Dossier 01 - Infrastructure

Réalisé par : El Majdouli Hamza

Table des matières

Dossier 01 - Infrastructure

Epreuve E6 - Cas GSB

Dossier 01 - Infrastructures (SI)

El Majdouli Hamza

Mot de passe de l'infrastructure :

ESXi hamza btsSIO351 Yahia btsSIO351

Switch A1.1 root btsSIO351

Switch A1.2 root cisco

Borne Wifi admin btsSIO351

PfSense admin btsSIO351

Client windows hamza btsSIO351 yahia btsSIO351

Client debian root root

Serveur AD Administrateur btsSIO351

Serveur Web root root

Management btsSIO351

Zabbix : root zabbix Admin zabbix (interface)

GLPI : glpi glpi(Super Admin) root root(Serveur)

Configurations des routeurs

Dossier 01 – Infrastructure (SI)

Active Directory (AD)

1. C'est quoi Active Directory ?

Active Directory (AD) est un service d'annuaire Microsoft. Il permet de :

Centraliser les comptes utilisateurs/PC

Gérer les droits et groupes

Déployer des stratégies (GPO)

Authentifier les utilisateurs dans le domaine

2. Configuration d'un Contrôleur de Domaine (DC)

Prérequis :

Windows Server 2016/2019/2022

IP fixe (ex : 192.168.10.8)

Nom de la machine : SRV-AD (par ex)

Un mot de passe fort admin

Étape 1 : Renommer le serveur + IP fixe

powershell

CopierModifier

Rename-Computer -NewName "SRV-AD" -Restart

Configurer l'IP statique dans Panneau de configuration > Réseau > Propriétés

Étape 2 : Installer le rôle AD DS (Active Directory Domain Services)

Server Manager > Manage > Add Roles and Features

Choisir "Active Directory Domain Services"

Laisse les services par défaut, puis Install

Étape 3 : Promouvoir le serveur en contrôleur de domaine

Une fois AD DS installé, clique sur "Promote this server to a domain controller"

Choisir : Ajouter une nouvelle forêt

Nom de domaine : entreprise.local (ou ton nom de domaine interne)

Définir un mot de passe DSRM

Laisse les chemins par défaut, puis Install + redémarrage

3. Création d'utilisateurs et de groupes

Dans le menu Outils > Utilisateurs et ordinateurs Active Directory :

Créer une OU :

Clic droit sur le nom du domaine → Nouvelle unité d'organisation (OU)

Nom : Utilisateurs, PC, Stagiaires, etc.

Créer un utilisateur :

Clic droit dans l'OU → Nouvel utilisateur

Nom : El Majdouli Hamza

Identifiant : Hamza

Mot de passe + options (obliger changement, etc.)

4. Rejoindre un PC au domaine

Sur un poste client Windows (dans le même réseau) :

Renommer la machine (ex : PC-Hamza)

Aller dans Propriétés système > Modifier le domaine

Entrer entreprise.local

Authentifier avec un compte admin du domaine

Redémarrer

1. Qu'est-ce que le DNS ?

Le DNS (Domain Name System) sert à traduire des noms de domaine (ex. serveur.local, google.com) en adresses IP (ex. 192.168.10.8), et inversement. C'est un service indispensable pour naviguer et accéder aux ressources sur un réseau.

2. Installer le rôle DNS sur Windows Server

Étapes :

Ouvre le Server Manager

Clique sur Manage > Add Roles and Features

Choisis Role-based or feature-based installation

Sélectionne ton serveur

Dans la liste des rôles, coche DNS Server

Clique sur Next puis Install

3. Configurer le serveur DNS

a) Ouvrir la console DNS

Server Manager > Tools > DNS

b) Ajouter une zone DNS

Zone principale (Primary Zone)

Clique droit sur Forward Lookup Zones

Choisis New Zone

Suis l'assistant :

Type : Primary zone

Zone name : ex. entreprise.local

Stockage : par défaut

Activer la mise à jour dynamique (option recommandée)

5. Configurer les clients pour utiliser ton DNS

Sur les clients Windows, configure l'adresse IP de ton serveur DNS (ex. 192.168.10.8) dans les paramètres réseau.

Si pfSense est utilisé comme routeur, tu peux configurer le DNS dans le DHCP pour distribuer automatiquement l'IP du serveur DNS aux clients.

