

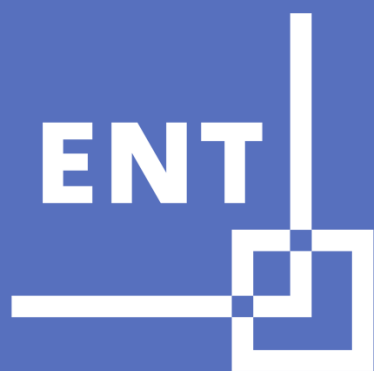


MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

*Liberté
Égalité
Fraternité*

SDET

Schéma Directeur des Espaces numériques
de Travail pour l'enseignement scolaire



Espace numérique de travail

Annexe opérationnelle - Ensemble annuaire
Annexe 5 : Exploitation et exploitabilité de l'annuaire ENT
version 6.5
Juin 2022

CC BY SA 3.0 F

Table des matières

1. Introduction	3
1.1. Objectif du document.....	3
1.2. Organisation du document	3
1.3. Niveaux de recommandation	4
2. Recommandations générales pour l'exploitation et l'exploitabilité de l'annuaire ENT	5
2.1. Gestion du système et procédures d'exploitation.....	6
2.1.1. Cahier d'exploitation	6
2.1.2. Gestion des traitements.....	6
2.1.3. Gestion des incidents	7
2.1.4. Gestion des fichiers journaux	7
2.1.5. Sauvegarde	7
2.1.6. Surveillance.....	8
2.1.7. Maintien en conditions opérationnelles.....	8
2.2. Disponibilité	8
2.3. Capacité et Performances	8
2.4. Sécurité	9
2.4.1. Accès à l'annuaire et à son contenu	9
2.4.2. Tests avant mise en production	9
3. Recommandations d'exploitation et d'exploitabilité spécifiques à certains services de l'annuaire ENT	10
3.1. Cas de l'accès à l'annuaire au travers de l'ENT	10
3.1.1. Disponibilité / gestion des incidents.....	11
3.1.2. Performances	11
3.2. Cas du chargement de fichiers.....	11
3.2.1. Recommandations générales pour le chargement de fichiers	12
3.2.2. Cas du chargement d'un fichier « complet »	13
3.2.3. Cas du chargement d'un fichier « delta »	14
3.2.4. Cas d'une alimentation « multi-annuaires ».....	15
3.3. Cas de la suppression d'un compte.....	15
4. Récapitulatif des exigences et recommandations	16

Table des illustrations et tableaux

Figure 1 : Niveaux de recommandation	4
Figure 2 : accès au référentiel annuaire depuis l'ENT	11
Figure 3 : Alimentation de l'annuaire par chargement de fichiers.....	12
Tableau 1 : récapitulatif des exigences et recommandations.....	20

1. Introduction

1.1. Objectif du document

Ce document fournit des recommandations pour l'exploitation et l'exploitabilité de l'annuaire des espaces numériques de travail (ENT).

Exploitation : action d'assurer la production d'un service. Ici, c'est assurer la mise à disposition et le bon fonctionnement de l'ensemble des traitements requis autour des processus d'annuaire ENT, dans le respect des exigences posées (disponibilité, capacité, performances, sécurité...).

Exploitabilité : caractère de ce qui est exploitable. Ici, c'est assurer que la solution comporte des procédures et des outils pour surveiller le respect des exigences et permettre la bonne exploitation du service annuaire ENT ainsi que son rétablissement en cas d'incident.

Il complète ainsi l'annexe 1bis (« Alimentation depuis le SI du MEN pour le premier degré ») et l'annexe 4 (« Alimentation depuis le SI du MEN et depuis d'autres SI externes pour le second degré ») de l'ensemble Annuaire du schéma directeur des ENT (SDET).

Il s'articule également avec le chapitre 3 « Stratégie d'exploitation » de l'annexe opérationnelle du SDET dont il reprend ou complète certaines recommandations en les appliquant au service annuaire.

1.2. Organisation du document

Le chapitre 2 formule des recommandations applicables de façon générale à l'ensemble des services de l'annuaire ENT.

Le chapitre 3 fournit des recommandations complémentaires spécifiques à certains services.

