PROSIT 4

Groupe :

CARVAL Mathéo – Scribe
RABATEL Antonin – Tous

LUU Philippe - Animateur

BOUHAMED Allan – Gestionnaire du temps

RIVET Alexandre - Secrétaire

1. Contexte

BERRIA rachète IKASI, une TPE voisine. IKASI possède son propre Active Directory (2 DC), un serveur de fichiers, un ERP, quelques applis maison, des postes Windows 10/11 et une petite infra virtualisée (2 ESXi, NAS, ~4 VM). La direction veut une intégration rapide et peu perturbatrice puis, à terme, une migration complète dans le domaine de BERRIA.

L'équipe identifie des risques : machines/server non mises à jour, authentification encore basée sur NTLM, permissions NTFS probablement mal configurées, mots de passe faibles, manque de contrôles. Marco refuse l'accès direct aux ressources internes sans audit et sécurisation préalable. Pierre demande : inventaires, DNS, modèle logique de forêt, rôles FSMO, GPO, partages, droits NTFS, SSO/LDAP des applis. Léo et Leila participent à la visite et doivent produire : diagramme réseau logique, diagramme AD cible et liste de GPO à déployer pour sécuriser rapidement IKASI avant intégration.

2. Mots inconnus / notions à maîtriser

- **Active Directory (AD)** : annuaire d'identités Microsoft (forêt, domaine, OU, contrôleur de domaine).
- **Forêt / Domaine / OU** : niveaux d'organisation AD.
- **Contrôleur de domaine (DC)** : serveur hébergeant l'annuaire.
- **Rôles FSMO** : 5 rôles critiques (Schema, DomainNaming, RID, PDC Emulator, Infrastructure).
- **Niveau fonctionnel** : compatibilité des fonctions AD selon version (2012R2, 2016, 2019…).
- **RODC** : Read-Only Domain Controller (contrôleur en lecture seule).
- **Relation d'approbation (trust)** : lien d'authentification entre domaines/forêts (one-way, two-way).
- **NTLM vs Kerberos** : NTLM = ancien, moins sûr ; Kerberos = privilégié pour AD.
- **AGDLP / AGUDLP** : bonnes pratiques de délégation (Accounts → Global → Domain Local → Permissions).
- **GPO (Group Policy Objects)** : stratégies centralisées Windows (configuration sécurité, scripts, etc.).
- **LAPS** : Local Administrator Password Solution (gestion des mots de passe admin locaux).

- **ADMT** : outil de migration des comptes entre domaines.
- **SSO / LDAP** : méthodes d'authentification des applications (Single Sign-On / annuaire LDAP).
- **NTFS permissions** : ACLs sur fichiers/partages.
- **Kerberos constrained delegation, SID filtering, Selective Authentication** : contrôles d'accès avancés lors d'un trust.
- **DNS Active Directory-integrated** : stockage de zones DNS dans AD.

3. Problématique

Comment intégrer rapidement IKASI au SI de BERRIA avec un minimum de perturbations tout en garantissant sécurité et conformité, puis préparer une migration complète vers le domaine BERRIA (ou un modèle cible) ?

4. Plan d'action (version courte et propre)

1. Préparer l'audit (5h)

- Rassembler les informations existantes sur IKASI.
- Préparer une liste de points à vérifier
- (AD, DNS, GPO, permissions, sécurité, etc.).
- Préparer quelques scripts PowerShell utiles (lecture inventaire AD).

2. Réaliser l'audit (5h)

- Vérifier l'état de l'Active Directory d'IKASI (DC, FSMO, niveau fonctionnel).
- Vérifier l'authentification (Kerberos/NTLM).
- Relever la structure : OU, GPO, groupes, partages et droits NTFS.
- Identifier les faiblesses (sécurité, mots de passe, patchs, etc.).
- Cartographier leur réseau + serveurs.

