Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-withaccess-reviews
Azure Active Directory (Azure AD) 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. Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.
Why are access reviews important?
"Azure AD enables you to collaborate with users from inside your organization and with external users. Users can join groups, invite guests, connect to cloud apps, and work remotely from their work or personal devices. The convenience of using self-service has led to a need for better access management capabilities."

QUESTION 36
You have an Azure subscription. The subscription has a blob container that contains multiple blobs. Ten users in the finance department of your company plan to access the blobs during the month of April. You need to recommend a solution to enable access to the blobs during the month of April only. Which security solution should you include in the recommendation?

A. shared access signatures (SAS)
B. access keys
C. conditional access policies
D. certificates

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview
This allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.

QUESTION 37
You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain.
You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication.
Some users work remotely and do NOT have VPN access to the on-premises network.
You need to provide the remote users with single sign-on (SSO) access to WebApp1.
Which two features should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure AD Application Proxy
B. Azure AD Privileged Identity Management (PIM)
C. Conditional Access policies
D. Azure Arc
E. Azure AD enterprise applications
F. Azure Application Gateway

Answer: AC

Explanation:
A: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. You can configure single sign-on to an Application Proxy application.
C: Microsoft recommends using Application Proxy with pre-authentication and Conditional Access policies for remote access from the internet. An approach to provide Conditional Access for intranet use is to modernize applications so they can directly authenticate with AAD.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-config-ssohow-to
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deploymentplan

---

QUESTION 38
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group'. Group i is configured Tor assigned membership. Group I has 50 members. including 20 guest users.

You need To recommend a solution for evaluating the member ship of Group1. The solution must meet the following requirements:
The evaluation must be repeated automatically every three months
Every member must be able to report whether they need to be in Group1
Users who report that they do not need to be in Group 1 must be removed from Group1 automatically
Users who do not report whether they need to be m Group1 must be removed from Group1 automatically.
What should you include in me recommendation?

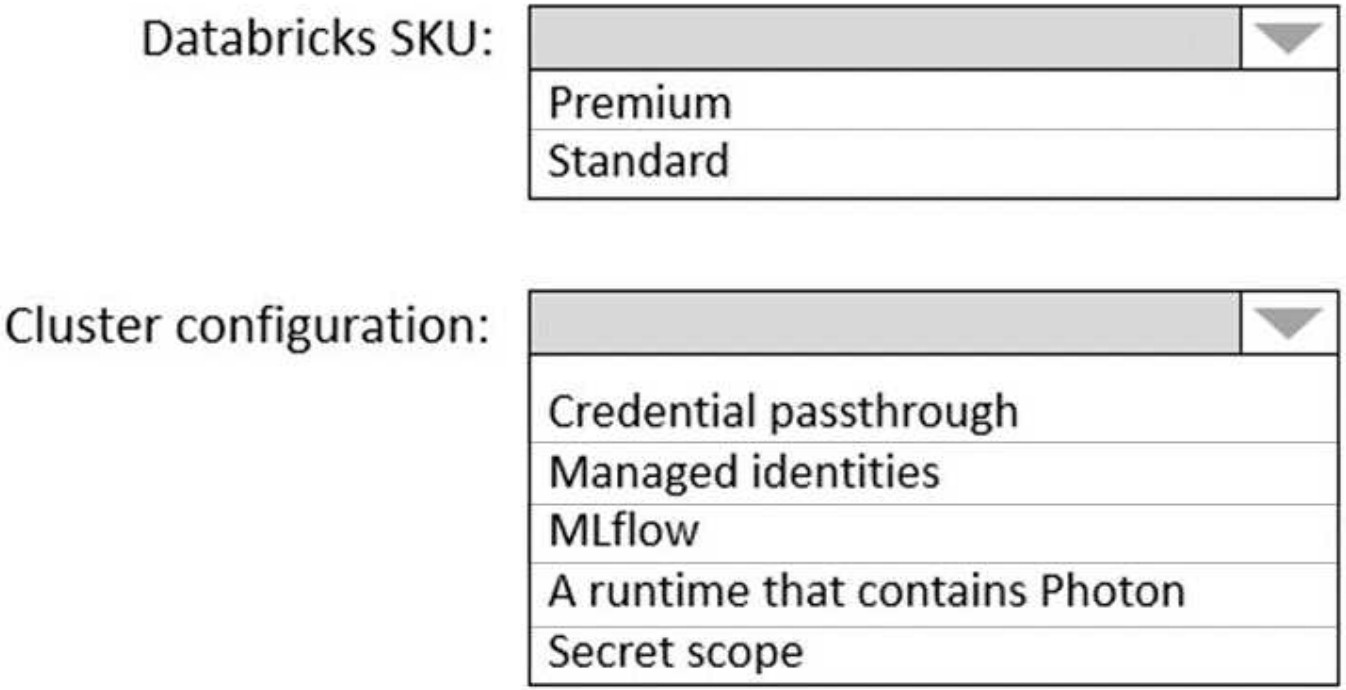
A. implement Azure AU Identity Protection.
B. Change the Membership type of Group1 to Dynamic User.
C. Implement Azure AD Privileged Identity Management.
D. Create an access review.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviewsoverview#learn-about-access-reviews
Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.
An administrator creates an access review of Group C with 50 member users and 25 guest users. Makes it a self-review. 50 licenses for each user as self-reviewers.* https://docs.microsoft.com/enus/azure/active-directory/governance/access-reviews-overview#example-license-scenarios
There are 4 requirements and every single one is only met by access reviews.
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviewsoverview#when-should-you-use-access-reviews
Dynamic User is needed if a user must be automatically granted access on base of its attributes (department, jobtitle, location, etc.) https://techcommunity.microsoft.com/t5/itops-talkblog/dynamic-groups-in-azure-ad-and-microsoft-365/ba-p7494
Implementing Azure AD PIM is no solution and absolutely not necessary for access reviews.
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviewsoverview#where-do-you-create-reviews

