Activité 10 – Services d'annuaire et domaine Active Directory

Propriétés	Description
Matière	SIO 1 – Bloc 2 – Administration systèmes et réseaux
Présentation	Création d'une machine virtuelle Hyper-V sur la machine hôte 2019 Serveur. Plan réseau IP Installation d'un service d'annuaire Active Directory et d'un service DHCP. Gestion des utilisateurs, des groupes et des unités d'organisation Gestion des droits d'accès et des stratégies de groupes
Savoirs	Installation et configuration de systèmes serveur, mise en production
Compétences	Analyser un besoin exprimé et son contexte juridique Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue Installer et configurer des éléments d'infrastructure Administrer sur site et à distance des éléments d'une infrastructure Automatiser des tâches d'administration
Transversalité	Bloc 1 & Bloc 2
Pré-requis	Bloc 1 & Bloc 2
Outils	Hyper-V, GPO
Mots-clés	Annuaire, virtualisation, habilitations, stratégie, environnement
Durée	5 x 2h
Auteur	Toanui MALINOWSKI
Version	v 1.21
Date de publication	11 août 2020
Dernière modification	20 avril 2022

Embauché récemment à la Direction des Systèmes d'Information de l'Université de Polynésie Française, vous êtes en charge de l'administration des serveurs qui permettent la gestion des habilitations et des accès sécurisés des utilisateurs et des machines clientes autorisées dans le SI (Système d'Information).

A. L'Université dans ses grandes lignes

La carte d'identité de l'UPF : l'UPF, créé le 31 mai 1999, est présidée aujourd'hui par le Professeur Patrick CAPOLSINI.

C'est un établissement public à caractère scientifique, culturel et professionnel qui compte environ 3.200 étudiants, 110 enseignants à temps plein, 280 vacataires et 107 personnels administratifs.

Ses missions principales sont :

- La **formation initiale et continue** au travers d'une gamme très diversifiée de diplômes d'État ou d'université.
- La **recherche scientifique et technique** ainsi que la valorisation de ses résultats :
  - Cinq laboratoires dont une unité mixte de recherche.
  - Contribution au développement scientifique et technologique en collaboration avec les organismes de recherche, l'État et la Polynésie française.
  - Participation à l'étude et à la mise en valeur des éléments du patrimoine polynésien.

http://www.upf.pf/fr/annuaire?title=&field_service_target_id=331

Service d'annuaire Active Directory

La gestion de nombreux utilisateurs, plus de 3.000 à l'UPF, nécessite l'utilisation d'outils adaptés tels qu'un annuaire utilisant le protocole LDAP (Lightweight Directory Access Protocol). Pour Windows, l'outil de référence est Service de Domaine Active Directory ou AD-DS en anglais, lui aussi basé sur le protocole LDAP. En effet **la création et la gestion d'un domaine permet de référencer l'ensemble des comptes utilisateurs, des comptes machines, les dossiers partagés, les imprimantes et d'en définir les habilitations**.

L'AD-DS permet de centraliser bien d'autres tâches d'administration système, comme la gestion des informations personnelles et des autorisations d'accès. Il permet également l'attribution et l'application de stratégies de groupe, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs.

Question 1 : Trouvez et proposez une explication de ce qu'est un contrôleur de domaine.
Question 2 : Active Directory introduit les notions de domaine, forêt, arborescence. Définissez ces termes.
Question 3 : Donnez trois exemples d'annuaire LDAP sur trois systèmes d'exploitation différents.

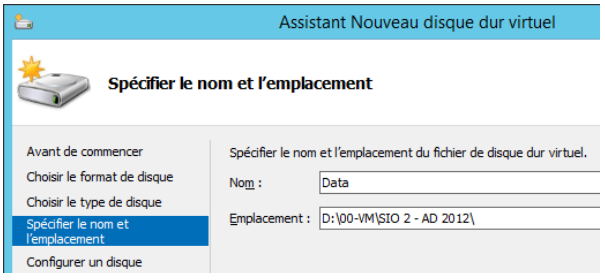
B. Installation des rôles et services nécessaires

A partir de la procédure simplifiée suivante, mettez en place votre serveur d'annuaire et serveur DNS. Pensez à faire des captures d'écran.

