Administration tenant 365

Tout pour l'administration d'un tenant 365

- Création d'un compte W365 (récupérer la licence d'un user)
- Les listes de distribution
- Archivage d'un compte 365
- Les licences 365
- Groupes 365
- Bloquer les connexion depuis une plage d'adresses IP
- Rôle e-discovery et exportation de contenu
- Un compte de votre entreprise est déjà connecté

Création d'un compte W365 (récupérer la licence d'un user)

- Connexion a la console Partner.
- Trouver le client et se connecter à sa plateforme d’administration.
- Trouver l’utilisateur de référence et noter quelle licence est utilisée (ici business basic)
- Création de la nouvelle adresse mail.
  - Noter dans description privée les informations de connexion.
- Archivage de la boîte existante (regarder la nomenclature en vigueur dans l'entreprise ici ZZ_ARCHIVE BAL)
- Enlever la licence associée dans utilisateurs actif.
- Associer la licence a la nouvelle boîte mail
- Sécurité : pour l'ancienne boîte mail, on peut réaliser les actions suivantes:
  - Réinitialiser le MDP
  - Router les mail vers une nouvelle boîte mail
  - Déconnecter les appareils utilisant cette boîte mail
  - Interdire les connexion
- Vérifier en se connectant sur ce compte en navigation privée.
- Envoyer les informations d’identification au client (utiliser Sharepass pour chiffrer les infos).

Les listes de distribution

Une liste de distribution est **un groupe d'adresses e-mail contenues dans une liste avec une adresse e-mail commune**. Quand un message e-mail est envoyé à une liste de distribution, l'e-mail est envoyé à tous ceux dont l'adresse est incluse dans la liste de distribution.

Ajouter des membres à une liste de distribution.

- Se connecter à la plateforme d'administration du client
- Admin > équipes actives et groupes > Listes de distribution > voir tous les membres, ajouter des membres.

Pourquoi transformer les listes de distribution en Groupes Office 365

Basculer des listes de diffusion (ou listes de distribution) aux Groupes Office signifie simplement que vous bénéficiez d'un outil amélioré. 365 Groupes se dote de plus de possibilités qui simplifient la collaboration. Contrairement aux listes, les groupes intègrent :

- Une synchronisation automatique des calendriers partagés ;
- Un accès unique aux documents partagés puisqu'ils sont hébergés sur SharePoint ;
- Une boîte mail partagée ;
- Et surtout, l'accès et le partage immédiat des fonctionnalités et Apps SharePoint, Yammer, Microsoft Team, OneNote, Planner et PowerBI.

Du côté du Centre d'Administration Exchange (CAE), les nouveautés sont moindres : les listes et groupes sont créés de la même façon, la gestion des fonctionnalités disponibles très intuitive. Côté utilisateurs, les deux outils sont gérés de manière assez similaire, pour ne pas perturber l'usage. Le passage de la solution « liste » à la solution « groupe » se fait donc sans douleur pour les collaborateurs, rendant l'expérience fluide.

Les avantages des Groupes Office 365

Ils sont nombreux ! Manipulation, extension ou accès sont désormais simplifiés.

Créer un groupe, ajouter ou supprimer des membres, gérer les accès invités, utiliser les groupes depuis sa boîte aux lettres, communiquer… Les Groupes Office 365 sont radicalement plus simples que les listes, ils évoluent avec les besoins des usagers. Les Groupes peuvent également être publics ou privés, ce qui facilite le contrôle de la part du propriétaire du groupe.

L'ajout de membre abonné (*subscribe members* en V.O) dans un groupe actif permet d'étendre la collaboration et donne accès à toutes les informations nécessaires.

Les Groupes sont accessibles depuis de nombreux points : Outlook sur le web, Planner, SharePoint, PowerShell, OWA… Les utilisateurs choisissent leur outil, dans le cadre de la configuration décidée par la DSI, qui peut gérer facilement les applications liées et autorisations.

Les Groupes Office 365 représentent donc de formidables opportunités pour les SI et pour les utilisateurs : leur fonctionnement est connu puisqu'inspiré des listes si chères à nos cœurs, les fonctionnalités sont multipliées et les points d'entrée, diversifiés. Une version 2.0 des listes de distribution pour une collaboration toujours plus globale.

Les listes de distribution dynamiques

Les groupes de distribution dynamiques (DDG) sont des objets de groupe Active Directory à extension messagerie créés pour accélérer l'envoi en masse de messages électroniques et d'autres informations au sein d'un organization Microsoft Exchange.

