BTS Services Informatiques aux Organisations

Option SISR – Épreuve E6

Ressources documentaires – Réalisation professionnelle n°1

Mise en place d'une infrastructure Active Directory avec GPO,
partages réseau sécurisés (DFS) et déploiement automatisé de logiciels

Candidat : EZZAMOURI Yanis
Établissement : Lycée Saint-Exupéry – Saint-Raphaël
Date : 05/05/2026
Lien vers la production : https://yanis-ezzamouri.fr/?p=781

1. Contexte et besoins

1.1 Présentation de l'organisation

Le port de Cherbourg est une infrastructure portuaire française accueillant des activités variées : transport de passagers, ferries, fret maritime, croisières ainsi que des opérations de maintenance navale. Son système d'information repose sur plusieurs postes de travail répartis entre différents services (direction, exploitation, maintenance, informatique).

1.2 Problèmes identifiés

- Les comptes utilisateurs et les droits d'accès sont gérés localement sur chaque poste, sans centralisation de l'authentification ni des stratégies de sécurité.
- Aucune stratégie de groupe n'est appliquée : chaque poste est configuré manuellement, ce qui génère des incohérences et des risques de sécurité.
- Il n'existe pas de partage réseau sécurisé par département, ni de déploiement automatisé de logiciels.
- La gestion des comptes représente une charge importante pour l'administrateur.

1.3 Objectifs fixés

Le directeur des systèmes d'information, M. Richard, souhaitait moderniser l'infrastructure afin de :

- Centraliser l'authentification et la gestion des utilisateurs via un domaine Active Directory.
- Déployer des stratégies de groupe (GPO) pour uniformiser et sécuriser les postes.
- Mettre en place un serveur de fichiers DFS avec des permissions NTFS et des quotas par département.
- Automatiser le déploiement de logiciels sur les postes du domaine via GPO.

2. Solutions envisagées et solution retenue

2.1 Comparatif des solutions

Solution	Avantages	Inconvénients
Active Directory (Windows Server 2022)	Natif Windows, GPO puissantes, DNS/DHCP/DFS intégrés, large documentation	Licence Microsoft requise
Samba AD (Linux)	Open-source, compatible clients Windows, gratuit	Gestion des GPO plus limitée, configuration complexe
FreeIPA	Open-source, gestion centralisée des identités	Principalement orienté Linux, peu adapté à un parc Windows

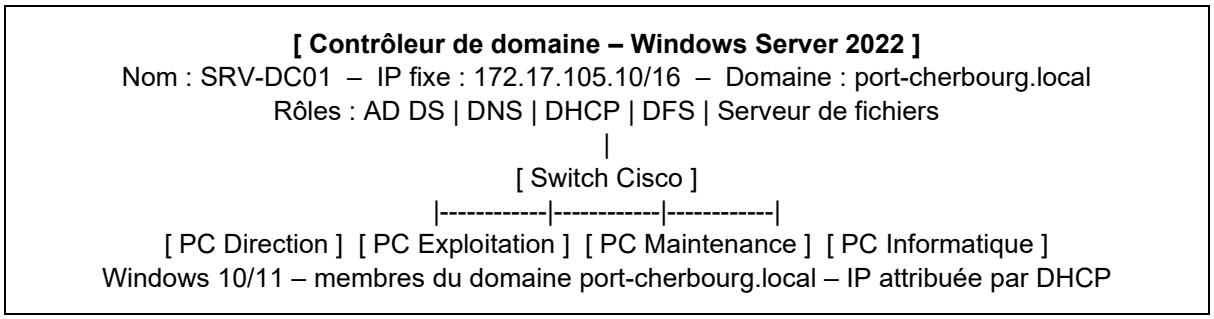
2.2 Solution retenue

- Active Directory sur Windows Server 2022 a été retenu pour sa compatibilité native avec les postes Windows du port, sa richesse fonctionnelle (GPO, DNS, DHCP, DFS) et sa large documentation.
- Le serveur de fichiers DFS (Distributed File System) a été retenu pour organiser et sécuriser les partages réseau par département, grâce à sa gestion centralisée des espaces de noms, des permissions NTFS et des quotas disque.
- Le déploiement de logiciels via GPO (fichiers MSI) a été retenu pour automatiser l'installation sur tous les postes du domaine sans intervention manuelle.

3. Architecture réseau

3.1 Schéma de l'infrastructure

L'infrastructure repose sur un réseau local avec adressage IP fixe. Le contrôleur de domaine (Windows Server 2022) centralise l'authentification et les services DNS, DHCP et DFS. Le schéma ci-dessous représente l'architecture mise en place :



3.2 Plan d'adressage

Équipement	Adresse IP	Masque	Rôle
Contrôleur de domaine (SRV-DC01)	172.17.105.10	/16	AD DS, DNS, DHCP, DFS, Fichiers
Postes clients (par département)	172.17.105.20 – .50	/16	Membres du domaine (DHCP)
Passerelle / Routeur	172.17.250.3	/16	Accès réseau

4. Mise en oeuvre

Phase 1 – Installation de l'environnement

4.1 Installation de Windows Server 2022

- Installation du système depuis l'ISO Windows Server 2022 (édition Standard).
- Configuration du nom d'hôte : SRV-DC01.
- Attribution de l'adresse IP fixe : 172.17.105.10/16, passerelle 172.17.250.3.
- Installation des mises à jour système.