1.3. Niveaux de recommandation

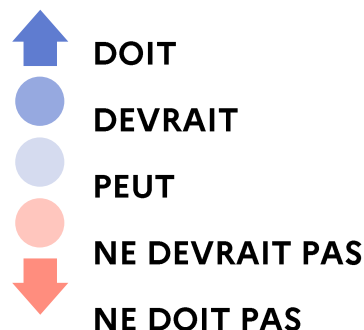


Figure 1 : Niveaux de recommandation

Comme dans le document principal et dans l'annexe opérationnelle, le niveau de recommandations formulé est exprimé en utilisant des termes issus de la terminologie RFC2119¹, notés en caractères gras et en majuscules dans le texte, dont la définition appliquée à ce document est la suivante :

- **DOIT** : ce mot signifie que la définition est une exigence absolue de la spécification (c'est-à-dire du présent document) ;
- **NE DOIT PAS** : cette expression signifie que la définition est une interdiction absolue de la spécification (c'est-à-dire du présent document) ;
- **DEVRAIT** : ce mot signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ne pas appliquer cette recommandation, mais les conséquences doivent être comprises et analysées soigneusement avant de choisir une autre option ;
- **NE DEVRAIT PAS** : cette expression signifie qu'il peut exister des raisons valables, dans des circonstances particulières, quand le comportement particulier est acceptable ou même utile, de ne pas suivre cette recommandation mais les conséquences doivent être comprises et le cas soigneusement pesé ;
- **PEUT** : ce mot exprime une suggestion ou proposition facultative.

¹ RFC 2119 (<https://www.ietf.org/rfc/rfc2119.txt>)

2. Recommandations générales pour l'exploitation et l'exploitabilité de l'annuaire ENT

Au-delà de la fonctionnalité offerte, le bon fonctionnement de l'annuaire ENT se mesure au respect des exigences posées pour les services attendus, que l'on peut décliner selon les axes suivants :

- gestion du système et procédures d'exploitation ;
- disponibilité ;
- capacité et performances ;
- sécurité ;
- contraintes fonctionnelles ;
- contraintes techniques.

Ces exigences sont à formuler selon des caractéristiques « SMART » : **S**pécifiques, **M**esurables, **A**tteignables, **R**éalistes, inscrites dans le **T**emps.

Elles doivent être validées et acceptées par tous les acteurs concernés : hébergeur/exploitant, éditeur/intégrateur, porteur de projet et support.

2.1. Gestion du système et procédures d'exploitation

2.1.1. Cahier d'exploitation

Préambule : se reporter au chapitre 3.4.4 « Livrables » du chapitre 3 « Stratégie d'exploitation » de l'annexe opérationnelle.

L'éditeur / intégrateur **DOIT** fournir à l'exploitant un dossier d'exploitation contenant l'ensemble des informations lui permettant d'assurer le service : processus à lancer, contraintes d'enchaînement, liste des commandes, codes erreur avec leur signification et les procédures à suivre pour les traiter, sondes et indicateurs disponibles, etc.

L'hébergeur / exploitant **DOIT** rédiger un cahier d'exploitation, décliné de celui de l'éditeur / intégrateur, adapté au contexte du projet, et intégrant les contraintes des différents acteurs.

Ce cahier d'exploitation de l'annuaire ENT indique les objectifs à atteindre, la surveillance mise en place, les procédures d'exploitation. Il traite de l'organisation mise en place, des procédures d'installation du service annuaire et de ses composants, du paramétrage des composants, il décrit les processus de gestion de l'annuaire et détaille la gestion des traitements, des changements, des incidents, des journaux.

2.1.2. Gestion des traitements

Pour l'annuaire ENT, les traitements suivants **DOIVENT** être décrits dans le cahier d'exploitation :

- démarrage de la solution ENT ;
- arrêt de la solution ENT ;
- surveillance de la solution ENT ;
- chargement de « complets »².

Pour l'annuaire ENT, les traitements suivants **DEVRAIENT** être décrits dans le cahier d'exploitation :

- arrêt / démarrage indépendant du service annuaire seul ;
- surveillance du service annuaire ;
- lancement d'un traitement particulier sans interruption de service ;
- chargement de « deltas » ;

² Le contenu des fichiers « complets » et « deltas » est décrit dans les annexes 1bis et 4 et rappelé au chapitre 3.2 de ce document.

- cohérence et intégrité de l'annuaire (comptes fantômes, comptes isolés, comptes en doublon, comptes anciens, groupes incomplets, groupes vides).

Pour l'annuaire ENT, les traitements suivants **PEUVENT** être décrits dans le cahier d'exploitation :

- démarrage du service annuaire avec reprise sur incident ;
- arrêt immédiat du service annuaire ;
- reprise d'un traitement interrompu volontairement ou non.

2.1.3. Gestion des incidents

Préambule : se reporter au chapitre 10.2.4.4. « Assistance utilisateur [SOC-SUP-ASU] » du document principal (Services Socle / Services Support).

L'ENT ne fonctionnant pas sans service annuaire, il faut porter une attention particulière à tout incident impactant ce service.

2.1.4. Gestion des fichiers journaux

Un journal des opérations effectuées sur l'annuaire, alimenté automatiquement par les traitements de mise à jour, et contenant au minimum les informations nécessaires au diagnostic pour chaque incident, **DOIT** être mis en place.

La liste des erreurs possibles **DOIT** être fournie par l'éditeur/intégrateur avec pour chacune une description, son identification et le plan d'actions pour la traiter.

