

Projet

Durée : 15h (4 séances de TP)

L'objectif de ce projet est d'installer et de configurer les services DNS, d'accès à distance et de messagerie.

1. Objectifs

1.1 Attente pour le service DNS :

Vous devrez acheter un domaine de nom auprès d'un « registrar » représenté par votre enseignant.

- Le domaine que vous aurez à gérer sera un sous-domaine du tld (privé) .tp .
- Le serveur primaire de cette zone sera un serveur windows 2016 dont le nom sera R303_« groupe »_1. Le nom défini ci-avant sera utilisé comme nom de VM et comme nom système. Le nom DNS de votre machine pourra être différent.
- Vous devrez assurer une redondance du service DNS en créant un serveur DNS secondaire (OS : windows serveur 2016). Le nom de ce serveur sera R303_« groupe »_2.
- Vous devrez créer deux sous-domaines de vos zones. La gestion d'un des sous-domaines devra être déléguée à un autre serveur (OS : windows serveur 2016) dont le nom sera R303_« groupe »_3.

1.2 Attente pour le service d'accès à distance :

Vous devrez configurer le serveur R303_« groupe »_3, pour qu'il autorise plus de deux connexions simultanées. Les utilisateurs du domaine peda.rt.local devront pouvoir utiliser les applications Thunderbird (client de messagerie utilisé pour vos tests) et wireshark installées sur ce serveur via un accès distant (**Remote Desktop web**).

1.3 Attente pour le service de messagerie :

Sur un 4^{ème} serveur (OS : windows serveur 2016, nom du serveur R303_« groupe »_4.), vous devrez installer un serveur de messagerie (logiciel à utiliser : « hmailserver ») qui permettra la gestion de la messagerie de votre domaine de nom. Les services imap, pop et smtp devront être proposés par ce serveur. On vous demande de créer deux comptes utilisateurs.

Pour tester le bon fonctionnement de votre service, vous aurez à configurer les clients de messagerie (installés sur la machine définie aux paragraphes précédent) avec deux comptes utilisateurs : un des comptes devra utiliser le service pop et l'autre le service IMAP pour récupérer leurs messages. Cela vous permettra de voir les différences de fonctionnement.

Votre serveur de messagerie permettra de transférer les mails vers des domaines extérieurs (ceux gérés par vos camarades, par exemple). Un serveur de test, géré par l'enseignant, est déjà configuré (compte utilisateur à utiliser pour l'envoi de mail : maurice@tp.rt)

Remarque : faites attention à la sécurité.

2. Planning

1. Fin de la première séance :
 - Un modèle VM Windows serveur 2016 doit être créé.
 - Les VMs gérant le service DNS doivent être créées.
 - Le service DNS doit être configuré (création des différents enregistrements nécessaires, délégation de gestion de zone, redirection, autorisation des transferts de zone)
 - Un rapport d'activité de cette séance doit être fourni en tout début de la séance suivante sur Moodle, contenant, entre autres, les procédures d'installation des services et la justification de toutes les opérations réalisées.
2. Fin de la deuxième séance :
 - Le service DNS doit être testé et validé.
 - Le service accès à distance pour des connexions multiples est configuré et testé
 - Un rapport d'activité de cette séance doit être fourni en tout début de la séance suivante sur Moodle, contenant entre autres les procédures d'installation des services et la justification de toutes les opérations réalisées.
3. Fin de la troisième séance :
 - La mise à disposition d'application à distance (thunderbird et wireshark) doit être réalisée sur le serveur R303_« groupe »_4.
 - Les tests concernant les accès distants doivent être réalisés.
 - Le service de messagerie doit être installé.
 - Un rapport d'activité de cette séance doit être fourni en tout début de la séance suivante sur Moodle, contenant entre autres les procédures d'installation des services et la justification de toutes les opérations réalisées.
4. Fin de la quatrième séance :
 - Les clients de messagerie doivent être installés et configurés.
 - Un service de anti-virus et d'anti-spam devra être installé sur le serveur de messagerie.
 - Les tests doivent être réalisés.
5. Après la dernière séance, vous aurez quelques jours pour rendre le dossier final : ce dossier présentant votre infrastructure doit être rendu sur Moodle. (Cf. paragraphe 4 pour avoir le détail des informations que devra contenir ce dossier).

