



PLAN DE MATCH · KORTEXS AI

Migrer vers les principaux de service

La procédure complète pour retirer la dépendance à un compte de service transversal — progressivement, flux par flux, sans interruption. De l'inventaire au démantèlement.

Préparé par : Nicolas Boulet-Lavoie · Kortexs AI

Pour : les équipes qui automatisent avec la Power Platform et veulent des identités de service propres, sécurisées et gouvernées.

kortexs.com/principaux-service-power-platform

De quoi part-on, et où va-t-on ?

Un principal de service ne consomme aucune licence et ne « part » jamais avec un employé. L'objectif de ce plan : y migrer sans casser ce qui tourne aujourd'hui.

POINT DE DÉPART

Un **compte de service transversal** utilisé un peu partout dans l'organisation, avec **Power Automate Premium** rattaché. Le convertir d'un coup casserait les flux.

LA CIBLE

Des **principaux de service dédiés par usage** (courriels, Dataverse...), secrets en coffre, droits au minimum, et un compte transversal **vidé puis démantelé**.

ACCÈS REQUIS

Ce qu'il faut avoir en main

Entra ID — Admin d'application (ou global)

Exchange Online — Admin

Power Platform — Admin

Azure Key Vault

Power Automate Premium (conservé)

Le principe directeur

- **Rien ne se retire avant validation.** Le compte transversal reste le filet de sécurité jusqu'au bout.
- **Un flux à la fois**, du moins risqué au plus critique — un retour arrière ne touche jamais qu'un seul flux.
- **L'économie de licence arrive à la fin.** Le vrai gain immédiat, c'est la robustesse et la gouvernance.

Sept phases, dans l'ordre

Chaque phase se coche quand elle est terminée. On n'entame la suivante qu'une fois la précédente validée.

Phase 00

≈ 1-2 jours

Préparation & inventaire

On ne migre rien tant qu'on ne sait pas ce qui tourne sous le compte.

- ☐ **Recenser tous les flux exécutés sous le compte de service**
Power Automate / centre d'administration. Le CoE Starter Kit accélère l'inventaire s'il est en place.
- ☐ **Noter pour chaque flux : connecteurs, courriels ?, Dataverse ?, criticité, fréquence**
Ce tableau déterminera l'ordre de migration.
- ☐ **Relever les droits actuels du compte**
Rôles Dataverse, appartenances Entra, accès Exchange. Objectif : reproduire au minimum, pas à l'identique.
- ☐ **Définir une convention de nommage**
Ex. `svc-courriels-prod`, `svc-dataverse-rh-prod`.
- ☐ **Préparer Azure Key Vault pour héberger les secrets**
Vérifier l'existant ou créer un coffre dédié, avec rotation prévue.

Créer le premier principal — envoi de courriels

On monte l'identité et on l'autorise à envoyer, sans encore toucher aux flux.

☐ **Créer l'inscription d'application dans Entra ID**

Noter le client ID et le tenant ID.

☐ **Générer un certificat (prod) ou un secret à échéance courte**

Déposer la valeur dans Key Vault. Jamais en clair dans un flux.

☐ **Ajouter la permission Graph `Mail.Send` (application) + consentement admin**

☐ **Créer / choisir la boîte partagée d'envoi**

Gratuite sous 50 Go, sans archive ni conservation légale.

☐ **Restreindre le principal à cette seule boîte (Application Access Policy)**

`New-ApplicationAccessPolicy` puis `Test-ApplicationAccessPolicy`.

Phase 02

≈ 2 h

Pilote sur un flux non critique

Valider la mécanique de bout en bout avant de toucher quoi que ce soit d'important.

- ☐ **Cloner un flux d'envoi non critique (ou en créer un de test)**
- ☐ **Remplacer l'action Outlook par une action HTTP → Graph `sendMail`**
Authentification « Active Directory OAuth », secret lu depuis Key Vault.
- ☐ **Tester : réponse `202` et courriel bien reçu**
Vérifier l'expéditeur, le rendu HTML et les pièces jointes si applicable.
- ☐ **Confirmer la traçabilité**
Connexion du principal dans les journaux Entra ; exécution propre dans l'historique du flux.

Phase 03

≈ 1-3 semaines

Migration progressive des flux de courriel

Un flux à la fois, du moins risqué au plus critique. Le compte transversal reste en place.

- ☐ **Ordonner les flux : non critiques d'abord, critiques ensuite**
- ☐ **Migrer, tester et valider chaque flux individuellement**
On ne passe au suivant qu'une fois le précédent confirmé en production.
- ☐ **Documenter chaque bascule**
Quel flux, quand, par qui, ancien vs nouveau.
- ☐ **Ne rien retirer au compte transversal pour l'instant**

Principaux pour Dataverse & autres connecteurs

Même logique côté Entra, mais sans Graph : on branche le principal dans l'environnement.

- ☐ **Créer un (ou des) principal(aux) dédié(s) par usage Dataverse**
- ☐ **Ajouter chaque principal comme utilisateur d'application dans l'environnement**
- ☐ **Attribuer un rôle de sécurité minimal (idéalement sur mesure)**
- ☐ **Créer les connexions « avec principal de service » et migrer les flux**

Répéter pour SQL et les autres connecteurs compatibles.

Phase 05

En continu

Gouvernance & surveillance

Une identité qui agit sans humain derrière doit être documentée et surveillée.

- ☐ Documenter chaque principal : usage, responsable, droits, échéance du secret
- ☐ Configurer des alertes d'expiration des secrets et certificats
- ☐ Mettre en place la surveillance
Journaux de connexion Entra, audit Dataverse, historique des flux.
- ☐ Planifier une revue périodique des accès

Phase 06

Quand plus rien n'en dépend

Démantèlement du compte transversal

L'économie de licence arrive ici — pas avant.

- ☐ Confirmer qu'aucun flux ni connexion ne dépend plus du compte
- ☐ Bloquer la connexion interactive / désactiver le compte
Étape réversible avant toute suppression définitive.
- ☐ Réévaluer la licence Power Automate Premium
Récupérer ou réaffecter, une fois la stabilité confirmée.
- ☐ Archiver la documentation de la bascule

Garde-fous — à ne jamais enfreindre

- **Jamais retirer une licence ou convertir une boîte avant** d'avoir migré et validé les flux concernés.
- **Secrets jamais en clair** — toujours via Azure Key Vault.
- **Mail.Send** sans **Application Access Policy** = **accès à tout le tenant**. La restriction est obligatoire.
- **Garder Power Automate Premium pendant toute la transition** : l'action HTTP vers Graph en dépend.
- **Un principal par usage** — pas de nouveau compte « fourre-tout ».

Plan de repli

- Le compte transversal reste actif tant que la migration n'est pas terminée : c'est le filet.
- Si un flux migré échoue, repointer sur l'ancienne version ou réactiver l'action Outlook, le temps de corriger.
- Chaque bascule étant faite une à une, un retour arrière ne touche qu'un seul flux.

Besoin d'un coup de main pour la migration ?

De l'inventaire au démantèlement, on met en place des identités de service propres et gouvernées, sans interrompre vos automatisations.

Nicolas Boulet-Lavoie · Kortexs AI

kortexs.com/#contact