1. Qu'est-ce qu'une GPO ?

Une GPO (stratégie de groupe) permet d'appliquer automatiquement des configurations aux :

Utilisateurs (ex. : interdire le panneau de config, définir un fond d'écran…)

Ordinateurs (ex. : désactiver le pare-feu Windows, déployer un script…)

2. Où se trouvent les GPO ?

Tu les gères dans : Outils > Gestion des stratégies de groupe (gpmc.msc)

3. Structure de base

Tu appliques une GPO à :

Une Unité d'Organisation (OU) (ex. Utilisateurs, PC Bureaux)

Jamais directement au domaine entier (mauvaises pratiques)

4. Exemple : GPO pour désactiver le panneau de configuration

Va dans GPMC > clic droit sur l'OU > Créer une GPO

Nom : Bloquer_Panneau_Config

Clic droit > Modifier

Va dans :

vbnet

Configuration utilisateur > Modèles d'administration > Panneau de configuration

Active : Interdire l'accès au panneau de configuration

7. Forcer l'application des GPO

Sur un poste client :

gpupdate /force

Vérifier les GPO appliquées :

gpresult /r

Pourquoi utiliser SSH sur un switch ?

Pour administrer le switch à distance via le terminal

C'est chiffré, contrairement à Telnet

Obligatoire dans les bonnes pratiques de sécurité (BTS SIO, pro, etc.)

1. Pré-requis

Le switch doit supporter SSH (les modèles "managed" comme les Cisco Catalyst, TP-Link JetStream, HP ProCurve…)

Une adresse IP configurée sur une interface VLAN (souvent VLAN 1)

Une passerelle et un accès réseau entre ton PC et le switch

2. Configuration SSH sur un switch Cisco

plaintext

Switch> enable

Switch# configure terminal

a) Définir un nom d’hôte et un domaine

Switch(config)# hostname SWITCH

SWITCH(config)# ip domain-name entreprise.local

b) Générer les clés RSA

SWITCH(config)# crypto key generate rsa

Quand il demande la taille : 2048 bits minimum

c) Créer un utilisateur local

SWITCH(config)# username admin privilege 15 secret motdepasse

d) Activer SSH et le vty (console réseau)

SWITCH(config)# line vty 0 15

SWITCH(config-line)# login local

SWITCH(config-line)# transport input ssh

SWITCH(config-line)# exit

e) Activer le service SSH

SWITCH(config)# ip ssh version 2

SWITCH(config)# exit

3. Affecter une IP au switch (VLAN 1, par exemple)

SWITCH(config)# interface vlan 1

SWITCH(config-if)# ip address 192.168.1.8 255.255.255.0

SWITCH(config-if)# no shutdown

SWITCH(config-if)# exit

SWITCH(config)# ip default-gateway 192.168.1.1

4. Tester la connexion SSH depuis ton PC

a) Sous Linux / Mac / Windows (terminal) :

bash

ssh admin@192.168.1.8

b) Sous Windows avec PuTTY :

Adresse IP : 192.168.1.8

Port : 22

Connexion type : SSH

Login : admin, mot de passe défini plus haut

GLPI

1. Qu'est-ce que GLPI ?

GLPI (Gestionnaire Libre de Parc Informatique) permet de :

Gérer un inventaire de matériel et logiciels

Suivre les tickets d'assistance (helpdesk)

Suivre les licences, contrats, utilisateurs

Superviser avec des plugins (FusionInventory, OCS…)

2. Prérequis techniques

Tu peux installer GLPI sur un serveur Linux avec :

Apache ou Nginx

PHP (8.1 ou 8.2 recommandé)

MariaDB ou MySQL

Exemple de stack : LAMP (Debian/Ubuntu)

sudo apt update

sudo apt install apache2 mariadb-server php php-mysql php-xml php-curl php-mbstring php-intl php-bz2 php-gd php-ldap unzip -y

3. Télécharger et installer GLPI

a) Télécharger la dernière version :

wget https://github.com/glpi-project/glpi/releases/download/10.0.14/glpi-10.0.14.tgz

b) Extraire et déplacer dans /var/www/html : tar -xvzf glpi-10.0.14.tgz

sudo mv glpi /var/www/html/

c) Donner les droits : sudo chown -R www-data:www-data /var/www/html/glpi

sudo chmod -R 755 /var/www/html/glpi

4. Configuration MySQL

sudo mysql -u root -p

CREATE DATABASE glpidb;

CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'MotDePasseFort';

GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost';

FLUSH PRIVILEGES;

EXIT;

5. Installation web de GLPI

Ouvre ton navigateur : http://ip_du_serveur/glpi

Choisis la langue, accepte la licence

Sélectionne "Installer"

Rentre les infos MySQL :

Base : glpidb

Utilisateur : glpiuser

Mot de passe : celui défini ci-dessus

Laisse GLPI créer les tables automatiquement

À la fin : identifiants par défaut :

