DUMPSARENA

Managing Microsoft Teams

Microsoft MS-700

Version Demo

Total Demo Questions: 52

Total Premium Questions: 526

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Plan and configure a Microsoft Teams environment	106
Topic 2, Manage chat, teams, channels, and apps	173
Topic 3, Manage Teams meetings and calling	140
Topic 4, Monitor, report on, and troubleshoot Teams	56
Topic 5, Mix Questions	1
Topic 6, Case Study Contoso, Ltd	27
Topic 7, Case Study Litware, inc	14
Topic 8, Case Study A. Datum Corporation	9
Total	526

QUESTION NO: 1

Scenario: 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. Once you answer a question in this section, you cannot return to it, and it will not appear in the review screen.

Your organization has a Microsoft 365 subscription, and you plan to configure the environment to permit external users to collaborate in Microsoft Teams through guest access.

The organization implements a new security policy with the following requirements:

Only guest users from specific domains are allowed to connect and collaborate using Microsoft Teams.
Guest users must be prevented from inviting additional guests.

Your task is to recommend a solution to meet these security policy requirements.

Solution: You execute the New-AzureADPolicy and Set-AzureADPolicy PowerShell cmdlets.

Question: Does this solution meet the goal?

A. Yes

B. No

ANSWER: B

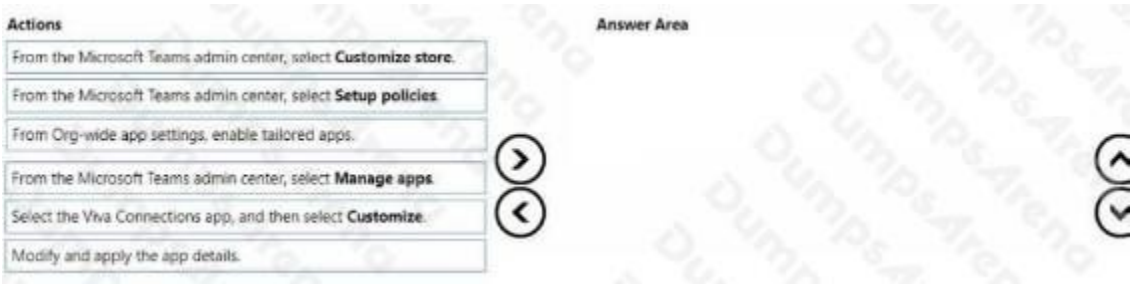
Explanation:

No is correct because running New-AzureADPolicy and Set-AzureADPolicy by itself is not a complete way to satisfy both stated security requirements for Teams guest collaboration. Microsoft Teams guest access is backed by Microsoft Entra B2B collaboration, so domain allowlisting and guest invitation permissions must be controlled through the appropriate Microsoft Entra external collaboration settings. The requirement to allow guests only from specific domains maps to collaboration restrictions, where an organization can allow invitations only to specified domains. The requirement to prevent guest users from inviting additional guests maps to guest invite settings, where invitation permissions are limited to members or selected admin roles rather than guests. These controls are managed in the Microsoft Entra admin center or with the corresponding Microsoft Graph/Microsoft Entra policy settings, not simply by executing the legacy AzureAD policy cmdlets named in the proposed solution. Because the proposed solution does not clearly configure both the domain allowlist and the guest invitation restriction required by the policy, it does not meet the goal. See Microsoft guidance on configuring external collaboration settings and guest access in Microsoft Teams.

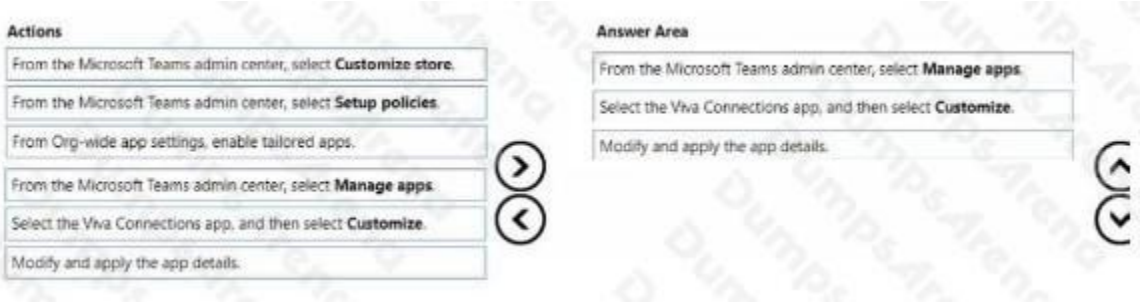
QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

You need to implement the planned changes for Viva Connections. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



ANSWER:



Explanation:

To implement changes to Viva Connections app details in Microsoft Teams, the workflow starts in the Microsoft Teams admin center under the app management area. Viva Connections is treated as a Teams app that can be customized by an administrator, so the correct place to begin is **Manage apps**. From there, an admin can locate the Viva Connections app, open it, and use the **Customize** option to change the app's visible details for users. This is the supported administrative path for tailoring the app experience in Teams, such as updating app branding or other app metadata that users see.

After selecting the Viva Connections app and choosing **Customize**, the admin modifies the required app details and applies the configuration. Applying the changes is important because the customization is not effective until the updated app details are saved and submitted through the Teams admin center workflow. Microsoft documents this customization model as part of managing apps in Teams, where admins can customize supported apps directly from the Teams admin center. See Microsoft's guidance on customizing apps in Microsoft Teams and the overview for Microsoft Viva Connections.

Because the requested task is about implementing Viva Connections changes, the sequence must follow the actual management flow: open the app inventory, customize the Viva Connections app, and then save/apply the edited details. That sequence ensures the change is made to the Viva Connections Teams app itself, rather than to unrelated app store settings, setup policies, or organization-wide app availability settings.

QUESTION NO: 3

Your company holds a Microsoft 365 subscription that includes the use of Microsoft Teams.

You have acquired an application called App1 from the Microsoft Teams Store.

Your task is to add App1 to the Microsoft Teams client for a designated group of users.

What two actions must you take in the Microsoft Teams admin center to achieve this? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. From the Meeting settings, modify the Network settings.

B. From App setup policies, create a new app setup policy.

C. From App setup policies, modify the global app setup policy.

D. From the properties of each user, edit the assigned policies.

E. From the Org-wide settings, modify the Devices settings.

ANSWER: B D

Explanation:

To add App1 to the Teams client for only a designated set of users, you should use a Teams app setup policy and then assign that policy to the intended users. "From App setup policies, create a new app setup policy" is correct because app setup policies control which apps are installed and pinned in the Teams client for users. After creating a custom policy, you can add App1 as an installed app, and optionally pin it so it appears in the Teams app bar for those users. "From the properties of each user, edit the assigned policies" is also correct because the custom app setup policy must be assigned to the users who should receive App1. In the Teams admin center, admins can open a user's profile and update the assigned policies, including the app setup policy. Microsoft documents that app setup policies are used to install and pin apps for

users, and that policies can be assigned directly to users from the Teams admin center. See Manage app setup policies in Microsoft Teams and Assign policies to users and groups in Microsoft Teams.

QUESTION NO: 4

Your company is subscribed to Microsoft 365. You need to enable collaboration between users from a partner company, Contoso, Ltd., and your company's users in Microsoft Teams. The solution should allow Contoso's users to exchange chat messages within the Teams channels.

What are the three necessary actions you must take before adding the Contoso users to Teams? Each correct answer contributes to the overall solution.

NOTE: Each correct selection is worth one point.

A. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group members outside the organization access group content to On.

B. From the Guest access settings in the Microsoft Teams admin center, set Allow guest access in Microsoft Teams to On.

C. From the External collaboration settings in the Azure Active Directory admin center, add Contoso's domain to the list of target domains.

D. From the External access settings in the Microsoft Teams admin center, add Contoso's domain to the Allowed list of domains.

E. From the External collaboration settings in the Azure Active Directory admin center, set Guest users permissions are limited to No.

F. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group owners add people outside the organization to groups to On.

ANSWER: A B F

Explanation:

To allow Contoso users to exchange messages inside Teams channels, they must be added as guest users to teams, because channel conversations are part of the team's Microsoft 365 group-backed workspace. The required preparation is to enable guest access in Teams and ensure Microsoft 365 Groups allow external guests to be added and to access group content. "Allow guest access in Microsoft Teams" enables the Teams service to support guests in teams and channels. "Let group owners add people outside the organization to groups" allows team owners, through the underlying Microsoft 365 group, to add external users as guests. "Let group members outside the organization access group content" permits those guests to access the group resources that Teams relies on, including conversations and shared collaboration content. These settings align with Microsoft's Teams guest access checklist, which calls out Teams guest access plus Microsoft 365 Groups guest settings as dependencies for guest collaboration. See Microsoft's guidance on guest access in Microsoft Teams and the Teams guest access checklist.

QUESTION NO: 5

Note: This question is part of a series where each question presents the same scenario. Each question in this series contains a unique solution that might achieve the stated goals. Some sets of questions may have more than one correct solution, while others may not have a correct solution. After responding to a question in this section, you will NOT be able to return to it. Therefore, these questions will not appear in the review screen.

Your organization has a Microsoft 365 subscription that utilizes an Azure Active Directory (Azure AD) tenant named contoso.com. You need to ensure that guest users within the tenant are restricted from using cameras during Microsoft Teams meetings.

Proposed Solution: Modify the External sharing settings from the Microsoft Teams admin center.

Does this approach fulfill the requirement?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because restricting camera use in Microsoft Teams meetings is controlled through Teams meeting policy settings, not through external sharing configuration. The requirement is specifically about whether guest users can use video during meetings, which is an audio and video meeting policy behavior. In the Teams admin center, meeting policies include controls for IP video and related media capabilities, allowing admins to define whether assigned users can use video in Teams meetings. To meet this requirement, an administrator would configure an appropriate Teams meeting policy that disables camera/video capability and apply it to the relevant guest users or guest user scope as supported by the organization's policy assignment approach.

