IDENTITY DAYS

20 octobre 2026
PARIS · NEWCAP

Gestion des identités (Entra ID,...)
Carve-in et carve-out

Ludovik DOPIERALA

Migration tenant-to-tenant

Agenda

01 Contexte et deux logiques
02 Objets Entra et coexistence
03 Approches et cinq phases
04 Vigilance et checklist
05 Synthèse & échanges

Public · RSSI · DSI

Ludovik DOPIERALA
Service Line Manager
alt-up by Artemys
Plus de 30 ans sur Microsoft et la sécurisation des identités. Je conduits les carve-in et les carve-out vers Entra ID au sein du groupe Artemys.

Public

Fil rouge : le cas fictif de NordHorizon

Cas fictif Helia : comptes, UPN, groupes, applications, MFA et appareils.

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

NordHorizon cède Helia (480 personnes, 2 usines) à AltaVia. Les comptes quittent nordhorizon.onmicrosoft.com pour altavia.com. Bascule le samedi, usines ouvertes le lundi.
Objectif : séparer deux tenants ne se limite pas à changer les UPN.
Continuité : la paie (Business Central) est en SSO. Si helias.fr n'est pas vérifié, le pointage est bloqué.
Carve-out : ne pas couper Entra Connect avant la carte des dépendances. Le compte svc-helix-edi est hors export RH.
Carve-in : 12 comptes @altavia.com existent déjà. Table de correspondance figée. Première vague : 60 comptes.
Risques : boîte planning-usine sans propriétaire, SG-Helia-Admins encore admin, certificat SAP qui expire samedi.
Volume : 480 utilisateurs, 1 200 groupes, 40 applications, 90 identités non humaines.

UPN : identifiant de connexion · MFA : authentification multifacteur · SSO : authentification unique · TSA : services transitoires · J+90 : 90 jours après le Jour J

Ce que vous emporterez

Quatre décisions à prendre avant le week-end de bascule, dans l'ordre de la session.

01 · COMPRENDRE

Deux opérations, deux plans

- Carve-out : cloner puis isoler le tenant
- Carve-in : faire correspondre les comptes, puis fusionner par vagues
- Le plan de l'un ne s'applique pas à l'autre

02 · MIGRER

Ces objets ne suivent pas la boîte

- ImmutableID, UPN, groupes, applications
- Accès conditionnel, MFA et appareils Intune à refaire
- Comptes de service, certificats et secrets : hors export RH

03 · CHOISIR

L'outil ne choisit pas la cible

- Natif Microsoft (CTIM), puis migration des données
- Outil tiers si le volume ou la coexistence l'exige
- Scripts Graph seulement pour les écarts restants

04 · PROUVER

Checklist du Jour J, à 8 h

- Correspondance validée et MFA réenregistré
- Accès conditionnel cible, journaux dès le Jour J
- Retour arrière écrit, avec une heure limite

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Helia quitte nordhorizon.onmicrosoft.com pour altavia.com. Séparer un tenant et intégrer des comptes dans un tenant existant, ce n'est pas le même plan.

CA : accès conditionnel · NHI : identités non humaines · CTIM : correspondance des identités entre tenants · TSA : services transitoires

01 · Contexte et deux logiques

Le juridique et la finance closent le deal. Sans identités, MFA et SSO, le lundi n’est pas un nouveau départ : c’est un incident.

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

NordHorizon cède Helia à AltaVia. 480 identités quittent le tenant source pour altavia.com. Bascule le samedi, usines ouvertes le lundi.

MFA : authentification multifacteur · SSO : authentification unique · IdP : fournisseur d’identité

L’IAM, condition du Jour J

Ce n’est pas un projet de plus. Sans accès le lundi, la cession n’est pas opérable.

