MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

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

https://www.passapply.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

DRAG DROP You have an on-premises Hyper-V infrastructure that contains the following: An Active Directory domain

A domain controller named Server1

A member server named Server2

A security policy specifies that Server1 cannot connect to the Internet. Server2 can connect to the Internet.

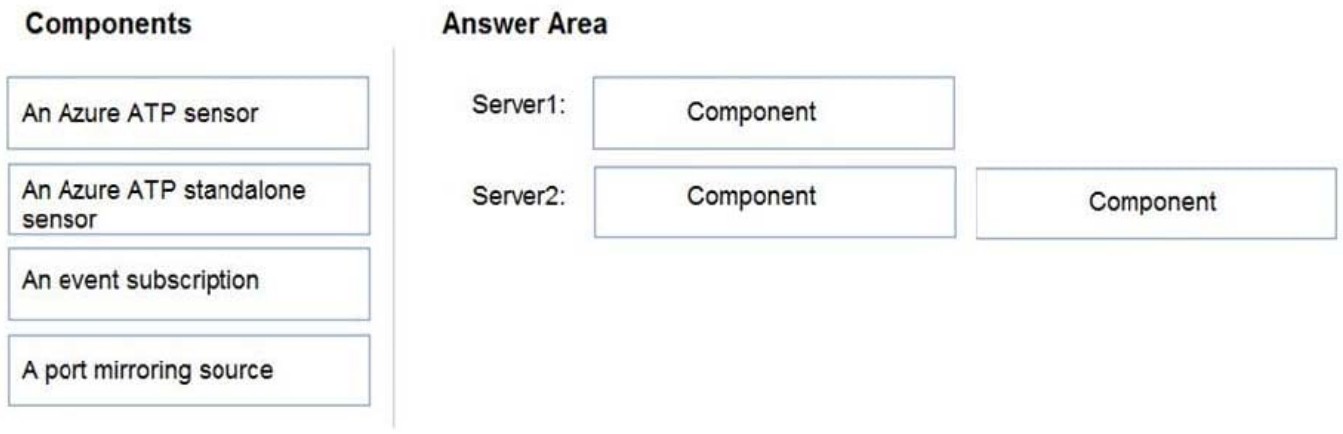
You need to implement Azure Advanced Threat Protection (ATP) to monitor the security of the domain.

What should you configure on each server? To answer, drag the appropriate components to the correct servers. Each component may only be used once, more than once, or not at all. You may need to drag the split bar between panes or

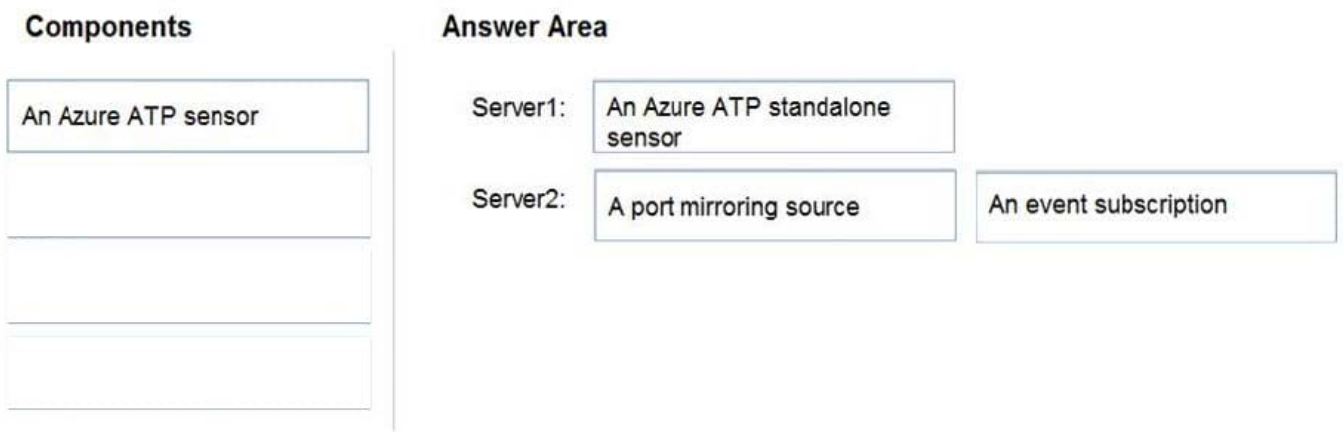
scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



QUESTION 2

SIMULATION

You need to create a policy that identifies content in Microsoft OneDrive that contains credit card numbers.

