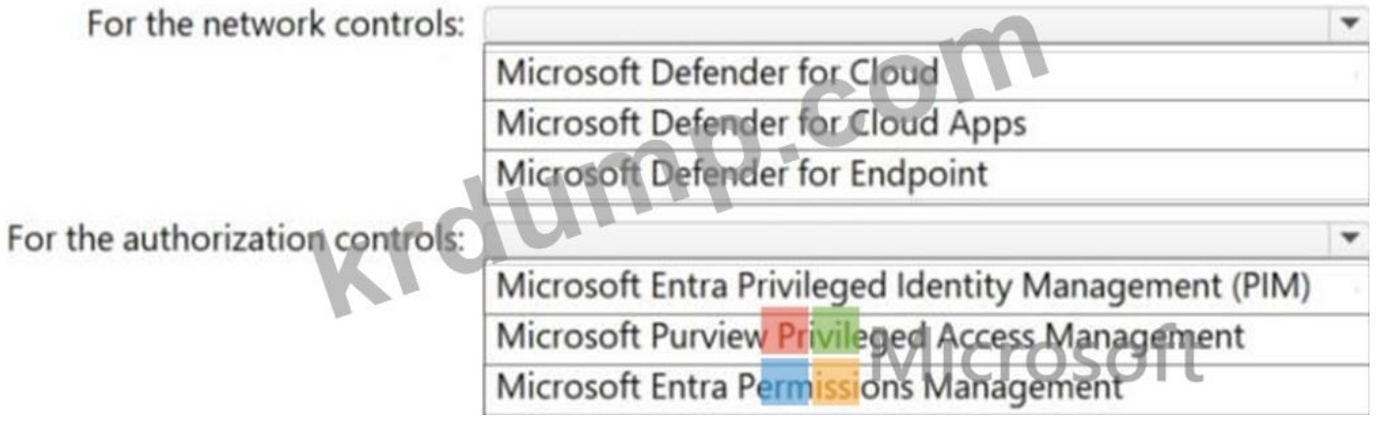
- □□ □□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□□□.

JIT VM □□□ □□ □□□ □□□□ □□(RBAC) □□ □□ □□ □□.

□□ □□□ □□ Microsoft □□□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area

Explanation:

Box 1: Microsoft Defender for Cloud

Restrict access to the virtual machines based on an originating IP address or a connection request by using just-in-time (JIT) VM access network- based controls.

Microsoft Defender for Cloud offers JIT. With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Box 2: Microsoft Entra Privileged Identity Management (PIM)

Restrict access to the virtual machines based on role-based access control (RBAC) role assignments by using JIT VM access authorization controls.
Multilayered protection for Azure virtual machine access
This solution offers a multilayered strategy for protecting virtual machines (VMs) in Azure. Users need to connect to VMs for management and administrative purposes. It's crucial to maintain accessibility while minimizing the attack surface.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview
https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/multilayered-protection-azure-vm

NEW QUESTION: 34
App1□□□ □□□□□ □□ □□□□.
□□ □□□□ VPN □□□ □□□□ App1□ □□□□□□.
App2□□ □□□ □□ SaaS(Software as a Service) □□ □□□□.
App1□ App2□ □□ □□□□ □□□□□ Global Secure Access□ □□□□ □□□.
□ □□ □□□ □□□□ □□□?
A. App2□ Microsoft Entra Private Access □ App1□ Microsoft Entra Internet Access
B. App1□ Microsoft Entra Private Access □ App2□ Microsoft Entra Internet Access
C. App1 □ App2□ Microsoft Entra □□□ □□□
D. App1 □ App2□ □□ Microsoft Entra Private Access
Answer: (SHOW ANSWER)
* App1
The features of Microsoft Entra Private Access provide a quick and easy way to replace your VPN to allow secure access to your internal resources with an easy-one time configuration, using the secure capabilities of Conditional Access.
* App2
Microsoft Entra Internet Access is an identity-centric Secure Web Gateway (SWG) for SaaS apps and internet traffic that protects against malicious internet traffic, unsafe or non-compliant content, and other threats from the open internet. Working alongside Microsoft Entra Private Access and the rest of Microsoft Entra identity stack it unifies your access policies across all internet resources and SaaS apps, including Microsoft 365 with Microsoft Entra Conditional Access.
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/concept-private-access
https://techcommunity.microsoft.com/t5/microsoft-entra-blog/microsoft-entra-internet-access-an-identity-centric-secure-web/ba-p/3922548

NEW QUESTION: 35
□□ □□ □□□ □□ □□ □□□ □□□□ Sub1□ Sub2□□ □ □□ Azure □□□ □□□□.

Name	Type	Location	Subscription
RSVault1	Recovery Services vault	East US	Sub1
BackupVault1	Azure Backup vault	East US	Sub2
RSVault2	Recovery Services vault	West US	Sub2
BackupVault2	Azure Backup vault	West US	Sub1

□□ □□ □□□ □□ □□ □□□ □□ □□(MUA) □□□□ □□□□ □□□. □□□□ □□ □ □ □□□ □□□□ □□□.

* RSVault1 □ RSVault2□ □□□ □□ □□□□, MUA □□ □□, □□□ □□□□□ □□ MUA □ □□□□□.

* BackupVault1 □ BackupVault2□ □□□ □□□ □□□□□□ MUA □□□ □□□□□ MUA□ □□□□□.

□□□ □ □□ Resource Guard □□□□ □□□□□?

A. 1

B. 2

C. 3

D. 4

Answer: (SHOW ANSWER)

* RSVault1 and RSVault2 must require MUA for disabling soft delete, removing MUA protection, and disabling immutability.

RSVault1 is in Sub1 in East US.

RSVault2 is in Sub2 in West US.

Need two Resource Guards. One in East US, and one in West US.

* BackupVault1 and BackupVault2 must require MUA for disabling soft delete and removing MUA protection.

Need two Resource Guards. One in East US, and one in West US.

As a Resource Guard can be configured both for Recovery Vaults and Backup Vaults, we need only two; one in each region.

Note 1: Create a Resource Guard

The Security admin creates the Resource Guard. We recommend that you create it in a different subscription or a different tenant as the vault.

However, it should be in the same region as the vault.

Note 2: Select operations to protect using Resource Guard

Choose the operations you want to protect using the Resource Guard out of all supported critical operations. By default, all supported critical operations are enabled. However, you (as the security admin) can exempt certain operations from falling under the purview of MUA using Resource Guard.

To exempt operations, follow these steps:

1. In the Resource Guard created above, go to Properties > Recovery Services vault tab.

2. Select Disable for operations that you want to exclude from being authorized using the Resource Guard.
Attention:
You can't disable the protected operations - Disable soft delete and Remove MUA protection.
3. Optionally, you can also update the description for the Resource Guard using this blade.
4. Select Save.
Reference:
https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

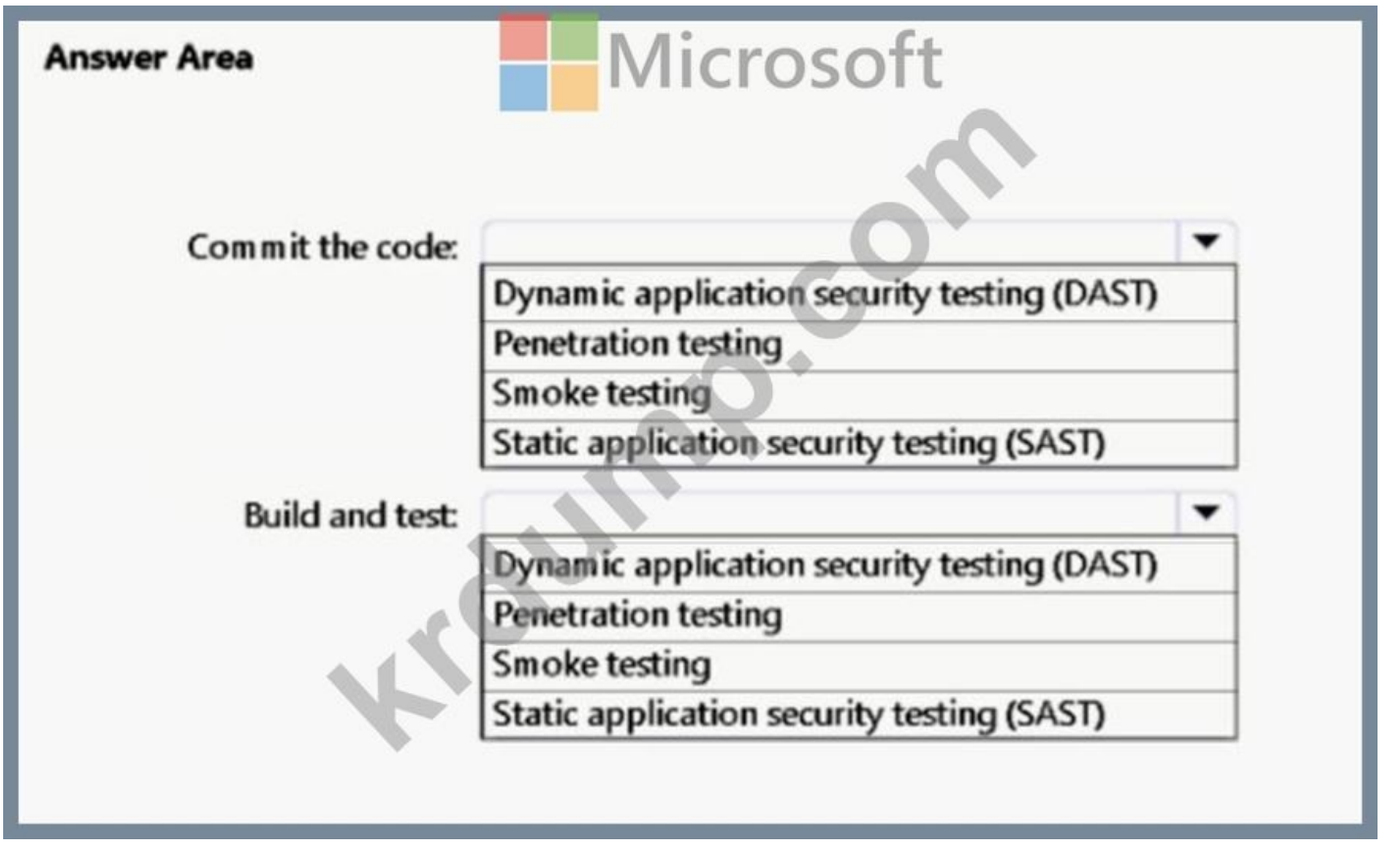
NEW QUESTION: 36
Active Directory □□□ □□□(AD DS) □□□□ □□□□□ Microsoft Entra □□□□ □□□□.
100□□ □□□ □□ □□□□□ □□□ □□□ □□□□. □ □□□ Windows Server□ □□□□ Microsoft Azure Backup Server(MABS)□ □□□□ □□□□□.
□□□□ □□□ □□ □□ □□□□ □□□□ □□□□. □ □□□□ Microsoft □□ □□ □□□ □□□□□.
□□□ □□□ □□□ □□□□ □□□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. Azure Backup□□ Resource Guard□ □□□□ □□ □□□ □□ □□□ □□□□□.
B. Microsoft Azure Backup □□□□ MABS□ Recovery Services □□ □□ □□□ □□□□□.
C. □□ □□□ □□□□□ □□□ □□□ □□ □□ PIN□ □□□□□.
D. Microsoft Entra Privileged Identity Management(PIM)□□ □□ □□□ □□□ □□ □□ □□ □ □□□□.
Answer: A (LEAVE A REPLY)
Multi-user authorization (MUA) for Azure Backup allows you to add an additional layer of protection to critical operations on your Recovery Services vaults and Backup vaults. For MUA, Azure Backup uses another Azure resource called the Resource Guard to ensure critical operations are performed only with applicable authorization.
Critical operations
The following table lists the operations defined as critical operations and can be protected by a Resource Guard. You can choose to exclude certain operations from being protected using the Resource Guard when associating vaults with it.
* Delete Backup Instance
Delete protection by stopping backups and performing delete data.
Reference:
https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization-concept

NEW QUESTION: 37
□□□ □□
□□ □□ □□□ Azure □□□ □□□□. □□ Azure DevOps□ CCD(□□□ □□) □ CCD(□□ □ □□) □□□□□□ □□□□ □□□□□.

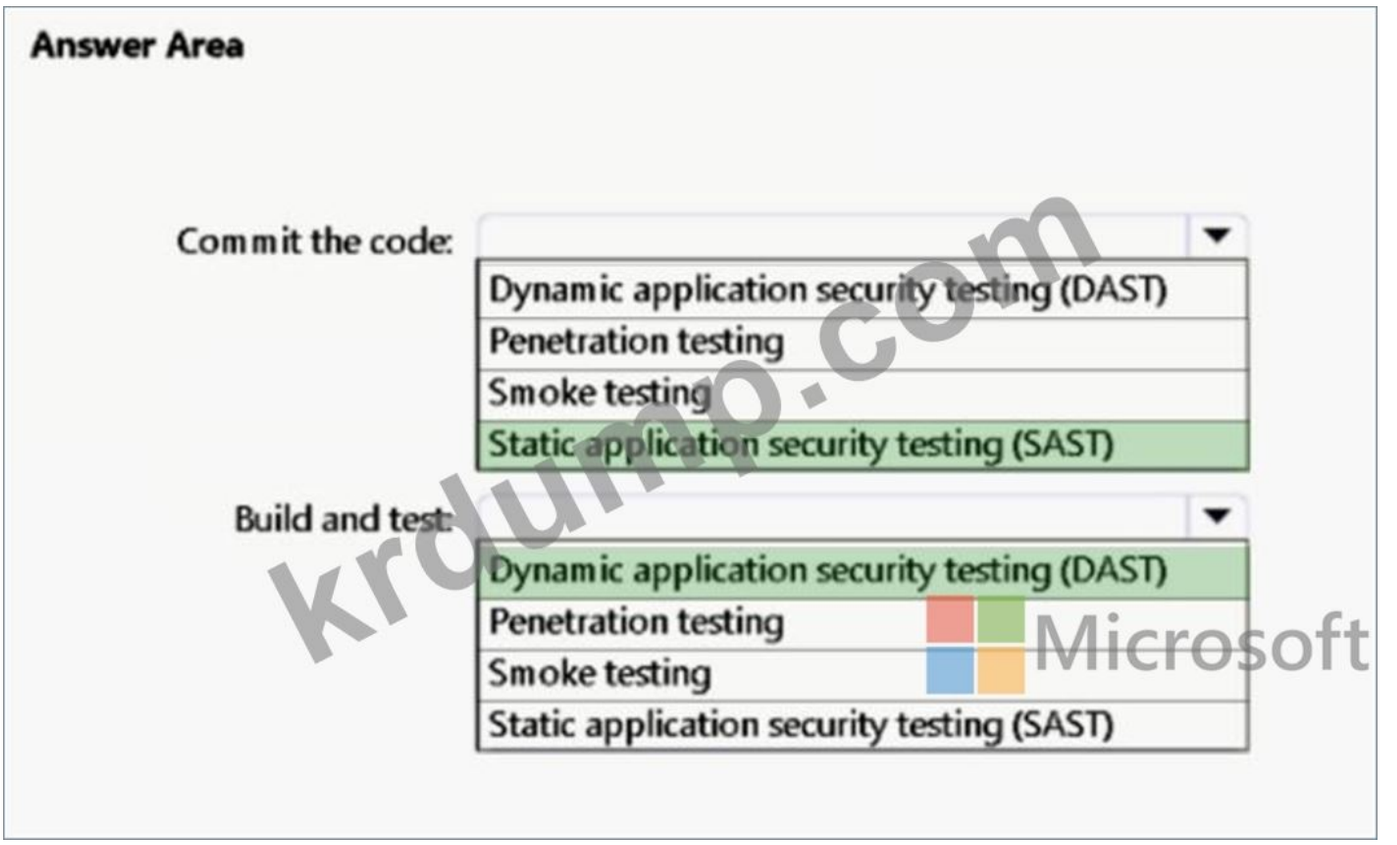
Azure□ Microsoft □□□□ □□ □□□□□□ □□□□ □□ □□ □ CI/CD □□ □ □□□ □□ □□ □□□ □□ DevSecOps □□□□ □□□□ □□□.

□ □□□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Static application security testing (SAST)

Commit the code

Box 2: Dynamic application security testing (DAST)

Build and test

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

NEW QUESTION: 38

□□□ □□
□□ □□ □□ □□ □□□□ □□□□.

Name	Type	Description
contoso.com	Microsoft Entra tenant	Associated with Sub1
fabrikam.com	Microsoft Entra tenant	Associated with Sub2
Sub1	Azure subscription	Contains multiple Recovery Services vaults in the US East Azure region
Sub2	Azure subscription	Currently unused

Recovery Services □□ □□ □□□ □□□□□ Azure Backup□ □□ □□□ □□ □□(MUA)□ □□□□ □□□. □□□□ MUA □□□ □□□ □□□□□ □□□.
Resource Guard□ □□ □□□ □□□□ □□, Resource Guard □□ □□ □□ □□ □□ □□ □□ □□(RBAC) □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

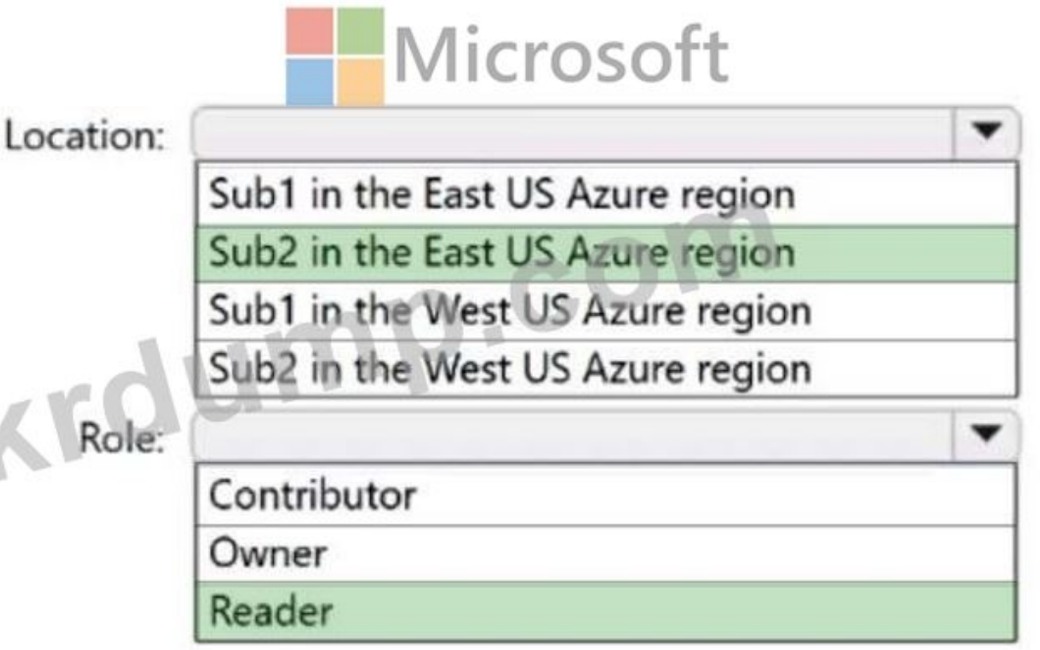
Answer Area

Location:
- Sub1 in the East US Azure region
- Sub2 in the East US Azure region
- Sub1 in the West US Azure region
- Sub2 in the West US Azure region

Role:
- Contributor
- Owner
- Reader

Answer:

Answer Area



Explanation:
Box 1: Sub2 in the US East Azure region
The Recovery service vaults are in Sub1 in the US East Azure region.
We should use the other subscription Sub2 (which also contains the other tenant).
We should use the same region.
Note: Configure Multi-user authorization using Resource Guard in Azure Backup Create a Resource Guard The Security admin creates the Resource Guard. We recommend that you create it in a different subscription or a different tenant as the vault. However, it should be in the same region as the vault. The Backup admin must NOT have Contributor, Backup MUA Admin, or Backup MUA Operator access on the Resource Guard or the subscription that contains it.
Box 2: Reader
Assign permissions to the Backup admin on the Resource Guard to enable MUA To enable MUA on a vault, the admin of the vault must have Reader role on the Resource Guard or subscription containing the Resource Guard.
Reference:
https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

NEW QUESTION: 39
Azure □□□ □□□□. □ □□□□ Windows Server□ □□□□ □□ □□ 50□□ Linux□ □□ □□ □□ □□ 50□□ □□□□ □□□□.
□□ □□□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □□□□□ □□□□ □□ □□□ □□□□□.
- Qualys □□□ □□□□□.
□□□ □□□□ □□□?
A. □□□ Microsoft Defender
B. Microsoft Defender □□ □□□□□(Defender TI)

C. □□□□□□ Microsoft Defender

D. Microsoft Defender □□ □□ □□ □□(Defender EASM)

Answer: (SHOW ANSWER)

https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-servers-plan

NEW QUESTION: 40

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.

Azure Front Door □□□□□ □□ Azure App Service □□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□. □□□ Front Door □□□□□ □□□□ □□□□ □□□□□ □□ □ □□□ □□□□ □□□.

□□ □□: Front Door ID□ □□ HTTP □□□ □□□□ □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

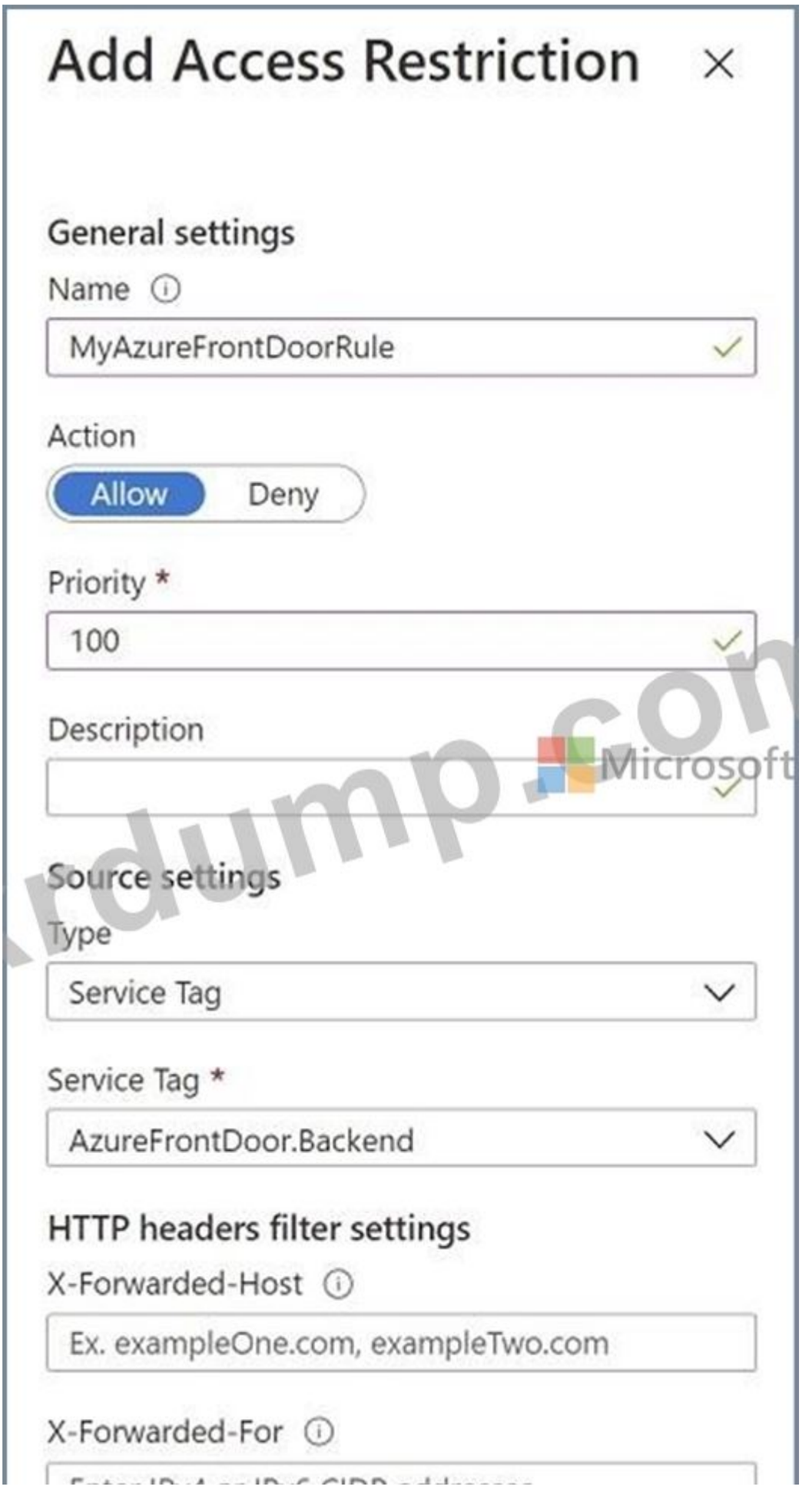
A. □

B. □□□

Answer: A (LEAVE A REPLY)

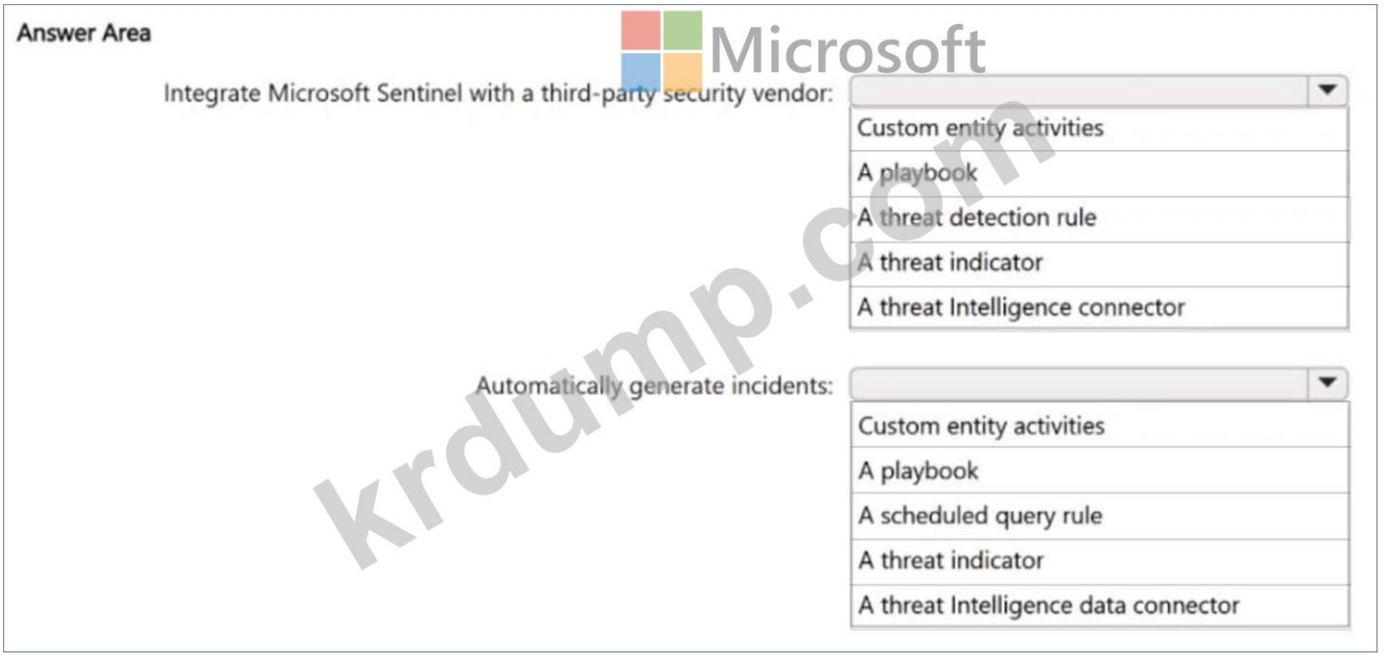
Restrict access to a specific Azure Front Door instance.

Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

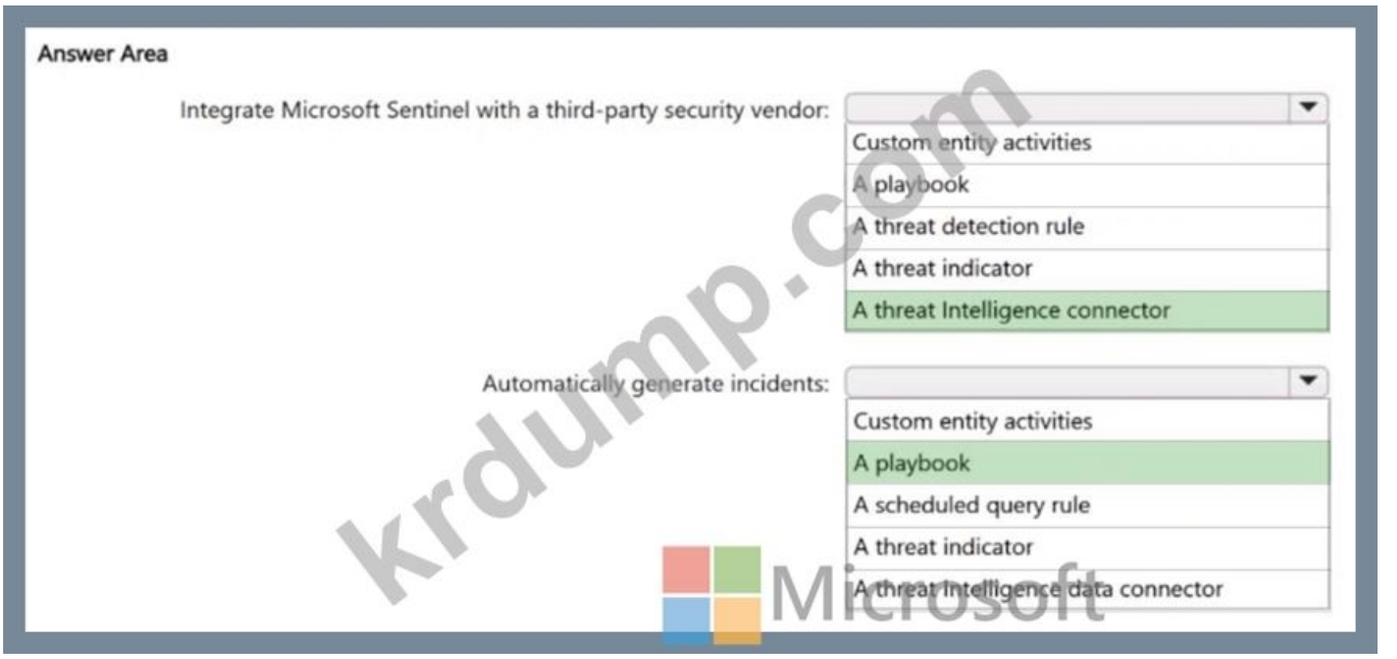

Add Access Restriction
General settings
Name
MyAzureFrontDoorRule
Action
Allow
Deny
Priority *
100
Description
Source settings
Type
Service Tag
Service Tag *
AzureFrontDoor.Backend
HTTP headers filter settings
X-Forwarded-Host
Ex. exampleOne.com, exampleTwo.com
X-Forwarded-For

Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

NEW QUESTION: 41
□□□ □□
Microsoft 365 Defender□ □□□□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft Sentinel□ □□□□ Microsoft 365 □ Microsoft 365 Defender□ □□□□ □□□□□□ □□ □□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□□□ □□□□ □□□.
- Microsoft Sentinel□ □□ □□ □□□□□ □□□□□.
□□□ □□□□ □□ □□□ □□□□□.
- □□□ IP □□□ □□ □ □□□□ □□□□□ □□□□□.
□□□□□ and-control □□□ □□□□□□□.
□ □□ □□□ □□□□□ Microsoft Sentinel□□ □□□ □□□□ □□□? □□ □□□□ □□ □ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: A threat Intelligence connector

To best integrate a third-party security vendor with Microsoft Sentinel and access information about known malware, utilize the built-in data connectors or APIs provided by the vendor within Microsoft Sentinel.

Box 2: A playbook

Automatically generate incidents when the IP address of a command-and-control server is detected in the events.

Sentinel, automatically check and record IP address reputation information in incidents You can use Microsoft Sentinel automation rules and playbooks to automatically check IP addresses in your incidents.

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-tip

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-enrich-ip-information

NEW QUESTION: 42

Microsoft 365 E5 □□□ Azure □□□ □□□□.

□□□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □□□. □ □ □□□ Microsoft □□□ □□ □□ □□□□(MCRA)□ □□ □□□□ □□□ □□□□ □□ □□ □.

□□□□□ □□□ □□□□ □□□?

A. □□□ □□□

B. Microsoft Defender for Identity

C. □□□□□ Microsoft Defender

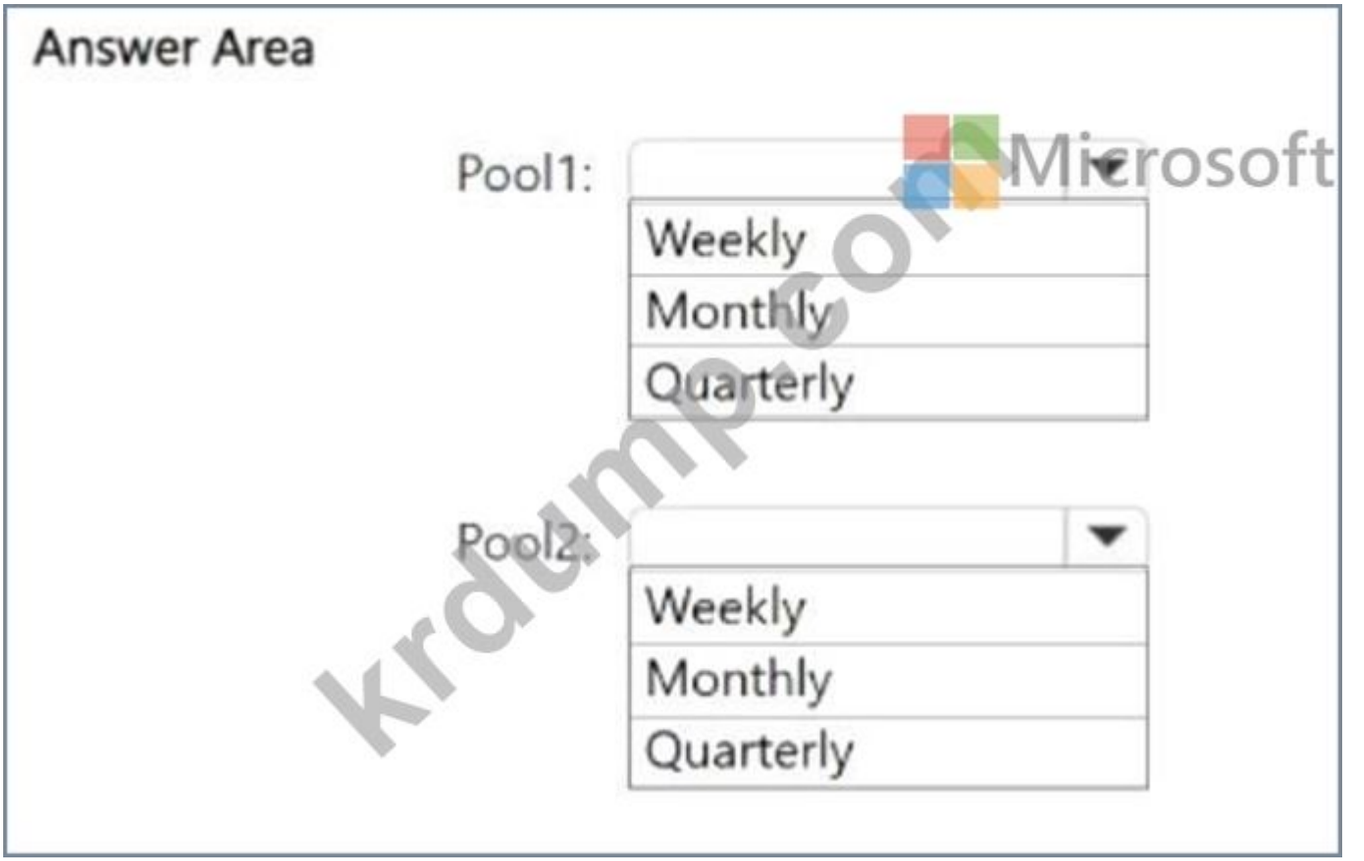
D. Microsoft Entra ID ID □□□□

Answer: A (LEAVE A REPLY)

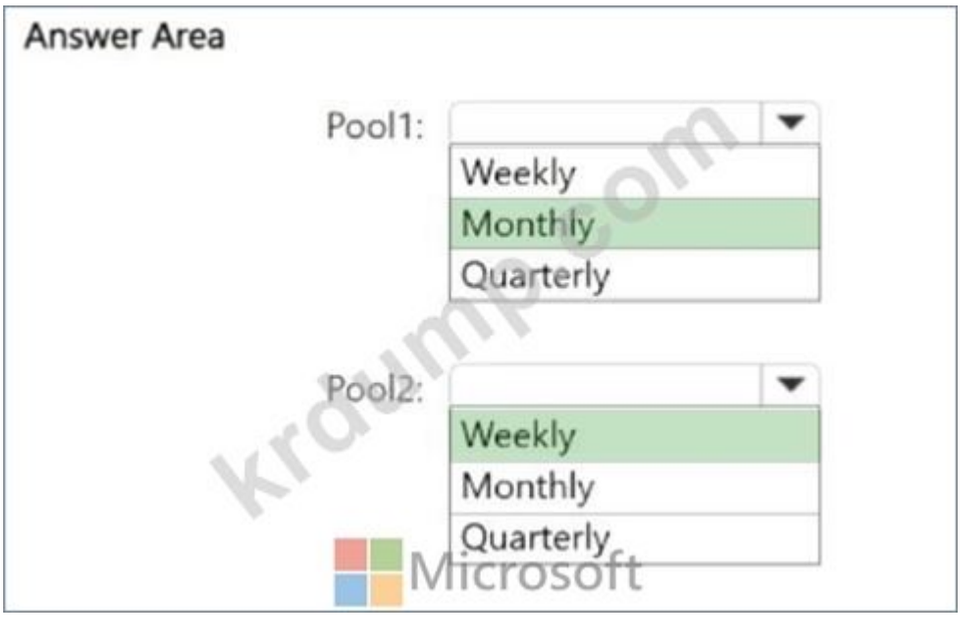
To enforce Zero Trust explicit subscription verification in Microsoft 365, focus on verifying users

and devices before granting access, using Microsoft Entra ID for identity and access management and leveraging Conditional Access policies. This involves configuring authentication methods, managing device compliance, and enforcing access based on user roles and device health.
Reference:
https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/

NEW QUESTION: 43
□□□ □□
AKS1□□□ Azure Kubernetes Service(AKS) □□□□□ □□□ Azure □□□ □□□□. AKS1□ Pool1□□□ Windows □□ □□ Pool2□□ Linux □□ □□ □□□□□□.
AKS1□ □□ □ □□□□ □□□ □□□□ □□□□.
□□□ □□□ □□ □□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□□□ □□□ □ □□ □□ □□□□□ □□□□ □ □□□ □□□ □□□□□□.
- □□□ □□□ □□□□□□.
□ □□□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Monthly

Windows supports monthly node image version upgrades.

Box 2: Weekly

Linux supports weekly node image version upgrades.

Note: Azure Kubernetes Service patch and upgrade guidance

This section of the Azure Kubernetes Service (AKS) day-2 operations guide describes patching and upgrading strategies for AKS worker nodes and Kubernetes versions. As a cluster operator, you need to have a plan for keeping your clusters up to date and monitoring Kubernetes API changes and deprecations over time.

Reference:

https://learn.microsoft.com/en-us/azure/architecture/operator-guides/aks/aks-upgrade-practices

NEW QUESTION: 44

□□ □□ 1 - Fabrikam, Inc

□□

Fabrikam, Inc.□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□□□.

□□ □□

□□□□□ □□

□□□□□ □□□□□□ corp.fabrikam.com□□□ □□ Active Directory □□□ □□□(AD DS) □□□□ □□□□ □□□□.

Azure □□

Fabrikam□ □□□ □□ Azure □□□□ □□□□ □□□□.

