OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen SC-300

Administrateur identité et accès Microsoft

Certification : Microsoft Certified — Identity and Access Administrator Associate

Niveau : Associate | Public : Administrateurs Microsoft Entra ID / IAM

1. Présentation de la certification

L'examen **SC-300 : Microsoft Identity and Access Administrator** valide les compétences des administrateurs en charge de la conception, de l'implémentation et de l'exploitation des systèmes de gestion des identités et des accès d'une organisation à l'aide de Microsoft Entra. Cette certification atteste de votre capacité à configurer et gérer les identités tout au long de leur cycle de vie pour les utilisateurs, les appareils, les ressources Azure et les applications, en appliquant les principes Zero Trust.

La réussite de cet examen unique conduit à l'obtention de la certification **Microsoft Certified : Identity and Access Administrator Associate**, particulièrement valorisée pour les rôles d'administrateur IAM, d'architecte d'identité et de consultant en gouvernance des identités. Elle est aussi l'un des prérequis Associate du parcours expert Cybersecurity Architect (SC-100).

Informations clés

Code de l'examen	SC-300
Intitulé officiel	Microsoft Identity and Access Administrator
Certification obtenue	Microsoft Certified : Identity and Access Administrator Associate
Niveau	Associate
Statut	Actif (mise à jour le 27 avril 2026)
Durée de l'examen	Environ 100 à 120 minutes (selon planification)
Nombre de questions	40 à 60 questions (QCM, études de cas, glisser-déposer, scénarios pratiques)
Score de réussite	700 / 1000
Langues disponibles	Anglais, français, allemand, italien, espagnol, portugais (Brésil), japonais, coréen, chinois (simplifié), chinois (traditionnel), russe, arabe (Arabie saoudite), indéonsien
Validité	1 an, renouvellement gratuit en ligne via Microsoft Learn
Modalité	En centre agréé (OpenCertif — Pearson VUE) ou à distance (OnVUE)

2. Profil du candidat

En tant qu'administrateur identité et accès Microsoft, vous concevez, implémentez et exploitez la gestion des identités et des accès d'une organisation via Microsoft Entra. Vous configurez et gérez les identités tout au long de leur cycle de vie pour :

- Les utilisateurs (internes et externes).
- Les appareils.
- Les ressources Microsoft Azure.
- Les applications (SaaS, on-premises, custom).
- Vous êtes responsable de l'application des principes Zero Trust pour les solutions d'identité et d'accès.

En tant qu'administrateur identité et accès, vous offrez aux utilisateurs des expériences fluides et des capacités de gestion en libre-service. Vous planifiez et implémentez l'identité, l'authentification et l'autorisation pour permettre l'accès aux applications et ressources. Vous êtes aussi responsable du dépannage, de la supervision et du reporting. Vous devez être familier avec :

- Microsoft Azure et Microsoft 365.
- Active Directory Domain Services (AD DS).
- PowerShell pour l'administration scriptable.
- Kusto Query Language (KQL) pour l'analyse des logs.

3. Prérequis et public cible OpenCertif

Aucun prérequis formel n'est exigé, mais OpenCertif recommande aux candidats de disposer d'une expérience préalable dans les domaines suivants :

- Notions de Microsoft 365 Fundamentals (idéalement certification MS-900).
- Notions de Microsoft Security, Compliance and Identity Fundamentals (SC-900).
- Familiarité avec Active Directory et Microsoft Entra ID (anciennement Azure AD).
- Compréhension des concepts d'authentification (SSO, MFA, SAML, OIDC).
- Expérience pratique d'un environnement Microsoft 365 / Azure.
- Le SC-300 est aussi l'un des prérequis Associate pour le parcours SC-100 Expert.

Public cible OpenCertif

- Administrateurs Microsoft Entra ID (anciennement Azure AD).
- Administrateurs IAM (Identity and Access Management).
- Architectes d'identité et consultants en gouvernance.
- Administrateurs Microsoft 365 spécialisés sur l'identité.
- Profils en transition d'AD DS on-premises vers Microsoft Entra cloud.
- Candidats au parcours expert SC-100 cherchant un prérequis Associate.

4. Domaines de compétences mesurées

L'examen est structuré autour de 4 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version du 27 avril 2026).