CONTINUITÉ

Sans accès, l’activité s’arrête

- Messagerie, ERP, paie, VPN, SSO métier
- IdP ou MFA en panne : le métier s’arrête
- Chemin normal et repli testés avant le lundi

SÉCURITÉ

La cession laisse des accès ouverts

- Comptes du groupe encore valides dans l’entité, et l’inverse
- Admins, partages, délégations, groupes trop larges
- Chaque oubli reste un point d’entrée tant qu’il n’est pas daté

CONFORMITÉ

Il faudra le prouver

- SOX, RGPD, NIS2, audit interne
- Qui avait accès, qui a approuvé, quels journaux restent
- Sans journaux au Jour J, la séparation ne se valide pas

COÛT

Un TSA sans date s’installe

- IdP, MFA, messagerie ou PAM encore opérés par le groupe
- Souvent 6 à 18 mois, sans prix ni pénalité de sortie
- Le traitement au ticket allonge le coût et le délai

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Lundi 8 h : la paie Helia passe par Business Central en SSO. Si helias.fr n’est pas vérifié, ou si le MFA source est coupé trop tôt, le pointage est bloqué.

IdP : fournisseur d’identité · TSA : services transitoires · PAM : accès à privilèges · ERP : progiciel de gestion

Carve-out et carve-in : deux plans

Carve-out : on sépare l'entité du groupe. Carve-in : on l'intègre chez l'acquéreur. Le plan d'identités se choisit avant le contrat de cession, pas le week-end du closing.

CONDUITE DU CHANGEMENT => UN CHANTIER A NE PAS NEGLIGER

CARVE-OUT · SÉPARER

Cloner, puis isoler

- Répliquer annuaire, comptes, groupes et applications critiques
- Ensuite seulement : couper trusts, synchro, admins et journaux
- Le clone fait tenir le lundi. Ce n'est pas la cible.

CARVE-OUT · TSA

Qui opère, jusqu'à quand

- IdP, MFA, messagerie ou PAM encore tenus par le groupe
- Périmètre, coût, droit d'audit, date de sortie, pénalité
- Sans date de fin, le TSA devient l'architecture

CARVE-IN · INTÉGRER

Faire correspondre, puis fusionner

- Deux annuaires, deux nommages, attributs RH incompatibles
- Table de correspondance validée avant le closing
- Intégration par vagues, pas un ticket par personne

CARVE-IN · DROITS

Le moindre privilège, dès le Jour J

- Lots d'accès par métier, pas une copie des groupes source
- Une pratique admise à la source peut être interdite chez l'acquéreur et inversement
- Toute exception a une date de fin

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

Carve-out : répliquer les 480 comptes, puis retirer Helia des accès conditionnels NordHorizon. Carve-in : UPN en @helia.altavia.com, sans recopier le groupe ALL-NORDHORIZON.

SPA : contrat de cession · TSA : services transitoires · UPN : identifiant de connexion · PAM : accès à privilèges

02 · Objets Entra et coexistence

Les boîtes et les fichiers se migrent avec un outil. Les identités, pas toujours. Il faut séparer sans couper l'activité, et intégrer sans ouvrir tous les droits.

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

Deux erreurs classiques : couper Entra Connect trop tôt, ou laisser SG-Helia-Admins en Global Admin après la cession.

M365 : Microsoft 365 · SG : Security Group (groupe de sécurité)

Carve-out : séparer sans interrompre

On ne coupe pas un annuaire d'un coup. On cartographie les dépendances, on clone pour séparer, puis on isole.

Réussir un carve-out, c'est couper les liens sans couper l'activité

ANNUAIRES

Ce qui casse si l'on coupe trop tôt

- AD, Entra ID, synchro, trusts, applications encore authentifiées sur le groupe
- Sans cette carte, le Jour J coupe la paie en même temps que le pont

ACCÈS CROISÉS

Les liens qui restent

- Comptes croisés, admins cloud, partages, boîtes déléguées, invités Teams
- Chaque accès est coupé, daté, ou confié à un propriétaire nommé

JOUR J

Cloner, puis séparer

- D'abord identités, groupes et applications critiques
- Ensuite admins, journaux, comptes d'urgence et secrets

IDENTITÉS NON HUMAINES

L'angle mort

- Comptes de service, certificats, API, robots : absents de l'export RH
- À la fin du TSA, ils cassent la production ou laissent un accès ouvert

EN SALLE
Question
- Quelles applications s'authentifient encore sur l'annuaire du groupe ?

