Glossaire Microsoft 365 DSC

Introduction

Ce document a pour objectif de fournir un glossaire détaillé des cmdlets utilisés dans les scripts Microsoft 365 DSC pour l'analyse de votre tenant Microsoft 365. Il est structuré en catégories selon les différents services et applications de Microsoft 365, afin de faciliter la navigation et la compréhension des divers composants et de leur utilisation.

Catégories des Cmdlets

1. **Teams**
    - Cmdlets liés à la configuration et à la gestion de Microsoft Teams, y compris les politiques d'application, la configuration des clients, etc.
2. **OneDrive**
    - Cmdlets pour gérer les paramètres et les politiques de OneDrive for Business.
3. **Exchange Online**
    - Cmdlets dédiés à la configuration et à l'administration d'Exchange Online, incluant les politiques de filtrage, les connecteurs, etc.
4. **SharePoint**
    - Cmdlets pour la gestion de SharePoint Online, incluant les configurations de site, les politiques de partage, etc.
5. **PowerApps**
    - Cmdlets spécifiques à la gestion des paramètres et des politiques liés à PowerPoint dans Microsoft 365.
6. **Office 365**
    - Cmdlets généraux pour la gestion de différents aspects d'Office 365, y compris les paramètres de sécurité, de conformité, etc.
7. **Intune**
    - Cmdlets pour la gestion et la configuration de Microsoft Intune, concernant les politiques de conformité, les profils de configuration, etc.
8. **Azure Active Directory (EntraID)**
    - Cmdlets pour la gestion d'Azure Active Directory, incluant la gestion des utilisateurs, des groupes, des politiques d'accès conditionnel, etc.

Note au Client

Les analyses effectuées par les scripts Microsoft 365 DSC seront disponibles dans un document détaillé sur un canal Microsoft Teams. Ce document permettra une compréhension approfondie des configurations et des politiques en place au sein de votre tenant Microsoft 365.

Table des matières

Teams 3

OneDrive 5

Exchange Online 6

SharePoint 9

PowerApps 10

Office 365 11

Intune 12

Azure Active Directory (EntraID) 16

Teams

1. **TeamsAppPermissionPolicy**: Gère les politiques de permissions pour les applications Teams. Elle définit quelles applications sont autorisées et les types de données auxquelles elles peuvent accéder.
2. **TeamsAppSetupPolicy**: Configure les politiques de configuration d'applications Teams, déterminant quelles applications sont installées par défaut pour les utilisateurs et comment elles sont organisées.
3. **TeamsClientConfiguration**: Définit les paramètres de configuration du client Teams, comme les paramètres d'interface utilisateur, les fonctionnalités activées/désactivées, etc.
4. **TeamsComplianceRecordingPolicy**: Gère les politiques d'enregistrement de conformité dans Teams, permettant d'enregistrer et de stocker des communications pour des raisons légales ou de conformité.
5. **TeamsEnhancedEncryptionPolicy**: Configure les politiques de chiffrement amélioré pour les réunions Teams, offrant un niveau de sécurité supplémentaire pour les données échangées pendant les réunions.
6. **TeamsFilesPolicy**: Définit les politiques de gestion des fichiers dans Teams, y compris les paramètres de partage et de stockage des fichiers.
7. **TeamsGroupPolicyAssignment**: Attribue des politiques Teams à des groupes spécifiques, permettant une gestion personnalisée en fonction des groupes d'utilisateurs.
8. **TeamsGuestCallingConfiguration**: Configure les paramètres d'appels pour les invités dans Teams, y compris les restrictions et les fonctionnalités disponibles pour les utilisateurs invités.
9. **TeamsGuestMeetingConfiguration**: Gère les paramètres de réunions pour les invités dans Teams, définissant ce que les invités peuvent faire pendant les réunions.
10. **TeamsGuestMessagingConfiguration**: Détermine les paramètres de messagerie pour les invités dans Teams, y compris les capacités de messagerie et les restrictions.
11. **TeamsIPPhonePolicy**: Configure les politiques pour les téléphones IP utilisant Teams, incluant les paramètres de sécurité et de configuration.
12. **TeamsMeetingConfiguration**: Définit les paramètres globaux des réunions dans Teams, comme les options par défaut pour les réunions et les paramètres audio/vidéo.
13. **TeamsMeetingPolicy**: Gère les politiques de réunion dans Teams, y compris les contrôles de réunion et les fonctionnalités disponibles pour les organisateurs et participants.
14. **TeamsTemplatesPolicy**: Permet la création et la gestion de modèles d'équipe dans Teams, facilitant la création d'équipes avec des paramètres prédéfinis.
15. **TeamsTenantNetworkRegion**, **TeamsTenantNetworkSite**, **TeamsTenantNetworkSubnet**: Ces trois commandes aident à gérer la topologie réseau pour Teams, optimisant la performance du réseau et la qualité des appels et réunions.

