Active directory : les bases

Cette fiche ARSI a pour objectif de présenter, de manière accessible, les principes fondamentaux de l'Active Directory (AD) et son rôle essentiel dans la gestion des ressources au sein des réseaux informatiques. À RTE, l'application Hyena est l'outil qui permet à la filière SI de visualiser l'AD.

1) Qu'est-ce que l'Active Directory ?

Active Directory (AD), développé par Microsoft, est un service essentiel pour centraliser la gestion des utilisateurs, des ressources (comme les ordinateurs ou imprimantes) et des droits d'accès au sein d'un réseau. Comparable à un annuaire numérique, il structure, organise et sécurise ces éléments clés.

Grâce à la gestion centralisée des identités (utilisateurs, mots de passe) et des accès (qui peut accéder à quoi), l'AD simplifie la supervision et améliore l'efficacité des administrateurs. Il leur permet de piloter l'ensemble du réseau de manière uniforme, depuis un point unique, réduisant ainsi la complexité de la maintenance.

Pour une entreprise comme RTE, avec plus de 10 000 collaborateurs, l'Active Directory devient un outil stratégique qui garantit, par exemple, que seuls les utilisateurs autorisés peuvent accéder à des documents sensibles, tels que des fichiers confidentiels.

2) Quelle est la structure d'un Active Directory (forêt, domaine, unité organisationnelle) ?

La structure de l'Active Directory est hiérarchique :

- Une **unité organisationnelle** (OU) est une subdivision d'un domaine utilisée pour organiser logiquement ces objets, comme par service ou département. Prenons l'exemple suivant : l'administrateur crée des OU comme **RH**, **IT** et **Marketing** pour organiser les utilisateurs et appliquer des stratégies spécifiques à chaque département, comme des restrictions de logiciel ou des politiques de mot de passe.

Par exemple, dans l'AD tertiaire de RTE, l'OU Ouest ou l'OU Rhone-Alpes-Auvergne.

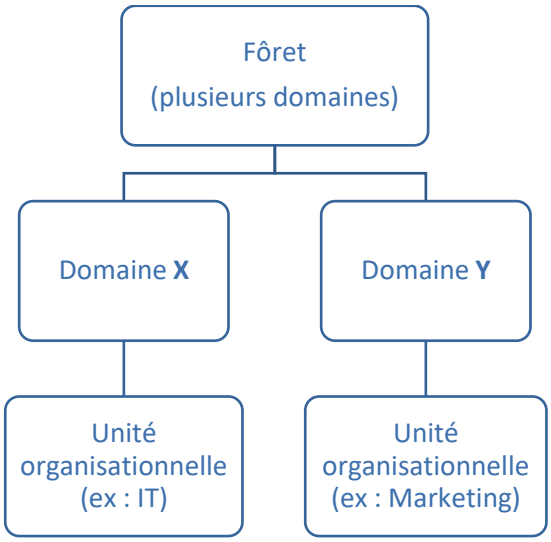
- Un **domaine** est une unité de base qui contient les utilisateurs, groupes et ressources gérés ensemble. Prenons l'exemple d'une entreprise nationale avec un domaine nommé **Z** : tous les employés, ordinateurs et imprimantes sont regroupés dans ce domaine (« **Z** »). Les règles, comme les mots de passe et permissions, sont définies de manière uniforme pour tout le domaine **Z**.

Par exemple, dans l'AD tertiaire de RTE, le domaine bureau et le domaine applis.

- Une **forêt** regroupe plusieurs domaines connectés et partageant le même schéma. Pour illustrer ces propos : chaque domaine peut avoir ses propres utilisateurs et stratégies locales, mais ils sont tous liés dans la même forêt. La relation de confiance permet, par exemple, qu'un employé du domaine **X**

puisse accéder à des ressources situées dans **Y**, à condition que les domaines appartiennent à la même forêt et que des autorisations spécifiques lui soient accordées pour accéder aux ressources du domaine **Y**.