External sharing settings are intended for controlling how users collaborate with people outside the organization, such as sharing or access behavior, rather than controlling in-meeting device features like cameras. Microsoft documents Teams meeting audio and video policy controls in Manage meeting policies for audio and video, and guest collaboration configuration separately in Collaborate with guests in a team.

QUESTION NO: 6

You need to configure Microsoft Teams to fulfill specific collaboration and meeting requirements.

Which two actions should you perform in the Microsoft Teams admin center? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. Modify the Meeting settings.

B. Create a team's policy.

C. Create a meeting policy.

D. Create a live events policy.

E. Modify the Teams settings.

ANSWER: B C

Explanation:

Create a team's policy is correct because Teams policies in the Microsoft Teams admin center are used to control collaboration capabilities that apply to users when they work with teams and channels. These policies can govern features such as whether users can create private channels, create shared channels, invite external users to shared channels, or join external shared channels. When collaboration requirements must be applied to a defined set of users, creating and assigning an appropriate Teams policy is the right administrative approach. See Microsoft's guidance on manage teams policies in Microsoft Teams.

Create a meeting policy is also correct because meeting policies control the meeting experience and meeting-related features available to users. In the Teams admin center, admins can create custom meeting policies and assign them to users or groups to manage settings such as meeting scheduling, recording, transcription, content sharing, lobby behavior, meeting chat, and related meeting capabilities. This is the standard way to meet user- or group-specific meeting requirements in Teams. Microsoft documents these controls in meeting policies in Microsoft Teams.

QUESTION NO: 7

Your organization subscribes to Microsoft 365. You aim to personalize your meeting invitation emails by incorporating the company logo. Which action should you take within the Microsoft Teams admin center to achieve this customization?

A. From Teams settings, modify the Email integration settings.

B. From Meeting settings, modify the Email invitation settings.

C. From Meeting policies, create a new meeting policy and assign the policy.

D. From Meeting policies, modify the Global (Org-wide default) policy.

ANSWER: B

Explanation:

From Meeting settings, modify the Email invitation settings is correct because Microsoft Teams provides organization-wide customization for Teams meeting invitations in the Teams admin center under Meetings > Meeting settings. In the Email invitation section, an administrator can specify a logo URL so that the company logo appears in Teams meeting invite emails. This same area also supports other invitation branding and informational elements, such as a legal URL, help URL, and custom footer text, depending on what the organization wants included in meeting invitations. These settings are designed specifically for customizing the content that users see in Teams meeting invitations, making them the appropriate place to add corporate branding such as a logo. Microsoft documents these controls as part of Teams meeting settings, and the configuration is managed centrally from the Teams admin center rather than through per-user meeting policies. For more details, see Microsoft's documentation on meeting settings in Microsoft Teams and the Teams admin center guidance for admin center management.

QUESTION NO: 8

You are tasked with determining the necessary steps for implementing the voice pilot project. Which two actions should you take? Each correct answer is part of the overall solution.

NOTE: Each correct selection awards one point.

A. Assign an additional license and phone number to each user.

B. Deploy a Session Border Controller (SBC) for Litware.

C. Purchase a Phone System license for each user.

D. Create a dial plan for Litware.

E. Purchase a Calling Plan for Litware.

ANSWER: B C

Explanation:

To implement the voice pilot project by using Microsoft Teams Phone with Direct Routing, Litware must have a supported voice connection path to the PSTN and the users must be licensed for Teams Phone capabilities. Deploy a Session Border Controller (SBC) for Litware is correct because Direct Routing uses a certified SBC to connect Microsoft Phone System to the organization's telephony carrier or existing PSTN infrastructure. The SBC is the required component that securely routes calls between Teams and the PSTN provider. Purchase a Phone System license for each user is also correct because users who make and receive PSTN calls through Teams require Teams Phone/Phone System functionality unless it is already included in their assigned Microsoft 365 plan. Microsoft's Direct Routing planning guidance lists the SBC and appropriate Teams Phone licensing as core prerequisites for enabling users for Direct Routing. See Plan Direct Routing and Configure Direct Routing for Microsoft's requirements and configuration flow.

QUESTION NO: 9

Consider you have a Microsoft 365 subscription configured with Microsoft Teams and the groups listed in the table below:

You decide to create a new team named Project1. Out of the existing groups, which can be added to Project1?

A. Group1 only

B. Group2 only

C. Group3 only

D. Group1 and Group3 only

E. Group1, Group2, and Group3

ANSWER: C

Explanation:

Group3 only is correct because Microsoft Teams supports adding/importing members from an existing distribution list, security group, or Microsoft 365 group only when the group is within the supported import size limit. Microsoft's Teams limits and specifications state that the maximum size of a distribution list, security group, or Microsoft 365 group that can be imported into a team is 3,500 members. In this scenario, Group3 is the existing group that satisfies the Teams membership import requirements shown in the table, so it can be added to the newly created Project1 team. When a supported group is added, Teams expands the group membership and adds the individual users to the team; it does not maintain the source group as a nested group membership object. This is why the group must meet the Teams import constraints at the time it is added. For the official limit, see Microsoft Learn: Limits and specifications for Microsoft Teams.

QUESTION NO: 10

You are a Systems Administrator at your company, which subscribes to Microsoft 365 and all employees have a Microsoft 365 E3 license. You are planning to conduct live events using Microsoft Teams. However, you've found that external users are not able to join the live events, while internal employees and users with guest accounts can access them without any issue.

What configuration change should be made to allow external users without guest accounts access to these live events?

A. The External Access Org-wide settings

B. The default Meeting policy

C. The Live events settings

D. The default Live events policy

ANSWER: D

Explanation:

The default Live events policy is correct because Microsoft Teams live event attendee access is controlled through live event policies assigned to organizers. In the Teams admin center, the relevant setting is the live event policy option that controls who can join scheduled live events. To allow people outside the organization who do not have guest accounts to attend, the policy must permit broader attendee access, typically by setting the join permission to "Everyone." When this is configured in the default Live events policy, users who receive that default policy can schedule live events that anonymous external attendees can join through the event link.

This fits the scenario because internal users and guest users can already access the events, which means the issue is not basic Teams licensing or event scheduling. The missing permission is specifically for external attendees who are not authenticated as guests in the tenant. Microsoft documents Teams live event configuration as being managed through live event policies and setup requirements in the Teams admin center. See Microsoft's guidance on setting up Teams live events and planning Teams live events.

QUESTION NO: 11

You have a Microsoft 365 subscription with Microsoft Teams enabled. You need to prioritize Microsoft Teams' audio, video, and screen sharing data over other types of network traffic. Which action should you perform within the Microsoft Teams admin center to achieve this?

A. Modify the global (Org-wide default) meeting policy and configure the Media bit rate (Kbs) setting.

B. Modify the global (Org-wide default) meeting policy and configure the Mode for IP video setting.

C. From the Meeting settings, select automatically use any available ports

D. From the Meeting settings, set Insert Quality of Service (QoS) markers for real-time media traffic to On.

E. Configure Quality of Service (QoS) settings for real-time media.

ANSWER: D E

Explanation:

To prioritize Microsoft Teams real-time media traffic, the correct action in the Teams admin center is to enable QoS marking by setting **Insert Quality of Service (QoS) markers for real-time media traffic** to **On** in Meeting settings. This causes Teams clients to apply DSCP markings to real-time media packets, such as audio, video, and screen sharing, so that network devices can identify and prioritize those packets over less time-sensitive traffic. **Configure Quality of Service (QoS) settings for real-time media** is also correct because QoS for Teams is the Microsoft-recommended approach for improving real-time media performance on managed networks. In practice, this includes enabling QoS markers in Teams and ensuring the network is configured to honor the DSCP markings and media port ranges. Microsoft documents this configuration as part of implementing QoS for Teams media workloads, including audio, video, and application sharing. For more details, see Use QoS in Microsoft Teams and Meeting settings in Microsoft Teams.

QUESTION NO: 12

Your organization subscribes to Microsoft 365, and all employees have been given a Microsoft 365 E3 license.

You are tasked with implementing information barriers between two specific groups of users within the company.

Identify the two licensing add-ons that enable this functionality. Each correct selection represents a full solution.

Note: Each correct selection is worth one point.

A. Microsoft Defender for Office 365

B. Insider Risk Management

C. Compliance

D. Communications Credits

ANSWER: B C

Explanation:

Insider Risk Management and Compliance are correct because Microsoft Purview Information Barriers require eligible compliance licensing beyond a base Microsoft 365 E3 subscription. Information barriers are a Microsoft Purview compliance capability used to restrict communication and collaboration between defined user segments, including in Microsoft Teams. For users licensed with Microsoft 365 E3, Microsoft lists qualifying add-on paths that include the Microsoft 365 E5 Compliance add-on and the Microsoft 365 E5 Insider Risk Management add-on. Either add-on can provide the required entitlement to configure and apply information barrier policies for the affected users. In practice, this means the organization can keep Microsoft 365 E3 as the base license and add either the Compliance or Insider Risk Management licensing component to enable the information barriers feature. Microsoft documents information barriers as part of Purview compliance and provides Teams-specific guidance for using these policies to control discoverability and communication between groups. See Microsoft's guidance for Microsoft Purview Information Barriers and information barriers in Microsoft Teams.

QUESTION NO: 13

You have a Microsoft 365 subscription that utilizes Microsoft Teams and includes the groups listed in the following table.

You create a new team called Project1.

Which of the following groups can be added to the Project1 team?

A. Group1 only

B. Group2 only

C. Group3 only

D. Group1 and Group3 only

E. Group1. Group2. and Group3

ANSWER: D

Explanation:

Group1 and Group3 only is correct because Microsoft Teams allows team owners or admins to add supported group types, such as Microsoft 365 groups, security groups, and distribution lists, by importing their members into a team. The key constraint is the supported import size: the maximum size of a distribution list, security group, or Microsoft 365 group that can be imported into a team is 3,500 members. Based on the groups shown in the table, Group1 and Group3 meet the Teams requirements for both supported group type and member count, so their members can be added to the Project1 team. This operation does not add the group object itself as a nested member; instead, Teams expands the group and adds the individual users from that group to the team membership. Microsoft documents this limit in the Teams limits and specifications guidance. See Limits and specifications for Microsoft Teams for the official import limit.

QUESTION NO: 14

You have a Microsoft 365 subscription that includes Microsoft Teams.

You are planning to implement voice functionality in Microsoft Teams. To configure this, which two specific settings will necessitate the use of a resource account? Each correct answer is a part of the overall solution.

NOTE: Each correct selection is worth one point.

A. Call park policies

B. Auto attendant

C. Call queues

D. Emergency polices

E. Guest access

ANSWER: B C

Explanation:

Auto attendant and Call queues are correct because Teams resource accounts are specifically used to provide an identity for these voice application services. In Microsoft Teams Phone, an auto attendant needs a resource account so callers can reach an automated menu, greeting, or routing flow through an assigned phone number. Similarly, a call queue needs a resource account so inbound calls can be delivered to a group of agents through a shared service identity. In both cases, the resource account can be assigned a phone number and, when required, an appropriate Microsoft Teams Phone Resource Account license, allowing the voice application to receive and route calls correctly. Microsoft documentation describes

resource accounts as required for auto attendants and call queues, and Teams admin guidance shows that these accounts are associated directly with those voice apps during configuration. See Microsoft Learn for details on managing resource accounts and planning auto attendants and call queues.

QUESTION NO: 15

Your company uses Teams.

You plan to deploy Teams to a branch office that has limited bandwidth.

Which Two features can he used when the Teams client has a bandwidth restriction of 150 kilobit/s up and 150 kilobit/s down? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. one-to-one seen sharing

B. one-to-one video

C. video during meetings

D. screen sharing during meetings

E. audio during meetings

ANSWER: A E

Explanation:

With a bandwidth restriction of 150 Kbit/s upstream and 150 Kbit/s downstream, the usable Teams features are the ones whose minimum bandwidth requirements fit within that limit. Microsoft's Teams network guidance indicates that audio is highly bandwidth-efficient, with meeting audio requiring well below 150 Kbit/s in each direction, so audio during meetings is supported in this scenario. Microsoft also documents low minimum requirements for peer-to-peer sharing scenarios, where one-to-one screen sharing can operate at approximately 130 Kbit/s, which fits within the stated 150 Kbit/s up/down constraint. Therefore, one-to-one seen sharing and audio during meetings are the two features that can be used under this bandwidth restriction. For planning Teams deployments in bandwidth-constrained locations, Microsoft recommends validating network capacity and expected media workloads by using Teams network planning guidance and the Teams Network Planner. See Prepare your organization's network for Microsoft Teams and Use Network Planner for Microsoft Teams.

QUESTION NO: 16

You are working as a Systems Administrator at your company which has a subscription to Microsoft 365. All users in the organization are equipped with a Microsoft 365 E3 license and utilize Microsoft Teams for collaboration. According to the company's security policy, it is mandatory that all files used in personal chats or team collaborations be retained for at least one year. Your task is to configure a retention policy to conform to this security requirement. Which two locations should the retention policy be applied to in order to adhere to this policy? (Choose two).

A. OneDrive accounts

B. Exchange email

C. Teams chat

D. SharePoint sites

E. Teams channel messages

ANSWER: A D

Explanation:

To retain files used in Microsoft Teams personal chats and team collaboration, the retention policy must target the workloads where those files are actually stored. OneDrive accounts is correct because files shared in Teams one-on-one or group chats are stored in the OneDrive account of the user who shares the file, typically in the Microsoft Teams Chat Files folder. Applying retention to OneDrive accounts ensures those chat-shared files are retained for the required period. SharePoint sites is also correct because files shared in standard Teams channels are stored in the SharePoint site connected to the team, usually in the document library for that team and channel. Applying retention to SharePoint sites ensures files used for team collaboration in channels are retained for at least one year. Microsoft documents this storage behavior for Teams files and explains that Microsoft 365 retention policies for SharePoint and OneDrive apply to files stored in those services. See Share files in Microsoft Teams and Learn about retention for SharePoint and OneDrive.

QUESTION NO: 17

You are planning to deploy Microsoft Teams for 300 users. During the initial phase of this deployment, the following features will be enabled:

Audio
Video
Screen sharing

However, users will be restricted from utilizing the following features:

File sharing
PSTN calling
Conference audio
Conference video
Conference screen sharing

To determine the network bandwidth necessary for this first phase of deployment, what tool should you use?

A. Network Assessment Tool

B. Advisor for Teams

C. Bandwidth Utilization Analyzer

D. Network Planner

ANSWER: D

Explanation:

Network Planner is the correct tool because it is designed specifically to help organizations estimate bandwidth requirements for Microsoft Teams based on the expected usage profile, locations, network sites, and enabled real-time communication workloads. In this scenario, the deployment phase includes Teams audio, video, and screen sharing for 300 users, while excluding conferencing and PSTN-related capabilities. Network Planner lets administrators model this kind of staged rollout by defining personas, assigning users to locations, and estimating the bandwidth needed for Teams media traffic. It is available in the Microsoft Teams admin center and is intended for planning network readiness before or during a Teams deployment. Microsoft describes Network Planner as a tool that helps determine and organize network requirements for connecting an organization to Teams. For more detail, see Microsoft's documentation for Network Planner for Microsoft Teams and the broader network preparation guidance for Teams.

QUESTION NO: 18

You are a Microsoft 365 Administrator for your organization, where all users hold Microsoft 365 licenses. Users frequently collaborate using private chats in Microsoft Teams. To ensure that a specific user cannot permanently delete private chats, what should you configure?

A. The user's Microsoft 365 license options in the Microsoft 365 Admin Center.

B. A meeting policy in Microsoft Teams.

C. A litigation hold on the user's mailbox.

D. A Sensitivity Label in the Security & Compliance Admin Center.

ANSWER: C

Explanation:

A litigation hold on the user's mailbox is correct because Microsoft Teams private chat messages are preserved through the user's Exchange Online mailbox for compliance and eDiscovery purposes. When a mailbox is placed on Litigation Hold, mailbox content is retained in the Recoverable Items structure, even if the user deletes messages from the client. For Teams, this means private 1:1 and group chat compliance records associated with that user are retained and remain available for discovery, investigation, and legal review according to the hold configuration. The user may still appear to delete chat content from their Teams interface, but the held copy is preserved and cannot be permanently removed by the user while the hold applies. This is the appropriate control when the requirement is to prevent permanent deletion for a specific user's private Teams chats. Microsoft documents Litigation Hold as a mailbox-level preservation feature in Exchange Online and describes Teams content as discoverable through Microsoft Purview eDiscovery workflows. See Litigation Hold in Exchange Online and eDiscovery workflow for content in Microsoft Teams.

QUESTION NO: 19

You are working as a Systems Administrator and your organization has recently acquired a subscription to Microsoft 365. All employees have been assigned a Microsoft 365 E3 license. You are tasked with deploying Microsoft Teams to all users within the organization. How can you ensure that only the managers are permitted to create teams in Microsoft Teams? What is the first step you should take?

A. Add all the managers to a Microsoft Team.

B. Add all the managers to a universal distribution group.

C. Add all the managers to an Office 365 group.

D. Add all the managers to a universal security group.

ANSWER: D

Explanation:

Add all the managers to a universal security group is correct because team creation in Microsoft Teams is governed by Microsoft 365 group creation. When a user creates a team, Microsoft Teams creates an underlying Microsoft 365 group and associated resources. To limit team creation to a defined set of users, Microsoft recommends creating or using a group that contains only the permitted users, then configuring Microsoft Entra ID group settings so only members of that group can create Microsoft 365 groups. In this scenario, the first practical step is to collect all managers into a universal security group so that the permission can be assigned centrally and maintained easily as managers join or leave the organization. After that, an administrator can use PowerShell to set group creation restrictions, including disabling general group creation and specifying the allowed group by using the group's object ID. Microsoft documents this approach in its guidance for controlling Microsoft 365 group creation and explains that Teams depends on Microsoft 365 groups for team-backed collaboration resources. See Manage who can create Microsoft 365 Groups and Microsoft 365 Groups and Microsoft Teams.

QUESTION NO: 20

Your company has a Microsoft 365 subscription that contains three groups named HR, Marketing, and Sales.

You need to configure the Microsoft Teams desktop client. The solution must meet the following requirements:

Members of the HR group must be prevented from pinning apps to their app bar.

Members of the Marketing group must have the Microsoft Planner app pinned to their app bar.

Members of the Sales group must not be affected by policies applied to the Marketing and HR groups.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Modify the global app setup policy.

B. Modify the global app permission policy.

C. Create an app setup policy for HR.

D. Create an app setup policy for Marketing.

E. Create an app permission policy for Marketing.

F. Create an app permission policy for HR.

ANSWER: C D

Explanation:

Create an app setup policy for HR and Create an app setup policy for Marketing are correct because Teams app setup policies control the apps that are pinned to the Teams app bar and whether users are allowed to pin their own apps. For the HR group, a dedicated app setup policy can be configured with user pinning turned off, which prevents members of that group from pinning apps to the app bar. For the Marketing group, a separate app setup policy can define the pinned apps list and include Microsoft Planner so that it appears on the app bar for those users. These policies can then be assigned directly to the relevant Microsoft 365 groups, ensuring that only HR and Marketing members receive the intended Teams client configuration. Since the Sales group is not assigned either policy, its members are not affected by the HR or Marketing-specific settings. Microsoft documents app setup policies as the mechanism for managing pinned apps and user pinning in Teams, and group policy assignment is supported for targeting policies to specific groups. See Manage app setup policies in Microsoft Teams and Assign policies to users and groups in Microsoft Teams.

QUESTION NO: 21 - (SIMULATION)

Task 8

You need to prevent guest users from calling your company ' s Teams users.

ANSWER: See Explanation Below For Answer

Explanation:

To prevent guest users from calling your company’s Teams users, the correct control is the **Make private calls** setting in the **Guest access** configuration of the Microsoft Teams admin center. Guest access settings define what external guest accounts can do after they have been added to the tenant, including whether they can use calling features inside Teams. When **Make private calls** is disabled, guest users are blocked from placing peer-to-peer Teams calls to people in the organization, which directly satisfies the requirement in the task.

The setting is managed by going to the **Microsoft Teams admin center**, opening **Users**, and then selecting **Guest access**. In that page, the calling-related control is the toggle labeled **Make private calls**. Turning this toggle off and saving the change applies the restriction for guest users. This is the intended administrative location because guest communication capabilities are not controlled by a standard user policy for internal users; they are controlled from the tenant-level guest access settings.

Microsoft documents guest access settings in Teams as the place where administrators configure guest permissions, including calling and meeting capabilities. The guest access configuration is described in Microsoft’s Teams guest access documentation, and the Teams admin center is the supported portal for managing these settings. Selecting the **Make private calls** toggle and setting it to **Off** prevents guests from initiating private Teams calls while still allowing other guest access features to remain configured according to the organization’s requirements.

QUESTION NO: 22 - (HOTSPOT)

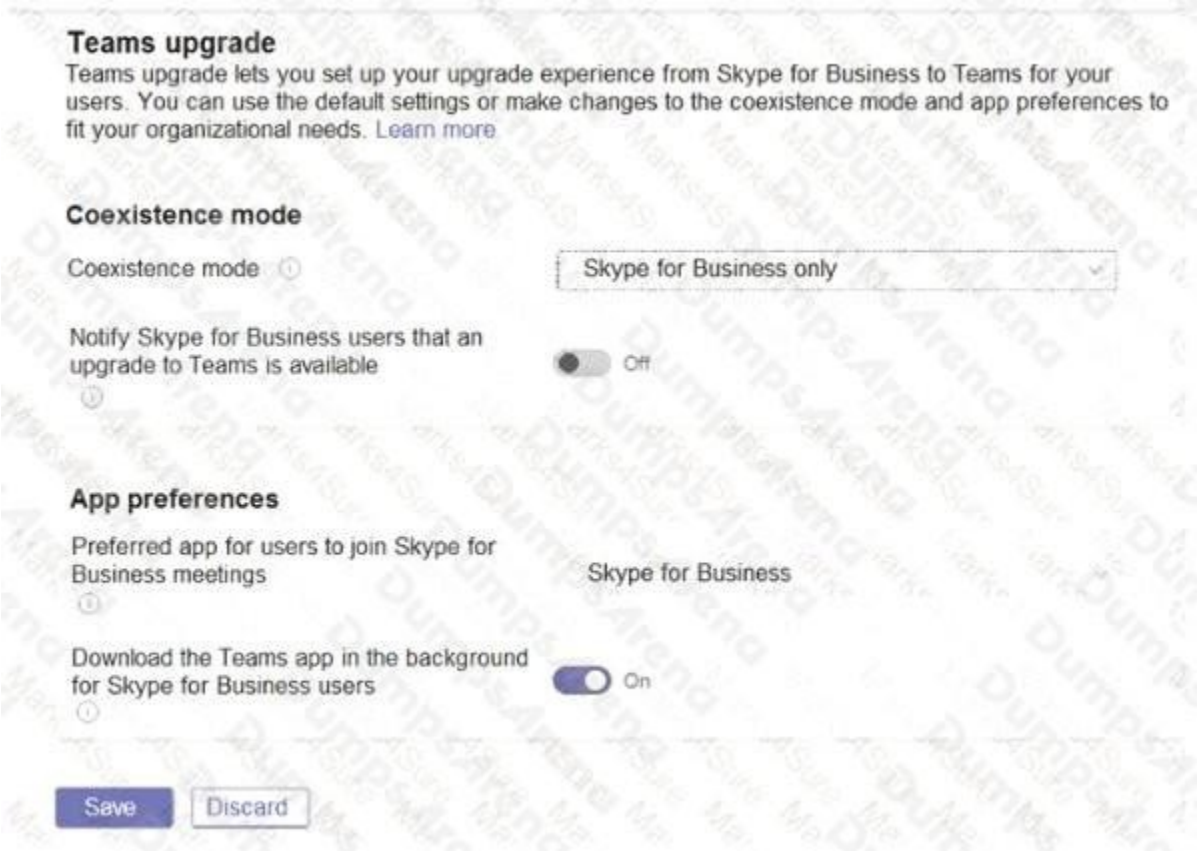
HOTSPOT

Your company uses Microsoft Skype for Business Online and Microsoft Teams.

All Skype for Business Online users can make and receive PSTN calls. Microsoft Teams is configured for PSTN calls.

You plan to upgrade the Skype for Business Online users to Microsoft Teams.

The Teams upgrade settings are configured as shown in the Teams upgrade exhibit. (Click the Teams upgrade tab.)



You apply TeamsUpgradePolicy to the user accounts of the company's R & D and human resources (HR) departments by using the coexistence modes shown in the following table.

Department	Coexistence mode
R&D	TeamsOnly
HR	SfbWithTeamsCollabAndMeetings

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Users in the R&D department will not be able to join Skype for Business Online meetings.	○	○
Existing Skype for Business Online meetings scheduled by users in the HR department will migrate automatically to Microsoft Teams.	○	○
Users in the HR department will be able to make and receive PSTN calls by using Microsoft Teams.	○	○

ANSWER:

Statements	Yes	No
Users in the R&D department will not be able to join Skype for Business Online meetings.	○	●
Existing Skype for Business Online meetings scheduled by users in the HR department will migrate automatically to Microsoft Teams.	●	○
Users in the HR department will be able to make and receive PSTN calls by using Microsoft Teams.	○	●

Explanation:

The correct selections are **No**, **Yes**, and **No**. In Microsoft Teams coexistence, the user-level TeamsUpgradePolicy assigned to a user determines that user's effective coexistence behavior. For the R&D department, the assigned mode is **TeamsOnly**. A TeamsOnly user uses Teams as the primary client for chat, calling, and scheduling meetings, but that does not prevent the user from joining Skype for Business meetings. Microsoft's coexistence guidance explains that TeamsOnly users can still participate in Skype for Business meetings, so the statement saying that R&D users will not be able to join Skype for Business Online meetings is not true. See Microsoft's coexistence mode details here: Teams and Skype for Business coexistence and interoperability.

For the HR department, the assigned mode is **SfbWithTeamsCollabAndMeetings**. In this mode, Teams is used for collaboration and meetings. When users are moved into this meetings-focused Teams mode, the Meeting Migration Service can automatically convert existing future Skype for Business meetings organized by those users into Teams meetings. This is why the existing Skype for Business Online meetings scheduled by HR users will migrate automatically to Microsoft Teams. Microsoft documents the meeting migration behavior here: Meeting Migration Service for Microsoft Teams.

However, **SfbWithTeamsCollabAndMeetings** does not move calling workloads to Teams. Users in that mode retain Skype for Business for chat and calling while using Teams for collaboration and meetings. Because PSTN calling is part of the calling workload, HR users in this mode would not make and receive PSTN calls by using Microsoft Teams.

QUESTION NO: 23

You need to configure the user accounts of the sales department users to meet the security requirements. What should you do for each user?

A. From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName SfBWithTeamsCollabAndMeetings cmdlet.

B. From the Microsoft Teams admin center, set the Microsoft Teams upgrade policy to Islands coexistence mode.

C. From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName Islands cmdlet.

D. From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName SfBOnly cmdlet.

ANSWER: A

Explanation:

From PowerShell, run the Grant-CsTeamsUpgradePolicy -PolicyName SfBWithTeamsCollabAndMeetings cmdlet is correct because the Skype for Business with Teams Collaboration and Meetings mode, also known as Meetings First, keeps Skype for Business as the client for chats and calls while allowing Teams for collaboration and meeting scheduling. This is the appropriate per-user coexistence configuration when users must be restricted from using Teams for peer-to-peer chat or calling but still need to use Teams capabilities such as channels and meetings. Microsoft supports assigning Teams upgrade modes at the user level by using the Grant-CsTeamsUpgradePolicy cmdlet, which is why this action fits the requirement to configure each sales department user account individually. The SfBWithTeamsCollabAndMeetings policy is one of the built-in Teams upgrade policy instances documented by Microsoft for managing coexistence and migration from Skype for Business to Teams. See Microsoft's guidance on Teams and Skype for Business coexistence and the Grant-CsTeamsUpgradePolicy cmdlet reference.

QUESTION NO: 24

You have a Microsoft 365 subscription and you have created an organization-wide team named Team1. Users User1 and User2 own Team1. To configure Team1 to comply with the following requirements, which two actions should be taken through the Microsoft Teams client? Each correct action is part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Team1 settings, clear Give members the option to edit their messages

B. From the General Channel settings of Team1, set the channel moderation preference to Anyone can post; show alert that postings will notify everyone (recommended for large teams)

C. From the General Channel settings of Team1. set the channel moderation preference to Only owners can post messages.

D. From the Team1 settings, disable all the Fun stuff settings.

E. From the Team1 settings, set Show members the option to @team or @[team name] to Off.

ANSWER: C E

Explanation:

For an organization-wide team, Microsoft recommends carefully controlling broad communication features because membership can include every user in the tenant. "From the General Channel settings of Team1. set the channel moderation preference to Only owners can post messages." is correct because channel moderation lets team owners restrict posting in a channel so that only owners can create new messages. This is commonly used for the General channel in large or org-wide teams when the channel should function as a controlled announcement space rather than an open discussion area. "From the Team1 settings, set Show members the option to @team or @[team name] to Off.

" is also correct because disabling team mentions prevents regular members from notifying the entire org-wide team with an @team or @[team name] mention. That helps reduce unnecessary tenant-wide notifications while still allowing owners to manage important communications. These settings are available from the Microsoft Teams client by using the team's settings and the General channel moderation settings. Microsoft documents org-wide team behavior and recommended management considerations in Create an org-wide team in Microsoft Teams and describes team member permissions and mentions in Change member permissions in Teams.

QUESTION NO: 25

You are managing a Microsoft 365 subscription for the domain contoso.com, which utilizes Microsoft Teams. Your objective is to enable Microsoft Teams users to perform the following functions:

Search for customers who use Skype (Consumer).
Initiate a Skype chat with these customers.

Which two actions should you take? Each correct answer forms part of the solution. NOTE: Each correct choice is worth one point.

A. From the Microsoft Teams admin center, turn on external access.

B. From the Azure portal, configure Azure AD B2C.

C. Add a _sipinternaltls SRV record to the contoso.com DNS domain.

D. From the Microsoft Teams admin center, turn on guest access.

E. Add a _sipfederationtls SRV record to the contoso.com DNS domain.

ANSWER: A E

Explanation:

To let Microsoft Teams users find and chat with Skype consumer users, you must enable Teams external access for Skype users and ensure the domain has the required federation DNS record. From the Microsoft Teams admin center, turn on external access is correct because Teams uses external access settings to control communication with users outside the organization, including Skype consumer users. In the Teams admin center, this is managed under external access by enabling communication with Skype users, allowing Teams users to search for Skype users and start chats with them. Microsoft documents this capability as part of external access management for Teams: Manage external access in Microsoft Teams.

Add a _sipfederationtls SRV record to the contoso.com DNS domain is also correct because Teams/Skype federation relies on SIP federation discovery for the organization's custom domain. The _sipfederationtls._tcp SRV record points federation traffic to Microsoft's online federation service and is one of the required DNS records used for Skype for Business/Teams interoperability and external federation scenarios. Microsoft lists this SRV record among the required DNS records for Microsoft 365 domains that support Skype for Business and federation services: Create DNS records for Microsoft 365.

QUESTION NO: 26

Your company has implemented a Quality of Service (QoS) solution across its network. Recently, Microsoft Teams was deployed for all users, each utilizing a domain-joined computer running Windows 10. However, users are experiencing poor audio quality while using Microsoft Teams from the company network. Upon investigation, it was found that media traffic from Microsoft Teams is not being handled by the QoS solution. You need to ensure that all media traffic is correctly managed by the QoS solution. Which two actions should you perform to resolve this issue? **Note:** Each correct selection will earn you one point and together they complete the solution.

A. From the Microsoft Teams admin center, set Insert Quality of Service (QoS) markers for real-time media traffic to On.

B. From the Microsoft Teams client, select a certified Microsoft Teams audio device.

C. From PowerShell, run the Set-CsQoEConfiguration cmdlet.

D. From Group Policy Management, create a Group Policy Object (GPO) that contains the Policy-based QoS settings, and then link the GPO to the domain.

E. From the Microsoft Teams admin center, turn on logging for the device configuration profile.

ANSWER: A D

Explanation:

To make Microsoft Teams media traffic work with an existing QoS implementation, Teams must be configured to mark real-time media packets and Windows clients must be configured to apply the correct DSCP markings through policy. Setting "Insert Quality of Service (QoS) markers for real-time media traffic" to On in the Microsoft Teams admin center enables Teams to insert QoS markers for real-time audio, video, and screen sharing traffic. This is required so Teams traffic can be identified and prioritized by the network QoS configuration. Because the users are on domain-joined Windows 10 computers, creating a Group Policy Object that contains Policy-based QoS settings and linking it to the domain is the appropriate way to deploy the DSCP settings consistently across managed clients. Microsoft's guidance for Teams QoS specifically describes

enabling QoS markers in Teams and using Group Policy-based QoS for Windows clients to assign DSCP values to Teams media traffic. See Implement Quality of Service in Microsoft Teams and Meeting settings in Microsoft Teams.

QUESTION NO: 27

You need to resolve the notification issues identified during the pilot project. What should you modify?

A. the global meeting policy

B. the global messaging policy

C. the org-wide Teams settings

D. the app permission policy

ANSWER: B

Explanation:

The correct choice is **the global messaging policy**. In Microsoft Teams, messaging policies control user chat and channel messaging capabilities, including whether users can send urgent messages by using priority notifications. Priority notifications repeatedly alert recipients for a defined period, so notification behavior tied to chat messages is managed through Teams messaging policy settings rather than meeting, app, or general organization settings. If the affected pilot users are using the default policy, modifying the global messaging policy is the appropriate administrative action because the global policy applies to users who do not have a custom messaging policy assigned. In the Teams admin center, this is managed under *Messaging policies*, where administrators can configure chat-related features such as priority notifications and other messaging experiences. Microsoft documents these controls in the Teams messaging policy guidance, including the setting for sending urgent messages with priority notifications: Manage messaging policies in Teams. Microsoft also describes priority notifications as a Teams messaging feature intended for urgent chat messages: Mark a message as important or urgent in Microsoft Teams.

QUESTION NO: 28 - (HOTSPOT)

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Teams.

You need to meet the following requirements:

- Users must be able to join meetings by dialing a phone number.
- Users must be able to apply custom branded meeting lobbies. - Auto attendants and call queues must be implemented.

Which Microsoft Teams feature should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Join meetings by dialing a phone number:
- Calling Plans
- Audio Conferencing
- Microsoft Teams Rooms
- Advanced Communications

Implement auto attendants and call queues:
- Calling Plans
- Communication credits
- Microsoft Teams Rooms
- Advanced Communications

Apply custom branded meeting lobbies:
- Communication credits
- Microsoft Teams Rooms
- Advanced Communications
- Microsoft 365 Audio Conferencing

ANSWER:

Answer Area

Join meetings by dialing a phone number:
- Calling Plans
- **Audio Conferencing**
- Microsoft Teams Rooms
- Advanced Communications

Implement auto attendants and call queues:
- **Calling Plans**
- Communication credits
- Microsoft Teams Rooms
- Advanced Communications

Apply custom branded meeting lobbies:
- Communication credits
- Microsoft Teams Rooms
- **Advanced Communications**
- Microsoft 365 Audio Conferencing

Explanation:

The correct selections align with the Teams features used for each required capability. Audio Conferencing is the Teams meeting add-on that allows meeting organizers to include dial-in phone numbers in meeting invitations so participants can join a Teams meeting by calling from a regular telephone. This is specifically intended for users who cannot use the Teams

client or need PSTN dial-in access to meetings. Microsoft describes this capability in the Teams Audio Conferencing documentation: Audio Conferencing in Microsoft Teams.

For auto attendants and call queues, the appropriate selection from the available choices is Calling Plans. Auto attendants and call queues are part of Teams voice/PSTN calling scenarios and require phone numbers and calling connectivity so callers can be routed through menus, greetings, queues, and agents. Calling Plans provide Microsoft-managed PSTN connectivity and phone numbers that can be used with Teams calling features. Microsoft's guidance for these voice features is available here: Set up a cloud auto attendant and Create a call queue.

Advanced Communications is the correct choice for applying custom branded meeting lobbies in this exam context. The Advanced Communications add-on included enhanced meeting customization and branding capabilities, including custom meeting lobby experiences, which let organizations apply corporate branding to Teams meeting join and lobby screens. This matches the requirement to allow custom branded meeting lobbies. Microsoft's Teams add-on licensing information describes Advanced Communications and related advanced meeting capabilities here: Microsoft Teams Advanced Communications add-on.

QUESTION NO: 29

Your company has a Microsoft 365 subscription that includes Microsoft Teams. You have purchased an application named App1 from the Microsoft Teams Store, and you need to deploy this app to a specific group of users within the Microsoft Teams client. What are the two actions you should perform using the Microsoft Teams admin center to achieve this? Each correct answer contributes to the solution.

Note: Each correct selection is worth one point.

A. From the Meeting settings, modify the Network settings.

B. From App setup policies, create a new app setup policy.

C. From App setup policies, modify the global app setup policy.

D. From the properties of each user, edit the assigned policies.

E. From the Teams settings, modify the Devices settings.

ANSWER: B D

Explanation:

To deploy App1 to a targeted set of users in the Microsoft Teams client, the correct actions are **From App setup policies, create a new app setup policy.** and **From the properties of each user, edit the assigned policies.** Teams app setup policies are used to control which apps are installed and pinned for users in Teams. By creating a dedicated app setup policy, you can add App1 as an installed app and optionally pin it so that users see it in the Teams app bar or relevant app experience. This provides a controlled way to make the purchased Teams Store app available only to the intended audience rather than applying it tenant-wide.

After the app setup policy is created, it must be assigned to the intended users. In the Teams admin center, one supported way to do this is by opening each user's properties and editing the assigned policies so that the custom app setup policy applies to them. Microsoft documents that app setup policies can be created and assigned to users to manage app installation and pinning behavior in Teams. See Manage app setup policies in Microsoft Teams and Assign policies to users and groups in Microsoft Teams.

QUESTION NO: 30

Users are reporting poor audio quality during Microsoft Teams conferences. You conduct a network trace from a user's device during an audio conference, as depicted in the following exhibit. What is the most likely cause of the audio quality issue?

[IMAGE_1_OCR_EXTRACTED_TEXT_START] Frame Details: ---------- Checksum: 0 (0x0) SourceAddress: 10.10.10.110 DestinationAddress: 52.114.188.31 ---------- O-Tcp: Flags=...A...., SrcPort=50008, DstPort=HTTPS(443), PayloadLen=0, SrcPort: 50008 DstPort: HTTPS(443) SequenceNumber: 4077031237 (0xF3028F45)

E AcknowledgementNumber: 223214542 (0xD4DFD5E) E B DataOffset: 80 (0x50) O Flags: ...A ---------- Window: 1025 (scale factor 0x8) = 262400 Checksum: 0x524, Disregarded UrgentPointer: 0 (0x0) ----------
[IMAGE_1_OCR_EXTRACTED_TEXT_END]

A. The source port range for audio is too narrow.

B. The source port for audio is above 50,000.

C. The UDP traffic is being limited.

D. The TLS traffic is being limited.

ANSWER: C

Explanation:

The UDP traffic is being limited is correct because Microsoft Teams real-time media, including audio, is designed to use UDP whenever possible. UDP is preferred for conferencing media because it avoids the retransmission and ordering behavior of TCP, which can add latency, jitter, and noticeable audio degradation during live calls. In the trace, the Teams media session is shown using TCP to destination port HTTPS(443). That is a strong indicator that the client could not use the preferred UDP media path and has fallen back to TCP 443. Microsoft's Teams network guidance recommends allowing UDP traffic for Teams media, including the defined client media port ranges, and emphasizes that forcing media over TCP can reduce call quality. When users report poor audio quality and a packet capture shows Teams audio using TCP 443 instead of UDP, the most likely cause is that UDP is blocked, restricted, or otherwise limited somewhere along the network path. See Microsoft's guidance on preparing the network for Teams at Prepare your organization's network for Microsoft Teams and Teams network requirements at Microsoft 365 and Teams network optimization.

QUESTION NO: 31

This question belongs to a series where a common scenario is provided. Each question in the series poses a unique solution that may or may not fulfill the given goals. Some sets may possess multiple correct solutions, but others may have no correct solutions at all. Once you've answered a question in this section, you cannot revisit it. Consequently, these questions will not be visible on the review screen.

Consider a Microsoft 365 subscription containing multiple SharePoint Online sites. Your task is to make the content from a modern SharePoint team site named 'Sales' accessible via Microsoft Teams. It is crucial that upon the addition of a new channel within a team, a corresponding folder is automatically generated within the Sales site.
Proposed Solution: Utilize the 'Create a Team' feature directly from the Sales site.
Does the proposed solution meet the intended goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. Creating a Microsoft Team directly from the modern SharePoint team site connects Teams to the existing Microsoft 365 group and its associated SharePoint site, rather than creating a completely separate SharePoint location for Teams files. This makes the Sales site content available through Microsoft Teams, particularly through the Files experience for channels. In Teams, files shared in a standard channel are stored in SharePoint, and each standard channel maps to a folder in the team's default document library. Therefore, when a new standard channel is added to the team, Teams automatically creates the corresponding folder in the connected Sales SharePoint site, satisfying the requirement. Microsoft's guidance describes creating a team from SharePoint as a supported way to bring an existing SharePoint team site into Teams, and Teams file storage documentation confirms that channel files are stored in SharePoint. See Create a Microsoft Team from SharePoint and Location of data in Microsoft Teams.

QUESTION NO: 32

Your company has a Microsoft 365 subscription that utilizes Phone System and Calling Plans. You are planning to set up a toll phone number for the helpdesk. The helpdesk phone number must have the following capabilities:

Include a greeting and hold music.
Bypass menu options when a call is routed to the helpdesk.

What two resources should you create to achieve these requirements? Each correct answer is a part of the solution.

Note: Each correct selection is worth one point.

A. a call queue

B. a call park

C. an auto attendant

D. a resource account

E. a calling policy

ANSWER: A D

Explanation:

A call queue is the right Teams Phone resource for a helpdesk number when callers should be routed directly to a group of agents without having to choose menu options. Microsoft Teams call queues support a custom greeting, music on hold while callers wait, agent routing methods, overflow handling, and timeout handling, making them well suited for service desks and support lines. To make the call queue reachable from the Public Switched Telephone Network by using a toll number, you also need a resource account. In Teams, resource accounts represent non-user voice applications such as call queues and auto attendants, and the phone number is assigned to the resource account that is associated with the call queue. Together, a call queue and a resource account satisfy the requirement to publish a toll helpdesk number with greeting and hold music while sending callers straight into the helpdesk routing experience. See Microsoft's guidance for creating Teams call queues and managing resource accounts.

QUESTION NO: 33

Your company has 10 offices in North America and Europe.

The company has 5,000 users.

You plan to deploy Microsoft Teams for all the users.

You run a pilot project for the planned deployment.

You need to identify the network packet loss from the pilot computers to Microsoft Teams during calls.

Solution: From the Microsoft Teams admin center, you review Usage reports.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because Microsoft Teams usage reports are intended to show adoption and activity metrics, such as active users, meetings, calls, chat messages, and channel activity. They do not provide the technical media-quality telemetry needed to identify packet loss from pilot computers during Teams calls. Packet loss is a call-quality metric, so the appropriate tools are Call analytics for investigating individual users or specific calls, or the Call Quality Dashboard for aggregated quality trends across locations, networks, devices, and time periods. In the Teams admin center, Call analytics

can expose detailed call-session information such as network, device, and media stream data, including packet loss, jitter, round-trip time, and other indicators that help diagnose poor call quality. For a pilot deployment where the goal is to validate network readiness and identify packet loss during calls, reviewing usage reports would not meet the requirement. Microsoft documents usage reports as activity and adoption reporting, while call quality troubleshooting is handled through Teams call analytics and CQD. See Microsoft Teams reports in the Teams admin center and Use Call Analytics to troubleshoot poor call quality in Microsoft Teams.

QUESTION NO: 34

Your organization has a Microsoft 365 subscription, which includes Microsoft Office 365 E5 licenses and Azure Active Directory Premium Plan 1 licenses. Within this subscription, there is a team named 'Sales' that encompasses all employees in the sales department.

Recently, several new staff members were employed in the sales department, but it has come to your attention that these new employees have not been automatically added to the 'Sales' team.

What steps should you take to ensure that when new sales department employees are hired, they are automatically added to the team?

A. From the Microsoft Teams client, modify the settings of the Sales team.

B. From the Azure Active Directory admin center, modify the membership type of the Sales group.

C. From the Microsoft Teams admin center, modify the properties of the Sales team.

D. From the Microsoft 365 admin center, modify the settings of the Sales group.

ANSWER: B

Explanation:

From the Azure Active Directory admin center, modify the membership type of the Sales group is correct because a Microsoft Teams team is backed by a Microsoft 365 group, and automatic team membership is implemented by configuring that underlying group with dynamic user membership. With Azure Active Directory Premium Plan 1, now Microsoft Entra ID P1, the organization can use dynamic membership rules such as a rule based on the user's department attribute, for example identifying users whose department equals Sales. When new employees are created or updated with the matching department value, Microsoft Entra ID evaluates the rule and automatically adds them to the Microsoft 365 group, which in turn adds them to the associated team. This is the intended Microsoft-supported method for keeping a department-based team synchronized with user attributes without manual owner or administrator action. Microsoft documents dynamic membership for Teams and the use of dynamic rules for groups in Microsoft Entra ID. See Microsoft Teams dynamic membership and dynamic membership rules for groups.

QUESTION NO: 35

You have a Microsoft 365 subscription which includes two users, User1 and User2, who are both set up for Microsoft Teams calling.

User1 will be on leave for two weeks and you are required to ensure that User2 receives notifications for all calls directed to User1 during this period.

Which **two** actions should be taken to accomplish this task? Each correct answer forms a part of the solution.

Note: Each correct selection is worth one point.

A. From Voice, add User2 to group call pickup.

B. From Voice, add User1 to group call pickup.

C. From Policies, modify the voice routing policy.

D. From the Microsoft Teams admin center, modify the settings of User2.

E. From the Microsoft Teams admin center, modify the settings of User1.

ANSWER: A E

Explanation:

To have User2 receive notifications for calls made to User1 while User1 is away, User2 must be added to User1's group call pickup configuration, and User1's call settings must be configured to use that group for incoming calls. In Microsoft Teams, group call pickup, also called a call group, lets a user share incoming call alerts with selected people so that those people can answer calls on the user's behalf. Therefore, "From Voice, add User2 to group call pickup." is correct because User2 needs to be a member of the call group associated with User1. "From the Microsoft Teams admin center, modify the settings of User1.
" is also correct because the call handling rule belongs to the user receiving the original calls, which is User1. The administrator can configure User1's call answering rules to also ring or forward to the call group. Microsoft documents this functionality in the Teams Phone guidance for call sharing and group call pickup and in the Teams admin center guidance for managing user call settings.

QUESTION NO: 36

You have a Microsoft 365 subscription that includes Teams. The subscription contains a user named User1. You are deploying 10 new Teams devices.

You need to ensure that User1 can restart the Teams devices remotely.

Solution: You assign the Teams Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. The Teams Administrator role provides broad administrative access in Microsoft Teams, including the ability to manage Teams-certified devices from the Teams admin center. Microsoft documents that Teams administrators can access administrative features for Teams and manage Teams devices, while device management tasks in the Teams admin center include actions such as restarting devices remotely. Because the requirement is simply to ensure that User1 can restart the Teams devices remotely, assigning the Teams Administrator role is sufficient to meet the goal. In a production environment, the Teams Devices Administrator role may often be preferred when following least-privilege principles for device-only administration, but the Teams Administrator role still includes the necessary permissions. Microsoft's role documentation describes the Teams Administrator role and its Teams admin center capabilities, and the Teams device management documentation describes managing Teams devices through the admin center. See Use Microsoft Teams administrator roles to manage Teams and Manage your devices in Microsoft Teams.

QUESTION NO: 37

You are planning to deploy Microsoft Teams to a remote location and have conducted a network readiness assessment using the Network Testing Companion. Which two tests are part of this assessment? Each correct answer is worth one point.

A. trace route information

B. video quality tests

C. open and blocked ports

D. audio quality tests

E. Quality of Service (QoS) validation

ANSWER: C D

Explanation:

The correct tests are open and blocked ports and audio quality tests. The Network Testing Companion was commonly used as a graphical companion for Microsoft's Teams/Skype for Business network assessment tooling, and its purpose was to validate whether a location was ready for real-time Teams media. A key part of that readiness check is confirming connectivity to the required Microsoft Teams media services, including whether required ports and protocols are reachable rather than blocked by firewalls, proxies, or network security devices. Another key part is media quality validation for audio, where the test measures conditions that directly affect Teams calls, such as latency, packet loss, and jitter. These results help determine whether users at the remote location can sustain acceptable Teams audio experiences before rollout. Microsoft's Teams network guidance emphasizes validating required network paths and media quality targets as part of preparing a network for Teams deployment. See Prepare your organization's network for Microsoft Teams and Quality of Service in Microsoft Teams.

QUESTION NO: 38

You have a Microsoft 365 E5 subscription that is associated with an Azure Active Directory (Azure AD) tenant. Within this tenant, the following groups are available:

Name	Type
Group1	Distribution
Group2	Security
Group3	Microsoft 365
Group4	Mail-enabled security

Your task involves creating a new team using the Microsoft Teams client.

Which group can be used to create this new team?

A. Group4

B. Group1

C. Group2

D. Group3

ANSWER: D

Explanation:

Group3
is the correct answer because a team in Microsoft Teams is backed by a Microsoft 365 group. When you create a team from an existing group in the Teams client, the existing group must be a Microsoft 365 group, because Teams uses that group for membership, identity, and the connected Microsoft 365 resources such as the SharePoint site, shared mailbox, Planner plan, and other group-connected services. In the scenario, Group3 is explicitly listed as the Microsoft 365 group, so it is the group that can be selected and converted into a team from the Teams client.

This behavior is documented by Microsoft in the guidance for creating a team from an existing group, which states that users can create a team from an existing Microsoft 365 group. Microsoft's Teams overview also explains that a team is built on a Microsoft 365 group and uses that group to manage access to shared resources. See Create a team from an existing group and Microsoft 365 Groups and Microsoft Teams.

QUESTION NO: 39

You have a Microsoft 365 subscription with two users, User1 and User2, who are both configured for Microsoft Teams calling. User1 is scheduled to be on leave for two weeks. Your task is to make sure User2 receives notifications for all calls directed to User1 during this period. What two actions should you take to achieve this? Each correct answer is part of the overall solution.

Note: Each correct selection is worth one point.

A. From Voice, add User2 to group call pickup.

B. From Voice, add User1 to group call pickup.

C. From Policies, modify the voice routing policy.

D. From the Microsoft Teams admin center, modify the settings of User2.

E. From the Microsoft Teams admin center, modify the settings of User1.

ANSWER: A E

Explanation:

The correct actions are to add User2 to group call pickup and modify the settings of User1 in the Microsoft Teams admin center. In Teams Phone, call handling settings are configured for the user who receives the original call. Because calls are directed to User1, User1's call answering rules must be changed so that calls can also ring, or be routed to, a call group. Adding User2 to group call pickup makes User2 a member of that call group, allowing User2 to be notified when User1 receives calls and to answer them during User1's leave. This aligns with how Teams manages user call settings: admins can configure call forwarding, simultaneous ringing, unanswered call handling, delegates, and call groups for a specific user. Microsoft documents these settings in the Teams admin center user call settings guidance, and the same configuration can also be managed through Teams PowerShell calling settings. See Manage user call settings in Microsoft Teams and Set-CsUserCallingSettings.

QUESTION NO: 40

Your organization has a Microsoft 365 subscription. You need to enable users from a partner organization named Contoso, Ltd. to collaborate with your company's users in Microsoft Teams. The solution must ensure that Contoso users can engage in chat conversations within channels.

Which three actions should you take prior to adding the Contoso users to Teams? Each correct choice constitutes a portion of the solution.

NOTE: Each correct selection is worth one point.

A. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group members outside the organization access group content to On.

B. From the Guest access settings in the Microsoft Teams admin center, set Allow guest access in Microsoft Teams to On.

C. From the External collaboration settings in the Azure Active Directory admin center, add Contoso's domain to the list of target domains.

D. From the External access settings in the Microsoft Teams admin center, add Contoso's domain to the Allowed list of domains.

E. From the External collaboration settings in the Azure Active Directory admin center, set Guest users permissions are limited to No.

F. From the Services & add-ins settings in the Microsoft 365 admin center, set Let group owners add people outside the organization to groups to On.

ANSWER: A B F

Explanation:

To let Contoso users participate in Teams channel conversations, they must be added as guests to teams, and the tenant must allow guest access across both Teams and the underlying Microsoft 365 Groups service. Setting **Allow guest access in Microsoft Teams** to On enables guest capabilities in Teams, including participation in team and channel experiences according to the configured guest permissions. Because every team is backed by a Microsoft 365 group, the Microsoft 365 Groups guest settings must also allow external users to be added and to access group resources. Enabling **Let group owners add people outside the organization to groups** permits team or group owners to invite Contoso users as guests. Enabling **Let group members outside the organization access group content** allows those guests to access the group-backed content that Teams relies on, including collaboration experiences associated with the team. Microsoft documents these dependencies for Teams guest collaboration and Microsoft 365 Groups guest access in Guest access in Microsoft Teams and Collaborate with guests in a team.

QUESTION NO: 41

You have a Microsoft 365 E5 subscription with Phone System enabled for all Microsoft Teams users.

You need to configure the Phone System to satisfy the following requirements:

Implement call management functionalities such as greeting and call transferring.
Ensure that calls are distributed to specific users or groups efficiently.

Which two resources should you create? Each correct answer contributes to providing a complete solution.

NOTE: Each correct selection is worth one point.

A. a call park policy

B. a call queue

C. a voice routing policy

D. a group call pickup

E. an auto attendant

F. a calling policy

ANSWER: B E

Explanation:

A call queue and an auto attendant are the correct Teams Phone resources for this scenario. An auto attendant provides automated call handling for incoming calls, including playing greetings, presenting menu options, and transferring callers to people, shared voicemail, other auto attendants, or call queues. This directly satisfies the requirement for greeting and call transferring as part of call management. A call queue is used to distribute incoming calls to a defined set of agents, such as specific users, Teams channels, or groups, using routing methods such as attendant routing, serial routing, round robin, or longest idle. This satisfies the requirement to distribute calls efficiently to the right users or groups. In many Teams Phone deployments, an auto attendant is placed in front to greet and direct callers, while the call queue manages the actual distribution of calls to available agents. Microsoft documents these resources as core components for Teams Phone call routing and organizational call handling. See Plan for Teams auto attendants and call queues and Create a call queue in Microsoft Teams.

QUESTION NO: 42

You are the Microsoft Teams administrator for your organization.

The organization has developed a new Microsoft Teams app named App1, which a developer has packaged into a ZIP file.

Your task is to enable the functionality that allows App1 to be uploaded in its ZIP format to Microsoft Teams.

Which application setting should you activate?

A. Allow uploading custom apps.

B. Enable new external apps by default.

C. Enable default apps.

D. Allow external apps in Microsoft Teams.

ANSWER: A

Explanation:

Allow uploading custom apps is correct because a Teams app that is packaged as a ZIP file is treated as a custom app package. Microsoft Teams requires custom app upload, often called sideloading, to be enabled before users or administrators can upload that ZIP package into Teams for testing or organizational use. This setting controls whether custom apps can be uploaded, so enabling it is the required administrative action for App1 to be added from its developer-provided package. In the Teams admin experience, custom app availability can be governed through organization-wide app settings and custom app policies, depending on whether you want to allow the capability broadly or only for selected users. Microsoft's guidance for managing custom app policies and settings explains how admins control custom app upload in Teams, while the Teams app publishing documentation describes uploading an app package as part of deploying or testing a custom Teams app. See Manage custom app policies and settings in Microsoft Teams and Upload your app in Microsoft Teams.

QUESTION NO: 43 - (DRAG DROP)

Your company uses Teams.

All users are assigned a Microsoft 365 E? license.

You need to purchase add-on licenses that will enable the following features for the Teams environment

To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all.

ANSWER:

Explanation:

The correct licensing matches each requested Teams capability to the Microsoft add-on that actually enables that feature set. Data loss prevention for Teams chat and channel messages is part of Microsoft Purview DLP. For users who already have a Microsoft 365 E3-type base license, the needed add-on is Microsoft 365 E5 Compliance because Teams message DLP is an advanced compliance feature governed through Microsoft Purview. Microsoft documents Teams DLP as a Purview DLP workload, and Purview subscription requirements place these advanced compliance features in the E5 compliance licensing family. See Microsoft Purview DLP for Microsoft Teams and Microsoft Purview subscription requirements.

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is part of Microsoft Defender for Office 365. This protection scans files in those collaboration workloads and can block users from opening malicious content. The minimum add-on in the provided choices that enables this functionality is Microsoft Defender for Office 365 Plan 1. Microsoft describes Safe Attachments as a Defender for Office 365 capability, including protection for files in SharePoint, OneDrive, and Teams. See Safe Attachments in Microsoft Defender for Office 365.

Microsoft Purview Information Barriers is also a compliance feature. It is used to restrict communication and collaboration between segments of users, which is especially relevant in Teams for regulated or conflict-sensitive organizations. With a Microsoft 365 E3 base license, the appropriate add-on from the available choices is Microsoft 365 E5 Compliance. Microsoft's Information Barriers documentation identifies the feature as a Microsoft Purview compliance capability. See Microsoft Purview Information Barriers.

QUESTION NO: 44 - (SIMULATION)

Task 11

You need to restrict external Teams communication for both calling and personal chat to only organizational users that use the microsoft.com domain.

ANSWER: See Explanation Below For Answer

Explanation:

The correct place to make this change is the External access configuration in the Microsoft Teams admin center. External access controls whether users in your tenant can find, chat with, and call Teams users in other organizations. To restrict this communication to a single external organization domain, the tenant must be configured to allow only specific external domains, and the permitted domain must be added as **microsoft.com**. After that, Teams external chat and calling are limited to users in that allowed domain, assuming the other organization also allows communication with your tenant.

Because the requirement says communication should be limited to **organizational users**, the configuration should not allow communication with Teams accounts that are not managed by an organization. In the Teams admin center, those unmanaged Teams accounts are controlled separately from the allowed external domain list, so leaving those settings enabled would allow communication outside the requested microsoft.com organizational domain restriction. The key setting for the hotspot is therefore the domain restriction under External access: select the option to allow only specific external domains, add **microsoft.com**, and save the change.

Microsoft documents this under Teams external access management, where administrators can allow all domains, block domains, or allow only specific domains for external Teams communication. See Microsoft's guidance here: Manage external access in Microsoft Teams.

QUESTION NO: 45

You have an Office 365 subscription and you need to ensure that guest users are unable to delete channels in a Microsoft Teams team. Which tool or feature should you utilize to accomplish this task?

A. the Microsoft Teams admin center

B. the Azure portal

C. the Microsoft Teams client

D. the Microsoft 365 security center

ANSWER: C

Explanation:

the Microsoft Teams client is correct because the setting that controls whether guest users can delete channels is configured at the individual team level from within Teams. A team owner can open the team in the Teams client, select the team's more options menu, choose Manage team, and then go to Settings > Guest permissions. From there, the owner can clear the permission that allows guests to create, update, or delete channels. This directly addresses the requirement to prevent guest users from deleting channels in that specific team. Microsoft documents this as a team-level guest permission managed from the Teams interface, rather than as a broad tenant-wide security setting. The same behavior can also be managed through Teams PowerShell for automation, but among the provided choices, the Teams client is the tool that exposes the required setting for team owners. For details, see Microsoft's guidance on setting guest permissions for channels in Teams and the Set-Team PowerShell documentation.

QUESTION NO: 46

Your company has a Microsoft 365 subscription that contains 200 Microsoft Teams users and 20 teams.

You discover that several teams do NOT have an owner.

You need to ensure that you receive a notification when a team is missing an owner.

What should you do?

A. From PowerShell, run the Set-Team cmdlet.

B. From the Microsoft Teams admin center, modify the Teams settings.

C. From PowerShell, run the Add-AzureADMSLifecyclePolicyGroup cmdlet.

D. From the Azure Active Directory admin center, modify the group expiration settings.

ANSWER: D

Explanation:

From the Azure Active Directory admin center, modify the group expiration settings is correct because Microsoft Teams teams are backed by Microsoft 365 groups, and Microsoft Entra ID, formerly Azure Active Directory, provides lifecycle settings for those groups. In the group expiration configuration, you can define an email contact for groups that have no owner. When an ownerless Microsoft 365 group reaches the renewal-notification stage, the notification is sent to the configured contact instead of a group owner. Since each team is associated with a Microsoft 365 group, this setting applies to ownerless teams as well and enables an administrator or designated mailbox to receive the relevant notification. Microsoft documents this behavior in the group lifecycle/expiration policy guidance, including how renewal notifications work for groups without owners. See Configure the expiration policy for Microsoft 365 groups and Manage ownerless Microsoft 365 groups and teams.

QUESTION NO: 47

You need to identify the requirements for the voice pilot project.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Assign an additional license and phone number to each user.

B. Deploy a Session Border Controller (SBC) for Litware.

C. Purchase a Calling Plan for each user.

D. Create a dial plan for Litware.

E. Purchase a Calling Plan for Litware.

ANSWER: A C

Explanation:

To enable users for a Microsoft Teams voice pilot that uses Microsoft Calling Plans, each pilot user must be enabled for Teams Phone capabilities and must have a telephone number assigned. Assign an additional license and phone number to each user is correct because Teams users need the appropriate Teams Phone/Phone System licensing before they can make and receive PSTN calls, and each user who will receive external calls needs an assigned phone number. Purchase a Calling Plan for each user is also correct because Microsoft Calling Plans are licensed at the user level; each user participating in the pilot needs an assigned Calling Plan, unless the organization uses another PSTN connectivity option such as Direct Routing or Operator Connect. Microsoft documents the required setup flow as acquiring phone numbers, assigning licenses, and assigning phone numbers to users for Calling Plan deployments. See Microsoft's guidance for Microsoft Calling Plans and setting up Calling Plans in Teams.

QUESTION NO: 48

Your organization holds a Microsoft 365 subscription, and all employees utilize computers operating on Windows 10 with Microsoft Teams installed. A user is experiencing multiple issues, including the following:

- Their connection drops during screen sharing.
- The time taken for the user selection process is significantly delayed.
- The Microsoft Teams application intermittently crashes and automatically restarts.

You are tasked with accessing the debug logs from Microsoft Teams to resolve these issues. What action will you take?

A. From the Microsoft Teams client, select F1. Open the ETL files in the %Appdata%\Microsoft\Teams\folder.

B. From the Microsoft Teams client, select Ctrl+Alt+Shift+1. Open the log files in the %Userprofile%\Downloads\ folder.

C. From Event Viewer, open the Application log and filter the log for a keyword of MSTeams.

D. Right-click the Microsoft Teams icon in the application tray, and then select Get logs. Open Logs.txt in the %Appdata%\Microsoft\Teams\ folder.

ANSWER: B

Explanation:

From the Microsoft Teams client, select Ctrl+Alt+Shift+1. Open the log files in the %Userprofile%\Downloads\ folder. is correct because Microsoft Teams provides a built-in keyboard shortcut for collecting client debug logs directly from the desktop app. On Windows, pressing Ctrl+Alt+Shift+1 in Teams generates the diagnostic/debug log package and saves it to the user's Downloads folder. Those logs are intended for troubleshooting client-side behavior such as crashes, performance delays, sign-in or user selection issues, and problems that occur during meetings or screen sharing. They give administrators and support engineers detailed client telemetry and diagnostic information without requiring the user to manually locate application folders or export Windows Event Viewer entries. This aligns with Microsoft's documented method for collecting Teams client logs on Windows. For additional troubleshooting, Microsoft also distinguishes between different Teams log types, such as debug logs and media logs, but the requested action here is specifically to access the Teams debug logs. See Microsoft's guidance on Teams log files and related client diagnostics in collecting logs from the Teams client.

QUESTION NO: 49

Your organization has a Microsoft 365 subscription and has deployed Microsoft Teams for 5,000 users. You need to generate a report providing the following details:

The number of active Microsoft Teams users in the past seven days.
The number of active team channels in the past seven days.
Which usage reports should you generate?

A. Teams device usage

B. Teams live event usage

C. Teams user activity

D. Teams usage

ANSWER: D

Explanation:

Teams usage is the correct report because it is designed to summarize how Teams is being used across the organization over a selectable reporting period, including the last 7 days. In the Teams admin center, the Teams usage report provides organization-level and team-level usage metrics such as active users and active channels, which directly match the requested details: the number of active Microsoft Teams users and the number of active team channels during the previous seven days. This report is intended for administrators who need to understand Teams adoption and activity trends across teams and channels, rather than focusing on device platforms, live events, or individual user activity actions. Microsoft documents the Teams usage report as including active users and active channels and explains that it can be generated for time ranges such as 7, 30, 90, and 180 days. See the Microsoft documentation for the Teams usage report and the broader Teams reporting reference.

QUESTION NO: 50

You have a Microsoft 365 E5 subscription that has Phone System enabled for all Microsoft Teams users.

You need to configure the Phone System to meet the following requirements:

▪ Provide a virtual receptionist that connects callers to either a specific user or the help desk. ▪ Route calls to the help desk on a First in, First out (FIFO) order.

Which two resources should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a call park policy

B. a call queue

C. a voice routing policy

D. a group call pickup

E. an auto attendant

F. a calling policy

ANSWER: B E

Explanation:

The correct resources are a call queue and an auto attendant. In Microsoft Teams Phone, an auto attendant provides the virtual receptionist experience. It can answer inbound calls, play greetings and menu prompts, and route callers to destinations such as a specific person, an operator, or another resource such as the help desk. This matches the requirement to connect callers either to a specific user or to the help desk. A call queue is the resource designed to distribute incoming calls to a group of agents, such as help desk staff. Teams call queues hold calls until an agent is available and use routing methods to determine how calls are offered to agents; the queue behavior supports serving callers in arrival order for a help desk scenario. Microsoft also documents auto attendants and call queues as commonly paired resources, where the auto attendant provides call handling and menu navigation, and the call queue manages distribution to agents. See Plan for Teams auto attendants and call queues and Create a call queue in Microsoft Teams.

QUESTION NO: 51

You have a Microsoft 365 E5 subscription and use Microsoft Teams.

A user named User1 reports that Microsoft Teams Meeting Add-in for Microsoft Outlook is unavailable and cannot be installed.

You need to ensure that the add-in can be installed.

What should you do?

A. Validate the Meeting policies settings.

B. Clear the Teams client cache of User1.

C. Validate the Teams policies settings.

D. Instruct User1 to update to the most recent version of the Teams client.

ANSWER: A

Explanation:

Validate the Meeting policies settings is correct because the Teams Meeting Add-in for Outlook can be controlled by Teams meeting policy settings. In the Teams admin center, meeting policies include an Outlook add-in setting that determines whether users can schedule Teams meetings from Outlook. If this setting is disabled for the policy assigned to User1, the add-in experience can be unavailable even if the user has Microsoft Teams and Outlook installed. To resolve the issue, an administrator should review the meeting policy assigned to the user and ensure that the Outlook add-in setting is enabled, along with any related meeting scheduling settings required for the user to create Teams meetings. Microsoft documents this under Teams meeting policy management, where the Outlook add-in setting controls whether Teams meetings can be scheduled from Outlook. See Microsoft Learn: Manage the Teams meeting add-in in Outlook and Microsoft Learn: Meeting policies in Teams.

QUESTION NO: 52

Your organization has a Microsoft 365 subscription, and you need to configure Teams so that only members of the IT group are permitted to create private channels. Which three actions should you perform to achieve this objective? Each correct choice contributes to a single point.

A. Modify the global teams policy.

B. Assign the members of the IT group to the policy.

C. Create a custom teams policy.

D. Run the Set-TeamsChannel cmdlet.

E. Modify the global messaging policy.

F. Create a custom messaging policy.

ANSWER: A B C

Explanation:

To allow only members of the IT group to create private channels, you use Teams policies because private channel creation is controlled by the Teams policy setting that determines whether users can create private channels. Modify the global teams policy so that private channel creation is disabled by default for the broader organization. Then create a custom teams policy in which private channel creation is enabled. Finally, assign the members of the IT group to that custom policy so they receive the exception that permits them to create private channels. This combination follows the standard Teams policy model: the global policy applies to users unless a more specific custom policy is assigned, and a custom policy can be targeted to selected users or groups. Microsoft documents Teams policies and their ability to control private channel creation in the Teams admin center and by policy assignment. See Manage Teams policies in Microsoft Teams and Assign policies to users and groups in Microsoft Teams.