16. **TeamsTenantTrustedIPAddress**: Définit des adresses IP de confiance pour le tenant Teams, utilisées pour des politiques de sécurité ou de filtrage.
17. **TeamsTranslationRule**: Gère les règles de traduction pour la numérotation et le routage des appels dans Teams.
18. **TeamsUpgradeConfiguration**: Configure la stratégie de migration de Skype Entreprise à Teams, y compris les paramètres de coexistence et les modes de mise à niveau.
19. **TeamsUpgradePolicy**: Définit les politiques de mise à niveau vers Teams pour les utilisateurs, contrôlant comment et quand les utilisateurs sont déplacés vers Teams.
20. **TeamsUser**: Gère les paramètres spécifiques aux utilisateurs dans Teams, comme les licences et les configurations de profil.
21. **TeamsUserCallingSettings**: Configure les paramètres d'appel pour les utilisateurs individuels dans Teams, y compris les paramètres de transfert d'appel et de sonnerie.
22. **TeamsUserPolicyAssignment**: Attribue des politiques Teams spécifiques à des utilisateurs individuels, permettant une gestion personnalisée des fonctionnalités utilisateur.
23. **TeamsVdiPolicy**: Configure les politiques pour l'utilisation de Teams dans les environnements Virtual Desktop Infrastructure (VDI), garantissant la compatibilité et la performance.

OneDrive

1. **ODSettings :** permet de configurer et de gérer les paramètres OneDrive pour l'ensemble de l'organisation, incluant des options de partage, de synchronisation et d'accès aux fichiers. Permet également de configurer divers paramètres de sécurité pour OneDrive, tels que le chiffrement des données en transit et au repos, et la mise en œuvre de politiques de sécurité supplémentaires.

Exchange Online

1. **EXOAcceptedDomain**: Gère les domaines acceptés pour l'organisation Exchange Online. Un domaine accepté est un domaine SMTP pour lequel une organisation Exchange Online reçoit du courrier électronique.
2. **EXOAntiPhishPolicy**: Configure les politiques anti-hameçonnage dans Exchange Online Protection (EOP) et Office 365 Advanced Threat Protection (ATP) pour protéger contre les tentatives de phishing.
3. **EXOAntiPhishRule**: Définit les règles associées aux politiques anti-hameçonnage, spécifiant les conditions et actions pour la détection et la gestion des tentatives de phishing.
4. **EXOAtpPolicyForO365**: Configure la politique de protection avancée contre les menaces (ATP) pour Office 365, y compris les paramètres pour les pièces jointes sécurisées, les liens sécurisés et l'anti-phishing.
5. **EXOAuthenticationPolicy**: Gère les politiques d'authentification pour les boîtes aux lettres Exchange Online, définissant les exigences d'authentification et de connexion.
6. **EXOAuthenticationPolicyAssignment**: Attribue les politiques d'authentification à des utilisateurs ou groupes spécifiques dans Exchange Online.
7. **EXODataClassification**: Permet de créer et gérer des classifications de données personnalisées pour la gouvernance des informations et la conformité dans Exchange Online.
8. **EXODataEncryptionPolicy**: Configure les politiques de chiffrement des données au repos pour Exchange Online, garantissant la sécurité des données stockées.
9. **EXODkimSigningConfig**: Gère la configuration DKIM (DomainKeys Identified Mail) pour la signature des e-mails envoyés depuis Exchange Online, améliorant la sécurité et l'authenticité des e-mails.
10. **EXOHostedConnectionFilterPolicy**: Configure les politiques de filtrage des connexions dans EOP pour contrôler le trafic de messagerie entrant et sortant.
11. **EXOHostedContentFilterPolicy**: Définit les politiques de filtrage du contenu pour la protection contre les spams et les malwares dans Exchange Online.
12. **EXOHostedContentFilterRule**: Crée des règles associées aux politiques de filtrage de contenu pour spécifier les conditions et actions appliquées aux messages.
13. **EXOHostedOutboundSpamFilterPolicy**: Gère les politiques de filtrage du spam sortant dans Exchange Online pour surveiller et gérer les e-mails envoyés.
14. **EXOHostedOutboundSpamFilterRule**: Crée des règles pour la politique de filtrage du spam sortant, définissant des conditions spécifiques pour le traitement des e-mails sortants.
15. **EXOInboundConnector**: Configure les connecteurs entrants dans Exchange Online, qui définissent la manière dont les e-mails entrants sont reçus de partenaires externes ou de systèmes de messagerie.

