Script de purge des comptes ldap-remnants

Contexte

Voici la procédure utilisée à l'université de Lorraine, nous permettant de supprimer les comptes dans Nextcloud ne faisant plus parti de notre Système d'Information.
Ils sont identifiés comme étant des comptes ldap-remnants.

Avant tout, il est important que les données issues d'un partage soient conservées, pour laisser le temps au destinataire final de les récupérer, si nécessaire.

		Suppression du compte	Archive de l'espace	On informe	Commentaires
Un utilisateur n'est plus présent dans notre ldap					
1	s'il n'a effectué aucun partage s'il reçoit des partages	✅	✅	❌	• On crée l'archive ℹ️ Conservation de l'archive pendant 6 mois • On supprime le compte

2	s'il a effectué des partages	✅
		à J+30
			✅	✅
				On informe les destinataires des partages
					• On ajoute les infos récupérées dans un fichier de traitement
					• On désactive le compte
					• On informe les destinataires du partage pour qu'il sauvegarde les données si besoin
					  ◦ 1er mail : J-30
					  ◦ 2ième mail : J-15
					  ◦ Dernier mail : J-1
					• On crée l'archive
					ℹ️ Conservation de l'archive pendant 6 mois
					• On supprime le compte

Dans les cas ci-dessous, on notera "User 0" l'utilisateur dont le compte LDAP a été supprimé (compte ldap-remnant dans Nextcloud) et qu'il faut supprimer.

1er cas - User 0 n'a fait aucun partage

Cas simple, on fait une archive de ses données et on supprime son compte (l'archive sera conservée sur le serveur pendant un an).

```
# Création archive
cd ${DIR_DATA}/${USER}/files && zip -r ${DIR_SAVE}/${DATE}-${USER}.zip * && cd ${DIR}

# Suppression du compte
sudo -u apache /usr/bin/php ${DIR_BUL}/php/console.php user:delete ${USER}
```

2ème cas - User 0 a partagé des documents

User 0 a partagé son dossier **Mon_dossier** avec User 1 et User 2

- On écrit les infos récupérés dans un fichier

```
uid_owner;uid_initiator;share_with;file_target;date_remove
User0;User0;User1;/Mon_dossier;<date format timestamp>
```

- On informe les destinataires du partage pour qu'il sauvegarde les données

Exemple des mails envoyés

```
Sujet J-30 : Les partages de {uid_owner} vont disparaître de votre B'UL le {date_remove}
Sujet J-15 : Rappel : Les partages de {uid_owner} vont disparaître de votre B'UL le {date_remove}
Sujet J-1 : Dernier rappel : Les partages de {uid_owner} vont disparaître de votre B'UL le {date_remove}

Bonjour,

{uid_owner} n'étant plus dans notre établissement, son compte B'UL et les données associées vont être supprimés
le {date_remove}.

Voici la liste de ses documents auxquels vous avez accès :
- {file_target} partagé à : User 1, User 2.
- ...

Pour chaque élément, plusieurs possibilités s'offrent à vous :
- Si les documents ne vous sont plus utiles, il n'y a rien à faire, ils seront supprimés le {date_remove} (en
même temps que le compte de {uid_owner}).
- Si les documents nécessitent un espace collaboratif dédié, vous pouvez, en concertation avec votre groupe de
travail, en créer un via GEC (voir la documentation https://<url de la documentation>), et les y déplacer.
- Si les documents vous sont encore utiles, récupérez-les sur votre ordinateur ou dans votre espace personnel
B'UL en suivant cette documentation : https://<url de la documentation>.

Si vous ne souhaitez plus recevoir de mail de rappel, il est nécessaire de désactiver les partages listés ci-
dessus (voir la documentation : https://<url de la documentation>).

Si vous avez des questions, vous pouvez les adresser à <adresse_contact>@univ-lorraine.fr.

Bonne journée,
Cordialement,

----------------
L'équipe en charge de la B'UL
```

