ANNEXE TECHNIQUE

Pierre-Antoine Amici · Détail des laboratoires et projets · 06 85 20 44 38 · pa_amici@proton.me

Ce document détaille les infrastructures montées, configurées et exploitées durant la formation Technicien Supérieur Systèmes et Réseaux, ainsi que les projets personnels menés en parallèle. L'ensemble a été virtualisé sous Hyper-V sur poste personnel, hors environnement pédagogique fourni.

INFRASTRUCTURE WINDOWS SERVER

Annuaire et services de domaine

RÔLES Active Directory Domain Services, DNS interne, DHCP avec réservations et étendues multiples, WINS, service de fichiers, serveur d'impression.

STRUCTURATION Découpage en unités d'organisation, création des comptes, des groupes et des ordinateurs, application du modèle AGDLP pour l'attribution des droits.

DROITS Permissions NTFS et permissions de partage, croisement des deux, listes de contrôle d'accès, propriétaires et héritage.

QUOTAS FSRM : quotas de répertoire, filtrage de fichiers, rapports de stockage.

AUTHENTIFICATION Fonctionnement de Kerberos, tickets, délégation.

Stratégies de groupe

MODÈLE Utilisation du mode Loopback en fusion pour les paramètres utilisateur dépendant de la machine.

MISES EN ŒUVRE Profils itinérants, redirection de dossiers, masquage sélectif de lecteurs, déploiement du certificat de l'autorité de certification, confiance envers l'éditeur RemoteApp, délégation d'identifiants pour le SSO, publication de l'URL du flux RD Web.

Services Bureau à distance

ARCHITECTURE Trois hôtes de session RDSH répartis en charge, un Connection Broker, un serveur RD Web Access, une RD Gateway, un serveur DNS externe dédié à la résolution depuis l'extérieur.

PUBLICATION Collections de sessions et publication de RemoteApp individuelles.

ACCÈS DISTANT Encapsulation du flux RDP dans un tunnel HTTPS sur le port 443 unique. Liaison du certificat serveur sur la RD Gateway via tsgateway.msc, publication de la CRL vers l'extérieur, aucune exposition directe du port 3389.

CERTIFICATS Justification et mise en place d'un certificat wildcard couvrant les hôtes RDSH en répartition de charge.

Autorité de certification interne et HTTPS

CHAÎNE Mise en place d'une autorité de certification d'entreprise, déploiement du certificat racine sur les postes du domaine par stratégie de groupe.

ÉMISSION Génération des CSR depuis les serveurs via la console MMC, émission, installation et liaison aux services IIS et RDS.

PUBLICATION Mise à disposition de la CRL, joignable depuis l'intérieur comme depuis l'extérieur du réseau.

Déploiement automatisé de postes

SOCLE WDS (Windows Deployment Services) et MDT (Microsoft Deployment Toolkit).

IMAGES Capture et préparation d'images de référence, résolution des échecs de Sysprep liés aux paquets AppX.

AUTOMATISATION unattend.xml avec passes specialize et oobeSystem, jonction de domaine via Microsoft-Windows-UnattendedJoin, AutoLogon, FirstLogonCommands.

APPLICATIONS Séquences de tâches MDT avec installation applicative silencieuse, distinction entre Bootstrap.ini, qui impose une réimportation dans WDS, et CustomSettings.ini, lu à l'exécution.

RÉSEAU ET ACCÈS DISTANTS

Routage et segmentation

TOPOLOGIE Trois zones distinctes : réseau interne, zone démilitarisée et zone externe, séparées par un routeur pare-feu ZeroShell.

FONCTIONS Routage inter-zones, translation d'adresses, redirection de ports, règles de filtrage des flux entrants et sortants selon la zone d'origine.

ADRESSAGE Découpage en sous-réseaux, calcul de masques de longueur variable, plan d'adressage documenté.

Réseaux privés virtuels

SITE À SITE Tunnel entre deux sites sous ZeroShell, et liaison à la demande sous Windows Server.

CLIENT À SITE Accès nomade sous Windows Server, permettant à un poste externe de rejoindre le réseau interne.

OPENVPN Déploiement complet avec infrastructure à clés dédiée : autorité de certification propre au VPN, génération et distribution des certificats clients, révocation.