---

QUESTION 39
HOTSPOT
You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.
You need to recommend a design for the planned Databrick deployment. The solution must meet the following requirements:
Ensure that the data engineers can only access folders to which they have permissions.
Minimize development effort.
Minimize costs.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



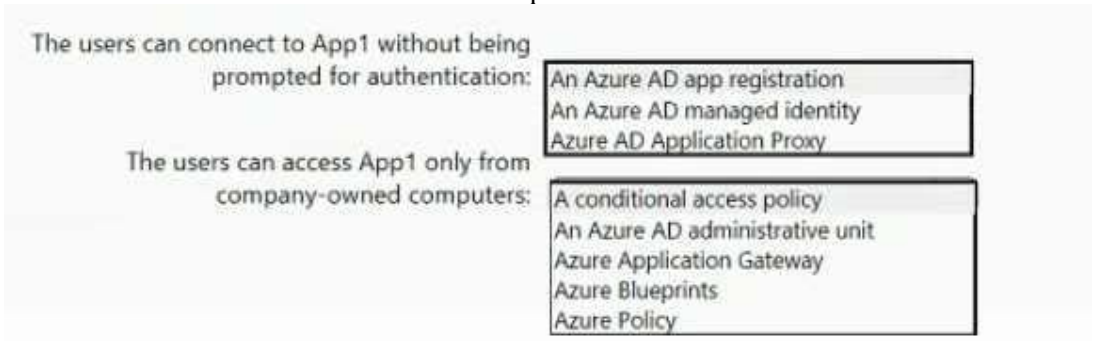
Answer:

Explanation:
Box 1: Standard

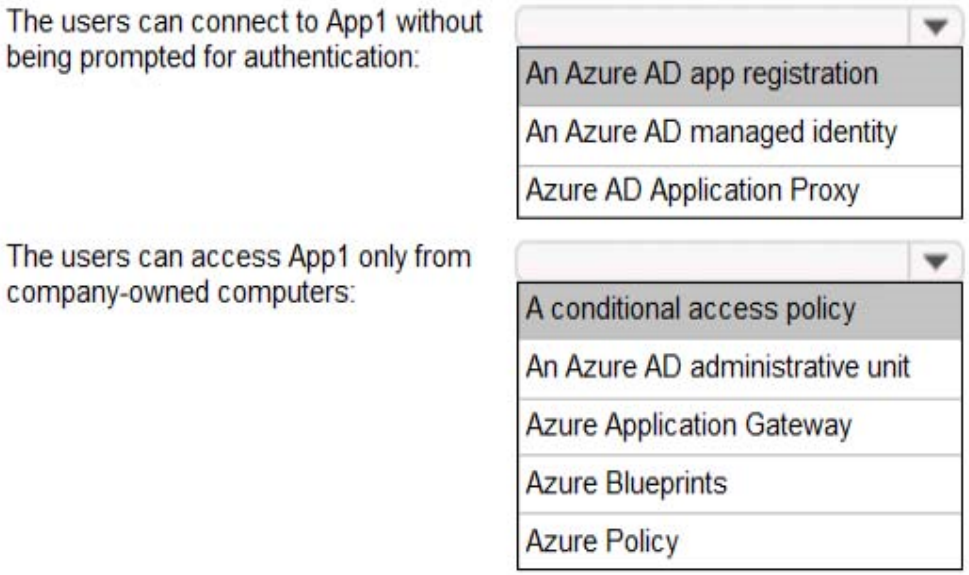
Choose Standard to minimize costs.
Box 2: Credential passthrough
Athenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.
Reference:
https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adlspassthrough