Les messages enregistrés dans le journal pour les erreurs **DOIVENT** avoir été conçus avec un objectif d'exploitation (vs d'aide au développement), afin que l'hébergeur/exploitant puisse comprendre et agir en totale autonomie en ne se référant qu'au cahier d'exploitation et au journal.

La pertinence des erreurs relevées **DEVRAIT** permettre la création d'indicateurs.

Ce journal **DOIT** aussi être soumis à un cycle d'exploitation (compression, archivage, purge,...).

2.1.5. Sauvegarde

La limitation de perte de données exigée par le marché **DOIT** être couverte par un plan de sauvegarde.

2.1.6. Surveillance

Au-delà de la surveillance de la solution ENT qui est indispensable, une surveillance spécifique du service annuaire **DEVRAIT** être active :

- surveillance de la disponibilité (par exemple vérification de la présence du service, vérification régulière du bon fonctionnement via un scénario applicatif) ;
- surveillance des tâches d'exploitation (en particulier sauvegardes, chargement de « deltas » ou « complets »).

2.1.7. Maintien en conditions opérationnelles

Même après un arrêt de service non planifié, où le service doit être rétabli dans l'urgence, les conditions pré-requises au démarrage **DOIVENT** être vérifiées avant réouverture du service.

Chaque condition non remplie **DOIT** déclencher l'activation d'un plan d'action permettant de restaurer l'état souhaité.

2.2. Disponibilité

La solution ENT ne fonctionnant pas sans service annuaire, la disponibilité du service annuaire **DOIT** être au minimum celle de la solution exigée par le marché. Un niveau d'exigence spécifique **PEUT** être demandé.

Si une disponibilité 24x7 est exigée alors une plage de maintenance **DOIT** être accordée à l'hébergeur/exploitant.

Les techniques de haute disponibilité **PEUVENT** être envisagées pour l'annuaire (actif / passif, actif / actif).

2.3. Capacité et Performances

Les objectifs de performance **DOIVENT** être surveillés par l'intermédiaire d'indicateurs pertinents.

Ces indicateurs **PEUVENT** être communs avec ceux surveillant la disponibilité. Par exemple :

- lors de l'exécution régulière d'un scénario applicatif par outil, le temps de réponse peut être un indicateur de performance ;

- le nombre et le type de requêtes traitées par le service annuaire peuvent être des indicateurs de capacité.

La solution ENT et le modèle opérationnel **DEVRAIENT** être extensibles, c'est-à-dire adaptables en fonction des volumes et usages.

2.4. Sécurité

2.4.1. Accès à l'annuaire et à son contenu

Tout accès illégitime aux données annuaire **DOIT** être interdit.

Tout accès à l'annuaire **DOIT** être auditable (toutes les opérations doivent être tracées : connexions réussies ou échouées, démarrage, arrêt, ajout, modification, suppression...).

2.4.2. Tests avant mise en production

Des tests préalables sont nécessaires avant toute mise en production : se référer au chapitre 3.4.5 « Tests » de l'annexe opérationnelle du SDET.

Même s'il est nécessaire que les données utilisées pour ces tests soient représentatives, elles **NE DEVRAIENT PAS** être celles de production.

Si des données de production sont utilisées, les données **DOIVENT** :

- soit être protégées par les mêmes règles de sécurité qu'en production (de façon qu'un testeur ne puisse pas accéder à une donnée à laquelle il n'aurait pas le droit en production) ;
- soit être anonymisées.

3. Recommandations d'exploitation et d'exploitabilité spécifiques à certains services de l'annuaire ENT

3.1. Cas de l'accès à l'annuaire au travers de l'ENT

Comme illustré sur la Figure 2, la mise en œuvre des services de l'ENT par un utilisateur déclenche régulièrement des requêtes d'accès à l'annuaire ENT.

Il s'agit en général d'accès en consultation : identification / authentification, vérification d'autorisation suivant les profils / rôles ou appartenance aux groupes, gestion des accès aux services / contenus, consultation de fiches utilisateurs, consultation par l'administrateur de l'école ou de l'établissement, etc.

De façon plus rare³, il peut s'agir d'accès au référentiel annuaire pour mise à jour : création / mise à jour de groupes opérationnels, création manuelle de comptes utilisateurs, enrichissement des données issues de systèmes d'information externes, par exemple : mise à jour d'informations personnelles, etc.