Les GDD de Exchange Online ont été modernisés pour offrir une expérience plus fiable, prévisible et plus performante. Cette modification réduit la latence de remise du courrier, améliore la fiabilité du service et vous permet de voir les membres d'un DDG avant d'envoyer un message.

La liste d'appartenances est désormais stockée pour chaque DDG et est mise à jour toutes les 24 heures. Vous saurez exactement à qui le message est envoyé, et il résout également les problèmes de conformité potentiels. En stockant la liste calculée des membres sur l'objet DDG, les messages peuvent être remis plus rapidement et notre service aura une plus grande fiabilité.

Comment créer un groupe dynamique

Pour créer et gérer des groupes dynamiques, votre entreprise doit posséder assez de licences P1 pour atteindre ou dépasser le nombre d'utilisateurs dans ces groupes.

Bien que les licences ne doivent pas être directement assignées, seules les licences Microsoft 365 P1 et supérieures telles que E3, E5, MF1 et MF3 comportent cette fonctionnalité premium d'Azure AD.

Groupes Dynamiques Microsoft 365 : Guide Du Débutant - AvePoint Blog

Règles d’appartenance aux groupes remplis dynamiquement - Microsoft Entra ID

Archivage d'un compte 365

- archives ZZ_Archive_Nom_Prénom
- Convertir en boite aux lettres partagée
  - Dans la plateforme Exchange > onglet others > convert to shared mailbox
- Déconnecter de toutes les sessions > ok (Ne le faire qu’une fois les données migrées).
- Réinitialiser le MDP > ok (Ne le faire qu’une fois les données migrées).
- Bloquer la connexion (si AD connect, désactiver le compte aura cette impact dans O365).
- Enlever de la liste d'adresse de l'entreprise > ok SI SYNCHRO DEPUIS L’AD (Pas nécessaire pour une boite aux lettres partagées ⇒ important pour se connecter en ligne)

Si synchro AD connect :

- EDITEUR D’ATRIBUT : proxy adresses ⇒ définir des alias, basculer entre des adresses.
- Pour masquer de la GAL
- show in adresse book > true ou false
- Pas de one drive associé à l'adresse mail.

Si un one drive est associé, récupérer les données grâce au lien et voir avec le client quoi en faire.