Domaine	Intitulé	Pondération
1	Implémenter et gérer les identités utilisateurs	20 — 25 %
2	Implémenter l'authentification et la gestion des accès	25 — 30 %
3	Planifier et implémenter les workload identities	20 — 25 %
4	Planifier et automatiser la gouvernance des identités	20 — 25 %

Remarque : la majorité des questions concernent des fonctionnalités en disponibilité générale (GA). Certaines questions peuvent porter sur des fonctionnalités en préversion couramment utilisées.

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen SC-300, conformément au guide d'étude officiel Microsoft (version du 27 avril 2026).

1 Implémenter et gérer les identités utilisateurs — 20 — 25 %

1.1 Configurer et gérer un locataire Microsoft Entra

- Configurer et gérer les rôles Microsoft Entra intégrés et personnalisés.
- Recommander quand utiliser les unités administratives.
- Configurer et gérer les unités administratives.
- Évaluer les permissions effectives pour les rôles Microsoft Entra.
- Configurer et gérer les domaines dans Microsoft Entra ID et Microsoft 365.
- Configurer les paramètres de Company branding.
- Configurer les propriétés du locataire, les paramètres utilisateurs, groupes et appareils.

1.2 Créer, configurer et gérer les identités Microsoft Entra

- Créer, configurer et gérer les utilisateurs.
- Créer, configurer et gérer les groupes.
- Gérer les attributs de sécurité personnalisés.
- Automatiser les opérations en masse via le centre d'administration Microsoft Entra et PowerShell.
- Gérer la jointure et l'enregistrement d'appareils dans Microsoft Entra ID.
- Attribuer, modifier et rapporter sur les licences.

1.3 Implémenter et gérer les identités pour utilisateurs et locataires externes

- Gérer les paramètres de collaboration externe dans Microsoft Entra ID.
- Inviter des utilisateurs externes, individuellement ou en masse.
- Gérer les comptes utilisateurs externes dans Microsoft Entra ID.
- Implémenter les paramètres d'accès cross-tenant.
- Implémenter et gérer la synchronisation cross-tenant.
- Configurer les fournisseurs d'identité externes, y compris protocoles SAML et WS-Fed.

1.4 Implémenter et gérer l'identité hybride

- Implémenter et gérer Microsoft Entra Connect Sync.
- Implémenter et gérer Microsoft Entra Cloud Sync.
- Implémenter et gérer la synchronisation des hash de mot de passe (password hash sync).
- Implémenter et gérer l'authentification pass-through.
- Implémenter et gérer le SSO transparent (seamless SSO).
- Migrer depuis AD FS vers d'autres mécanismes d'authentification et autorisation.
- Implémenter et gérer Microsoft Entra Connect Health.

2 Implémenter l'authentification et la gestion des accès — 25 — 30 %

2.1 Planifier, implémenter et gérer l'authentification utilisateur Microsoft Entra

- Planifier l'authentification.
- Implémenter et gérer les méthodes d'authentification : certificate-based authentication, Temporary Access Pass, tokens OAuth 2.0, Microsoft Authenticator, passkeys (FIDO2).
- Implémenter et gérer les paramètres MFA à l'échelle du locataire.
- Configurer et déployer la réinitialisation de mot de passe en libre-service (SSPR).
- Implémenter et gérer Windows Hello for Business.
- Désactiver les comptes et révoquer les sessions utilisateur.
- Implémenter et gérer Microsoft Entra Password Protection.
- Activer l'authentification Microsoft Entra Kerberos pour les identités hybrides.

2.2 Planifier, implémenter et gérer Microsoft Entra Conditional Access

- Planifier les stratégies de Conditional Access.
- Implémenter les attributions de stratégies de Conditional Access.
- Implémenter les contrôles de stratégies de Conditional Access.
- Tester et dépanner les stratégies de Conditional Access.
- Implémenter la gestion de session.
- Implémenter les restrictions appliquées par appareil.
- Implémenter Continuous Access Evaluation (CAE).
- Configurer l'authentication context.
- Implémenter les actions protégées (protected actions).
- Créer une stratégie de Conditional Access depuis un modèle.