Powershell (scripts)

1. Prérequis

Exécuter le script sur un contrôleur de domaine (ou un poste avec les RSAT installés)

Importer le module Active Directory :

Import-Module ActiveDirectory

2. Créer un utilisateur AD

New-ADUser `

-Name "Jean Dupont" `

-GivenName "Jean" `

-Surname "Dupont" `

-SamAccountName "jdupont" `

-UserPrincipalName "jdupont@domaine.local" `

-Path "OU=Utilisateurs,DC=domaine,DC=local" `

-AccountPassword (ConvertTo-SecureString "Password123*" -AsPlainText -Force) `

-Enabled $true

3. Créer un groupe et y ajouter un utilisateur

New-ADGroup -Name "Techniciens" -GroupScope Global -Path "OU=Groupes,DC=domaine,DC=local"

Add-ADGroupMember -Identity "Techniciens" -Members "jdupont"

Proxy

pfsense

Journalisation (ex. syslog, observateur d'événement)

1. Journalisation sur pfSense

Où voir les logs sur pfSense ?

Menu : Status > System Logs

Tu y trouveras plusieurs onglets :

Activer/Configurer les logs

a) Ajuster le niveau de log :

Status > System Logs > Settings

Tu peux :

Modifier la taille des logs

Choisir ce qui est affiché

Activer la journalisation en temps réel

2. Journalisation sur Windows Server

Où consulter les logs ?

Outil : Observateur d’événements (anglais : Event Viewer)

bashv

eventvwr.msc

Active Directory (AD):

Definitions :

Un serveur Active Directory (AD) est une infrastructure centralisée développée par Microsoft qui permet la gestion et l'administration des ressources d'un réseau informatique. Il constitue une base de données hiérarchique utilisée pour stocker et organiser des informations sur les utilisateurs, les ordinateurs, les groupes, les imprimantes, et autres objets d'un réseau.

L'Active Directory est essentiel pour :

L'authentification : Vérifier l'identité des utilisateurs et des machines avant d'autoriser l'accès aux ressources.

La gestion des autorisations : Définir les droits et les permissions d'accès aux fichiers, dossiers et applications.

L'administration centralisée : Permettre aux administrateurs système de configurer les paramètres du réseau depuis un seul endroit à l'aide des Group Policy Objects (GPO).

La scalabilité : Adapter le réseau à des environnements de toutes tailles, des petites entreprises aux grandes organisations.

En résumé, le serveur Active Directory joue un rôle fondamental dans la sécurisation et la simplification de la gestion des infrastructures réseau en entreprise.

Domain Name System (DNS)

Domain Name System (DNS) : Explication

Le DNS (Domain Name System) est un système essentiel pour le fonctionnement d'Internet et des réseaux locaux. Il agit comme un "annuaire téléphonique" qui traduit des noms de domaine faciles à lire pour les humains (ex. : www.google.com) en adresses IP compréhensibles par les machines (ex. : 142.250.183.78).

Fonctionnement du DNS

Résolution de noms Lorsqu'un utilisateur tape une adresse (par ex. www.example.com) dans un navigateur, une requête DNS est envoyée pour obtenir l'adresse IP correspondante.

Exemple : www.example.com → 192.168.1.1.

Hiérarchie du DNS Le DNS est organisé de manière hiérarchique en zones :

Racine (.) : La base de toute la hiérarchie.

Domaines de premier niveau (TLD) : .com, .org, .fr, etc.

Domaines de second niveau : example.com.

Sous-domaines : www.example.com.

Serveurs DNS

Serveurs récursifs : Interrogés en premier pour résoudre une requête DNS, ils trouvent les réponses en interrogeant d'autres serveurs si nécessaire.

Serveurs autoritaires : Détiennent les informations exactes d'un domaine spécifique (comme example.com).

Cache DNS : Stocke temporairement les réponses pour accélérer les requêtes futures.

Rôles du DNS

Simplification pour les utilisateurs : Permet d'utiliser des noms au lieu d'adresses IP.

Redondance et disponibilité : Plusieurs serveurs DNS garantissent un accès continu aux services en ligne.

Gestion des services réseau : Configure les enregistrements pour :

Les serveurs web (enregistrement A ou AAAA).

Les serveurs mail (enregistrement MX).

Les alias de domaine (enregistrement CNAME).

La localisation de services (enregistrement SRV).

Exemple Pratique

Requête utilisateur : Vous tapez www.google.com.

Processus DNS :

La requête est envoyée au serveur DNS local (ou récursif).

Si la réponse n'est pas dans son cache, il interroge d'autres serveurs (racine, TLD, autoritaire).