- corp.fabrikam.com□ □□□□□ fabrikam.onmicrosoft.com□□□ Microsoft Entra □□□
- Sub1□□□ □□ Azure □□
- □□ □□ Azure □□□ Vnet1□□□ □□ □□□□
- □□□ Azure □□□ Vnet2□□ □□ □□□□
- Azure WAF(□ □□□□□□ □□□)□ □□□□ FD1□□□ Azure Front Door □□□□

- Microsoft Sentinel □□ □□
- ClaimDetails□□ □□□□ □□□ ClaimsDB□□ Azure SQL □□□□□□
- □□□□□□ □□□ □□□□ Microsoft Defender for Cloud□ □□□□□ □□ 20□□ □□ □ □
- □□□ □□□□□ □□□□ TestRG□□ □□□ □□
- □□□ □□□ □□ □□□□ □□□□ Azure Virtual Desktop □□□ □
- Sub1□ □□ □□□□ □□ □□ □□ □□ □□ □□□ □□□□.

□□□

Fabrikam□ Contoso, Ltd.□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□□. Contoso □ □□□ □□ □□□□ □□□□ □□□□.

- contoso.onmicrosoft.com□□□ Microsoft Entra
- ContosoAWS1□□□ Amazon Web Services(AWS) □□□□ Fabrikam □□□□□□□ □□□ □□□□□ □□□□□ □ □□□□ AWS EC2 □□□□□ □□□□ □□□□. Contoso□ □□□ □ Fabrikam□ □□□□ □□□□ □□□□□□□ □□□□□□ □□□□□□□.

□□□□ fabrikam.onmicrosoft.com□ Contoso Developers□□ □□ □□□ □□□□, □ □□□ Sub1□ □□□ □□□□□. ContosoDevelopers □□□□ ClaimsDB □□□□□□□ db.owner □ □□ □□□□□.

□□ □□ □□□

Fabrikam□ □□□ □□ □□ □□ □□□ □□□□□.

- Defender for Cloud□ Sub1□ □□ □□□□ HIPAA HITRUST □□□ □□□□□ □□□□□ □ □□□ □□□□.
- □□ HIPAA HITRUST □□□ □□□□ □□ □□□□ □□□□ □□□□ □□□□.
- Qualys□ □□□ □□ □□□ □□ □□□ □□□□□.

□□ □□

Defender for Cloud□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□□. □□ □□ □□□ □□ □□□□ □□□ □□□. □□ □□ □□□ Defender for Cloud□ □□□□ □□ □.

ClaimApp □□

Fabrikam□ □□ □□□ □□ ClaimsApp□□□ □□□ □□ □□ □□□□□□□ □□□ □□□ □□.

- ClaimsApp□ Vnet1 □ Vnet2□ □□□□ Azure App Service □□□□□ □□□□□.
- □□□□ https://claims.fabrikam.com□ URL□ □□□□ ClaimsApp□ □□□□□.
- ClaimsApp□ ClaimsDB□ □□□□ □□□□□.
- ClaimsDB□ Azure □□ □□□□□□□ □□□□ □ □□□ □□□.
- ClaimsApp□ □□ □ □□□ □□□ ClaimsDB□ □□□□□ □□□.

□□□□□□ □□ □□ □□

Fabrikam□ □□□□□□ □□□ □□ □□□ □□ □□ □□□ □□□□□□.

- Azure DevTest □□ □□□□ □□□□ □□ □□□□□.
- □□ □□□□□□ □□□ GitHub Enterprise□ □□□□□ □□□.
- Azure Pipelines□ □□□□□□ □□□ □□□□ □ □□□□□.
- □□ □□□□□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□□. □□□□ □□□

□ □□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□. □□□ □□□ □□□□ □ □□ □ □□□□ □□□.

□□ □□ □□

Fabrikam□ □□□ □□ □□ □□ □□□ □□□□□.

- □□□ □□□ □□□ □□□□□□□ □□□□ □□□ □□□ □□□□ □□□.
- InfraSec□□□ □□□ □□□ □□□□ □□ □□(NSG)□ Azure Firewall, VJM, Sub1□ Front Door □□□□□ □□□ □ □□□ □□□.
- □□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□. □□ □□□□ □□□ □□ □□ □□ □□□□□ □□□□□□□□ □□□.

AWS □□ □□

Fabrikam□ ContosoAWSV□ □□□□ □□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.

- AWS EC2 □□□□□ □□ □□ □□ □□□ □□□□ □□ □□ Fabrikam□ □□ □□□□□ □□□□.
- □□ □□□□ Azure □□□□ □□ AWS □□□ □□□ □□□ □ □□□ □□□□□.

Contoso □□□ □□ □□

Fabrikam□ Contoso □□□□ □□ □□□ □□ □□ □□□ □□□□□□.

- □□ ContosoDevelopers □□□ □□□□ □□□□ □□□.
- Contoso □□□□ Sub1□ □□□□ □□□□□□ □□ contoso.onmicrosoft.com □□ □□□ □□□□ □□□.
- □□□ □□□□ ClaimDetails □□□□ MedicalHistory□□ □□ □□ □□□□ □ □ □□□ □ □□.

□□ □□ □□

Fabrikam□ Sub1□ □□ □□□ HIPPA HITRUST □□□ □□□□□ □□□□ □□□□□ □□ □. TestRG□ □□ □□□ □□ □□ □□□□ □□□□ □□□.

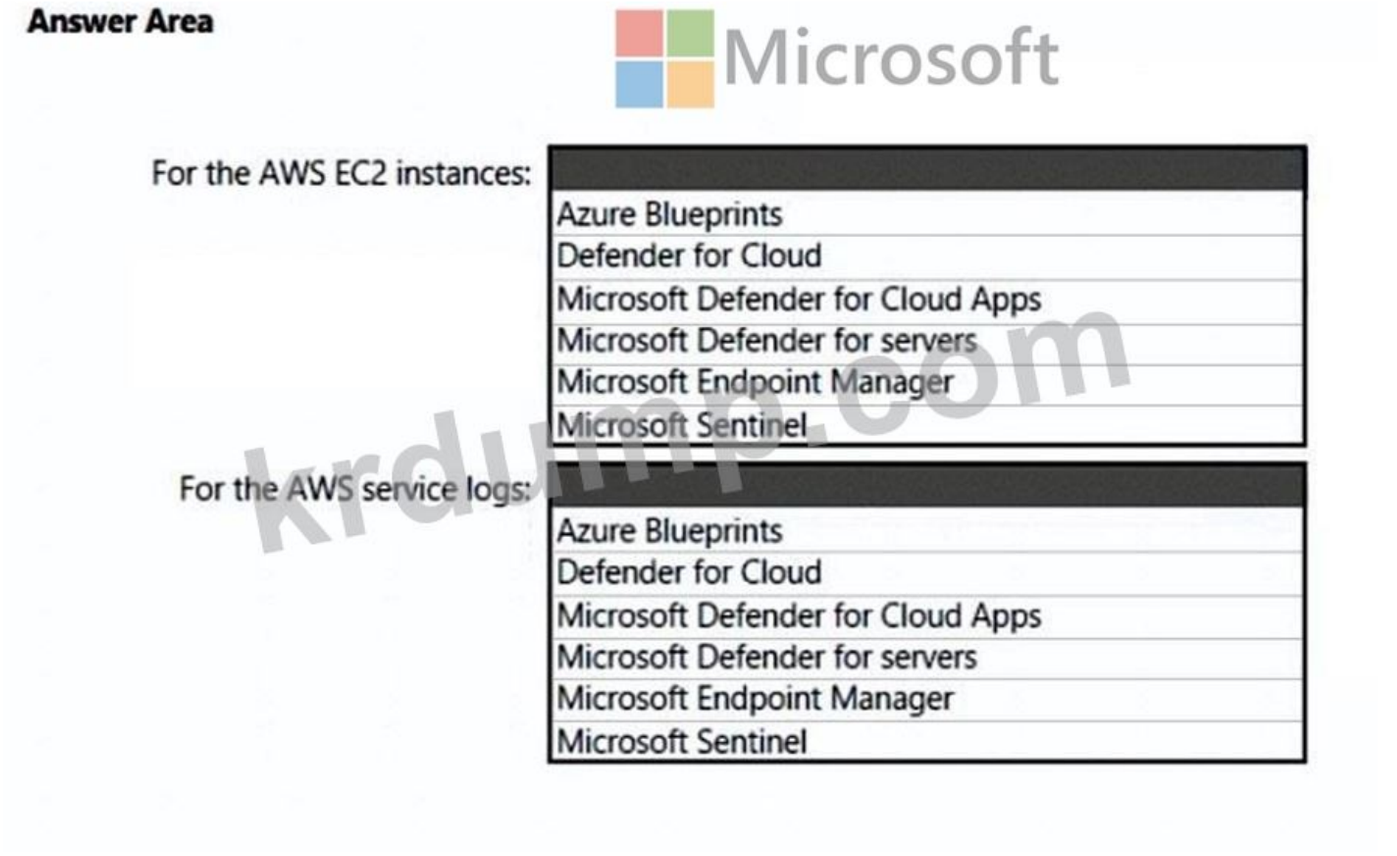
□□□ □□

AWS □□ □□□ □□□□ □□□□ □□□□ □□□.

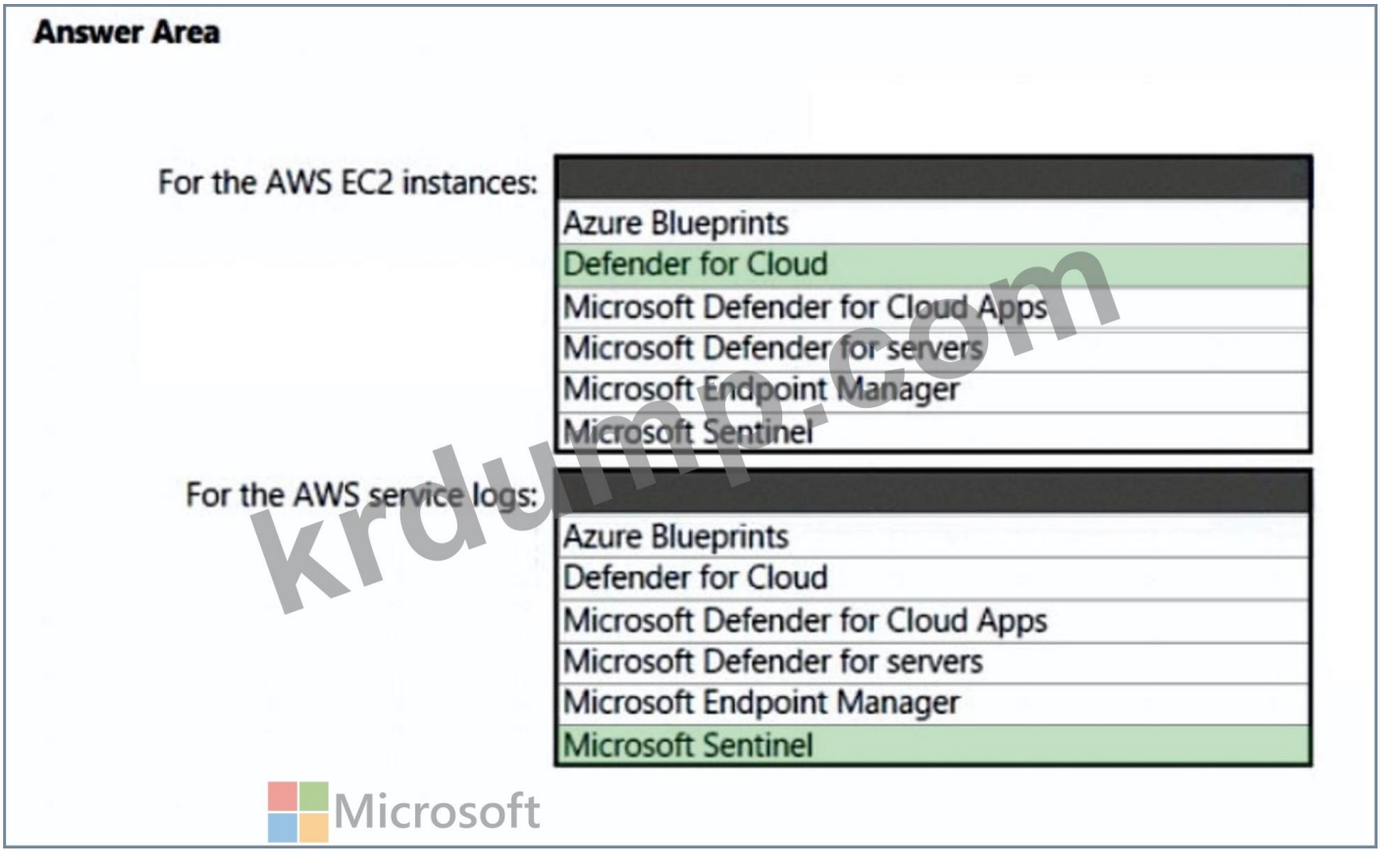
□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area



Answer:



Explanation:

Box 1: Defender for Cloud

The requirement is to identify EC2 instances which are noncompliant with secure score recommendations.

Box 2: Microsoft Sentinel
Use the Amazon Web Services (AWS) connectors to pull AWS service logs into Microsoft Sentinel. These connectors work by granting Microsoft Sentinel access to your AWS resource logs. Setting up the connector establishes a trust relationship between Amazon Web Services and Microsoft Sentinel. This is accomplished on AWS by creating a role that gives permission to Microsoft Sentinel to access your AWS logs.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings
https://docs.microsoft.com/en-us/azure/sentinel/connect-aws?tabs=s3

NEW QUESTION: 45
□□□□□ Azure□ Microsoft □□□□ □□ □□□□□□ □□□ □□ Azure □□□ □□□ □ □□ □□□□□.
Azure □□□□ NIST(National Institute of Standards and Technology) □□□ □□ □□□□□ (CSF)□ □□□□□ □□□□□ □□□□ □□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Purview□ □□ □□ □□□
B. □□□□□ Microsoft Defender
C. Microsoft Sentinel
D. □□□□ □□ Microsoft Defender
Answer: B (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

NEW QUESTION: 46
□□ □□ Azure □□□ □□, □ □□□□ □□ □□ □□□ □□□ □□□□ □□□□.
□ □□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□□ □□□. □□□□ □□ □□□ □□ □□□ □□□.
□□□ □□□□ □□□?
A. Privileged Identity Management(PIM)□ □□□ □□
B. Microsoft Entra ID Identity Governance□□ □□□ □□
C. Microsoft Defender □□ □□ □□ □□(Defender EASM) □□
D. Microsoft Entra □□ □□□ □□ □□□□
Answer: A (LEAVE A REPLY)
List role assignments at a scope
Important
Azure role assignment integration with Privileged Identity Management is currently in PREVIEW.
Follow these steps:
1. In the Azure portal, click All services and then select the scope. For example, you can select

Management groups, Subscriptions, Resource groups, or a resource.
2. Click the specific resource.
3. Click Access control (IAM).
4. Click the Role assignments tab to view the role assignments at this scope.
Reference:
https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-list-portal

NEW QUESTION: 47
Microsoft 365 □□□ Azure □□□ □□□□. Microsoft 365 Defender□ Microsoft Defender for Cloud□ □□□□□ □□□□.
Azure □□□□ 50□□ □□ □□□ □□□□ □□□□. □ □□ □□□ Windows Server 2019□ □ □□ □□ □□□□□□□ □□□□□.
□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□ □□, □□□□ □□ □□□□□□□ □□□ □ □□ □□□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. □□□□ □□ Microsoft Defender□ □ □□ □□ □□ □□
B. Defender for Cloud□ □□□ □□□□□□ □□
C. Defender for Cloud□ Azure Security Benchmark □□ □□ □□
D. Microsoft Endpoint Manager□ □ □□ □□
Answer: B (LEAVE A REPLY)
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes.
Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy
https://docs.microsoft.com/en-us/security/benchmark/azure/overview

NEW QUESTION: 48
□□□ □□□ Azure App Service □□□ □□□□ □□□□. □□□ □□□ □□□ □□□□ □ □ □□□ □□□ □□□□ □□□□.
□□□□ □□ □□ □□, □□□ □□□ □□□□(XSS), SQL □□□ □□ □□□□ □□ □ □□ □□□□□ □□ □□□□ □□□□ □□□. □□□ □□□ □□□□ □□□?
A. □□□ □□□□□□ □□ □□□(IAST)
B. □□ □□□□□□ □□ □□□(SAST)
C. □□□ □□□□□□ □□ □□(RASP)
D. □□ □□□□□□ □□ □□□(DAST)
Answer: D (LEAVE A REPLY)
DAST tools analyze programs while they are executing to find security vulnerabilities such as memory corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.
Reference:
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

NEW QUESTION: 49
□□□□□ □□□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□ □ Windows Server 2022□ □□□□ Serve1□□□ □□□ □□□□.
□□□□□ Microsoft Entra □□□□ □□□ Azure □□□ □□□, □ □□□□ User1□□□ □□ □□ □□□□ □□□□. User1□ □□□□ □□□□□.
User1□ □□□□ □□ Server1□ RDP □□□ □□□ □ □□□ □□□□ □□□. □□□□ User1□ □□ □□(MFA)□ □□□□ □□□□□ □□ □□□.
□□□□ □□□ □□□□ □□□?
A. Windows □□ □□
B. Microsoft Entra □□□ □□□
C. Azure □□
D. Microsoft Entra Private Access
Answer: (SHOW ANSWER)
Azure Bastion can be used to establish RDP connections for a user in an Azure tenant to an on-premises server in an Active Directory Domain Services (AD DS) domain, and it can be configured to require multifactor authentication (MFA) for those connections. Azure Bastion provides secure and seamless RDP connectivity to VMs, including those within an AD DS domain, directly from the Azure portal over SSL, without exposing them to public IP addresses.
Reference:
https://learn.microsoft.com/en-us/entra/identity/domain-services/secure-remote-vm-access
NEW QUESTION: 50
□□□ □□

Linux□ □□□□ □□□□□ □□□ 1,000□ □□□□.
WS1□□□ Microsoft Sentinel □□ □□□ □□□ Azure □□□ □□□□.
Linux□ □□□□ □□ □□□ 1,000□ □□□□.
□□ □□□□□ Linux □□□ Azure Arc□ □□□□□.
Microsoft Sentinel□ Azure Monitor Agent □□□□ □□□□ CEF(Common Event Format) □□ □ □□□ □□□□□.
□□□□ □□ □□□□ □□□□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □ □□□.
- □□□ Microsoft Entra ID□ □□ □□□□□□.
- WS1□ □□□□ □□□ □□ □□□□□□.
- □□□ □□ □□□□ □□□□□□ □□□□□.
- □□□ □□□ □□□□□□.
□□□ □□□ □□□□ □□□? □□□□ □□□□ □□□□ □□□□□.
□□: □□□ 1□□□□.

Answer Area

To minimize the number of events:

- Create Data collection rules (OCRs).
- Filter Microsoft Sentinel scheduled query rules.
- Set a daily cap for WS1.

To minimize the number of Microsoft Entra ID identities, enable:

- System-assigned managed identities for all the on-premises servers and Azure virtual machines
- System-assigned managed identities for the on-premises servers and user-assigned managed identities for the Azure virtual machines
- User-assigned managed identities for all the on-premises servers and Azure virtual machines
- User-assigned managed identities for the on-premises servers and system-assigned managed identities for the Azure virtual machines

Answer:

Answer Area

To minimize the number of events:

- Create Data collection rules (OCRs).
- Filter Microsoft Sentinel scheduled query rules.
- Set a daily cap for WS1.

To minimize the number of Microsoft Entra ID identities, enable:

- System-assigned managed identities for all the on-premises servers and Azure virtual machines
- System-assigned managed identities for the on-premises servers and user-assigned managed identities for the Azure virtual machines
- User-assigned managed identities for all the on-premises servers and Azure virtual machines
- User-assigned managed identities for the on-premises servers and system-assigned managed identities for the Azure virtual machines

Explanation:

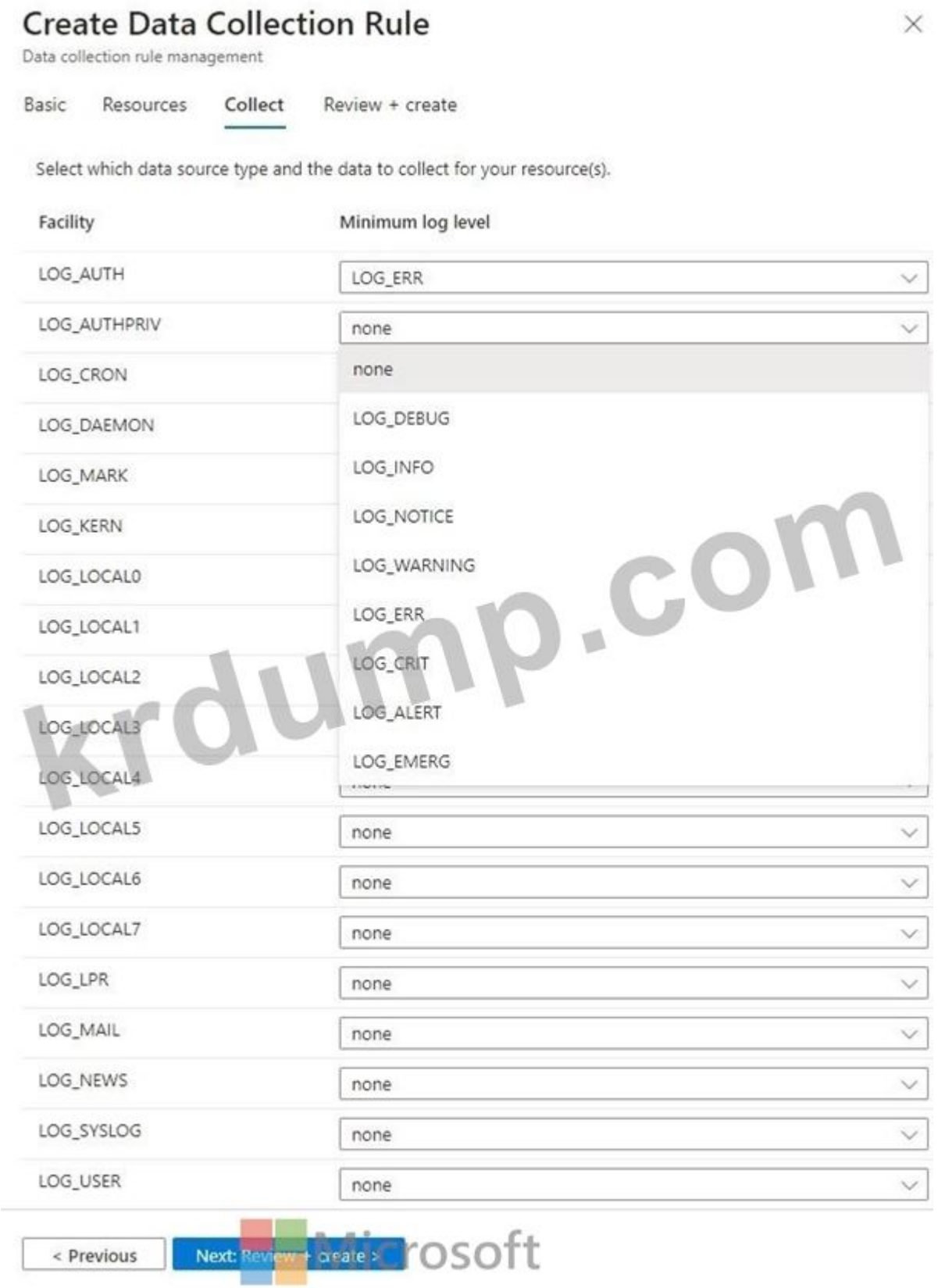
Box 1: Create Data collection rules (OCRs)

Minimize the number of events delivered to WS1.

Ingest syslog and CEF messages to Microsoft Sentinel with the Azure Monitor Agent Use the Syslog via AMA and Common Event Format (CEF) via AMA connectors to quickly filter and ingest syslog messages, including messages in Common Event Format (CEF), from Linux machines and from network and security devices and appliances.

Create data collection rule (DCR)

To get started, open either the Syslog via AMA or Common Event Format (CEF) via AMA data connector in Microsoft Sentinel and create a data collection rule (DCR).
Note: See step 10 below.
1. For Microsoft Sentinel in the Azure portal, under Configuration, select Data connectors. For Microsoft Sentinel in the Defender portal, select Microsoft Sentinel > Configuration > Data connectors.
2. For syslog, type Syslog in the Search box. From the results, select the Syslog via AMA connector. For CEF, type CEF in the Search box. From the results, select the Common Event Format (CEF) via AMA connector.
3. Select Open connector page on the details pane.
4. In the Configuration area, select +Create data collection rule.
5. In the Basic tab:
Type a DCR name.
Select your subscription.
Select the resource group where you want to locate your DCR.
6. Select Next: Resources >.
7. Use the available filters or search box to find your log forwarder VM. Expand a subscription in the list to see its resource groups, and a resource group to see its VMs.
8. Select the log forwarder VM that you want to install the AMA on. The check box appears next to the VM name when you hover over it.
9. Select the log forwarder VM that you want to install the AMA on. The check box appears next to the VM name when you hover over it.
*-> 10. In the Collect tab, select the minimum log level for each facility. When you select a log level, Microsoft Sentinel collects logs for the selected level and other levels with higher severity. For example, if you select LOG_ERR, Microsoft Sentinel collects logs for the LOG_ERR, LOG_CRIT, LOG_ALERT, and LOG_EMERG levels.



11. Review your selections and select Next: Review + create.

Box 2: System-assigned managed identities for all on-premises servers and uses-assigned managed identities for the Azure virtual machines.

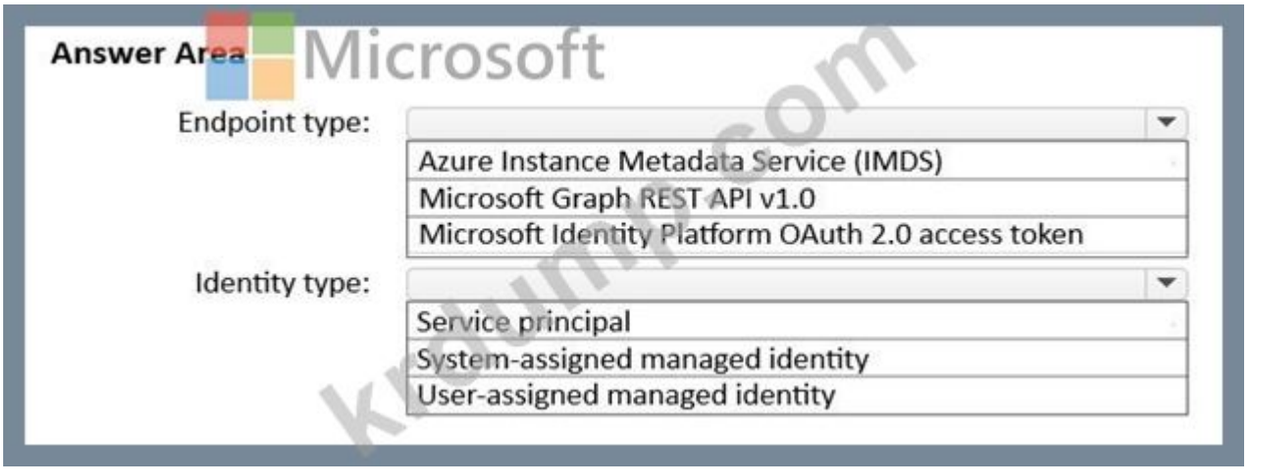
Minimize the number of Microsoft Entra ID identities required.

* On-premises servers

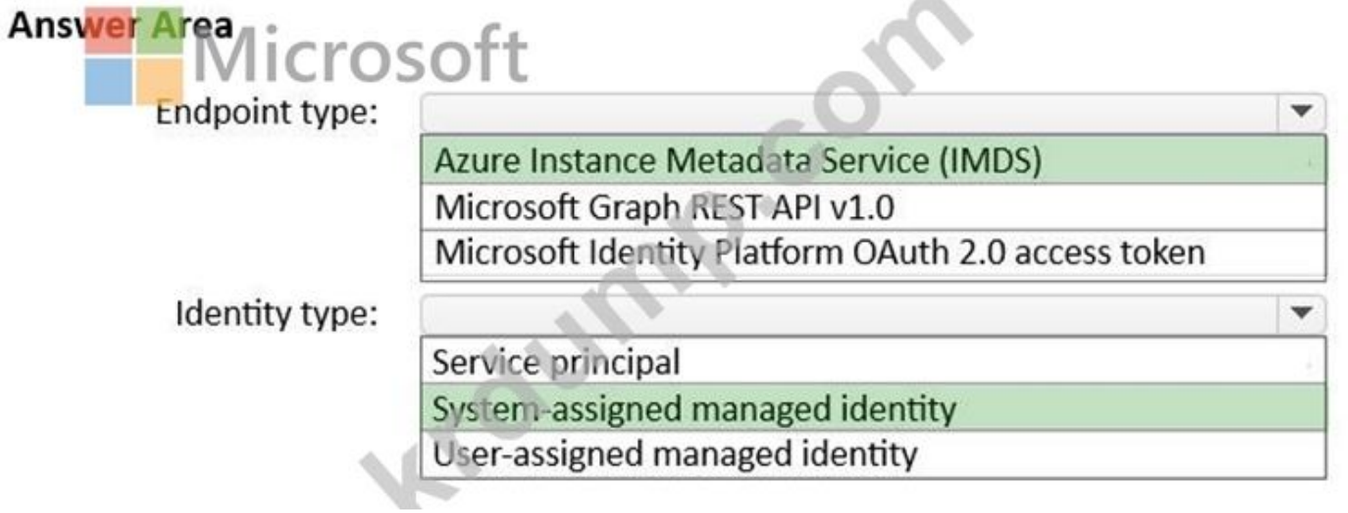
Managed identity

At creation, the Microsoft Entra ID system-assigned identity can only be used to update the status of the Azure Arc-enabled servers, for example, the 'last seen' heartbeat. Grant identity access to Azure resources to enable applications on your server to access Azure resources, for example, to request secrets from a Key Vault.
* Azure virtual machines
User assigned managed identities can be used on more than one resource.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/hybrid/arc-enabled-servers/eslz-identity-and-access-management

NEW QUESTION: 51
□□□ □□
Vault1□□□ □□□ Azure Key Vault□ □□□ Azure □□□ □□□□.
App1□□□ □□□ □□ □□ □□□□ □□ □□ □□□ □□□ □□□□□. App1□ Vault1□ □ □□ □□ □□□ □□□□□. □□ □□□ App1□ □□ □□□ □□ □□□□□ □□□□□□.
App1□ Vault1□ □□□ □□□ □□□ □ □□□ □□ □□□□ □□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□.
- Vault1□ □□□□ □ □□ □□ □□□ □□ □□□□□□.
- □□ □□□ □□□ □□□□ □□□□ □□ □□□□□□.
- □□□ □□□ □□□□□□.
App1□ □□□ □□□□ □□ □□ □□□ □□□□□□ □□□□ □□, □□ □□□ ID□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Azure Instance Metadata Service (IMDS)

You can use Azure Instance MetaData Service (IMDS) to access KeyVault and more from applications inside VM.

Why do we need IMDS API's?

Applications inside the VM cannot be mapped to a Managed Identity and hence the only way they can establish connection to other Azure Resources is via connection string or some key. This is what we are trying to avoid.

With the help of these dedicated API's we will try to connect to azure resources without the need of keys and connection string Important Points to remember about IMDS APIs

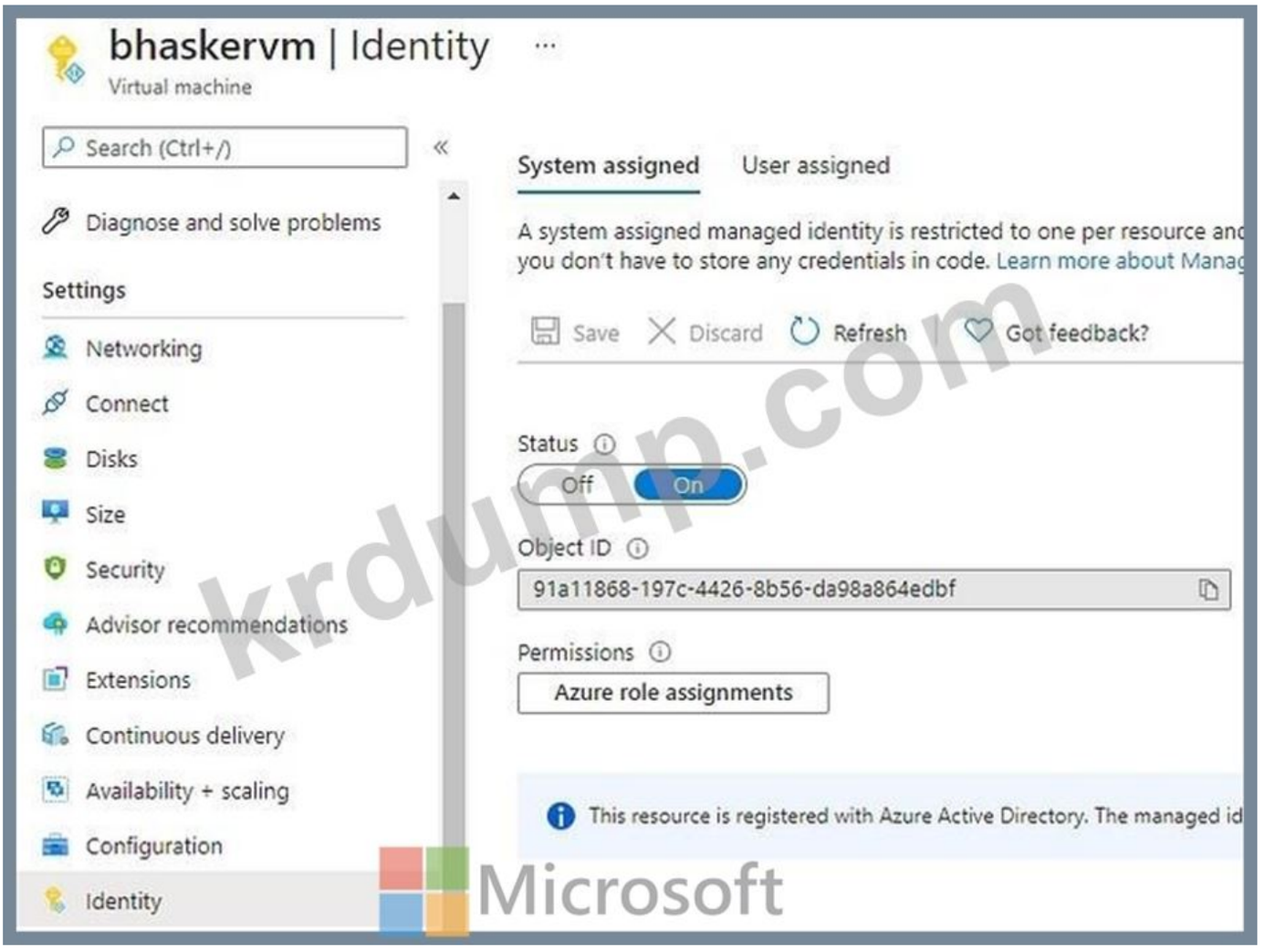
1. These API endpoints are available at a well-known non-routable IP address (169.254.169.254)
2. It can be accessed only from within VM
3. Communication between IMDS and VM never leaves the host

Note: The Azure Instance Metadata Service (IMDS) provides information about currently running virtual machine instances. You can use it to manage and configure your virtual machines. This information includes the SKU, storage, network configurations, and upcoming maintenance events.

Box 2: System-assigned managed identity

DEMO

In this demo we will try to establish connection from an running inside virtual machine to key vault.



1. Go to the Virtual Machine you created
2. Click on Identity tab on your Virtual Machine Blade.
3. Toggle "On" of the status under System assigned.

* Details omitted *

You have successfully communicated to Key Vault without using any credentials not saving sensitive information anywhere. The same rules apply to access other azure resources.

NEW QUESTION: 52

□□□ □□

Microsoft 365 □□□□ □□□□.

□□□□ □□□ □□□□ □□ Microsoft 365 Defender □□□□ □□□□ □□□.

□□□□ □□ □□ □□□ □□□□ □□□.

- Microsoft SharePoint Online □□□□□ □□□□□□ □□ □□ □□□ □□□□□□ □□□ □□ □□□ □□□□□ □□□□ □□ □□□□ □□□□□.

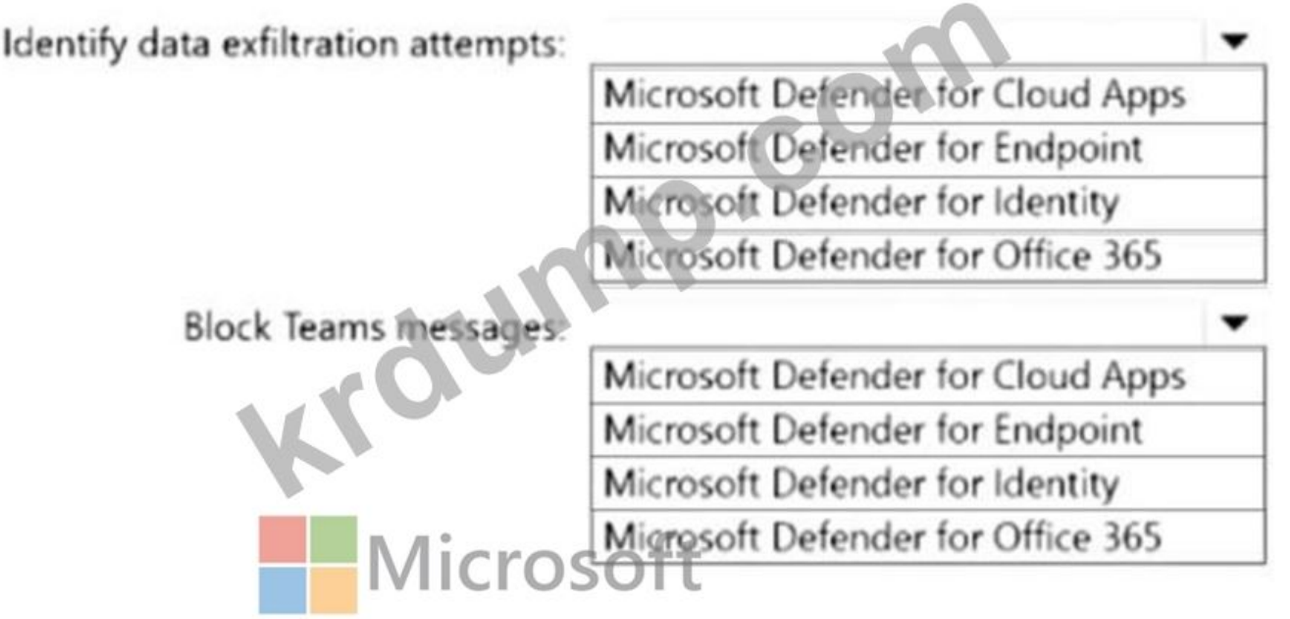
- □□□□□ □□□□ □□□ □□□□ Microsoft Teams □□□□ □□□□□.

0□□ □□ □□(ZAP)□ □□□□ □□□□ □□□□□.

