

Microsoft Discussions



Exam AZ-900 All Questions

View all questions & answers for the AZ-900 exam

Go to Exam

EXAM AZ-900 TOPIC 1 QUESTION 223 DISCUSSION

Actual exam question from Microsoft's AZ-900

Question #: 223

Topic #: 1

[\[All AZ-900 Questions\]](#)

HOTSPOT -

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
Azure Sentinel stores collected events in an Azure Storage account.	<input type="radio"/>	<input type="radio"/>
Azure Sentinel can remediate incidents automatically.	<input type="radio"/>	<input type="radio"/>
Azure Sentinel can collect Windows Defender Firewall logs from Azure virtual machines.	<input type="radio"/>	<input type="radio"/>


Show Suggested Answer

by [xian05](#) at Aug. 30, 2021, 8:09 p.m.

Comments

Type your comment...

Submit

  **wendyy** Highly Voted  3 years, 1 month ago


I think the first should be NO. Azure Sentinel use Log Analytics workspace to stored log. After 90 days if Sentinel is enabled. Then you can export of logs from your Log Analytics workspace to destinations such as Azure Storage and Event Hub.

   upvoted 34 times

  **wendyy** 3 years, 1 month ago

More for this: Log Analytics workspace will keep your log inforatmion, after 90 days, you need pay money per G/month. If you want to use your storage account to store log, you need pay money to export log into your storage account or Event Hub. So first one is NO. storage account is only one option you can transfer log if you don't want pay money to keep. Log Analytics workspace is correct place.

   upvoted 5 times

  **Fosnefes** 1 year, 8 months ago

By default, logs ingested into Microsoft Sentinel are stored in Azure Monitor Log Analytics.




See - <https://learn.microsoft.com/en-us/azure/sentinel/store-logs-in-azure-data-explorer?tabs=adx-event-hub>

   upvoted 1 times

  **Vincentvds** Highly Voted  3 years, 1 month ago

Sentinel Stores your events in a Log Analytics workspace and can retrieve events from a starage location. it doesnt store the events in a storage location.

   upvoted 11 times


  **e3ddceb** Most Recent  3 months, 2 weeks ago

No. Azure Sentinel stores collected events in Azure Log Analytics workspaces, not in an Azure Storage account.

Yes. Azure Sentinel can remediate incidents automatically using Playbooks, which are collections of procedures that can be run from Azure Sentinel.

Yes. Azure Sentinel can collect Windows Defender firewall logs from Azure VMs.

   upvoted 3 times

  **siculoct** 4 months, 2 weeks ago

N,Y,Y is correct

   upvoted 2 times

  **Pcservices** 5 months, 2 weeks ago

N,Y,Y is the correct answer

   upvoted 1 times

  **xqzit** 10 months ago

YYY

<https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/azure-storage-account>

Azure Storage account is a cloud solution for modern data storage scenarios. It contains all your data objects: blobs, files, queues, tables, and disks. This connector lets you stream Azure Storage accounts diagnostics logs into your Microsoft Sentinel workspace, allowing you to continuously monitor activity in all your instances, and detect malicious activity in your organization. For more information, see the

   upvoted 1 times

  **Wablo** 1 year ago

Hi guys, please check the below link for clarity, I will go with NYY.

As you plan your Microsoft Sentinel deployment, you typically want to understand its pricing and billing models to optimize your costs. Microsoft Sentinel's security analytics data is stored in an Azure Monitor Log Analytics workspace. Billing is based on the volume of data analyzed in Microsoft Sentinel and stored in the Log Analytics workspace.

<https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=simplified%2Ccommitment-tiers>

   upvoted 2 times



  **Rajivjain** 1 year, 4 months ago

YYY : Yes, Azure Sentinel can store collected events in an Azure Storage account. Azure Sentinel is a cloud-native security information and event management (SIEM) solution provided by Microsoft. It enables organizations to collect, analyze, and respond to security events and incidents across their environment.

Azure Sentinel can ingest data from various sources, including logs and events from Azure services, on-premises infrastructure, and third-party systems. The collected events can be stored in an Azure Storage account, which provides a scalable and durable storage solution for the data. This allows organizations to retain and analyze security event data over a longer period of time as required by their compliance or investigative needs

longer period of time, as required by their compliance or investigative needs.

   upvoted 3 times

  **Ciupaz** 1 year, 8 months ago

Microsoft Sentinel security analytics data is stored in an Azure Monitor Log Analytics workspace. Billing is based on the volume of that data in Microsoft Sentinel and the Azure Monitor Log Analytics workspace storage.

   upvoted 3 times

  **mmatchev** 1 year, 8 months ago

No, Azure Sentinel does not store collected events in an Azure Storage account. Azure Sentinel stores events in a centralized Log Analytics workspace. The Log Analytics workspace acts as the data repository for Azure Sentinel and provides a single place for storing, analyzing, and querying security-related data from various sources.

   upvoted 2 times

  **Contactfornitish** 2 years, 7 months ago

First answer is incorrect. As pointed out by others, Sentinel doesn't store content in storage account but in Log Analytics. Can say for sure since completed SC-200 few weeks back and SC-900 with 1000/1000 and one of the question was similar

   upvoted 9 times

  **PreethiP** 2 years, 9 months ago

NY - Stores events in Log Analytics workspace

   upvoted 1 times

  **atilla** 2 years, 10 months ago

now called Microsoft Sentinel

   upvoted 2 times



  **peymani** 2 years, 10 months ago

<https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/>

Microsoft Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an Azure Monitor Log Analytics workspace. Microsoft Sentinel is billed based on the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace. Microsoft Sentinel offers a flexible and predictable pricing model. There are two ways to pay for the Microsoft Sentinel service: Capacity Reservations and Pay-As-You-Go.

Q1: NO

   upvoted 4 times

  **mufflon** 2 years, 10 months ago

By default, logs ingested into Microsoft Sentinel are stored in Azure Monitor Log Analytics, So Q1 is NO

   upvoted 2 times

  **swapnasantoshi** 2 years, 10 months ago

what is the ans for Q1?

   upvoted 1 times

  **jonnyazure** 2 years, 11 months ago

SO for #1 whats the answer?

   upvoted 1 times

[Load full discussion...](#)

Start Learning for free



Social Media

[Facebook](#) , [Twitter](#)

[YouTube](#) , [Reddit](#)

[Pinterest](#)



We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.



© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.