- Vous aurez besoin d'un « Commutateur interne » Hyper-V et le serveur sera un Win 2016.
- Le serveur doit avoir un nom de serveur explicite et une adresse IP fixe dans votre plage d'équipe. Il est préférable de réaliser ces opérations avant d'installer le rôle ADDS.
- Installer le rôle service DNS puis installer le rôle Active Directory DS (Domain Services).
- Une fois le rôle installé, il faut promouvoir le serveur en contrôleur de domaine. Le nom de domaine sera « upf.pf », le mot de passe P@ssW0rd, vous pouvez laisser les autres options par défaut.
- Ouvrez l'outil « Utilisateurs et ordinateurs Active Directory » et créez un utilisateur avec votre prénom, l'ajouter aux membres « d'administrateurs Admins du domaine ». Vérifier que votre compte fonctionne.
- Ajouter une machine Windows 7 dans le domaine, pour cela configurez son adresse IP :
    - Adresse IP fixe dans la plage (pas besoin de passerelle pour l'instant),
    - l'adresse du serveur DNS est celle du serveur AD-DS sur laquelle le service a été installé. C'est ce serveur qui sera contacté pour connaître le contrôleur du domaine upf.pf lorsque vous intégrerez la machine au domaine. Une erreur habituelle est d'oublier la configuration du DNS qui a pour résultat l'impossibilité de trouver le domaine.
- Vérifier que
    - Cette machine apparaît dans Computer de l'outil « utilisateurs et ordinateurs AD »
    - votre compte personnel peut ouvrir une session sur cette machine.

C. Gestion des habilitations et des ressources

Comme expliqué précédemment, le service d'annuaire doit permettre d'assurer une gestion centralisée des utilisateurs et des machines du SI. Dans la suite, vous allez mettre en place l'accès à des répertoires et fichiers partagés sur un deuxième disque connecté au serveur AD.



Commencez par ajouter un second disque à votre serveur, il sera stocké dans le même répertoire que le disque 1. On peut laisser la taille par défaut, 127 Go alloué dynamiquement.

Redémarrez le serveur et finaliser la configuration de ce nouveau disque E: en créant la partition nécessaire et en le formatant en NTFS (New Technology File System) puis créez le répertoire E:\Data.

La gestion des habilitations se fait habituellement à partir de la hiérarchie de l'organisation, on utilisera pour cela, l'organigramme général et l'organigramme détaillé de chaque service.

Question 4 : Active Directory dispose de deux outils importants qui sont les groupes (voir document *Groupes AD - Bonnes pratiques.pdf*) et les unités d'organisation. Citez deux rôles de chacun qui les différentient ?

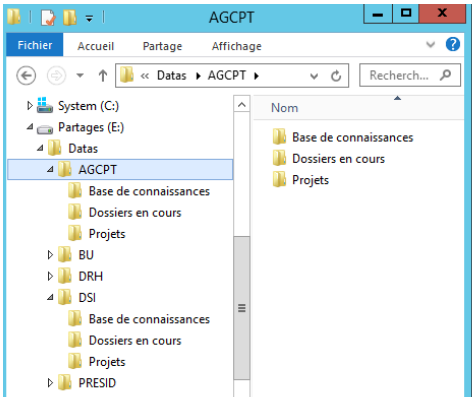
Vous disposez normalement d'un premier compte utilisateur que vous avez créé et qui est le vôtre. En utilisant l'annuaire de l'UPF et sachant que le « Nom d'ouverture de session » est composé de cette façon : Prénom.Nomfamille@upf.pf :