2.3 Gérer le risque via Microsoft Entra ID Protection

- Implémenter et gérer le risque utilisateur via Microsoft Entra ID Protection ou Conditional Access.
- Implémenter et gérer le risque de connexion via Microsoft Entra ID Protection ou Conditional Access.
- Implémenter et gérer l'enregistrement MFA via les méthodes d'authentification et les campagnes d'enregistrement.
- Superviser, enquêter et remédier aux utilisateurs et connexions risqués.
- Superviser, enquêter et remédier aux workload identities risquées.

2.4 Implémenter Global Secure Access

- Déployer les clients Global Secure Access.
- Déployer et gérer Private Access.
- Déployer et gérer Internet Access.
- Déployer et gérer Internet Access pour Microsoft 365.

3 Planifier et implémenter les workload identities — 20 — 25 %

3.1 Planifier et implémenter les identités pour applications et workloads Azure

- Sélectionner les identités appropriées : managed identities, service principals, comptes utilisateurs, comptes de service gérés.
- Créer des managed identities.
- Attribuer une managed identity à une ressource Azure.
- Utiliser une managed identity attribuée à une ressource Azure pour accéder à d'autres ressources Azure.

3.2 Planifier, implémenter et superviser l'intégration des applications d'entreprise

- Planifier et implémenter les paramètres des applications d'entreprise : niveau application et niveau locataire.
- Attribuer les rôles Microsoft Entra appropriés aux utilisateurs pour gérer les applications d'entreprise.
- Concevoir et implémenter l'intégration d'applications on-premises via Microsoft Entra Application Proxy.
- Concevoir et implémenter l'intégration d'applications SaaS.
- Attribuer, classer et gérer les utilisateurs, groupes et rôles d'application pour les applications d'entreprise.
- Configurer et gérer le consentement utilisateur et administrateur.
- Créer et gérer des collections d'applications.

3.3 Planifier et implémenter les enregistrements d'application (app registrations)

- Planifier les enregistrements d'application.
- Créer des enregistrements d'application.
- Configurer l'authentification d'application.
- Configurer les permissions API.
- Créer des rôles d'application.

3.4 Gérer et superviser l'accès aux applications via Microsoft Defender for Cloud Apps

- Configurer et analyser les résultats de Cloud Discovery via Defender for Cloud Apps.
- Configurer les applications connectées.
- Implémenter les restrictions appliquées par application.
- Configurer le Conditional Access App Control.
- Créer des stratégies d'accès et de session dans Defender for Cloud Apps.
- Implémenter et gérer les stratégies pour les applications OAuth.
- Gérer le catalogue Cloud app.

4 Planifier et automatiser la gouvernance des identités — 20 — 25 %

4.1 Planifier et implémenter l’entitlement management dans Microsoft Entra

- Planifier les entitlements.
- Créer et configurer des catalogues.
- Créer et configurer des access packages.
- Gérer les demandes d’accès.
- Implémenter et gérer les terms of use (ToU).
- Gérer le cycle de vie des utilisateurs externes.
- Configurer et gérer les organisations connectées.

4.2 Planifier, implémenter et gérer les access reviews dans Microsoft Entra

- Planifier les access reviews.
- Créer et configurer des access reviews.
- Superviser l’activité des access reviews.
- Répondre manuellement à l’activité des access reviews.

4.3 Planifier et implémenter l’accès privilégié

- Planifier et gérer les rôles Microsoft Entra dans Privileged Identity Management (PIM), y compris paramètres et attributions.
- Planifier et gérer les ressources Azure dans PIM, y compris paramètres et attributions.
- Planifier et configurer PIM for Groups.
- Gérer le processus de demande et d’approbation PIM.
- Analyser l’historique d’audit et les rapports PIM.
- Créer et gérer les comptes break-glass.

4.4 Superviser l’activité des identités via logs, workbooks et rapports

- Examiner et analyser les logs de connexion, audit et provisionnement via le centre d’administration Microsoft Entra.
- Configurer les paramètres de diagnostic, y compris les destinations : workspaces Log Analytics, comptes de stockage et Azure Event Hubs.
- Superviser Microsoft Entra ID via requêtes KQL dans Log Analytics.
- Analyser Microsoft Entra ID via workbooks et reporting.
- Superviser et améliorer la posture de sécurité via Identity Secure Score.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au SC-300 à travers un parcours blended-learning complet, combinant ressources e-learning interactives, sessions tutorées et ateliers techniques pratiques sur les technologies Microsoft Entra ID, Conditional Access, PIM, Global Secure Access, Defender for Cloud Apps et identity governance.