- Retirer la licence business standard

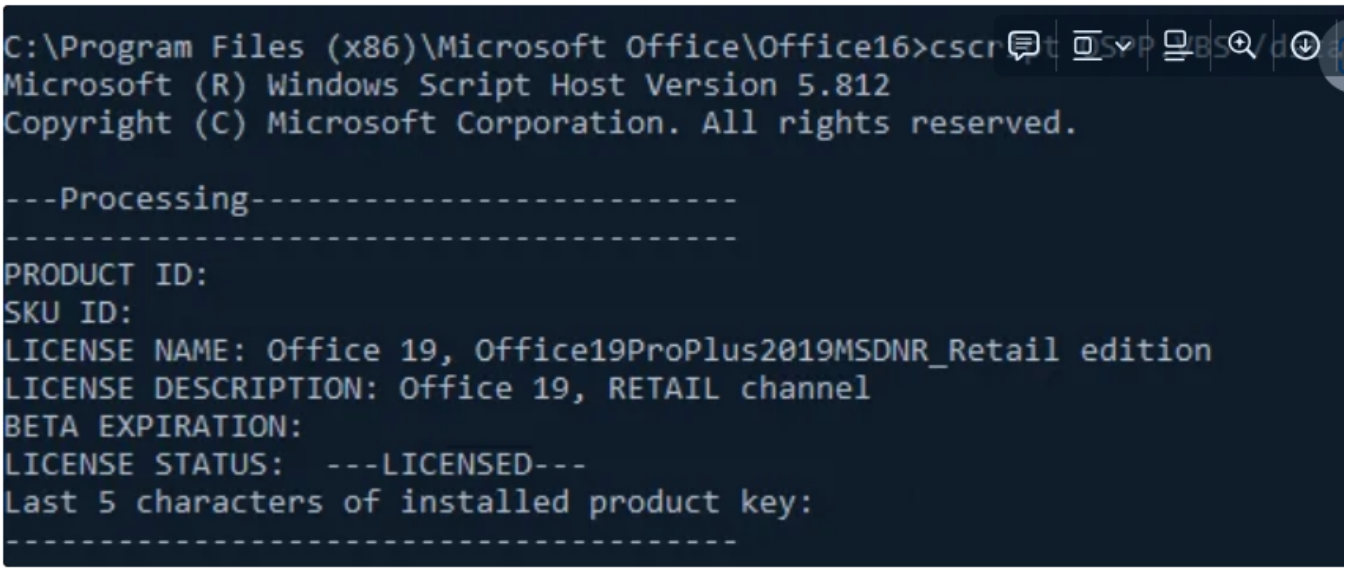
Les licences 365

VERIFIER SA LICENCE

Utilisation de la ligne de commande pour vérifier le type de licence

1. Ouvrez une fenêtre d'invite de commandes avec élévation de privilèges.
2. Tapez la commande ci-dessous pour accéder au dossier Office :
   Pour Office 32 bits (x86)
   `cd c:\\Program" "Files" "(x86)\\Microsoft" "Office\\Office16\\`
   Pour Office 64 bits (x64)
   `cd c:\\Program" "Files\\Microsoft" "Office\\Office16\\`
3. Tapez `cscript ospp.vbs /dstatus`, puis appuyez sur Entrée.

   https://learn.microsoft.com/fr-fr/microsoft-365/troubleshoot/admin/licensing/media/determine-office-license-type/retail-type-license.png
   Dans l'exemple ci-dessus, l'écran affiche la licence de **type Version commerciale**. Si vous disposez d'un produit à licence en volume (VL), le type de licence s'affiche sous la forme **VL** ou **Volume Licensing**.

4. 

   - Licence pour activation archivage en ligne sur les BAL partagées pas cher
     Solutions d'archivage du courrier Microsoft Exchange

Groupes 365

Attention, les utilisateurs doivent s’abonner à la conversation de groupe sinon, ils ne recevront pas de copie du mail envoyé au groupe 0365.

Exchange Online: Subscribe Existing Members to Microsoft 365 Group Using PowerShell

- On peut forcer l’abonnement en SHELL.
- On peut redéfinir la politique par défaut > abonnement automatique.

Bloquer les connexion depuis une plage d'adresses IP

Bloquer l’accès à Office 365 à partir d’une adresse IP

Introduction

De plus en plus de collaborateurs travaillent en dehors des locaux de leur entreprise, depuis l’étranger, ou simplement lors de déplacements ponctuels. Afin d’assurer la sécurité et l’identité des utilisateurs, il est impératif de mettre en place des stratégies de sécurité. Nous verrons dans cet article comment faire cela avec Azure AD.

Prérequis

Avons de commencer, veuillez vérifier que vous disposez d’un abonnement ainsi que des licences utilisateurs « *Azure AD Premium P2*« .

Mise en place

Cliquer dans un premier temps sur votre Azure Active Directory. Puis dans la catégorie « **Sécurité** », allez dans « **Accès conditionnel** ».

Une nouvelle fenêtre apparait. Cliquez sur « **Nouvelle stratégie** ».

Dans cet exemple, nous souhaitons bloquer toutes les connexions pour l'utilisateur testazure en dehors des IP de sa société. Dans le champ « **Utilisateurs et groupes** », on spécifie le(s) utilisateur(s) qui seront affectés par la stratégie.

Nous pouvons également sélectionner « **Tous les utilisateurs** », puis dans l'onglet « **Exclure** » granuler en fonction de la stratégie. Dans le champ « **Applications cloud** », vous déterminez quelles seront les applications accessibles ou non. Si vous souhaitez que l'individu malveillant n'ait accès à aucunes applications, choisissez l'option « **Toutes les applications cloud** ».

Le champ « **Conditions** » comprend plusieurs onglets. Remarque : La stratégie s'activera si et seulement si la situation remplie **toutes les conditions**. Si vous laissez les onglets en statut « **Non configuré** », il ne prendra pas en compte cette élément. L'onglet « **Risque de connexion** » est présent grâce à la souscription de la licence P2. Il permettra l'automatisation de la sécurisation d'accès. Activer la condition en cliquant sur « **Oui** » puis « **Moyen** ». Vous trouverez les correspondances des niveaux de risques en cliquant sur le lien suivant :

https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-reporting-risk-events.

Cliquez sur l'onglet « **Emplacements** ». Ici, nous voulons bloquer l'accès au compte partout dans le monde sauf dans les locaux. Pour cela, activer la condition en cliquant « **Oui** » et on inclut l'option « **Tous les emplacements** ».

On exclut alors de cette stratégie notre adresse IP des locaux. Pour cela, aller dans l'onglet « **Exclure** ». On coche la case et on clique sur « **Configurer tous les emplacements approuvés** ».

Une nouvelle fenêtre s'ouvre. On spécifie une plage d'adresse à exclure, ou bien une seule adresse en /32. Puis cliquez tout en bas sur « **enregistrer** ».

