

ActualtestsIT

ActualtestsIT

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

CART (0)



Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.

PDF format: Easy to read and print learning materials, our products are available in PDF file format.

Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.

Select a vendor...

Select an test...

Your email address

Free Download Demo

Instant Download



After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates



Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

<http://www.actualtestsit.com/>

Topping Certification Exam Prep, Test Dumps Materials - ActualTestsIT

Exam : **AB-900**

Title : Microsoft 365 Copilot & Agent
Administration Fundamentals

Vendor : Microsoft

Version : DEMO

NO.1 Your organization has a Microsoft 365 subscription that contains Microsoft SharePoint sites and Microsoft Teams teams.

You discover that the sites and the teams are shared to users outside your organization.

You need to identify which sites and teams were shared to the external users.

What should you use?

- A.** the SharePoint admin center
- B.** the Microsoft Teams admin center
- C.** the Microsoft 365 admin center
- D.** the Microsoft Defender portal

Answer: A

Explanation:

The correct answer is A. the SharePoint admin center . Microsoft documents that the SharePoint admin center includes Data access governance reports and site-level sharing reports that help administrators identify where content is shared externally. Microsoft also documents that every standard Microsoft Teams team is connected to a SharePoint site for file storage and collaboration. Because Teams files and many sharing scenarios for teams are backed by SharePoint sites, the SharePoint admin center is the correct place to investigate which sites are shared externally, including Teams-connected SharePoint sites .

The other options are less suitable for this requirement. The Teams admin center is primarily for Teams policy, user, device, and workload administration, but it is not the main portal Microsoft documents for identifying externally shared site content. The Microsoft 365 admin center focuses on broad tenant administration and usage reporting, and the Microsoft Defender portal is for security investigation rather than SharePoint/Teams sharing governance. For identifying externally shared SharePoint sites and Teams- connected sites, Microsoft's documented reporting path is the SharePoint admin center .

NO.2 Your company is piloting the use of Microsoft 365 Copilot and has purchased 100 Microsoft 365 Copilot licenses.

You need to view detailed reports about Copilot usage in Microsoft Teams, such as meeting hours summarized by Copilot and meeting actions taken by using Copilot.

What should you use?

- A.** the Microsoft 365 Apps usage report in the Microsoft 365 admin center
- B.** the Microsoft 365 Copilot readiness report in the Microsoft 365 admin center
- C.** the Microsoft 365 Copilot dashboard in Microsoft Viva Insights
- D.** the Microsoft 365 Copilot usage report in the Microsoft 365 admin center

Answer: C

Explanation:

The correct answer is C. the Microsoft 365 Copilot dashboard in Microsoft Viva Insights . Microsoft documents that the Microsoft Copilot Dashboard in Viva Insights provides detailed organizational reporting for Copilot usage and impact, including meeting-related metrics such as total meeting hours summarized or recapped , intelligent recap actions taken using Copilot , and summarize meeting actions taken using Copilot in Teams . Those metrics directly match the scenario in the question.

The other options are less suitable. The Microsoft 365 Apps usage report focuses on app usage generally, not detailed Copilot-in-Teams behavior. The Copilot readiness report is for readiness and

deployment planning, not deep Teams usage metrics. The Microsoft 365 Copilot usage report in the admin center provides adoption information, but Microsoft's detailed meeting-action and meeting-hours metrics are documented in the Viva Insights Copilot Dashboard . Therefore, for detailed Teams-specific Copilot reporting during a pilot, the best answer is the Microsoft 365 Copilot dashboard in Microsoft Viva Insights .

NO.3 Your organization has a Microsoft 365 subscription.

All users have Microsoft 365 Copilot licenses.

You need to identify where sensitive content is being used during Copilot interactions, analyze the content usage patterns, and provide recommendations on applying the appropriate protections.

What should you use?

