Mise en place d'un serveur AD, DNS avec redondance

Sommaire

Cahier des charges – Expression des besoins

Descriptif de l'existant

L'infrastructure est inexistante, j'ai seulement accès à une sortie Internet via le LAN du GRETA.

Besoin(s)

Dans le cadre d'un TP pédagogique, je dois mettre en place deux serveurs AD et DNS avec de la redondance. Je dois aussi configurer un routeur qui servira uniquement à lier les 2 sous-réseaux ainsi qu'à leur donner accès à Internet.

Contrainte(s)

J'ai 16 heures pour mettre en place cette solution et tester si la redondance AD et DNS fonctionnent correctement.

Ressources

Ressources mises à disposition

J'ai à ma disposition une machine hôte qui possède Hyper-V comme logiciel de virtualisation, de plus j'ai accès au réseau LAN du GRETA ce qui me permet d'avoir un accès à Internet.

Ressources nécessaires à la mise en place

J'ai besoin d'une machine hôte qui a un logiciel de virtualisation, j'ai aussi besoin d'un accès à Internet, ainsi que les ISO de Windows Server 2025 et de Windows 11.

Gestion des ressources

J'ai déjà à ma disposition l'ISO de Windows Server 2025 et de Windows 11 25H2.

Analyse

Descriptifs des solutions

Active Directory Windows est la solution officielle de Microsoft pour centraliser l'authentification, gérer les utilisateurs, les ordinateurs et appliquer des stratégies via les GPO dans un environnement Windows.

Il s'installe sur Windows Server, offre une intégration native avec tous les systèmes Microsoft, fournit des outils d'administration graphiques complets et garantit une réplication stable entre plusieurs contrôleurs de domaine. C'est l'option la plus fiable, la plus compatible et la plus simple à maintenir lorsque l'infrastructure repose majoritairement sur des postes Windows, même si cette dernière implique un coût de licence.

Active Directory Linux, basé sur Samba 4, est une ré-implémentation open-source permettant d'offrir un contrôleur de domaine compatible avec les standards Active Directory. Il fonctionne sur n'importe quelle distribution Linux, prend en charge l'authentification Kerberos, la jointure de postes Windows et l'application de GPO basiques, tout en étant totalement gratuite. Sa configuration est plus technique, la réplication et les GPO sont parfois plus limitées, et son administration passe surtout par la ligne de commande, mais il constitue une alternative économique et flexible pour les environnements avec un budget assez faible.

Comparaison des solutions (tableau)

Critères	**Active Directory Windows**	**Active Directory Linux (Samba AD DC)**
Type	Solution officielle Microsoft	Alternative open-source
Coût	Payant (licence Windows Server)	Gratuit
Installation	Simple, guidée, outillée	Plus technique, configuration manuelle
Administration	Outils graphiques complets (ADUC, GPO, DNS)	Ligne de commande + RSAT partiel
GPO	Support complet	Support partiel, certaines fonctions limitées
Intégration Windows	Parfaite	Fonctionnel mais pas 100% identique
Intégration Linux	Moyenne	Excellente
Réplication	Très stable	Fonctionnelle mais plus sensible
DNS	Intégré avec AD	DNS Samba ou Bind9
Usage recommandé	Entreprises, environnements Microsoft	Environnements à budget faibles

Choix d'une solution - Argumentation

J'ai choisi de mettre en place un Active Directory Windows, bien que cette solution soit payante, elle reste nettement plus simple à déployer et bien moins risquée à maintenir qu'un contrôleur de domaine basé sur Linux. L'intégration native avec les postes Windows, les outils d'administration complets et la stabilité de la réplication en font une solution plus fiable et plus adaptée à un environnement professionnel, sans être limité par la complexité technique d'une implémentation Samba.

Plan d'adressage - Tables de routage

- Tableau d'adressage :

Nom des réseaux	Adresse réseau	Masque de sous réseau	Première adresse	Dernière adresse	Adresse de broadcast
WAN	172.26.0.0	255.255.248.0	172.26.0.1	172.26.7.254	172.26.7.255
SR-01	172.28.0.0	255.255.255.128	172.28.0.1	172.28.0.126	172.28.0.127
SR-02	172.28.0.128	255.255.255.128	172.28.0.129	172.28.0.254	172.28.0.255