Vous pouvez désormais fermer la fenêtre puis retourner sur le portail Azure et cliquer en bas « **Terminer** ». Dans le champ « **Application clientes** », cochez les deux applications clientes. Cliquez sur « **Terminer** » pour finaliser le champ « **Condition** ».

Pour finir, dans le champ « **Octroyer** », choisissez naturellement « **Bloquer l'accès** » et « **Demander un des contrôles sélectionnés** ». Pour finir, cliquez sur « **Activé** » pour mettre en marche la stratégie, puis « **Enregistrer** »

Notez que la mise en place de la stratégie peut ne pas être instantanée. Prévoyez quelques minutes avant la prise en compte.

Surveillance avec le module Identity Protection

Identity Protection est disponible après souscription d'une licence « *Azure AD Premium P2*« . Il permet de protéger les identités des utilisateurs, et d'empêcher proactivement l'accès aux identités compromises. Cela est possible grâce aux algorithmes de Machine Learning utilisé par Azure AD prévenant ainsi des dangers potentiels. Pour utiliser Azure Identity Protection, il faut dans un premier temps aller dans le Market Place, puis taper « Identity Protection » et cliquer sur le service. Il faudra épingler le service au tableau de bord. (Veuillez ensuite rafraîchir la page). S'affiche alors sur votre tableau de bord Azure Identity Protection. Cliquez dessus. On observe 3 fenêtres dans l'onglet « **Vue d'ensemble** ». La première fenêtre correspond à l'environnement des risques liés aux utilisateurs. Par exemple si les identifiants d'un utilisateur ont été volés. La deuxième fenêtre indique le niveau de risque des événements des sessions qui peuvent être anormale ou issu d'un environnement non-identifié. On remarque qu'il y'a 3 niveaux de criticité : **Haute**, **Moyenne** et **Faible** Enfin, la dernière fenêtre correspond aux failles de notre environnement pouvant être exploitées.

Si un des utilisateurs de l'organisation possède le niveau de criticité « Haute », on peut par exemple forcer la réinitialisation de son mot de passe.

Vérification

Afin de vérifier, on pourra tenter de se connecter à partir d'une autre adresse IP en dehors de la société. (Pour cela, j'utilise un VPN afin de simuler une IP externe). On remarque bien que l'accès n'est pas autorisé.

Conclusion

Il est donc primordial de sécuriser nos accès à Office365 ou autres applications en cas de vol d'identités. Identity Protection nous permet d'ajouter une couche supplémentaire de protection et de gérer les différents cas possibles comme la connexion simultané dans deux pays à un intervalle de temps quasi-nul et par conséquent obliger une réinitialisation du mot de passe par exemple. En fonction de votre environnement, vous pourrez donc définir plusieurs stratégies permettant d'accroitre considérablement la sécurité d'accès aux ressources de l'entreprise.

Rôle e-discovery et exportation de contenu

Comment utiliser l’outil d’exportation PST eDiscovery dans Office 365

Un compte de votre entreprise est déjà connecté

https://learn.microsoft.com/fr-fr/office/troubleshoot/activation/another-account-already-signed-in

- Pour les appareils Windows, procédez comme suit :
  1. Déconnectez-vous de toutes les applications Microsoft 365, puis reconnectez-vous.
  2. Si le problème persiste, modifiez le magasin de comptes OneAuth sur l'appareil :
     1. Accédez au dossier `%localappdata%\Microsoft\OneAuth\accounts`. Il contient un fichier <GUID> ou plusieurs fichiers ayant des GUID différents s'il existe plusieurs comptes.
     2. Ouvrez les fichiers à l'aide du Bloc-notes, examinez la valeur **account_hints** et identifiez les fichiers qui ne sont pas associés au compte utilisé pour vous connecter.
     3. Dans chaque fichier identifié à l'étape b, recherchez l'entrée **association_status**. Modifiez le statut d'association de `com.microsoft.Office` en **dissocié**, puis enregistrez le fichier. Par exemple, modifiez "*association_status": "{\"**com.microsoft.Office**\":\"**associated** \",\"com.microsoft.Outlook\":\"associated\"}*" au "*association_status": "{\"**com.microsoft.Office**\":\"**disassociated** \",\"com.microsoft.Outlook\":\"associated\"}*".
     4. Essayez de vous reconnecter.
  3. Si le problème persiste, déconnectez-vous de toutes les applications Microsoft 365, supprimez tous les dossiers aux emplacements suivants, puis reconnectez-vous :
     - `%localappdata%/Microsoft/OneAuth`
     - `%localappdata%/Microsoft/IdentityCache`
  4. Si le problème persiste, essayez d'autres méthodes de dépannage.