3. Proposer des mesures immédiates (1h)

- Appliquer GPO de sécurité essentielles.
- Améliorer mots de passe / activer LAPS.
- Limiter l'accès réseau tant que l'environnement n'est pas sécurisé.

- Mettre à jour postes & serveurs.

4. Imaginer les scénarios d'intégration (1.5h)

- Trust entre les deux domaines (one-way / two-way).
- Site AD supplémentaire.
- Sous-domaine IKASI dans forêt BERRIA.
- Option migration complète ultérieure.

5. Produire les livrables demandés (~3h)

- Diagramme du SI d'IKASI.
- Diagramme AD cible.
- Liste des GPO recommandées.
- Liste des informations à vérifier durant la visite.

5. Réalisation

Suite à la réunion d'équipe et à l'analyse du contexte, voici les livrables techniques produits pour l'intégration de la société IKASI.

A. Liste de contrôle d'Audit (Check-list pour la visite sur site)

Pour répondre à la demande de Pierre et rassurer Marco, voici les points précis à auditer physiquement et logiquement chez IKASI :

1. **Santé de l'Active Directory & Infrastructure :**
    a. **Version d'OS des DC :** Sont-ils en fin de vie (2008/2012) ?
    b. **Niveau Fonctionnel (FFL/DFL) :** Vérifier s'il est au moins en 2016 pour supporter les fonctionnalités modernes.
    c. **Réplication (Sysvol/NTDS) :** Lancer un `repadmin /showrepl` pour voir s'il y a des erreurs de réplication.
    d. **Rôles FSMO :** Qui détient les 5 rôles ? Sont-ils sur un seul serveur ?
    e. **DNS :** Les zones sont-elles intégrées à AD ? Y a-t-il des redirecteurs (forwarders) vers des DNS publics ou FAI ?
    f. **Sauvegardes :** Existence et test de restauration de l'état du système (System State).
2. **Sécurité & Identités :**
    a. **Protocoles :** Audit des logs pour détecter l'usage de NTLMv1 (à bannir).

b. **Groupes Admin :** Vérifier qui est membre de "Domain Admins" et "Enterprise Admins".
c. **Mots de passe :** Vérifier la *Default Domain Policy* (complexité, longueur, expiration).
d. **Comptes de service :** Sont-ils configurés avec "Le mot de passe n'expire jamais" ? Ont-ils des droits Admin du domaine (mauvaise pratique) ?

3. **Applications & Fichiers :**
   a. **Partages :** Vérifier les droits NTFS vs Droits de partage. Respect de la règle **AGDLP** (Account -> Global -> Domain Local -> Permission) ?
   b. **Applications métier (ERP) :** Méthode d'authentification actuelle (LDAP simple texte ? Kerberos ?).

B. Diagramme Logique du SI actuel (IKASI)

Reconstitution de l'architecture d'IKASI basée sur l'inventaire préliminaire.

Infrastructure Physique & Virtualisation :

- **Hyperviseurs :** 2 hôtes ESXi en cluster (Haute Dispo probable).
- **Stockage :** 1 NAS (partagé via iSCSI ou NFS pour les ESXi).
- **Sauvegarde :** Dispositif inconnu (à vérifier sur site).

Machines Virtuelles (VMs) & Rôles :

1. **DC-IKASI-01 :** Contrôleur de Domaine Principal + DNS + DHCP.
2. **DC-IKASI-02 :** Contrôleur de Domaine Secondaire + DNS.
3. **SRV-FILE :** Serveur de fichiers (Partages).
4. **SRV-APP :** Hébergement de l'ERP et des applis maison.

Réseau :

- VLAN unique (probablement) ou séparation basique (Serveurs / Postes de travail).
- Postes clients : Flotte hétérogène Windows 10/11.

C. Diagramme AD Cible & Stratégie d'Intégration

Pour satisfaire la contrainte "intégration rapide" tout en isolant les risques (demande de Marco).