- Complétez, dans l'AD, les informations personnelles vous concernant en éditant les propriétés de votre compte. Vous êtes affecté à la DIRECTION DES SYSTÈMES D'INFORMATION (DSI), Pôle AMSI, Administrateur systèmes et réseaux, 40 866 947, prenom.nomfamille@upf.pf
- Créez 4 personnels de l'Agence comptable en intégrant le même type d'informations personnelles que pour vous. Vous trouverez ces informations dans l'annuaire et vous cocherez « le mot de passe n'expire jamais ».
- Créez le compte complet de Franck MEVEL, Directeur des SI (voir annuaire).
- Créez les **groupes globaux** grpe_DSI, grpe_AGCPT, grpe_Directions et affectez les utilisateurs au groupe qui convient. Franck MEVEL étant directeur sera aussi affecté à grpe_Directions.
- grpe_DSI sera membre de « Admins du domaine »
- Ajoutez les **groupes locaux de domaine** grpe_Data1_AGCPT_modif et grpe_Data1_AGCPT _lecture.

Ces deux types de groupes nous permettront de gérer les accès utilisateurs en suivant les bonnes pratiques décrites dans le document pdf (Extrait page 4 de *Groupes AD - Bonnes pratiques)*.

> ✔ ***Les groupes locaux de domaine*** *permettent de* ***gérer les autorisations des ressources****.*
>
> ✔ ***Les groupes globaux*** *servent principalement à* ***définir des collections d'objets*** *de domaine (utilisateurs, autres groupes globaux et ordinateurs)* ***en fonction des rôles métiers*** *[…] (par exemple, « RH » ou « Marketing »)*

L'arborescence des répertoires du lecteur partages est la suivante.

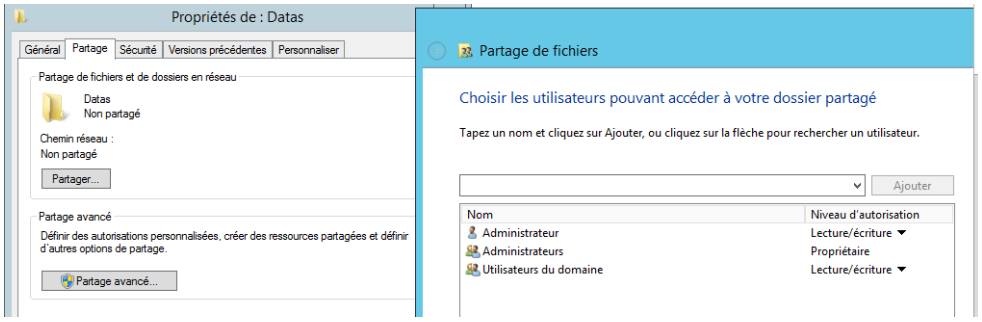


- ✔ On trouve un répertoire pour chaque direction
- ✔ Chaque direction dispose d'au moins 3 répertoires identiques
  - Base de connaissances en lecture seule pour les agents de l'UPF mais en modification pour les directions.
  - Dossier en cours en lecture écriture pour les agents du service uniquement.
  - Projets en lecture seule pour les agents du service mais en modification pour les directions.

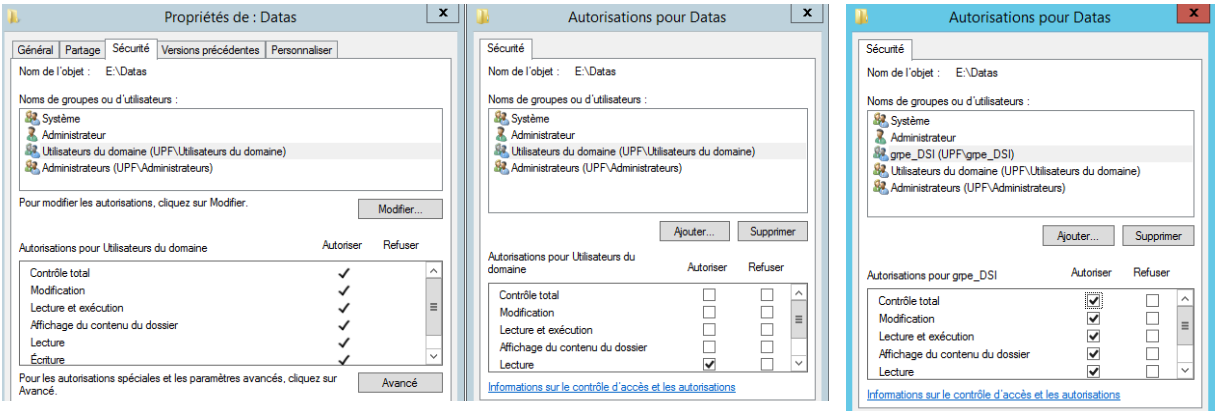
- Créez l'arborescence des répertoires tels qu'ils sont présentés dans l'illustration précédente.