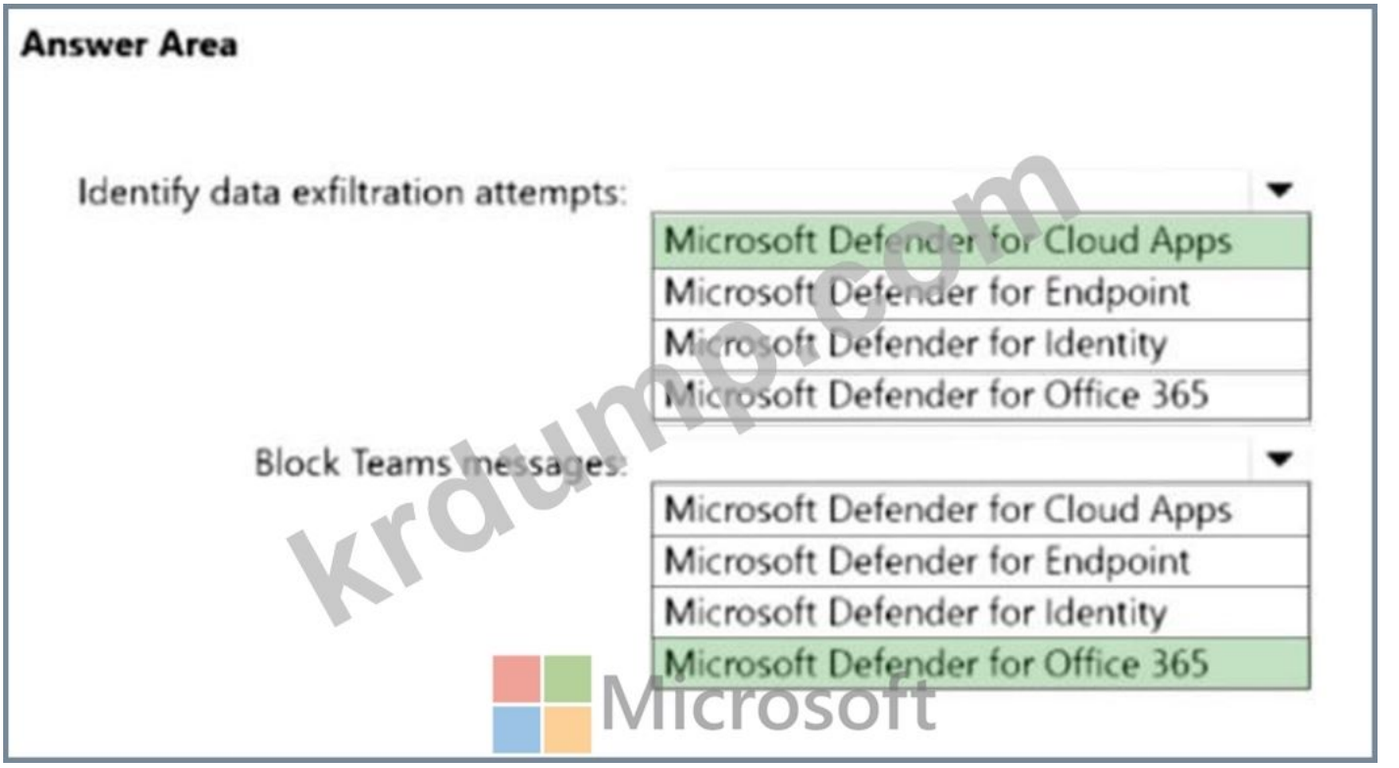
□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □.

□□: □□ □□□ 1□□□□.

Answer Area



Answer:



Explanation:

Box 1: Microsoft Defender for Cloud Apps

Identify users that are downloading an unusually high number of files from Microsoft SharePoint Online sites and are possibly involved in a data exfiltration attempt.

Data exfiltration protection access controls

Microsoft Defender for Cloud Apps

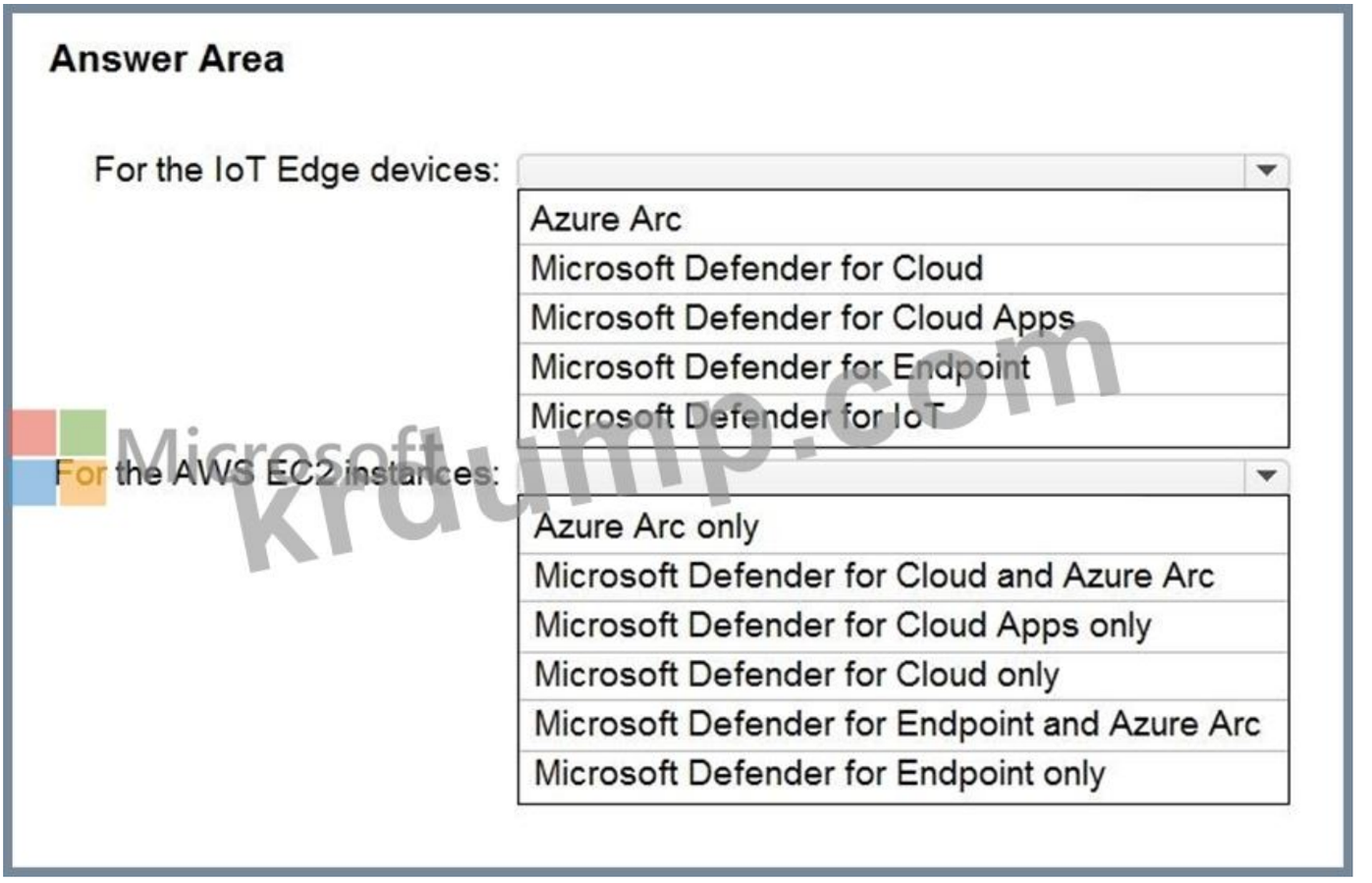
Actions that would compromise the security of customer data must be detected and prevented. For example, employees may be using an unapproved cloud application for storing sensitive

corporate data or downloading a vast number of sensitive files for exfiltration. These actions can be prevented by Microsoft Defender for Cloud Apps.
Box 2: Microsoft Defender for Office 365
Block Microsoft Teams messages that contain potentially malicious content by using zero-hour auto purge (ZAP).
Zero-hour auto purge (ZAP) is a feature of Microsoft Defender for Office 365.
Reference:
https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge

NEW QUESTION: 53
Microsoft Defender XDR□ Microsoft Purview□ □□□□ Microsoft 365 □□□ □□□□.
Microsoft SharePoint Online □□□□□ □□□ □□□□ □□□ File1□□□ □□□ □□□□.
□□□□ SharePoint □□□□□ FileI□ □□□□□ □ □□□ □□□ □□□ □□ □□□□ □□ □□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□□□ □□ Microsoft Defender
B. □□□□□ Microsoft Defender
C. Office 365□ Microsoft Defender
D. Microsoft Entra □□□□□□ □□□
Answer: (SHOW ANSWER)
Conditional Access app control in Microsoft Defender for Cloud Apps
Activities in Conditional Access app control
Conditional Access app control uses access policies and session policies to monitor and control user app access and sessions in real time, across your organization.
Each policy has conditions to define who (which user or group of users), what (which cloud apps), and where (which locations and networks) the policy is applied to. After you determine the conditions, route your users first to Defender for Cloud Apps. There, you can apply the access and session controls to help protect your data.
Access and session policies include the following types of activities:
* Require authentication context
Reevaluate Microsoft Entra Conditional Access policies when a sensitive action occurs in the session, such as requiring multifactor authentication.
* Etc.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

NEW QUESTION: 54
□□□ □□
□□□ □□□□ Microsoft 365 □□, Azure □□ □ Amazon Web Services(AWS) □□□ □□□

□□ □□□□ □□□ □□□□.
□□ □□ □□□ □□ □□ □□ □□ □□□□ □□□□ □□□.
- Azure IoT Edge □□□□
- AWS EC2 □□□□
□□□□ □□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□□ 1□□□□.



Answer:

Answer Area

For the IoT Edge devices:

- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:

- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Explanation:

Box 1: Microsoft Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Azure IoT Edge provides powerful capabilities to manage and perform business workflows at the edge. The key part that IoT Edge plays in IoT environments make it particularly attractive for malicious actors.

Defender for IoT azureiotsecurity provides a comprehensive security solution for your IoT Edge devices. Defender for IoT module collects, aggregates and analyzes raw security data from your Operating System and container system into actionable security recommendations and alerts.

Box 2: Microsoft Defender for Cloud and Azure Arc

Microsoft Defender for Cloud provides the following features in the CSPM (Cloud Security Posture Management) category in the multi-cloud scenario for AWS.

Take into account that some of them require Defender plan to be enabled (such as Regulatory Compliance):

* Detection of security misconfigurations
* Single view showing Security Center recommendations and AWS Security Hub findings
* Incorporation of AWS resources into Security Center's secure score calculations
* Regulatory compliance assessments of AWS resources

Security Center uses Azure Arc to deploy the Log Analytics agent to AWS instances.

Incorrect:

AWS EC2 Microsoft Defender for Cloud Apps

Amazon Web Services is an IaaS provider that enables your organization to host and manage their entire workloads in the cloud. Along with the benefits of leveraging infrastructure in the cloud, your organization's most critical assets may be exposed to threats. Exposed assets include storage instances with potentially sensitive information, compute resources that operate some of your most critical applications, ports, and virtual private networks that enable access to your organization.
Connecting AWS to Defender for Cloud Apps helps you secure your assets and detect potential threats by monitoring administrative and sign-in activities, notifying on possible brute force attacks, malicious use of a privileged user account, unusual deletions of VMs, and publicly exposed storage buckets.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/security-edge-architecture
https://samilamppu.com/2021/11/04/multi-cloud-security-posture-management-in-microsoft-defender-for-cloud/

NEW QUESTION: 55
□□ □□ □□(OT) □□□ IoT □□□ □□□□.
Microsoft □□□ □□ □□ □□□□(MCRA)□ □□□□ OT □ IoT □□□ □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□□□ □□ □□ □□□ □□□□□ □ □□.
□□ □□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□ □□ □□□□ □□□ □□□□ □.
□□: □□ □□□ 1□□□□.
A. □□ □□□
B. □□ □□□□
C. □□□□□ □□
D. □□ □□□ □□□□
Answer: B,D (LEAVE A REPLY)
Adapt processes to Operational Technology (OT) - Adjust your tools and processes to the constraints of OT environments as you integrate them. These environments prioritize safety and often have older systems which don't have patches available and may crash from an active scan. Focusing on approaches like passive network detections for threats and isolation of systems is often the best approach.
https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/3-recommend-for-protecting-from-insider-external-attacks

NEW QUESTION: 56
□□□ □□□ 10□□ □□□ □□□□ □□□□. □ □□□□ Windows Server□ □□□□ □□ □□□ □□ □□□ Windows 11 □□ macOS□ □□□□ □□ □□ □□□ □□□□. □ □□□ □ Microsoft Intune□ □□□□ □□□□.

Microsoft Entra □□□□ □□□□.
□□□□□ □□□□ □□ □□□□ □□ □ □□□□ □□□□□ Global Secure Access□ □□ □□ □□□. □ □□□□ □□ □ □□□ □□ □ □□□□ Global Secure Access□ □□ □□□ □□ □□ □□□.
□ □□□□ □□ □□ □□□ □□ □□□?
A. □ □□□ Microsoft Defender for Endpoint□ □□□□□ □□ Intune □□□ □□□□□.
B. □□□□ IPsec □□□ □□□□□.
C. □□ □□□ Microsoft Entra □□ □□□□ □□□□ □□□□□.
D. □ □□□ Global Secure Access □□□□□□ □□□□ □□ Intune □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Configure private network connectors for Microsoft Entra Private Access and Microsoft Entra application proxy Connectors are lightweight agents that sit on a server in a private network and facilitate the outbound connection to the Global Secure Access service.
Connectors must be installed on a Windows Server that has access to the backend resources and applications. You can organize connectors into connector groups, with each group handling traffic to specific applications.
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors

NEW QUESTION: 57
Microsoft 365 □□□ Azure □□□ □□□□. Microsoft 365 Defender□ Microsoft Defender for Cloud□ □□□□□ □□□□.
Azure □□□□ 50□□ □□ □□□ □□□□ □□□□. □ □□ □□□ Windows Server 2019□ □ □□ □□ □□□□□□□ □□□□□.
□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□ □□, □□□□ □□ □□□□□□□ □□□ □ □□ □□□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. □□□□ □□ Microsoft Defender□ □ □□ □□ □□ □□
B. Azure AD □□□ □□□ □ □□ □□
C. Defender for Cloud□ □□□ □□□□□□ □□
D. Microsoft Endpoint Manager□ □ □□ □□
Answer: C (LEAVE A REPLY)
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any

application runs other than the ones you've defined as safe.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy
https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy
https://docs.microsoft.com/en-us/security/benchmark/azure/overview

NEW QUESTION: 58
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□ □□□ Windows 10□ □□□□ 45□□ □□□ □□ □□□ □□□□□ □□□ □□□□□. □ □□□□ □□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□ □.
* □□□□□□ □□□ □□□□□□□ □□□ □ □□□ □□□.
* □□□ □□□ □□□ □□□□□ □□□□□ □□□□□.
□□ □ □□ □□□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□. □□:
□ □□□ 1□□□□.
A. □□□□□ Azure Monitor□ □□□□□.
B. □□□□□ □□ □□ □□ □□□ □□□□□□(PAW)□ □□□□□.
C. Microsoft Defender for Endpoint□ □□ □□ □ □□(AIR)□ □□□□□.
D. Endpoint□ Microsoft Defender□□ □□ □ □□□ □□□ □□□□□.
E. Microsoft Intune□ Microsoft Defender for Endpoint□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
Vuln management sits on top of defender for endpoint.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide

NEW QUESTION: 59
□□□ Microsoft 365 □□□ □□□□ □□□ Microsoft Defender for Identity□ □□□□ □□□ □.
□□ □□□ □□□ □□□ □□ □□□□□□.
□□□□ □□□ □ □□□ □□ □□□ □□□□ □□□□ □□□□ □□□. □□□□ □□□ □ □□□□ □□ □□□ □□□□□□ □□□. □□ Defender for Identity □□□ □□□ □□□□ □ □□?
A. □□□ □□
B. □□□□ □□□ □□
C. □□□ □□□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)
Honeytoken tags
Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.

https://docs.microsoft.com/en-us/defender-for-identity/entity-tags

NEW QUESTION: 60

□□□ □□

MSW1□□□ Microsoft Sentinel □□ □□□ □□□ Azure □□□ □□□□.

MSW11□□ 50□□ □□□ □□ □□□ □□□□ □□□□.

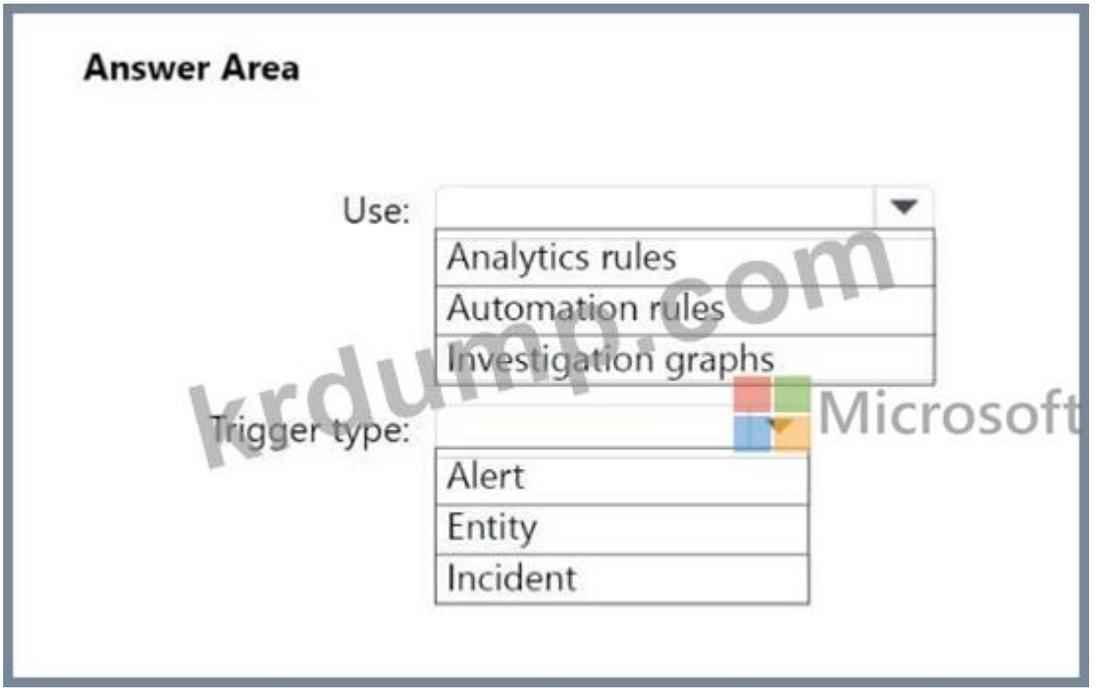
Microsoft Sentinel □□□□□ □□□□ □□ □□□□□□□ □□ □□(SOAR) □□□□ □□□ □ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

- □□□□□ □□□ □ □□ □□□ □□□ □ □□□ □□□□□.
- □□ □□□ □□□ □□ □□□ □□□□□□.

□□ □□.

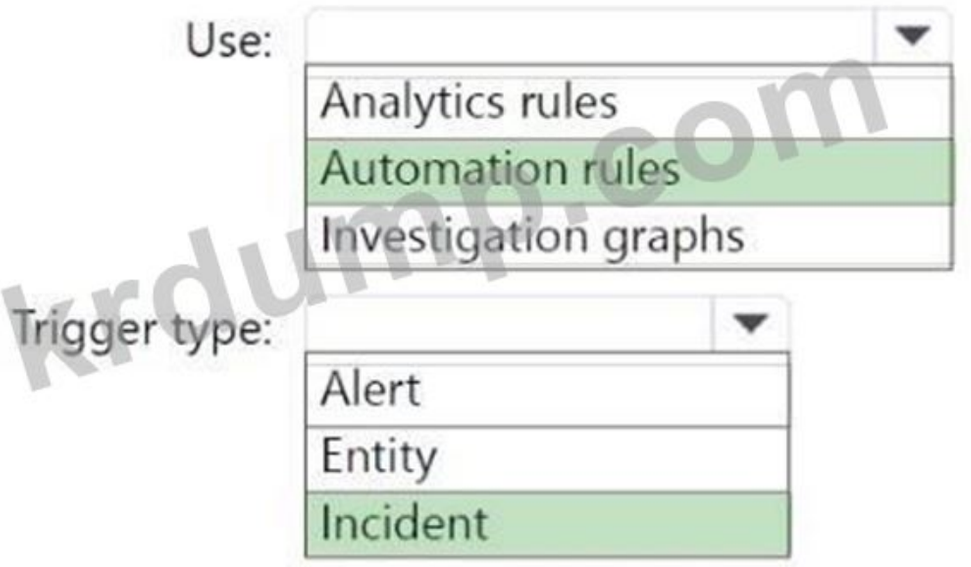
□□□□□ □□□□□ □□□ □□□□ □□, □□ □□□ Microsoft Sentinel □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:

Answer Area



Explanation:
Box 1: Automation rules
You can respond to threats by using playbooks with automation rules in Microsoft Sentinel Box 2: Incident Use triggers and actions in Microsoft Sentinel playbooks For most use cases, incident-triggered automation is the preferable approach. In Microsoft Sentinel, an incident is a "case file" ?an aggregation of all the relevant evidence for a specific investigation. It's a container for alerts, entities, comments, collaboration, and other artifacts.
Unlike alerts which are single pieces of evidence, incidents are modifiable, have the most updated status, and can be enriched with comments, tags, and bookmarks. The incident allows you to track the attack story which keeps evolving with the addition of new alerts.
For these reasons, it makes more sense to build your automation around incidents. So the most appropriate way to create playbooks is to base them on the Microsoft Sentinel incident trigger in Azure Logic Apps.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION: 61
Microsoft 365 □□□ Azure □□□ □□□□. Microsoft 365 Defender□ Microsoft Defender for Cloud□ □□□□□ □□□□.
Azure □□□□ 50□□ □□ □□□ □□□□ □□□□. □ □□ □□□ Windows Server 2019□ □ □□ □□ □□□□□□□ □□□□□.

□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□ □□, □□□□ □□ □□□□□□□ □□□ □ □□ □□□□ □□□□ □□□.

□□ □□ □□□ □□□□ □□□?

A. □□□□ □□ Microsoft Defender□ OAuth □ □□

B. Defender for Cloud□ Azure Security Benchmark □□ □□ □□

C. Endpoint□ Microsoft Defender□ □□ □□□□ □□ □□

D. □□□□ □□ Microsoft Defender□ □ □□ □□ □□ □□

Answer: C (LEAVE A REPLY)

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

NEW QUESTION: 62

Microsoft Cloud Adoption Framework for Azure□ □□ □□ □□□ □□□□ □□□ Azure □□ □ □□□□ □□□□. □ □□□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□□□□ □ □ □□ □□ □ □□ □□□□□.

□□□□ □□ □□(NSG), Azure Firewall, Azure Key Vault, Azure Bastion□ □□□□ □□ □□ □□ □□□□ □□□. □ □□□□ □□ □□□ □□□□□ Azure□ Microsoft □□□□ □□ □ □□□□□ □□ □□ □□□ □□□□ □□□.

□□□□□ □□□ □□□□ □□□?

A. Azure □□ □ □□□

B. Azure Well-Architected □□□□□

C. Azure □□ □□□□ v3

D. Azure □□□□□

Answer: A (LEAVE A REPLY)

The most simple solution is to host a jumpbox on the virtual network of the data management landing zone or data landing zone to connect to the data services through private endpoints.

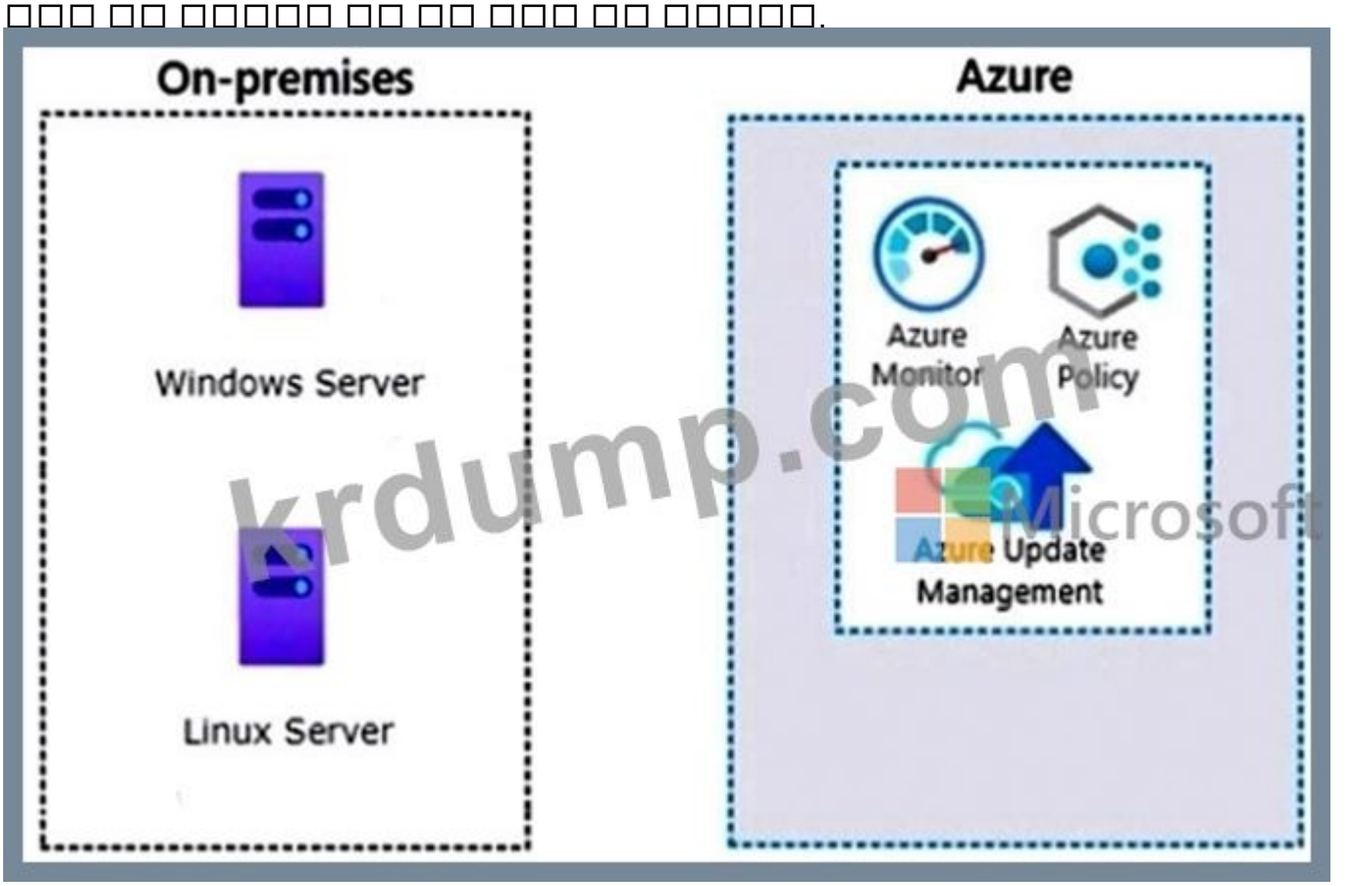
Azure Bastion provides a few other core security benefits, including:

* The service integrates with native security appliances for an Azure virtual network, such as Azure Firewall.

Note:

* Platform landing zones: Subscriptions deployed to provide centralized services, often operated by a central team, or a number of central teams split by function (e.g. networking, identity), which will be used by various workloads and applications. Platform landing zones represent key services that often benefit from being consolidated for efficiency and ease of operations. Examples include networking, identity, and management services.
* The Azure App Service landing zone accelerator is an open-source collection of architectural guidance and reference implementation to accelerate deployment of Azure App Service at scale. It can provide a specific architectural approach and reference implementation via infrastructure as code templates to prepare your landing zones. The landing zones adhere to the architecture and best practices of the Cloud Adoption Framework.
Reference:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/cloud-scale-analytics/architectures/connect-to-environments-privately
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/
https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v3
https://learn.microsoft.com/en-us/azure/architecture/framework/

NEW QUESTION: 63
□□□ □□□ □□□□□ □□□□ □□□□ □□□ □□□□.
□□□□ □□□□□□□ □□□□ □□ □□ □□□□□ □□□□□.
□□□ □□ □□□□□ □□ □□ □□□ □□ □□□□□.



□□□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□. □□□□ □□ □ □ □□□ □□□□ □□□.

- □□ □□□□ □□ □□□ □□□ □□□□□.
- □□ □□□□ □□ □□□□ □□ □□□ □□□□□.
Azure Policy□ □□□□.
□□□□□ □□□□□ □□ □ □□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □ □□□□.
□□: □□ □□□ 1□□□□.
A. Azure VPN □□□□□
B. Azure Policy□ □□□ □□
C. □□□□□ □□□ □□□□□
D. Azure □□
E. Azure Arc
Answer: B,E (LEAVE A REPLY)
B: Azure Policy's guest configuration feature provides native capability to audit or configure operating system settings as code, both for machines running in Azure and hybrid Arc-enabled machines. The feature can be used directly per-machine, or at-scale orchestrated by Azure Policy.
Configuration resources in Azure are designed as an extension resource. You can imagine each configuration as an additional set of properties for the machine.
E: Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.
Microsoft recently [2019/2020] released Azure Arc, which unlocks new hybrid scenarios for organizations by bringing new Azure services and management features to any infrastructure.
Reference:
https://techcommunity.microsoft.com/t5/azure-developer-community-blog/azure-arc-for-servers-getting-started/ba-p/1262062
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/guest-configuration

NEW QUESTION: 64
Microsoft 365 □□□ □□□□.
Microsoft □□□ □□ □□ □□□□(MCRA)□ Zero Trust □□□ □□□ □□□ □□□ □□□□ □□□□ □□□□.
□□ Azure AD □□□□ □□ □□□□ □□ □□□(NRT)□□ Microsoft Exchange Online, SharePoint Online □ Teams□ □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□.
- □□□ □□□ □□□□□□□ □□□□□□□.
- □□□□ □□□□□ □□□□□ □□□□□□.
- □□□□ □□ □□ □□ □□□ □□□□□.
- □□□□ □□ □□ □□ □□(MFA)□ □□□□□ □□□□.
□□□□ □□ □ □□ □□□ □□□□ □□□? □□□ □□ □□□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

A. □□□□ □□ □□
B. Azure AD □□□□□□ □□□
C. □□□ □□ □□
D. Azure AD □□ □□ ID □□(PIM)
E. □□□ □□□
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

NEW QUESTION: 65
Azure Cosmos DB Core(SQL) API □□□ □□ □□ □□ □□□ □□□□ □□□□. Azure Cosmos DB □□□ □□□□ □□□□□ □□ □□□□ □□□□ □□□□ □□□□ □□□. □ □□ □□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□. □□: □ □□ □ 1□□□□.
A. Cosmos DB□ Microsoft Defender□ □□□□□□.
B. Azure Active Directory(Azure AD) □□□ □□□ Log Analytics □□ □□□□ □□□□.
C. Azure Cosmos DB□ □□ □□ □□□ □□□□□□□□.
D. Microsoft Defender for Identity□ □□□□□□.
E. Azure Cosmos DB □□□ Log Analytics □□ □□□□ □□□□.
Answer: B,C (LEAVE A REPLY)
LT-2: Enable threat detection for Azure identity and access management
Guidance: Azure Active Directory (Azure AD) provides the following user logs, which can be viewed in Azure AD reporting or integrated with Azure Monitor, Microsoft Sentinel, or other SIEM/monitoring tools for more sophisticated monitoring and analytics use cases:
Sign-ins - The sign-ins report provides information about the usage of managed applications and user sign-in activities.
Audit logs - Provides traceability through logs for all changes done by various features within Azure AD. Examples of audit logs include changes made to any resources within Azure AD, like adding or removing users, apps, groups, roles, and policies.
Disable local authentication methods so that your Cosmos DB database accounts exclusively require Azure Active Directory identities for authentication.
Enforcing RBAC as the only authentication method
In situations where you want to force clients to connect to Azure Cosmos DB through RBAC exclusively, you have the option to disable the account's primary/ secondary keys. When doing so, any incoming request using either a primary/secondary key or a resource token will be actively rejected.
Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline
https://docs.microsoft.com/en-us/azure/cosmos-db/policy-reference
https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac#disable-local-auth

NEW QUESTION: 66

□□□ □□

Microsoft 365 Defender□ □□□□ □□□□ Microsoft 365 □□□ □□□□.

Microsoft Sentinel□ □□□□ Microsoft 365 □ Microsoft 365 Defender□ □□□□ □□□□□□ □□ □□ □□□ □□□□ □□□□.

□□ □□ □□□ □□□□ □□□□ □□□□ □□□.

- Microsoft Sentinel□ □□ □□ □□□□□ □□□□□.

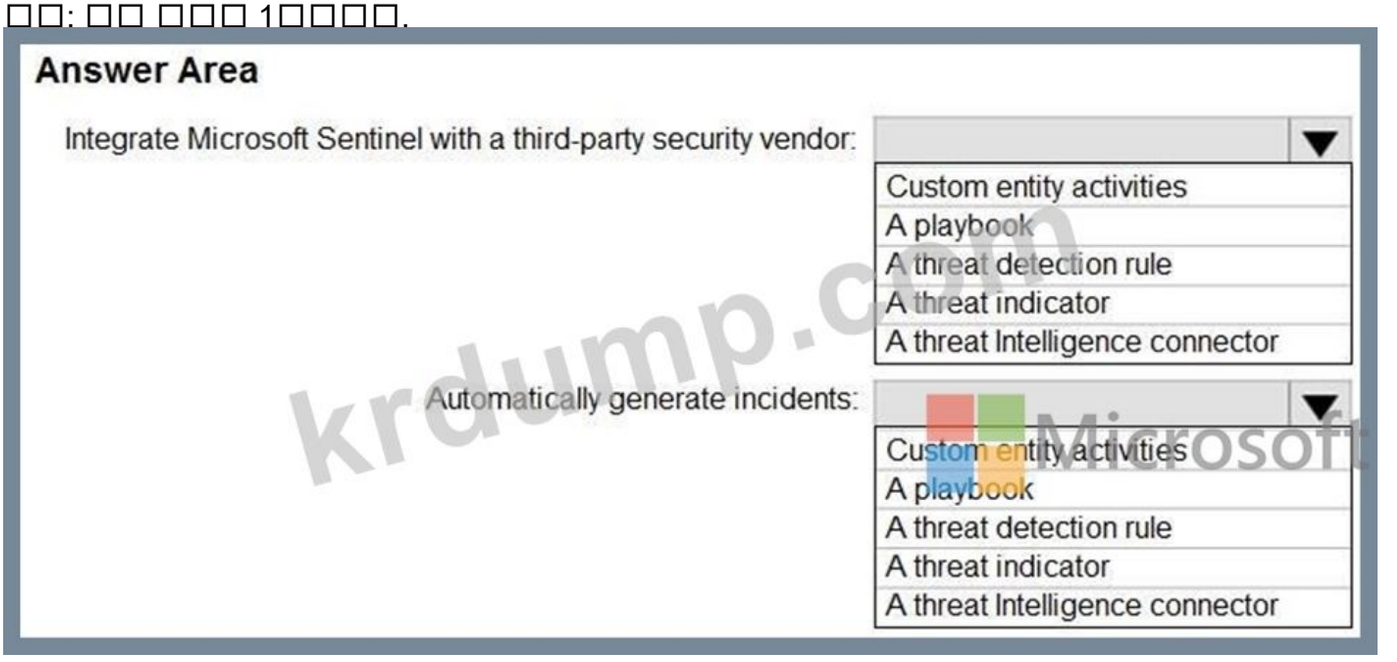
□□□ □□□□ □□ □□□ □□□□□.

- □□□ IP □□□ □□ □ □□□□ □□□□□ □□□□□.

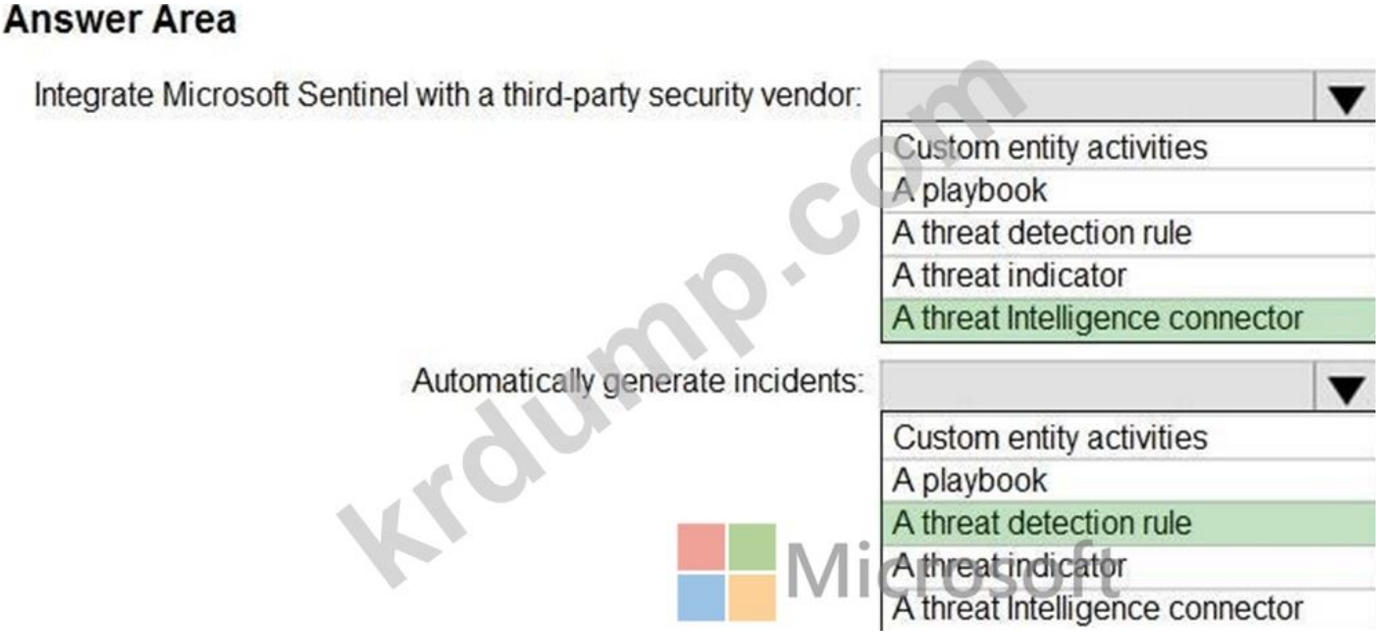
□□□□□ and-control □□□ □□□□□□□.

□ □□ □□□ □□□□□ Microsoft Sentinel□□ □□□ □□□□ □□□? □□ □□□□ □□ □ □□□ □□□□ □□□□□.

□□: □□ □□□ 1□□□□.