Stratégie retenue : Approbation de Forêt (Forest Trust)

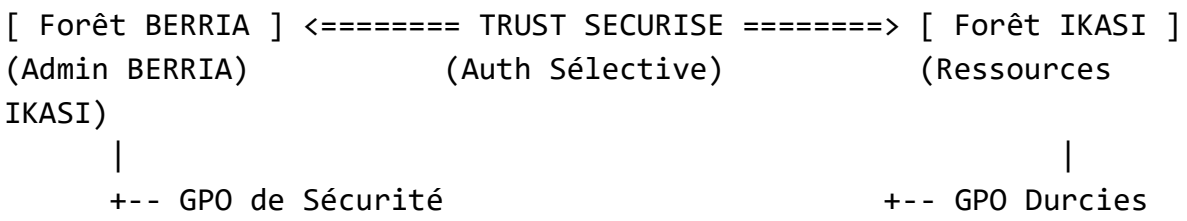
Plutôt que de migrer tout de suite, nous créons un pont sécurisé entre la forêt berria.lan et ikasi.local.

1. **Type de Trust :** Bidirectionnel (Two-way) ou Unidirectionnel (One-way, BERRIA fait confiance à IKASI) selon besoin utilisateurs.

    a. *Recommandation Marco :* **Trust Unidirectionnel** au début (BERRIA accède à IKASI pour administrer, mais IKASI n'accède pas à BERRIA).
2. **Sécurité du Trust :** Activation de **"Selective Authentication"** (Authentification sélective).
    a. *Pourquoi ?* Cela empêche les utilisateurs d'IKASI d'accéder à tout le réseau BERRIA par défaut. On doit explicitement autoriser l'accès serveur par serveur.
3. **Résolution de noms :** Mise en place de **Rechargeurs conditionnels DNS** (Conditional Forwarders) sur chaque domaine pour qu'ils puissent résoudre les IP de l'autre.

Schéma Cible (Logique) :

Plaintext



D. Liste des GPO Prioritaires à déployer

Pour sécuriser l'environnement IKASI avant toute connexion au réseau BERRIA.

Nous avons préparé une structure d'OU (Unités d'Organisation) pour appliquer ces GPO sans impacter la production existante brutalement.

Nom de la GPO	Cible (OU)	Paramètres Clés	Objectif
SEC_Password_Policy	Domaine (Racine)	Min 12 caractères, complexité activée, verrouillage après 5 échecs.	Stopper les attaques par force brute.
SEC_LAPS_Deploy	Workstations	Installation de l'agent LAPS + Activation gestion MDP Admin local.	Empêcher le mouvement latéral (Pass-the-Hash).
SEC_Audit_Log	Servers & DCs	Activer l'audit des connexions (Réussite/Echec) et accès objets.	Traçabilité des actions (si incident).