- Étape suivante (Jour J)

```
# Création archive
cd ${DIR_DATA}/${USER}/files && zip -r ${DIR_SAVE}/${DATE}-${USER}.zip * && cd ${DIR}

# Suppression du compte
sudo -u apache /usr/bin/php ${DIR_BUL}/php/console.php user:delete ${USER}
```

Déroulement

```
Scénario traitement compte LDAP_Remanent_BUL
-------------------------------------------

        - On liste des comptes 'ldap-remnants'
        - On vérifie pour chaque utilisateur, qu'il ne soit pas présent dans le fichier de traitement
"<nom_du_script>.txt"
                SI OUI
                        - On vérifie si l'utilisateur a des partages
                        SI OUI
                                - On alimente le fichier de traitement "<nom_du_script>.txt" avec les
informations récupérées de la BDD, date_remove est au format timestamps et valué à la date du jour +31 jours :
                                        uid_owner;uid_initiator;share_with;file_target;date_remove
                        SINON
                                - Création de l'archive : `cd ${DIR_DATA}/${USER}/files && zip -r ${DIR_SAVE}
/${DATE}-${USER}.zip * && cd ${DIR}`
                                - Suppression du compte 'ldap-remnants' : `sudo -u apache /usr/bin/php
${DIR_BUL}/php/console.php user:delete ${USER}`
                        FI
                SINON
                        - On vérifie la date de suppression du compte : $date_remove
                        Cas 1 (J-30)
                                - On vérifie dans le fichier "<nom_du_script>.txt", que $share_with n'est pas
vide
                                SI OUI
                                        - On construit le corps du mail en listant les partages et les
personnes ayant l'accès
                                        - On envoie le mail
                                SINON
                                        - On ne fait rien
                        Cas 1 (J-15)
                                - On vérifie dans le fichier "<nom_du_script>.txt", que $share_with n'est pas
vide
                                SI OUI
                                        - On construit le corps du mail en listant les partages et les
personnes ayant l'accès
                                        - On envoie le mail
                                SINON
                                        - On ne fait rien
                        Cas 2 (J-1)
                                - On vérifie dans le fichier "<nom_du_script>.txt", que $share_with n'est pas
vide
                                SI OUI
                                        - On construit le corps du mail en listant les partages et les
personnes ayant l'accès
                                        - On envoie le mail
                                SINON
                                        - On ne fait rien
                        Cas 3 (Jour J)
                                - Création de l'archive : `cd ${DIR_DATA}/${USER}/files && zip -r ${DIR_SAVE}
/${DATE}-${USER}.zip * && cd ${DIR}`
                                - Suppression du compte 'ldap-remnants' : `sudo -u apache /usr/bin/php
${DIR_BUL}/php/console.php user:delete ${USER}`
                                - Suppression de la ligne dans le fichier "<nom_du_script>.txt" : `sed -i "
/^${USER}/d" ${FILE_TRAITEMENT}`

                        - On vérifie la cohérence des partages entre la BDD et le fichier de traitement, ce qui
permettra aux personnes ayant désactiver le partage de ne plus recevoir de mail de rappel.
                        - On effectue un diff entre la requête SQL pour alimenter le fichier de traitement et
le fichier de traitement
                                SI il y a des (-) on supprime du fichier de traitement
                                SI il y a des (+) on ajoute au fichier de traitement en fin de fichier
                FI
        - On vérifie s'il existe des archives depuis plus de 6 mois, si c'est le cas, on supprime
                find ${DIR_SAVE}/*.zip -mtime +${JRS_SUPP} -delete
```

Sources

Description	Fichier
Fichier principal de traitement	bul-traitement_cpt_ldap_remnants.sh
Fichier des fonctions utilisées	functions.sh
Fichier de configuration LDAP	ldap-config

Contact

Pour toutes questions vous pouvez me contactez à mon adresse email : camille.herry@univ-lorraine.fr