3. Elément fournis

- Une plage d'adresses IP à utiliser (envoyée par mail)
- Un accès à la plateforme de virtualisation (envoyée par mail). Toutes les machines virtuelles devront être créées dans le centre de données dell_2018.
- Une image de Windows Serveur 2016 (zone de stockage **ISO** lié au centre de données dell_2018)
- Un contrôleur de domaine « PEDA.rt.local » dont le FQDN est « ad.lan.rt »
- Un compte qui vous permet d'intégrer une machine au domaine AD (peda.rt.local). A demander auprès de l'enseignant. (cf procédure d'intégration de vos machines)
- Un serveur de licence gérant les licences d'accès client (CAL) dont le FQDN est « RCLicencespeda.peda.rt.local »
- Un serveur de messagerie stpmail.lan.rt qui administre les mails du domaine tp.rt et qui vous permettra de faire des tests de votre messagerie)

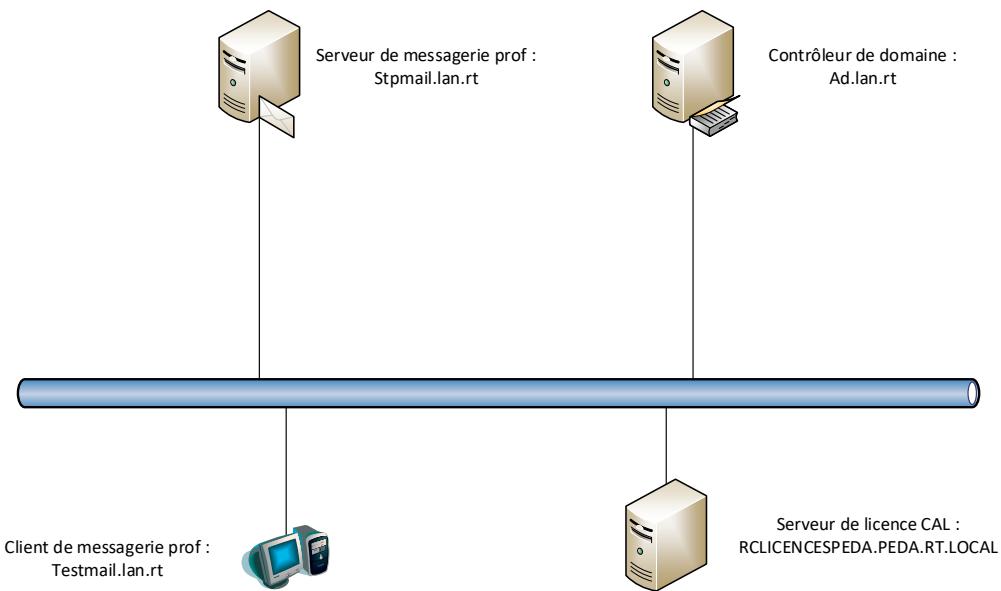
- Un client de messagerie de test (compte de messagerie maurice@tp.rt) (déjà configuré) est présent sur la machine testmail.lan.rt. Cette application est disponible à l'adresse <https://testmail.lan.rt/RDweb>. (Compte de connexion à la machine distante: login « peda\etu_essai » et password : « rtM2103 »).

4. Eléments à fournir à la fin des 4 séances

- Les machines virtuelles hébergeant les différents services.
- Une preuve de compatibilité des applications installées avec l'OS utilisé.
- Un schéma visio ou draw.io de votre infrastructure contenant toutes les informations nécessaires pour se connecter à ces machines :
 - adresse IP,
 - mot de passe admin de la machine
 - login et mot de passe des services installés si besoin,
 - machine intégrée au domaine ou non.
- Eléments de preuves permettant de vérifier que **l'ensemble des services configurés** fonctionnent correctement :
 - dns : résolution de noms internes et externes, redondance, délégation de gestion de zone,
 - service accès distant : accès multiples, web access,
 - messagerie : envoi mail interne et externe, différences pop et imap)

Les éléments qui peuvent être fournis sont :

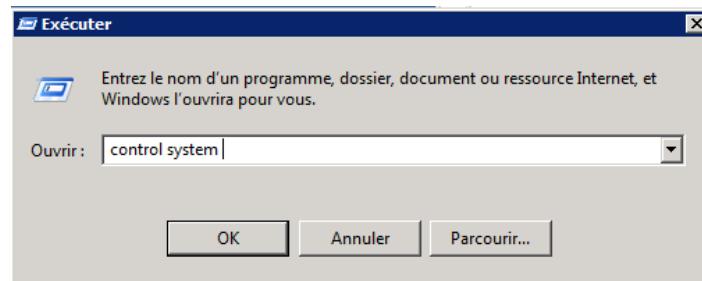
- les procédures de tests
- les captures d'écran des tests,
- les fichiers « wireshark » montrant les échanges réalisés ainsi que l'analyse de ces échanges.
- Un client de messagerie configuré pour permettre tous les tests.
- Pour chaque fonctionnalité, indiquer clairement les rôles qui ont été nécessaire : serveur DNS, accès distant par le web
- Un tuto utilisateur pour utiliser le remote web access
- Une présentation des différentes fonctionnalités du client d'accès à distance (RDP-conexion) proposé par Windows.