Le serveur autoritaire de google.com répond avec l'adresse IP correspondante.

Le navigateur se connecte à l'adresse IP obtenue.

Avantages

Efficacité : Réduction du temps de réponse grâce au cache DNS.

Flexibilité : Possibilité de rediriger un domaine vers différentes adresses (Load Balancing).

Sécurité : Des extensions comme DNSSEC protègent contre les attaques DNS (ex. : falsification de cache).

Le DNS est indispensable non seulement pour Internet, mais aussi pour les environnements d'entreprise, où il est utilisé pour gérer les noms d'hôte, les services internes et la communication entre les serveurs.

Group Policy Object (GPO) : Explication

Les GPO (Group Policy Objects) sont des objets utilisés dans les environnements Windows pour centraliser et automatiser la gestion des configurations, des paramètres de sécurité, et des restrictions applicables aux utilisateurs et aux ordinateurs d'un domaine Active Directory (AD).

Rôles et Fonctionnement des GPO

Définition des GPO Une GPO est un ensemble de règles appliquées aux utilisateurs ou aux ordinateurs via un contrôleur de domaine Active Directory. Elle permet d'uniformiser les configurations sur l'ensemble du réseau.

Types de GPO

GPO locale : Appliquée sur un seul ordinateur, même hors du domaine AD.

GPO de domaine : Appliquée aux objets AD (utilisateurs, groupes, ordinateurs) via les Unités Organisationnelles (OU).

Héritage et Priorité Les GPO suivent une hiérarchie :

Local

Site

Domaine

Unité Organisationnelle (OU) Si des paramètres se chevauchent, la GPO de niveau inférieur (par exemple, celle appliquée à une OU) prend le dessus.

Utilisations des GPO

Sécurité

Configurer des politiques de mots de passe (longueur, complexité, expiration).

Restreindre l'accès à certaines fonctionnalités ou applications.

Configuration des postes de travail

Définir un fond d'écran ou empêcher la modification des paramètres d'affichage.

Bloquer les clés USB pour des raisons de sécurité.

Déploiement logiciel

Installer automatiquement des logiciels ou mises à jour sur les postes clients via des fichiers MSI.

Gestion des connexions réseau

Configurer les partages réseau, les imprimantes, et les connexions VPN.

Scripts de démarrage/arrêt

Exécuter des scripts spécifiques lors du démarrage ou de l'arrêt des machines.

Outils pour Gérer les GPO

Gestion des Stratégies de Groupe (GPMC) La console de gestion des stratégies de groupe (Group Policy Management Console) permet de :

Créer, modifier et supprimer des GPO.

Les associer à des sites, domaines ou unités organisationnelles.

RSOP (Resultant Set of Policy) Un outil qui permet de vérifier quelles stratégies sont appliquées sur un utilisateur ou un ordinateur.

Commandes PowerShell Utilisez PowerShell pour automatiser la gestion des GPO (par ex. : Get-GPO, New-GPO).

Exemple de GPO

Bloquer l'accès au Panneau de Configuration

Paramètre : "Accès au Panneau de Configuration et aux Paramètres" → Désactivé.

Effet : Les utilisateurs ne peuvent plus accéder au panneau de configuration sur leur machine.

Définir un fond d'écran

Paramètre : "Longueur minimale du mot de passe" → 8 caractères.

Effet : Les utilisateurs ont tous un fond d'écran créer des mots de passe avec au moins 8 caractères.

Avantages des GPO

Centralisation : Gestion facile des configurations réseau depuis une seule interface.

Automatisation : Réduction des interventions manuelles sur les postes clients.

Sécurité : Contrôle accru des postes et utilisateurs.

Flexibilité : Applique des règles spécifiques selon les besoins (par utilisateur ou par machine).

Les GPO sont un outil puissant pour toute organisation utilisant Active Directory, car elles garantissent un environnement réseau cohérent, sécurisé et facile à administrer.

Secure Shell (SSH) : Explication

Le Secure Shell (SSH) est un protocole réseau qui permet de communiquer et d'administrer à distance des systèmes informatiques de manière sécurisée. Il est principalement utilisé pour l'administration des serveurs et pour le transfert sécurisé de données.

Principes de Fonctionnement de SSH

Connexion Sécurisée SSH utilise un chiffrement fort pour protéger la communication entre deux machines (un client et un serveur). Cela empêche toute interception ou modification des données échangées.

Authentification

Par mot de passe : L'utilisateur doit fournir un mot de passe pour accéder au serveur.

Par clé publique/privée : Une méthode plus sécurisée où l'utilisateur utilise une paire de clés cryptographiques (clé publique sur le serveur, clé privée sur le client).

