Calcul des droits des utilisateurs Allegro

Historique des révisions

|  |  |  |  |
| --- | --- | --- | --- |
| **Révision** | **Date** | **Modifications** | **Auteurs** |
| 1.3 | 10-06-2013 | Version initiale répondant à la demande Mantis [15955](https://forge.ifremer.fr/mantis/view.php?id=15955) | Benoit Lavenier, Lionel Touseau |
| 1.4 | 30-09-2013 | Document complété suite aux demandes d'Ifremer/CLS.  Terminologie, descriptions plus exhaustives des privilèges, intégration d'éléments issus de l'analyse des droits menée par M. Bourbigot.  Suppression de la gestion manuelle des privilèges de supervision et déplacement de la partie concernant l'outil d'administration dans le document de spécifications global de l'outil.  Détail des règles mises en œuvre dans la fonction de remplissage des droits F\_FILL\_PERSON\_SESSION | Lionel Touseau, Matthieu Bourbigot (CLS) |
| 1.5 | 01-10-2013 | Mise en page | Lionel Touseau |
| 1.6 | 29-11-2013 | Prise en compte des retours de S. Bocande et M. Bourbigot.  Disparition du terme « supervision ».  Changement des libellés des types de privilèges.  Déplacement de la procédure d’exploitation en annexe.  Clarifications diverses.  Modèle de données en annexe. | Lionel Touseau, Matthieu Bourbigot (CLS), Stéphane Bocande |
| 1.7 | 28-02-2014 | Duplication automatique de droits | Lionel Touseau |
| 1.8 | 21/10/2014 | Evolution du privilège « Gestion des programmes/stratégies ». Le privilège permet la modification d’une stratégie | Matthieu Bourbigot (CLS) |

Table des matières

[1 Terminologie 5](#_Toc381365250)

[1.1 Droits 5](#_Toc381365251)

[1.2 Privilèges 5](#_Toc381365252)

[1.3 Profils (Allegro) 5](#_Toc381365253)

[1.4 Valideur d’une société prestataire 6](#_Toc381365254)

[1.5 Valideur Ifremer 6](#_Toc381365255)

[1.6 Superviseur 6](#_Toc381365256)

[2 Privilèges 7](#_Toc381365257)

[2.1 Description des différents privilèges 7](#_Toc381365258)

[2.1.1 Gestion des programmes/stratégies 7](#_Toc381365259)

[2.1.2 Saisie 7](#_Toc381365260)

[2.1.3 Consultation 8](#_Toc381365261)

[2.1.4 Validation 8](#_Toc381365262)

[2.1.5 Qualification 9](#_Toc381365263)

[2.2 Privilèges des services 9](#_Toc381365264)

[2.3 Note sur le processus de validation/qualification des données dans Allegro 10](#_Toc381365265)

[2.4 Tableau récapitulatif 11](#_Toc381365266)

[2.5 Duplication automatique de privilèges 11](#_Toc381365267)

[3 Fonction de remplissage des droits depuis les privilèges par programme 12](#_Toc381365268)

[3.1 Paramètres et constantes d'exploitation 13](#_Toc381365269)

[3.1.1 Paramètres 13](#_Toc381365270)

[3.1.2 Constantes d’exploitation 13](#_Toc381365271)

[3.2 Règles mises en œuvre pour le remplissage des droits 14](#_Toc381365272)

[3.2.1 Privilèges sur des personnes 16](#_Toc381365273)

[3.2.2 Privilèges par lieu(x) 16](#_Toc381365274)

[3.2.3 Héritage du droit des services 17](#_Toc381365275)

[3.2.4 Règles de correspondances périodes d'immatriculations – périodes d'ouverture de droits 17](#_Toc381365276)

[3.2.5 Cas des portefeuilles volumineux 19](#_Toc381365277)

[4 Annexes 20](#_Toc381365278)

[4.1 Modèle de données de l’ancienne gestion des droits par portefeuilles de navires 20](#_Toc381365279)

[4.2 Modèle de données de la nouvelle gestion des droits 21](#_Toc381365280)

[4.3 Modèle de données des droits Allegro 22](#_Toc381365281)

[4.4 Procédure de migration des portefeuilles de navires (pour l'équipe d'exploitation) 22](#_Toc381365282)

[4.4.1 SIH-OBSMER, SIH-OBSVENTE et CAM-CGFS 23](#_Toc381365283)

[4.4.2 SIH-ACTIPRED, SIH-ACTIFLOT 23](#_Toc381365284)

[4.4.3 Cas des superviseurs pour les calendriers d'activité 25](#_Toc381365285)

# Terminologie

## Droits

Il s'agit simplement des droits d'accès aux données (lecture, écriture, validation).