EN SALLE
Preuve
- Carte des flux, comptes à privilèges isolés, repli testé

EN SALLE
Alerte
- Synchro coupée trop tôt, compte technique sans propriétaire

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Entra Connect Helia dépend encore de l'AD NordHorizon. Le couper trop tôt bloque les mises à jour de comptes. svc-helix-edi, compte SAP, n'est pas dans l'export RH.

AD : annuaire local · NHI : identités non humaines · TSA : services transitoires · API : interface applicative

Carve-in : intégrer sans tout ouvrir

Des centaines de personnes doivent travailler dès le closing. Un ticket par personne et le support ne pourra pas absorber pas ce volume.

Réussir un carve-in, c’est donner à chacun sa place sans lui ouvrir toutes les portes.

DEUX ANNUAIRES

Une table de correspondance

- UPN, samAccountName et attributs RH ne se correspondent pas
- Avant le closing : fusion, renommage, invité, ou coexistence

APRÈS LE JOUR J

Des vagues, pas une file d’attente

- D’abord direction, paie, support et ateliers
- Le reste suit un calendrier, pas l’urgence d’un manager

POLITIQUES

Deux règles de sécurité à aligner

- MFA, accès conditionnel, durée de session, revues d’accès
- Ce qui était admis à la source peut être interdit chez l’acquéreur et réciproquement

DOUBLONS

Une personne, deux comptes

- Messagerie en conflit, licence payée deux fois, coffre à privilèges dupliqué
- À trancher avant la bascule : après, on ne sait plus quel compte fait foi

EN SALLE

Question

- Quel compte devient la référence, pour chaque personne ?

EN SALLE

Preuve

- Table approuvée, lots d’accès testés, doublons tranchés

EN SALLE

Alerte

- Deux comptes actifs, groupe source recopié, exception sans date

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

Douze personnes Helia ont déjà un compte @altavia.com. La table tranche : fusion, renommage en @helia.altavia.com, ou invité B2B limité à 90 jours. Vague 1 : 60 comptes.

UPN : identifiant de connexion · B2B : invité Entra · PAM : accès à privilèges · SoD : séparation des tâches

Sept objets qui ne suivent pas la messagerie

Boîtes et fichiers : un outil suffit. Ces objets Entra se préparent avant, sinon le lundi casse.

NE PAS OUBLIER L'IDENTITE PRICIPALE => L'UTILISATEUR !!!

1
ImmutableID
– sourceAnchor = ImmutableID. Hard match avant l'import
– Un soft match sur l'UPN peut créer un second compte

2
UPN et domaines
– Le suffixe doit être vérifié dans le tenant cible
– Domaine absent : le SSO de la paie ne répond plus

3
Groupes
– Les appartenances se rejouent, elles ne se copient pas
– SG-Helia-Admins ne devient pas admin de la cible

4
Applications
– Apps d'entreprise, consentements, secrets, propriétaires
– svc-helix-edi n'est pas dans l'export RH

5
Accès conditionnel
– Les stratégies se reconstruisent, elles ne se collent pas
– Revoir l'exclusion des comptes d'urgence avant la bascule

6
Méthodes MFA
– Authenticator ne migre pas avec le compte
– Réenregistrement prévu, mode d'emploi envoyé avant

7
Appareils Intune
– Jonction Entra, Autopilot, conformité
– Un poste d'usine non testé bloque le lundi

EN SALLE
Question
– Quel objet n'a pas encore de règle de correspondance ?

EN SALLE
Preuve
– ImmutableID, UPN, accès conditionnel et postes pilotes validés

EN SALLE
Alerte
– Soft match non contrôlé, MFA découvert le samedi

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Helia : ImmutableID figé avant l'import, helias.fr à vérifier, 15 postes pilotes, MFA à réenregistrer. SG-Helia-Admins n'est pas repris.

UPN : identifiant de connexion · MFA : authentification multifacteur · CA : accès conditionnel

Sécurité et conformité : cinq risques

Accès conditionnel, Zero Trust, RGPD, audit. Chaque risque a un responsable, un indicateur et une date.