16. **EXOIntraOrganizationConnector**: Gère les connecteurs intra-organisationnels pour le flux de messagerie sécurisé entre les organisations Exchange Online et Exchange sur site.
17. **EXOIRMConfiguration**: Configure la gestion des droits relatifs à l'information (IRM) dans Exchange Online pour protéger les informations sensibles dans les e-mails.
18. **EXOMailboxPermission**: Gère les autorisations de boîte aux lettres dans Exchange Online, y compris l'accès délégué et les autorisations de boîte aux lettres partagée.
19. **EXOMalwareFilterPolicy**: Définit les politiques de filtrage des malwares dans EOP pour protéger contre les logiciels malveillants dans les e-mails.
20. **EXOMalwareFilterRule**: Crée des règles associées aux politiques de filtrage des malwares, spécifiant les conditions et actions pour la détection et la gestion des malwares.
21. **EXOMobileDeviceMailboxPolicy**: Gère les politiques de boîte aux lettres pour les appareils mobiles, contrôlant l'accès et les fonctionnalités pour les utilisateurs mobiles.
22. **EXOOMEConfiguration**: Configure le chiffrement de message Office 365 (OME) pour chiffrer et sécuriser les e-mails envoyés à l'extérieur de l'organisation.
23. **EXOOnPremisesOrganization**: Gère les paramètres pour les organisations Exchange sur site dans un environnement hybride avec Exchange Online.
24. **EXOOrganizationConfig**: Configure les paramètres globaux de l'organisation Exchange Online, y compris les limites, les fonctionnalités et d'autres options globales.
25. **EXOOrganizationRelationship**: Établit des relations d'organisation pour la fédération et le partage de calendriers entre organisations Exchange Online et/ou sur site.
26. **EXOPerimeterConfiguration**: Configure les paramètres de sécurité du périmètre pour Exchange Online, y compris les connecteurs et les paramètres de transport.
27. **EXOQuarantinePolicy**: Gère les politiques de mise en quarantaine pour les e-mails suspects ou malveillants dans Exchange Online.
28. **EXORemoteDomain**: Configure les paramètres pour les domaines distants, contrôlant la manière dont les e-mails sont gérés pour des domaines spécifiques en dehors de l'organisation.
29. **EXOResourceConfiguration**: Gère les paramètres de configuration des ressources de boîtes aux lettres (comme les salles de réunion) dans Exchange Online.
30. **EXORoleGroup**: Gère les groupes de rôles dans Exchange Online, qui définissent les autorisations et l'accès aux fonctionnalités d'administration.
31. **EXOSafeAttachmentPolicy**: Configure les politiques pour les pièces jointes sécurisées dans ATP, offrant une protection avancée contre les menaces inconnues dans les pièces jointes.
32. **EXOSafeAttachmentRule**: Crée des règles associées aux politiques de pièces jointes sécurisées, définissant des conditions spécifiques pour leur traitement.
33. **EXOSafeLinksPolicy**: Configure les politiques pour les liens sécurisés dans ATP, protégeant contre les liens malveillants dans les e-mails et les documents Office.