Dans le SIH (et donc dans Allegro) les droits fonctionnent par navire, périodes et types de données (ex : données de calendriers d’activités, données d’observations, …). Ainsi un utilisateur peut avoir des droits de lecture sur les données d'un navire qui concernent ses calendriers d'activité, et ceci sur les 3 dernières années.

## Privilèges

A la différence des droits qui concernent directement des données, les privilèges sont accordés par programme de collecte.

Le privilège définit également les opérations possibles sur la donnée d'un programme : lecture seule, écriture, validation, qualification, ...

## Profils (Allegro)

Un profil donne l’accès à des fonctionnalités supplémentaires dans le logiciel Allegro telles que l’accès à certains écrans, à des champs de saisie, etc. Un profil ne permet pas de gérer l’accès aux données (marées, ventes, calendriers …) en dehors des référentiels.

Les trois profils principaux sont :

* ALLEGRO\_UTILISATEUR (anciennement SIH\_ROBS)
* ALLEGRO\_SUPER\_UTILISATEUR (anciennement SIH\_PROJET)
* ALLEGRO\_ADMINISTRATEUR (anciennement SIH\_ADM)

Le tableau ci-dessous dresse un récapitulatif des profils.

|  |  |
| --- | --- |
| **PROFIL** | **Fonctionnalités accessibles au profil** |
| **ALLEGRO\_ADMINISTRATEUR** | \* Administration des référentiels engins et types d'engin (création/modification/suppression)  \* Administration de tous les programmes (création/modification/suppression) \* Administration de toutes les stratégies (création/modification/suppression) |
| **ALLEGRO\_UTILISATEUR** | Ce profil est considéré comme le profil par défaut dans Allegro  \* Accès en lecture aux référentiels (taxons, lieux, métiers engins, psfm …)  \* Accès en lecture aux programmes/stratégies  \* Accès en lecture aux modèles d’arbre d’échantillonnage  \* Accès aux données selon les privilèges de l’utilisateur |
| **ALLEGRO\_SUPER\_UTILISATEUR** | Ce profil accède aux mêmes fonctionnalités que « ALLEGRO\_UTILISATEUR», plus les fonctionnalités supplémentaires suivantes :  \* Validation Ifremer des marées et des ventes \* Synchronisation des données d'historique \* Consultation de toutes les références au plan d'échantillonnage (pas de filtre selon la société d'appartenance) |

## Valideur d’une société prestataire

Il s’agit de la personne en charge de la validation des données saisies par les saisisseurs de la société prestataire (Privilège « validation » et Profil "SIH\_UTILISATEUR"), nommés « Superviseur » dans l’ancienne terminologie.

Cf §.2.3- Note sur le processus de validation/qualification des données dans Allegro

## Valideur Ifremer

Il s’agit de la personne en charge de la validation Ifremer des données (Privilège « validation » - Profil " ALLEGRO\_SUPER\_UTILISATEUR ").

Cf §.2.3- Note sur le processus de validation/qualification des données dans Allegro

## Superviseur

Cette terminologie était utilisée dans l’ancienne gestion des droits par portefeuille. Un superviseur (MANAGED\_DATA.SUPERVISOR\_PERSON\_FK) avait des droits en lecture/écriture sur un ou plusieurs portefeuilles de navires.

Dans la nouvelle gestion des droits, elle est remplacée par la notion plus large de privilège « validation ».

# Privilèges

## Description des différents privilèges

Un privilège décrit les opérations disponibles vis à vis d'un ensemble de données d’un programme de collecte, contrairement à un profil d’utilisateur (qui lui est transversal et indépendant des programmes de collecte).

### Gestion des programmes/stratégies

Le privilège  « gestion des programmes/stratégies » (anciennement privilège « administrateur ») ne confère pas de droits d'accès aux données.

Il permet en revanche de modifier le programme de collecte, créer et supprimer des stratégies et gérer les PSFM et engins liés aux stratégies.