- A. Microsoft Viva Insights
- B. the Microsoft Purview DSPM for AI solution
- C. Microsoft Security Copilot
- D. the Microsoft Purview Insider Risk Management solution

Answer: B

Explanation:

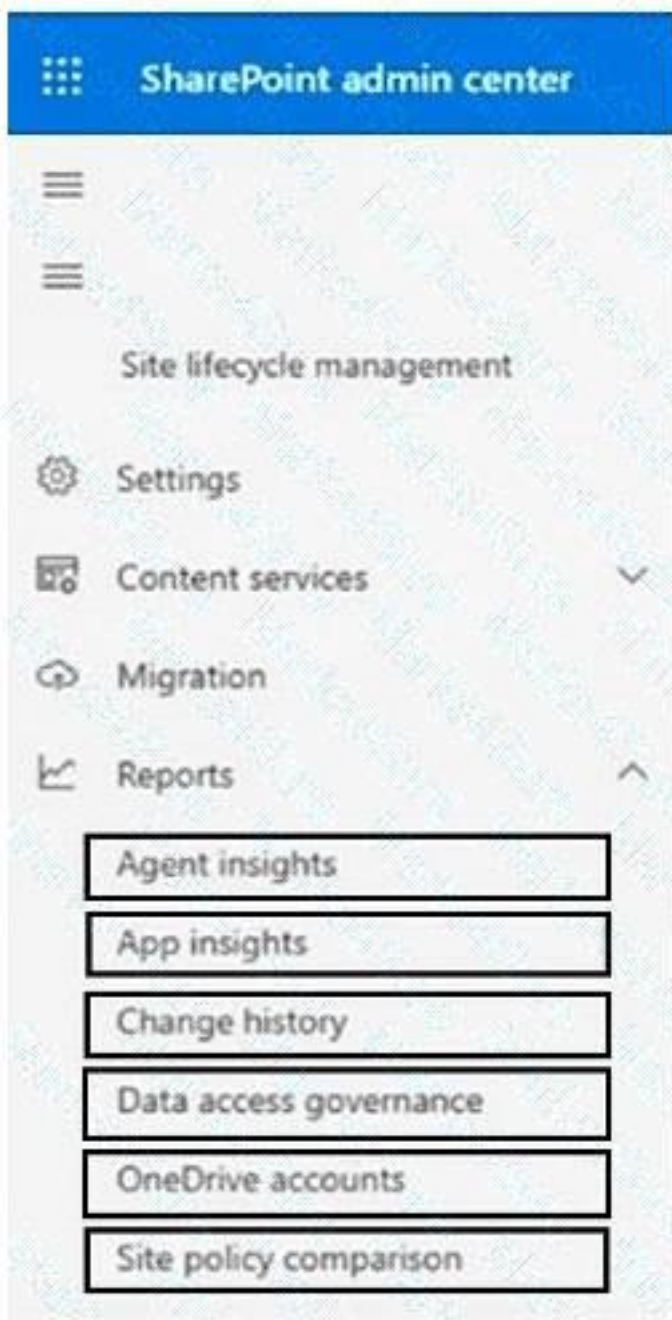
The correct answer is B. the Microsoft Purview DSPM for AI solution . Microsoft documents that Data Security Posture Management for AI (DSPM for AI) in Microsoft Purview provides a central place to secure data for AI apps and proactively monitor AI use , including Copilots and agents . Microsoft also states that DSPM for AI helps organizations identify where sensitive content is used in AI interactions , review Copilot prompts and responses , analyze usage patterns , assess exposure and oversharing risks, and get recommendations for protections such as sensitivity labels and DLP policy coverage. The other options do not fit this requirement. Microsoft Viva Insights focuses on productivity and work- pattern analytics, not sensitive-data protection in Copilot interactions. Microsoft Security Copilot is a security assistant for analysts, not the Purview governance solution that analyzes sensitive content use in Copilot and recommends data protections. Insider Risk Management is for identifying risky user behavior, not for broad AI interaction posture analysis and protection recommendations. Microsoft specifically positions DSPM for AI as the "front door" for discovering, monitoring, and protecting AI-related data usage in Microsoft 365 Copilot.

NO.4 Your organization has a Microsoft 365 subscription.