34. **EXOSafeLinksRule**: Établit des règles pour la politique de liens sécurisés, spécifiant les conditions et actions pour la vérification des liens.
35. **EXOSharingPolicy**: Gère les politiques de partage de calendriers et de contacts dans Exchange Online, contrôlant le partage avec des domaines externes.
36. **EXOTransportConfig**: Configure les paramètres de transport globaux pour Exchange Online, y compris les règles de flux de messagerie et les paramètres de connecteur.
37. **EXOTransportRule**: Crée et gère des règles de transport (règles de flux de messagerie) dans Exchange Online pour contrôler et manipuler le flux de messagerie.

SharePoint

1. **SPOAccessControlSettings**: Ce composant gère les paramètres de contrôle d'accès pour SharePoint Online. Il permet de configurer les restrictions d'accès basées sur le réseau, les appareils non gérés, et d'autres paramètres de sécurité qui déterminent comment les utilisateurs peuvent accéder aux sites SharePoint Online.
2. **SPOSearchManagedProperty**: Ce composant permet de créer, mettre à jour, ou supprimer des propriétés gérées dans la recherche SharePoint Online. Les propriétés gérées sont utilisées pour personnaliser et améliorer l'expérience de recherche en permettant de définir comment les informations sont indexées et présentées dans les résultats de recherche.
3. **SPOSharingSettings**: Ce composant configure les paramètres de partage au niveau du tenant SharePoint Online. Il inclut des options pour activer ou désactiver le partage externe, définir le niveau de partage par défaut, et contrôler d'autres aspects du partage de contenu à l'intérieur et à l'extérieur de l'organisation.
4. **SPOSiteAuditSettings**: Ce composant configure les paramètres d'audit pour les collections de sites SharePoint Online. Il permet de spécifier les types d'événements à enregistrer, tels que l'édition de documents, les suppressions, et les activités de recherche, ce qui est crucial pour la conformité et la sécurité.
5. **SPOStorageEntity**: Ce composant est utilisé pour gérer les entités de stockage (parfois appelées « propriétés du tenant ») dans SharePoint Online. Ces entités de stockage peuvent être utilisées pour stocker des informations de configuration personnalisées qui peuvent être lues par des solutions SharePoint, telles que des applications ou des scripts.
6. **SPOTenantCdnEnabled**: Ce composant active ou désactive le réseau de distribution de contenu (CDN) au niveau du tenant pour SharePoint Online. Le CDN peut améliorer les performances en mettant en cache des ressources statiques sur des serveurs situés plus près des utilisateurs finaux.
7. **SPOTenantCdnPolicy**: Ce composant gère les politiques du CDN pour SharePoint Online. Cela inclut la configuration des types de fichiers qui peuvent être servis à partir du CDN, ainsi que la gestion des origines autorisées pour les ressources CDN.
8. **SPOTenantSettings**: Ce composant configure divers paramètres au niveau du tenant pour SharePoint Online. Il couvre un large éventail de fonctionnalités et de paramètres, y compris mais non limité à, la personnalisation des scripts utilisateur, la gestion des applications, les paramètres de recherche, et plus encore.

PowerApps

1. **PPPowerAppsEnvironment**: Cette commande est utilisée pour configurer des environnements dans Microsoft Power Apps. Un environnement Power Apps est un espace qui permet de stocker, gérer et partager les ressources de l'entreprise (applications, flux de travail, etc.).
2. **PPTenantIsolationSettings**: Cette ressource permet de gérer les paramètres d'isolation au niveau du tenant pour Power Platform. Ces paramètres déterminent comment les données et les ressources sont isolées et partagées entre les différents environnements au sein du même tenant.
3. **PPTenantSettings**: Cette commande sert à configurer les paramètres globaux du tenant pour Power Platform. Elle permet de gérer les paramètres qui s'appliquent à tous les environnements et utilisateurs de Power Platform au sein d'un tenant Microsoft 365.