Le privilège « gestion des programmes/stratégies » permet également de modifier une stratégie. L’outil positionne automatiquement l’utilisateur comme responsable de toutes les stratégies liées au programme. D’un point de vue technique, l’outil d’administration met à jour la table STRATEGY2MANAGER\_PERSON lorsque ce privilège est ajouté à un droit sur un programme. De plus, un mécanisme de mise à jour/nettoyage des responsables de stratégies est mis en place par la procédure P\_FILL\_STRATEGY2MANAGER\_PERSON lancée par l’outil d’administration.

Allegro : pas de synchronisation longue nécessaire, car pas de droits sur les données. Mais donne l’accès à l'administration de programmes et de stratégies.

### Saisie

Le privilège « saisie » donne des droits de lecture/écriture sur les données d'un programme.

Le privilège peut porter tous les lieux ou sur des lieux particuliers (généralement des QIM), avec ajout possible d’exceptions (inclusion ou exclusion de certains navires).

Les données concernées sont alors celles rattachées aux navires immatriculés dans ces lieux (et leurs fils) +/- exceptions.

Dans Allegro, une restriction de privilège existe pour les utilisateurs externes Ifremer. Une donnée créée par un utilisateur externe Ifremer ne peut être consultée/modifiée par un utilisateur externe d'une autre société. **La vérification est faite directement sur le département de la personne** (département fils du département « EXTERIEUR »).

Dans l’ancienne gestion par portefeuille, ce privilège était l'équivalent de la personne propriétaire du portefeuille (MANAGED\_DATA.MANAGER\_PERSON\_FK).

### Consultation

Ce privilège n'ouvre que des droits de lecture sur les données d'un programme.

Le privilège peut porter sur :

* tous les lieux ou sur des lieux particuliers (généralement des QIM), avec ajout possible d’exceptions (inclusion ou exclusion de certains navires).  
  Les données concernées sont alors celles rattachées aux navires immatriculés dans ces lieux (et leurs fils) +/- exceptions d’inclusion/exclusion de navires.
* Une ou plusieurs personnes; les données accessibles sont celles des personnes listées mais en lecture seule.

Dans l’ancienne gestion par portefeuille, ce niveau correspond aux “viewer” (MANAGED\_DATA2VIEWER\_USER).

Allegro : Synchronisation des données en local, mais droit uniquement en lecture seule.

### Validation

Le privilège « validation » donne des droits de lecture/écriture/validation sur les données d’un programme.

Le privilège peut porter sur :

* tous les lieux ou sur des lieux particuliers (généralement des QIM), avec ajout possible d’exceptions (inclusion ou exclusion de certains navires).  
  Les données concernées sont alors celles rattachées aux navires immatriculés dans ces lieux (et leurs fils) +/- exceptions d’inclusion/exclusion de navires.
* Une ou plusieurs personnes; les données accessibles sont celles des personnes listées mais en lecture/écriture/validation.

Cf §.2.3- Note sur le processus de validation/qualification des données dans Allegro

Allegro : synchronisation des données en local, droits de lecture/écriture et de modification de certains PSFM (VALIDATION\_xxx, etc.)

### Qualification

Le privilège qualificateur donne des droits d’affectation des flags qualité sur une donnée validée, et éventuellement d’application de corrections.

Dans l’ancienne gestion par portefeuille, ce niveau n’existait pas.

Allegro : Pas encore utilisé.

## Privilèges des services

Les privilèges des services sont identiques à ceux des personnes à la différence que les droits portent uniquement sur le couple [programme de collecte / lieu]. Il n’y a pas de personne(s) supervisée(s), ni de gestion d’exceptions d’inclusion/exclusion de navires.

Toutes les personnes directement dépendantes du service hériteront de ces droits (l'héritage de droits de service en service n'est pas géré).

Remarque de Stéphane Bocande : un service doit-il avoir des droits de validation ?

Si c'est un cas possible (ex : service ayant un rôle de supervision sur un programme particulier), alors oui, sinon il faudrait que l'outil d'administration des référentiels ne laissent pas cette possibilité bien que le modèle le permette (règle métier à ajouter). (cf mantis évolution #[0018630](https://forge.ifremer.fr/mantis/view.php?id=18630))

## Note sur le processus de validation/qualification des données dans Allegro

En l’absence d’un cahier des charges thématique sur le processus de validation/qualification de la donnée dans Allegro, un processus de validation « à minima » a été implémenté.