La structure hiérarchique d'un Active Directory :



Forêt : niveau le plus élevé, elle englobe plusieurs domaines reliés par des relations de confiance et partageant un schéma commun.

Domaine : niveau intermédiaire, unité de gestion contenant utilisateurs, groupes et ressources avec des règles uniformes.

Unité Organisationnelle (OU) : niveau le plus bas, subdivisions logiques au sein d'un domaine, permettant d'organiser les objets selon des départements ou services précis avec leurs propres stratégies locales.

3) Groupe local/groupe global

a. Qu'est-ce qu'un groupe local/groupe global ?

Dans l'Active Directory, la gestion des permissions s'appuie sur deux types de groupes distincts mais complémentaires :

Le groupe local est limité à un domaine spécifique et a pour fonction principale d'attribuer des permissions précises à des ressources locales telles que des dossiers partagés, des imprimantes ou des fonctions d'administration spécifiques sur un serveur.

Le groupe global permet de regrouper des utilisateurs selon une fonction commune (comme l'appartenance à un même département ou une même équipe), ou selon leur situation géographique (par exemple, une même région). Ces groupes globaux peuvent inclure des utilisateurs provenant de plusieurs domaines d'une même forêt et facilitent ainsi l'attribution uniforme des droits d'accès.

À RTE, l'utilisation combinée de ces groupes simplifie significativement la gestion des ressources et des accès :

Lorsqu'un nouvel utilisateur rejoint l'entreprise, il est simplement ajouté au **groupe global** correspondant (selon son département ou sa région) via la création de son compte bureautique. Aucune autre action supplémentaire sur les serveurs locaux ou régionaux n'est nécessaire, ce qui simplifie considérablement les opérations quotidiennes.

Illustrations concrètes chez RTE :

Exemple du département RH :

Un dossier partagé nommé « Fiches de paie » doit être accessible uniquement aux employés du département RH. Pour cela, l'administrateur crée :

Un **groupe global** nommé « *RH-Local* », regroupant tous les utilisateurs RH du domaine **entreprise local**.

Un **groupe local** nommé « *RH_Local* », auquel des permissions spécifiques sur ce dossier sont attribuées. Le **groupe global** « RH-Local » est intégré au **groupe local** « *RH_Local* ».

Résultat : Seuls les membres de « *RH_Local »* peuvent consulter et modifier les fiches de paie.

Exemple d'une équipe informatique multi-sites :

Une équipe informatique comprenant des collaborateurs répartis entre Marseille (Massilia) et Lyon (Jonage) doit accéder à un serveur commun. Pour gérer efficacement les droits d'accès :

L'administrateur crée un **groupe global** nommé « *IT-Global* », incluant les techniciens des deux sites.

Un **groupe local** nommé « *ITcommun_local* » est créé pour accorder précisément les permissions d'accès au serveur commun. Le **groupe global** « *IT-Global* » est ensuite inclus dans ce **groupe local**.

Résultat : Les techniciens des bureaux de Marseille (Massilia) et de Lyon (Jonage) peuvent facilement collaborer et accéder au serveur central grâce à ce dispositif.

Principe d'attribution des droits :

Compte utilisateur -> Groupe global -> Groupe local -> Permissions sur les ressources.

C'est le principe de la règle AGLP qui décrit un chemin d'attribution des droits en suivant une logique d'entonnoir : on part d'un utilisateur (Account), qui est membre d'un groupe, lui-même inclus dans un groupe local auquel sont associées les permissions sur une ressource.

Account	Global Group	Local Group	Permission
Compte utilisateur	Groupe Global	Groupe Local	Permission

b. Reconnaitre un groupe local d'un groupe global sur Hyena ?