1. **O365OrgSettings** : Cette ressource est utilisée pour configurer divers paramètres au niveau de l'organisation dans Office 365. Cela peut inclure des paramètres qui affectent plusieurs services Office 365, comme Exchange Online, SharePoint Online et Teams. Les paramètres contrôlés par cette ressource peuvent couvrir des domaines tels que la sécurité, la conformité, les fonctionnalités utilisateur, et d'autres préférences générales de l'organisation. Par exemple, vous pourriez utiliser cette ressource pour activer ou désactiver certaines fonctionnalités à l'échelle de l'organisation ou pour configurer des politiques de sécurité qui s'appliquent à tous les utilisateurs.

2. **O365SearchAndIntelligenceConfigurations** : Cette ressource gère les paramètres de recherche et d'intelligence pour Office 365. Elle peut être utilisée pour personnaliser l'expérience de recherche au sein de l'environnement Office 365, y compris la manière dont les résultats de recherche sont affichés et triés pour les utilisateurs. Cette ressource peut influencer des aspects tels que les paramètres de pertinence de la recherche, les configurations de l'intelligence artificielle qui améliorent la recherche, et les politiques de découverte de contenu. En ajustant ces paramètres, les administrateurs peuvent optimiser l'efficacité et la pertinence des résultats de recherche, améliorant ainsi l'expérience utilisateur globale dans Office 365.

Intune

1. **IntuneAccountProtectionLocalAdministratorPasswordSolutionPolicy**: Gère la politique de protection des comptes pour les mots de passe des administrateurs locaux dans les appareils Windows 10.
2. **IntuneAccountProtectionLocalUserGroupMembershipPolicy**: Définit les politiques concernant les groupes d'utilisateurs locaux et leurs membres sur les appareils Windows 10.
3. **IntuneAccountProtectionPolicy**: Configure les politiques de protection des comptes pour les appareils gérés par Intune.
4. **IntuneAntivirusPolicyWindows10SettingCatalog**: Définit les paramètres de la politique antivirus pour les appareils Windows 10 dans le catalogue de paramètres Intune.
5. **IntuneAppConfigurationPolicy**: Gère les politiques de configuration d'applications pour les applications gérées sur les appareils Intune.
6. **IntuneApplicationControlPolicyWindows10**: Configure les politiques de contrôle d'application pour les appareils Windows 10, telles que les restrictions d'exécution des logiciels.
7. **IntuneAppProtectionPolicyAndroid**: Définit les politiques de protection des applications pour les appareils Android dans Intune.
8. **IntuneAppProtectionPolicyiOS**: Configure les politiques de protection des applications pour les appareils iOS gérés par Intune.
9. **IntuneASRRulesPolicyWindows10**: Gère les politiques de règles de réduction de la surface d'attaque (ASR) pour Windows 10.
10. **IntuneAttackSurfaceReductionRulesPolicyWindows10ConfigManager**: Configure les politiques ASR pour Windows 10 via Configuration Manager.
11. **IntuneDeviceAndAppManagementAssignmentFilter**: Gère les filtres d'affectation pour les appareils et les applications dans Intune.
12. **IntuneDeviceCategory**: Permet de catégoriser les appareils dans Intune pour un meilleur tri et gestion.
13. **IntuneDeviceCleanupRule**: Définit les règles de nettoyage pour les appareils inactifs ou non conformes dans Intune.
14. **IntuneDeviceCompliancePolicyAndroid**: Gère les politiques de conformité des appareils Android dans Intune.
15. **IntuneDeviceCompliancePolicyAndroidDeviceOwner**: Configure les politiques de conformité pour les appareils Android gérés en tant que "Device Owner".
16. **IntuneDeviceCompliancePolicyAndroidWorkProfile**: Définit les politiques de conformité pour les profils de travail Android dans Intune.