³ Ces écritures via l'ENT sont peu fréquentes, elles représentent moins de 1/10 000 des requêtes reçues par le service annuaire

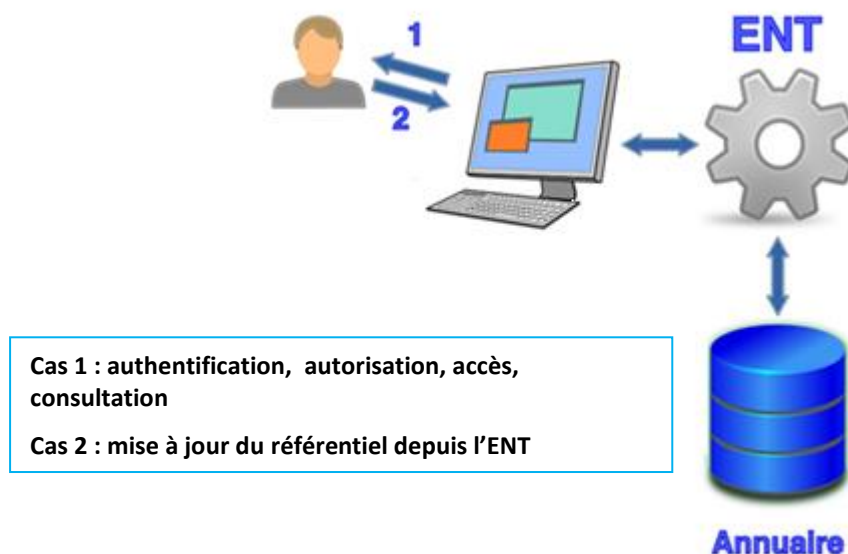


Figure 2 : accès au référentiel annuaire depuis l'ENT

3.1.1. Disponibilité / gestion des incidents

Toute erreur non applicative sur ces accès en lecture ou en écriture de l'annuaire **DOIT** être considérée comme critique par l'équipe d'exploitation, car elle est révélatrice d'une indisponibilité du service annuaire.

3.1.2. Performances

Les données accédées en lecture **PEUVENT** être mises en cache.

Si les données ont été mises en cache, les écritures **DOIVENT** invalider le cache.

3.2. Cas du chargement de fichiers

Préambule : se référer au chapitre 6.1.1 « Services d'alimentation » du cahier des charges de l'annuaire ENT pour le second degré, ainsi qu'à l'annexe 1bis et l'annexe 4 de l'ensemble annuaire.

Comme illustré en Figure 3, l'alimentation des comptes de l'annuaire ENT s'effectue généralement via le chargement de fichiers :

- fichiers issus de l'Annuaire académique fédérateur (AAF) fournis par le ministère en charge de l'Éducation nationale ou l'équivalent (SAPIA⁴) pour le ministère en charge de l'Agriculture (cf. cas 3 figure 3) ; ces fichiers sont fournis :
 - ▶ soit sous forme de « complets » contenant les données académiques du SI du MEN pour les personnes et les structures appartenant au périmètre du projet ENT concerné,
 - ▶ soit sous forme de « deltas » contenant tous les objets créés, modifiés ou supprimés pendant un nombre de jours donné ;
- fichiers en provenance d'autres sources externes, comme par exemple les comptes des agents de collectivités territoriales (cf. cas 2 et 4 figure 3).

Le chargement s'effectue via des traitements de masse déclenchés par l'hébergeur / exploitant. Selon les solutions ENT, il peut être également possible pour un administrateur ENT de l'école ou de l'établissement de charger un fichier de mise à jour depuis l'interface de l'ENT (traitement interactif, asynchrone ou traitement par lots).

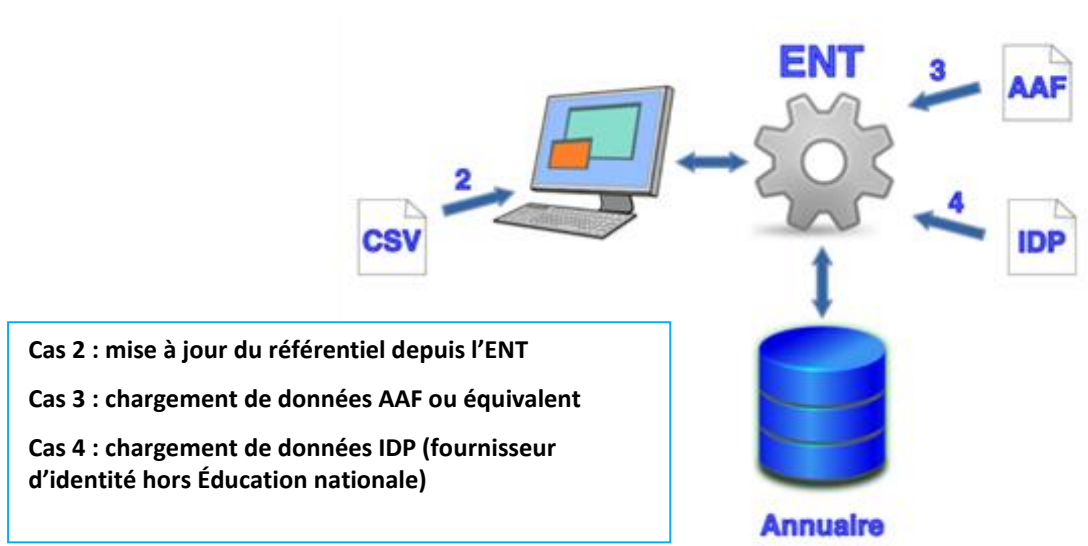


Figure 3 : Alimentation de l'annuaire par chargement de fichiers

3.2.1. Recommandations générales pour le chargement de fichiers

Un suivi du déroulement du traitement **DOIT** être fourni à l'utilisateur ou l'opérateur.