WIREGUARD Mise en place d'un accès client à site, comparaison des performances et de la simplicité de configuration avec les solutions précédentes.

Haute disponibilité

CLUSTER Mise en cluster de serveurs avec stockage partagé, tests de basculement.

INFRASTRUCTURE LINUX

Parc multi-distributions

PÉRIMÈTRE Six serveurs répartis sur Debian, Fedora et openSUSE, choisis pour couvrir les différences de gestion de paquets, de services et de configuration réseau.

SERVICES BIND9 en DNS split-horizon, ISC-DHCP, Apache2 en VirtualHosts multi-sites, partages Samba interopérables avec les postes Windows, GLPI.

EXPLOITATION Gestion des droits, des propriétaires et des listes de contrôle d'accès, délégation de privilèges par utilisateur et par commande, configuration réseau statique adaptée à chaque distribution.

ACCÈS DISTANT Administration à distance en SSH, authentification par échange de clés.

Scripts d'administration

COMPTES Scripts de création et de suppression d'utilisateurs en masse, avec contrôles de saisie et gestion des erreurs.

DIAGNOSTIC Script de diagnostic système : état des disques, taux d'occupation, alertes de seuil.

RÉSEAU Script de balayage réseau et d'inventaire des hôtes actifs.

TECHNIQUES Variables, conditions, boucles, expressions régulières, redirections, filtres et chaînage de commandes.

SUPERVISION ET TÉLÉPHONIE

Plateforme de supervision

SOCLE Centreon 21.10 sur CentOS 7, base de données MariaDB, résolution des difficultés d'installation liées au mode d'authentification de la base.

COLLECTE Supervision d'un parc mixte Windows Server 2022 et Linux via SNMP, NRPE et NSClient++.

DÉVELOPPEMENT Conception d'une sonde PowerShell exposée par NRPE pour surveiller le taux d'occupation des pools DHCP, besoin non couvert par les sondes standard.

RESTITUTION Modèles d'hôtes et de services, seuils d'alerte, tableaux de bord.

Téléphonie sur IP

ARCHITECTURE Deux IPBX FreePBX (Asterisk) interconnectés par un trunk SIP, avec configuration SIP derrière NAT : adresse externe, réseaux locaux déclarés, ouverture de la plage RTP.

CONFIGURATION Création des extensions, plan de numérotation, règles de routage des appels sortants, cascade Follow Me entre les deux sites.

SÉCURITÉ

Accès physique et durcissement

ANALYSE Étude des vecteurs d'attaque par accès physique sur poste de travail et sur contrôleur de domaine, dans le cadre du module sécurité.

CONTRE-MESURES BitLocker avec TPM et code PIN au démarrage, verrouillage de la séquence de boot, hygiène du compte DSRM.

DÉTECTION Identification des Event ID 4720, 4728, 4732 et 4738 pour la création de comptes et les modifications de groupes privilégiés, en vue d'une centralisation des journaux.

AUTOMATISATION ET DÉVELOPPEMENT

Gestionnaire de machines virtuelles à interface graphique

OBJET Application PowerShell avec interface graphique permettant de créer, paramétrer et supprimer des machines virtuelles sans passer par la console Hyper-V.

FONCTIONS Gabarits prédéfinis pour serveurs Windows, postes clients Windows 10 et 11, routeurs, machines Linux, serveur Centreon et IPBX FreePBX. Verrouillage automatique de l'ISO selon le type de VM retenu, mode de suppression sécurisé avec confirmation.

ÉVOLUTION Six versions successives, enrichies au fil des besoins du laboratoire.

COMPLÉMENT Script de création en masse de comptes Active Directory à partir d'un fichier CSV.

Serveur de jeu Linux compilé depuis les sources

COMPILATION Compilation complète du serveur sous Linux, résolution des dépendances, application des correctifs, gestion des options de compilation.

EXPLOITATION Configuration réseau et publication de ports, persistance en base MariaDB, administration via HeidiSQL, sauvegardes, mises à jour et maintenance.

RÉSULTAT Infrastructure exploitée en conditions réelles avec jusqu'à 200 joueurs connectés.

Développement et hébergement personnels

APPLICATIF Robot Discord développé en Node.js avec persistance des données en base SQLite.

WEB Site personnel pierre-amici.fr, mise en ligne, configuration et maintenance.