Deux types d'utilisateurs valident la donnée saisie sur les marées observées en mer (programme de collecte SIH-OBSMER) et les ventes en criée (programme de collecte SIH-OBSVENTE)

* Les valideurs des sociétés prestataires (Privilège « validation » - Profil "SIH\_UTILISATEUR"), nommés « Superviseur » dans l’ancienne terminologie
* Les valideurs Ifremer (Privilège « validation » - Profil "Membre de l'équipe Projet")
* L'acte de validation est géré par 2 psfms accessibles dans Allegro au niveau de la marée ou de la vente:
* IS\_VALIDATED - Validation société
  + Non / Données valides / Données invalides/ Corrections demandées.
  + La saisie de ce PSFM est obligatoire et la valeur par défaut est positionnée à "Non"
  + Ce PSFM est éditable uniquement par un « valideur d’une société prestataire »
  + Si la valeur saisie = « Données valides », alors il est impossible pour un observateur de reprendre la saisie de la marée ou de la vente (Seuls les valideurs peuvent effectuer cette action)
* IS\_VALIDATED\_PRG : Validation Programme
  + Données valides/Données invalides/Corrections demandées auprès de la société
  + La saisie de ce PSFM est optionnelle et la valeur par défaut est vide.
  + Le PSFM est éditable uniquement par un « valideur  Ifremer »
  + Si une valeur est saisie et est différente de « Correction demandée auprès de la société"», alors seul le valideur Ifremer est autorisé à reprendre la saisie de la marée ou de la vente

## Tableau récapitulatif

|  |  |  |  |
| --- | --- | --- | --- |
| **Privilège** | **Droits sur les données (Allegro / PersonSessionVessel)** | **Accès aux données / navire** | **Equivalence dans l’ancienne gestion par portefeuilles** |
| **Gestion des programmes/stratégies** | - | - | - |
| **Saisie** | R / W | Lieu (0..n QIM ou pays) + exceptions | Manager |
| **Consultation** | R | 2 types de source:   * Lieu + exceptions * mêmes données qu’une ou plusieurs personnes | Viewer |
| **Validation** | R / W / V | 2 types de source:   * Lieu + exceptions * mêmes données qu’une ou plusieurs personnes | Supervisor |
| **Qualification** | ? | - | - |

Note: si aucun lieu ni aucune personne ne sont définis, on regarde les exceptions.

S’il y a au moins une exception d’inclusion de navire, les droits portent UNIQUEMENT sur ces navires.

S’il y a seulement des exceptions d’exclusion de navires, les droits portent sur TOUS les navires sauf exceptions.

## Duplication automatique de privilèges

L’outil d’administration permet depuis la v1.1.2 de dupliquer automatique les privilèges d’un programme pour un autre programme cible.

L’exemple qui a nécessité cette fonctionnalité est le programme SIH-ACTIFLOT et sa pré-documentation SIH-ACTIPRED.

A l’ajout de privilèges sur le programme SIH-ACTIFLOT, l’utilisateur doit également bénéficier de droits en lecture seule sur le programme SIH-ACTIPRED.

Deux variables de configuration de l’outil d’administration permettent respectivement de définir ces associations de programmes par liste de triplets, et de cacher les programmes et privilèges associés à ces programmes :

* **privilege.program.duplicate.mapping**
  + SIH-ACTIFLOT|SIH-ACTIPRED|3,<progamme\_source>|<programme\_cible>|<privilegeId>
* **privilege.program.mask.list**
  + SIH-ACTIPRED,<programme\_à\_masquer>

Le tableau ci-dessous détaille le fonctionnement de la duplication automatique dans différents cas de figure :

|  |  |
| --- | --- |
| Action sur le programme source | Duplication sur le programme cible |
| Ajout de privilèges | Les nouveaux privilèges sont dupliqués |
| Mise à jour de privilèges sans changement de programme | Le privilège dupliqué existant est aussi mis à jour |
| Mise à jour de privilèges avec changement de programme | * Si le programme original était dupliqué, supprimer les privilèges précédemment dupliqués * Si le nouveau programme fait partie des programmes déclarés, dupliquer le privilège mis à jour |
| Suppression de privilèges | Supprimer les privilèges dupliqués |
| Mise à jour des exceptions navires | Mise à jour des exceptions navires sur les privilèges dupliqués |
| Duplication d’un privilège | Si le doit cible de la duplication est déclaré comme devant être dupliqué automatiquement, il est aussi dupliquer |

Note : lors de la duplication automatique, le niveau de privilège accordé au duplicata est celui défini dans la variable de configuration, et non celui du privilège source (ex : *saisie* pour ACTIFLOT et *consultation* pour ACTIPRED).