Port Utilisé SSH écoute par défaut sur le port 22, mais il peut être configuré pour utiliser un autre port pour des raisons de sécurité.

Utilisations de SSH

Administration à Distance SSH permet aux administrateurs système de se connecter à distance à des serveurs pour effectuer des tâches comme :

Installer ou configurer des logiciels.

Surveiller les performances.

Résoudre des problèmes.

Transfert de Fichiers Sécurisé SSH prend en charge des outils comme SCP (Secure Copy Protocol) et SFTP (Secure File Transfer Protocol) pour transférer des fichiers de manière sécurisée.

Tunnels SSH SSH peut être utilisé pour créer des tunnels sécurisés afin de chiffrer le trafic entre un client et un serveur.

Exécution de Commandes à Distance Les utilisateurs peuvent exécuter des commandes sur un serveur distant sans avoir à s'y connecter directement via des outils comme ssh [commande].

Avantages de SSH

Chiffrement des communications, empêchant les attaques d'interception (man-in-the-middle).

Support de l'authentification forte par clé publique/privée.

Polyvalence

Compatible avec les systèmes Linux, macOS, et Windows (via des outils comme OpenSSH ou PuTTY).

Peut être utilisé pour une variété de tâches : administration, transfert de fichiers, tunnels.

Efficacité

Léger, rapide, et idéal pour une utilisation sur des réseaux à faible bande passante.

Exemple de Commandes SSH

Se connecter à un serveur : bash CopierModifier ssh utilisateur@adresse_ip

Exemple : bash CopierModifier ssh admin@192.168.1.8

Copier un fichier via SCP : bash CopierModifier scp fichier.txt utilisateur@adresse_ip:/chemin/destination/

Exemple : bash CopierModifier scp document.pdf admin@192.168.1.8:/home/admin/

Créer un tunnel SSH : bash

CopierModifier ssh -L port_local:destination:port_distant utilisateur@serveur

Sécurisation du SSH

Pour renforcer la sécurité :

Désactiver l'authentification par mot de passe et utiliser les clés SSH.

Modifier le port par défaut (22) pour réduire les tentatives de brute force.

Restreindre l'accès à SSH à des IP spécifiques (via un pare-feu).

Activer Fail2Ban ou d'autres outils pour bloquer les tentatives de connexion suspectes.

SSH est un outil incontournable pour tout administrateur ou développeur gérant des systèmes distants. Il combine sécurité, flexibilité, et simplicité d'utilisation pour répondre à une grande variété de besoins réseau et serveur.

GLPI : Explication

GLPI (Gestion Libre de Parc Informatique) est une application open-source dédiée à la gestion des services informatiques (ITSM) et à l'inventaire des ressources informatiques.

Elle permet aux entreprises de centraliser la gestion des équipements, des incidents, des demandes, et des projets informatiques.

Fonctionnalités Principales de GLPI

Gestion des Ressources (Parc Informatique)

Inventorier automatiquement les matériels informatiques (ordinateurs, imprimantes, périphériques) et les logiciels.

Suivre les configurations matérielles et logicielles.

Planifier la maintenance des équipements.

Gestion des Incidents et des Demandes

Centraliser et suivre les tickets d'incidents ou de demandes des utilisateurs.

Assigner des tickets à des techniciens.

Générer des rapports sur la résolution des problèmes.

Gestion des Licences

Surveiller l'utilisation des licences logicielles pour éviter les problèmes de conformité.

Identifier les licences arrivant à expiration.

Gestion des Contrats et Finances

Suivre les contrats de maintenance, de garantie ou de location.

Gérer les budgets liés aux équipements et services informatiques.

Gestion de Projet

Planifier, suivre et gérer les projets informatiques.

Identifier les ressources nécessaires et surveiller les délais.

Extensions et Plugins

GLPI est hautement personnalisable grâce à des plugins, tels que l'intégration avec des systèmes de supervision (ex. : FusionInventory) ou des outils de gestion des identités.

Avantages de GLPI

Open Source

GLPI est gratuit, ce qui le rend accessible pour les organisations de toutes tailles.

Interface Intuitive

Une interface web conviviale, accessible depuis un navigateur, facilite son adoption.

Flexibilité et Évolutivité

GLPI peut être adapté aux besoins spécifiques grâce à une communauté active et de nombreux plugins.

Interopérabilité

Intégration avec des outils tiers comme FusionInventory pour l'automatisation de l'inventaire ou OCS Inventory.

Conformité

GLPI aide les organisations à se conformer aux réglementations liées à la gestion des actifs et des données.