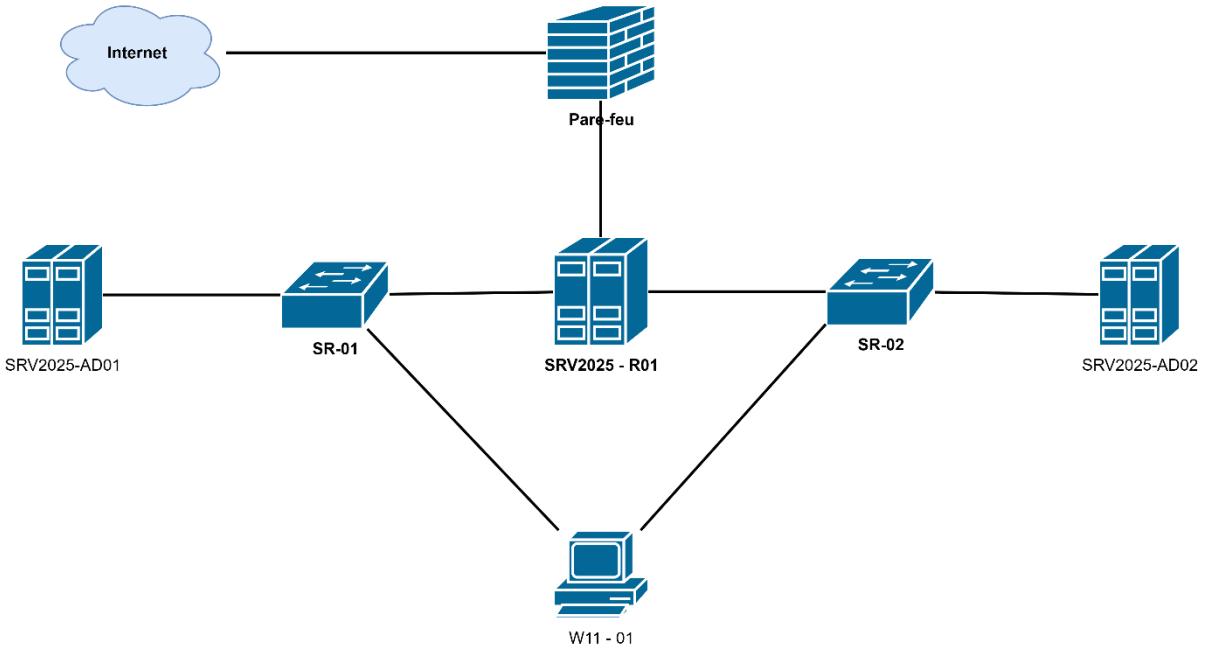
- Tableau des IP :

Serveurs	Adresse IP	Masque de sous réseau	Passerelle par défaut	DNS
R01	1) Sortie GRETA : 172.26.5.16 2) SR-01 : 172.28.0.126 3) SR-02 : 172.28.0.254	1) 255.255.248.0 2) 255.255.255.128 3) 255.255.255.128	1) 172.26.7.254 2) ø 3) ø	1) 1.1.1.1 & 8.8.8.8
AD01	172.28.0.1	255.255.255.128	172.28.0.126	172.28.0.1 & 172.28.0.129
AD02	172.28.0.129	255.255.255.128	172.28.0.254	172.28.0.129 & 172.28.0.1
W11-01	DHCP	255.255.255.128	DHCP	172.28.0.1 & 172.28.0.129

- Table de routage du serveur R01 :

Adresse réseau	Masque réseau	Adresse passerelle	Métrique
0.0.0.0	0.0.0.0	172.26.7.254	Par défaut
172.28.0.0	255.255.255.128	On-link	1
172.28.0.128	255.255.255.128	On-link	1

Schéma du réseau



Étude de l'impact sur le SI existant

La mise en place d'une infrastructure Active Directory redondée apporte une évolution majeure au fonctionnement d'un système d'information. Elle renforce la disponibilité des services, améliore la sécurité et structure plus efficacement la gestion des postes et des utilisateurs. Cette intégration génère cependant plusieurs impacts : techniques, organisationnels, humains, stratégiques et juridiques.

- **Impact technique :**

La mise en place de deux contrôleurs de domaine nécessite une architecture réseau stable et cohérente.
La réplication AD entre les serveurs doit fonctionner correctement et dépend d'une horloge synchronisée, des liaisons réseau et d'une bonne configuration DNS.
Cette architecture nécessite la mise en place d'une stratégie de sauvegarde adaptée aux services AD et DNS, incluant les États du système, afin de pouvoir restaurer proprement un contrôleur de domaine en cas de défaillance.

- **Impact organisationnel :**

L'arrivée d'Active Directory centralise la gestion des utilisateurs, des machines et des stratégies via les GPO.
Les techniciens n'administrent plus les postes individuellement : toutes les configurations, règles de sécurité et autorisations passent désormais par les contrôleurs de domaine.
Cette centralisation oblige le service informatique à structurer davantage :

- la gestion des comptes (création, suppression, verrouillage)
- les règles de sécurité internes
- les procédures d'intégration et de sortie des utilisateurs
- les droits d'accès aux différentes ressources du réseau

La redondance des serveurs AD impose aussi une procédure claire en cas de panne : ordre de bascule, contrôles à effectuer, redémarrage des services, etc.

