Distribution EOLE - Demande #36440

Ajout de comptes "admin" spécifiques sur AD scribe et seth

14/02/2025 14:05 - Charles TOBAJAS

Statut:	Classée sans suite	**Début:**	14/02/2025
Priorité:	Normal	**Echéance:**	01/01/2026
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

Bonjour

L'objectif est une architecture full EOLE dans un établissement regroupant la zone pédago et la zone administrative dans le même AD avec 2 serveurs de fichiers bien isolés entre eux.
L'existant est un scribeAD dans la zone pédagogique alimenté automatiquement par l'AAF (personnels + élèves). Les personnels sont toutes les personnes de l'établissement, DIR, CPE, ENS, etc.

L'idée est de rajouter un seth

- avec le rôle ~~de contrôleur de domaine~~ membre du scribeAD qui est contrôleur principal
- et d'un partage de fichiers dans la zone administrative uniquement sur l'OU des postes et des machines administratifs de l'AD.

Le problème est le compte admin du scribeAD qui à un accès total à tout l'AD du scribe mais aussi aux partages associés à tous les utilisateurs (problème de confidentialité).

La demande est :

- La création de 2 comptes "admin" génériques, avec les droits d'accès restreints associés et spécifiques à chaque zone (pédago et administratif)
- Le compte administrator, admin et eole du scribeAD restent donc en possession uniquement des responsables du SI (collectivités)
- Les 2 comptes "admin" spécifiques avec des droits restreints à leurs zones respectives seraient donnés à des responsables locaux de chaque zones (chef et RUPN) pour la gestion au quotidien.

Merci par avance

Charles TOBAJAS
Référent collectivités
Région académique Occitanie

Historique

#1 - 01/03/2025 09:52 - Joël Cuissinat

- Tracker changé de Demande à Scénario

- Echéance mis à 01/01/2026

- Version cible mis à Carnet MENSR

#2 - 01/03/2025 10:19 - Joël Cuissinat

- Description mis à jour

Pour commencer, j'ajouterais une variable (exemple : Activer la gestion d'un serveur administratif) et certainement un onglet dédié.
Sur AmonEcole, la fonctionnalité devra être masquée (dans un premier temps en tout cas) et ne pas entraîner de régression ;)

Pré-requis

L'exploitant déploie, configure et joint au domaine AD du Scribe un Seth en mode membre sur lequel il active/ajoute les services de son choix (ex : MySQL).
L'exploitant fait en sorte que ce serveur ne soit pas accessible depuis le réseau pédagogique.
L'exploitant s'assure que le mot de passe de l'utilisateur admin n'est plus connu par les enseignants

Groupes et partages

Les répertoires personnels des personnels administratifs sont déclarés sur le serveur membre (FIXME : ajouter les variables nécessaires)
Cette information pourra être positionnée dans l'annuaire OpenLDAP (sambaHomePath) à la création de l'utilisateur et sera répliquée dans l'AD (homeDirectory) par LSC.
On utilisera prioritairement les groupes de type Service pour gérer les droits
Les partages de groupes seront gérés directement sur le serveur membre via les outils RSAT.
Certains pourront être standardisés (variante Zéphir) en les déclarant directement dans la configuration du Seth membre :
https://eole.ac-dijon.fr/documentations/2.9/completes/HTML/ModuleSeth/co/03_ActiveDirectory_Expert.html#rdN6ad

Utilisateurs spéciaux

- ajouter un utilisateur admin-pedago et adapter ses droits dans l'EAD/EOP (en "dur" dans le code si nécessaire) notamment pour :
  - qu'il ne puisse pas gérer les utilisateurs de type "personnel administratif"
  - qu'il ne puisse pas gérer les groupes de type "service administratif"
  - *(en gros des droits qui ressemblent à ceux d'un administrateur de classe qui aurait toutes les classes)*
- ajouter un utilisateur admin-??? et adapter ses droits dans l'EAD/EOP (en "dur" dans le code si nécessaire) notamment pour :
  - qu'il ne puisse gérer les utilisateurs de type "personnel administratif"
  - qu'il ne puisse gérer les groupes de type "service administratif"

FIXME : vérifier les autres interfaces / outils nécessaires

Arborescence AD

Les personnels administratifs devraient être placés dans une OU dédiée.
Une configuration spécifique pourrait être mise en place dans LSC mais le plus simple est d'utiliser eole-ad-dc-ou, avec une règle "objectClass=administratif" ou "membreDe=administratifs". C'est potentiellement déjà le cas dans la plupart des établissement d'Occitanie.

#3 - 02/06/2025 18:05 - Joël Cuissinat

Après discussion, nous n'avons pas le feu vert de la DNE pour travailler et promouvoir cette proposition d'architecture.
Cette problématique sera évoquée lors des J-SR.

#4 - 10/03/2026 15:00 - Joël Cuissinat

- Tracker changé de Scénario à Demande

- Statut changé de Nouveau à Classée sans suite

- Version cible Carnet MENSR supprimé