Le temporaire ne doit pas devenir la règle

01
Comptes orphelins
- Actifs, sans manager, souvent hors SIRH
- Prestataires partis, boîtes génériques
- Admins de projet jamais repris
- Porte d'entrée classique après la cession

02
Accès trop larges
- Rôles hérités du groupe cédant
- Groupes AD fourre-tout, admins locaux
- Droits ouverts « pour que ça marche »

03
Applications hors inventaire
- SaaS absent de l'inventaire
- Consentements OAuth inconnus
- Invisibles pendant l'audit préalable
- Visibles au premier incident, ou … à la facture

04
Service interrompu
- MFA en panne, SSO non basculé
- Certificat expiré pendant le week-end
- Synchronisation arrêtée trop tôt
- Le repli se teste avant le samedi

05
Preuve absente
- Personne ne peut dire qui avait accès
- Journaux perdus à la fin du TSA
- Séparation des tâches impossible à démontrer
- Sans journaux au Jour J, l'audit ne s'applique pas

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
planning-usine n'a pas de propriétaire. SG-Helia-Admins est encore Global Admin. Le certificat SAP expire pendant le week-end. Sans journaux au Jour J, l'audit ne se défend pas.

MFA : authentification multifacteur · SSO : authentification unique · TSA : services transitoires · SIRH : système RH

Trois façons de migrer, un seul scénario

Le modèle Microsoft fixe d'abord le scénario : bascule unique, par vagues, ou scission. L'outil vient après.

Outils tiers et scripts => se faciliter la vie

MICROSOFT · NATIF

Correspondre avant de déplacer

- CTIM : correspondance 1 pour 1, avant les données
- Écrit ExchangeGuid, adresses X.500 et proxyAddresses
- Bascule unique, par vagues, ou scission

OUTIL TIERS

Quand le natif ne couvre pas le parc

- Quest, BitTitan, AvePoint, ShareGate, Cloudyway, PSP,...
- Utile si le volume est important, si la coexistence est longue ou qu'on se facilite la vie
- La table de correspondance reste obligatoire

SCRIPTS

Graph et PowerShell, sur le delta

- Vagues, licences, groupes, orphelins, accès conditionnel
- Un script qu'on ne peut pas rejouer n'est pas un plan
- Pour les écarts seulement, pas pour tout migrer

MODÈLE MICROSOFT

Choisir le scénario d'abord

- Bascule unique : une usine, un samedi
- Par vagues : accès invité B2B pendant le TSA
- Scission : le tenant se sépare, puis rejoint la cible

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

Helia : scission. CTIM pour les 480 identités, scripts pour l'écart sur les groupes, outil tiers pour les boîtes. Pas l'inverse.

CTIM : correspondance des identités entre tenants · TSA : services transitoires · B2B : invité Entra

03 · Approches et cinq phases

Le scénario se choisit avant le closing. Plus le rapprochement des comptes est fait tôt, plus le Jour J est une bascule, pas un sauvetage.

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
On n'improvise pas le samedi. CTIM, table des UPN et postes pilotes Intune sont prêts avant le contrat, pas le week-end.

UPN : identifiant de connexion · SPA : contrat de cession · CTIM : correspondance entre tenants

Cinq phases, du contrat au Jour J

Ce qui n’est pas inventorié et testé avant le closing se paie le lundi, en incident.

Chaque étape ignorée devient un incident à gérer après.

1
Audit préalable
– IdP, IGA, PAM, MFA, comptes techniques
– Applications en SSO et flux critiques
– Risques écrits dans le contrat

2
Cible
– Séparer, fusionner ou orchestrer
– Périmètre du TSA et date de sortie
– Qui approuve, qui opère, qui audite

3
Préparation
– Désactiver orphelins et dormants
– Table source vers cible, figée
– Tester MFA, SSO et le repli

4
Exécution
– Carve-out : cloner, puis isoler
– Carve-in : intègre par vagues
– Go / no-go et heure de retour

5
Après
– Exceptions datées, revue des accès
– Sortie du TSA, licences en double
– Le SIRH redevient la source

EN SALLE
Phases 1-2
– Inventaire validé, risques au contrat, responsable nommé

EN SALLE
Phases 3-4
– Lots d’accès testés, frontières coupées, journaux au Jour J

EN SALLE
Phase 5
– TSA daté, ancien IdP éteint, mode d’emploi du prochain deal

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Phase 1 : 480 utilisateurs, 1 200 groupes, 40 applications, 90 identités non humaines. Samedi : boîtes, UPN, MFA AltaVia. À J+90 : helias.fr retiré, licences sources libérées.

