

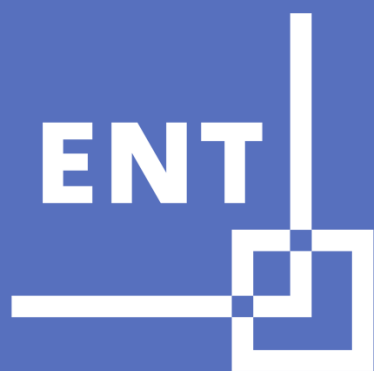


MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

*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 6.6
Juillet 2023

CC BY SA 3.0 F

Table des matières

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

Table des illustrations

| | |
|---|----|
| Figure 1 : accès au référentiel annuaire depuis l'ENT | 10 |
| Figure 2 : Alimentation de l'annuaire par chargement de fichiers..... | 11 |

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.

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 [GSP]

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.

- **GSP-01** : L'éditeur / intégrateur fournit 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.
- **GSP-02** : L'hébergeur / exploitant rédige 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

- **GSP-03** : Pour l'annuaire ENT, les traitements suivants sont décrits dans le cahier d'exploitation :
 - ▶ démarrage de la solution ENT ;
 - ▶ arrêt de la solution ENT ;
 - ▶ surveillance de la solution ENT ;
 - ▶ chargement de « complets »¹.
- **GSP-04** : Pour l'annuaire ENT, les traitements suivants sont 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 » ;

¹ 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).

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

- **GSP-05** : traitements de mise à jour, et contenant au minimum les informations nécessaires au diagnostic pour chaque incident, est mis en place.
- **GSP-06** : La liste des erreurs possibles est fournie par l'éditeur/intégrateur avec pour chacune une description, son identification et le plan d'actions pour la traiter.
- **GSP-07** : Les messages enregistrés dans le journal pour les erreurs ont 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.
- **GSP-08** : La pertinence des erreurs relevées permet la création d'indicateurs.
- **GSP-09** : Ce journal est soumis à un cycle d'exploitation (compression, archivage, purge,...).

2.1.5. Sauvegarde

- **GSP-10** : La limitation de perte de données exigée par le marché est couverte par un plan de sauvegarde.

2.1.6. Surveillance

- **GSP-11** : Au-delà de la surveillance de la solution ENT qui est indispensable, une surveillance spécifique du service annuaire est 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

- **GSP-12** : Même après un arrêt de service non planifié, où le service doit être rétabli dans l'urgence, les conditions pré-requises au démarrage sont vérifiées avant réouverture du service.
- **GSP-13** : Chaque condition non remplie déclenche l'activation d'un plan d'action permettant de restaurer l'état souhaité.

2.2. Disponibilité [DIS]

- **DIS-01** : La solution ENT ne fonctionnant pas sans service annuaire, la disponibilité du service annuaire est au minimum celle de la solution exigée par le marché.
- **DIS-02** : Si une disponibilité 24x7 est exigée alors une plage de maintenance est accordée à l'hébergeur/exploitant.

2.3. Capacité et Performances [CAP]

- **CAP-01** : Les objectifs de performance sont surveillés par l'intermédiaire d'indicateurs pertinents.
- **CAP-02** : La solution ENT et le modèle opérationnel sont extensibles, c'est-à-dire adaptables en fonction des volumes et usages.

2.4. Sécurité [SEC]

2.4.1. Accès à l'annuaire et à son contenu

- **SEC-01** : Tout accès illégitime aux données annuaire est interdit.
- **SEC-02** : Tout accès à l'annuaire est 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.

- **SEC-03 :** Même s'il est nécessaire que les données utilisées pour ces tests soient représentatives, elles ne sont pas celles de production.
- **SEC-04 :** Si des données de production sont utilisées, les données sont :
 - ▶ soit 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 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 [AAE]

Comme illustré sur la Figure 1, 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 rare², 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.

² Ces écritures via l'ENT sont peu fréquentes, elles représentent moins de 1/10 000 des requêtes reçues par le service annuaire

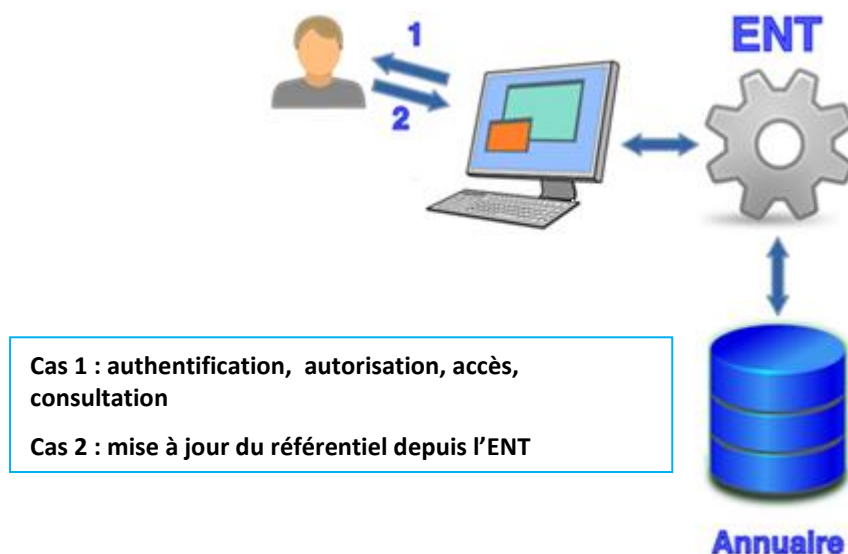


Figure 1 : accès au référentiel annuaire depuis l'ENT

3.1.1. Disponibilité / gestion des incidents

- **AAE-01** : Toute erreur non applicative sur ces accès en lecture ou en écriture de l'annuaire est considérée comme critique par l'équipe d'exploitation, car elle est révélatrice d'une indisponibilité du service annuaire.