- **Impact humain :**

Les techniciens doivent monter en compétence sur :

- le fonctionnement interne d'Active Directory
- la réplication entre contrôleurs de domaine
- la gestion du DNS intégré à AD
- l'utilisation d'outils d'administration (RSAT)

L'AD modifie également la façon dont les utilisateurs interagissent avec leur environnement : authentification centralisée, mots de passe gérés par l'entreprise, restrictions appliquées par GPO, homogénéité des postes.
Cette uniformisation améliore la sécurité mais nécessite une communication interne pour expliquer les changements.

- **Impact stratégique :**

Active Directory devient un socle central pour l'entreprise.
La redondance des services AD et DNS améliore considérablement la continuité d'activité : même en cas de panne d'un serveur, les utilisateurs continuent de s'authentifier et de travailler.
Sur le plan stratégique :

- L'entreprise améliore sa résilience face aux incidents.
- Les services critiques (authentification, résolution DNS, GPO) restent disponibles.
- La gestion informatique devient plus structurée, prévisible et conforme aux bonnes pratiques.

Cette infrastructure constitue une base solide pour des évolutions futures : déploiement automatisé de postes, centralisation des applications, renforcement de la sécurité, audit interne, etc.

- **Impact juridique :**

L'introduction d'Active Directory implique la manipulation d'un nombre important de données à caractère personnel : noms, prénoms, comptes utilisateurs, groupes d'appartenance, mots de passe chiffrés, informations techniques liées aux machines. Dans un contexte professionnel réel, cette centralisation doit respecter les exigences du RGPD :

- contrôle strict des accès à l'annuaire
- conservation limitée des comptes inactifs
- traçabilité des actions administratives
- politique de mots de passe conforme aux normes internes
- protection des données stockées dans AD (sauvegardes sécurisées, chiffrement, accès restreint)

La présence de deux contrôleurs de domaine augmente également les exigences en termes de logs, de conformité et de protection des données lors des sauvegardes et restaurations.

Phasage de l'intervention

Je commencerai par déployer les quatre machines virtuelles sur Hyper-V. Ensuite j'installerai et configurerai les services de routage et de DHCP sur le serveur SRV2025-R01, ces étapes ne seront pas détaillées dans la procédure. Je procéderai ensuite à l'installation puis à la configuration du service DNS sur les serveurs SRV2025-AD01 et SRV2025-AD02. Après validation des tests DNS, j'installerai le service Active Directory sur SRV2025-AD01 puis sur SRV2025-AD02. Enfin je réaliserai une phase de tests dédiée à l'AD.

Prévision des tests de validation

Je procéderai d'abord à une série de tests dédiés aux services DNS afin de vérifier la redondance entre les deux serveurs avant le déploiement d'Active Directory. Cette phase inclura le contrôle de la synchronisation des zones DNS, la résolution de noms en interne et

vers Internet, ainsi que la bascule automatique d'un serveur DNS à l'autre en cas d'indisponibilité de l'un des deux serveurs.
La seconde phase portera sur les services Active Directory, une fois les deux contrôleurs de domaine opérationnels. Je validerai d'abord la synchronisation entre les deux AD, puis l'intégration de la VM cliente au domaine. Enfin, je vérifierai la continuité de service en simulant la panne d'un contrôleur de domaine et en observant la reprise par le second.

Mise en place

La partie Mise en place a été rédigée sur Notion, vous la trouverez via le lien suivant : https://mathys-demon.notion.site/Installation-AD-et-DNS-avec-redondance-2b78102ecdc980a5b7a7ebc4db697e7d.

Bilan

Conclusion

La réplication fonctionne correctement, les tests DNS et AD sont concluants, et la VM cliente peut s'authentifier via les deux serveurs. L'architecture répond au besoin du TP : disposer d'un AD fiable, d'une résolution DNS fonctionnelle sur deux sous-réseaux et d'une infrastructure capable de basculer automatiquement.

Auto-évaluation

Ce TP m'a permis de mieux comprendre le fonctionnement d'Active Directory, la réplication entre contrôleurs de domaine et l'importance du DNS dans une infrastructure Microsoft. J'ai pu valider les principes de redondance, réaliser des tests de bascule et structurer une procédure claire. L'ensemble m'a aidé à renforcer mes compétences en environnement Windows Server et en gestion d'infrastructures réseau.