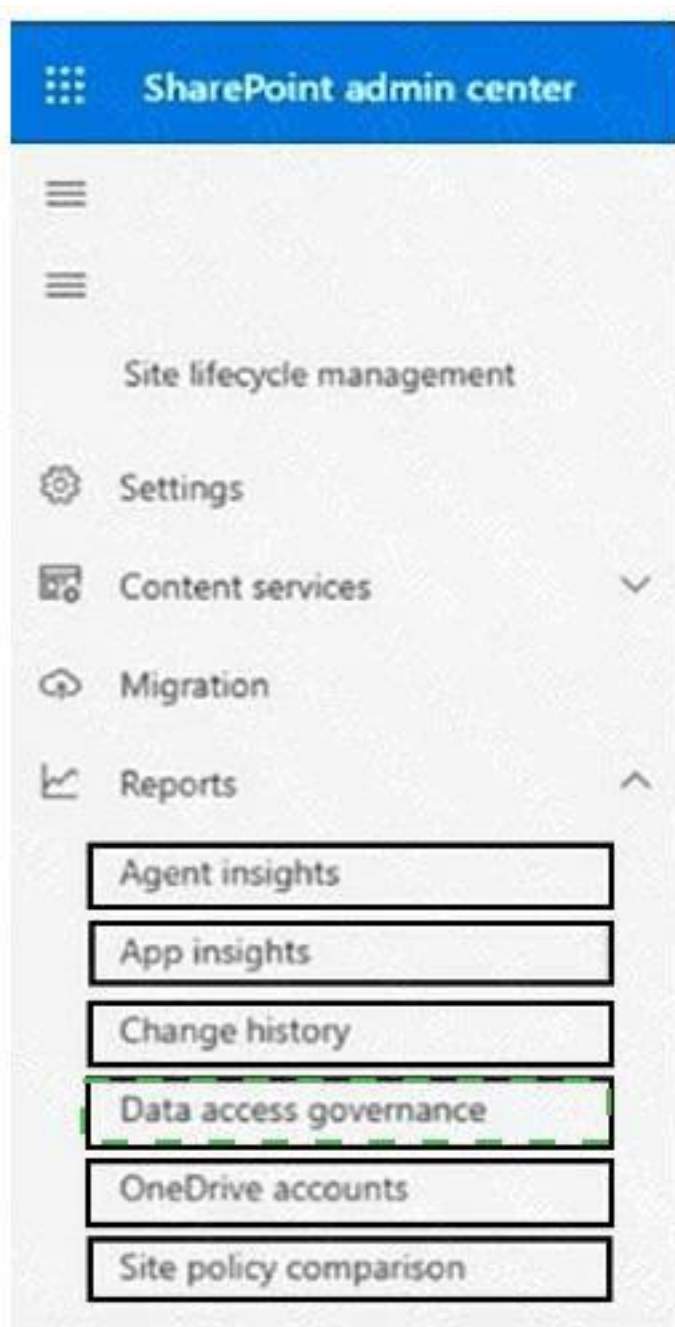
You discover that Microsoft SharePoint files are being shared to users outside your organization.

You need to identify which files are being shared to the external users.

Which report should you use in the SharePoint admin center? To answer, select the appropriate report in the answer area.



Answer:



Explanation:

The correct answer is Data access governance . Microsoft documents that Data access governance reports in the SharePoint admin center help administrators discover overshared or sensitive SharePoint content and assess sharing exposure. More specifically, Microsoft's sharing links activity reports under Data access governance are designed to monitor sharing activity and identify sites where links such as Anyone , People in the organization , and Specific people links have been created. This is the SharePoint admin reporting area Microsoft provides for investigating external sharing patterns and related exposure.

The other listed reports do not fit this requirement. Agent insights is for Copilot/agent usage, App insights is for application-related insights, Change history tracks configuration changes, OneDrive accounts focuses on OneDrive administration, and Site policy comparison compares site settings. None of those is the SharePoint report family intended for identifying externally shared SharePoint content. Based on Microsoft's documentation, the report area you should use is Data access

governance .