Pour différencier un groupe local d'un groupe global sur Hyena, vous pouvez vous référer aux icônes. En effet, les groupes globaux sont représentés par  tandis que les groupes locaux en ont un autre distinct  . Ces visuels vous permettront de les identifier rapidement. En théorie, les règles de nommage permettent également la différenciation :

- Les groupes globaux disposent d'un préfixe GG et de séparateurs de type « - »
- Les groupes locaux disposent d'un préfixe GL et de séparateur de type « _ »

Ces règles ne sont pas toujours respectées. Il n'est pas rare de voir des groupes créés sans respecter les préfixes « GG- » ou « GL_ », rendant leur identification difficile. Par exemple, des noms comme « RHlocal » ou « ITEquipe » ne permettent pas de distinguer clairement s'il s'agit d'un groupe local ou global. De plus, certains utilisateurs sont parfois ajoutés directement à des groupes locaux sans passer par un groupe global, en contradiction avec la logique AGLP.

c. Comment identifier quels groupes donnent l'accès à un répertoire ?

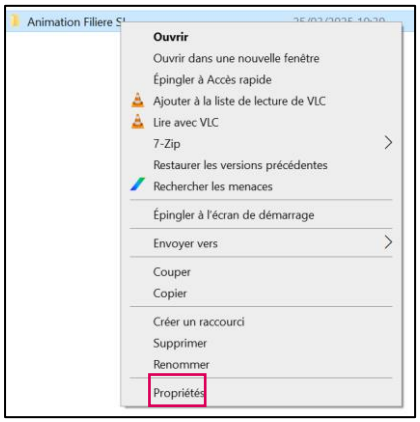
Pour connaître à quoi un groupe local ou global donne accès, il faut vérifier les listes de contrôle d'accès des dossiers. Ces listes définissent les actions que les membres de ces groupes peuvent effectuer, comme lire, modifier ou supprimer des éléments d'un dossier.

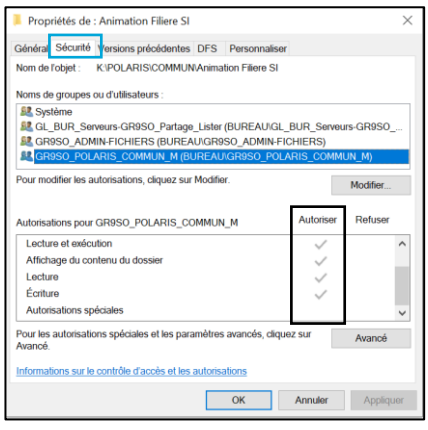
Illustration concrète chez RTE :

Une fois que l'on est sur le dossier où vous souhaitez vérifier la liste de contrôle :

1. Faites un clic droit sur le dossier, dans notre cas, « **Animation Filière SI** » ;
2. Cliquez sur « **Propriétés** » ;
3. Sélectionnez « **Sécurité** » ;
4. Vous avez désormais accès aux différents groupes ainsi qu'aux listes de contrôle d'accès de ces derniers, dans notre cas, « **GR9S0_POLARIS_COMMUN_M** ».

   Attention, cela ne fonctionne que si vous avez accès au répertoire en question (soit parce que vous avez les droits MOA SI sur le serveur, soit parce que vous avez effectivement les accès). Le cas échéant vous pouvez demander à un utilisateur ayant les droits d'accès de réaliser la manipulation.

