PROCÉDURE DE MIGRATION

Active Directory On-Premise

Microsoft Azure Active Directory (Entra ID)

Propriété	Valeur
Référence	PRO-INFRA-001
Version	1.0
Date de création	Avril 2025
Dernière mise à jour	Avril 2025
Auteur	Direction des Systèmes d'Information
Statut	Approuvé
Classification	CONFIDENTIEL

Ce document décrit l'ensemble des étapes nécessaires à la migration sécurisée de l'Active Directory on-premise vers Microsoft Azure Active Directory (Entra ID). Il est destiné aux équipes DSI et administrateurs système.

1. Préambule et objectifs

1.1. Contexte

La migration de l'Active Directory (AD) on-premise vers Microsoft Azure Active Directory (désormais nommé Microsoft Entra ID) s'inscrit dans le cadre de la transformation numérique de l'organisation. Elle vise à tirer parti des avantages du cloud en matière de sécurité, de scalabilité et de gestion unifiée des identités.

1.2. Objectifs de la migration

- Centraliser la gestion des identités et des accès dans le cloud
- Activer l'authentification unique (Single Sign-On – SSO) pour toutes les applications
- Renforcer la sécurité via l'authentification multi-facteurs (MFA) et l'accès conditionnel
- Réduire les coûts liés à l'infrastructure on-premise
- Faciliter le travail hybride et le télétravail
- Assurer la conformité avec les réglementations en vigueur (RGPD, ISO 27001)

1.3. Périmètre de la migration

Elément	Inclus	Exclus
Comptes utilisateurs	Oui ✓	
Groupes de sécurité	Oui ✓	
Stratégies de groupe (GPO)	Partiel	GPO complexes à évaluer
Comptes de service	Oui ✓	
Objets ordinateurs	Hybride	Ordinateurs non compatibles
Applications LDAP		Non ✗ (migration séparée)

2. Prérequis et évaluation de l'environnement

2.1. Prérequis techniques

2.1.1. Infrastructure requise

- Abonnement Microsoft Azure actif avec un tenant Azure AD (Entra ID) configuré
- Licence Microsoft Entra ID P1 ou P2 (recommandée pour accès conditionnel et PIM)
- Serveur Windows Server 2016 ou supérieur pour l'hébergement d'Azure AD Connect
- Connectivité réseau entre l'AD on-premise et Azure (ExpressRoute ou VPN recommandé)
- Certificat SSL valide pour la fédération ADFS (si applicable)

2.1.2. Prérequis logiciels

Logiciel	Version minimale	Usage
Azure AD Connect	2.x (dernière)	Synchronisation des identités
PowerShell	5.1 ou 7.x	Scripts de migration

Logiciel	Version minimale	Usage
Module MSOnline	Dernière version	Administration Azure AD
Module AzureAD	Dernière version	Gestion des objets
Microsoft Graph SDK	Dernière version	Automatisation avancée
IdFix	Dernière version	Correction des attributs AD

2.2. Audit de l'Active Directory existant

Avant toute migration, un audit complet de l'AD on-premise doit être réalisé afin d'identifier les éventuels problèmes de compatibilité.

2.2.1. Exécution d'IdFix

IdFix est un outil Microsoft gratuit permettant d'identifier et de corriger les erreurs d'attributs dans l'AD qui pourraient empêcher la synchronisation.

1. Télécharger IdFix depuis le GitHub officiel Microsoft
2. Exécuter IdFix en tant qu'administrateur du domaine
3. Lancer l'analyse complète de l'annuaire
4. Corriger les erreurs identifiées : UPN dupliqués, caractères invalides, attributs manquants
5. Réexécuter l'analyse jusqu'à l'obtention d'un rapport sans erreur critique

> ⚠ Les attributs les plus fréquemment problématiques sont : mail, proxyAddresses, userPrincipalName et sAMAccountName. Assurez-vous que tous les UPN correspondent à un domaine vérifié dans Azure.