NO.5 Your organization has a Microsoft 365 subscription.

You need to evaluate your organization s Identity Secure Score.

Which two factors affect the score? Each correct answer presents a complete the solution.

NOTE: Each correct selection is worth one point.

A. the number of global administrators

B. the SharePoint site permissions

C. the location of the users

D. passwords that are never expired

Answer: A D

Explanation:

The correct answers are A and D because Microsoft Entra Identity Secure Score is based on identity security recommendations, and Microsoft Learn specifically lists recommendations such as "Designate more than one Global Administrator" and "Do not expire passwords." That means the number of global administrators in the tenant and whether password expiration is disabled directly influence the Identity Secure Score. Microsoft also notes that the score measures how closely an organization aligns with Microsoft's recommended identity security best practices.

Option B is incorrect because SharePoint site permissions are related to SharePoint and Microsoft 365 workload permissions, not to the Entra identity-focused scoring model. Option C is incorrect because user location may be evaluated in Conditional Access and Zero Trust scenarios, but it is not itself listed as a direct Identity Secure Score factor in the Microsoft Entra recommendations referenced by Microsoft Learn. Identity Secure Score is driven by tracked identity recommendations and security configurations, not by simple geographic placement of users.

NO.6 Your organization has a Microsoft 365 subscription that contains a user named User1. User1 plans to leave your company in two weeks. You need to capture the activity of User1 to identify whether the user is exfiltrating data. Which Microsoft Purview solution should you use?

A. Communication Compliance

B. Data Security Posture Management

C. Insider Risk Management

D. Data Lifecycle Management

Answer: C

Explanation:

The correct answer is C. Insider Risk Management . Microsoft documents that Microsoft Purview Insider Risk Management helps organizations detect, investigate, and act on potentially risky internal activities, including data theft and data leakage . Microsoft specifically provides policy templates for departing users

, describing scenarios where users who are leaving an organization might download files, print files, or copy data to personal cloud storage or messaging services near their resignation or end date. That matches this question exactly, where User1 is leaving in two weeks and you need to determine whether the user is exfiltrating data.

The other options do not fit. Communication Compliance is for reviewing risky communications, Data Security Posture Management focuses on broader data exposure posture, and Data Lifecycle Management is for retention and deletion. None of those is the Microsoft Purview solution

specifically built to monitor suspicious user activity and data exfiltration risk for departing employees. Microsoft positions Insider Risk Management as the correct tool for this scenario.

NO.7 Your company has a Microsoft SharePoint site named Site1. Site1 contains all the policies of the company's HR department. The policies are saved as Microsoft Word documents.

All users have read access to Site1.

The HR department manager reports that user requests about the policies are NOT being addressed in a timely manner, especially around major holidays.

You need to recommend a solution to enable the users to find the HR department policies. The solution must provide the users with a list of common queries and ensure that responses are grounded only in Site1.

What should you include in the recommendation?

- A.** the personal assistant in Copilot in Word
- B.** a Microsoft 365 Copilot notebook
- C.** a custom Microsoft 365 Copilot agent
- D.** the Researcher agent in Microsoft 365 Copilot

Answer: C

Explanation:

The correct answer is C. a custom Microsoft 365 Copilot agent . Microsoft Learn explains that Agent Builder in Microsoft 365 Copilot lets you create agents with specific instructions , dedicated knowledge sources , and starter prompts . Starter prompts are designed to help users understand the most common supported scenarios, which directly matches the requirement to provide users with a list of common queries.

Microsoft also documents that an agent can be grounded in selected SharePoint sites, folders, or files , allowing the response scope to be targeted to the HR policy content in Site1 rather than broad enterprise or web data.

The other options do not fit the requirement. Copilot in Word is document-focused and is not intended to create a reusable, shared query experience grounded only in one SharePoint source. Copilot notebooks group materials and chats, but they are not the right tool for publishing a guided HR policy assistant with starter prompts. Researcher is designed for broader, multi-step research using work data and web content, so it does not satisfy the requirement to keep answers grounded only in Site1.