IGA : gouvernance des identités · PAM : accès à privilèges · TSA : services transitoires · JML : arrivées, mobilités, départs

Public

Voir clair, puis décider

Phases 1 et 2 : le Jour J se joue ici, pas dans la cellule de crise du dimanche.

Chaque décision repoussée prépare la crise du Jour J

PHASE 1 · AUDIT

Un inventaire utile au deal

- IdP, annuaires, IGA, PAM, MFA, applications en SSO
- Accès critiques et identités non humaines
- Trusts, synchros, et flux dont le métier dépend vraiment

PHASE 1 · PREUVES

Ce qui entre dans la data room

- Écarts, licences manquantes, dépendances, risques au contrat
- Une IAM non écrite est un passif au closing

PHASE 2 · CIBLE

Une décision, datée

- Annuaires séparés, ou fusion vers un seul IdP
- Ou une couche d'orchestration, le temps du TSA
- Une cible, une date, et ce qui reste hors périmètre

PHASE 2 · GOUVERNANCE

Qui décide

- Rôles cibles, accès par rôle ou par attribut, MFA
- Qui approuve un accès le Jour J, qui opère, qui audite
- Sans nom sur la fiche, la cellule de crise n'a personne à appeler

EN SALLE
Question
- Quelle cible, quel TSA, quel responsable ?

EN SALLE
Preuve
- Inventaire signé, risques au contrat, rôles approuvés

EN SALLE
Alerte
- Dépendance inconnue, cible non tranchée, rôle non nommé

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Data room : 14 applications OAuth inconnues, 22 Global Admins, une exclusion d'accès conditionnel sur breakglass-nord. Cible : tenant AltaVia, invités B2B 90 jours, pas de fusion des annuaires.

IGA : gouvernance des identités · SPA : contrat de cession · TSA : services transitoires · B2B : invité Entra

Nettoyer, puis basculer

Phases 3 et 4 : on ne déplace pas une dette d'identités. On la réduit avant de bouger.

SE BASER SUR LE FICHIER RH => UNE FAUSSE BONNE IDEE

PHASE 3 · NETTOYAGE

Moins de dette, moins de surprises

- Désactiver orphelins, dormants et comptes sans propriétaire
- Revoir les privilèges et les comptes d'urgence
- Préparer les lots d'accès du Jour J, par population

PHASE 3 · ESSAI

Tester avant le week-end

- MFA, SSO des applications critiques, repli, comptes d'urgence
- Message figé : nouvel identifiant, ce qui change, qui appeler
- Un test raté le jeudi vaut mieux qu'une usine arrêtée le lundi

PHASE 4 · CARVE-OUT

Cloner, puis fermer

- Isoler admins, journaux et comptes d'urgence
- Couper les accès croisés à l'heure dite, ou leur donner une date de fin
- Le clone ne doit pas devenir un second groupe, par oubli

PHASE 4 · CARVE-IN

Par vagues

- Provisionnement automatique de la vague 1
- Critères de go / no-go affichés dans la cellule de crise
- Preuves : journaux, revue des lots, inventaire du Jour J

EN SALLE

Question

- Qu'est-ce qui déclenche le go, le no-go, ou le retour arrière ?

EN SALLE

Preuve

- Pilotes OK, lots validés, retour arrière chronométré

EN SALLE

Alerte

- Test incomplet, accès temporaire sans date, heure de retour inconnue

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA

Jeudi : 15 boîtes pilotes, avec Teams et OneDrive. Samedi 22 h : vague 1 migrée. Invités B2B NordHorizon révoqués, sauf le compte du TSA messagerie, jusqu'au 14 juin.

MFA : authentification multi facteur · SSO : authentification unique · TSA : services transitoires · B2B : invité Entra

Public

Après le Jour J, le travail continue

Le closing n'éteint ni les exceptions, ni le TSA, ni l'ancien fournisseur d'identité.

Le carve se termine quand la dernière dépendance est coupée !