2.2.2. Inventaire des objets AD

Elément à inventorier	Nombre estimé	Remarques
Comptes utilisateurs actifs		À renseigner avant migration
Comptes utilisateurs inactifs		Désactiver avant migration
Groupes de sécurité		À renseigner avant migration
Unités organisationnelles (OU)		Cartographier la structure
Stratégies de groupe (GPO)		Identifier les équivalents Intune
Comptes de service		Créer des identités gérées Azure
Applications intégrées à l'AD		Planifier la migration applicative

3. Architecture de la solution cible

3.1. Modèles de déploiement

Trois approches de migration sont possibles selon le contexte de l'organisation :

Modèle	Description	Recommandé si
Azure AD seul	Migration complète vers le cloud. L'AD on-premise est décommissionné.	Environnement 100% cloud, nouvelles organisations
Hybride (synchronisé)	AD on-premise synchronisé avec Azure AD via Azure AD Connect. Les deux coexistent.	Environnement mixte, applications LDAP existantes
Hybride fédéré (ADFS)	Fédération via ADFS pour une authentification déléguée. Complexité plus élevée.	Besoins d'authentification spécifiques, exigences réglementaires

ℹ La présente procédure couvre principalement le modèle hybride synchronisé (Azure AD Connect), qui est le plus utilisé dans les migrations progressives. Adaptez les étapes selon le modèle choisi.

3.2. Méthodes de synchronisation

- Synchronisation de hachage de mot de passe (PHS) : recommandée pour la simplicité et la résilience
- Authentification directe (PTA) : les mots de passe sont vérifiés on-premise
- Fédération (ADFS) : pour des exigences d'authentification avancées

4. Procédure de migration pas à pas

4.1. Phase 1 – Préparation (J-30 à J-15)

4.1.1. Création et configuration du tenant Azure AD

6. Se connecter au portail Azure (https://portal.azure.com) avec un compte Administrateur global
7. Naviguer vers Microsoft Entra ID > Vue d'ensemble
8. Vérifier que le nom de domaine personnalisé est ajouté et vérifié
9. Configurer les informations du tenant (pays, fuseau horaire, contacts de sécurité)
10. Activer les licences Entra ID P1/P2 via le centre d'administration Microsoft 365

4.1.2. Vérification des domaines

11. Aller dans Entra ID > Noms de domaine personnalisés
12. Cliquer sur « Ajouter un domaine personnalisé » et saisir le nom de domaine FQDN
13. Ajouter l'enregistrement TXT indiqué dans la zone DNS du domaine
14. Cliquer sur « Vérifier » une fois la propagation DNS effective (de 15 min à 48 h)
15. Définir le domaine comme domaine principal si nécessaire

⚠ Les utilisateurs dont l'UPN contient un domaine non vérifié dans Azure AD seront synchronisés avec un UPN de type @<tenant>.onmicrosoft.com. Vérifiez tous les domaines avant la synchronisation.

4.2. Phase 2 – Installation et configuration d'Azure AD Connect (J-14 à J-7)

4.2.1. Installation d'Azure AD Connect

16. Télécharger la dernière version d'Azure AD Connect depuis le site Microsoft
17. Copier le fichier d'installation sur le serveur dédié (ne pas installer sur un contrôleur de domaine)
18. Exécuter le programme d'installation en tant qu'administrateur local
19. Choisir « Personnalisé » pour un contrôle complet de la configuration
20. Sélectionner la méthode d'authentification : Synchronisation de hachage de mot de passe (recommandé)
21. Saisir les informations d'identification de l'Administrateur global Azure AD
22. Saisir les informations d'identification de l'Administrateur d'entreprise AD on-premise
23. Sélectionner les forêts et domaines AD à synchroniser
24. Configurer le filtrage par unité organisationnelle si nécessaire
25. Activer l'option « Démarrer le processus de synchronisation » à la fin de la configuration

4.2.2. Validation de la synchronisation initiale

26. Ouvrir le Gestionnaire de services de synchronisation (Synchronization Service Manager)
27. Vérifier que le cycle de synchronisation s'est terminé sans erreur
28. Contrôler dans le portail Azure que les utilisateurs et groupes sont bien apparus
29. Vérifier les journaux d'événements Windows (Event Viewer > Azure AD Connect)
30. Comparer le nombre d'objets synchronisés avec le nombre d'objets dans l'AD on-premise

> **i** Commande PowerShell pour vérifier l'état de synchronisation : Start-ADSyncSyncCycle -PolicyType Delta Get-ADSyncConnectorRunStatus