17. **IntuneDeviceCompliancePolicyiOS**: Gère les politiques de conformité des appareils iOS dans Intune.
18. **IntuneDeviceCompliancePolicyMacOS**: Configure les politiques de conformité des appareils macOS dans Intune.
19. **IntuneDeviceCompliancePolicyWindows10**: Gère les politiques de conformité pour les appareils Windows 10 dans Intune.
20. **IntuneDeviceConfigurationAdministrativeTemplatePolicyWindows10**: Gère les modèles administratifs de configuration des appareils Windows 10 dans Intune.
21. **IntuneDeviceConfigurationCustomPolicyWindows10**: Permet de créer et de gérer des politiques de configuration personnalisées pour Windows 10 dans Intune.
22. **IntuneDeviceConfigurationDefenderForEndpointOnboardingPolicyWindows10**: Configure les politiques d'intégration de Microsoft Defender for Endpoint pour les appareils Windows 10.
23. **IntuneDeviceConfigurationDeliveryOptimizationPolicyWindows10**: Gère les politiques d'optimisation de la distribution pour les appareils Windows 10.
24. **IntuneDeviceConfigurationDomainJoinPolicyWindows10**: Configure les politiques d'intégration des appareils Windows 10 au domaine.
25. **IntuneDeviceConfigurationEmailProfilePolicyWindows10**: Gère les profils de messagerie pour les appareils Windows 10 dans Intune.
26. **IntuneDeviceConfigurationEndpointProtectionPolicyWindows10**: Définit les politiques de protection des points de terminaison pour Windows 10.
27. **IntuneDeviceConfigurationFirmwareInterfacePolicyWindows10**: Configure les politiques relatives à l'interface du firmware des appareils Windows 10.
28. **IntuneDeviceConfigurationHealthMonitoringConfigurationPolicyWindows10**: Gère les politiques de surveillance de la santé des appareils Windows 10.
29. **IntuneDeviceConfigurationIdentityProtectionPolicyWindows10**: Configure les politiques de protection de l'identité pour les appareils Windows 10.
30. **IntuneDeviceConfigurationImportedPfxCertificatePolicyWindows10**: Gère les politiques de certificats PFX importés pour Windows 10.
31. **IntuneDeviceConfigurationKioskPolicyWindows10**: Configure les politiques pour les appareils en mode Kiosque Windows 10.
32. **IntuneDeviceConfigurationNetworkBoundaryPolicyWindows10**: Définit les politiques de limites réseau pour Windows 10.
33. **IntuneDeviceConfigurationPkcsCertificatePolicyWindows10**: Gère les politiques de certificats PKCS pour Windows 10.
34. **IntuneDeviceConfigurationPolicyAndroidDeviceAdministrator**: Configure les politiques pour les appareils Android en tant qu'administrateurs de dispositifs.

35. **IntuneDeviceConfigurationPolicyAndroidDeviceOwner**: Gère les politiques pour les propriétaires de dispositifs Android.
36. **IntuneDeviceConfigurationPolicyAndroidOpenSourceProject**: Configure les politiques pour les appareils Android Open Source Project.
37. **IntuneDeviceConfigurationPolicyAndroidWorkProfile**: Gère les politiques pour les profils de travail Android.
38. **IntuneDeviceConfigurationPolicyiOS**: Définit les politiques de configuration pour les appareils iOS.
39. **IntuneDeviceConfigurationPolicyMacOS**: Gère les politiques de configuration pour les appareils macOS.
40. **IntuneDeviceConfigurationPolicyWindows10**: Configure les politiques de configuration pour Windows 10.
41. **IntuneDeviceConfigurationSCEPCertificatePolicyWindows10**: Gère les politiques de certificats SCEP pour Windows 10.
42. **IntuneDeviceConfigurationSecureAssessmentPolicyWindows10**: Configure les politiques d'évaluation sécurisée pour Windows 10.
43. **IntuneDeviceConfigurationSharedMultiDevicePolicyWindows10**: Gère les politiques pour les appareils Windows 10 partagés entre plusieurs utilisateurs.
44. **IntuneDeviceConfigurationTrustedCertificatePolicyWindows10**: Configure les politiques de certificats de confiance pour Windows 10.
45. **IntuneDeviceConfigurationVpnPolicyWindows10**: Définit les politiques VPN pour les appareils Windows 10.
46. **IntuneDeviceConfigurationWindowsTeamPolicyWindows10**: Gère les politiques pour les appareils Windows 10 Team.
47. **IntuneDeviceConfigurationWiredNetworkPolicyWindows10**: Configure les politiques de réseau câblé pour Windows 10.
48. **IntuneDeviceEnrollmentLimitRestriction**: Définit les restrictions sur le nombre d'appareils qu'un utilisateur peut inscrire dans Intune.
49. **IntuneDeviceEnrollmentPlatformRestriction**: Gère les restrictions d'inscription des appareils par plateforme dans Intune.
50. **IntuneDeviceEnrollmentStatusPageWindows10**: Configure la page de statut d'inscription des appareils pour Windows 10.
51. **IntuneEndpointDetectionAndResponsePolicyWindows10**: Gère les politiques de détection et réponse aux incidents pour Windows 10.
52. **IntuneExploitProtectionPolicyWindows10SettingCatalog**: Configure les politiques de protection contre les exploits pour Windows 10 dans le catalogue de paramètres Intune.
53. **IntunePolicySets**: Gère les ensembles de politiques dans Intune.