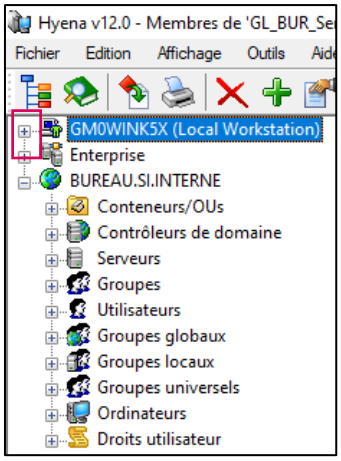


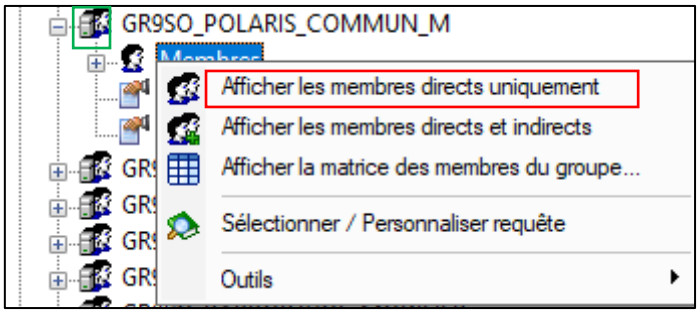


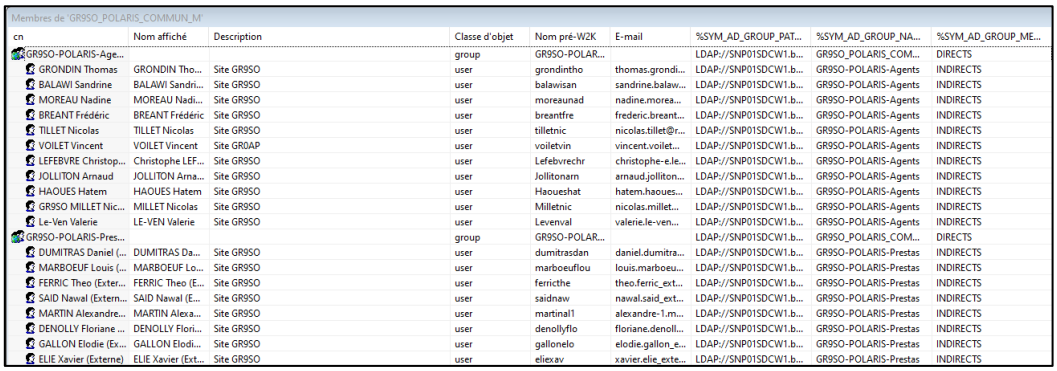
Pour connaitre le nom des utilisateurs qui composent ces groupes rendez vous sur Hyena :

1. Ouvrez les groupes locaux et globaux en question en cliquant sur le ;
2. Recherchez le nom du groupe dans notre exemple « **GR9SO_POLARIS_COMMUN_M** » puis cliquez sur le ;
3. Faites un clic droit sur « **Membres** » ;

4. Sélectionnez « **Afficher les membres directs et indirects** » ;
5. Vous avez désormais accès à la liste des membres qui composent le groupe que vous avez recherché.







Membres de 'GR9SO_POLARIS_COMMUN_M'