To complete this task, sign in to the Microsoft 365 portal.

Correct Answer: See explanation below.

You need to configure auto-labeling in 'simulation' mode. In the policy, you can select the 'Credit Card' sensitive info type.

1.

In the Microsoft 365 compliance center, navigate to sensitivity labels: Solutions > Information protection

2.

Select the Auto-labeling (preview) tab.

3.

Select + Create policy.

4.

For the page Choose info you want this label applied to: Select one of the templates, such as Financial or Privacy. You can refine your search by using the Show options for dropdown. Or, select Custom policy if the templates don\\'t meet your requirements. Select Next.

5.

For the page Name your auto-labeling policy: Provide a unique name, and optionally a description to help identify the automatically applied label, locations, and conditions that identify the content to label.

6.

For the page Choose locations where you want to apply the label: Select OneDrive. Then select Next.

7.

For the Define policy settings page: Keep the default of Find content that contains to define rules that identify content to label across all your selected locations. The rules use conditions that include sensitive information types and sharing options. For sensitive information types, you can select both built-in and custom sensitive information types.

8.

Then select Next.

9.

For the Set up rules to define what content is labeled page: Select + Create rule and then select Next.

10.On the Create rule page, name and define your rule, using sensitive information types and then select Save.

11.Click Next.

12.For the Choose a label to auto-apply page: Select + Choose a label, select a label from the Choose a sensitivity label pane, and then select Next.

13.For the Decide if you want to run policy simulation now or later page: Select Run policy in simulation mode if you\\'re ready to run the auto-labeling policy now, in simulation mode. Otherwise, select Leave policy turned off.

Select Next. 14.For the Summary page: Review the configuration of your auto-labeling policy and make any changes that needed, and complete the wizard.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-labelautomatically?view=o365-worldwide

---

QUESTION 3

You have a Microsoft 365 E5 subscription that uses Azure Active Directory (Azure AD) Privileged identity Management (PIM).

A user named User! is eligible for the User Account Administrator role.

You need User1 to request to activate the User Account Administrator role.

From where should User1 request to activate the role?

A. the My Access portal

B. the Microsoft 365 Defender portal

C. the Azure Active Directory admin center

D. the Microsoft 365 admin center

Correct Answer: C

the Azure Active Directory admin center -> Azure portal ->Privileged Identity Management https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role

---

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

You have a custom compliance manager template named Regulation1.

You have the assessments shown in the following table.

Name	Score	Status	Group	Product	Regulation
Assessment1	1200	Incomplete	Group1	Microsoft 365	Regulation1
Assessment2	900	Incomplete	Group2	Microsoft 365	Regulation2

Assessment1 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Enable multi-factor authentication for admins	Failed high risk	+27 points	0/27	Technical
Enable multi-factor authentication for non-admins	Failed high risk	+27 points	0/27	Technical

Assessment2 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Establish a threat intelligence program	None	+9 points	0/9	Operational
Configure a privileged access policy	Failed high risk	+15 points	0/15	Technical

You perform the following actions:

For Assessment2, change the Test status of Establish a threat intelligence program to Implemented.

Enable multi-factor authentication (MFA) for all users.

Configure a privileged access policy.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	○	○
The Assessment1 score will increase by only 54 points.	○	○
The Assessment2 score will increase by only 78 points.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	○	○
The Assessment1 score will increase by only 54 points.	○	○
The Assessment2 score will increase by only 78 points.	○	○

QUESTION 5

You have a Microsoft 365 tenant.

You have 500 computers that run Windows 10.

You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.

You need to ensure that the computers connect to Windows Defender ATP.

How should you prepare Intune for Windows Defender ATP?

A. Configure an enrollment restriction

B. Create a device configuration profile

C. Create a conditional access policy

D. Create a Windows Autopilot deployment profile

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/intune/advanced-threat-protection