54. **IntuneRoleAssignment**: Gère les attributions de rôle dans Intune.
55. **IntuneRoleDefinition**: Définit les rôles et les permissions dans Intune.
56. **IntuneSettingCatalogASRRulesPolicyWindows10**: Gère les politiques de règles ASR pour Windows 10 via le catalogue de paramètres Intune.
57. **IntuneSettingCatalogCustomPolicyWindows10**: Permet de créer des politiques personnalisées pour Windows 10 dans le catalogue de paramètres Intune.
58. **IntuneWiFiConfigurationPolicyAndroidDeviceAdministrator**: Gère les politiques de configuration WiFi pour les appareils Android en tant qu'administrateurs de dispositifs.
59. **IntuneWifiConfigurationPolicyAndroidEnterpriseDeviceOwner**: Configure les politiques WiFi pour les appareils Android Enterprise Device Owner.
60. **IntuneWifiConfigurationPolicyAndroidEnterpriseWorkProfile**: Gère les politiques WiFi pour les profils de travail Android Enterprise.
61. **IntuneWifiConfigurationPolicyAndroidForWork**: Configure les politiques WiFi pour Android for Work.
62. **IntuneWifiConfigurationPolicyAndroidOpenSourceProject**: Gère les politiques WiFi pour les appareils Android Open Source Project.
63. **IntuneWifiConfigurationPolicyIOS**: Configure les politiques WiFi pour les appareils iOS.
64. **IntuneWifiConfigurationPolicyMacOS**: Gère les politiques WiFi pour les appareils macOS.
65. **IntuneWifiConfigurationPolicyWindows10**: Définit les politiques WiFi pour les appareils Windows 10.
66. **IntuneWindowsAutopilotDeploymentProfileAzureADHybridJoined**: Gère les profils de déploiement Autopilot pour les appareils Azure AD Hybrid Joined.
67. **IntuneWindowsAutopilotDeploymentProfileAzureADJoined:** Ce composant gère les profils de déploiement Autopilot pour les appareils qui seront joints à Azure AD. Il permet de configurer des paramètres comme la réinitialisation de l'appareil, le nom de l'appareil, le comportement du profil utilisateur, le mode de déploiement (par exemple, auto-déployé ou utilisateur-driven), etc.
68. **IntuneWindowsInformationProtectionPolicyWindows10MdmEnrolled:** Ce composant gère les politiques de protection des informations Windows (WIP) pour les appareils Windows 10/11 inscrits via Mobile Device Management (MDM). Il offre des options pour définir des politiques de protection des données au niveau de l'application et du réseau, y compris des paramètres pour contrôler le transfert de données entre les applications professionnelles et personnelles.
69. **IntuneWindowsUpdateForBusinessFeatureUpdateProfileWindows10:** Ce composant configure les profils de mise à jour des fonctionnalités pour Windows Update for Business. Il permet de définir quand et comment les mises à jour de fonctionnalités sont déployées sur les appareils, y compris les délais pour le report des mises à jour et les périodes de grâce.

70. **IntuneWindowsUpdateForBusinessRingUpdateProfileWindows10:** Gère les profils de mise à jour pour les "rings" (ou canaux) de mise à jour dans Windows Update for Business. Permet de configurer des paramètres tels que le niveau de service (par exemple, Semi-Annual Channel), le report des mises à jour de qualité et de fonctionnalités, et les plages horaires actives pour les mises à jour.