3.1.2. Performances

- **AAE-02** : Si les données ont été mises en cache, les écritures invalident le cache.

3.2. Cas du chargement de fichiers [CHF]

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 2, 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 (SAPIA³) 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).

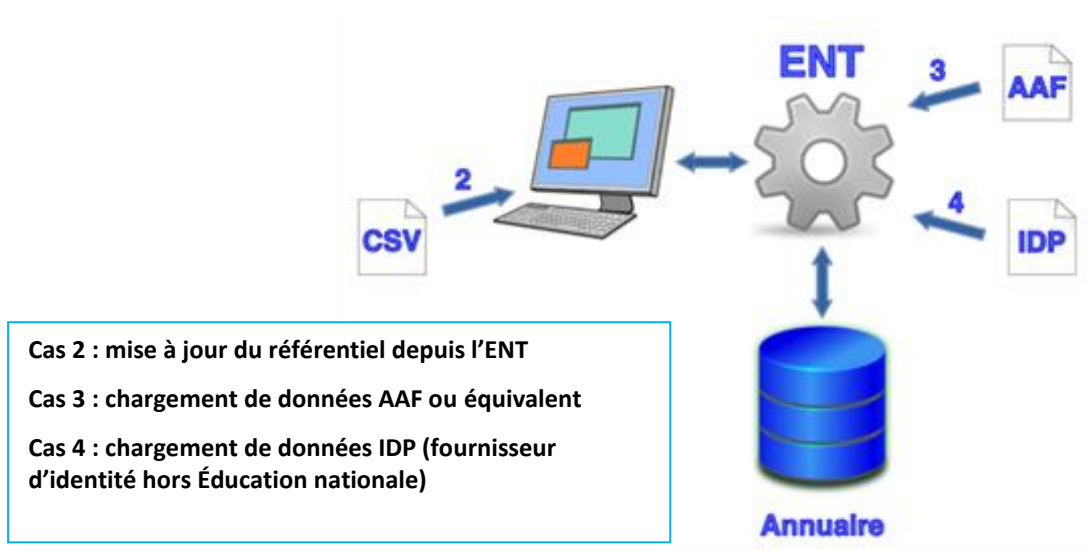


Figure 2 : Alimentation de l'annuaire par chargement de fichiers

3.2.1. Recommandations générales pour le chargement de fichiers

- **CHF-01** : Un suivi du déroulement du traitement est fourni à l'utilisateur ou l'opérateur.
- **CHF-02** : Des rapports « utilisateur » sont 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 » :

³ SAPIA (système d'authentification et propagation d'identités pour l'enseignement agricole)

- contiennent l'information des requêtes n'ayant pas pu aboutir et les données nécessaires à la résolution ;
- contiennent un bilan du chargement (nombre de requêtes exécutées par typologie et par statut).
- **CHF-03** : Un rapport « exploitant » est généré par chaque chargement.

Ce rapport « exploitant » :

- contient les données nécessaires aux diagnostics de tous les incidents rencontrés ;
- contient 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

- **CHF-04** : Une sauvegarde des données est ordonnancée avant le traitement de chargement d'un « complet » afin de permettre une restauration en cas de problèmes.
- **CHF-05** : Chaque traitement met à disposition des points de reprise intermédiaires pour respecter toutes les exigences d'exploitation.

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

- **CHF-06** : 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 » est planifié durant la plage de faible activité de la solution : plage de maintenance et / ou jour de plus faible activité (souvent le samedi).
- **CHF-07** : L'éditeur / intégrateur met 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

- **CHF-08** : Le chargement d'un « delta » est quotidien sauf s'il est remplacé par un « complet ».
- **CHF-09** : Le délai entre la réception et le chargement d'un « delta » est 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

- **CHF-10** : Cependant, le chargement d'un « delta » est planifié durant une plage de faible activité de la solution comme la plage de maintenance.
- **CHF-11** : Le chargement d'un « complet » est programmé occasionnellement, pour resynchroniser les données entre l'AAF et la solution ENT, et pallier 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.
- **CHF-12** : Le traitement de chargement enregistre dans son annuaire et incorpore 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 [CSC]

- **CSC-01** : Une requête de suppression de compte a comme résultat de désactiver le compte tout en le conservant pendant une durée déterminée avant sa suppression réelle (la purge).
- **CSC-02** : Cette désactivation interdit pour cet utilisateur l'accès à l'ENT et à ses services.
- **CSC-03** : Une exception à la règle précédente permet à l'utilisateur, si le projet l'accepte, de récupérer ses données personnelles.
- **CSC-04** : Les données à caractère personnel traitées dans le cadre d'un compte ENT sont 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 sont supprimés (purgés) lors de la procédure de changement d'année scolaire.