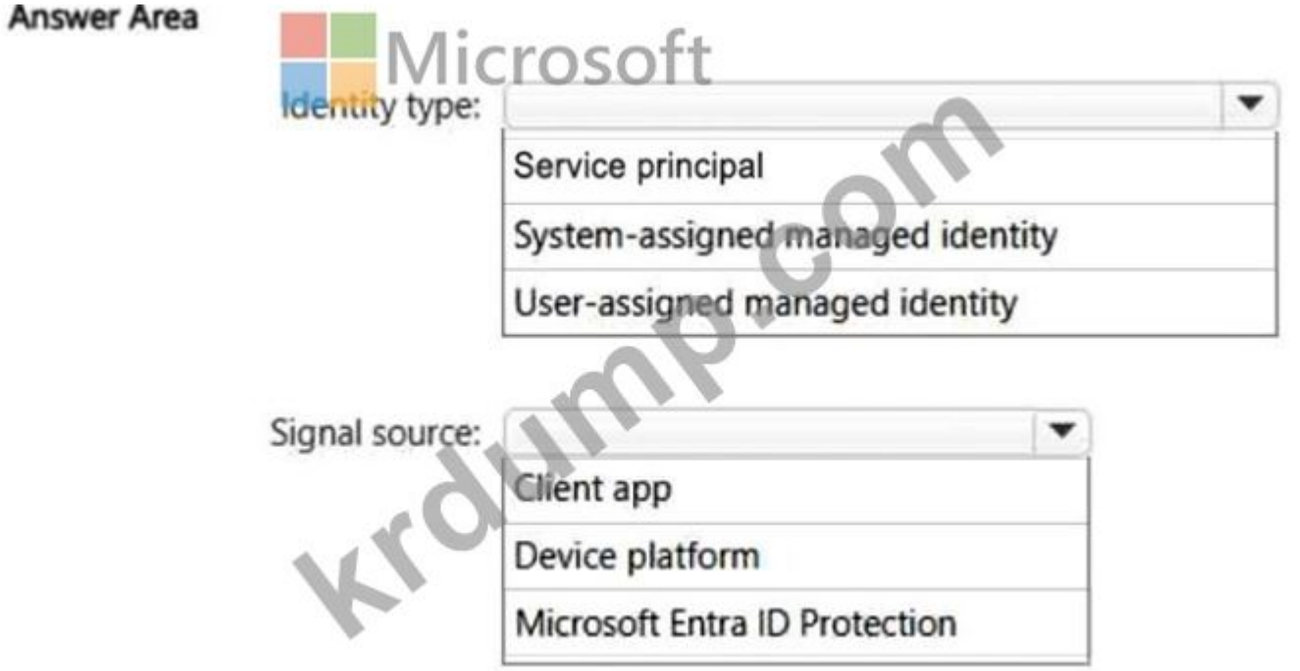
Answer:



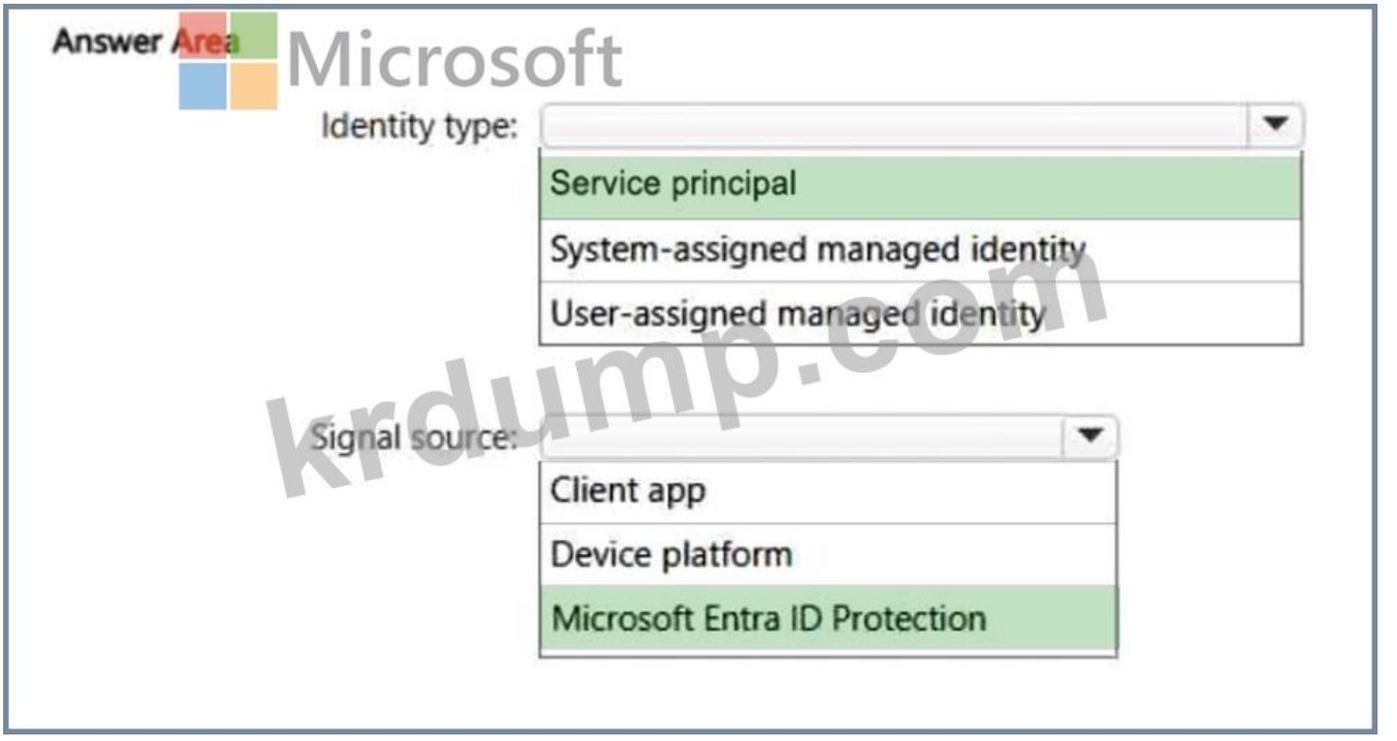
Explanation:
1. Threat Intelligence connector - Allow you to integrate Microsoft Sentinel with third-party security vendors to access information about known threats, such as malware and command- and-control servers.
2. Threat detection rule- Allow you to define conditions that, when met, will automatically generate an incident in Microsoft Sentinel.
https://learn.microsoft.com/en-us/azure/sentinel/partner-integrations
https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts

NEW QUESTION: 67
Azure □□□ □□□□. □ □□□□ Windows Server 2022□ □□□□ Microsoft Defender for Servers Plan 1□ □□□□ 200□□ □□ □□□ □□□□ □□□□. Amazon Web Services(AWS) □□□ □□□□.
AWS □□□ Windows Server 2022□ □□□□ 100□□ □□ □□□ □□□ □□□□□.
AWS □□□ □□ □□□ □□ □□□□□ □□□□ □□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□.
- □□ □□□□ □□□□□ □□□ □□□□ □□□ □□□□□.
- □ □□ □□□ □□□□ □□□□ □□ □□□□□□.
□□□ □□□□ □□□?
A. □□ □□ □□□□
B. Azure Connected Machine □□□□
C. Endpoint□ Microsoft Defender □□□□
D. Azure Monitor □□□□
Answer: B (LEAVE A REPLY)
The Azure Connected Machine agent can be used to manage Windows Server 2022 virtual machines hosted on Amazon Web Services (AWS). This allows you to extend Azure management capabilities to your non-Azure VMs, including those running on AWS.
Reference:
https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview

NEW QUESTION: 68
□□□ □□
Microsoft Entra □□□□ Azure □□□ □□□□.
□□ □□ □□□ □□□ □□□ □□□□ □□□□ ID□ □□□ □□□□ □□□□ □□ □□□ □ □□□□.
□□ □□□ □□□ □□□ □□□□ □□, □□ □□ □□□ □□□ □□□ □□□ □ □□□□?
□□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Service principal

For controlling access of workload identities to resources with a risk-based Conditional Access policy in Microsoft Entra, the service principal identity type is the most suitable.

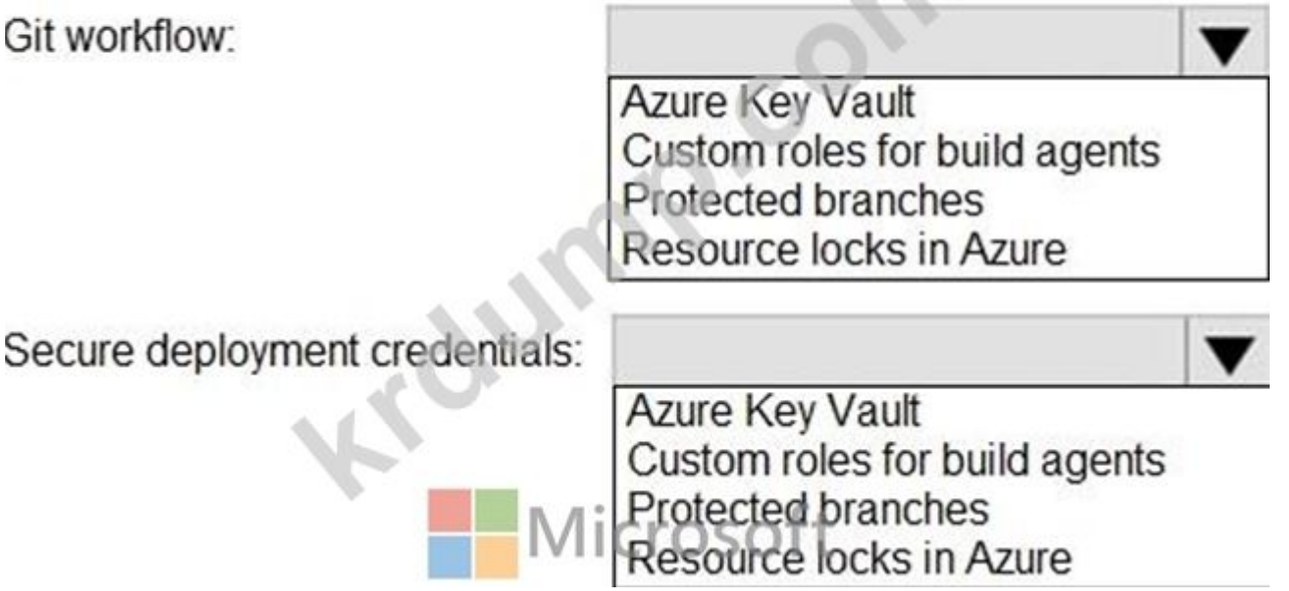
Box 2: Microsoft Entra ID Protection

For risk-based Conditional Access policies in Microsoft Entra ID that control access for workload identities, the best signal source is Microsoft Entra ID Protection, specifically the service principal risk signals. This allows you to identify and respond to potentially risky service principals based on their behavior and activities.

Reference:
https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-risk-policies

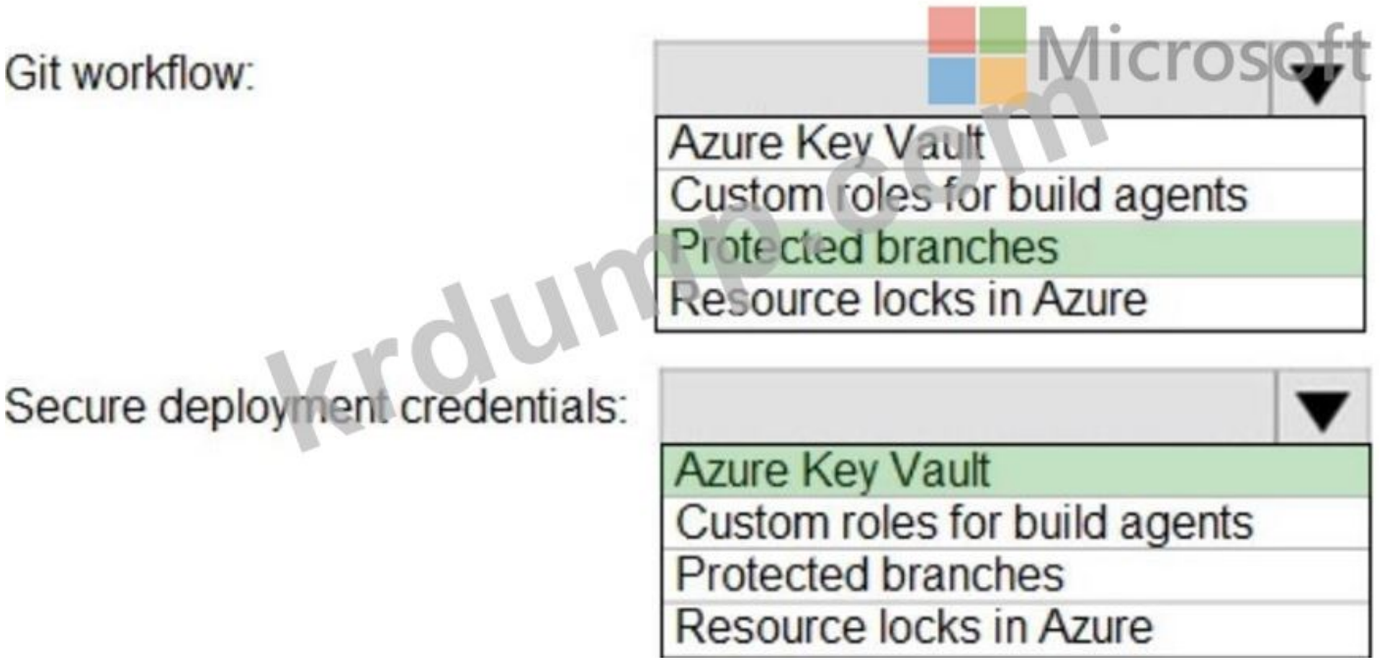
NEW QUESTION: 69
□□□ □□
Azure Policy□ Azure Repos□ □□ □□□□ CI/CD(□□□□ □□ □ □□□□ □□) □□□□□ □□□ □ □□□□.
Azure□ Microsoft □□□□ □□ □□□□□□ □□□□ CI/CD □□□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□.
□ □□□ □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□ □□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops

NEW QUESTION: 70
□□□ □ □□ □□
□□□□ □□□ □□□□ □□□□□ Azure AD □□□□ □□□□.
□□□ □□ □□ □□□ □□□□ □□□□.
□□□ □□ □□□ □□□□□ ID□ □□□ □□ □□□□ □□ □□□ □□□□□ □□□.
□□□□ □□□ □□□□ □□□? □□ □□□ □□□ □□□ □□ □□□ □□ □□□□□ □□ □□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.

Answer:

NEW QUESTION: 71

□+□□□□ Windows 11 □□□ Global Secure Access □□□□□□ □□□□ □□□□.
Microsoft SharePoint Online □ Exchange Online□ □□□□ Microsoft 365 □□□ □□□□.
□+□□□□ □□□□□□□ Microsoft 365□ Microsoft Entra Internet Access□ □□□□□. □□□
□ Microsoft 365 □□□□ □□□□□ □□□ □□□ □□□□□.

* Microsoft 365 □□□□ □□ □□ □□□ □□

* □□□□ □□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□□□ □□ □□ □□□ □□□ □□□ □□

* □□ □□□ □□ □□

* □+□□□□ □□□□□ □□□ □□ □□□□□ □□ □□ □□□□ □□□ □□□ □□□□ □ □□□ Microsoft 365 □□□□ □□□□□?

A. SharePoint Online □□

B. Exchange Online □□

C. SharePoint Online□ Exchange Online □□

Answer: (SHOW ANSWER)

Compliant network enforcement reduces the risk of token theft/replay attacks. Compliant network enforcement happens at the authentication plane (generally available) and at the data plane (preview). Authentication plane enforcement is performed by Microsoft Entra ID at the time of user authentication. If an adversary has stolen a session token and attempts to replay it from a device that is not connected to your organization's compliant network (for example, requesting an access token with a stolen refresh token), Entra ID will immediately deny the request and further access will be blocked. Data plane enforcement works with services that support Continuous Access Evaluation (CAE) - currently, *only SharePoint Online*. With apps that support CAE, stolen access tokens that are replayed outside your tenant's compliant network will be rejected by the application in near-real time. Without CAE, a stolen access token will last up to its full lifetime (default 60-90 minutes).

Reference:

https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-compliant-network

NEW QUESTION: 72

□□ □□ 1 - Fabrikam, Inc

□□

Fabrikam, Inc.□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□□□.

□□ □□

□□□□□ □□

□□□□□ □□□□□□□ corp.fabrikam.com□□□ □□ Active Directory □□□ □□□(AD DS) □□□□ □□□□ □□□□.

Azure □□

Fabrikam□ □□□ □□ Azure □□□□ □□□□ □□□□.

- corp.fabrikam.com□ □□□□□ fabrikam.onmicrosoft.com□□□ Microsoft Entra □□□
- Sub1□□□ □□ Azure □□
- □□ □□ Azure □□□ Vnet1□□□ □□ □□□□
- □□□ Azure □□□ Vnet2□□ □□ □□□□
- Azure WAF(□ □□□□□□ □□□)□ □□□□ FD1□□□ Azure Front Door □□□□
- Microsoft Sentinel □□ □□
- ClaimDetails□□ □□□□ □□□ ClaimsDB□□ Azure SQL □□□□□□
- □□□□□□ □□□ □□□□ Microsoft Defender for Cloud□ □□□□□ □□ 20□□ □□ □□
- □□□ □□□□□ □□□□ TestRG□□ □□□ □□
- □□□ □□□ □□ □□□□ □□□□ Azure Virtual Desktop □□□ □
- Sub1□ □□ □□□□ □□ □□ □□ □□ □□ □□□ □□□□.

□□□

Fabrikam□ Contoso, Ltd.□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□□. Contoso □ □□□ □□ □□□□ □□□□ □□□□.

- contoso.onmicrosoft.com□□□ Microsoft Entra
- ContosoAWS1□□□ Amazon Web Services(AWS) □□□□ Fabrikam □□□□□□□ □□□ □□□□□ □□□□□ □ □□□□ AWS EC2 □□□□□ □□□□ □□□□. Contoso□ □□□ □ Fabrikam□ □□□□ □□□□ □□□□□□□ □□□□□□ □□□□□□□.

□□□□ fabrikam.onmicrosoft.com□ Contoso Developers□□ □□ □□□ □□□□, □ □□□ Sub1□ □□□ □□□□□. ContosoDevelopers □□□□ ClaimsDB □□□□□□□ db.owner □ □□ □□□□□.

□□ □□ □□□

Fabrikam□ □□□ □□ □□ □□ □□□ □□□□□.

- Defender for Cloud□ Sub1□ □□ □□□□ HIPAA HITRUST □□□ □□□□□ □□□□□ □ □□□ □□□□.
- □□ HIPAA HITRUST □□□ □□□□ □□ □□□□ □□□□ □□□□ □□□□.
- Qualys□ □□□ □□ □□□ □□ □□□ □□□□□.

□□ □□

Defender for Cloud□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□□. □□ □□ □□□ □□ □□□□ □□□ □□□. □□ □□ □□□ Defender for Cloud□ □□□□ □□ □.

ClaimApp □□

Fabrikam□ □□ □□□ □□ ClaimsApp□□□ □□□ □□ □□ □□□□□□□ □□□ □□□ □□.

- ClaimsApp□ Vnet1 □ Vnet2□ □□□□ Azure App Service □□□□□ □□□□□.
- □□□□ https://claims.fabrikam.com□ URL□ □□□□ ClaimsApp□ □□□□□.
- ClaimsApp□ ClaimsDB□ □□□□ □□□□□.
- ClaimsDB□ Azure □□ □□□□□□□ □□□□ □ □□□ □□□.
- ClaimsApp□ □□ □ □□□ □□□ ClaimsDB□ □□□□□ □□□.

□□□□□□ □□ □□ □□

Fabrikam□ □□□□□□ □□□ □□ □□□ □□ □□ □□□ □□□□□□.

- Azure DevTest □□ □□□□ □□□□ □□ □□□□□.
- □□ □□□□□□ □□□ GitHub Enterprise□ □□□□□ □□□.
- Azure Pipelines□ □□□□□□ □□□ □□□□ □ □□□□□.
- □□ □□□□□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□□. □□□□ □□□ □ □□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□. □□□ □□□ □□□□ □ □□ □ □□□□ □□□.

□□ □□ □□

Fabrikam□ □□□ □□ □□ □□ □□□ □□□□□.

- □□□ □□□ □□□ □□□□□□□ □□□□ □□□ □□□ □□□□ □□□.
- InfraSec□□□ □□□ □□□ □□□□ □□ □□(NSG)□ Azure Firewall, VJM, Sub1□ Front Door □□□□□ □□□ □ □□□ □□□.
- □□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□. □□ □□□□ □□□ □□ □□ □□ □□□□□ □□□□□□□□ □□□.

AWS □□ □□

Fabrikam□ ContosoAWSV□ □□□□ □□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.

- AWS EC2 □□□□□ □□ □□ □□ □□□ □□□□ □□ □□ Fabrikam□ □□ □□□□□ □□□□.
- □□ □□□□ Azure □□□□ □□ AWS □□□ □□□ □□□ □ □□□ □□□□□.

Contoso □□□ □□ □□

Fabrikam□ Contoso □□□□ □□ □□□ □□ □□ □□□ □□□□□□.

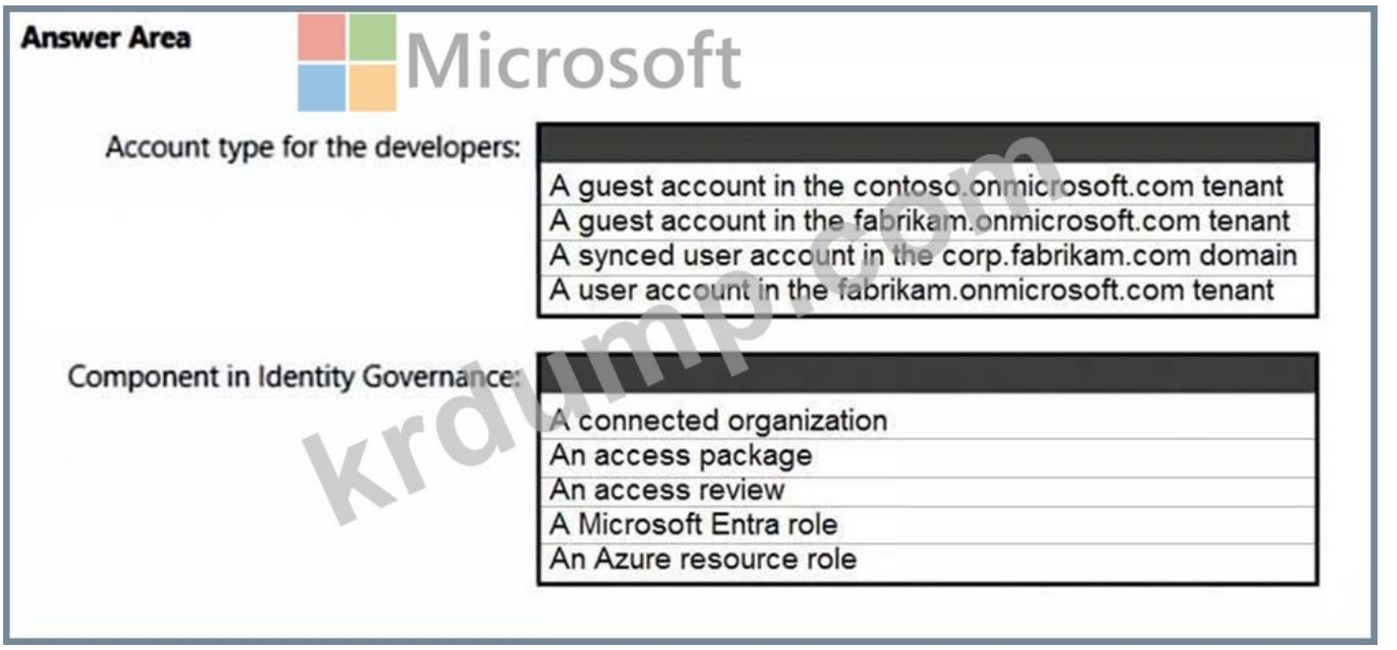
- □□ ContosoDevelopers □□□ □□□□ □□□□ □□□.
- Contoso □□□□ Sub1□ □□□□ □□□□□□ □□ contoso.onmicrosoft.com □□ □□□ □□□□ □□□.
- □□□ □□□□ ClaimDetails □□□□ MedicalHistory□□ □□ □□ □□□□ □ □ □□□ □ □□.

□□ □□ □□

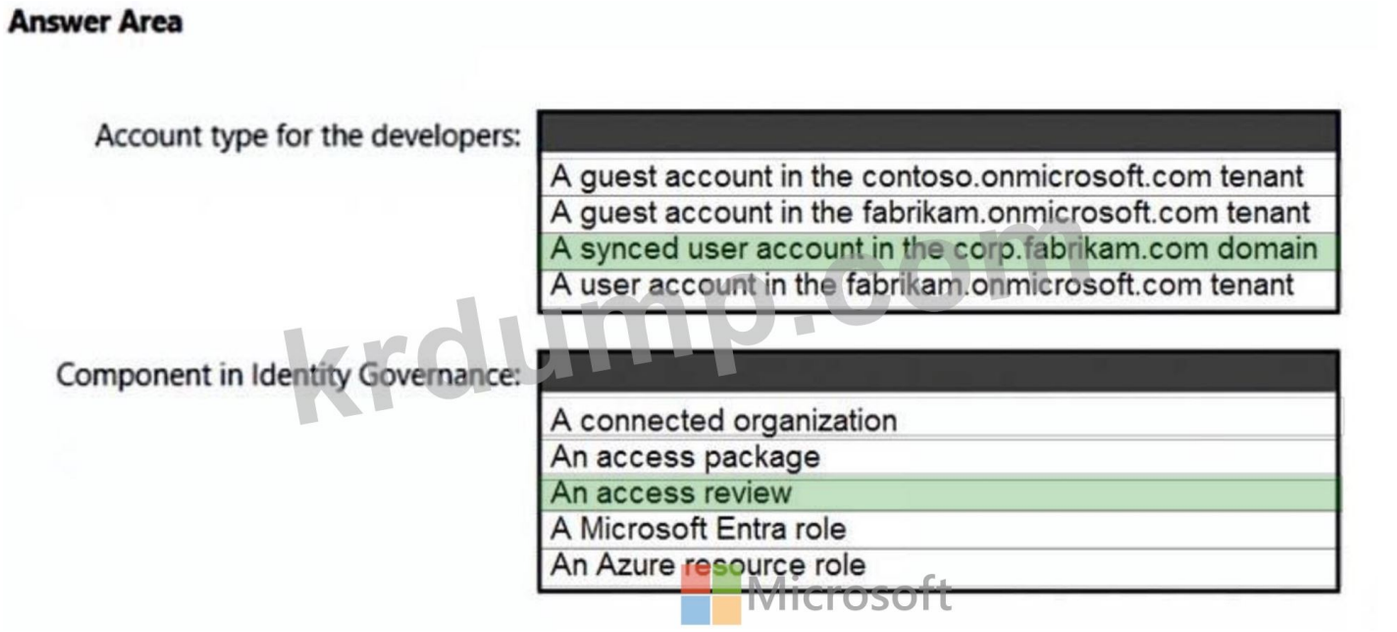
Fabrikam□ Sub1□ □□ □□□ HIPPA HITRUST □□□ □□□□□ □□□□ □□□□□ □□ □. TestRG□ □□ □□□ □□ □□ □□□□ □□□□ □□□.

□□□ □□

Contoso □□□ □□ □□□ □□□□□ Microsoft Entra ID□□ □□□ □□□□ □□□?



Answer:



Explanation:

Box 1: A guest account in the fabrikham.onmicrosoft.com tenant

The Contoso devlopers must use their existing contoso.onmicrosoft.com credentials.

Box 2: An access review

Scenario: Every month, the membership of the ContosoDevelopers group must be verified.

Microsoft Entra ID access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Access review is part of Microsoft Entra ID governance.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

NEW QUESTION: 73

□□□ □ □□ □□

Microsoft 365 □□□ □□□□.

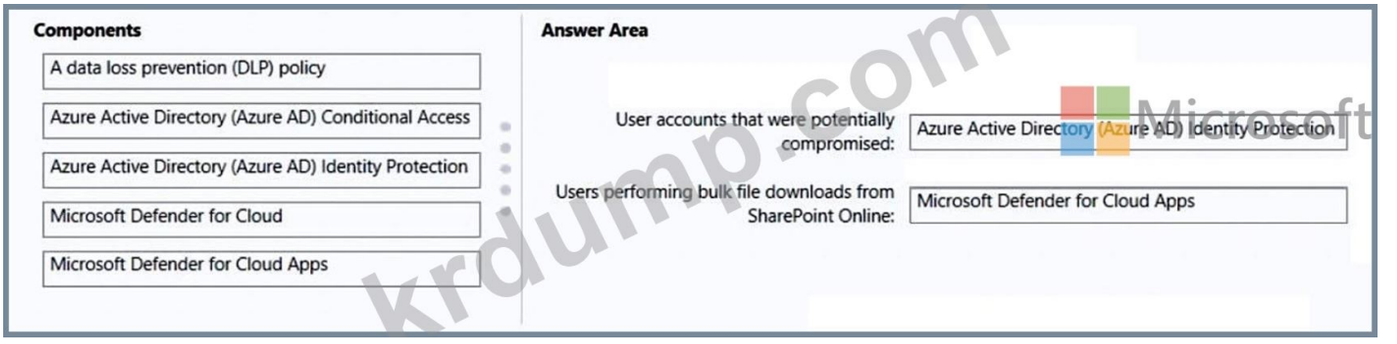
□□ □□□ □□□□□□ □□ □□ □□□□ □□□□ □□□.

- □□□□□ □□□□□ □ □□ □□□ □□

- Microsoft SharePoint Online□□ □□ □□ □□□□□ □□□□ □□□ □ □□□ □□ □□ □ □□□ □□□ □□□□ □□□? □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□. □ □ □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□ □□□ □□□□□ □ □□ □□□□.

□□: □□ □□□ 1□□□□.

Answer:



Explanation:

Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

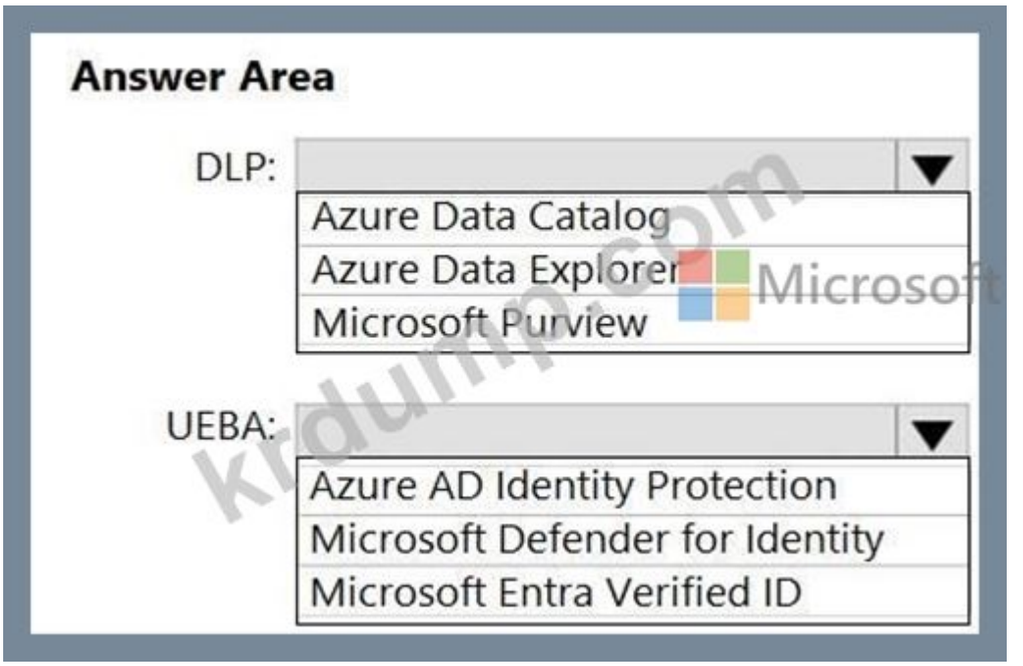
Premium sign-in risk detections include:

* Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.

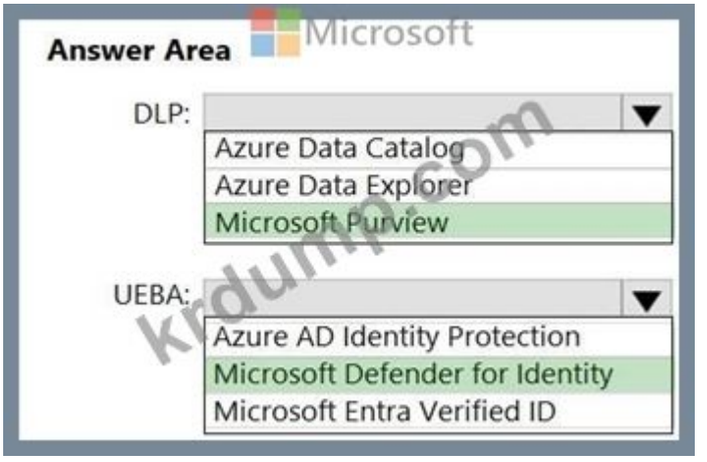
* Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This detection may indicate that the user's account is compromised, that messages are being intentionally hidden, and that

the mailbox is being used to distribute spam or malware in your organization.
* Etc.
Incorrect:
Not: Microsoft 365 Defender for Cloud
Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365 Defender portal from Incidents & alerts > incident > Users.
Box 2: Microsoft 365 Defender for App
Defender for Cloud apps detect mass download (data exfiltration) policy Detect when a certain user accesses or downloads a massive number of files in a short period of time.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

NEW QUESTION: 74
□□□ □□
□□□□ □□ □□□ □□ □□ □□□□□ □□□□ □□□□.
Microsoft Cybersecurity Reference Architectures(MCRA)□ □□□□ Microsoft 365 Defender□ □□ Microsoft □□□□ □□□ □□ □□ □□□ □□□□ □□□□.
Microsoft 365 Defender□ □□ □□□□ □□ □□ □□□ □□□□ Microsoft □□□□ □□□□ □□□□ □□□.
- □□ □□□ □□□ □□ □□(DLP) □□□ □□□□□.
Microsoft 365 Defender □□□□ □□.
- □□□ □ □□□ □□ □□ □□ □□ □ □□
□□ □□ □□□ □□ □□ □□(UEBA)
□ □□ □□□ □□ □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

1. Purview - For the requirement to enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal, you should include Microsoft Purview in your recommendation. https://learn.microsoft.com/en-us/microsoft-365/security/defender/dlp-investigate-alerts-defender?view=o365-worldwide

2. MS Defender for Identity. Microsoft Defender for Cloud Apps provides user entity behavioral analytics (UEBA) in the cloud. This can be extended to your on-premises environment by integrating with Microsoft Defender for Identity. After you integrate with Defender for Identity, you'll also gain context around user identity from its native integration with Active Directory. https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-ueba

NEW QUESTION: 75

Microsoft Sentinel □□ □□□ □□□ Azure □□□ □□□□.

□□□□□ □□□□□□ CEF(Common Event Format) □□□ □□□ □□ □□□ □□□□ □□ □□ □□□□. □ □□□□□ Microsoft Sentinel □□□□ □□ □□□□ □□□□.

□□□□□ Microsoft Sentinel□ □□□□ □□□□ □□□□ □□□□ □□□.

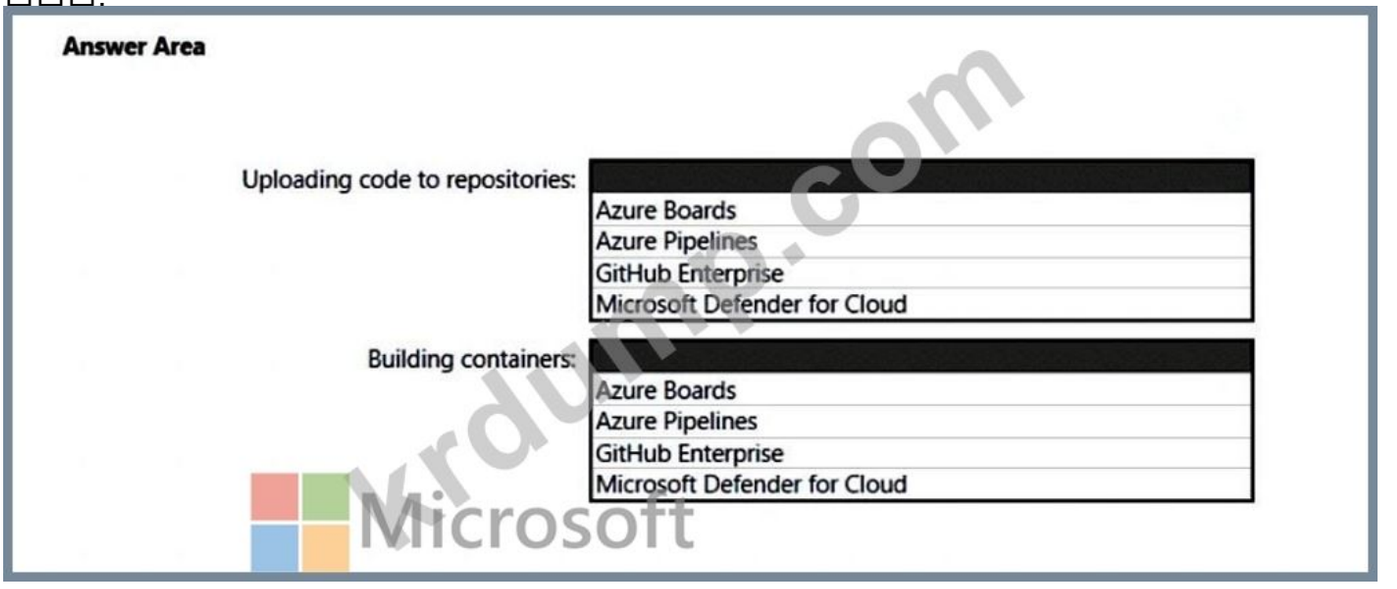
□□□□□ □□□ □□□□ □□□?

A. Azure □□ □
B. □□□□□ Syslog □□
C. □□□□□ □□□ □□□□□
D. Azure □□□ □□□
Answer: B (LEAVE A REPLY)
Many networking and security devices and appliances send their system logs over the Syslog protocol in a specialized format known as Common Event Format (CEF). This format includes more information than the standard Syslog format, and it presents the information in a parsed key-value arrangement. The Log Analytics Agent accepts CEF logs and formats them especially for use with Microsoft Sentinel, before forwarding them on to your Microsoft Sentinel workspace.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/connect-common-event-format

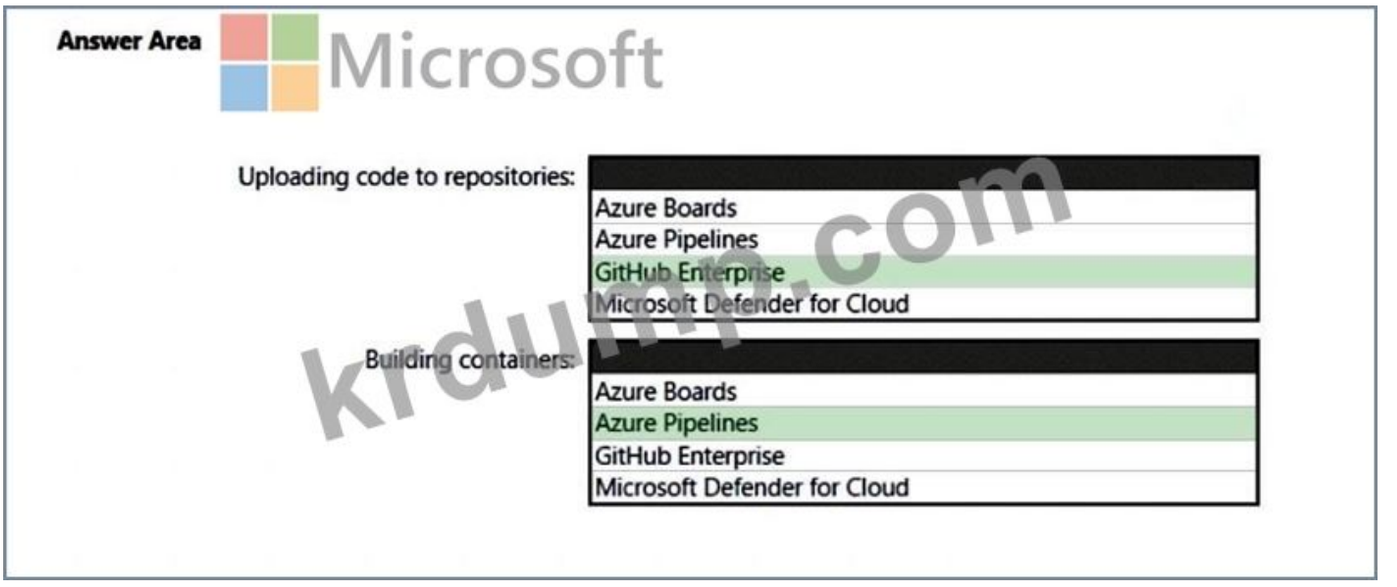
NEW QUESTION: 76
Azure □□□ □□□□.
Microsoft Cloud Adoption Framework for Azure□ □□□□ □□□□□□□ □□ □□ □□□ □ □□□□. □□□□ □□ □□ □□□□ □□ □□ □□□ □□ □□ □□ □□ Azure □□□□□ □□ □□□□□ □ □□ □□□□□□ □□ □□ □□□□□.
□ □□ □□ □□ □□□□ □□□□ □□□□ □□□. □□□□ □□□□□□□ □□ □□ □□ □□□□ □□ □□□□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Azure □□□
B. Azure □□ □□□□ □□□□□
C. Azure □□ DNS □□
D. Azure □ □□□
Answer: C (LEAVE A REPLY)
Landing zones and Azure regions
Azure landing zones consist of a set of resources and configuration. Some of these items, like management groups, policies, and role assignments, are stored at either a tenant or management group level within the Azure landing zone architecture. These resources aren't deployed to a particular region and instead are deployed globally. However, you still need to specify a deployment region because Azure tracks some of the resource metadata in a regional metadata store.
If you deploy a networking topology, you also need to select an Azure region to deploy the networking resources to. This region can be different from the region that you use for the resources listed in the preceding list. Depending on the topology you select, the networking resources that you deploy might include:
Azure Virtual WAN, including a Virtual WAN hub
Azure virtual networks
VPN gateway
Azure ExpressRoute gateway

Azure Firewall
Azure DDoS Protection plans
*-> Azure private DNS zones, including zones for Azure Private Link
Resource groups, to contain the preceding resources
Reference:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/regions

NEW QUESTION: 77
□□□ □□
□□□ □□□□ □□□□□□ □□□ □□□□ □ □□□□ Azure App Service □□□ □□□□.
App Service □□□ □ □□ □□□□ □□ □□□ DevOps □□□ □□□□ □□□□.
□□□ □□□□□ □□ □□□□□□□ □□ □□□ □□□ □□□□ □□□ □□□□ □□□.
□□□ □□ □ □□□□ □□□□□ □□□.
- □□□□ □□ □□□
- □□□□ □□.
□ □□□ □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□.