Des rapports « utilisateur » **DOIVENT** être générés (un rapport par école ou par établissement), à destination de l'administrateur propriétaire des données pour les imports AAF, ou les imports d'autres sources externes, ou de l'utilisateur ayant déclenché le traitement d'import depuis l'ENT.

Ces rapports « utilisateur » :

⁴ SAPIA (système d'authentification et propagation d'identités pour l'enseignement agricole)

- **DOIVENT** contenir l'information des requêtes n'ayant pas pu aboutir et les données nécessaires à la résolution ;
- **DEVRAIENT** contenir un bilan du chargement (nombre de requêtes exécutées par typologie et par statut).

Un rapport « exploitant » **DOIT** être généré par chaque chargement.

Ce rapport « exploitant » :

- **DOIT** contenir les données nécessaires aux diagnostics de tous les incidents rencontrés ;
- **DEVRAIT** contenir un bilan du chargement (nombre de requêtes exécutées par typologie et par statut) utilisable comme indicateur.

3.2.2. Cas du chargement d'un fichier « complet »

3.2.2.1. Disponibilité

Une sauvegarde des données **DEVRAIT** être ordonnancée avant le traitement de chargement d'un « complet » afin de permettre une restauration en cas de problèmes.

Chaque traitement **DEVRAIT** mettre à disposition des points de reprise intermédiaires pour respecter toutes les exigences d'exploitation. Une solution **PEUT** être le découpage en tâches unitaires.

Par exemple, la durée d'un traitement de chargement d'un « complet » peut s'avérer extrêmement longue et poser problème pour le respect des exigences de niveau de service requises pour le projet. Dans le cas où la perte de données maximale tolérée par le projet est inférieure, à 2 heures, aucune des tâches du chargement d'un « complet » ne devrait excéder ces 2 heures et le traitement devrait pouvoir être repris à partir de chacune de ces tâches.

Le chargement d'un fichier AAF complet (ou delta) **PEUT** être transactionnel, c'est-à-dire que la solution a la capacité de valider l'intégralité des modifications de données engendrées par ce chargement ou de les ignorer en cas d'incident ou d'interruption.

3.2.2.2. Performances

Afin d'optimiser la performance des composants et réduire les temps de traitement, en particulier dans le cas de LDAP, le traitement de chargement d'un « complet » **PEUT** être découpé selon les étapes :

- 1) analyse, vérification ;
- 2) préparation des mises à jour des données ;
- 3) exécution de ces mises à jour.

La première étape d'analyse et vérifications vise à écarter les anomalies qui mettraient en péril le bon déroulement du chargement. Les vérifications suivantes peuvent par exemple être effectuées :

- nomenclature de nommage ;
- vérification de la complétude des fichiers ;
- vérification syntaxique de tous les fichiers ;
- établissement d'un comptage des requêtes soumises ;
- vérification de ce comptage si la source de l'annuaire est en capacité de le fournir ;
- dans le cadre d'un chargement automatique, demande de confirmation si le comptage paraît anormal, par exemple si le nombre de requêtes des fichiers est très différent du nombre de comptes dans l'annuaire pour cette source ;
- éventuellement vérification de respect du calendrier.

La deuxième étape de préparation des mises à jour permet de limiter le nombre d'écritures en regroupant les mises à jour successives d'un même enregistrement. C'est une option efficace pour réduire le temps de traitement dans le cas d'un annuaire exploitant LDAP, ce protocole n'étant pas optimisé pour les écritures. Les mises à jour temporaires peuvent être stockées dans des tables temporaires (des tables si un SGBD est présent).

3.2.2.3. Sécurité

Le chargement d'un « complet » peut entraîner temporairement une perte de cohérence des données. Il peut également dégrader les performances des services en ligne de l'ENT accédant à l'annuaire. Pour ces raisons, le traitement d'import d'un « complet » **DEVRAIT** être planifié durant la plage de faible activité de la solution : plage de maintenance et / ou jour de plus faible activité (souvent le samedi).

L'éditeur / intégrateur **DEVRAIT** mettre à disposition de l'hébergeur / exploitant un outil de vérification et de correction de cohérence des données annuaires.