Exemples d'Utilisation de GLPI

Inventaire Automatisé Une entreprise peut connecter GLPI à FusionInventory pour identifier automatiquement tous les équipements connectés au réseau.

Gestion des Tickets d'Incidents Lorsqu'un utilisateur signale un problème (ex. : une imprimante hors service), GLPI enregistre un ticket, notifie un technicien et permet de suivre la résolution.

Planification des Interventions Un administrateur IT peut utiliser GLPI pour planifier une mise à jour des serveurs et notifier les équipes concernées.

Technologies Utilisées dans GLPI

Langages : PHP, SQL (bases de données comme MySQL ou MariaDB).

Plateformes : Fonctionne sur des systèmes Linux ou Windows avec un serveur web (Apache, Nginx).

Clients : Accessible via navigateur web.

Pour Résumer

GLPI est une solution robuste et polyvalente pour gérer efficacement les infrastructures informatiques, tout en améliorant la productivité et en optimisant les coûts. Son utilisation permet une meilleure visibilité sur l'état du parc informatique et garantit une réponse rapide aux besoins des utilisateurs.

PowerShell : Explication

PowerShell est un outil puissant de ligne de commande et un langage de script développé par Microsoft. Il est conçu pour automatiser les tâches d'administration système et de gestion des configurations, principalement dans des environnements Windows, mais il est également compatible avec d'autres systèmes d'exploitation comme Linux et macOS.

Caractéristiques Principales de PowerShell

Interface en Ligne de Commande (CLI) PowerShell permet d'exécuter des commandes interactives pour administrer des systèmes et des applications.

Langage de Script PowerShell utilise un langage basé sur des objets (objet .NET), ce qui facilite la manipulation de données complexes, comme les fichiers, les processus ou les services réseau.

Modules et Cmdlets

Les Cmdlets (Command-Lets) sont des commandes légères intégrées dans PowerShell pour exécuter des tâches spécifiques (ex. : Get-Process, Get-Service).

Les Modules regroupent plusieurs Cmdlets et fonctions pour étendre les fonctionnalités de PowerShell.

Interopérabilité PowerShell peut interagir avec d'autres technologies, comme WMI (Windows Management Instrumentation), les API REST, et même des applications comme Active Directory ou Microsoft 365.

Open Source Depuis PowerShell Core, l'outil est open source et multiplateforme, avec une prise en charge de Windows, Linux, et macOS.

Utilisations de PowerShell

Automatisation des Tâches Répétitives

Exécution de scripts pour créer, modifier ou supprimer des comptes utilisateurs.

Automatisation de tâches comme la sauvegarde ou la gestion des permissions.

Gestion des Systèmes

Surveillance et gestion des services ou des processus.

Installation et configuration de logiciels ou de mises à jour.

Administration de Réseaux

Gestion des connexions réseau, des ports, ou des adresses IP.

Automatisation de la configuration DNS, DHCP, et autres services réseau.

Gestion des Environnements Cloud

Administration des services cloud comme Microsoft Azure ou AWS via des modules spécifiques.

Analyse et Extraction de Données

Collecte et manipulation de journaux (logs) ou de données pour générer des rapports personnalisés.

Exemples de Commandes PowerShell

Lister les processus actifs : powershell CopierModifier Get-Process

Vérifier les services en cours d'exécution : powershell CopierModifier Get-Service | Where-Object {$_.Status -eq 'Running'}

Créer un utilisateur Active Directory : powershell CopierModifier New-ADUser -Name "John Doe" -SamAccountName "jdoe" -Path "OU=Users,DC=example,DC=com"

Vérifier l'espace disque disponible : powershell CopierModifier Get-PSDrive -PSProvider FileSystem

Extraire des informations système : powershell CopierModifier Get-ComputerInfo

Avantages de PowerShell

Flexibilité PowerShell permet de gérer une large gamme de systèmes et services, qu'ils soient locaux ou distants.

Automatisation Les scripts PowerShell réduisent les interventions manuelles, améliorant ainsi l'efficacité et minimisant les erreurs.

Communauté Active Grâce à sa communauté et à des outils comme la PowerShell Gallery, des milliers de modules et scripts sont disponibles.

Multiplateforme Avec PowerShell Core, il est possible d'administrer des environnements Windows, Linux, et macOS.

Limitations de PowerShell

Courbe d'Apprentissage Les utilisateurs novices peuvent trouver PowerShell difficile à maîtriser en raison de sa syntaxe basée sur les objets.

Sécurité Bien que PowerShell inclue des protections (ex. : politiques d'exécution de scripts), un usage inapproprié peut présenter des risques.