Un clic droit sur le répertoire Datas permet d'accéder à ses propriétés de partage et de sécurité. Comme indiqué page 5 du document *Permissions NTFS - Bonnes pratiques.pdf* vous configurerez des droits de partage assez souples. C'est l'onglet sécurité qui va vous permettre d'affiner les droits d'accès.

- Commencez par partager le répertoire Datas avec les utilisateurs du domaine en lecture/écriture.



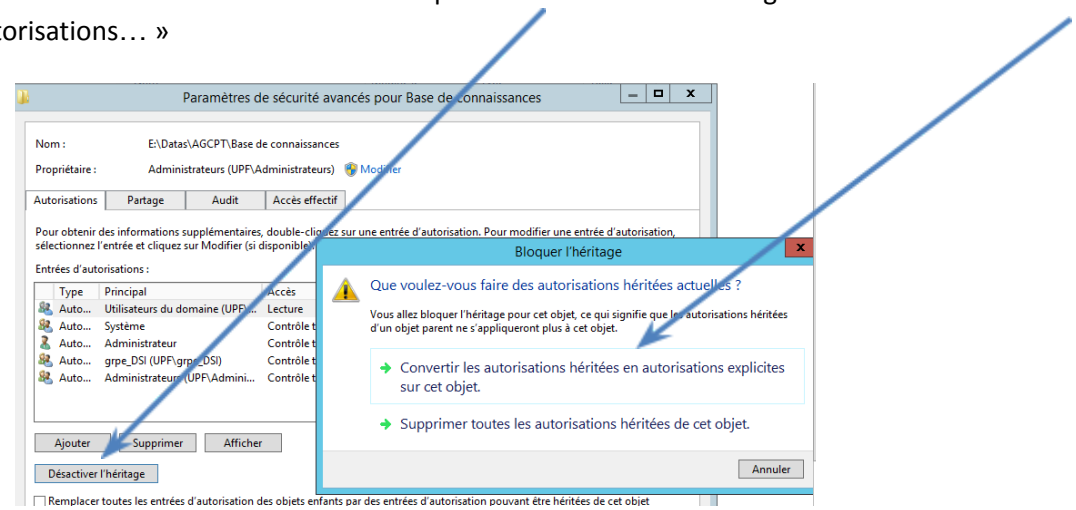
- Puis éditez les propriétés de sécurité et appliquez la règle 2 page 5, *« Veillez à ce que seul le service informatique puisse créer des dossiers au niveau racine. Ne laissez ni même les directeurs ni les cadres créer des dossiers aux deux premiers niveaux. »* Ici, les deux premiers niveaux sont les répertoires E:\Datas et E: \Datas\NomDeLaDirection. Restreignez les droits de sécurité des « utilisateurs du domaine » à la lecture uniquement. Ajoutez le contrôle total au groupe DSI.



Question 5 : Expliquer les différentes autorisations disponibles à partir de cette source ?

Vous remarquerez que les droits se sont propagés aux répertoires inclus dans Datas par le mécanisme d'héritage, les sous dossiers récupèrent les configurations de sécurité du dossier parent. Il devient alors impossible de les modifier sans « Désactiver l'héritage ».

Pour cela allez dans « Avancé » puis « Désactiver l'héritage » et enfin « Conserver les autorisations… »



Vous pouvez à présent personnaliser les autorisations telles que décrites page 3.

Question 6 : Est-il possible de conserver les autorisations que vous avez configurées des 3 dossiers de ACGPT si vous les copiez vers les autres dossiers des directions (BU, DRH, DSI) ?