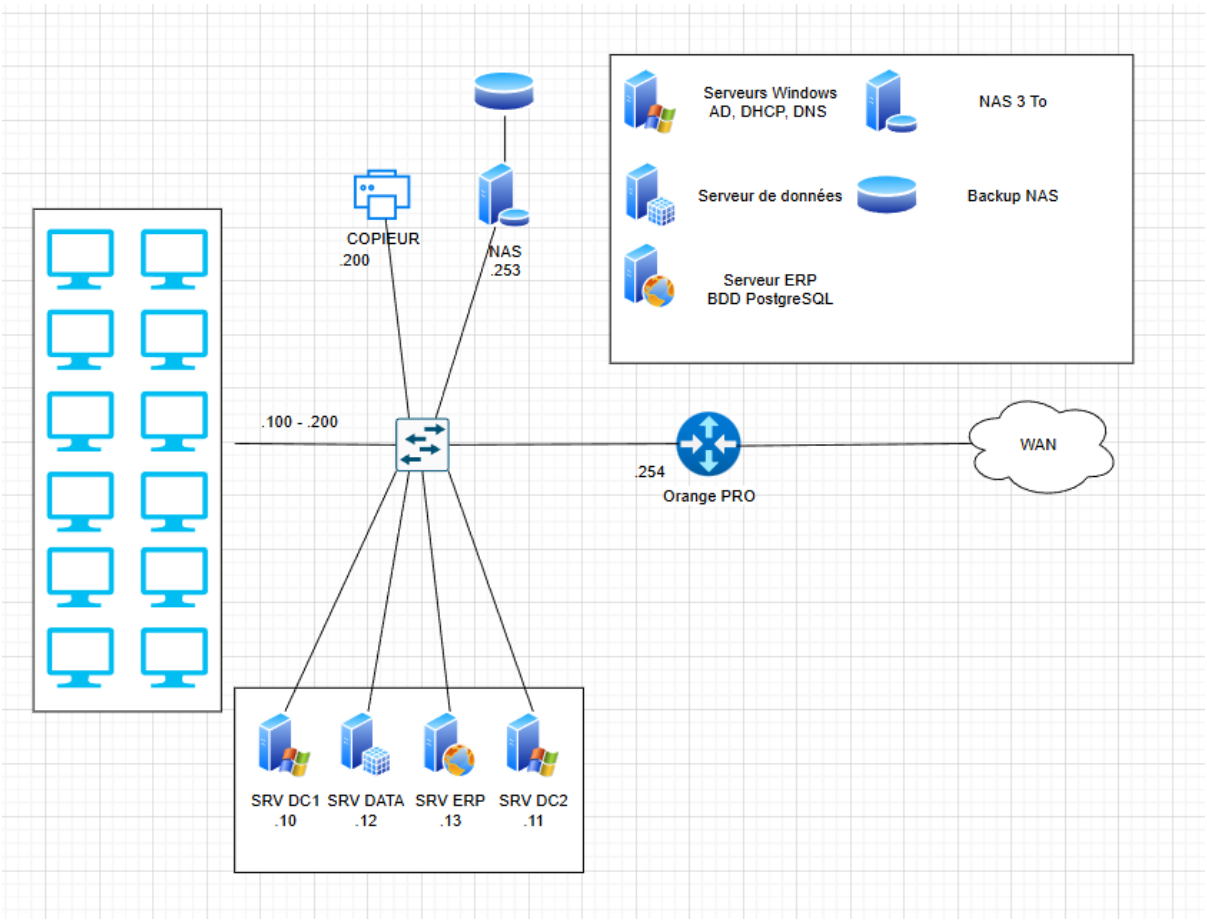
SEC_Restrict_Admin	Workstations	Restreindre le groupe "Administrateurs locaux" via *Restricted Groups*.	Retirer les droits admin aux utilisateurs standards.
SEC_Network_Harden	Tous	Désactiver **NTLMv1** et **SMBv1**. Activer le Pare-feu Windows.	Bloquer les protocoles obsolètes et vulnérables (Ransomware).
SEC_WinRM	Servers	Activer WinRM (HTTPS) pour l'administration à distance.	Permettre l'administration moderne par BERRIA.

E. Préparation de la Migration (Futur)

Anticipation de la demande "migration complète à terme".

Une fois l'environnement sécurisé et le Trust établi, nous utiliserons **ADMT (Active Directory Migration Tool)** pour :

1. Migrer les utilisateurs et les groupes (avec conservation de l'historique des mots de passe si possible).
2. Utiliser le **SID History** pour que les utilisateurs migrés accèdent encore à leurs anciens fichiers chez IKASI pendant la transition.
3. Migrer les postes de travail vers le domaine BERRIA.
4. Décommissionner les DC IKASI.


Serveurs Windows
AD, DHCP, DNS
NAS 3 To
Serveur de données
Backup NAS
Serveur ERP
BDD PostgreSQL
COPIEUR
.200
NAS
.253
.100 - .200
.254
Orange PRO
WAN
SRV DC1
.10
SRV DATA
.12
SRV ERP
.13
SRV DC2
.11