PowerShell est un outil incontournable pour les administrateurs système, permettant une gestion centralisée et efficace des environnements informatiques. Sa puissance réside dans sa capacité à automatiser, surveiller et administrer un large éventail de services et de systèmes, que ce soit en local ou dans le cloud.

Proxy : Explication

Un proxy est un serveur qui agit comme intermédiaire entre un utilisateur (client) et une ressource (serveur) sur Internet ou un réseau. Il relaie les requêtes des clients vers le serveur cible et retourne les réponses à ces clients.

Types de Proxys

Proxy Direct

Relaye simplement la requête du client vers le serveur cible sans modification majeure.

Proxy Inverse

Placé devant un ou plusieurs serveurs pour gérer les requêtes entrantes (ex. : équilibrage de charge, mise en cache).

Proxy Transparent

Intercepte les communications sans nécessiter de configuration sur les clients.

L'utilisateur n'est pas forcément conscient qu'un proxy est utilisé.

Proxy Anonyme

Cache les informations du client (comme son adresse IP) pour garantir l'anonymat en ligne.

Proxy Socks

Supporte tous les types de trafic réseau (HTTP, FTP, P2P, etc.), offrant plus de flexibilité.

Rôles et Fonctions du Proxy

Filtrage et Sécurité

Bloque l'accès à certains sites ou contenus non autorisés (contrôle parental ou politique d'entreprise).

Protège contre les attaques en cachant les adresses IP des clients.

Amélioration des Performances

Mise en cache des ressources fréquemment demandées pour réduire la latence et économiser la bande passante.

Anonymat et Confidentialité

Masque les adresses IP des utilisateurs pour préserver leur anonymat sur Internet.

Contrôle d'Accès

Restreint l'accès à Internet en fonction des règles définies (par exemple, autorisation basée sur les heures de travail ou l'identité des utilisateurs).

Répartition de Charge (Load Balancing)

Répartit les requêtes entre plusieurs serveurs pour éviter la surcharge.

Exemples d’Utilisation du Proxy

Dans une Entreprise

Bloquer l'accès à des sites non professionnels comme les réseaux sociaux.

Optimiser la bande passante en mettant en cache les contenus les plus consultés.

Pour un Particulier

Utiliser un proxy pour contourner des restrictions géographiques (par exemple, accéder à des services non disponibles dans votre pays).

Dans le Commerce Électronique

Les proxys inverses permettent de sécuriser les serveurs web en interceptant les requêtes malveillantes avant qu’elles n’atteignent le serveur cible.

Avantages du Proxy

Sécurité Améliorée

Empêche les menaces directes contre les clients et les serveurs.

Permet une navigation anonymisée.

Performance Optimisée

Réduit la latence grâce à la mise en cache des données.

Économise la bande passante réseau.

Contrôle et Gestion

Offre une visibilité sur l’utilisation d’Internet.

Permet de configurer des règles précises pour l'accès aux ressources réseau.

Inconvénients du Proxy

Coût et Maintenance

Les proxys avancés (comme ceux utilisés pour les grandes entreprises) nécessitent une infrastructure et une maintenance coûteuses.

Complexité

Configurer un proxy efficace peut être complexe, surtout pour les proxys inverses ou les proxys SOCKS.

Limitation de la Vitesse

Si le proxy est surchargé, il peut ralentir la connexion Internet.

Exemple de Fonctionnement

Un utilisateur souhaite visiter www.example.com.

La requête passe d'abord par le proxy, qui vérifie :

Si l'accès est autorisé.

Si une copie du site est déjà en cache.

Si autorisé et non en cache, le proxy contacte www.example.com et transmet la réponse à l'utilisateur.

Un proxy est un outil essentiel pour améliorer la sécurité, gérer les connexions réseau et optimiser les performances. Il est utilisé dans de nombreux domaines, allant des entreprises aux particuliers cherchant à protéger leur vie privée ou contourner des restrictions géographiques.

Journalisation (Logs) : Explication

La journalisation, ou logs, désigne le processus d'enregistrement des événements et des activités d'un système informatique, d'une application ou d'un serveur dans des fichiers appelés logs. Ces fichiers contiennent des informations détaillées sur les opérations effectuées, ce qui permet de suivre, analyser, et résoudre des problèmes en cas d'incidents.

Types de Logs

Logs Système

Enregistrent les événements du système d'exploitation (ex. : démarrage, arrêt, erreurs système).

Exemple : /var/log/syslog sur Linux ou le Journal des événements dans Windows.

Logs d'Application

Contiennent des informations générées par des applications spécifiques (ex. : serveur web, bases de données).

Exemple : les logs d'un serveur Apache (/var/log/apache2/) ou les logs d'une application métier.