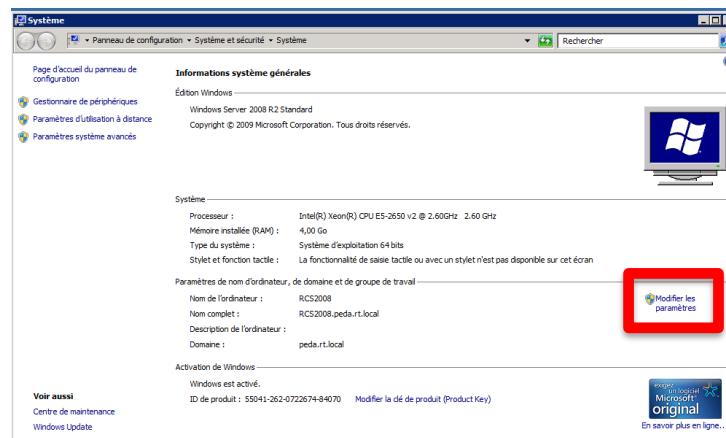
Votre compte « etux » ne vous permet pas d'accéder directement au contrôleur de domaine. Par contre, vous avez les droits pour intégrer une machine dans le domaine « peda.rt.local »

1. Intégration d'une machine dans le domaine

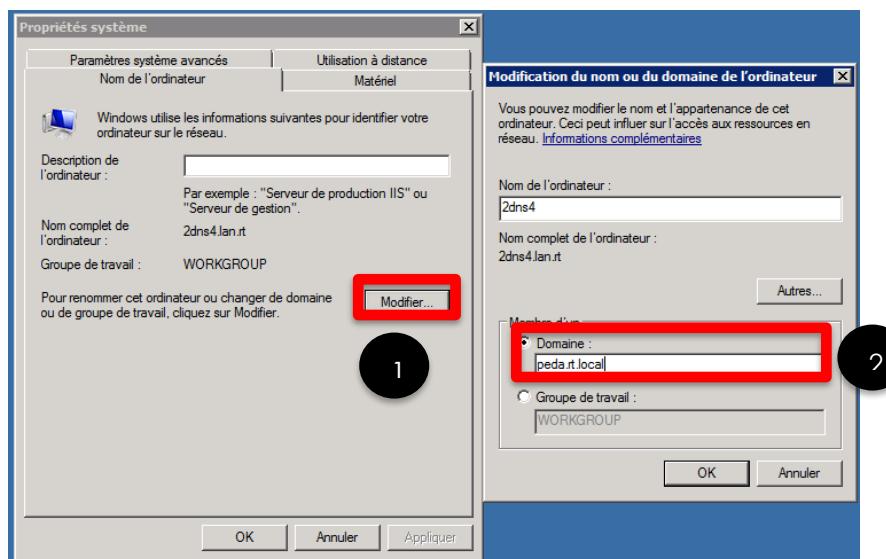
Dans l'onglet « Démarrer », sélectionner « exécuter ».



La fenêtre suivante s'ouvre :



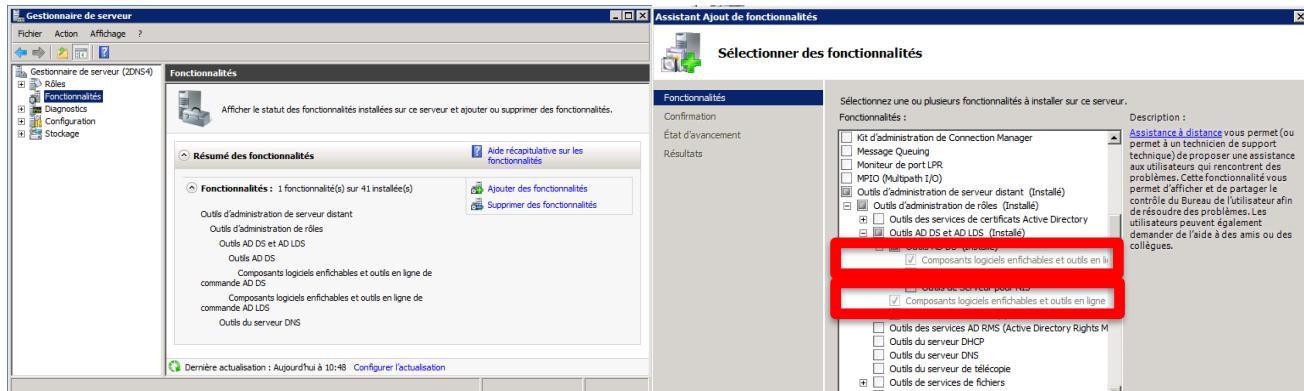
Dans la partie « système », sélectionner « Modifier les paramètres ».