4.2 Installation des rôles

- Ajout des rôles AD DS, DNS et DHCP via le Gestionnaire de serveur.
- Promotion du serveur en contrôleur de domaine : domaine port-cherbourg.local.
- Configuration de la plage DHCP : 172.17.105.20 à 172.17.105.50, option DNS pointant sur 172.17.250.3.
- Ajout du rôle DFS (Distributed File System) – Espaces de noms.

Phase 2 – Configuration du domaine

4.3 Arborescence des Unités d'Organisation (UO)

L'arborescence suivante a été créée dans le domaine port-cherbourg.local :

```
port-cherbourg.local
├── UO_Direction
│   ├── Utilisateurs
│   └── Groupes
├── UO_Exploitation
│   ├── Utilisateurs
│   └── Groupes
├── UO_Maintenance
│   ├── Utilisateurs
│   └── Groupes
└── UO_Informatique
    ├── Utilisateurs
    └── Groupes
```

4.4 Intégration des postes au domaine

- Sur chaque poste client : Système > Renommer ce PC (paramètres avancés) > Domaine : port-cherbourg.local.
- Saisie des identifiants administrateur du domaine pour valider l'intégration.
- Redémarrage du poste et vérification de l'authentification avec un compte du domaine.

Phase 3 – GPO et serveur de fichiers DFS

4.5 Stratégies de groupe (GPO) configurées

GPO	Paramètre	Cible
GPO_Securite	Politique de mots de passe : 10 car. min, complexité obligatoire, verrouillage après 5 tentatives	Tout le domaine
GPO_Bureau	Fond d'écran imposé, restriction du panneau de configuration, verrouillage de session après 10 min	Tous les postes clients
GPO_LecteursReseau	Mappage automatique du lecteur DFS selon le groupe de l'utilisateur à la connexion	Par UO de département

4.6 Serveur de fichiers DFS – Espace de noms et partages

L'espace de noms DFS créé est : \\port-cherbourg.local\Partages

Dossier DFS	Groupe autorisé	Permissions NTFS
\Partages\Direction	GRP_Direction	Contrôle total
\Partages\Exploitation	GRP_Exploitation	Lecture / Écriture
\Partages\Maintenance	GRP_Maintenance	Lecture / Écriture
\Partages\Informatique	GRP_Informatique	Contrôle total

Phase 4 – Tests et validation

4.7 Tableau de recette

Test	Action réalisée	Résultat attendu	Résultat obtenu
Authentification domaine	Connexion avec compte du domaine sur poste client	Session ouverte	OK
Application GPO bureau	Connexion utilisateur, vérification fond d'écran et restrictions	GPO appliquée	OK
Mappage lecteur DFS	Connexion utilisateur, vérification lecteur réseau mappé	Lecteur DFS mappé	OK

Droits NTFS DFS	Tentative d'accès au dossier d'un autre département	Accès refusé	OK
Déploiement logiciel GPO	Connexion poste client, vérification logiciel installé	Logiciel présent	OK
Politique mots de passe	Tentative de création avec mot de passe faible	Refus + message d'erreur	OK
Attribution DHCP	Connexion nouveau poste au réseau	IP attribuée automatiquement	OK

5. Ressources matérielles et logicielles

5.1 Matériel utilisé

Équipement	Rôle	Caractéristiques
Serveur virtuel	Contrôleur de domaine	Héberge Windows Server 2022
Switch Cisco	Interconnexion réseau local	Commutateur manageable
Postes clients Windows 10/11	Tests d'intégration au domaine	Membres du domaine, accès DFS

5.2 Logiciels utilisés

Logiciel	Version	Usage
Windows Server	2022	Contrôleur de domaine, DNS, DHCP, DFS, fichiers
Windows	10 / 11	Postes clients membres du domaine
Gestionnaire DFS	Intégré WS2022	Configuration des espaces de noms et des partages

6. Bilan

Le déploiement de cette infrastructure Active Directory a permis de centraliser la gestion des utilisateurs, des postes et des droits d'accès du port de Cherbourg. La solution répond pleinement aux besoins identifiés lors de la phase d'analyse.

Les principaux bénéfices sont les suivants :

- Centralisation de l'authentification : les utilisateurs se connectent avec un compte unique sur n'importe quel poste du domaine.
- Uniformisation et sécurisation des postes via les GPO : fond d'écran, restrictions, politique de mots de passe.
- Partages réseau DFS organisés par département avec permissions NTFS et quotas disque adaptés.
- Déploiement automatisé des logiciels via GPO, supprimant les installations manuelles poste par poste.

Compétences mobilisées :

- Concevoir une solution d'infrastructure réseau.
- Installer, tester et déployer une solution d'infrastructure réseau.
- Exploiter, dépanner et superviser une solution d'infrastructure réseau.