Logs de Sécurité

Enregistrent les événements liés à la sécurité, comme les tentatives de connexion, les modifications des paramètres de sécurité, ou les attaques potentielles.

Exemple : journaux des tentatives d'accès ou des événements de pare-feu.

Logs de Réseau

Fournissent des informations sur le trafic réseau, les connexions établies, et les communications réseau.

Exemple : logs de pare-feu, de proxy, ou de routeur.

Logs d'Audit

Permettent de suivre les actions spécifiques d'un utilisateur ou d'un groupe d'utilisateurs pour des raisons de conformité ou d'investigation.

Rôles et Importance de la Journalisation

Débogage et Résolution de Problèmes

Permet d'identifier la cause des erreurs, des pannes ou des dysfonctionnements en examinant les événements précédant ou suivant le problème.

Exemple : Si un serveur web plante, les logs peuvent révéler une surcharge ou une erreur spécifique dans le code.

Sécurité et Surveillance

Les logs de sécurité permettent de détecter des activités suspectes, telles que des tentatives d'intrusion ou des actions malveillantes.

Exemple : des tentatives de connexion échouées répétées peuvent indiquer une attaque par force brute.

Audit et Conformité

Pour répondre aux exigences légales ou réglementaires, les entreprises doivent souvent maintenir des journaux d'audit détaillés pour démontrer la traçabilité des actions.

Exemple : les logs peuvent aider à prouver qu'un employé a accédé à des informations sensibles dans un contexte particulier.

Optimisation des Performances

Les logs peuvent fournir des informations sur la charge du système, le temps de réponse des services ou les erreurs fréquentes, ce qui aide à optimiser les performances.

Exemple : les logs d'un serveur web peuvent indiquer des pages lentes ou un nombre excessif de requêtes, suggérant la nécessité de modifications ou d'optimisations.

Outils de Journalisation

Syslog

Un protocole standard pour la collecte de logs, utilisé dans les systèmes Linux/Unix.

Permet l'envoi de logs à un serveur centralisé pour une gestion et une analyse facilitées.

Windows Event Viewer

Outil intégré de Windows qui permet de visualiser, d'analyser et de filtrer les événements systèmes, d'application et de sécurité.

Splunk

Un outil d’analyse de logs puissant qui permet de collecter, indexer et visualiser les logs pour identifier des tendances et des anomalies.

Logstash et Elasticsearch

Utilisés ensemble dans le ELK stack (Elasticsearch, Logstash, Kibana), ces outils permettent de collecter, indexer, rechercher et visualiser les logs en temps réel.

Graylog

Une plateforme de gestion des logs qui centralise, analyse et visualise les journaux d’événements pour les entreprises.

Exemples de Logs et Informations Utiles

Logs d'Apache

Un log Apache typique pourrait inclure :

plaintext CopierModifier 192.168.1.8 - - [22/Jan/2025:10:00:00 +0000] "GET /index.html HTTP/1.1" 200 1024

Cela indique qu'une requête GET a été effectuée à 10h00 sur la page index.html depuis l'IP 192.168.1.10, et que la page a été renvoyée avec succès (200).

Logs de Sécurité Windows

Exemple d’événement de connexion :

plaintext CopierModifier Event ID: 4624

Logon Type: 3

Account Name: user1

IP Address: 192.168.1.100

Cela indique qu’un utilisateur (user1) s’est connecté via le réseau (type de connexion 3) depuis l’adresse IP 192.168.1.100.

Meilleures Pratiques en Matière de Journalisation

Centralisation des Logs

Centraliser les logs sur un serveur dédié permet une gestion plus facile et une analyse en temps réel, réduisant le risque de perdre des informations cruciales.

Rotation et Archivage des Logs

Mettre en place une politique de rotation des logs pour éviter que les fichiers ne deviennent trop volumineux, ce qui pourrait ralentir le système ou entraîner la perte d'informations anciennes.

Analyse et Alertes Automatiques

Utiliser des outils de surveillance pour analyser les logs en temps réel et générer des alertes automatiques en cas de détection d’anomalies.

Confidentialité et Sécurité des Logs

Protéger les logs avec des contrôles d'accès appropriés pour empêcher l'accès non autorisé aux informations sensibles.

La journalisation est un aspect essentiel de l’administration des systèmes informatiques, permettant de suivre les activités, d’identifier des problèmes, d’assurer la sécurité et de répondre aux exigences de conformité. Les logs sont cruciaux pour maintenir un environnement informatique stable et sécurisé, et ils permettent aux administrateurs et aux responsables de la sécurité de réagir rapidement en cas d'incident.