Format de la formation

Durée recommandée	50 à 65 heures de formation (selon profil et niveau d'entrée)
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Modules interactifs Articulate Rise 360, scénarios immersifs VTS, ateliers techniques
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert certifié + classes virtuelles bimensuelles
Évaluations	Quiz formatifs par module, ateliers pratiques, examen blanc final, simulation OnVUE
Certification finale	Passage de l'examen SC-300 en centre OpenCertif (Pearson VUE) ou OnVUE

Parcours d'apprentissage proposé

- **Module 1 :** Architecture Microsoft Entra ID et rôle de l'administrateur IAM.
- **Module 2 :** Configuration et gestion d'un locataire Microsoft Entra.
- **Module 3 :** Rôles, unités administratives et permissions effectives.
- **Module 4 :** Gestion des utilisateurs, groupes et licences.
- **Module 5 :** Identités externes — B2B, cross-tenant, SAML, WS-Fed.
- **Module 6 :** Identité hybride — Entra Connect Sync, Cloud Sync, PHS, PTA.
- **Module 7 :** Méthodes d'authentification — MFA, FIDO2, passkeys, certificate-based.
- **Module 8 :** SSPR, Windows Hello for Business, Password Protection.
- **Module 9 :** Conditional Access — conception, attribution, contrôles, CAE.
- **Module 10 :** Microsoft Entra ID Protection — risques utilisateur et connexion.
- **Module 11 :** Global Secure Access — Private Access et Internet Access.
- **Module 12 :** Workload identities — managed identities et service principals.
- **Module 13 :** Applications d'entreprise — SSO, Application Proxy, SaaS.
- **Module 14 :** App registrations, permissions API, consentement.

- **Module 15 :** Defender for Cloud Apps — Cloud Discovery, App Control.
- **Module 16 :** Entitlement management — access packages, catalogues, ToU.
- **Module 17 :** Access reviews et lifecycle des utilisateurs externes.
- **Module 18 :** Privileged Identity Management (PIM) — rôles, ressources, groupes.
- **Module 19 :** Supervision — logs, KQL, workbooks, Identity Secure Score.
- **Module 20 :** Examen blanc et préparation finale.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources Microsoft Learn suivantes sont fortement recommandées :

- Documentation Microsoft Entra ID (learn.microsoft.com/azure/active-directory).
- Documentation Microsoft Entra External Identities.
- Documentation Microsoft Entra Multi-Factor Authentication.
- Documentation Microsoft Entra ID Protection.
- Documentation Conditional Access.
- Documentation Microsoft Entra Privileged Identity Management (PIM).
- Documentation Microsoft Entra ID Governance.
- Documentation Microsoft Defender for Cloud Apps.
- Documentation Microsoft Entra Global Secure Access.
- Azure Identity Management and access control best practices.
- Microsoft Entra monitoring and health documentation.
- Parcours d’apprentissage Microsoft Learn dédiés au SC-300.
- Évaluation pratique gratuite proposée par Microsoft.
- Espace de simulation d’examen (aka.ms/examdemo).
- Security, compliance, and identity community hub.
- Chaînes vidéo : Exam Readiness Zone.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement sur learn.microsoft.com
Centre d’examen	OpenCertif — Centre agréé Pearson VUE
Examen à distance	Mode OnVUE (surveillance en ligne, conditions strictes)
Pièce d’identité	2 pièces d’identité obligatoires le jour de l’examen
Aménagements	Demande possible (temps additionnel, assistance) sur Microsoft Learn
Résultat	Score communiqué immédiatement à la fin de l’examen
Renouvellement	Annuel, via évaluation gratuite en ligne sur Microsoft Learn
Politique de reprise	Délai d’attente de 24 heures pour la 1re reprise, puis 14 jours entre les tentatives suivantes (maximum 5 tentatives sur 12 mois)

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au SC-300, l'équipe OpenCertif reste à votre disposition.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base du guide d'étude officiel Microsoft SC-300, dans sa version applicable (version du 27 avril 2026). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Microsoft.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle : learn.microsoft.com/credentials/certifications/resources/study-guides/sc-300