Answer:



Explanation:

Box 1: GitHub Enterprise

A GitHub Advanced Security license provides the following additional features:

Code scanning - Search for potential security vulnerabilities and coding errors in your code.

Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also detects secrets when they are pushed to your repository.

Etc.

Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub Enterprise Cloud.

Box 2: Azure Pipelines

Building Containers with Azure DevOps using DevTest Pattern with Azure Pipelines The pattern enabled as to build container for development, testing and releasing the container for further reuse (production ready).

Azure Pipelines integrates metadata tracing into your container images, including commit hashes and issue numbers from Azure Boards, so that you can inspect your applications with confidence.

Incorrect:

* Not Azure Boards: Azure Boards provides software development teams with the interactive and customizable tools they need to manage their software projects.

It provides a rich set of capabilities including native support for Agile, Scrum, and Kanban processes, calendar views, configurable dashboards, and integrated reporting.

* Not Microsoft Defender for Cloud

Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.

You cannot use Microsoft Defender for Cloud to scan code, it scans images.

Reference:

https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-

github-advanced-security
https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-container-dev-test-release/

NEW QUESTION: 78
Microsoft 365 □□□ □□□□.
Azure □□□ □□□□.
Microsoft Teams □ Yammer□ □□ Microsoft Purview □□□□□□ □□ □□ □□□□ □□□ □ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □□□ □□□□ Microsoft 365 □□□ □□ □□ □□ □□
Microsoft Exchange Online □□.
- □□ □□ □□□ □□ □□□□□□.
- □□□ □□□ □□□□□□.
□□□□ □□□ □□□□ □□□?
A. Microsoft Purview □□ □□
B. Microsoft 365 Defender □□□ □□
C. □□□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
When you create a communication compliance policy or a policy for retention, you can create or add an adaptive scope for your policy. A single policy can have one or many adaptive scopes. An adaptive scope uses a query that you specify, so you can define the membership of users or groups included in that query. These dynamic queries run daily against the attributes or properties that you specify for the selected scope. You can use one or more adaptive scopes with a single policy.
Reference:
https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

NEW QUESTION: 79
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□. Amazon Web Services(AWS) □□□ □□□□.
Azure □□ □□□ AWS □□□□ □□□ □□□□□. □□□□ Azure Arc□ □□□□ □□□□. AWS □□□□ □□ □□□ □□□□ □□ □□ □ □□ □□□□ □□□ □ □□□□? □ □□□ □□□ □□□□ □□□□□. □□: □ □□□ 1□□□□.
A. Azure Active Directory(Azure AD) □□ □□ ID □□(PIM)
B. Azure Active Directory(Azure AD) □□□ □□□
C. □□□ Microsoft Defender
D. Azure □□
E. □□□□□ Microsoft Defender
Answer: (SHOW ANSWER)
PIM is supported: https://docs.microsoft.com/en-us/azure/architecture/reference-

architectures/aws/aws-azure-ad-security#advanced-azure-ad-identity-management-with-aws-accounts To enable the Defender for Servers plan Azure Arc for servers installed on your EC2 instances (https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env- settings) Azure Policy not supported. But the CSPM part of Defender for Cloud is. So you could deploy CIS Benchmark for AWS.

NEW QUESTION: 80

1,000□□ □□□□ Group1□□□ □□□ □□□ Microsoft 365 □□□ □□□□. □□ □□□□ Windows 11 □□□ □□□□ □□□□. □□□□ Microsoft Entra □□□ □□□□ □□□ □□□ □□□. □□□□□□ □□□ □□ □□ □□□ □□□□.

□□ 1□ □□□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□. □□ □□ □□□ □□ □□ □□□□ □□ □□□□□□ □□□□□.

□□ 1 □□□□ □□□ □□□ □□ □□ □□□ □□□ □□ □□□ □ □□□ □□ □□□□ □ □□□ □□□. □□ □□□□ □□ □□□□ □ □□ □□□□ □□□□□□ □□□□□ □□ □ □□.

□□□□□ □□□ □□□□ □□□?

A. Windows □□ □□□ □□ □□□(Windows LAPS)

B. Microsoft Entra □□ □□

C. Microsoft Intune □□□□□ □□ □□

D. Microsoft Entra ID□ □□ □□ ID □□(PIM)

Answer: C (LEAVE A REPLY)

With Microsoft Intune Endpoint Privilege Management (EPM) your organization's users can run as a standard user (without administrator rights) and complete tasks that require elevated privileges. Tasks that commonly require administrative privileges are application installs (like Microsoft 365 Applications), updating device drivers, and running certain Windows diagnostics. Endpoint Privilege Management supports your Zero Trust journey by helping your organization achieve a broad user base running with least privilege, while allowing users to still run tasks allowed by your organization to remain productive. For more information, see Zero Trust with Microsoft Intune.

Reference:

https://learn.microsoft.com/en-us/mem/intune/protect/epm-overview

NEW QUESTION: 81

□□□ □□□□ Microsoft 365 E5 □□□ □□□□.

□□□□ Microsoft Teams, Exchange Online, SharePoint Online, OneDrive□ □□□□ □□□□ □□□□□. □□□ □□□ □□□ □□□□□□□□ □□□ □□ □□(PHI)□ □□□□□. PHI□ □□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□□?

A. □□□ □□ □□ □□

B. □□□ □□ □□(DLP) □□

C. □□□ □□□ □□

D. □□ □□

Answer: B (LEAVE A REPLY)

Sensitivity labels classify PHI. DLP uses those labels to prevent it from leaving the protected environment.
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp- policy?view=o365-worldwide

NEW QUESTION: 82
□□ □□ 2 - Litware, inc.
□□
Litware, Inc.□ □□□ □□□□□□□ □□□ □ □□ □□□ □□□□□. Litware□ □□ □□□ 30□□ □□□ □□ □□ □□□ □□ □□□□. □□ □□ □□□ VPN□ □□□□ □□□ □□□ □□.
Litware□ □□ 2□□ □□□□□ □□ □□ □□□□□□. □□ □□□□ □□□□ □□□ □ □ □ □□□ □□□□□.
□□ □□
Litware□□ litware.com□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□□ 20 □□ Azure □□□ □□□ Microsoft Entra □□□□ □□□□. Microsoft Entra Connect□ □□ □ □□ □□□□ □ □□□□□. □□ □□ □□□□ □□□□□□ □□ □□ □□□ □□□□□□.
□□ Litware □□□□ Microsoft 365 E5 □□□□□ □□□□□.
□ □□□□ Litware□ □□□□ □□□ □□ AD DS □□□□, Microsoft Entra □□□ □ □□ □ □ Azure □□□ □□□□□.
□□ □□. □□□ □□ □□
Litware□ □□□ □□ □□ □□□ □□□ □□□□□.
- □ Microsoft Entra □□□□ □□ □□ □□ □□ □□□ □□□□.
- Litware□ □□ Azure □□□ □□□□□□ □□ □□ Azure □□□□□ □□□□ □□ □□ □ □□□ □□□□□.
- VPN□ □□□□ □□ □□□□□ □□ □□□□□□□ □□ □□ □□□□ □□□□ □□ Microsoft Entra Application Proxy□ □□□□□.
□□ □□. □□□□ □□ □□
Litware□ □□□ □□ □□□□ □□ □□□ □□□□□.
- □□□□ □□□□□ □□□□ □□□□□□.
- □□□ □□□□□ □□□ □□□□□ □□□□□□.
□□ □□. □□□□□ □□ □□
Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.
- □□□ □□□□ Azure□□ □-□□□□ □□□□ □□□ □ □□□□.
o Azure Policy□ □□□□ □□ □ □□ □□□ □□□□□.
o □□ □□ □□ □ □□ □□□□□ □□□□□.
o □□ □□□ □□□□□.
- □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
□□ □□. Microsoft Sentinel □□ □□
Litware□ Microsoft Sentinel□ □□ □□ □ □□□ □□(SIEM)□ □□ □□□□□□□ □□ □□ (SOAR) □□□ □□□ □□□□□. □□ Microsoft Sentinel□ □□□□ □□ □□ □□(SOC)□

□□ □□□□□□ □□□.
□□□□. □□ □□□□
Litware□ □□□ □□ □□ □□ □□□ □□□□□.
- AD DS □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □□ □□ □□□ □□□□□.
- Microsoft Entra □□□ □□□ □□□□ □□ □□□ □□ □□□□ □□ AD DS □□□ □□□ □□□ □□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □ □□□ □□□ □□□ □□□□□. □□□□ □ □□ □□□□□.
o □□ □□, □□□ □ □□□□ □□
o □□□ □□, □□□□ □ □□□□ □□
o □□□□ □□□ □□ □□
□□ □□. □□ □□ □□ □□
Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.
- □□□ □□□□ □□ □ □□□□ □□□ □□, □□ □□ □ □□□□ □□□ □ □□□ □□ □ □□ □□□□□.
- □□ □□ Azure Policy □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
- □□ □□□ □□□ □□□□□.
□□ □□. Azure Landing Zone □□ □□
Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.
- □□ Azure □□□□ Azure Firewall□ □□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □.
- □□ □□□ □□ □□□ □□□ □□□□□.
- □ □□ □□ Azure □□ □□□ □□ □□□□□□ □□ Microsoft □□ □□□□□ □□ □□□ □□ Azure App Service □□□ □□□□□ □□□□□.
- □□□ □□ □□□□ □□□□□□.
- □□□□ □□□□ □□□□□□.
□□ □ □□□□□□ □□□ □ □□□□□ □□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□. □ □□ □□ □□□ □□ □□□ □□□□.
- □□ □□□□ □□□□□.
- litware.com□ DNS □□□□□□□ □□□□□.
□□ □□. □□□□□□ □□ □□ □□
Litware□ □□□ □□ □□□□□□ □□ □□ □□□ □□□□□.
- Microsoft Entra Application Proxy□ □□□□ SSO(Single Sign-On)□ □□□□ □□ □□□□□ □□ □□□□□.
- Microsoft SharePoint Online □ Exchange Online □□□□ □□ □□□□ □□□□□ □□□□ □□ □□□□□.
□□ □□□ □□□ □□ □□□□ □□□□ □□□.
□□□□ □□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□□.
□ □□ □□ □□ □□□ □□□□ □□□?
A. Azure DDoS □□ □□

B. Azure □□ DNS □□

C. □□□□□ Microsoft Defender

D. ExpressRoute □□□□□

Answer: B (LEAVE A REPLY)

A specific virtual network can be linked to only one private zone if automatic registration of VM DNS records is enabled. You can however link multiple virtual networks to a single DNS zone.
https://docs.microsoft.com/en-us/azure/dns/private-dns-overview

NEW QUESTION: 83

□□□ □□

App1□□□ Azure App Service □□□ □□ □□ □□ □□□ □□□ □□□□.

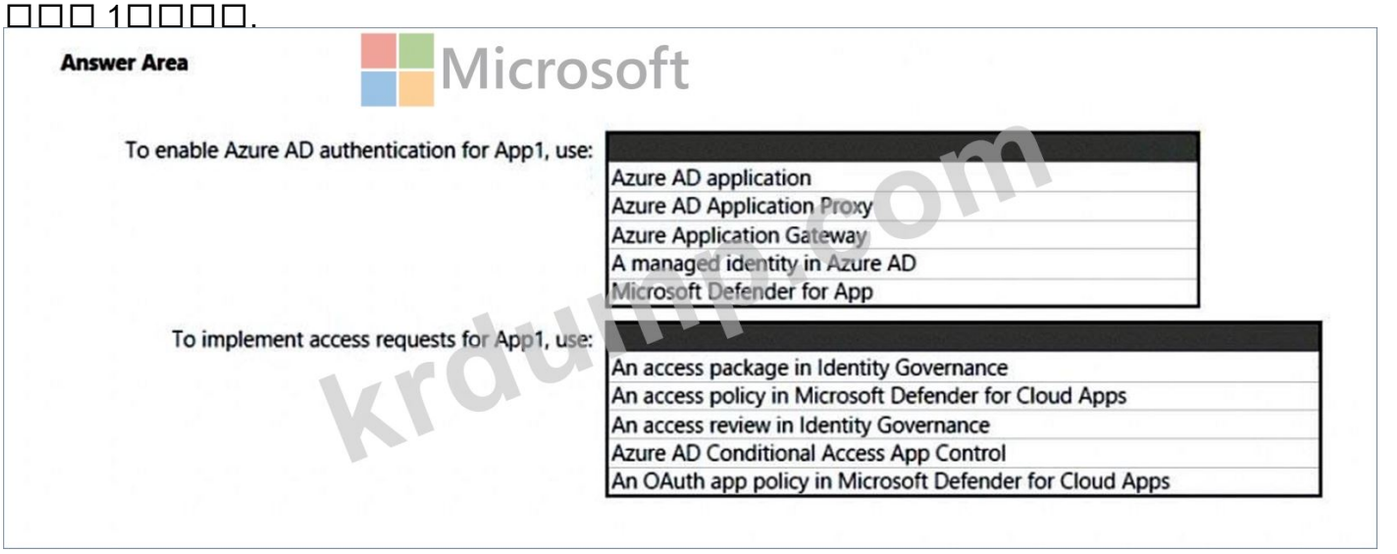
App1□ □□□ □□□ □□□□.

- □□□□ My Apps □□□ □□ App1□ □□ □□ □□□ □□□□□. □□ □□□□ □□□ □ □□□□.
- □□□□ Azure Active Directory(Azure AD)□ □□□□ □□□□□.

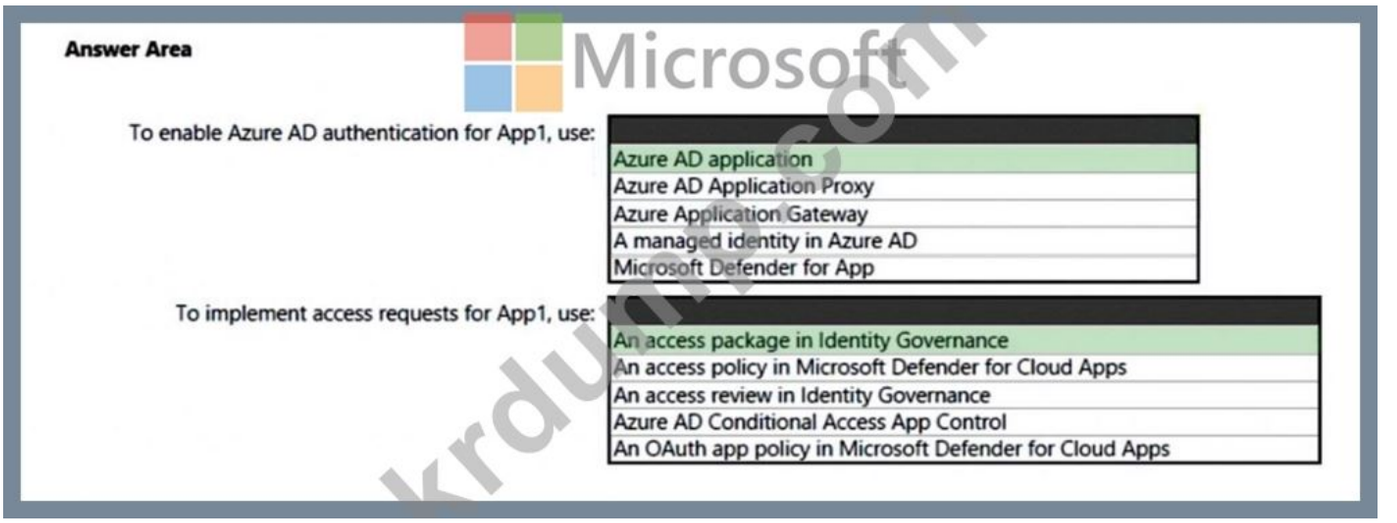
□□□ □□.

App1□ □□ □□□ □□ □□□□□ □□□□ □□□.

□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□□ 1□□□□.



Answer:



Explanation:

Box 1: Azure AD application

You need first to register your app in AAD, then add users or group to this app so they can used it.

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app Box 2: An access package in identity governance Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

NEW QUESTION: 84

□□ □□ 2 - Litware, inc.

□□

Litware, Inc.□ □□□ □□□□□□□ □□□ □ □□ □□□ □□□□□. Litware□ □□ □□□ 30□□ □□□ □□ □□ □□□ □□ □□□□. □□ □□ □□□ VPN□ □□□□ □□□ □□□ □□.

Litware□ □□ 2□□ □□□□□ □□ □□ □□□□□□. □□ □□□□ □□□□ □□□ □ □ □ □□□ □□□□□.

□□ □□

Litware□□ litware.com□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□□ 20 □□ Azure □□□ □□□ Microsoft Entra □□□□ □□□□. Microsoft Entra Connect□ □□ □ □□ □□□□ □ □□□□□. □□ □□ □□□□ □□□□□□ □□ □□ □□□ □□□□□□. □□ Litware □□□□ Microsoft 365 E5 □□□□□ □□□□□.

□ □□□□ Litware□ □□□□ □□□ □□ AD DS □□□□, Microsoft Entra □□□ □ □□ □ □ Azure □□□ □□□□□.

□□ □□. □□□ □□ □□

Litware□ □□□ □□ □□ □□□ □□□ □□□□□.

- □ Microsoft Entra □□□□ □□ □□ □□ □□ □□□ □□□□.
- Litware□ □□ Azure □□□ □□□□□□ □□ □□ Azure □□□□□ □□□□ □□ □□ □ □□□ □□□□□.

- VPN□ □□□□ □□ □□□□□ □□ □□□□□□□ □□ □□ □□□□ □□□□ □□ Microsoft Entra Application Proxy□ □□□□□.

□□ □□. □□□□ □□ □□

Litware□ □□□ □□ □□□□ □□ □□□ □□□□□.

- □□□□ □□□□□ □□□□ □□□□□□.
- □□□ □□□□□ □□□ □□□□□ □□□□□□.

□□ □□. □□□□□ □□ □□

Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.

- □□□ □□□□ Azure□□ □-□□□□ □□□□ □□□ □ □□□□.

o Azure Policy□ □□□□ □□ □ □□ □□□ □□□□□.

o □□ □□ □□ □ □□ □□□□□ □□□□□.

o □□ □□□ □□□□□.

- □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

□□ □□. Microsoft Sentinel □□ □□

Litware□ Microsoft Sentinel□ □□ □□ □ □□□ □□(SIEM)□ □□ □□□□□□□ □□ □□ (SOAR) □□□ □□□ □□□□□. □□ Microsoft Sentinel□ □□□□ □□ □□ □□(SOC)□ □□ □□□□□□ □□□.

□□□□. □□ □□□□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

- AD DS □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □□ □□ □□□ □□□□□.
- Microsoft Entra □□□ □□□ □□□□ □□ □□□ □□ □□□□ □□ AD DS □□□ □□□ □□□ □□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □ □□□ □□□ □□□ □□□□□. □□□□ □ □□ □□□□□.

o □□ □□, □□□ □ □□□□ □□

o □□□ □□, □□□□ □ □□□□ □□

o □□□□ □□□ □□ □□

□□ □□. □□ □□ □□ □□

Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.

- □□□ □□□□ □□ □ □□□□ □□□ □□, □□ □□ □ □□□□ □□□ □ □□□ □□ □ □□ □□□□□.
- □□ □□ Azure Policy □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
- □□ □□□ □□□ □□□□□.

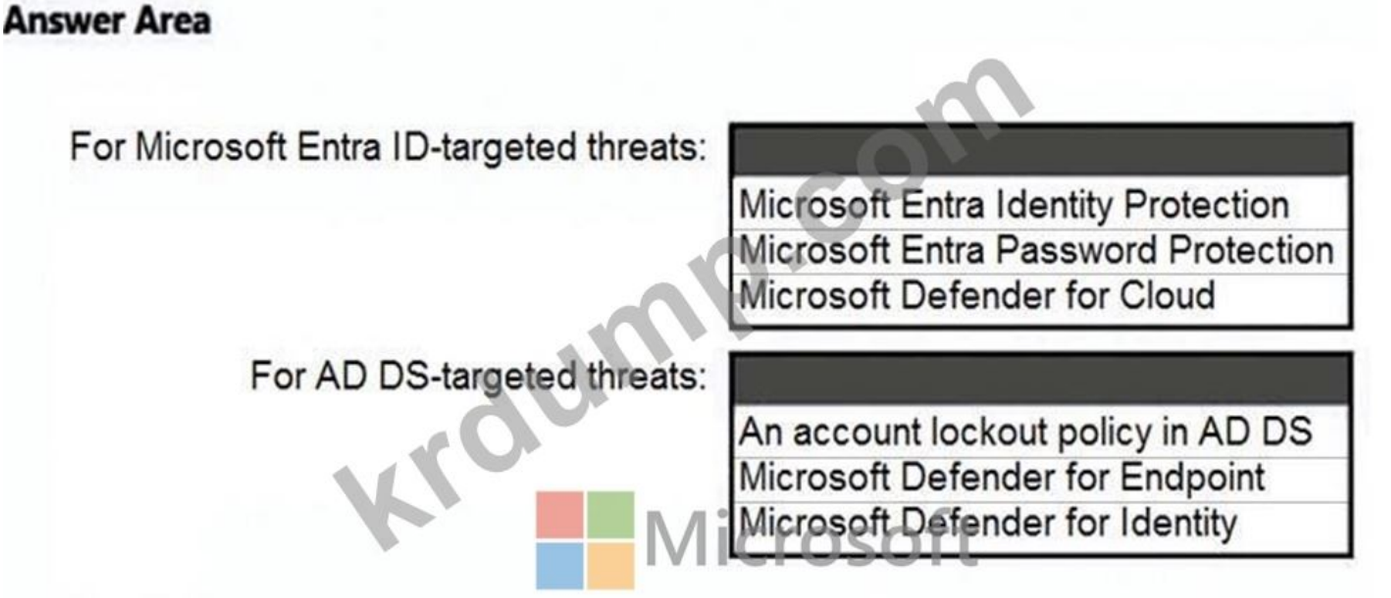
□□ □□. Azure Landing Zone □□ □□

Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.

- □□ Azure □□□□ Azure Firewall□ □□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □.
- □□ □□□ □□ □□□ □□□ □□□□□.
- □ □□ □□ Azure □□ □□□ □□ □□□□□□ □□ Microsoft □□ □□□□□ □□ □□□ □□ Azure App Service □□□ □□□□□ □□□□□.

- □□□ □□ □□□□ □□□□□□.
- □□□□ □□□□ □□□□□□.
□□ □ □□□□□□ □□□ □ □□□□□ □□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□. □ □□ □□ □□□ □□ □□□ □□□□.
- □□ □□□□ □□□□□.
- litware.com□ DNS □□□□□□□ □□□□□.
□□ □□. □□□□□□ □□ □□ □□
Litware□ □□□ □□ □□□□□□ □□ □□ □□□ □□□□□.
- Microsoft Entra Application Proxy□ □□□□ SSO(Single Sign-On)□ □□□□ □□ □□□□□ □□ □□□□□.
- Microsoft SharePoint Online □ Exchange Online □□□□ □□ □□□□ □□□□□ □□□□ □□ □□□□□.
□□□ □□
litware.com □□□□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□. □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□. □ □: □□□ 1□□□□.

Answer Area



Answer:

Answer Area

Explanation:

Box 1: Microsoft defender for cloud

Scenario: Prevent AD DS user accounts from being locked out by brute force attacks that target Microsoft Entra user accounts.

When Microsoft Defender for Cloud detects a Brute-force attack, it triggers an alert to bring you awareness that a brute force attack took place. The automation uses this alert as a trigger to block the traffic of the IP by creating a security rule in the NSG attached to the VM to deny inbound traffic from the IP addresses attached to the alert. In the alerts of this type, you can find the attacking IP address appearing in the 'entities' field of the alert.

Box 2: An account lockout policy in AD DS

Scenario:

Detect brute force attacks that directly target AD DS user accounts.

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign- ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

Verify on-premises account lockout policy

To verify your on-premises AD DS account lockout policy, complete the following steps from a domain-joined system with administrator privileges:

1. Open the Group Policy Management tool.
2. Edit the group policy that includes your organization's account lockout policy, such as, the Default Domain Policy.
3. Browse to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.
4. Verify your Account lockout threshold and Reset account lockout counter after values.

Reference:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/automation-to-block-brute-force-attacked-ip-detected-by/ba-p/1616825

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#verify-on-premises-account-lockout-policy

NEW QUESTION: 85

Azure □□□ □□□□.

□□□□ □□□ □□ □□□ Azure □□□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □ □□□.

□□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□?

A. □□□ □□ Azure □□

B. Microsoft Defender for Cloud□ □□ □□ □□

C. Azure □□ □□

D. Azure □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 86

□□□ □□

contoso.com□□□ Microsoft Entra □□□□ □□□□. contoso.com□ □□□ Azure □□ 30□ □ □□□□. □ □□□□□ □□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Description
Mgmt1	Contains 15 subscriptions
Mgmt2	Contains 15 subscriptions

□□ □□□ □□ □□ Azure Storage □□□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

- □□□ □□ □□ □□ □□□ □□(RBAC)□ □□□□ □□□□ □□ □□□ □□□□□.

□□ □□□ □□□ □□ □□□ □□ □□□.

- □□□ □□□ □□□□□□.

□□ □□□□ □□□ □□□□ □□, □□□ □□ □□ □□ □ □□□□? □□□□□ □□ □□ □□ □□□ □□□ □□□□□.

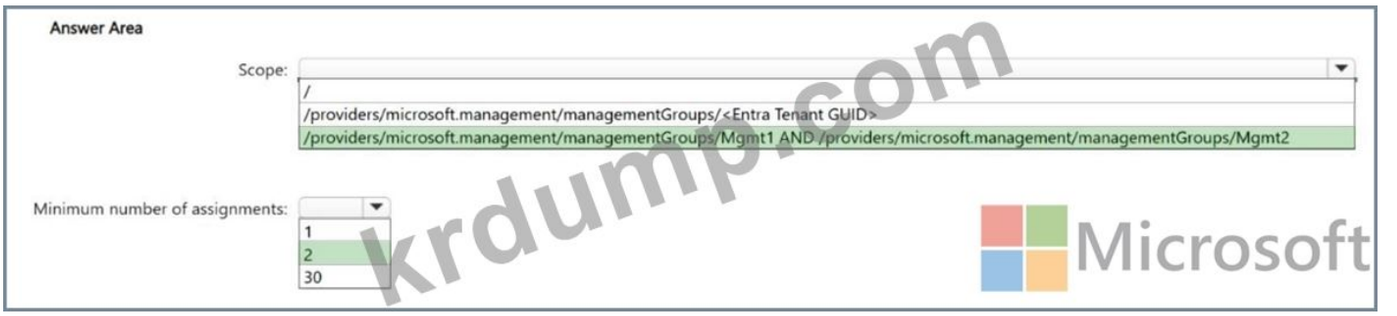
□□: □□ □□□ 1□□□□.

Answer Area

Scope:
- /
- /providers/microsoft.management/managementGroups/<Entra Tenant GUID>
- /providers/microsoft.management/managementGroups/Mgmt1 AND /providers/microsoft.management/managementGroups/Mgmt2

Minimum number of assignments:
- 1
- 2
- 30

Answer:



Explanation:

Box 1: ..Mgmt1 AND .. Mgmt2

For Microsoft Entra's two management groups, the appropriate scope for assigning roles is the management group level itself. This is because management groups are designed to be a broader scope for managing access and policies across multiple subscriptions.

Box 2: 2

Note:

Broadest Scope:

Management groups are the broadest scope in Azure, encompassing multiple subscriptions.

Reference:

https://learn.microsoft.com/en-us/azure/governance/management-groups/overview

NEW QUESTION: 87

□□ □□ 100□, VNet1□□□ □□ □□□□, □□□ □□□ 20□□ □□□ Azure □□□ □□□ □. □□ □□□ Windows Server□ □□□□ VNet1□ □□□□ □□□□. □□□□ □□□□ □ □□□ Linux □□□□□□□□ Azure □□□□ □□□□□□.

□□□□ SSH(Secure Shell)□ □□□□ □□□□□□□□ □□ □□□ □□□ □ □□□ □□ □ □□. □□□□ □□ □□ □□□ □□□□ □□□.

- □□□□ Microsoft Entra□ □□□□ □□□□□□ □□□□□□.

□□□.

- □□□□ □□ □□□□ □□□ □□□□ □□□□ □□□.

SSH□ □□□□.

- □□□□ □□ □□□ □□ □□□□□ □□□□ □□□□□.

□□ □□□ □□ IP □□□ □□□□□.

□□□□ □□□ □□□□ □□□?

A. Azure NAT □□□□□

B. JIT(Just-In-Time) VM □□□

C. Azure □□

D. □□ □(P2S) VPN

Answer: (SHOW ANSWER)

Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.

Azure Bastion supports Kerberos Entra authentication.

Reference:

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

NEW QUESTION: 88

□□□ □□

Azure □□□ Amazon Web Services(AWS) □□□ □□□ □□ □□□□ □□□ □□□□.

□ □□□ □□□□ □□□□□ Azure□□ □□ □□□□ □□□□ □□□.

□□□□ □□ □□ □□□ □□□□ □□□.

- AWS CloudTrail □□□□□ □□□ □□□ □□□□ □□□□□.
- Azure□ □□□□ AWS □□ □□□ □□ □□ □□

□□.

□ □□ □□□ □□ □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Automatically identify threats:

- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Enforce security settings:

- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Answer:

Answer Area

Automatically identify threats:

- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

Enforce security settings:

- Azure Arc
- Azure Log Analytics
- Microsoft Defender for Cloud
- Microsoft Sentinel

NEW QUESTION: 89

□□□□ □□ SaaS(Software as a Service) □□□□ □□□□□.
□□□□ □□□ □□ □□ □□□□ □□□ □□□ □□□. □□ □□□□ Microsoft □□ □□ □ □□ □□□□ □□□.
□□□ □□ □□ □□ □□□?
A. □□ ID □□□ □□□□□.
B. □□□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
https://learn.microsoft.com/en-us/training/modules/design-resiliency-strategy-common-cyberthreats-like-ransomware/3-ransomware-protection Microsoft best practices for ransomware protection are based on a three step approach:
- Prepare your recovery plan
- Limit the scope of the damage
- Make it hard to get in

NEW QUESTION: 90
□□□ □□
Tenant1, Tenant2, Tenant3□□□ □ □□ Microsoft Entra □□□□ □□□□.
Sub1, Sub2, Sub3□□□ □ □□ Azure □□□ □□□□. □ □□□□ □□ Azure □□□ □□□ □ □□□□.
□□ □□ □□□ □□ □ □□□□ □□ Microsoft Sentinel □□ □□□ □□□□□.

Name	Subscription	Associated tenant
Sentinel1	Sub1	Tenant1
Sentinel2	Sub2	Tenant2
Sentinel3	Sub3	Tenant3

□□ □□ □□□ □□□□ □□□□ □□□□ □□□.
- Tenant1□ □□□□ Sub2□ □□□□ □□□ □ □□□ □□□□□.
□□□ □□□□□ □□□□□ □□□ Sub3□ □□□ □ □□□□.
□□ □□□.
- Sentinel2 □ Sentinel3□ □□ □□ □□ □□ □□□ □□□□□.
□□□ □□□□□ □□□ □□□□ □□, □□ □□ □□ □□□□ □□□□ □□□ □ □□ Microsoft Sentinel □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Answer:
Answer Area

Explanation:

Box 1: Azure Lighthouse

Delegate permissions by using

You can manage workspaces across tenants using Azure Lighthouse.

In many scenarios, the different Microsoft Sentinel workspaces can be located in different Microsoft Entra tenants. You can use Azure Lighthouse to extend all cross-workspace activities across tenant boundaries, allowing users in your managing tenant to work on Microsoft Sentinel workspaces across all tenants.

Once Azure Lighthouse is onboarded, use the directory + subscription selector on the Azure portal to select all the subscriptions containing workspaces you want to manage, in order to ensure that they'll all be available in the different workspace selectors in the portal.

When using Azure Lighthouse, it's recommended to create a group for each Microsoft Sentinel role and delegate permissions from each tenant to those groups.

Box 2: Workbooks

Microsoft Sentinel feature

Use cross-workspace workbooks

Workbooks provide dashboards and apps to Microsoft Sentinel. When working with multiple workspaces, workbooks provide monitoring and actions across workspaces.

Note: Extend Microsoft Sentinel across workspaces and tenants
When you onboard Microsoft Sentinel, your first step is to select your Log Analytics workspace. While you can get the full benefit of the Microsoft Sentinel experience with a single workspace, in some cases, you might want to extend your workspace to query and analyze your data across workspaces and tenants.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

NEW QUESTION: 91
Microsoft 365 □□□ Azure □□□ □□□□. Microsoft 365 Defender□ Microsoft Defender for Cloud□ □□□□□ □□□□.
Azure □□□□ 50□□ □□ □□□ □□□□ □□□□. □ □□ □□□ Windows Server 2019□ □ □□ □□ □□□□□□□ □□□□□.
□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□ □□, □□□□ □□ □□□□□□□ □□□ □ □□ □□□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. Azure AD□ □ □□
B. Endpoint□ Microsoft Defender□ □□ □□□□ □□ □□
C. □□□□ □□ Microsoft Defender□ □ □□ □□ □□ □□
D. Azure AD □□□ □□□ □ □□ □□
Answer: B (LEAVE A REPLY)
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy
https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy
https://docs.microsoft.com/en-us/security/benchmark/azure/overview

NEW QUESTION: 92

□□□□□ Azure □□□ □□□□□ Microsoft Defender for Cloud□ □□□□ □□□□.

Defender for Cloud□□ □□ □□ □□□ □□□□.

* □□□ □ □□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□□ □□□□□ □□□.
* □□□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □□□□ □□□.
* □□□ □□□ □□ □□ □□□ □□□□ □□□.
* □□□ □□□ □□ □□□ □□□□ □□□ □□□.

□□ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□. □□□ □□□□ □ □□?

A. Azure Storage □□

B. Azure □□□□ □□□

C. Microsoft Sentinel

D. Azure □□

Answer: (SHOW ANSWER)

An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled. Built in definitions include things like controlling what type of resources can be deployed or enforcing the use of tags on all resources. You can also create your own custom policy definitions.

Note: Azure security baseline for Azure Storage

This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Azure Storage. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Azure Security Benchmark and the related guidance applicable to Azure Storage.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud dashboard.

For example:

* 1.1: Protect Azure resources within virtual networks

Guidance: Configure your storage account's firewall by restricting access to clients from specific public IP address ranges, select virtual networks, or specific Azure resources. You can also configure Private Endpoints so traffic to the storage service from your enterprise travels exclusively over private networks.

* 1.8: Minimize complexity and administrative overhead of network security rules Guidance: For resource in Virtual Networks that need access to your Storage account, use Virtual Network

Service tags for the configured Virtual Network to define network access controls on network security groups or Azure Firewall. You can use service tags in place of specific IP addresses when creating security rules.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

NEW QUESTION: 93
□□□ □□□ Azure □□ □ □□ □□□ □□□□ □□ □□□□□□□. □□ □□□□ □□□ □ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□.
□□□□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□□.
□□ □ □□□(PKI)□ □□□□□ □□ □□ Azure Key Vault□ □□□□ □□ □□□□.
□□□ □□ □□□ □□□□ □□ □□ □□ □ □□□ □□□□□? □ □□□ □□□□ □□□ □□□□□.
A. □□ □□□ □□□□□.
B. □□□ □□□□ □□□□□□.
C. □□□ □□□□ □□□ □□□□ □□□.
D. □□□ □□□ □□□□□.
E. □□ □□□ □□□□□.
Answer: A,E (LEAVE A REPLY)
Your recommendation will ensure non-repudiation and prevent information disclosure. Both of these are benefits provided by Public Key Infrastructure (PKI). PKI provides a framework for creating, managing, and deploying X.509 certificates that can be used to digitally sign data. A digital signature ensures nonrepudiation, meaning that the signer cannot deny, or repudiate, that their signature was used. Certificates are also used on apps and web servers to facilitate encrypted communications, such as with Hypertext Transfer Protocol Secure (HTTPS). Azure Key Vault can be used to create and manage digital certificates.
PKI does not facilitate the recovery of lost data. Azure Backup can be used to provide this benefit.
PKI does not prevent data modifications. However, digital signatures can be used to detect data modifications. If signed data has been modified, the signature will be invalid.
PKI does not enhance data availability. This is typically done using data replication schemes, clustering, and other resiliency approaches. Services like Azure Load Balancer and Azure Application Gateway can be used to enhance data availability.
NEW QUESTION: 94
□□ Azure Blob Storage □□□ □□□ Azure □□□ □□□□.
□□□ Blob □□□□□ □□□□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Microsoft Defender for Storage□□ □□□ □□□ □□ □□
B. □□□□□ Microsoft Defender□ □□□ □□ □□
C. □□□□□ Microsoft Defender□ □□□ □□
D. Microsoft Defender for Storage□ □□□ □□

Answer: D (LEAVE A REPLY)

Malware Scanning in Defender for Storage helps protect your Azure Blob Storage from malicious content by performing a full malware scan on uploaded content in near real time, using Microsoft Defender Antivirus capabilities. It's designed to help fulfill security and compliance requirements for handling untrusted content.

The Malware Scanning capability is an agentless SaaS solution that allows simple setup at scale, with zero maintenance, and supports automating response at scale.

