Laboratoire Active Directory

Ce document permet de détailler la conception du laboratoire active directory.

1. Arborescence

A diagram of a triangle with icons

AI-generated content may be incorrect.

1. Architecture du réseau

A computer screen with blue squares

AI-generated content may be incorrect.

1. Détails des VM

* A chaque pc ou serveur de la partie réseau va correspondre une VM
* Chaque VM aura pour nom le User Principal Name (UPN) de sa représentation
* Les services DNS, et DHCP seront configuré sur le dc1(2)@entreprise.local
* Le [srv@lyon.entreprise.local](mailto:srv@lyon.entreprise.local) est un server de messagerie ouvert à tous les utilisateurs
* et le [srv@paris.entreprise.local](mailto:srv@paris.entreprise.local) est un server de fichier ouverts à des types précis d’utilisateurs

1. GPO (Group Policy Objects) et stratégies de sécurité

* Mot de passe : 10 caractères minimum, diversité (majuscule, minuscume, chiffre, caractère spécial), expiration au bout de 60 jours.
* Blocage temporaire de l’accès à un compte d’utilisateur après3 tentatives infructuses de connexion
* Verrouillage de la session au bout de 10 minutes d’inactivités
* Désactivation des ports USB
* Sauvegarde des logs de connexions/déconnexions, sur un serveur de log
* Mise à jour et installation centralisé des OS et logiciels
* Bloquer les ports réseau non utilisés
* Le server de mesagerie est accesible à tout les users
* Le server de fichier n’est accessible qu’aux user du DC root (finances et admins)

1. Tests

|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Description** | **Résultat attendu** | **Validation (✓ / ✗)** |
| Mot de passe - Complexité | Tenter de créer un mot de passe sans majuscule, ou sans chiffre, ou moins de 10 caractères | Refus, message d’erreur |  |
| Mot de passe - Expiration | Vérifier qu’un utilisateur doit changer son mot de passe après 60 jours | Demande de changement à la connexion après 60 jours |  |
| Blocage compte après 3 échecs | Essayer 3 connexions infructueuses sur un compte utilisateur | Compte bloqué temporairement, accès refusé |  |
| Verrouillage session après 10 min | Laisser un poste inactif pendant 10 minutes | Session verrouillée automatiquement |  |
| Désactivation des ports USB | Brancher une clé USB sur un poste utilisateur | Clé USB non reconnue ou accès bloqué |  |
| Sauvegarde des logs | Vérifier que les logs de connexion/déconnexion sont sauvegardés sur le serveur de logs | Logs correctement sauvegardés et accessibles |  |
| Mise à jour centralisée OS | Déployer une mise à jour sur une VM via WSUS ou équivalent | Mise à jour installée avec succès |  |
| Blocage ports réseau non utilisés | Tester la connexion sur un port réseau non autorisé | Connexion refusée |  |
| Accessibilité serveur de messagerie | Se connecter au serveur mail à partir de plusieurs comptes utilisateurs | Accès possible pour tous les utilisateurs |  |
| Restriction accès serveur de fichiers | Essayer d’accéder au serveur de fichiers depuis un utilisateur hors du DC root | Accès refusé |  |
| Authentification inter-domaines | Un utilisateur de lyon.entreprise.local se connecte à une ressource sur laris.entreprise.local | Accès autorisé si les droits sont corrects |  |
| Réplication AD entre DC root et secondaires | Modifier un objet sur le DC root et vérifier la propagation sur DC secondaire | Modification visible rapidement sur DC secondaire |  |
| Redondance DC - basculement | Éteindre DC principal et tester connexion utilisateur | Connexion possible via DC secondaire sans interruption |  |