3.2.3. Cas du chargement d'un fichier « delta »

3.2.3.1. Disponibilité

Le chargement d'un « delta » **DEVRAIT** être quotidien sauf s'il est remplacé par un « complet ».

Le délai entre la réception et le chargement d'un « delta » **DEVRAIT** être réduit au minimum, afin que les modifications soient disponibles au plus vite dans l'ENT (dès le lendemain si possible).

3.2.3.2. Sécurité

Cependant, le chargement d'un « delta » **DEVRAIT** être planifié durant une plage de faible activité de la solution comme la plage de maintenance.

Le chargement d'un « complet » **DEVRAIT** être programmé occasionnellement, pour resynchroniser les données entre l'AAF et la solution ENT, et pallier à la non-complétude du traitement d'un « delta ».

3.2.4. Cas d'une alimentation « multi-annuaires »

Le chargement de l'annuaire ENT peut mettre en œuvre plusieurs annuaires source de type AAF, par exemple dans le cas :

- d'un projet ENT incluant un import premier degré et un import second degré ;
- d'un projet ENT recouvrant plusieurs académies ;
- d'un projet ENT mettant en œuvre un import de l'AAF et un import de l'enseignement agricole SAPIA.

Le traitement de chargement **DOIT** enregistrer dans son annuaire et incorporer dans ses identifiants la source d'alimentation correspondante à l'alimentation qu'il est en train d'effectuer, afin de :

- pouvoir gérer correctement les différentes sources d'alimentation ;
- séparer les identifiants identiques s'ils sont présents dans plusieurs sources ;
- savoir traiter les « suppressions » lors des chargements de « complets ».

3.3. Cas de la suppression d'un compte

Une requête de suppression de compte **DEVRAIT** avoir comme résultat de désactiver le compte tout en le conservant pendant une durée déterminée avant sa suppression réelle (la purge).

Cette désactivation **DEVRAIT** interdire pour cet utilisateur l'accès à l'ENT et à ses services.

Une exception à la règle précédente **DEVRAIT** permettre à l'utilisateur, si le projet l'accepte, de récupérer ses données personnelles.



Les données à caractère personnel traitées dans le cadre d'un compte ENT **DOIVENT** être supprimées de l'ENT dans un délai de 3 mois dès lors que la personne concernée n'a plus vocation à détenir un compte.

Remarque : pour les personnes ayant une légitimité à conserver leur compte pendant une période supérieure à 3 mois, les comptes désactivés depuis plus de trois mois **DOIVENT** être supprimés (purgés) lors de la procédure de changement d'année scolaire.



4. Récapitulatif des exigences et recommandations



Les recommandations sont récapitulées dans le Tableau 1 pour lequel, en regard de chaque préconisation, une lettre rappelle le niveau d'exigence applicable à l'enseignement du premier degré ou du second degré ; la signification de cette lettre est la suivante :

- la lettre « E » pour « exigé » correspond à une exigence de type « **DOIT** » ou « **NE DOIT PAS** » ;
- la lettre « R » pour « recommandé » correspond à une recommandation de type « **DEVRAIT** » ou « **NE DEVRAIT PAS** » ;
- la lettre « F » pour « facultatif » correspond à une préconisation optionnelle de type « **PEUT** ».

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 	Préconisation 2nd degré 
01	Gestion du système et procédures d'exploitation / cahier d'exploitation	L'éditeur/intégrateur DOIT fournir à l'exploitant un dossier d'exploitation contenant l'ensemble des informations lui permettant d'assurer le service : processus à lancer, contraintes d'enchaînement, liste des commandes, codes erreur avec leur signification et les procédures à suivre pour les traiter, sondes et indicateurs disponibles, etc.	E	E
02	Gestion du système et procédures d'exploitation / cahier d'exploitation	L'hébergeur/exploitant DOIT rédiger un cahier d'exploitation, décliné de celui de l'éditeur/intégrateur, adapté au contexte du projet, et intégrant les contraintes des différents acteurs.	E	E
03	Gestion du système et procédures d'exploitation / cahier d'exploitation	Pour l'annuaire ENT, les traitements suivants DOIVENT être décrits dans le cahier d'exploitation : <ul style="list-style-type: none"> ■ démarrage de la solution ENT ; ■ arrêt de la solution ENT ; ■ surveillance de la solution ENT ; ■ chargement de « complets » 	E	E