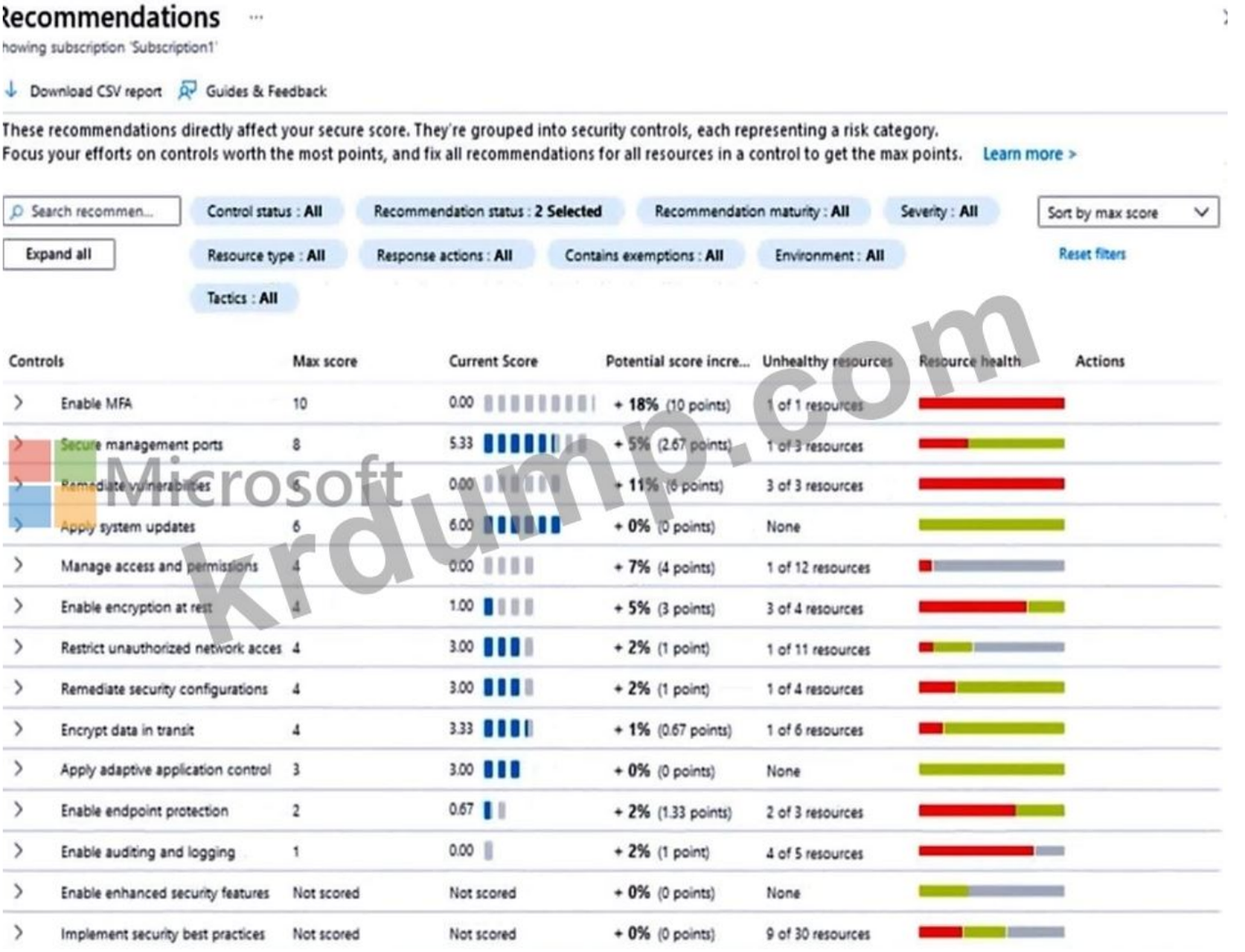
Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-malware-scan

NEW QUESTION: 95

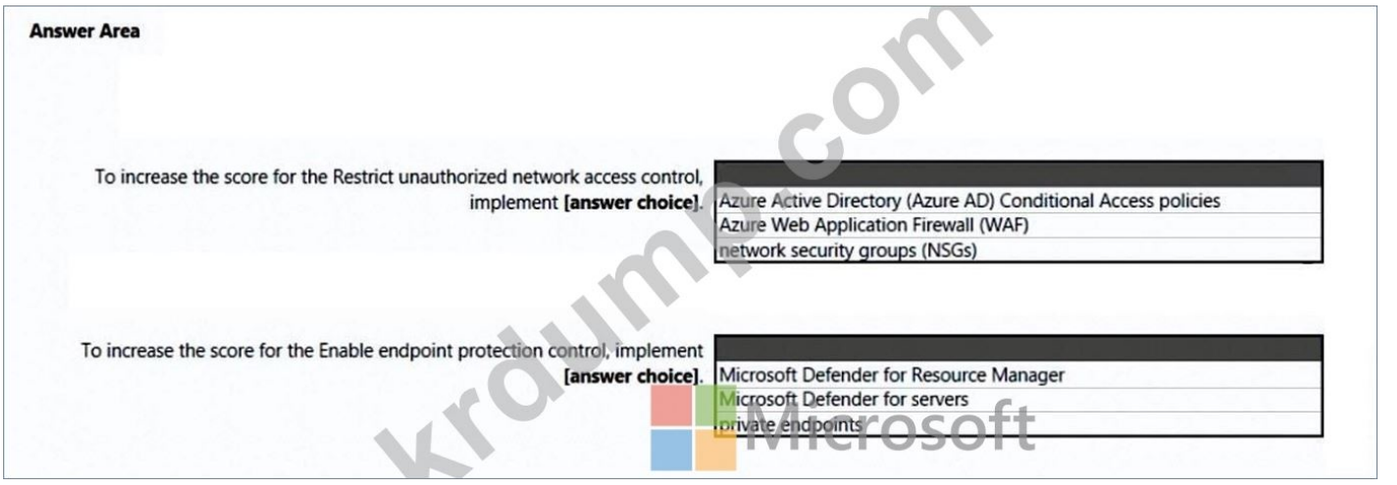
□□□ □□

□□ □□□ □□ Microsoft Defender for Cloud□ □□□.

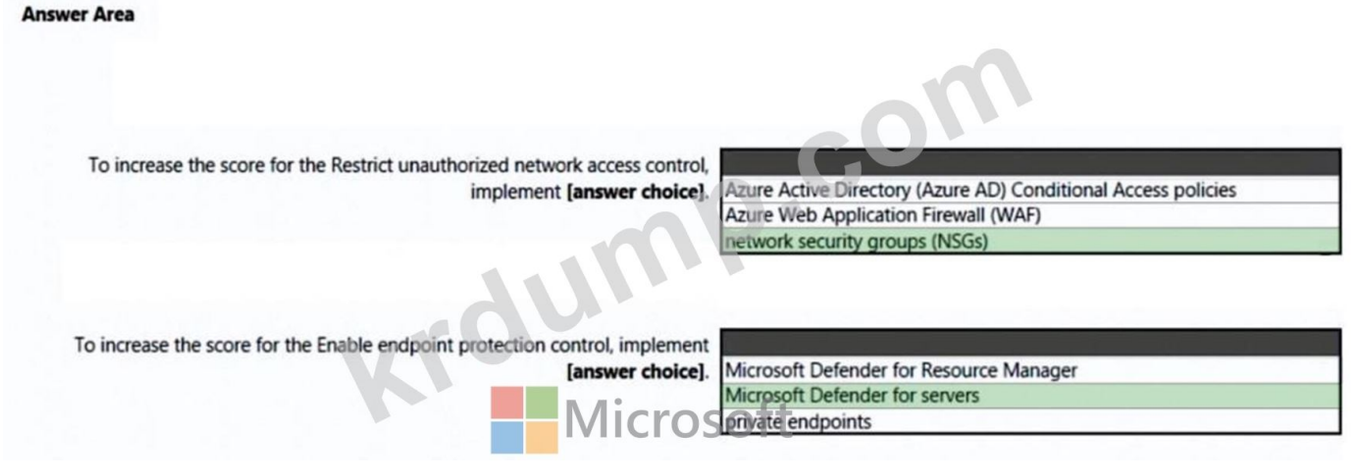


□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □ □□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: network security groups (NSGs)

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833 Box 2: Microsoft Defender for servers Enable endpoint protection - Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

NEW QUESTION: 96

Microsoft 365 □□□ Azure □□□ □□□□. Microsoft Defender XDR□ Microsoft Defender for Cloud□ □□□□□ □□□□.

Azure □□□□ 50□□ □□ □□□ □□□□ □□□□. □ □□ □□□ Windows Server 2019□ □ □□ □□ □□□□□□□ □□□□□.

□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□ □□, □□□□ □□ □□□□□□□ □□□ □

□□ □□□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. Microsoft Entra □□□□ □ □□
B. □□□□ □□ Microsoft Defender□ OAuth □ □□
C. Microsoft Endpoint Manager□ □ □□ □□
D. Endpoint□ Microsoft Defender□ □□ □□□□ □□ □□
Answer: D (LEAVE A REPLY)
Microsoft Defender for Endpoint includes application control policies that allow you to define which applications are authorized to run on a machine.
This can help block any unauthorized applications and provide an approval mechanism, ensuring that only approved software is allowed to run.
The solution aligns with the requirement to block unauthorized applications from running on the virtual machines automatically until approved by an administrator.

NEW QUESTION: 97
□□ □□ 2 - Litware, inc.
□□
Litware, Inc.□ □□□ □□□□□□□ □□□ □ □□ □□□ □□□□□. Litware□ □□ □□□ 30□□ □□□ □□ □□ □□□ □□ □□□□. □□ □□ □□□ VPN□ □□□□ □□□ □□□ □□.
Litware□ □□ 2□□ □□□□□ □□ □□ □□□□□□. □□ □□□□ □□□□ □□□ □ □ □ □□□ □□□□□.
□□ □□
Litware□□ litware.com□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□□ 20 □□ Azure □□□ □□□ Microsoft Entra □□□□ □□□□. Microsoft Entra Connect□ □□ □ □□ □□□□ □ □□□□□. □□ □□ □□□□ □□□□□□ □□ □□ □□□ □□□□□□.
□□ Litware □□□□ Microsoft 365 E5 □□□□□ □□□□□.
□ □□□□ Litware□ □□□□ □□□ □□ AD DS □□□□, Microsoft Entra □□□ □ □□ □ □ Azure □□□ □□□□□.
□□ □□. □□□ □□ □□
Litware□ □□□ □□ □□ □□□ □□□ □□□□□.
- □ Microsoft Entra □□□□ □□ □□ □□ □□ □□□ □□□□.
- Litware□ □□ Azure □□□ □□□□□□ □□ □□ Azure □□□□□ □□□□ □□ □□ □ □□□ □□□□□.
- VPN□ □□□□ □□ □□□□□ □□ □□□□□□□ □□ □□ □□□□ □□□□ □□ Microsoft Entra Application Proxy□ □□□□□.
□□ □□. □□□□ □□ □□
Litware□ □□□ □□ □□□□ □□ □□□ □□□□□.
- □□□□ □□□□□ □□□□ □□□□□□.
- □□□ □□□□□ □□□ □□□□□ □□□□□□.
□□ □□. □□□□□ □□ □□

Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.
- □□□ □□□□ Azure□□ □-□□□□ □□□□ □□□ □ □□□□.
o Azure Policy□ □□□□ □□ □ □□ □□□ □□□□□.
o □□ □□ □□ □ □□ □□□□□ □□□□□.
o □□ □□□ □□□□□.
- □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
□□ □□. Microsoft Sentinel □□ □□
Litware□ Microsoft Sentinel□ □□ □□ □ □□□ □□(SIEM)□ □□ □□□□□□□ □□ □□ (SOAR) □□□ □□□ □□□□□. □□ Microsoft Sentinel□ □□□□ □□ □□ □□(SOC)□ □□ □□□□□□ □□□.
□□□□. □□ □□□□
Litware□ □□□ □□ □□ □□ □□□ □□□□□.
- AD DS □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □□ □□ □□□ □□□□□.
- Microsoft Entra □□□ □□□ □□□□ □□ □□□ □□ □□□□ □□ AD DS □□□ □□□ □□□ □□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □ □□□ □□□ □□□ □□□□□. □□□□ □ □□ □□□□□.
o □□ □□, □□□ □ □□□□ □□
o □□□ □□, □□□□ □ □□□□ □□
o □□□□ □□□ □□ □□
□□ □□. □□ □□ □□ □□
Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.
- □□□ □□□□ □□ □ □□□□ □□□ □□, □□ □□ □ □□□□ □□□ □ □□□ □□ □ □□ □□□□□.
- □□ □□ Azure Policy □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
- □□ □□□ □□□ □□□□□.
□□ □□. Azure Landing Zone □□ □□
Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.
- □□ Azure □□□□ Azure Firewall□ □□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □.
- □□ □□□ □□ □□□ □□□ □□□□□.
- □ □□ □□ Azure □□ □□□ □□ □□□□□□ □□ Microsoft □□ □□□□□ □□ □□□ □□ Azure App Service □□□ □□□□□ □□□□□.
- □□□ □□ □□□□ □□□□□□.
- □□□□ □□□□ □□□□□□.
□□ □ □□□□□□ □□□ □ □□□□□ □□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□. □ □□ □□ □□□ □□ □□□ □□□□.
- □□ □□□□ □□□□□.
- litware.com□ DNS □□□□□□□ □□□□□.
□□ □□. □□□□□□ □□ □□ □□

Litware□ □□□ □□ □□□□□□ □□ □□ □□□ □□□□□.
- Microsoft Entra Application Proxy□ □□□□ SSO(Single Sign-On)□ □□□□ □□ □□□□□ □□ □□□□□.
- Microsoft SharePoint Online □ Exchange Online □□□□ □□ □□□□ □□□□□ □□□□ □□ □□□□□.
□□□□□□ □□ □□ □□□ □□□□□ □□□□□□□ □□ □ □□ □□ □□□ □□□□ □□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □□ □□□ □□□ □□(SAML)
B. NTLMv2
C. □□□ □□ □□
D. □□□□□
Answer: (SHOW ANSWER)
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Microsoft Entra Application Proxy.
You can provide single sign-on (SSO) to on-premises applications that are secured with SAML authentication and provide remote access to these applications through Application Proxy. With SAML single sign-on, Microsoft Entra ID authenticates to the application by using the user's Microsoft Entra account.
You can provide single sign-on for on-premises applications published through Application Proxy that are secured with integrated Windows authentication.
These applications require a Kerberos ticket for access. Application Proxy uses Kerberos Constrained Delegation (KCD) to support these applications.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

NEW QUESTION: 98
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□.
Azure Security Benchmark V3 □□□□ □□□□ □□□□.
□□ □□ □□ □□□□ □□□□ 8□ □ 0□□ □□□□ □□ □□ □□□□□.
□□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□□ □□□.

□□ □□: □□ □□ □□□□ JIT(Just-In-Time) VM □□□□ □□□□□ □□ □□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.

Recommendations:

- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION: 99

Azure□ Microsoft □□□□ □□ □□□□□□ □□□□ □□ □□ □□□ □□□□.
□□□□□, □□□□□□, □□, □□□□ □□ □□ □□□□ □□□□ □□ □□□□ □□ □□ □□□ □□□ □□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?

A. □□□□ □□□

B. □□ □□ □□

C. □□□□ □□

D. Microsoft □□□□ □□ □□□□□ □□ □□

Answer: D (LEAVE A REPLY)

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multi-cloud environment. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

Controls include:

* Endpoint Security (ES)

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in cloud environments.

* Data Protection (DP)

Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key management and certificate management.

* Etc.

Reference:

https://learn.microsoft.com/en-us/security/benchmark/azure/overview

NEW QUESTION: 100

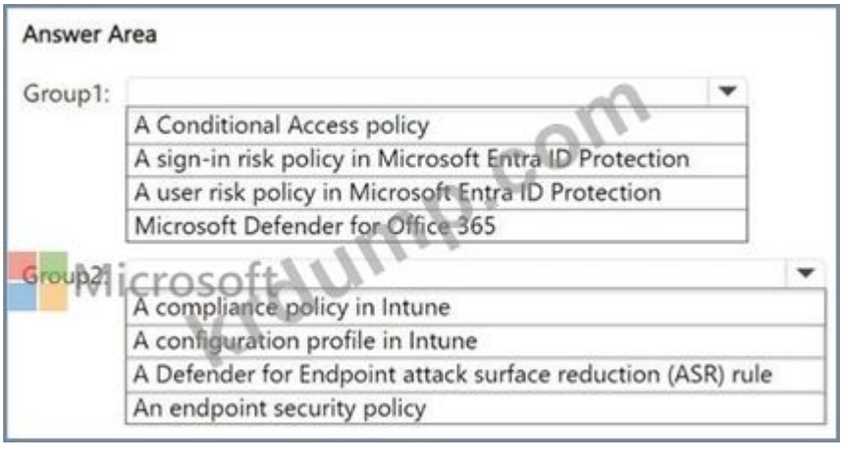
□□□ □□

Microsoft 365 □□□□ □□□ 1,000□□ □□ 1, □□ 2□□ □ □□□ □□□□. □□ □□□□ Microsoft Intune□ Microsoft Defender for Endpoint□ □□□□ □□□ □□□ □□□□. □□ 1□ Microsoft Entra□ Microsoft 365 □□□□ □□□□, □□ 2□ Intune□ Defender for Endpoint□ □□□□□.

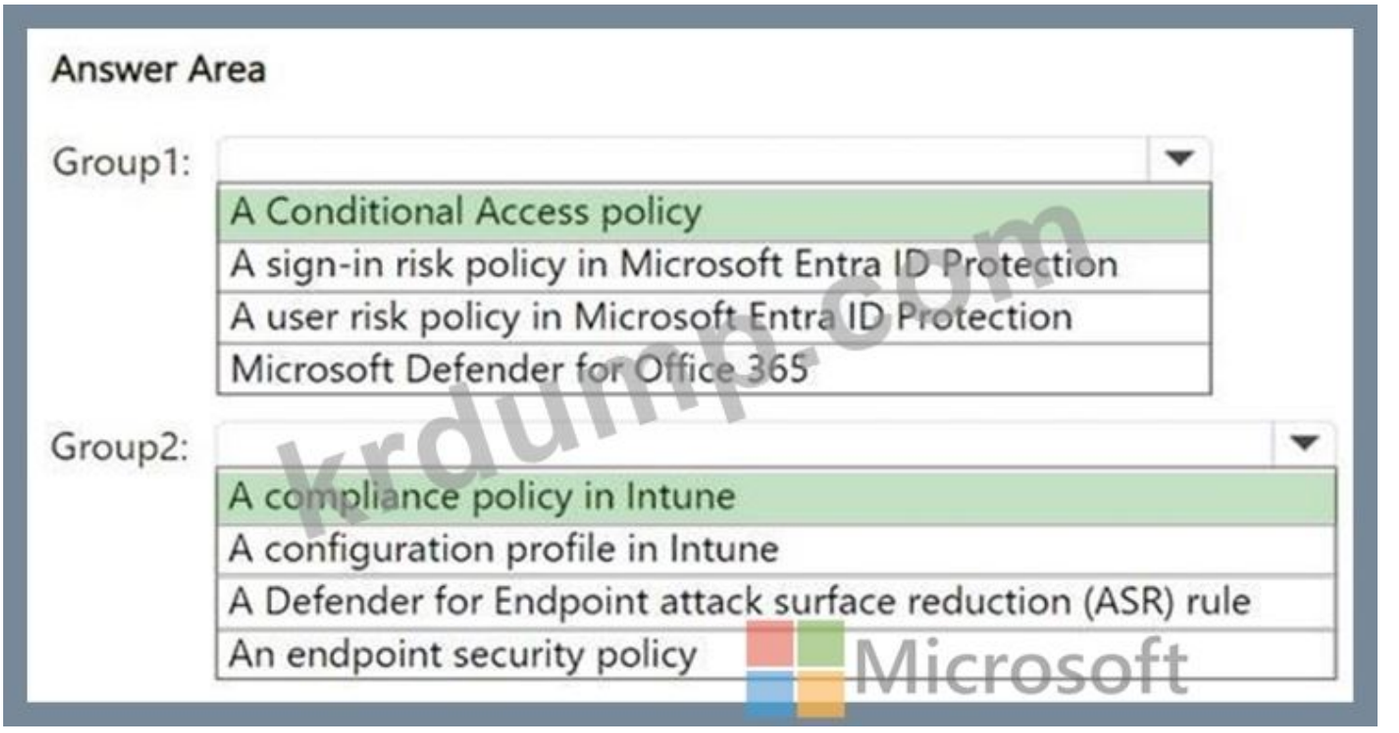
□□□□ □□□□□ □□□□ □□□□ Microsoft 365 □□□□ □□□□ □□□□ □□ □□□ □ □□□□ □□□.

□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□□□.

□□: □□□ 1□□□□.



Answer:



Explanation:

Box 1: A Conditional Access policy

Group1 manages Microsoft Entra and Microsoft 365 services.

Microsoft Entra ID, Conditional Access, Common Conditional Access policy: Require a compliant device, Microsoft Entra hybrid joined device, or multifactor authentication for all users

Organizations who deploy Microsoft Intune can use the information returned from their devices to identify devices that meet compliance requirements such as:
Requiring a PIN to unlock
*-> Requiring device encryption
Requiring a minimum or maximum operating system version
Requiring a device isn't jailbroken or rooted
Box 2: A compliance policy in Intune
Group2 manages Intune and Defender for Endpoint.
Device Compliance settings for Windows 10/11 in Intune includes:
* Encryption
Encryption of data storage on a device:
This setting applies to all drives on a device.
Not configured (default)
Require - Use Require to encrypt data storage on your devices.
DeviceStatus CSP - DeviceStatus/Compliance/EncryptionCompliance
Reference:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-compliant-device
https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

NEW QUESTION: 101
□□ □□ 2 - Litware, inc.
□□
Litware, Inc.□ □□□ □□□□□□□ □□□ □ □□ □□□ □□□□□. Litware□ □□ □□□ 30□□ □□□ □□ □□ □□□ □□ □□□□. □□ □□ □□□ VPN□ □□□□ □□□ □□□ □□.
Litware□ □□ 2□□ □□□□□ □□ □□ □□□□□□. □□ □□□□ □□□□ □□□ □ □ □ □□□ □□□□□.
□□ □□
Litware□□ litware.com□□□ Active Directory □□□ □□□(AD DS) □□□□□ □□□□□ 20 □□ Azure □□□ □□□ Microsoft Entra □□□□ □□□□. Microsoft Entra Connect□ □□ □ □□ □□□□ □ □□□□□. □□ □□ □□□□ □□□□□□ □□ □□ □□□ □□□□□□.
□□ Litware □□□□ Microsoft 365 E5 □□□□□ □□□□□.
□ □□□□ Litware□ □□□□ □□□ □□ AD DS □□□□, Microsoft Entra □□□ □ □□ □ □ Azure □□□ □□□□□.
□□ □□. □□□ □□ □□
Litware□ □□□ □□ □□ □□□ □□□ □□□□□.
- □ Microsoft Entra □□□□ □□ □□ □□ □□ □□□ □□□□.
- Litware□ □□ Azure □□□ □□□□□□ □□ □□ Azure □□□□□ □□□□ □□ □□ □ □□□ □□□□□.
- VPN□ □□□□ □□ □□□□□ □□ □□□□□□□ □□ □□ □□□□ □□□□ □□

Microsoft Entra Application Proxy□ □□□□□.

□□ □□. □□□□ □□ □□

Litware□ □□□ □□ □□□□ □□ □□□ □□□□□.

- □□□□ □□□□□ □□□□ □□□□□□.
- □□□ □□□□□ □□□ □□□□□ □□□□□□.

□□ □□. □□□□□ □□ □□

Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.

- □□□ □□□□ Azure□□ □-□□□□ □□□□ □□□ □ □□□□.

o Azure Policy□ □□□□ □□ □ □□ □□□ □□□□□.

o □□ □□ □□ □ □□ □□□□□ □□□□□.

o □□ □□□ □□□□□.

- □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

□□ □□. Microsoft Sentinel □□ □□

Litware□ Microsoft Sentinel□ □□ □□ □ □□□ □□(SIEM)□ □□ □□□□□□□ □□ □□ (SOAR) □□□ □□□ □□□□□. □□ Microsoft Sentinel□ □□□□ □□ □□ □□(SOC)□ □□ □□□□□□ □□□.

□□□□. □□ □□□□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

- AD DS □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □□ □□ □□□ □□□□□.
- Microsoft Entra □□□ □□□ □□□□ □□ □□□ □□ □□□□ □□ AD DS □□□ □□□ □□□ □□ □□□□□.
- Litware□ Microsoft Entra □□□□□ □□□ □ □□□ □□□ □□□ □□□□□. □□□□ □ □□ □□□□□.

o □□ □□, □□□ □ □□□□ □□

o □□□ □□, □□□□ □ □□□□ □□

o □□□□ □□□ □□ □□

□□ □□. □□ □□ □□ □□

Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.

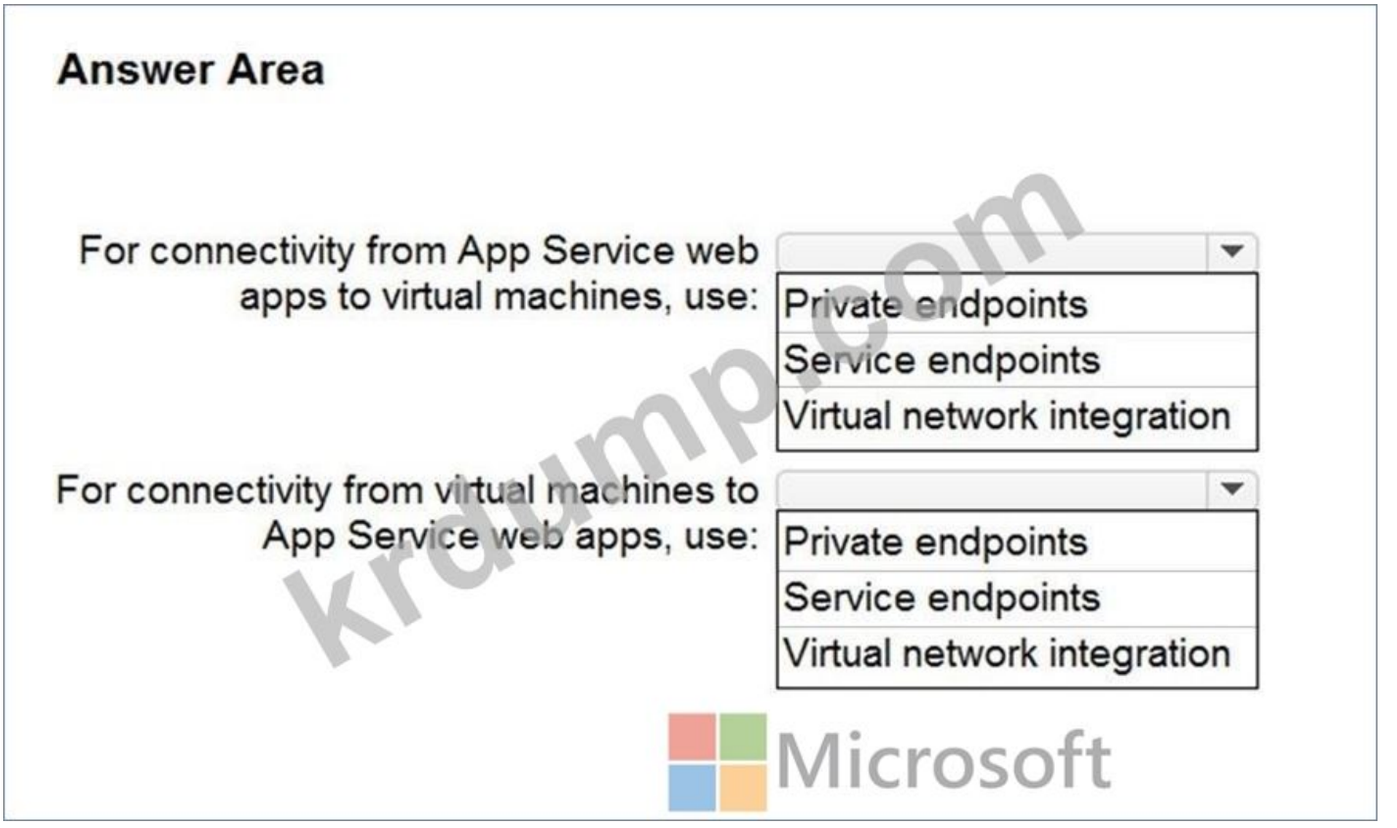
- □□□ □□□□ □□ □ □□□□ □□□ □□, □□ □□ □ □□□□ □□□ □ □□□ □□ □ □□ □□□□□.
- □□ □□ Azure Policy □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
- □□ □□□ □□□ □□□□□.

□□ □□. Azure Landing Zone □□ □□

Litware□ □□□ □□ □□ □□ □□ □□□ □□□□□.

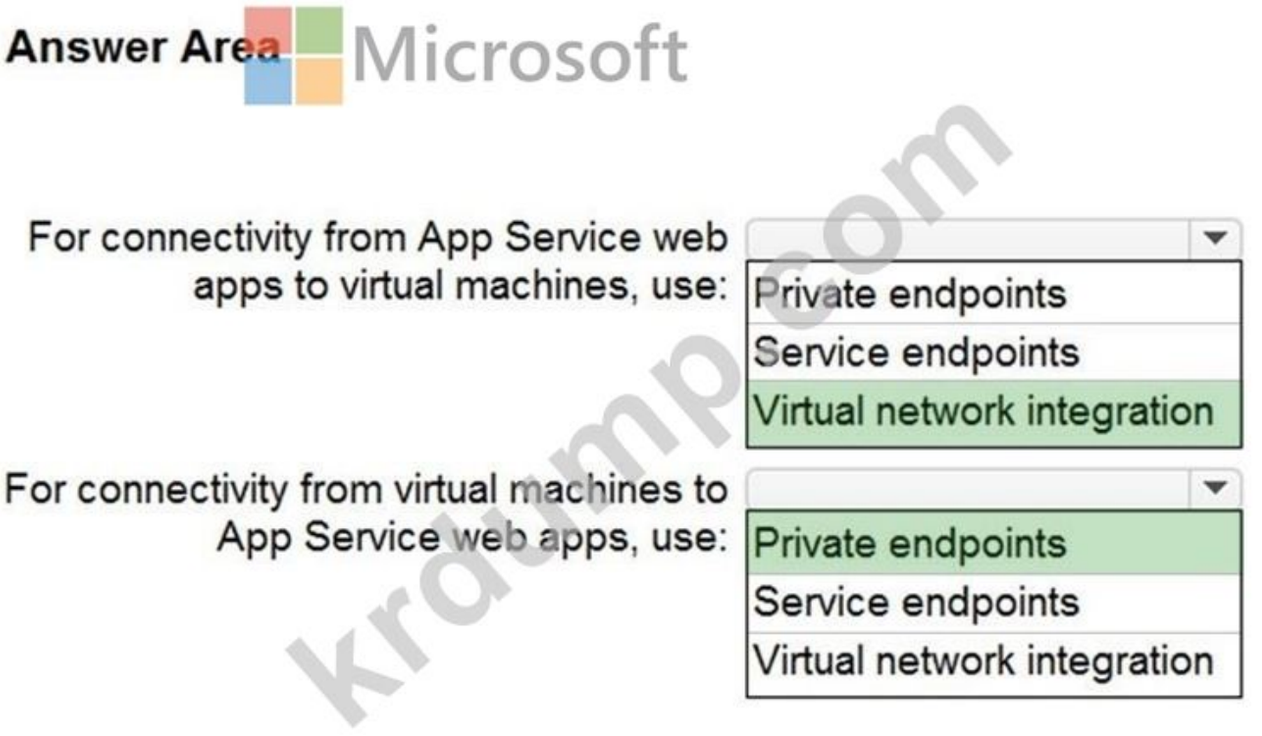
- □□ Azure □□□□ Azure Firewall□ □□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □.
- □□ □□□ □□ □□□ □□□ □□□□□.
- □ □□ □□ Azure □□ □□□ □□ □□□□□□ □□ Microsoft □□ □□□□□ □□ □□□ □□ Azure App Service □□□ □□□□□ □□□□□.
- □□□ □□ □□□□ □□□□□□.

- □□□□ □□□□ □□□□□□.
□□ □ □□□□□□ □□□ □ □□□□□ □□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□. □ □□ □□ □□□ □□ □□□ □□□□.
- □□ □□□□ □□□□□.
- litware.com□ DNS □□□□□□□ □□□□□.
□□ □□. □□□□□□ □□ □□ □□
Litware□ □□□ □□ □□□□□□ □□ □□ □□□ □□□□□.
- Microsoft Entra Application Proxy□ □□□□ SSO(Single Sign-On)□ □□□□ □□ □□□□□ □□ □□□□□.
- Microsoft SharePoint Online □ Exchange Online □□□□ □□ □□□□ □□□□□ □□□□ □□ □□□□□.
□□□ □□
App Service □□ □□□ □□ □□□ □□□□ □□□. □□□□ □□ □ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□□ □□ □□□ □□□ 1□□ □□□□□.



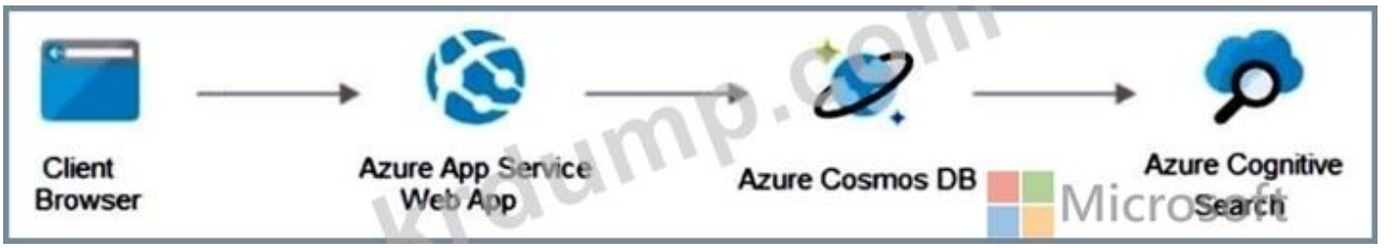
Answer:

Answer Area



Explanation:
Box 1: Virtual Network Integration
Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network.
Box 2: Private Endpoints
You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration
https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-webapp-portal

NEW QUESTION: 102
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
□+□□□□ □□□□□ Angular □ Node.js□ □□□ □□□□□ □□□ □□□□. □ □□□ MongoDB □□□□□□□ □□□□□. □ □□□ Azure□ □□□□□□□ □□□□□.
□□□ □□□□ □□ Azure □□ □□□ □□□ □□ □□□□□ □□□□□.



□ □□ □□□□□□ □ □□□ □□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□ □□□ □□□ □□□.

□□□: Azure WAF(□ □□□□□□ □□□)□ □□ Azure Front Door□ □□□□ □□ □□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

NEW QUESTION: 103

□□□ □□□□ Windows 10, Windows 11 □□ Windows Server□ □□□□ □□□ □□□□.

□□□ □□ □□□ □□□□ □□□□.

Microsoft Security Compliance Toolkit□ □□ □□□ □□□ □□□□□.

□□□□ □□ □□ □□□ □□□□ □ □□□ □□□□ □□ □□□□?

A. Microsoft Intune

B. □□ □□□

C. □□ □□ □□ □□(LGPO)

D. □□□ □□ □□ □□

Answer: B (LEAVE A REPLY)

Microsoft Security Compliance Toolkit 1.0, Policy Analyzer.

The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:

- Highlight when a set of Group Policies has redundant settings or internal inconsistencies.
- Highlight the differences between versions or sets of Group Policies.
- Compare GPOs against current local policy and local registry settings
- Export results to a Microsoft Excel spreadsheet

Policy Analyzer lets you treat a set of GPOs as a single unit. This treatment makes it easy to determine whether particular settings are duplicated across the GPOs or are set to conflicting values. Policy Analyzer also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.

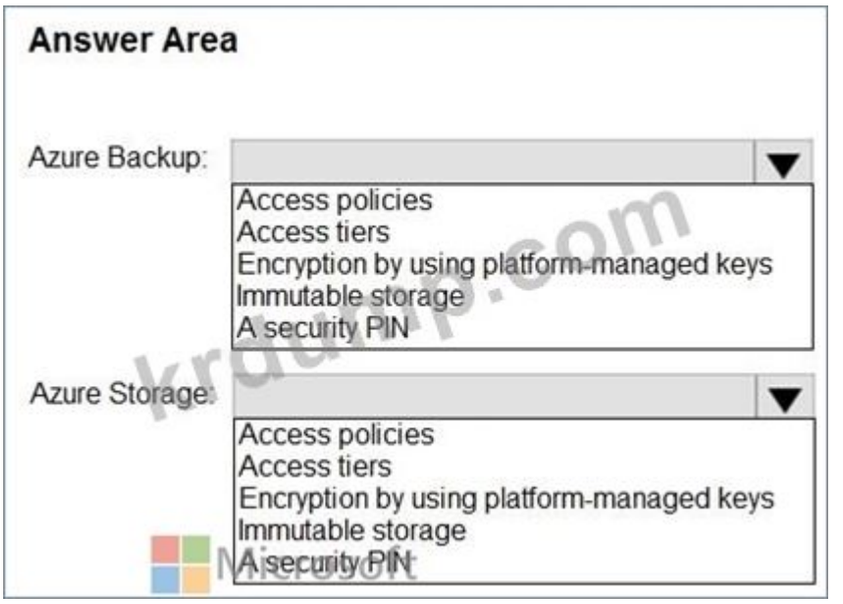
Note: The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft- recommended security configuration baselines for Windows and other Microsoft products.

The SCT enables administrators to effectively manage their enterprise's Group Policy Objects

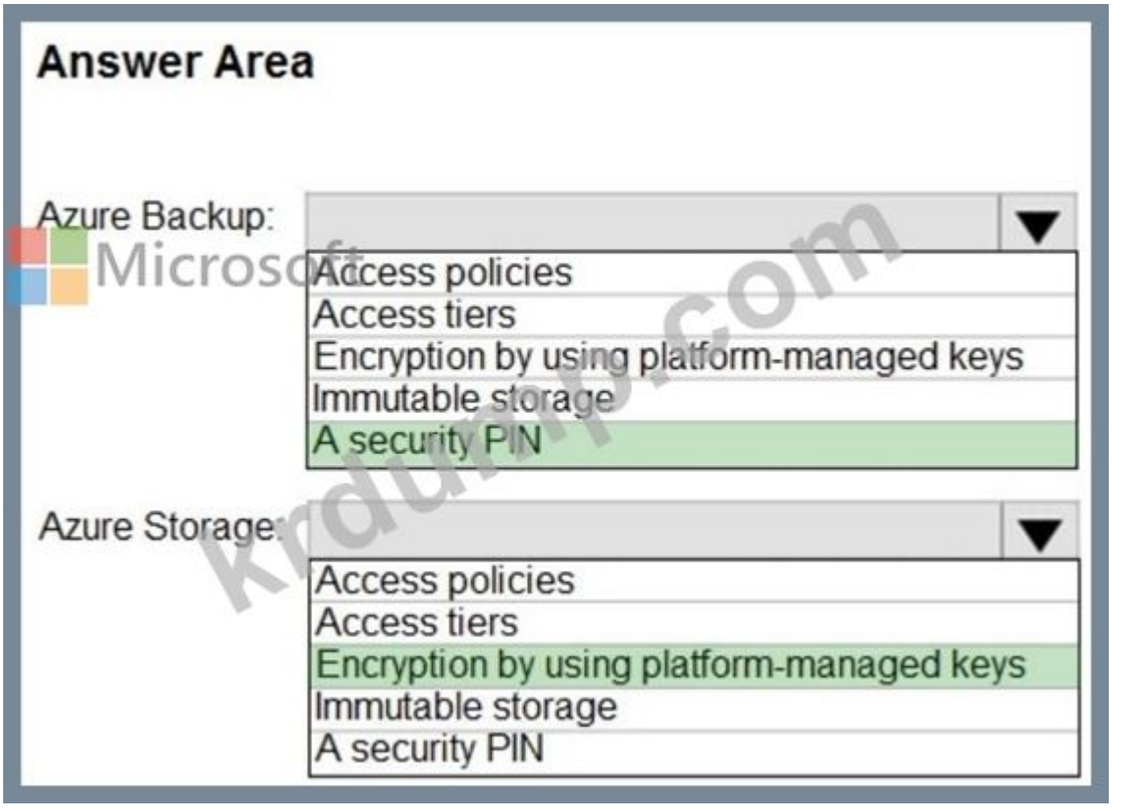
(GPOs). Using the toolkit, administrators can compare their current GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active Directory or individually through local policy.
Security Compliance Toolkit Tools:
Policy Analyzer -
Local Group Policy Object (LGPO)
Set Object Security -
GPO to Policy Rules -
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

NEW QUESTION: 104
Microsoft 365 E5 □□□ □□□□. □ □□□□ Windows 11 Pro□ □□□□ Microsoft Intune□ □□□ □□ 500□□ □□□□ □□□□.
□□□ □□ □□ □□ □□ □□□ □□□□□ Microsoft Defender Vulnerability Management□ □□□ □□□□ □□□.
□□□□ □□ □□□ □□□□□ □□ Endpoint □□ □□□ □□□□ □□□?
A. □□ □□
B. □□ □□ □□
C. □□□□□ □□ □ □□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)
For Microsoft Intune enrolled Windows 11 Pro devices protected by Microsoft Defender Vulnerability Management, the Endpoint security policy for Attack Surface Reduction would provide recommended configuration changes. This policy allows you to manage settings for Microsoft Defender Antivirus and the Windows Security experience on your devices, enabling you to implement best practices and mitigate potential vulnerabilities.
Reference:
https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

NEW QUESTION: 105
□□□ □□
□□□□□ □□□□□□□ □□□□ □□□□ □□ Azure□ □□□□□□ □□□.
Azure Backup□ Azure Storage □ □□ □□□ □□□□ □□□□□□ □□ □□□ □□ □□□ □□□□□ □□□□ □□□. □□ □□□□ Microsoft □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 106

Microsoft □□□□ □□□ □□ Microsoft □□□□ □□ □□□□□ □□□□ □□ □□□□□ □ □□□ □□□□.