4.3. Phase 3 – Migration des postes de travail (J-7 à J0)

4.3.1. Jonction hybride Azure AD (Hybrid Azure AD Join)

31. Configurer la jonction hybride dans Azure AD Connect (onglet Jonction de périphériques)
32. Vérifier que le point de connexion de service (SCP) est correctement configuré dans l'AD
33. Vérifier que les postes Windows 10/11 peuvent atteindre les URL Microsoft nécessaires
34. Déclencher la jonction sur un poste pilote : dsregcmd /join
35. Vérifier l'état avec la commande : dsregcmd /status
36. Contrôler l'affichage du poste dans Entra ID > Périphériques
37. Déployer la jonction sur le parc complet via GPO ou Microsoft Intune

4.3.2. Migration des politiques (GPO vers Intune)

- Identifier les GPO actives et leur équivalent dans Microsoft Intune
- Utiliser l'outil « Group Policy Analytics » dans Intune pour analyser la compatibilité
- Créer les profils de configuration Intune correspondants
- Tester les profils sur un groupe pilote avant déploiement général
- Documenter les GPO sans équivalent Intune pour traitement spécifique

4.4. Phase 4 – Activation du MFA et de l'accès conditionnel (J0 à J+7)

4.4.1. Déploiement de l'authentification multi-facteurs

38. Aller dans Entra ID > Sécurité > Méthodes d'authentification
39. Activer Microsoft Authenticator comme méthode principale

40. Déployer en mode « rapport uniquement » d'abord pour mesurer l'impact
41. Communiquer aux utilisateurs les instructions d'inscription au MFA
42. Définir une période d'inscription de 14 jours avant application forcée
43. Activer la politique MFA en mode forcé après la période d'inscription

4.4.2. Configuration de l'accès conditionnel

- Politique 1 : Exiger le MFA pour tous les utilisateurs hors réseau de confiance
- Politique 2 : Bloquer l'accès depuis des pays non autorisés
- Politique 3 : Exiger un appareil conforme (Compliant Device) pour l'accès aux données sensibles
- Politique 4 : Exiger le MFA pour les administrateurs en toutes circonstances
- Politique 5 : Bloquer l'authentification héritée (Legacy Authentication)

⚠	Testez toujours les politiques d'accès conditionnel en mode « Rapport uniquement » avant de les activer. Une mauvaise configuration peut bloquer l'accès à tous les utilisateurs, y compris les administrateurs.

5. Plan de bascule et coupure

5.1. Prérequis à la bascule

Contrôle préalable à la bascule	Statut	Responsable
100% des utilisateurs synchronisés dans Azure AD	En attente	Administrateur AD
MFA activé sur 100% des comptes actifs	En attente	Administrateur Sécurité
Tous les postes en jonction hybride Azure AD	En attente	Administrateur Poste
Applications cibles migrées vers SSO Azure AD	En attente	Architecte Applicatif
Plan de retour arrière testé et validé	En attente	Chef de Projet
Communication utilisateurs effectuée	En attente	DSI / Communication
Sauvegarde complète de l'AD on-premise	En attente	Administrateur AD

5.2. Procédure de bascule

44. Planifier la bascule un vendredi soir ou en période de faible activité
45. Notifier les utilisateurs 48 h avant la bascule
46. Réaliser une sauvegarde complète de l'AD on-premise et d'Azure AD Connect
47. Lancer un cycle de synchronisation forcé final
48. Désactiver les comptes utilisés uniquement on-premise
49. Basculer les applications vers l'authentification Azure AD
50. Vérifier le bon fonctionnement des applications critiques
51. Surveiller les journaux d'audit Azure AD pendant les 24 premières heures
52. Activer le support étendu pour les 72 premières heures post-bascule

6. Plan de retour arrière (Rollback)

En cas d'échec critique de la migration, la procédure suivante permet de revenir à l'état initial :

1. Identifier la nature et l'impact de l'incident
2. Activer l'escalade d'urgence (contact DSI + RSSI)
3. Si retour arrière nécessaire : désactiver Azure AD Connect (mode de transit)
4. Rétablir les authentifications vers l'AD on-premise pour les applications concernées
5. Restaurer les contrôleurs de domaine depuis la sauvegarde si nécessaire
6. Documenter l'incident et les actions correctives
7. Planifier une nouvelle date de migration après correction des causes

ℹ	Le plan de retour arrière doit être testé en environnement de pré-production avant toute migration en production. La durée maximale acceptée pour un retour arrière est de 4 heures.