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 	Préconisation 2nd degré 
04	Gestion du système et procédures d'exploitation / cahier d'exploitation	Pour l'annuaire ENT, les traitements suivants DEVRAIENT être décrits dans le cahier d'exploitation : <ul style="list-style-type: none"> ■ arrêt / démarrage indépendant du service annuaire seul ; ■ surveillance du service annuaire ; ■ lancement d'un traitement particulier sans interruption de service ; ■ chargement de « deltas » ; ■ cohérence et intégrité de l'annuaire (comptes fantômes, comptes isolés, comptes en doublon, comptes anciens, groupes incomplets, groupes vides). 	R	R
05	Gestion du système et procédures d'exploitation / cahier d'exploitation	Pour l'annuaire ENT, les traitements suivants PEUVENT être décrits dans le cahier d'exploitation : <ul style="list-style-type: none"> ■ démarrage du service annuaire avec reprise sur incident ; ■ arrêt immédiat du service annuaire ; ■ reprise d'un traitement interrompu volontairement ou non. 	F	F
06	Gestion du système et procédures d'exploitation / fichiers journaux	Un journal des opérations effectuées sur l'annuaire, alimenté automatiquement par les traitements de mise à jour, et contenant au minimum les informations nécessaires au diagnostic pour chaque incident, DOIT être mis en place.	E	E
07	Gestion du système et procédures d'exploitation / fichiers journaux	La liste des erreurs possibles DOIT être fournie par l'éditeur / intégrateur avec pour chacune une description, son identification et le plan d'actions pour la traiter.	E	E
08	Gestion du système et procédures d'exploitation / fichiers journaux	Les messages enregistrés dans le journal pour les erreurs DOIVENT avoir été conçus avec un objectif d'exploitation (vs d'aide au développement).	E	E
09	Gestion du système et procédures d'exploitation / fichiers journaux	La pertinence des erreurs relevées DEVRAIT permettre la création d'indicateurs.	R	R
10	Gestion du système et procédures d'exploitation / fichiers journaux	Ce journal DOIT aussi être soumis à un cycle d'exploitation (compression, archivage, purge,...).	E	E
11	Gestion du système et procédures d'exploitation / sauvegarde	La limitation de perte de données exigée par le marché DOIT être couverte par un plan de sauvegarde.	E	E
12	Gestion du système et procédures d'exploitation / surveillance	Une surveillance spécifique du service annuaire DEVRAIT être active : <ul style="list-style-type: none"> ■ surveillance de la disponibilité ; ■ surveillance des tâches d'exploitation. 	R	R

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 	Préconisation 2nd degré 
13	Gestion du système et procédures d'exploitation / Maintien en conditions opérationnelles	Même après un arrêt de service non planifié, où le service doit être rétabli dans l'urgence, les conditions pré-requises au démarrage DOIVENT être vérifiées avant réouverture du service.	E	E
14	Gestion du système et procédures d'exploitation / Maintien en conditions opérationnelles	Chaque condition non remplie DOIT déclencher l'activation d'un plan d'action permettant de restaurer l'état souhaité	E	E
15	Disponibilité	La disponibilité du service annuaire DOIT être au minimum celle de la solution exigée par le marché pour la solution ENT.	E	E
16	Disponibilité	Un niveau d'exigence spécifique PEUT être demandé pour la disponibilité du service annuaire.	F	F
17	Disponibilité	Si une disponibilité 24x7 est exigée alors une plage de maintenance DOIT être accordée à l'hébergeur/exploitant.	E	E
18	Disponibilité	Les techniques de haute disponibilité PEUVENT être envisagées pour l'annuaire (actif / passif, actif / actif).	F	F
19	Capacité et Performances	Les objectifs de performance DOIVENT être surveillés par l'intermédiaire d'indicateurs pertinents.	E	E
20	Capacité et Performances	Ces indicateurs PEUVENT être communs avec ceux surveillant la disponibilité.	F	F
21	Capacité et Performances	La solution ENT et le modèle opérationnel DEVRAIENT être extensibles, c'est-à-dire adaptables en fonction des volumes et usages.	R	R
22	Sécurité	Tout accès illégitime aux données annuaire DOIT être interdit.	E	E
23	Sécurité	Tout accès à l'annuaire DOIT être auditable (toutes les opérations doivent être tracées : connexions réussies ou échouées, démarrage, arrêt, ajout, modification, suppression...).	E	E
24	Tests avant mise en production	Même s'il est nécessaire que les données utilisées pour ces tests soient représentatives, elles NE DEVRAIENT PAS être celles de production.	R	R
25	Tests avant mise en production	Si des données de production sont utilisées, les données DOIVENT : <ul style="list-style-type: none"> soit être protégées par les mêmes règles de sécurité qu'en production (de façon qu'un testeur ne puisse pas accéder à une donnée à laquelle il n'aurait pas le droit en production) ; soit être anonymisées. 	E	E
26	Gestion des incidents	Toute erreur non applicative sur les accès en lecture ou en écriture de l'annuaire DOIT être considérée comme critique par l'équipe d'exploitation, car elle est révélatrice d'une indisponibilité du service annuaire.	E	E
27	Performances	Les données accédées en lecture PEUVENT être mises en cache.	F	F