Azure Security Benchmark□ □□ ID □□□ □ □□ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

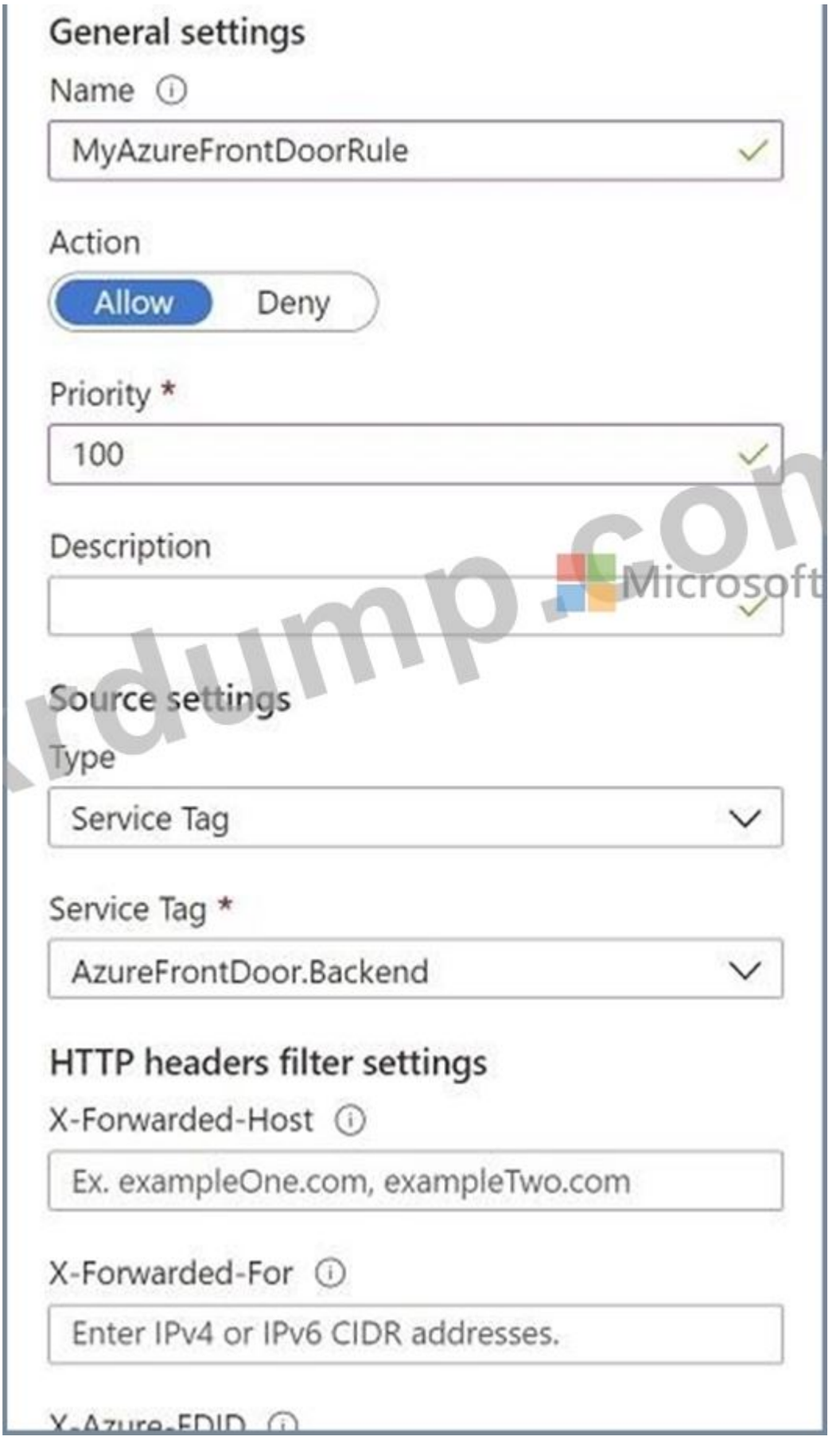
A. □□□□□□ ID□ □□□□ □□□□ □□□□□.

B. ID □ □□□ □□ □□□ □□□□□.

C. □□ □ □□ □□□□ □□□□□.

D. ID □ □□□ □□□ □□ □□ □□□ □□□□□□.
E. □□□□ ID □ □□ □□□□ □□□□□.
Answer: A,C,E (LEAVE A REPLY)
https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v2-identity-management

NEW QUESTION: 107
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
Azure Front Door □□□□□ □□ Azure App Service □□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□.
□ □□ Front Door □□□□□ □□□□ □□□□ □□□□□ □□ □□□□ □□□□ □□□.
□□ □□: □□□□□□ □□□ □□ □□□□ □□□ □□□□ □□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.



Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

NEW QUESTION: 108
Azure □□□ □□□□.
□□ DNS □□ □□□□ □□□□□ contoso.com□□□ DNS □□□□ □□□□.
□□□□ Azure DevOps□ □□□□ □□□ App Service Environment□ □□□□□. □ □□ □ □□□ □□ □□ CNAME □□□□ contoso.com□ □□□□□.
□ □ □□ DNS □□□□ □□□□ □□ □□□□ □□□ □□□ □□□. □□ □□□□ □□ □ □ □□□ □□□□ □□□.
- □□ □□□□ □□ CNAME □□□□ □□□ □□ □□□ □□□□□.
□□ □□□.
- □□□ □□□ □□□□□□.
□□□□□ □□□ □□□□ □□□?
A. □□□□ □□ Microsoft Defender
B. DevOps□ □□ Microsoft Defender
C. □ □□□□ Microsoft Defender
D. DNS□ Microsoft Defender
Answer: (SHOW ANSWER)
Defender for App Service identifies any DNS entries remaining in your DNS registrar when an App Service website is decommissioned - these are known as dangling DNS entries. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection

NEW QUESTION: 109
□□□ Microsoft Azure□ Microsoft 365 □□□ □□□□ □□□ □□ □□□□□, □□ □□□□ □□□ □□□□□.
□□ □□□ □□, □□□ □□□□ □ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□ □ □□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□ □□□□□□.
□□ □□□ □□ □□□ □□, □□, □□, □□□□ □□ □□□□□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□ □ □□□□?
A. Microsoft Sentinel
B. □□□□□ Microsoft Defender
C. 365 □□ Microsoft Defender
D. □□□□□□ □□ □□□
Answer: (SHOW ANSWER)
Option A is correct because Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.
Option B is incorrect because Microsoft Defender for Cloud does not provide proactive hunting

and threat response.
Option C is incorrect because Microsoft Defender for 365 Apps will not provide attack detection, threat visibility, proactive hunting, and threat response for Azure resources.
Option D is incorrect because Defender for Endpoint will not offer a single solution for attack detection, threat visibility, proactive hunting, and threat response.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/overview

NEW QUESTION: 110
Windows Server□ □□□□ DB1□□□ Microsoft SQL Server □□□□□□□ □□□□ □□□ □□ □□□ □□□□.
DB1□ Azure□ □□□□□□□ □□□□□.
□□ □□ □□□ □□□□ □□□□ Azure □□□□□□ □□□□ □□□□ □□□.
* □□ □□□ □□□□ □□□ □□□□ □□□□□ □□□□ □□□ □□□□□□.
* □□□□□□ □□□□ □□□ □□□□ □□□□□ □□ □□□□□.
* □□ □ □□□□□□ □□□ □□ □□ □□□ □□□□□□.
* Microsoft Azure Attestation □□
* □□□□ □□ □□□□ □□□□□
□□□□□ □□□ □□□□ □□□?
A. □□□ □□ □□(VBS) □□□□□□ □□ Azure Virtual Machines□ SQL Server
B. □□□ □□ □□(VBS) □□□□□□ □□ Azure SQL □□□□□□
C. Always Encrypted□ □□□ Azure SQL □□□ □□□□
D. Intel Software Guard Extensions(Intel SGX) □□□□□□ □□□ Azure SQL □□□□□□
Answer: D (LEAVE A REPLY)
Can use Azure Attestation for attesting Intel SGX (Intel Software Guard Extension) enclaves for Always Encrypted with secure enclaves in Azure SQL Database.
Secure enclave attestation
Enclave attestation is a defense-in-depth mechanism that can help detect attacks that involve tampering with the enclave code or its environment by malicious administrators.
Reference:
https://learn.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-enclaves-configure-attestation
https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-enclaves

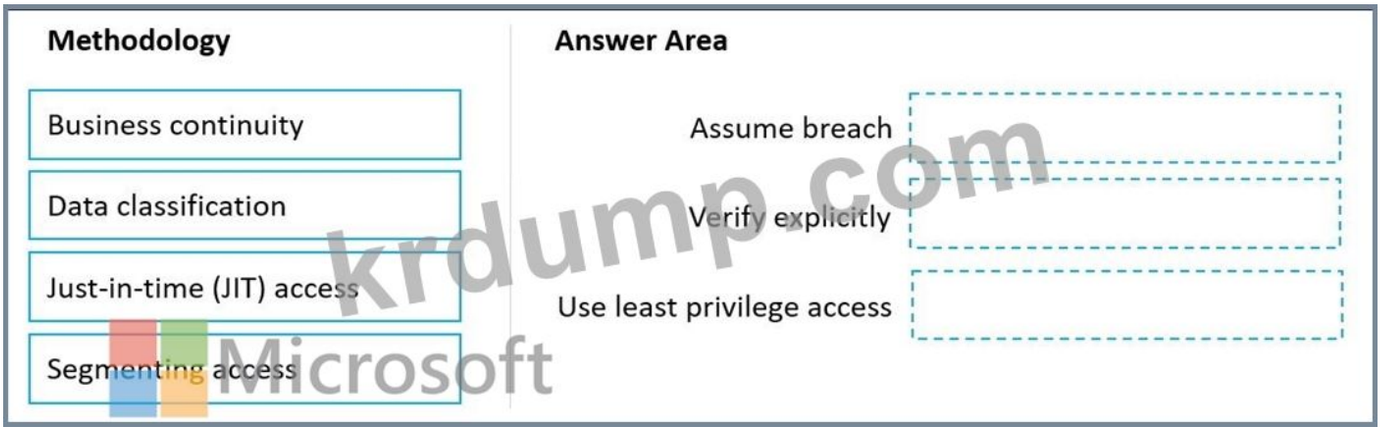
NEW QUESTION: 111
contoso.com□□□ Microsoft Entra □□□□ □□□□.
App1□□□ □□ □□□ □□□□□□□ □□□ □□□ □□□ □□□□. App1□ fabrikam.com □□□ Microsoft Entra □□□□ □□□□ □□□□.
contoso.com□ □□□□ App1□ □□□ □ □□□ □□□□ □□□.
contoso.com□□ □□□ □□□ □□ □□□□?

A. □□□ □□
B. □□□□□ □□□ □□ ID
C. □□□□□□ □□
D. □□□□ □□□ □□ ID
Answer: A (LEAVE A REPLY)
A service principal is needed in a tenant to authenticate users to a Microsoft Entra multi-tenant application located in another tenant. When a user from a different tenant signs in to a multi-tenant application, a service principal is automatically created in the user's tenant upon consent to the application's permissions. This service principal acts as the application's identity within that specific tenant, enabling authentication and access to resources secured by that tenant.
Reference:
https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals

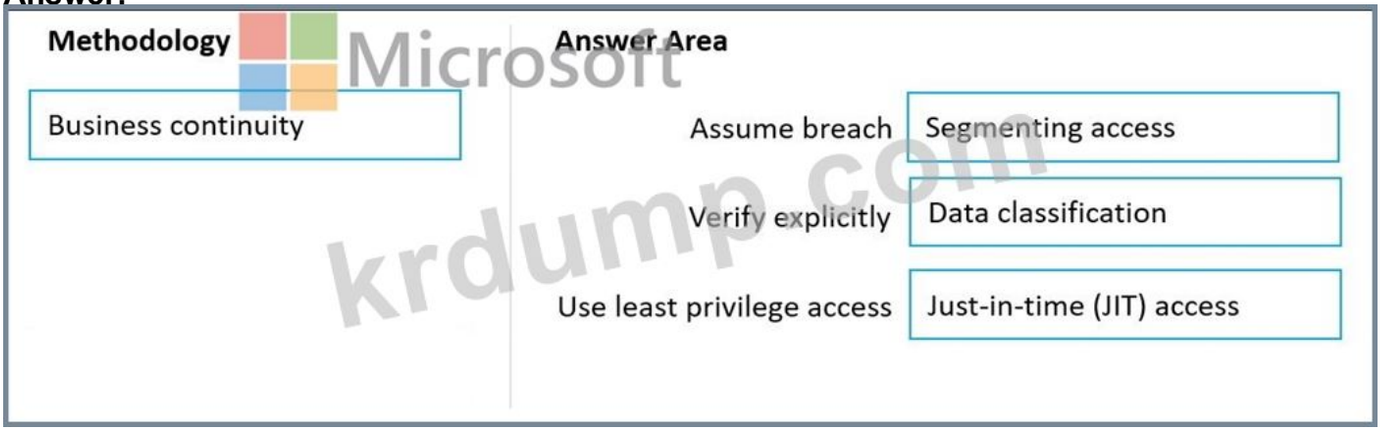
NEW QUESTION: 112
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
Azure □□□□ □□ □□□□ □□ □□□ □□□ □□□□ □□□□.
AES□ □□□□ □□ □□ □□□□ □□□□□□ □□ □□□ □□□□ □□□.
256□□ □. □□□□ □□□ □□ □□ □□□ □ □□□ □□□.
□□ □□: Azure Storage□ Blob □□□□□ □□ □□ □□ □(CMK)□ □□□□ □□□□ □□ □□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
We need to use customer-managed keys.
Azure Storage encryption for data at rest.
Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments.
Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.
Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to manage encryption with your own keys, you have two options. You can use either type of key management, or both:
* You can specify a customer-managed key to use for encrypting and decrypting data in Blob Storage and in Azure Files.
* You can specify a customer-provided key on Blob Storage operations. A client making a read or

write request against Blob Storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

NEW QUESTION: 113
□□□ □ □□ □□
Microsoft □□□□ □□□ □□ Microsoft □□□ □□ □□ □□□□(MCRA)□ Zero Trust □□□ □□□ □□ □□□□□ □□□□ □□□.
□□ □□□ □□ □□ □□□□ □□□□ □□□? □□□□ □□□ □□□□ □□□ □□□□ □ □□□□□. □ □□□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.



Answer:



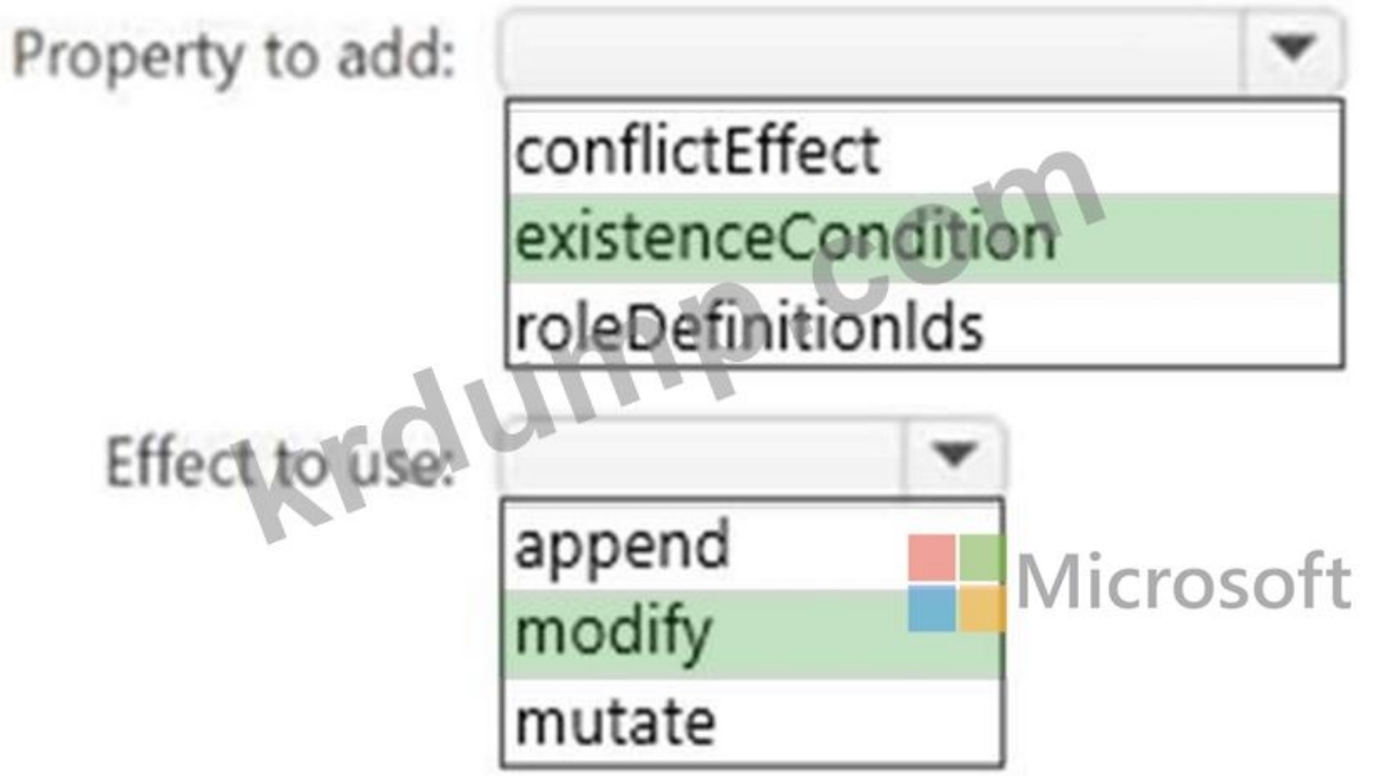
Explanation:

Zero Trust principles
Verify explicitly
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
Use least-privilege access
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.
Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.
https://www.microsoft.com/en-us/security/business/zero-trust

NEW QUESTION: 114
□□□ □□
Azure □□□ □□□□ □□□□.
□□ □ □□ □□□□ □□□ □□□□□ Azure □□□ □□□□ □□□. □□, □□ □□□ □□ □ □□□□ □□ □□□□ □□□□ □□□ □ □□□ □□ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Answer Area



Explanation:
Box 1: existenceCondition
a combination of the Azure Policy modify effect and a remediation task is the correct approach to ensure all resources in a subscription are tagged, and the existenceCondition property is a component of modify or auditIfNotExists policies, not typically for a simple modify policy that just adds a tag to the resource itself. To apply a tag to existing resources, you would assign the policy and then trigger a remediation task to update the non-compliant resources.
Box 2: modify
Azure Policy definitions modify effect
The modify effect is used to add, update, or remove properties or tags on a subscription or resource during creation or update. Existing non-compliant resources can also be remediated with a remediation task. Policy assignments with effect set as Modify require a managed identity to do remediation. A common example using modify effect is updating tags on resources such as 'costCenter'.
A modify effect policy assignment, combined with a remediation task for existing resources, is the standard and effective method to enforce tagging and ensure all resources in your subscription have the required tags.
Reference:
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-modify

NEW QUESTION: 115
Microsoft SharePoint Online☐ Microsoft Purview☐ ☐☐☐☐ Microsoft 365 ☐☐☐☐ ☐☐☐☐.

Microsoft Purview□□ SharePoint Online □□□□ □□□ □□□ □□□□ Label1□□□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□□ Microsoft Purview □□□ □□ □□(DLP) □□□ □□□□ □□□.
* □□□□ □3□ □□ □□□□□ □□□ □□□□□ □□ □□□□□.
* □□□□ Microsoft OneDrive for Business□ □□□ □□□□ □ □□□ □□□□□.
□□ □□□ DLP □□□ □□□□ □□□?
A. □□
B. OneDrive □□
C. SharePoint □□□
D. □□□□ □□ Microsoft Defender
Answer: A (LEAVE A REPLY)
To prevent users from uploading files with a specific sensitivity label (like Label1) to third-party external websites while allowing uploads to Microsoft OneDrive for Business, you would apply the Microsoft Purview Data Loss Prevention (DLP) policy to Devices. Applying the DLP policy to Devices allows control over what users do with files on their endpoints, enabling you to prevent data from being shared to untrusted locations while allowing uploads to trusted services such as OneDrive for Business.

NEW QUESTION: 116
□□□ 4□□ Azure □□□ □□ 10□□ Azure Kubernetes Service(AKS) □□□□ Docker □□□ □ □□□□ □□□□. □□□ □□ □□□□ □□□□ □□□□.
AKS □□□□ □□ □□ □□□□ □□□□□□ □□ □□ □□□□□. □□□ □□□ □□□□ □□ □□□ □□□□□□ □□□.
Microsoft Defender for Cloud□□ □□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□ □ □□□□□. □□: □ □□□ 1□□□□.
A. □□ □□□□□□ □□□□□.
B. □□ □□ □□□ □□□□□.
C. □□□ □□□□□.
D. □□□□ □□□□ □□□□□.
E. Defender □□□ □□□□□□.
Answer: (SHOW ANSWER)
Enable the defender for containers plan - then ensure it deploys to your container resources with auto provision.

NEW QUESTION: 117
□□□ □□ □□□□□ □□ □□□ Azure□ □□□ □□□□□. □□□□ □□□□□ □□ □□ □□ □□ Azure □□ □□□□ □□□ □□□□□.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

□□ □□ □□□ □□ □□□ □□ □□□□ □□□□ □□ Azure Bastion □□□ □□□□ □□ □. □□ □□□□ □□□ □□ □ □□ Azure Bastion □□□□ □□□□□?

A. 1

B. 2

C. 3

D. 4

E. 5

Answer: B (LEAVE A REPLY)

Its cause Vnet3 and Vnet4 have peering to each other. So a bastion subnet in either Vnet3 or Vnet4 is enough to access them both over the Vnet peering.

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

NEW QUESTION: 118

□□□□□□□ Azure □□ □□□ □□□□ Azure □□□ □□□□. □□ □□ □□ □□□□□ □□ □□□□ □□□□ □□□. □□ □□□ □□ □□□?

A. Microsoft Sentinel □□□ □□□□ □□□□□.

B. □□□□ □□/□□□□ □□(CI/CD) □□□ □□□□ □□□□□.

C. Microsoft Defender for Cloud□ □□ □□□ □□□ □□ Defender □□□ □□□□□□.

D. Azure Active Directory Premium Plan 2 □□□□□ □□□□.

Answer: C (LEAVE A REPLY)

https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone

NEW QUESTION: 119

□□□ □□□□ Microsoft 365 E5 □□□ □□□□.

□ □□□ Microsoft Teams, SharePoint Online, Exchange Online□□ □□□□ □□□□ □□□ □□ □□□.

□□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□.

□□ Microsoft Purview □□□ □□□ □□□□ □□□?

A. □□□ □□□

B. □□□ □□ □□(DLP)

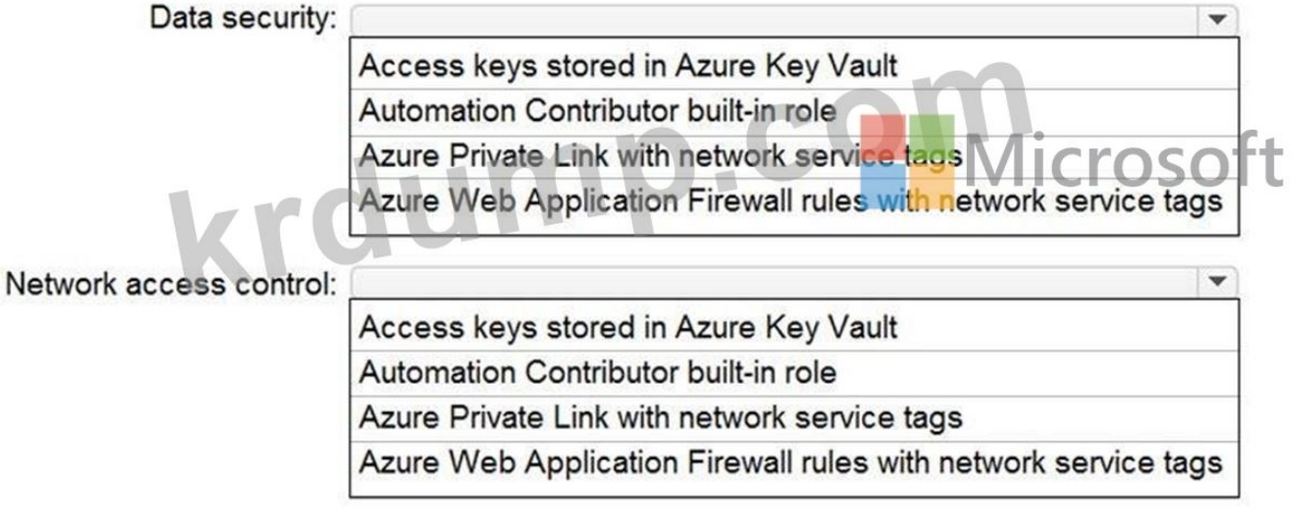
C. □□ □□ □□
D. □□□ □□ □□ □□
Answer: B (LEAVE A REPLY)
Data loss prevention (DLP)
With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.
Note: Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification with sensitivity and retention labels.
For this question the incorrect answers include:
* content explorer
Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.
* data classification content explorer
Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.
* data lifecycle management
* eDiscovery
* Information Governance
Reference:
https://docs.microsoft.com/en-us/security/compass/information-protection-and-storage-capabilities
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer

NEW QUESTION: 120
contoso.onmicrosoft.com□□□ Microsoft Entra □□□□ Sub1□□□ Azure □□□ □□□□.
□□ □□□ ID □□□ □□□□ Microsoft Entra □□□ ID□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. contoso.onmicrosoft.com□ □□ □□
B. contoso.onmicrosoft.com□ □□□ □□ □□□
C. Sub1□ □□□□ □□□ □□ ID
D. Sub1□ Azure □ □□□
Answer: (SHOW ANSWER)
Microsoft Entra Verified ID, Quick Microsoft Entra Verified ID setup
Prerequisites
* You need the Authentication Policy Administrator permission for the directory you want to configure. If you need to perform app registration tasks, you'll also need the Application Administrator permission.
* Ensure that you have a custom domain registered for the Microsoft Entra tenant. If you don't have one registered, the setup defaults to the advanced setup experience.
Reference:

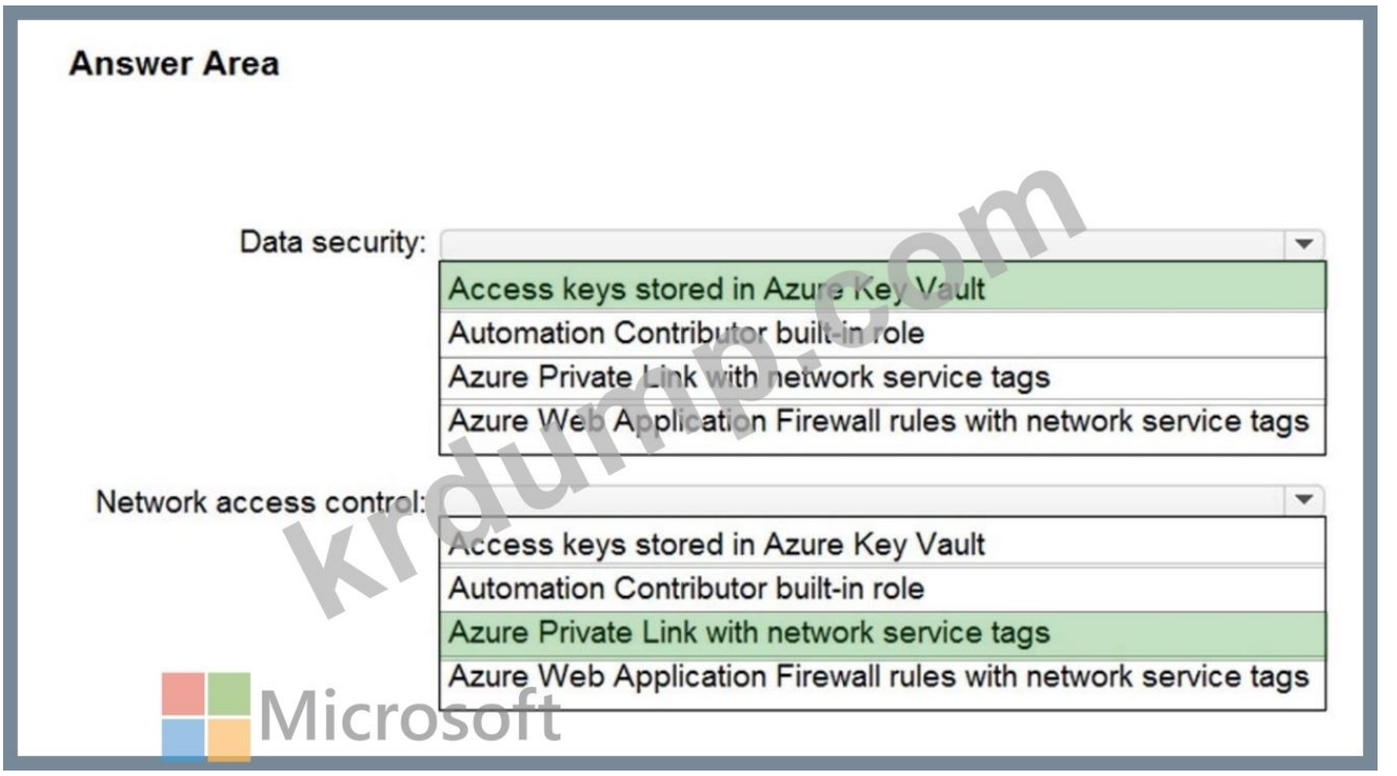
https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant-quick
https://learn.microsoft.com/en-us/entra/identity/users/domains-manage

NEW QUESTION: 121
□□□ □□
Azure Automation □□□□ □□□ □□ □□□ □□□□ □□□□. □□□ Azure Data Lake Storage Gen2□ □□□□ □□□□□.
□□ □□□□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□.
□ □□ □□□ □□ □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □□ □□□□□. □□: □□□ 1□□□□.

Answer Area



Answer:



Explanation:

Box 1: Access Keys stored in Azure Key Vault

Box 2: Azure Private Link with network service tags

https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security

NEW QUESTION: 122

□□□ □□ Windows Server□ □□□□ □□□□□ □□□ □□□□.

- Active Directory □□□ □□□(AD DS) □□□□ □ □□□ □□□□

- ASP.NET□ □□□□ Server1 □ Server2□□ □ □□ □□□□□□ □□

□ □

- RADIUS □ AD□ □□□□ □□□□ Served□□ VPN □□

□□□

□□ □□□□ VPN□ □□□□ □□□□ □□ □ □□ □□□□□□.

□ □ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□□□ □□□. □ □□□□ □□ □□□ □□□□□ Microsoft □□□ □□ □□ □□□□(MCRA)□ □□ □□□□ □□□ □□□ □ □□□.

□□□□□ □□□ □□□□ □□□?

A. □□□□ □□ Microsoft Defender□□ □□□□ □□□ □□□□□.

B. Azure AD □□□ □□□□□ VPN□ □□□□□.

C. Endpoint□ Microsoft Defender□□ □ □□□ □□□□□.
D. Azure AD □□□□□□ □□□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
Azure □□□□ □□ □□□□ □□ □□□ □□□ □□□□ □□□□.
AES□ □□□□ □□ □□ □□□□ □□□□□□ □□ □□□ □□□□ □□□.
256□□ □. □□□□ □□□ □□ □□ □□□ □ □□□ □□□.
□□□: Azure SQL □□□□□□□ □□ □□ □□ □(CMK)□ □□□□ TDE(□□ □□□ □□ □)□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
We need to use customer-managed keys.
Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.
In Azure, the default setting for TDE is that the Database Encryption Key (DEK) is protected by a built-in server certificate. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256.
TDE protector is either a service-managed certificate (service-managed transparent data encryption) or an asymmetric key stored in Azure Key Vault (customer- managed transparent data encryption).
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

NEW QUESTION: 124

□□: □ □□□□ □□□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□ □□□. □□□ □□ □ □ □□□ □□□□ □□□ □□□ □ □□□□. □□ □□□ □□ □□□ □ □□□□ □□□ □□□□ □□ □□ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□ □ □□□□.

Microsoft Defender XDR□ □□□□ Microsoft 365 □□□ □□□□. □ □□□□ Microsoft Intune □ □□□ □□□□ 500□□ □□□□ □□□□. □□, □ □□□□ □□□□□ □□□□ □□ SaaS(Software as a Service) □□ □□□□ □□□ 500□□ □□□□ □□□□.

□□ □□ □□□ □□□□ □□□□ □□□□ □□□.

* Microsoft□□ □□□□□ □□□ SaaS □□ □□ □□□ □□□□ □□□□□.

* Microsoft□□ □□□□□ □□□ SaaS □□ □□ □□□ □□□□ □□□□□.

□□□: □□□□ □□ Microsoft Defender□□ SaaS □□ □□□ □□(SSPM)□ □□□□ □□□ □□□ □□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

To allow access to only low-risk external SaaS apps in a Microsoft 365 environment with Defender XDR and Intune, you can use Microsoft Entra Conditional Access policies. These policies can leverage Learn Microsoft's Defender for Endpoint data to restrict access based on device compliance and threat level. Specifically, you can create policies that require a device to be compliant or have an app protection policy applied before allowing access to specific SaaS apps.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/posture-overview

https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

NEW QUESTION: 125

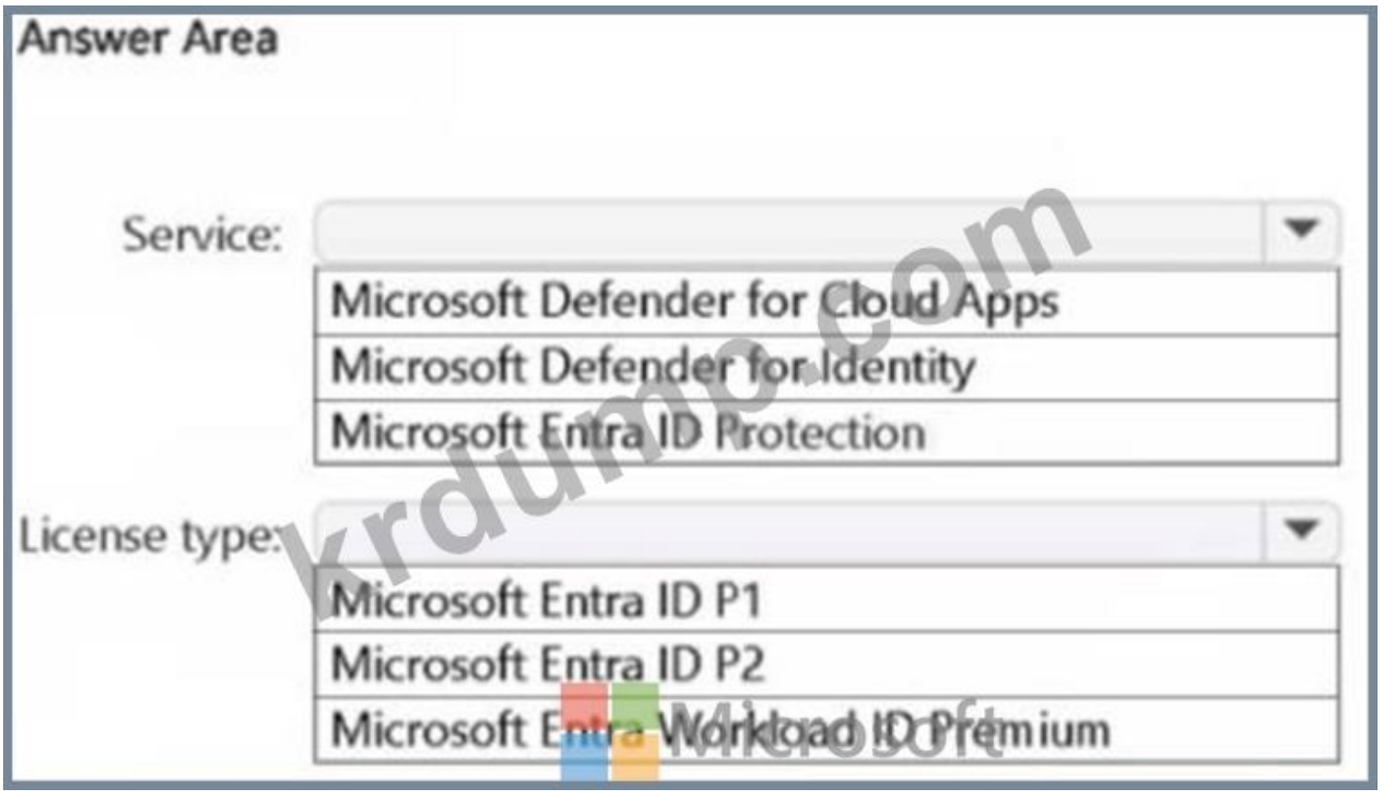
□□□ □□

Microsoft 365 □□□ Azure □□□ □□□ Microsoft Entra □□□□ □□□□. □ □□□□□ Azure □□□ □□□□□□□ □□□□□ □ □□□□ □□□ □□□ □□□□ □□□□.

□□□ □ □□□ □□□ □□□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□ □□ □□ □□□. □□□□ □□□ □□□□□ □□□.

□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Box 1: Microsoft Entra ID Protection

Service

Microsoft Entra ID Protection, Investigate risk

Microsoft Entra ID Protection provides organizations with reporting they can use to investigate identity risks in their environment. These reports includerisky users,risky sign-ins,risky workload identities, andrisk detections.

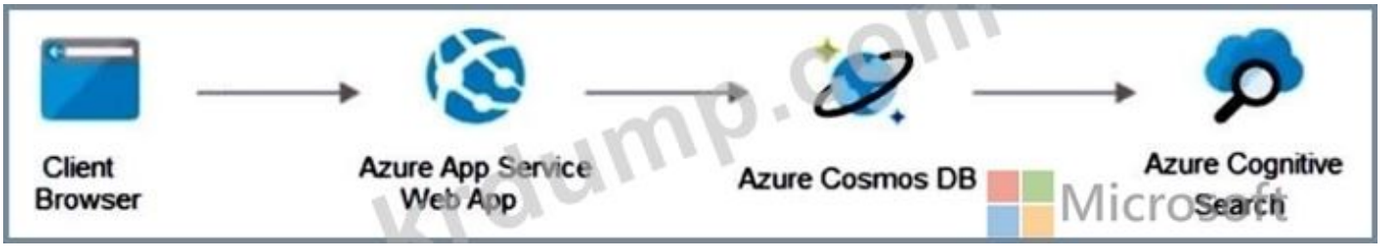
Box 2: Microsoft Entra ID P2
License type
Microsoft Entra ID and Microsoft Entra Suite

Reference:
https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk
https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing

NEW QUESTION: 126
□□□□ □□ □□□□□, Azure App Service(web-App0□□□ □□)□ □□ □□ □□□□ □□ □□ □□□ □□□□□. Web-App0□□ □□□ □□ □□ □□□ □□□□.
□□□□ □□ □□□ □□ web-App0□ □□ □□□□ □□□□ □□ □□ □□□□ □□□□□.
□□□ □□□ Azure AD□□ □□□□□ □□□.
web-app0□ □□ AD □□□ □□□□□ □□ □□□□ □□ □□□ □□□□□?
A. Azure AD □□□□□□
B. Azure AD □□□□□□ □□□
C. Microsoft Defender for 365
D. □□□□□□ □□□□□
Answer: (SHOW ANSWER)
Option A is correct because you can use application management in Azure AD, which is a process of creating and configuring applications in the cloud; when an application is registered in a Azure AD tenant, you can assign users to access the application securely.
Option B is incorrect because Azure AD Application Proxy provides secure remote access to on-premises web applications; this is not part of the objective.
Option C is incorrect because Microsoft Defender for Office 365 protects your organization against malicious risks posed by email messages, links (URLs), and collaboration tools; the objective of your task is to provide access using Azure AD.
Option D is incorrect because Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications, the function of this solution is not required.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management

NEW QUESTION: 127
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□

□□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
□Ł□□□□ □□□□□ Angular □ Node.js□ □□□ □□□□□ □□□ □□□□. □ □□□ MongoDB □□□□□□□ □□□□□. □ □□□ Azure□ □□□□□□□ □□□□□.
□□□ □□□□ □□ Azure □□ □□□ □□□ □□ □□□□□ □□□□□.



□ □□ □□□□□□ □ □□□ □□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□ □□□ □□□ □□□.
□□ □□: □□ □□□ □□□□ □□ Azure Key Vault□ □□□□ □□ □□□□.
□□□ □□□ □□□□□?