---

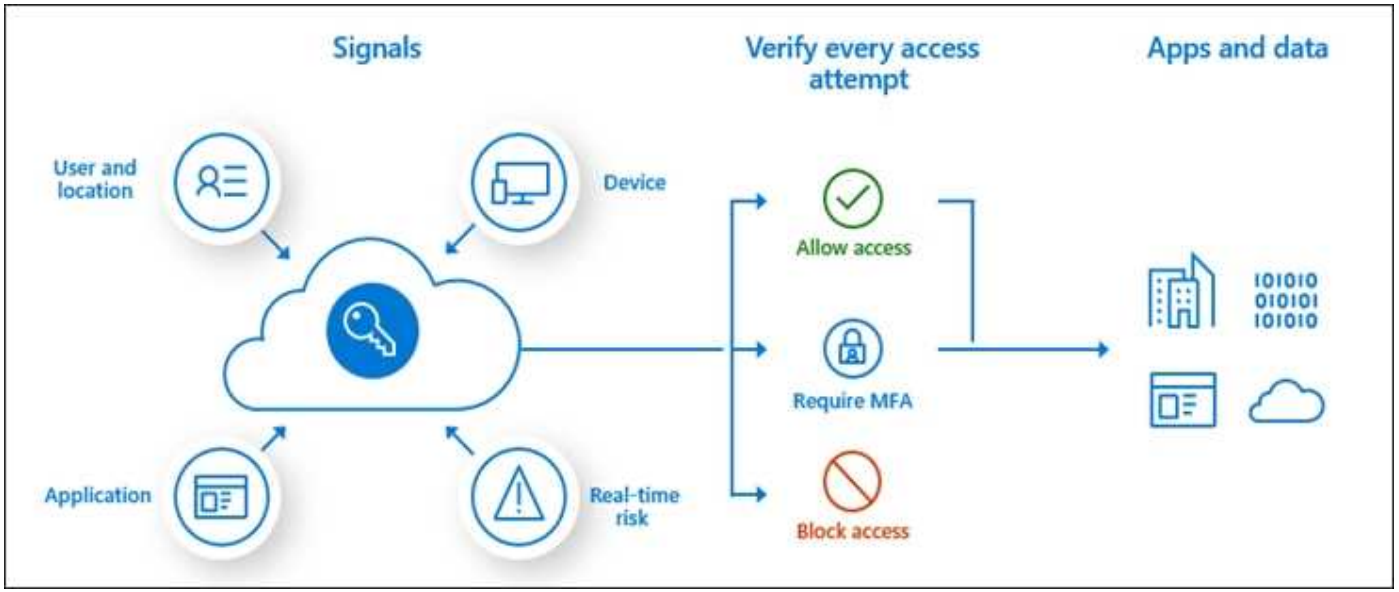
QUESTION 40
HOTSPOT
You plan to deploy an Azure web app named Appl that will use Azure Active Directory (Azure AD) authentication.
App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.
You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.
What should you recommend for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Box 1: An Azure AD app registration
Azure active directory (AD) provides cloud based directory and identity management services.You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory.
You register your application with Azure active directory tenant.
Box 2: A conditional access policy
Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.
By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Reference:
https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
https://docs.microsoft.com/en-us/powerapps/developer/data-platform/walkthrough-register-appazure-activedirectory#:~:text=Create%20an%20application%20registration%201%20Create%20an%20application,the%20options%20and%20click%20on%20Add%20permissions.%20
"After consenting to use their Dataverse account with the ISV's application, end users can connect to Dataverse environment from external application. The consent form is not displayed again to other users after the first user who has already consented to use the ISV's app. Apps registered in Azure Active Directory are multi-tenant, which implies that other Dataverse users from other tenant can connect to their environment using the ISV's app."

QUESTION 41
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is being

deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.
Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

---

QUESTION 42
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.
Several VMs are exhibiting network connectivity issues.
You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.
Solution: Use the Azure Advisor to analyze the network traffic.
Does the solution meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.
Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.
With Advisor, you can:
Get proactive, actionable, and personalized best practices recommendations.
Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.
Get recommendations with proposed actions inline.
Reference:
https://docs.microsoft.com/en-us/azure/advisor/advisor-overview

---

QUESTION 43
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.
Several VMs are exhibiting network connectivity issues.
You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.
Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic
Does the solution meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.
Note:
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

---

QUESTION 44
DRAG DROP
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.
You need to use Azure Log Analytics design an alerting strategy for security-related events.
Which Log Analytics tables should you query? To answer, drag the appropriate tables to the correct log types. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.