cn	Nom affiché	Description	Classe d'objet	Nom pré-W2K	E-mail	%SYM_AD_GROUP_PAT...	%SYM_AD_GROUP_NA...	%SYM_AD_GROUP_ME...
GR9SO-POLARIS-Age...			group	GR9SO-POLAR...		LDAP://SNP01SDCW1.b...	GR9SO_POLARIS_COM...	DIRECTS
GRONDIN Thomas	GRONDIN Tho...	Site GR9SO	user	grondintho	thomas.grondi...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
BALAWI Sandrine	BALAWI Sandri...	Site GR9SO	user	balawisan	sandrine.balaw...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
MOREAU Nadine	MOREAU Nadi...	Site GR9SO	user	moreaunad	nadine.morea...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
BREANT Frédéric	BREANT Frédéric	Site GR9SO	user	breantfre	frederic.breant...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
TILLET Nicolas	TILLET Nicolas	Site GR9SO	user	tilletnic	nicolas.tillet@r...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
VOILET Vincent	VOILET Vincent	Site GR0AP	user	voiletvin	vincent.voilet...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
LEFEBVRE Christop...	Christophe LEF...	Site GR9SO	user	Lefebvrechr	christophe-e.le...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
JOLLITON Arnaud	JOLLITON Arna...	Site GR9SO	user	Jollitonarn	arnaud.jolliton...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
HAOUES Hatem	HAOUES Hatem	Site GR9SO	user	Haoueshat	hatem.haoues...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
GR9SO MILLET Nic...	MILLET Nicolas	Site GR9SO	user	Milletnic	nicolas.millet...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
Le-Ven Valerie	LE-VEN Valerie	Site GR9SO	user	Levenval	valerie.le-ven...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Agents	INDIRECTS
GR9SO-POLARIS-Pres...			group	GR9SO-POLAR...		LDAP://SNP01SDCW1.b...	GR9SO_POLARIS_COM...	DIRECTS
DUMITRAS Daniel (...	DUMITRAS Da...	Site GR9SO	user	dumitrasdan	daniel.dumitra...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
MARBOEUF Louis (...	MARBOEUF Lo...	Site GR9SO	user	marboeuflou	louis.marboeu...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
FERRIC Theo (Exter...	FERRIC Theo (E...	Site GR9SO	user	ferricthe	theo.ferric_ext...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
SAID Nawal (Extern...	SAID Nawal (E...	Site GR9SO	user	saidnaw	nawal.said_ext...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
MARTIN Alexandre...	MARTIN Alexa...	Site GR9SO	user	martinal1	alexandre-1.m...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
DENOLLY Floriane ...	DENOLLY Flori...	Site GR9SO	user	denollyflo	floriane.denoll...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
GALLON Elodie (Ex...	GALLON Elodi...	Site GR9SO	user	gallonelo	elodie.gallon_e...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS
ELIE Xavier (Externe)	ELIE Xavier (Ext...	Site GR9SO	user	eliexav	xavier.elie_exte...	LDAP://SNP01SDCW1.b...	GR9SO-POLARIS-Prestas	INDIRECTS

4) Qu'est-ce qu'un compte utilisateur et un compte de service dans Active Directory ?

L'Active Directory distingue trois types de comptes essentiels pour gérer de manière sécurisée les accès aux ressources réseau : **les comptes utilisateurs**, **les comptes fonctionnels et les comptes de service**.

Compte utilisateur : Ce compte est nominatif et directement associé à une personne. Chez RTE, chaque utilisateur dispose d'un compte unique dans le domaine **bureau.si.interne**, lui permettant de se connecter à son poste de travail, accéder aux ressources réseau (documents partagés, applications, imprimantes, etc.) selon les autorisations qui lui sont attribuées. Ce compte contient des informations personnelles telles que le nom, l'email et le mot de passe. À l'arrivée d'un nouvel utilisateur, un compte est créé spécifiquement pour lui, puis supprimé à son départ afin de maintenir un niveau optimal de sécurité des accès.

Exemple concret : Martin, un employé de RTE, se connecte chaque jour à son réseau avec son identifiant personnel pour travailler sur ses dossiers et accéder aux ressources autorisées.

Compte fonctionnel : Ce type de compte est générique, non nominatif, et n'est pas associé à une personne physique. Il est utilisé pour accéder à des ressources partagées par une équipe ou un service, comme une boîte aux lettres fonctionnelle (BAL) ou un agenda utilisé collectivement.

Exemple concret : L'adresse mail rte-dsit-animation-filiere-si@rte-france.com est une BAL fonctionnelle consultée par plusieurs membres de l'équipe Animation Filière SI. Chacun peut lire et répondre aux messages en fonction de ses droits, sans que la BAL soit rattachée à une personne en particulier.

Pour effectuer une demande de dérogation concernant la création d'un compte fonctionnel cliquez ici.

Compte de service : Contrairement au compte utilisateur, le compte de service n'est pas lié à une personne physique mais à une application ou à un service automatisé. Il est utilisé pour sécuriser et automatiser l'exécution de tâches spécifiques sans nécessiter d'intervention humaine régulière.

Exemple concret : Un logiciel de sauvegarde automatique utilise un compte de service dédié afin d'accéder automatiquement, chaque nuit, aux données des serveurs pour les sauvegarder. Ceci garantit à la fois la sécurité et l'efficacité opérationnelle des processus informatiques automatisés.