7. Sécurité et conformité

7.1. Gestion des identités privilégiées (PIM)

- Activer Azure AD Privileged Identity Management (PIM) pour tous les rôles d'administrateur
- Configurer l'accès juste-à-temps (Just-in-Time) pour les rôles sensibles
- Définir une durée maximale d'activation de 4 heures pour les rôles d'administrateur global
- Exiger une justification et une approbation pour l'activation des rôles critiques
- Mettre en place des revues d'accès trimestrielles pour tous les rôles privilégiés

7.2. Surveillance et audit

- Activer Microsoft Defender for Identity pour la détection des menaces sur l'AD
- Configurer Microsoft Sentinel pour la collecte et l'analyse des journaux
- Définir des alertes sur les événements à risque : connexions inhabituelles, échecs MFA, etc.
- Conserver les journaux d'audit pendant minimum 90 jours (1 an recommandé)
- Réaliser des revues de sécurité mensuelles des politiques d'accès conditionnel

7.3. Conformité RGPD

- S'assurer que les données des utilisateurs sont hébergées dans une région conforme (Europe de l'Ouest)
- Documenter les flux de données entre l'AD on-premise et Azure AD
- Mettre à jour le registre des activités de traitement (RAT)
- Vérifier les clauses du contrat de traitement des données (DPA) avec Microsoft

8. Formation et accompagnement des utilisateurs

8.1. Plan de communication

Timing	Action de communication	Canal	Cible
J-30	Annonce de la migration	Email + Intranet	Tous les utilisateurs
J-21	Guide d'installation MFA	Email + Portail aide	Tous les utilisateurs
J-14	Webinaire de présentation	Teams	Managers et référents IT
J-7	Rappel et FAQ	Email	Tous les utilisateurs
J0	Confirmation de bascule	Email	Tous les utilisateurs
J+1	Enquête de satisfaction	Teams / Email	Tous les utilisateurs

8.2. Documentation utilisateur

- Guide d'installation et d'utilisation de Microsoft Authenticator
- Procédure de connexion au nouveau portail Azure AD (My Apps)
- FAQ sur les changements liés à la migration
- Procédure de réinitialisation du mot de passe en libre-service (SSPR)
- Guide de signalement des incidents à la DSI

9. Suivi et tableau de bord post-migration

9.1. Indicateurs clés de performance (KPI)

Indicateur	Cible	Fréquence de mesure
Taux d'adoption du MFA	> 99%	Hebdomadaire
Taux de synchronisation des objets	100%	Quotidienne
Nombre d'incidents post-migration	0	Quotidienne (J+30)
Délai de résolution des incidents	< 4 heures	Par incident
Taux de postes en jonction hybride	> 95%	Hebdomadaire
Satisfaction utilisateur	> 4/5	Mensuelle

9.2. Actions post-migration (J+30)

- Analyser les rapports de connexion Azure AD et identifier les anomalies
- Vérifier que tous les utilisateurs ont bien enregistré leurs méthodes MFA
- Désactiver les anciens comptes et références à l'AD on-premise
- Planifier le décommissionnement progressif des contrôleurs de domaine on-premise
- Réaliser un bilan de la migration et documenter les leçons apprises

10. Contacts et escalade

Rôle	Nom / Équipe	Contact	Disponibilité
Chef de projet migration	À compléter	À compléter	Jours ouvrés
Administrateur Azure AD	À compléter	À compléter	Jours ouvrés
RSSI	À compléter	À compléter	Jours ouvrés
Support Microsoft (P1)	À compléter	1-800-MICROSOFT	24h/24 - 7j/7
Helpdesk DSI	À compléter	À compléter	Jours ouvrés

11. Historique des révisions

Version	Date	Modifications	Auteur
1.0	Mai 2025	Création initiale du document	DSI

✓	Ce document doit être validé par le Responsable DSI et le RSSI avant tout début de migration en production. Toute modification doit faire l'objet d'une nouvelle version et d'une revalidation.