STABILISER
Chaque exception a une date
- Tickets, dérogations TSA, applications pas encore basculées
- Sans date, l'exception redevient la règle

GOUVERNER
Le cycle de vie reprend
- Re certification, séparation des tâches, revue des privilèges
- Le SIRH redevient la source. Les comptes « urgence » y rentrent

RATIONALISER
Éteindre les ponts
- Sortie des TSA, ancien IdP, licences et connecteurs en double
- Chaque mois de TSA est un coût et une dépendance

OUTILS
Industrialiser
- IGA pour le cycle de vie, PAM pour les privilèges, SIRH comme source
- Au ticket, le volume d'un carve dépasse l'équipe

EN SALLE
Question
- Qui ferme chaque exception, et chaque service du TSA ?

EN SALLE
Preuve
- Re certification faite, propriétaires confirmés, sortie du TSA suivie

EN SALLE
Alerte
- Exception sans date, connecteur historique encore actif

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
J+30 : revue des 40 applications reprises. J+90 : fin du TSA Exchange, helias.fr retiré de NordHorizon, licences E3 rendues. Les comptes « urgence » rentrent dans le processus AltaVia.

IGA : gouvernance des identités · PAM : accès à privilèges · TSA : services transitoires · JML : arrivées, mobilités, départs

04 · Vigilance et checklist

Sept réflexes à figer avant la signature, six façons de rater le week-end, et ce qui doit être vrai le lundi à 8 h.

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Trois semaines avant : le mode d'emploi MFA AltaVia est envoyé aux 480 personnes. Le samedi, on ne découvre pas Authenticator.

M365 : Microsoft 365 · MFA : Multi-Factor Authentication (authentification multifacteur)

Public

Sept réflexes, avant la signature

Tous se décident avant la signature, pas dans la cellule de crise.

1
Dès l'audit
– L'IAM est dans la data room et le contrat
– Pas un chantier ouvert après le closing

2
Nettoyer avant
– Orphelins, dormants, admins oubliés
– Moins de dette emportée le Jour J

3
Automatiser les arrivées
– Arrivées, mobilités, départs : par vagues datées
– Le ticket unitaire ne tient pas le volume

4
Privilèges à part
– PAM, comptes d'urgence, admins : inventaire dédié

5
Dater les TSA
– Prix, droit d'audit, date de sortie, pénalité
– Sans date, le provisoire devient définitif

6
Prévenir tôt
– Nouvel identifiant, MFA, qui appeler
– Personne ne le découvre le lundi matin

7
Mesurer le Jour J
– Accès OK, incidents P1, comptes encore croisés
– Sans chiffre, le go / no-go est une impression

EN SALLE
Question
– Quel sujet manque encore au plan ?

EN SALLE
Preuve
– Noms, automatisation prête, message envoyé

EN SALLE
Alerte
– Action sans propriétaire, aucun indicateur du Jour J

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
L'export Entra Helia est dans la data room avant le contrat. Les 22 Global Admins sortent du périmètre avant le clone. Le mode d'emploi UPN et MFA part trois semaines avant.

SPA : contrat de cession · PAM : accès à privilèges · JML : arrivées, mobilités, départs · P1 : incident critique

Six façons de rater la bascule

Six pièges vus sur le terrain. Tous se voient avant le week-end, si on les nomme.

ATTENDRE LE CLOSING
Le Jour J devient une urgence
– Trusts, synchros et applications se découvrent le week-end
– On répare au lieu de basculer

TOUT OUVRIR
Le temporaire reste
– Les droits « pour que ça marche » ne sont jamais retirés
– Ils deviennent le modèle d'accès, et sortent des revues

OUBLIER LES COMPTES TECHNIQUES
Hors liste, hors contrôle
– Comptes de service, API, certificats, robots
– Sans propriétaire, ils cassent le lundi ou survivent au TSA

TSA SANS DATE
La dépendance s'installe
– Coût flou, sortie jamais planifiée
– Un TSA est un pont négocié, pas l'architecture

PAS DE CELLULE DE CRISE
SSO en panne, personne ne sait
– Le lundi, les utilisateurs appellent
– Sans astreinte et sans retour arrière, tout s'arrête sur un MFA

AUCUNE PREUVE
L'audit arrive après
– Six mois plus tard, les journaux du TSA ont disparu
– Une séparation non écrite ne se défend pas

EN SALLE
Question
– Quel scénario peut encore stopper le métier le lundi ?