Azure Active Directory (EntraID)

1. **AADAdministrativeUnit**: Gère les unités administratives dans Azure Active Directory (AAD). Ces unités permettent de regrouper les objets AAD (comme les utilisateurs ou les groupes) pour une gestion déléguée.
2. **AADAuthenticationMethodPolicy**: Configure les politiques de méthode d'authentification pour AAD, comme les méthodes autorisées (par exemple, mot de passe, téléphone, etc.) et leurs paramètres.
3. **AADAuthenticationMethodPolicyAuthenticator**: Définit les paramètres spécifiques pour l'application Microsoft Authenticator dans le cadre des politiques d'authentification AAD.
4. **AADAuthenticationMethodPolicyFido2**: Configure les politiques relatives aux clés de sécurité FIDO2 utilisées pour l'authentification dans AAD.
5. **AADAuthenticationMethodPolicySoftware**: Gère les politiques concernant les méthodes d'authentification basées sur des logiciels, comme les applications d'authentification.
6. **AADAuthenticationMethodPolicyTemporary**: Définit les politiques pour les méthodes d'authentification temporaires dans AAD.
7. **AADAuthenticationStrengthPolicy**: Permet de spécifier les politiques de force d'authentification, définissant les exigences minimales pour les méthodes d'authentification dans AAD.
8. **AADAuthorizationPolicy**: Gère les politiques d'autorisation dans AAD, qui déterminent les permissions accordées aux utilisateurs et aux applications.
9. **AADConditionalAccessPolicy**: Configure les politiques d'accès conditionnel dans AAD. Ces politiques permettent de définir des conditions spécifiques (comme l'emplacement ou l'appareil utilisé) pour accéder aux ressources.
10. **AADCrossTenantAccessPolicy**: Gère les politiques d'accès inter-locataires dans AAD, contrôlant comment les utilisateurs d'autres locataires peuvent accéder aux ressources de votre locataire.
11. **AADCrossTenantAccessPolicyConfigurationDefault**: Configure les paramètres par défaut pour la politique d'accès inter-locataires dans AAD.
12. **AADCrossTenantAccessPolicyConfigurationPartner**: Définit les configurations spécifiques pour l'accès inter-locataires avec des partenaires spécifiques dans AAD.
13. **AADExternalIdentityPolicy**: Gère les politiques liées aux identités externes dans AAD, telles que les paramètres pour les invités ou les utilisateurs externes.

14. **AADGroup**: Ce composant gère les groupes dans Azure Active Directory (AAD). Il permet de créer, modifier ou supprimer des groupes, ainsi que de configurer leurs propriétés, comme les membres, les propriétaires, et les paramètres de sécurité.
15. **AADGroupLifecyclePolicy**: Ce composant gère les politiques de cycle de vie des groupes dans Azure AD. Ces politiques définissent comment les groupes sont gérés au fil du temps, y compris la durée de vie des groupes, les actions à prendre lorsque les groupes arrivent à expiration, et les notifications aux propriétaires de groupe.
16. **AADGroupsNamingPolicy**: Ce composant permet de définir des politiques de nommage pour les groupes dans Azure AD. Cela peut inclure des préfixes ou des suffixes obligatoires, des listes de mots bloqués, et des modèles pour assurer la cohérence et la clarté dans la création de groupe.
17. **AADGroupsSettings**: Gère les paramètres généraux pour les groupes dans Azure AD. Ces paramètres peuvent inclure des configurations liées à la visibilité des groupes, les paramètres de sécurité, et la gestion des groupes.
18. **AADNamedLocationPolicy**: Ce composant permet de configurer des emplacements nommés dans Azure AD, utilisés dans les politiques d'accès conditionnel. Un emplacement nommé peut être une adresse IP spécifique, une plage d'adresses IP, ou des emplacements géographiques, utilisés pour appliquer des politiques basées sur l'emplacement de l'utilisateur.
19. **AADServicePrincipal**: Gère les principaux de service dans Azure AD. Les principaux de service représentent des applications ou des services et peuvent être utilisés pour contrôler l'accès aux ressources et pour configurer les autorisations au niveau de l'application.
20. **AADTenantDetails**: Permet de gérer les détails du tenant Azure AD, y compris les informations de contact de l'entreprise, les préférences de langue, et d'autres paramètres liés à l'ensemble du tenant.