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 	Préconisation 2nd degré 
28	Performances	Si les données ont été mises en cache, les écritures DOIVENT invalider le cache.	E	E
29	Chargement de fichiers	Un suivi du déroulement du traitement DOIT être fourni à l'utilisateur ou l'opérateur.	E	E
30	Chargement de fichiers	Des rapports « utilisateur » DOIVENT être générés (un rapport par école ou par établissement), à destination de l'administrateur propriétaire des données pour les imports AAF, ou les imports d'autres sources externes, ou de l'utilisateur ayant déclenché le traitement d'import depuis l'ENT. Ils DOIVENT contenir l'information des requêtes n'ayant pas pu aboutir et les données nécessaires à la résolution.	E	E
31	Chargement de fichiers	Les rapports « utilisateur » DEVRAIENT contenir un bilan du chargement (nombre de requêtes exécutées par typologie et par statut).	R	R
32	Chargement de fichiers	Un rapport « exploitant » DOIT être généré par chaque chargement. Il DOIT contenir les données nécessaires aux diagnostics de tous les incidents rencontrés.	E	E
33	Chargement de fichiers	Le rapport « exploitant » DEVRAIT contenir un bilan du chargement (nombre de requêtes exécutées par typologie et par statut) utilisable comme indicateur.	R	R
34	Chargement d'un fichier « complet »	Une sauvegarde des données DEVRAIT être ordonnancée avant le traitement de chargement d'un « complet ».	R	R
35	Chargement d'un fichier « complet »	Chaque traitement DEVRAIT mettre à disposition des points de reprise intermédiaires pour respecter toutes les exigences d'exploitation.	R	R
36	Chargement d'un fichier « complet »	Une solution pour la mise à disposition de points de reprise intermédiaire PEUT être trouvée dans le découpage en tâches unitaires.	F	F
37	Chargement d'un fichier	Le chargement d'un fichier AAF complet (ou delta) PEUT être transactionnel.	F	F
38	Chargement d'un fichier « complet »	Afin d'optimiser la performance des composants et réduire les temps de traitement, en particulier dans le cas de LDAP, le traitement de chargement d'un « complet » PEUT être découpé selon les étapes : <ul style="list-style-type: none"> ■ analyse, vérification ; ■ préparation des mises à jour des données ; ■ exécution de ces mises à jour. 	F	F
39	Chargement d'un fichier « complet »	Le traitement d'import d'un « complet » DEVRAIT être planifié durant la plage de faible activité de la solution.	R	R
40	Chargement d'un fichier « delta »	Le chargement d'un « delta » DEVRAIT être quotidien sauf s'il est remplacé par un « complet ».	R	R
41	Chargement d'un fichier « delta »	Le délai entre la réception et le chargement d'un « delta » DEVRAIT être réduit au minimum, afin que les modifications soient disponibles au plus vite dans l'ENT (dès le lendemain si possible).	R	R
42	Chargement d'un fichier « delta »	le chargement d'un « delta » DEVRAIT être planifié durant une plage de faible activité de la solution comme la plage de maintenance.	R	R

Référence	Fonctions / Thèmes	Fonctionnalités / règles de gestion	Préconisation 1er degré 	Préconisation 2nd degré 
43	Chargement de fichiers	Le chargement d'un « complet » DEVRAIT être programmé occasionnellement, pour resynchroniser les données entre l'AAF et la solution ENT, et pallier à la non-complétude du traitement d'un « delta ».	R	R
44	Alimentation « multi-annuaires »	Dans le cas d'une alimentation par de multiples annuaires source de type AAF, le traitement de chargement DOIT enregistrer dans son annuaire et incorporer dans ses identifiants la source d'alimentation correspondante à l'alimentation qu'il est en train d'effectuer	E	E
45	Suppression d'un compte	Une requête de suppression de compte DEVRAIT avoir comme résultat de désactiver le compte tout en le conservant pendant une durée déterminée avant sa suppression réelle (la purge).	R	R
46	Suppression d'un compte	Cette désactivation DEVRAIT interdire pour cet utilisateur l'accès à l'ENT et à ses services.	R	R
47	Suppression d'un compte	Une exception à la règle précédente DEVRAIT permettre à l'utilisateur, si le projet l'accepte, de récupérer ses données personnelles.	R	R
48	Suppression d'un compte	Les données à caractère personnel traitées dans le cadre d'un compte ENT DOIVENT être « supprimées de l'ENT dans un délai de 3 mois dès lors que la personne concernée n'a plus vocation à détenir un compte »). Pour les personnes ayant une légitimité à conserver leur compte pendant une période supérieure à 3 mois, les comptes désactivés depuis plus de trois mois DOIVENT être supprimés (purgés) lors de la procédure de changement d'année scolaire.	E	E

Tableau 1 : récapitulatif des exigences et recommandations