A. □
B. □□□

Answer: B (LEAVE A REPLY)

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

NEW QUESTION: 128

Microsoft 365 □□□ Azure □□□ □□□□. Microsoft 365 Defender□ Microsoft Defender for Cloud□ □□□□□ □□□□.
Azure □□□□ 50□□ □□ □□□ □□□□ □□□□. □ □□ □□□ Windows Server 2019□ □ □□ □□ □□□□□□□ □□□□□.
□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□ □□, □□□□ □□ □□□□□□□ □□□ □ □□ □□□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?

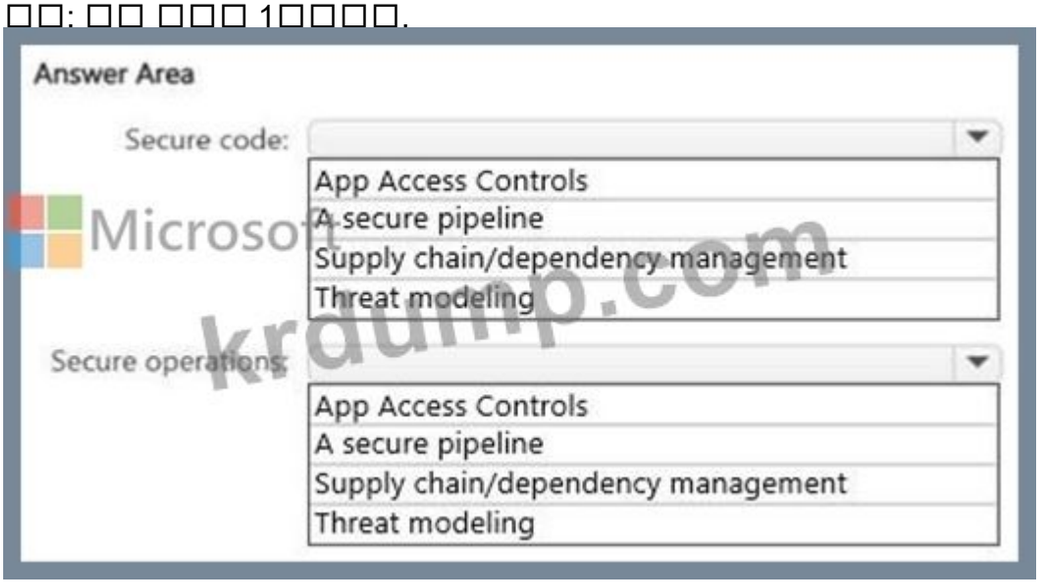
A. Azure AD□ □ □□
B. Azure AD □□□ □□□ □ □□ □□
C. Defender for Cloud□ □□□ □□□□□□ □□
D. □□□□ □□ Microsoft Defender□ □ □□ □□ □□ □□

Answer: C (LEAVE A REPLY)

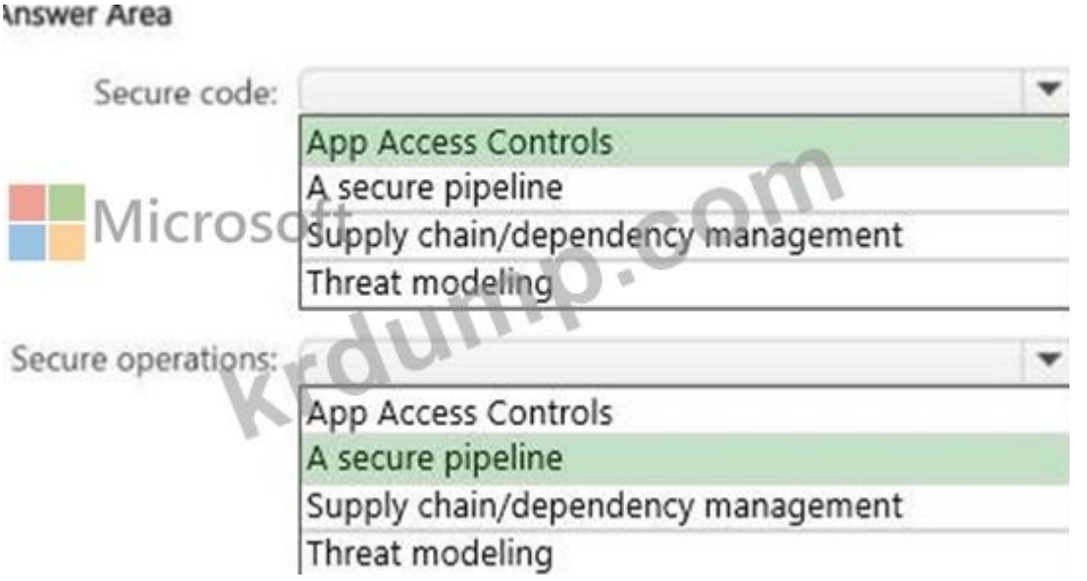
NEW QUESTION: 129

□□□ □□
□□ Azure □□□ □□ □□ □□ □ □□□ □□□□ □ □□□□ Azure DevOps □□□ □□□

□.
□□□ DevSecOps □□□ □□□□ □□□□.
□□ □□ □□□ □□ □□ □□ □□□ DevSecOps □□□ □□□□ □□□. □□□□ Microsoft Azure □□□□ □□ □□□□□ □□□ □□□□ □□ □□□.
□ □□□□ □□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



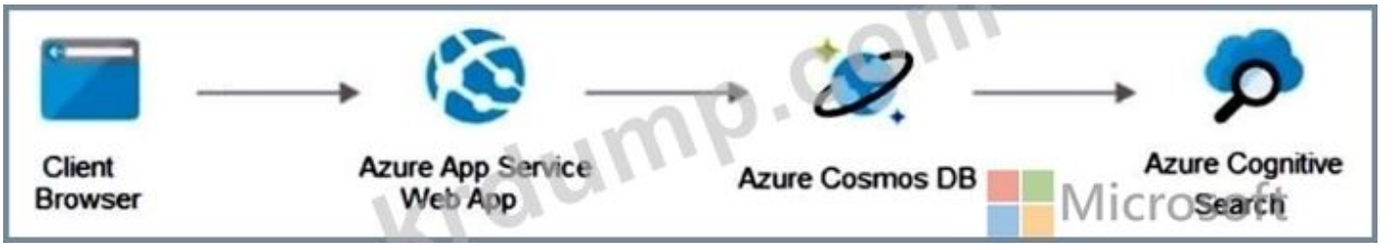
Answer:



Explanation:
Box 1: App access controls
Integrating application access controls into the code itself during the secure code stage of DevSecOps is a recommended practice to prevent unauthorized access to features and sensitive data within an application. Developers should define roles, assign permissions based on those roles, enforce strong password policies, and regularly test these controls to ensure they are effective at protecting the application's integrity and data throughout the software development life cycle.
Note: In DevSecOps, the Secure Code Stage involves integrating security practices and automated tools into the coding process to prevent vulnerabilities from entering the codebase.

Key activities include implementing secure coding standards, performing static code analysis (SAST) to find flaws, using software composition analysis (SCA) for dependencies, and performing secret scanning to catch hardcoded credentials. This stage aims to catch security issues early in the development lifecycle, reducing costs and risks.
Box 2: A secure pipeline
Using a secure pipeline is a core recommendation in the Secure Operations stage of DevSecOps, as it integrates automated security checks throughout the entire software development lifecycle (SDLC). This automated approach allows for early detection and remediation of vulnerabilities, fosters collaboration between development, operations, and security teams, and helps ensure that secure, high-quality software is delivered faster and more reliably.
Reference:
https://learn.microsoft.com/en-us/azure/devops/organizations/security/about-permissions
https://www.wiz.io/academy/devsecops-pipeline-best-practices

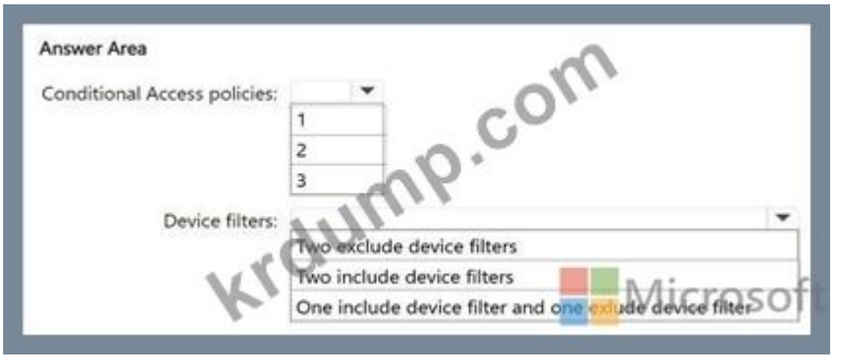
NEW QUESTION: 130
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□ □ □□□□ □□□□.
□+□□□□ □□□□□ Angular □ Node.js□ □□□ □□□□□ □□□ □□□□. □ □□□ MongoDB □□□□□□□ □□□□□. □ □□□ Azure□ □□□□□□□ □□□□□.
□□□ □□□□ □□ Azure □□ □□□ □□□ □□ □□□□□ □□□□□.



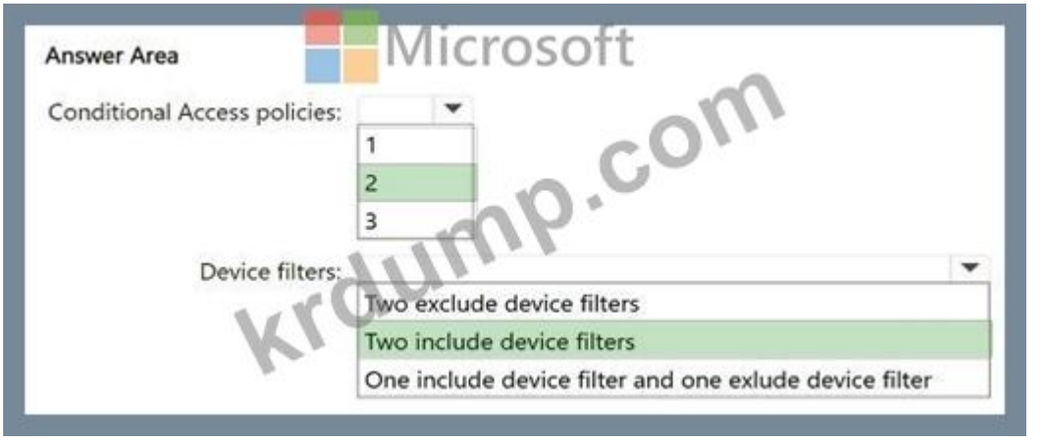
□ □□ □□□□□□ □ □□□ □□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□ □□□ □□□ □□□.
□□ □□: Azure Web Application Firewall(WAF)□ □□ Azure Application Gateway□ □□□□ □□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

NEW QUESTION: 131

□□□ □□
Microsoft Entra □□□□ □□□□. □ □□□□□ Group1□□□ □□ □□□ □□□□ □□□□.
Group1□□ □□ IT □□□ □□□□ □□□□□.
Azure □□□ □□□□. □ □□□□ Microsoft Entra□ □□□ Windows □□ 800□□ Microsoft Entra□ □□□ Windows □□ 200□□ □□□□ □□□□.
□□□ macOS □□□ 200□ □□□□.
Microsoft Entra□ □□□□ □□ Microsoft Entra ExtensionAttribute1 □□ SecureWorkstation□□ □□□ 10□□ Windows □□□ □□□□□.
□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□.
- Windows 10 □□ Windows 11□ □□□□ □□□□□ Microsoft Entra □□□□ □□ □□□□ □□□□□.
- Windows Azure □□□ □□ API □□□□ □□□□□.
□□ □□□:
- □□1□ □□□
- □□ □□(MFA)□ □□□□ □□□□ □□□
- SecureWorkstation□ □□ □□□□ □□□□ □□□
□□ □□1
□□□□ □□□ □□□ □□ □□□□□ □□□ □□□□□ □□□.
□□□□□ □□□ □□□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



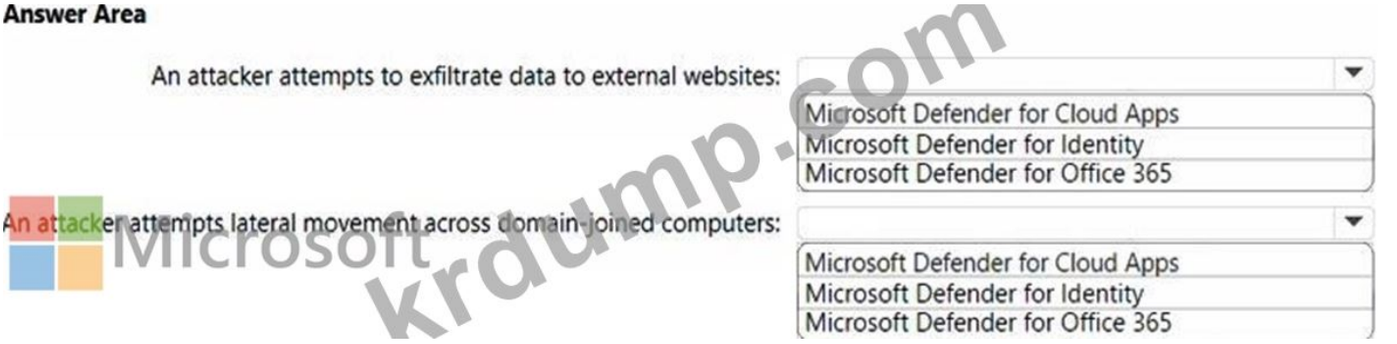
Explanation:
Box 1: 2
* Only allows access to Microsoft Entra resources from devices that run Windows 10 or Windows 11

Create one Conditional Access policy that uses one include device filter which includes only Windows 10 and Windows 11.
* Restricts Windows Azure Service Management API access to the following users:
The members of Group1
Users that authenticate by using multifactor authentication (MFA)
Users that connect from a device that has the SecureWorkstation ExtensionAttribute1 Create a second Conditional Access policy that includes Group1, requires MFA, and one include device for devices that has the SecureWorkstation ExtensionAttribute1. Grant access to Windows Azure Service Management API.
Box 2: Two include device filters
Reference:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-condition-filters-for-devices

NEW QUESTION: 132
□□□□□ □□ □□□□□ □□□□□ Azure□ Microsoft 365□ □□□□ □□□□. □□ □□ □□□ □□□□ Microsoft Sentinel□□ □□ □□□□□□□□, □□□ □ □□(SOAR) □□□ □□ □□ □□□.
- □□ □□ □□□□ □□ □□□ □□□□□□.
- Microsoft Teams □□ □□□ Waging □□ □□
□□□ □□□ □□□□ □□□?
A. □□□ □□□
B. □□□□
C. □□□
D. KQL
Answer: (SHOW ANSWER)
Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.
A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

NEW QUESTION: 133
□□□ □□
Microsoft □□□□ □□□ □□ Microsoft □□□ □□ □□ □□□□(MCRA)□ □□□□ □□ □ □□□□ □□□□ □□□□.

□□□ □□ □□ □□ □□ □□□□□□ □□□□ □□□.
- □□□□ □□ □□□□□ □□□□ □□□□□ □□□□□.
- □□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□.
□ □□□ □□ □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:
Employees may be using an unapproved cloud application for storing sensitive corporate data or downloading a vast number of sensitive files for exfiltration. These actions can be prevented by Microsoft Defender for Cloud Apps.
https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls

NEW QUESTION: 134
□□□ Azure Storage □□□ □□□□ Blob Storage□ □□□□□□ □□□□□. Blob Storage□ □□□□ 20□ □□□□□□ □□□□□ □□□□ □ □□□□. □□□□□□ □□□ Storage □ □□ □□□□ □ □□□ □□ □□□□ □□□□ □□□. Blob Storage□ □□□□ □□ □□□ □□□□ □□ □□□□?
A. □□□□ □□ □□(NSG)□ □□□ □□
B. Azure □ □□□□□□ □□□(WAF) □□□ □□□□ □□ □□
C. □□□□ □□ □□(NSG)□ □□□□ □□
D. □□□□ □□□ □□ □□□ □□
E. Azure Firewall□ □□□□ □□
Answer: (SHOW ANSWER)
Configure Azure Storage firewalls and virtual networks.
To secure your storage account, you should first configure a rule to deny access to traffic from all

networks (including internet traffic) on the public endpoint, by default. Then, you should configure rules that grant access to traffic from specific VNets. You can also configure rules to grant access to traffic from selected public internet IP address ranges, enabling connections from specific internet or on-premises clients. This configuration enables you to build a secure network boundary for your applications.

Storage firewall rules apply to the public endpoint of a storage account. You don't need any firewall access rules to allow traffic for private endpoints of a storage account. The process of approving the creation of a private endpoint grants implicit access to traffic from the subnet that hosts the private endpoint.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

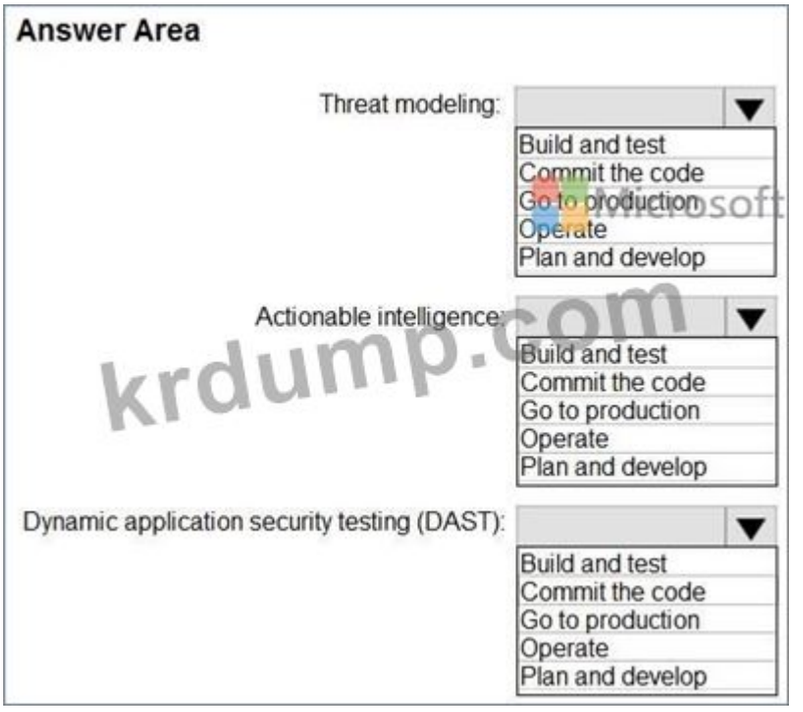
NEW QUESTION: 135

□□□ □□

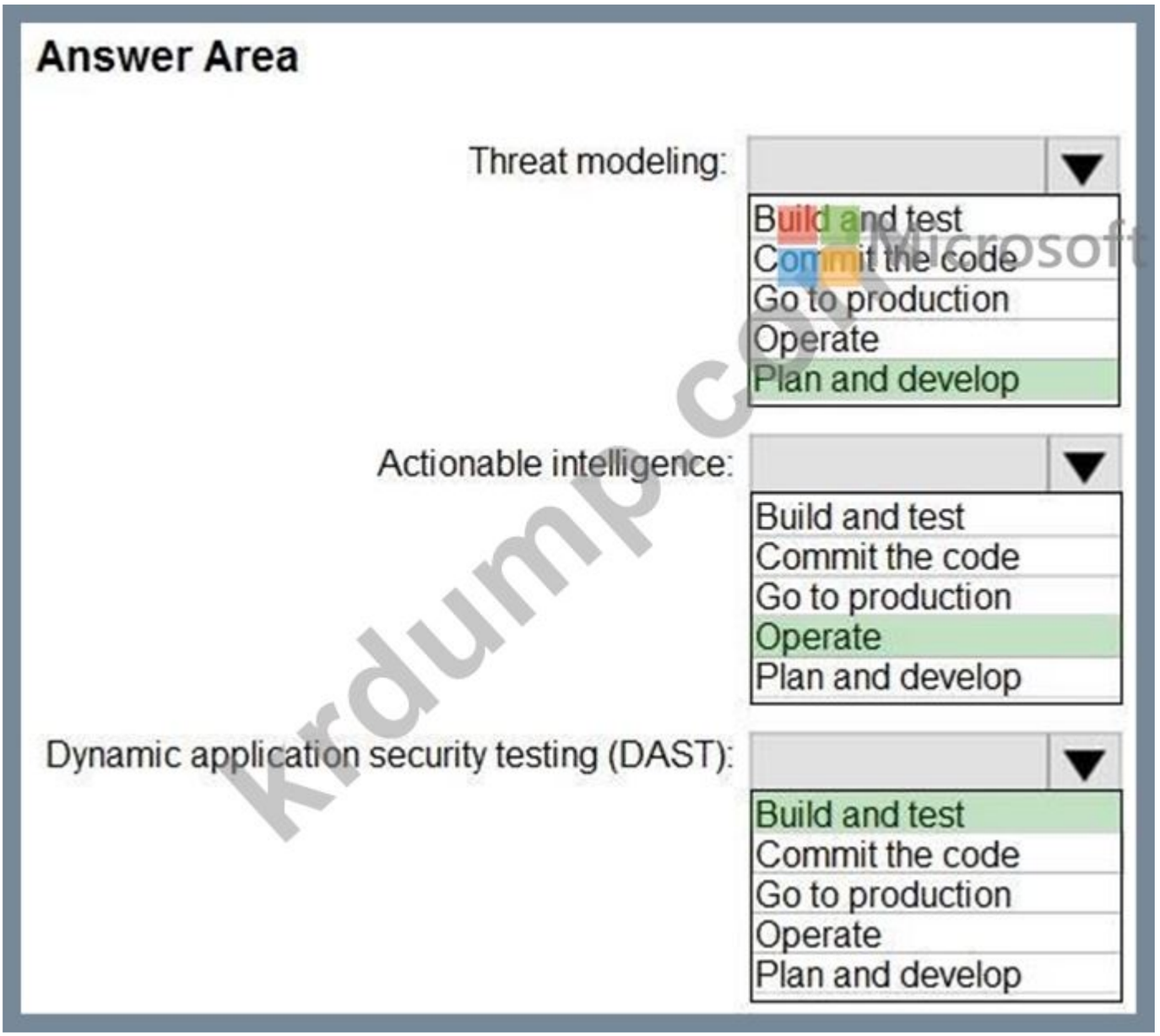
Azure□ Microsoft □□□□ □□ □□□□□□ □□□□ DevOps □□ □□□□□ □□ □□ □ □□□ □□□□ □□□.

□ □□ □□ □□□ CI/CD(□□□ □□ □ □□□ □□) DevOps □□□□□ □□ □□□□ □□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

NEW QUESTION: 136

□□□ □□

Azure App Service □□ 3□□ □□□ Azure □□□ □□□□.

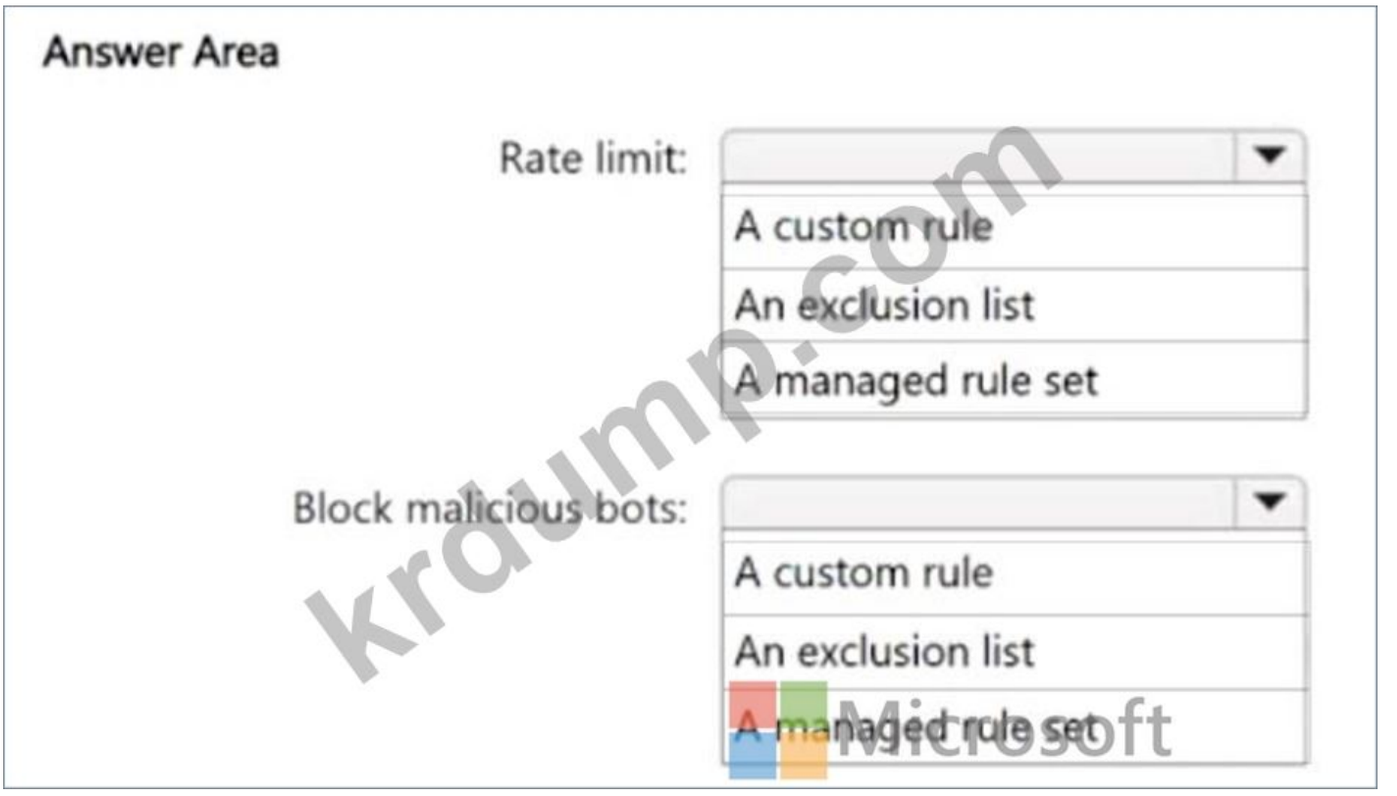
Azure Front Door□□ Azure WAF(□ □□□□□□ □□□)□ □□□□ □□ □□□□ □□□. □ □□□ □□ □□ □□□ □□□□ □□□.

- □□ □□ □□ □□□□□□ □□□ □□□□□.
- □□□ □□□□ □□ □□ □□.

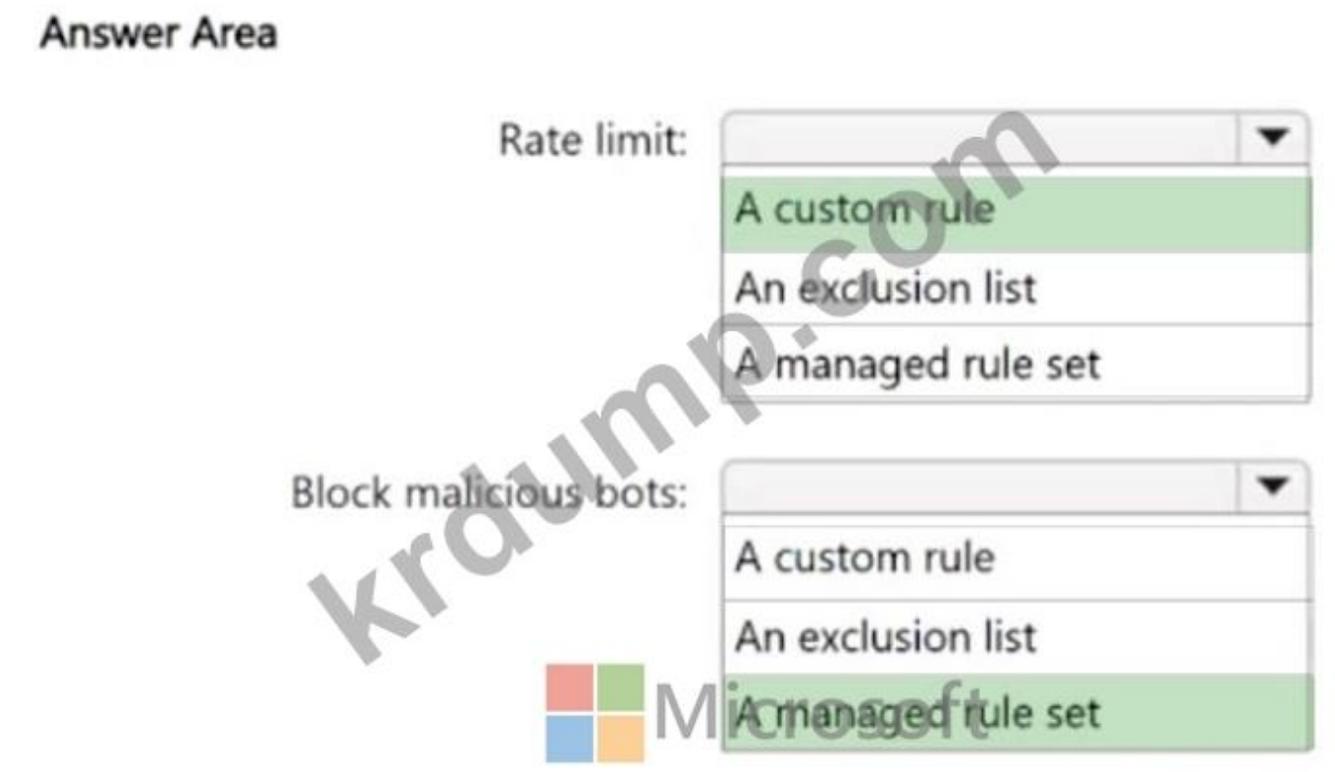
□□□□ □□□ □□□ □□□□□ □□□.

□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: A custom rule

To rate limit incoming connections to Azure App Services using Azure Web Application Firewall (WAF) with Azure Front Door, you need to configure a custom WAF rule within your Front Door WAF policy. This rule will specify a rate limit threshold and a match condition that determines when the rate limiting should be applied.

Box 2: A managed rule set

Block attempts to access the apps from malicious bots.
To block malicious bots with Azure Web Application Firewall (WAF) on Azure Front Door and Azure App Service, you can enable bot protection rules within the WAF policy. Specifically, you'll want to enable the Bot Manager rule set, which helps identify and manage bot traffic, distinguishing between good bots and malicious ones.
Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

NEW QUESTION: 137
□□ □□ 1 - Fabrikam, Inc
□□
Fabrikam, Inc.□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□□□.
□□ □□
□□□□□ □□
□□□□□ □□□□□□ corp.fabrikam.com□□□ □□ Active Directory □□□ □□□(AD DS) □□□□ □□□□ □□□□.
Azure □□
Fabrikam□ □□□ □□ Azure □□□□ □□□□ □□□□.
- corp.fabrikam.com□ □□□□□ fabrikam.onmicrosoft.com□□□ Microsoft Entra □□□
- Sub1□□□ □□ Azure □□
- □□ □□ Azure □□□ Vnet1□□□ □□ □□□□
- □□□ Azure □□□ Vnet2□□ □□ □□□□
- Azure WAF(□ □□□□□□ □□□)□ □□□□ FD1□□□ Azure Front Door □□□□
- Microsoft Sentinel □□ □□
- ClaimDetails□□ □□□□ □□□ ClaimsDB□□ Azure SQL □□□□□□
- □□□□□□ □□□ □□□□ Microsoft Defender for Cloud□ □□□□□ □□ 20□□ □□ □□
- □□□ □□□□□ □□□□ TestRG□□ □□□ □□
- □□□ □□□ □□ □□□□ □□□□ Azure Virtual Desktop □□□ □
- Sub1□ □□ □□□□ □□ □□ □□ □□ □□ □□□ □□□□.
□□□
Fabrikam□ Contoso, Ltd.□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□□. Contoso

□ □□□ □□ □□□□ □□□□ □□□□.
- contoso.onmicrosoft.com□□□ Microsoft Entra
- ContosoAWS1□□□ Amazon Web Services(AWS) □□□□ Fabrikam □□□□□□□ □□□ □□□□□ □□□□□ □ □□□□ AWS EC2 □□□□□ □□□□ □□□□. Contoso□ □□□ □ Fabrikam□ □□□□ □□□□ □□□□□□□ □□□□□□ □□□□□□□.
□□□□ fabrikam.onmicrosoft.com□ Contoso Developers□□ □□ □□□ □□□□, □ □□□ Sub1□ □□□ □□□□□. ContosoDevelopers □□□□ ClaimsDB □□□□□□□ db.owner □ □□ □□□□□.

□□ □□ □□□

Fabrikam□ □□□ □□ □□ □□ □□□ □□□□□.
- Defender for Cloud□ Sub1□ □□ □□□□ HIPAA HITRUST □□□ □□□□□ □□□□□ □ □□□ □□□□.
- □□ HIPAA HITRUST □□□ □□□□ □□ □□□□ □□□□ □□□□ □□□□.
- Qualys□ □□□ □□ □□□ □□ □□□ □□□□□.

□□ □□

Defender for Cloud□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□□. □□ □□ □□□ □□ □□□□ □□□ □□□. □□ □□ □□□ Defender for Cloud□ □□□□ □□ □.

ClaimApp □□

Fabrikam□ □□ □□□ □□ ClaimsApp□□□ □□□ □□ □□ □□□□□□□ □□□ □□□ □□.
- ClaimsApp□ Vnet1 □ Vnet2□ □□□□ Azure App Service □□□□□ □□□□□.
- □□□□ https://claims.fabrikam.com□ URL□ □□□□ ClaimsApp□ □□□□□.
- ClaimsApp□ ClaimsDB□ □□□□ □□□□□.
- ClaimsDB□ Azure □□ □□□□□□□ □□□□ □ □□□ □□□.
- ClaimsApp□ □□ □ □□□ □□□ ClaimsDB□ □□□□□ □□□.

□□□□□□ □□ □□ □□

Fabrikam□ □□□□□□ □□□ □□ □□□ □□ □□ □□□ □□□□□□.
- Azure DevTest □□ □□□□ □□□□ □□ □□□□□.
- □□ □□□□□□ □□□ GitHub Enterprise□ □□□□□ □□□.
- Azure Pipelines□ □□□□□□ □□□ □□□□ □ □□□□□.
- □□ □□□□□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□□. □□□□ □□□ □ □□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□□□. □□□ □□□ □□□□ □ □□ □ □□□□ □□□.

□□ □□ □□

Fabrikam□ □□□ □□ □□ □□ □□□ □□□□□.
- □□□ □□□ □□□ □□□□□□□ □□□□ □□□ □□□ □□□□ □□□.
- InfraSec□□□ □□□ □□□ □□□□ □□ □□(NSG)□ Azure Firewall, VJM, Sub1□ Front Door □□□□□ □□□ □ □□□ □□□.
- □□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□. □□ □□□□ □□□ □□ □□ □□ □□□□□ □□□□□□□□□ □□□.

AWS □□ □□
Fabrikam□ ContosoAWSV□ □□□□ □□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.
- AWS EC2 □□□□□ □□ □□ □□ □□□ □□□□ □□ □□ Fabrikam□ □□ □□□□□ □□□□.
- □□ □□□□ Azure □□□□ □□ AWS □□□ □□□ □□□ □ □□□ □□□□□.
Contoso □□□ □□ □□
Fabrikam□ Contoso □□□□ □□ □□□ □□ □□ □□□ □□□□□□.
- □□ ContosoDevelopers □□□ □□□□ □□□□ □□□.
- Contoso □□□□ Sub1□ □□□□ □□□□□□ □□ contoso.onmicrosoft.com □□ □□□ □□□□ □□□.
- □□□ □□□□ ClaimDetails □□□□ MedicalHistory□□ □□ □□ □□□□ □ □ □□□ □ □□.
□□ □□ □□
Fabrikam□ Sub1□ □□ □□□ HIPPA HITRUST □□□ □□□□□ □□□□ □□□□□ □□ □. TestRG□ □□ □□□ □□ □□ □□□□ □□□□ □□□.
InfraSec □□□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□.
□□ □□□ □□□□□ □□□ □□□□ □□□?
A. □□
B. □□□ □□ □□ □□ □□□ □□(RBAC) □□
C. □□□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
Scenario: Requirements. Security Requirements include:
Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.
If the Azure built-in roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group (in preview only), subscription, and resource group scopes.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

NEW QUESTION: 138
□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□ □□□ Microsoft Teams, SharePoint Online □ Exchange Online□□ □□□□ □□□□ □□ □□□ □□□.
□□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. □□□ □□ □□□ □□□
B. □□□ □□ □□(DLP)
C. □□ □□ □□

D. □□ □□□□

Answer: A (LEAVE A REPLY)

Content explorer. This tab provides visibility into the amount and types of sensitive data in an organization. It also enables users to filter by label or sensitivity type. Doing so displays a detailed view of locations where the sensitive data is stored. It provides admins with the ability to:

- index the sensitive documents that are stored within supported Microsoft 365 workloads.
- identify the sensitive information they're storing.

https://docs.microsoft.com/en-us/learn/modules/implement-data-classification-of-sensitive-information/6-view-sensitive-data-content-explorer-activity-explorer

NEW QUESTION: 139

□□□ Zero Trust □□□□□□ □□□□ □□ □□ □□□ □□□□ □□□□.

Tier 1 Microsoft Security Operations Center(SOC) □□□□ □□ □□□ □□□□□ □□□.

□□□ □□ □□□?

A. Azure Policy□□ □□ □□ □□ □□ □□□ □□□□□ □□□□□.

B. Microsoft 365 Defender□□ □□ □□ □□□ □□□□□□.

C. □□□ □□□ □□□□□□.

D. Microsoft 365 Defender□□ □□ □□□ □□□□.

Answer: B (LEAVE A REPLY)

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527

NEW QUESTION: 140

Azure □□□ □□□□. □ □□□□ Windows Server□ □□□□ □□ □□ 100□□ □□□□ □ □□□. □□ □□□ Azure Policy□ Microsoft Defender for Servers□ □□□□ □□□□□.

□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

- □□ □□□ □□ □□ □□□□□ □□□.
- □□□□□ □□ □□□ □□□ □ □□ □□□□□ □□□□□.
- □□ □□□□□ □□ □□□□ □□ □□ □□□□ □□ □□□ □□□□□.
- □□ □□□□ □□ □□□□ □□ □□□□□ □□□□□.

□□ □□□□ □□ □□□□.

□□□□ □□□ □□□□ □□□?

A. Azure Policy□ □□□ □□

B. □□□□ □□ Microsoft Defender□ □ □□□□

C. Microsoft Entra ID□ □□□□□□ □□□□□□□ □□ □□□ □□ □□

D. Defender for Servers□ □□□ □□□□□□ □□

Answer: D (LEAVE A REPLY)

Microsoft Defenders for Cloud's adaptive application controls enhance your security with this data-driven, intelligent automated solution that defines allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes.

Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations.
Note: Defender for Cloud needs at least two weeks of data to define the unique recommendations per group of machines. Machines that have recently been created, or which belong to subscriptions that were only recently protected by Microsoft Defender for Servers, will appear under the No recommendation tab.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-adaptive-application-controls

NEW QUESTION: 141
Active Directory □□□ □□□(AD DS) □□□□ □□□□□ Microsoft Entra □□□□ □□□□.
100□□ □□□ □□ □□□□□ □□□ □□□ □□□□. □ □□□□ Windows Server□ □□□ □ Microsoft Azure Backup Server(MABS)□ □□□□ □□□□□.
□□□□ □□□ □□ □□ □□□□ □□□□ □□□□. □ □□□□ Microsoft □□ □□ □□□ □□□□□.
□□□ □□ □□□ □□□ □□□□ □□□ □□□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. Azure Backup□□ Resource Guard□ □□□□ □□ □□□ □□ □□□ □□□□□.
B. Microsoft Entra Privileged Identity Management(PIM)□□ □□ □□□ □□□ □□ □□ □□ □ □□□□.
C. Microsoft Azure Backup □□□□ MABS□ Recovery Services □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□□ □□□ □□□ □□ □□ PIN□ □□□□□.
Answer: A (LEAVE A REPLY)
MUA for Azure Backup uses a new resource called the Resource Guard to ensure critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, are performed only with applicable authorization.
Reference:
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq