

Dur e : 3 jours soit 21 heures

R f rence : AB-650T00



Public vis  :

Profils concern s

- Administrateurs Microsoft 365
- Administrateurs syst mes et cloud
- Administrateurs Microsoft Entra ID
- Administrateurs s curit  Microsoft
- Administrateurs de collaboration Microsoft 365
- Responsables techniques en charge du d ploiement de Microsoft 365 Copilot et des services d'IA Microsoft

M tiers vis s

- Administrateur Microsoft 365
- Administrateur syst mes et r seaux
- Administrateur cloud Microsoft
- Administrateur s curit  Microsoft
- Ing nieur Modern Workplace
- Consultant Microsoft 365
- Consultant Microsoft Copilot
- Architecte Microsoft 365 junior   interm diaire
- Responsable exploitation Microsoft 365

Niveau attendu

Interm diaire   avanc 

Cette formation s'adresse principalement   des professionnels d j familiers avec l'administration Microsoft 365 et souhaitant d velopper des comp tences d'administration, de gouvernance, de s curit  et de d ploiement des services d'IA Microsoft 365 (Copilot et Agent 365).



Pr -requis :

Pr requis indispensables

- Disposer de connaissances g n rales sur les services Microsoft 365 et leur utilisation en entreprise.
- Comprendre les principes fondamentaux de l'administration informatique (utilisateurs, groupes, droits d'acc s, licences, s curit ).
- Poss der une connaissance de base des environnements Microsoft Entra ID (anciennement Azure Active Directory).
- Avoir d j utilis  les centres d'administration Microsoft 365 ou  tre familier avec leur fonctionnement g n ral.
- Ma triser les fonctions courantes d'un poste de travail Windows et d'un navigateur web.

Pr requis recommand s (non obligatoires mais fortement utiles)

- Avoir une premi re exp rience de l'administration Microsoft 365.
- Conna tre les concepts de cybers curit , d'authentification multifacteur (MFA) et d'acc s conditionnel.
- Poss der des notions de PowerShell ou d'automatisation Microsoft Graph.
- Avoir une connaissance g n rale des solutions Microsoft Teams, SharePoint Online et Exchange Online.



Objectifs p dagogiques :

  l'issue de la formation, le participant sera capable de :

- Configurer et administrer un tenant Microsoft 365 ainsi que ses principaux param tres organisationnels.
- G rer les identit s, les acc s, les r les administratifs et les licences au sein d'un environnement Microsoft 365.
- Configurer et s curiser les services Exchange Online, Microsoft Teams, SharePoint Online et OneDrive.
- Mettre en  uvre les fonctionnalit s de s curit , de conformit  et de protection des donn es avec Microsoft Defender et



Microsoft Purview.

- Évaluer l'état de préparation d'un environnement Microsoft 365 au déploiement de Microsoft 365 Copilot et réaliser sa mise en œuvre.
- Configurer les paramètres, les accès et les mécanismes d'extensibilité de Microsoft 365 Copilot.
- Administrer les identités d'agents d'IA et appliquer les règles de gouvernance associées.
- Superviser l'utilisation, l'adoption, la sécurité et les coûts des services Microsoft 365 et des services d'IA.



Compétences acquises à l'issue de la formation :

- Être capable d'administrer et de gouverner un tenant Microsoft 365 en configurant les identités, les rôles d'administration, les licences, les paramètres d'organisation et les principaux services Microsoft 365.
- Maîtriser la gestion des accès et de la sécurité dans Microsoft Entra en mettant en œuvre les mécanismes d'authentification, l'accès conditionnel, la gouvernance des identités, les rôles privilégiés et les contrôles de sécurité associés.
- Être en mesure de configurer et sécuriser les services collaboratifs Microsoft 365 (Exchange Online, Teams, SharePoint Online et OneDrive) tout en contrôlant les autorisations d'accès, le partage des données et l'exposition des contenus à l'intelligence artificielle.
- Savoir mettre en œuvre les fonctionnalités Microsoft Defender et Microsoft Purview afin de protéger les données, prévenir les pertes d'informations, classer les contenus sensibles et répondre aux incidents de sécurité et de conformité.
- Être capable d'évaluer, déployer et administrer Microsoft 365 Copilot en préparant l'environnement, en configurant les paramètres du tenant, en maîtrisant l'accès aux données et en pilotant un déploiement progressif et sécurisé.
- Maîtriser la gouvernance des agents d'IA Microsoft 365 en administrant les identités d'agents, les registres d'agents, les outils associés, les contrôles d'accès et les mécanismes de gouvernance tout au long de leur cycle de vie.
- Être en mesure de surveiller, auditer et optimiser les services Microsoft 365 et les services d'IA à l'aide des outils de supervision, des rapports d'utilisation, des indicateurs d'adoption, des contrôles de conformité et du suivi des coûts.



Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.



Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant

- Un support num rique (PDF ou Web)
- Acc s extranet pour partage de documents et  margement  lectronique



Modalit s d' valuation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une  valuation des pr requis est r alis e   l'aide d'un questionnaire en ligne ou lors d'un  change avec le formateur(trice), qui valide la base de connaissances n cessaires.

Les stagiaires disposent  galement, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d' valuer leur niveau de ma trise des comp tences vis es par la formation. Cette auto- valuation est r alis e avant le d marrage de la formation   l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus  lev .

Pendant

Apr s chaque module th orique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compr hension des notions abord es.

Apr s

  l'issue de la formation, les stagiaires r alisent une nouvelle **auto- valuation** sur les m mes comp tences que celles  valu es avant la formation. Cette comparaison permet de mesurer leur perception de la progression r alis e et de visualiser les comp tences d velopp es au cours de la formation.

Lorsque le programme de formation le pr voit, un examen de certification est organis  conform ment aux modalit s d finies par l' diteur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert...).

Le formateur r alise  galement une ** valuation individuelle des comp tences** de chaque stagiaire sur l'ensemble des comp tences vis es par la formation. Pour chacune d'elles, il indique si la comp tence est :

- Acquis e ;
- En cours d'acquisition ;
- Non acquis e.

Lorsque la comp tence est  valu e comme **en cours d'acquisition** ou **non acquis e**, le formateur formule des observations pr cisant les difficult s rencontr es ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa mont e en comp tences.

Enfin

Un questionnaire de satisfaction permet au participant d' valuer la qualit  de la prestation de formation.



Informations sur l'accessibilit  :

Nos formations sont, dans la mesure du possible, con ues pour  tre accessibles   toutes et   tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons   contacter notre r f rente handicap certifi e :

C line SOLATGES – 05 61 34 39 80 – csolatges@iform.fr

Nous vous remercions de bien vouloir nous communiquer toute information utile   ce sujet en amont de la formation, afin de mettre en place les adaptations n cessaires et d'assurer un accompagnement optimal.

Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- [AGEFIPH](#)
- [FIPHFP](#)
- MDPH de votre d partement

Description / Contenu

Disponible   partir du 01/12/2026

Module 1 : Provisionnez et personnalisez un tenant Microsoft 365

Configurez l'identit  fondamentale d'un tenant Microsoft 365 en ajoutant et en v rifiant un domaine personnalis , en

personnalisant l'image de marque de l'organisation et en configurant les param tres de l'organisation   l'aide de r les d'administrateur appliquant le principe du moindre privil ge.

- Comprendre le tenant Microsoft 365
- Attribuer des r les d'administrateur avec le principe du moindre privil ge

- Ajouter et vérifier un domaine personnalisé
- Exercice - Déléguer l'administration d'un domaine et ajouter un domaine personnalisé
- Configurer la personnalisation de l'organisation sur deux portails
- Exercice - Configurer la personnalisation de l'organisation
- Configurer les paramètres de l'organisation
- Exercice - Configurer les paramètres de l'organisation

Module 2 : Attribuer des licences Microsoft 365 et des services d'IA à grande échelle

Gérer les licences Microsoft 365 et les licences des services d'IA à grande échelle à l'aide d'attributions directes, basées sur des groupes et avec paiement à l'utilisation, résoudre les problèmes courants liés à l'attribution des licences et choisir le modèle d'accès approprié à Microsoft 365 Copilot, Copilot Studio ou Agent 365 en fonction des différentes populations d'utilisateurs.

- Attribuer et gérer les licences Microsoft 365
- Vérifier et résoudre les problèmes liés à l'attribution des licences
- Exercice - Attribuer, vérifier et résoudre les problèmes liés aux licences Microsoft 365 Copilot pour le déploiement de Relecloud auprès de l'équipe marketing
- Attribuer des licences aux services d'IA pour les populations appropriées
- Comprendre la structure de facturation de Microsoft 365
- Configurer la facturation à l'utilisation pour les services d'IA
- Exercice - Configurer la facturation à l'utilisation pour l'équipe pilote de Copilot Studio de Relecloud

Module 3 : Maintenir un tenant Microsoft 365 résilient et en bonne santé

Configurer Microsoft 365 Backup, surveiller l'intégrité des services et la connectivité réseau, notamment les exigences WebSocket de Copilot, et utiliser les rapports d'utilisation ainsi que le score d'adoption pour maintenir un tenant Microsoft 365 résilient, à jour et en amélioration continue.

- Configurer Microsoft 365 Backup pour les workloads critiques
- Exercice - Configurer Backup pour les workloads critiques de Relecloud
- Surveiller l'intégrité des services et configurer les notifications

- Diagnostiquer les problèmes de connectivité réseau affectant Copilot
- Exercice - Diagnostiquer l'échec de connectivité à Copilot du bureau satellite de Relecloud
- Surveiller l'utilisation et l'adoption de Microsoft 365
- Exercice - Interpréter les données d'adoption de Copilot de Relecloud
- Identifier l'écosystème de gestion des endpoints et des clients

Module 4 : Configurer les workloads Exchange Online et Microsoft Teams

Créer et gérer des boîtes aux lettres utilisateur et partagées avec les autorisations, le dimensionnement et les licences appropriés ; comprendre le cheminement des messages dans Exchange Online ; configurer les équipes et les canaux ; et activer Microsoft 365 Copilot dans les réunions Teams avec les paramètres de transcription appropriés.

- Créer et gérer des boîtes aux lettres
- Déléguer l'accès aux boîtes aux lettres : Full Access, Send As et Send on Behalf
- Exercice - Configurer les boîtes aux lettres partagées de Relecloud et déléguer les accès
- Comprendre le cheminement des messages dans Exchange Online
- Créer et gérer des équipes, des canaux, des propriétaires et des membres
- Configurer Copilot dans les réunions Teams
- Exercice - Créer une équipe compatible avec Copilot pour les responsables de comptes de Relecloud

Module 5 : Gouverner SharePoint et OneDrive pour Microsoft 365 Copilot

Configurer les sites SharePoint, les autorisations et les paramètres de partage, et appliquer Restricted Content Discovery, Restricted Access Control et Restricted SharePoint Search pour contrôler ce que Microsoft 365 Copilot peut découvrir et utiliser.

- Créer et gérer des sites SharePoint
- Définir les limites : paramètres de partage de SharePoint et OneDrive
- Identifier les sites faisant l'objet d'un partage excessif avant que Copilot ne les détecte
- Exercice - Configurer et auditer un site SharePoint gouverné
- Masquer du contenu dans les résultats de recherche sans en restreindre l'accès : Restricted Content Discovery
- Restreindre réellement l'accès : Restricted Access Control

- Une liste d'autorisation temporaire pour le d ploiement : Restricted SharePoint Search
- Choisir le contr le appropri  selon le besoin
- Exercice - Rem dier aux probl mes du site Finance et choisir le contr le appropri 

Module 6 : Provisionner et gouverner les identit s dans Microsoft Entra

Provisionner et gouverner les utilisateurs, les invit s, les groupes et les r les privil gi s dans Microsoft Entra   l'aide d'unit s administratives appliquant le principe du moindre privil ge, de Privileged Identity Management et de Microsoft Graph PowerShell.

- G rer le cycle de vie des utilisateurs et des contacts
- Effectuer la gestion des identit s en masse avec Microsoft Graph PowerShell
- Exercice - Provisionner en masse les utilisateurs nouvellement recrut s de Relecloud avec Microsoft Graph PowerShell
- G rer les invit s et la collaboration externe
- Cr er et g rer les groupes, les strat gies de nommage et les strat gies d'expiration
- D finir le p rim tre de l'administration d l gu e avec les unit s administratives
- Exercice - D finir le p rim tre d'administration des ressources humaines r gionales de Relecloud avec une unit  administrative
- Gouverner les r les avec les groupes de r les et Privileged Identity Management
- Exercice - Configurer un workflow d'approbation PIM pour un r le privil gi  de Relecloud

Module 7 : Mettre en  uvre l'authentification et les acc s dans Microsoft Entra

Configurer les m thodes d'authentification, Password Protection, la r initialisation de mot de passe en libre-service et les strat gies d'acc s conditionnel qui r agissent au risque li    la connexion, au risque utilisateur et   la conformit  des appareils, puis examiner les probl mes d'authentification   l'aide des journaux de connexion, de l'outil de diagnostic des connexions et de l'outil What If.

-  valuer et d finir le p rim tre du catalogue des m thodes d'authentification
- Appliquer Password Protection aux comptes cloud
- Activer et r soudre les probl mes li s   la r initialisation de mot de passe en libre-service
- Exercice - D finir le p rim tre des m thodes d'authentification et activer la r initialisation de mot de passe en libre-service pour l' quipe d'ing nierie de Relecloud

-  valuer les strat gies d'acc s conditionnel et les conditions relatives aux applications clientes
- Examiner et r soudre les probl mes d'authentification
- R soudre les probl mes li s au risque de connexion et   la conformit  des appareils dans l'acc s conditionnel
- Exercice - Cr er et v rifier une strat gie d'acc s conditionnel bas e sur le risque et la conformit  des appareils

Module 8 : S curiser la messagerie et la collaboration avec Microsoft Defender for Office 365

Prot ger les workloads de messagerie et de collaboration avec Microsoft Defender for Office 365, configurer les strat gies de protection contre les menaces, g rer les alertes, examiner et traiter les menaces, et ex cuter des simulations d'attaques, puis comprendre comment Microsoft Defender for Office 365 s'int gre   l'ensemble de solutions de s curit  Microsoft Defender.

- Configurer les strat gies de protection contre les menaces : strat gies pr d finies, strat gies personnalis es et ordre de priorit 
- Configurer les param tres de chaque strat gie de protection contre les menaces
-  tendre la protection   Teams, SharePoint et OneDrive
- Exercice - Configurer et d finir le p rim tre de la protection contre les menaces pour l' quipe Finance de Relecloud
- G rer les alertes et examiner les menaces
- Rem dier aux menaces et r duire les risques li s aux comportements humains : AIR et simulation d'attaques
- Exercice - Examiner une menace et r duire les risques li s aux comportements humains avec une simulation d'attaques
- Coordonner les actions avec l'ensemble des solutions de s curit  Microsoft Defender

Module 9 : Prot ger les informations avec la protection des informations Microsoft Purview

D finir les exigences en mati re de protection des informations pour les contenus sensibles, choisir la technique de classification appropri e en fonction de la structure des donn es et v rifier que la classification permet un ancrage s curis  de Microsoft 365 Copilot.

- Choisir une technique de classification en fonction de la structure des donn es

- Exercice - Créer un type d'informations sensibles personnalisé pour le modèle de transactions de Woodgrove
- Concevoir ce qu'une étiquette de confidentialité protège
- Publier des stratégies d'étiquetage et résoudre les conflits de paramètres
- Exercice - Configurer et publier une stratégie d'étiquetage de confidentialité, puis vérifier la résolution des priorités
- Vérifier le bon fonctionnement de la classification avec les rapports Purview
- Vérifier que la classification permet un ancrage sécurisé de Copilot

Module 10 : Prévenir la perte de données et gouverner le cycle de vie des données avec Microsoft Purview

Définir les exigences en matière de prévention de la perte de données pour les workloads Microsoft 365 et Microsoft 365 Copilot, répondre aux alertes DLP, définir les exigences en matière de gestion du cycle de vie des données et surveiller les activités liées à l'IA à l'aide de Data Security Posture Management (DSPM) for AI.

- Définir les exigences en matière de DLP pour les différents emplacements Microsoft 365
- Exercice - Créer une stratégie DLP pour Microsoft 365 Copilot
- Attribuer les alertes DLP aux différentes applications et agents d'IA
- Répondre aux alertes DLP dans Microsoft Defender XDR
- Exercice - Examiner une alerte DLP dans Microsoft Defender XDR
- Définir les exigences en matière de gestion du cycle de vie des données
- Surveiller les activités liées à l'IA et les risques de partage excessif avec DSPM for AI
- Exercice - Examiner une évaluation des risques liés aux données avec DSPM for AI
- Identifier l'ensemble des fonctionnalités de gouvernance de Microsoft Purview

Module 11 : Évaluer la préparation et déployer Microsoft 365 Copilot

Évaluer la préparation du tenant et des données pour Microsoft 365 Copilot, notamment à l'aide du Copilot Readiness Report et des canaux de mise à jour, résoudre les risques liés au partage excessif et à la conformité, et planifier un déploiement progressif au sein de votre organisation.

- Évaluer la préparation du tenant pour un déploiement de Copilot
- Exercice - Exécuter et interpréter le rapport de préparation de Copilot
- Identifier et résoudre les problèmes liés à la préparation des données
- Exercice - Remédier à un risque de partage excessif avant le déploiement
- Planifier un déploiement progressif au sein de l'organisation
- Exercice - Préparer un groupe pilote pour un déploiement progressif

Module 12 : Configurer les paramètres et l'extensibilité de Microsoft 365 Copilot

Configurer le catalogue des paramètres du tenant Microsoft 365 Copilot, gérer la recherche web pour Microsoft 365 Copilot et Copilot Chat, configurer Copilot Search et étendre les fonctionnalités de Copilot avec les Copilot Connectors et des fournisseurs d'IA tiers.

- Configurer le catalogue des paramètres du tenant Copilot
- Exercice - Configurer le catalogue des paramètres de Copilot
- Gérer la recherche web pour Copilot et Copilot Chat
- Configurer Copilot Search
- Exercice - Configurer la recherche web et Copilot Search
- Gérer les fournisseurs d'IA tiers
- Exercice - Activer un fournisseur d'IA tiers
- Configurer les Copilot Connectors
- Gouverner les compétences d'IA SharePoint et le programme Frontier

Module 13 : Établir les identités des agents et sécuriser les accès avec Microsoft Entra Agent ID

Établir des identités gouvernées pour les agents d'IA à l'aide de Microsoft Entra Agent ID, attribuer des sponsors et des propriétaires selon le principe du moindre privilège, automatiser les transitions du cycle de vie liées au transfert des sponsors et appliquer l'accès conditionnel pour sécuriser l'accès des agents.

- Comprendre le modèle d'objet Microsoft Entra Agent ID
- Attribuer un sponsor et un propriétaire selon le principe du moindre privilège
- Exercice - Attribuer un sponsor et un propriétaire à une identité d'agent
- Automatiser le transfert d'un sponsor avec les workflows de cycle de vie

- Exercice - Configurer un workflow de cycle de vie pour le transfert d'un sponsor
- Appliquer l'acc s conditionnel aux identit s d'agents et choisir la licence appropri e
- Exercice - Appliquer l'acc s conditionnel   un blueprint d'identit  d'agent

Module 14 : G rer et contr ler les agents avec le registre des agents et les outils Agent 365

Gouverner les agents qu'ils peuvent invoquer   l'aide des outils Agent 365, notamment les serveurs MCP, et g rer l'ensemble des agents de mani re continue   l'aide des actions du registre au-del  de leur int gration initiale.

- Examiner, approuver et bloquer les outils pour les agents
- Exercice - Examiner, approuver et bloquer un outil
- Gouverner vos propres serveurs MCP
- Exercice - Examiner l'enregistrement de votre propre serveur MCP (Model Context Protocol)
- Effectuer la gestion continue du registre des agents
- Exercice - R attribuer le propri taire d'un agent actif
- Auditer l'ensemble des agents par  diteur et par canal

Module 15 : Surveiller et g rer les agents avec Microsoft Agent 365

Microsoft Agent 365 offre une visibilit  en temps r el sur les agents de votre organisation afin de d tecter leur prolif ration, de comprendre leur utilisation et leur comportement, et d'agir en fonction des indicateurs de performance et de risque. La surveillance de ces agents permet de s'assurer qu'ils fonctionnent comme pr vu, qu'ils apportent de la valeur et qu'ils n'exposent pas l'organisation   des risques. Dans ce module, vous apprenez   surveiller et   g rer l'ensemble des agents de votre organisation.

- Introduction   Microsoft Entra Agent ID
- Surveiller et g rer les agents
- Sc nario
- Exercice – Surveiller les agents depuis la page de pr sentation
- Exercice - Surveiller l'inventaire des agents dans le registre
- Exercice - Surveiller les agents   l'aide de la carte des agents
- Exercice - Afficher les agents pr sentant des exceptions et prendre les mesures appropri es
- Exercice - Mesurer l'efficacit  des agents
- Exercice – Surveiller les plateformes connect es

Module 16 : Gouverner les agents avec Agent 365

La gouvernance des agents est essentielle, car elle garantit que les agents sont d ploy s et utilis s de mani re contr l e et s curis e. Microsoft Agent 365 permet d' tablir des contr les de gouvernance tout au long du cycle de vie des agents, notamment lors de leur int gration et de leur validation, de mettre en place des contr les de gouvernance des acc s pour assurer la s curit  et la conformit , et de garantir la conformit  des donn es. Dans ce module, vous apprenez   configurer les strat gies, les autorisations et les r gles permettant de gouverner les agents avec Agent 365.

- Sc narios de gouvernance des agents
- Exercice – Configurer les param tres et les acc s des agents
- Strat gies de s curit  et de gouvernance
- Exercice – Configurer un mod le de strat gie
- Exercice – Configurer les autorisations   l'aide de packages d'acc s
- Exercice – Int grer un agent
- Exercice – D ployer et activer des agents
- Exercice - Attribuer des propri taires aux agents pour pr venir leur prolif ration
- Exercice - Bloquer les agents pr sentant des risques de s curit 
- Exercice – Utiliser des r gles et automatiser la gestion des agents
- G rer les outils
- Exercice - Activer et g rer les outils
- Afficher les journaux d'audit

Module 17 : Surveiller et optimiser les services d'IA Microsoft 365

Surveiller l'utilisation, l'adoption et les co ts li s   Copilot et aux agents dans les services d'IA Microsoft 365, et utiliser l'int grit  des services Microsoft 365 ainsi que Copilot Control System pour maintenir les services d'IA en bon  tat de fonctionnement.

- Choisir la source de rapport appropri e pour r pondre   une question sur l'adoption de Copilot
- Exercice - Choisir la source de rapport appropri e
- Lire le rapport d'utilisation de Copilot et le rapport d'utilisation des agents
- Exercice - Lire le rapport d'utilisation de Copilot et le rapport d'utilisation des agents
- Rapprocher les co ts de Copilot et des agents entre les diff rentes surfaces
- Exercice - Rapprocher les co ts de Copilot et des agents entre les diff rentes surfaces
-  valuer l'int grit  des services d'IA avec Copilot Control System