Un mot de passe est demandé pour intégrer le domaine (utilisé le compte utilisateur du domaine fourni par l'enseignant). Un message de bienvenu dans le domaine apparaît.

2. Accès à l'AD

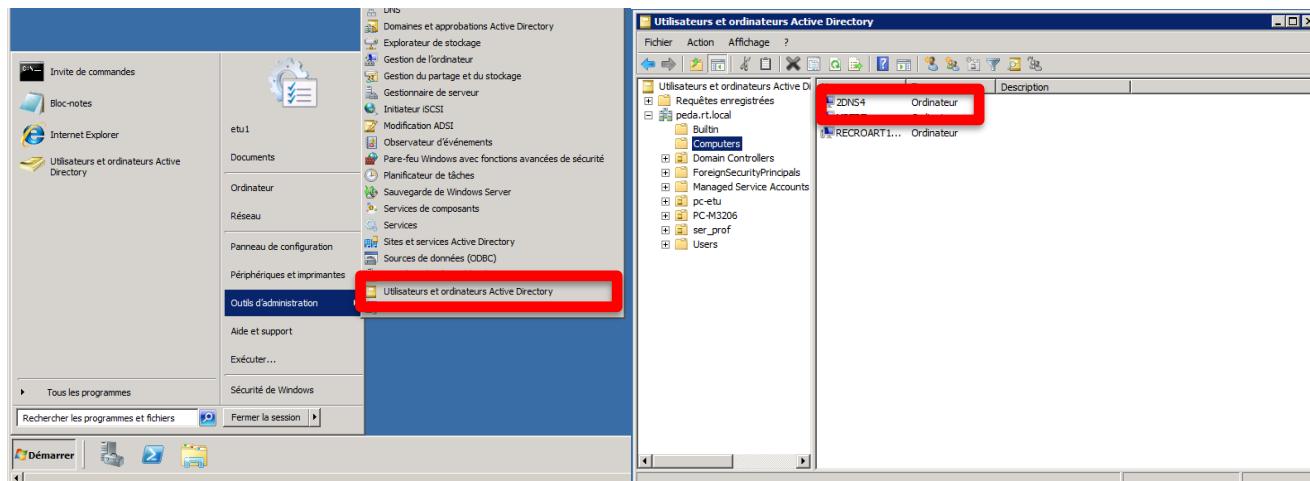
Pour des raisons de sécurité, tout le monde ne peut pas être administrateur du contrôleur de domaine. Par contre, il est possible d'avoir accès à un certain nombre d'information concernant le domaine active directory. Pour ce faire, il est nécessaire d'activer deux nouvelles fonctionnalités sur votre serveur.



Ces deux nouvelles fonctionnalités vont vous permettre d'accéder aux informations qui nous seront utiles.

3. Configuration de l'AD

Accéder à « Utilisateurs et ordinateurs Active Directory »



Après son intégration dans l'AD, votre serveur apparaît parmi le conteneur : Computer (dans le cas de l'exemple, il s'agit du serveur 2dns4).

Dans un AD, il est possible de définir des groupes d'ordinateurs (OU : unité d'organisation) auxquels on définit un ensemble de droit (par exemple : les utilisateurs qui peuvent se connecter à distance, le groupe d'utilisateur qui est administrateur local du poste, si les utilisateurs ont le droit de modifier les paramètres IP de la machines,...).

En ce qui nous concerne, on a créé une OU : « pc-etu » où le groupe etu (composé de tous les comptes etux) devient administrateur local de toutes les machines membres de cette OU.

Déplacer votre machine du conteneur « computeurs » dans l'OU pc-etu. Redémarrer votre machine pour que la stratégie de groupes soit prise en compte.