EN SALLE
Preuve
– Risques à jour, repli écrit, circuit d'appel défini

EN SALLE
Alerte
– Hypothèse non testée, dépendance invisible, aucun journal

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
« On met All Users en temporaire » : les 480 Helia voient le SharePoint Finance AltaVia. Sans date, Entra Connect reste branché à la source. Le certificat SAP, oublié, casse l'EDI le lundi.

NHI : identités non humaines · TSA : services transitoires · EDI : échanges informatiques

Checklist du lundi, 8 h

Dix contrôles avant la première connexion. Si une ligne critique est fausse, ce n’est pas un go.

1
Tenant cible joignable
– MFA actif, méthodes réenregistrées, repli testé

2
SSO critique validé
– Paie, ERP, messagerie, VPN : pas tout le catalogue

3
Correspondance figée
– ImmutableID et UPN validés, pas de rapprochement automatique

4
Comptes d’urgence testés
– Documentés, et hors du chemin normal

5
Admins isolés
– Plus aucun droit hérité du groupe sur le périmètre

6
Vague 1 et postes
– Lots d’accès créés, postes pilotes joints

7
Cellule de crise en place
– Noms, téléphones, critères de go / no-go affichés

8
Journaux et accès conditionnel
– Connexions, administration, stratégies : preuve dès 8 h

9
TSA écrits
– Périmètre, opérateur, escalade, date de sortie

10
Retour arrière connu
– Qui le déclenche, jusqu’à quelle heure, quel impact

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
8 h : helias.fr vérifié, MFA AltaVia réenregistré, SSO Business Central OK sur 15 pilotes, journaux collectés, TSA messagerie jusqu’au 14 juin.

UPN : identifiant de connexion · MFA : authentification multifacteur · SSO : authentification unique · TSA : services transitoires

05 · Synthèse et échanges

Cinq points pour la prochaine data room. Ensuite, vos retours : qu'est-ce qui a tenu, et qu'est-ce qui a cassé ?

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Helia tient sur cinq contrôles : UPN, MFA, messagerie, comptes techniques, TSA daté. Ensemble, ils décident si le lundi démarre.

UPN : identifiant de connexion · MFA : authentification multifacteur · TSA : services transitoires

Cinq points à retenir

À emporter dans la prochaine data room, et à afficher dans la cellule de crise.

1
Pas un projet informatique de plus
- Continuité, sécurité et preuve passent par les identités
- Sans accès le lundi, la cession n’est pas opérable

2
Carve-out n’est pas un carve-in
- Séparer : cloner, fermer les frontières, dater le TSA
- Intégrer : correspondance, vagues, moindre privilège

3
Ces objets ne suivent pas la messagerie
- ImmutableID, UPN, groupes, applications, accès conditionnel, MFA, postes
- La correspondance se fige bien avant la bascule, pas le samedi

4
Choisir le scénario avant l’outil
- CTIM natif, outil tiers, et script sur les écarts
- Bascule unique, par vagues, ou scission

5
Le Jour J se prouve
- Checklist de 8 h, journaux, cellule nommée, heure de retour
- Pas de « on verra lundi »

EXEMPLE FICTIF · MIGRATION M365 · HELIA → ALTAVIA
Helia n’est pas une migration de boîtes. Sans correspondance, UPN et MFA le lundi, l’usine s’arrête. La preuve : 15 pilotes réussis, et les accès NordHorizon coupés.

UPN : identifiant de connexion · CTIM : correspondance entre tenants · TSA : services transitoires · SPA : contrat de cession

ÉCHANGES

Questions et discussion

Sur vos carve-in et carve-out : qu'est-ce qui a cassé le lundi ? La correspondance des comptes, l'UPN, l'accès conditionnel, le MFA, Intune, ou un TSA sans date ?

UPN : identifiant de connexion · MFA : authentification multifacteur · TSA : services transitoires

Merci

@IdentityDays

#identitydays2026