# Fonction de remplissage des droits depuis les privilèges par programme

La fonction PL/SQL F\_FILL\_PERSON\_SESSION est utilisée par Allegro pour remplir les droits d’une personne (tables PERSON\_SESSION et PERSON\_SESSION\_VESSEL) faire référence à la documentation des tables ou à mettre en annexe. Cette fonction est appelée par Allegro avant la phase de synchronisation des données.

La version créée par SODIFRANCE pour les remplir à partir des portefeuilles de navires a été modifiée pour les remplir depuis les tables de privilèges par programme (i.e., la nouvelle gestion des droits).

Notons que les droits d’une personne nécessitent une période de validité, alors que les privilèges par programme ne donnent aucune indication temporelle. Il a été décidé que la fonction attribuerait comme périodes les dates d’entrée (et éventuellement de sortie) du navire dans le quartier d’immatriculation si un tel lieu est spécifié.

Les différents cas de figure sont décrits dans la section 3.2.

## Paramètres et constantes d'exploitation

### Paramètres

La fonction prend deux paramètres en entrée :

* **P\_PERSON\_FK** : l'identifiant de la personne dont les droits sont calculés
* **P\_SKIP\_LONG\_DURATION** (booléen, 0 ou 1) : si 1 (valeur par défaut), le calcul sera ignoré pour une personne dont le calcul des droits a été jugé trop long (cf. section 3.2.5 sur les portefeuilles volumineux).

### Constantes d’exploitation

Les constantes à régler concernent principalement :

* les types de privilèges
  + PRIVILEGE\_MANAGER *(= gestion des programmes/stratégies)*,
  + PRIVILEGE\_RECORDER *(= saisie)*,
  + PRIVILEGE\_VALIDATOR *(= validation)*
* les types d'objets (table OBJECT\_TYPE) :
  + CALENDAR\_OBJ\_TYPE *(= calendriers d’activités)*,
  + FISHING\_TRIP\_OBJ\_TYPE *(= marées)*,
  + PHYS\_GEAR\_SURVEY\_OBJ\_TYPE *(= enquêtes engins)*,
  + SALE\_OBJ\_TYPE *(= ventes)*,
  + SCIENT\_CRUISE\_OBJ\_TYPE *(=campagnes scientifiques)*
* les constantes relatives aux navires :
  + **VESSEL\_DEFAULT\_PROGRAM** (programme *SIH* par défaut)
  + **VESSEL\_TYPE\_PRO** *(= navires de pêche professionnels)*
  + VESSEL\_TYPE\_INFORMAL *(=navires informels : pirogues, etc…)*
  + VESSEL\_TYPE\_SCIENTIFIC *(=navires scientifiques)*

Deux constantes d’exploitation **YEAR\_SPAN\_FOR\_PTM** (15 ans pour un membre de l’équipe projet) et **YEAR\_SPAN\_DEFAULT** (3 ans par défaut) définissent le nombre d’années d’historique concerné.

Enfin, pour la gestion des « portefeuilles » volumineux, la constante MAX\_DURATION\_IN\_MS (30s) permet de fixer un seuil au temps de calcul de la fonction. La section 3.2.5 couvre les cas où ce seuil est dépassé.

Ces constantes peuvent être modifiées selon l'environnement.

## Règles mises en œuvre pour le remplissage des droits

La fonction se base sur les privilèges par programme (PROGRAM2PERSON) et ceux du service (ou de la société) de la personne (PROGRAM2DEPARTMENT) (cf modèle de données, paragraphe 4.2).

Le privilège (saisie, consultation, validation) définit les droits de lecture/écriture/validation sur un jeu de données.

Le privilège particulier *gestion des programmes stratégies* est ignoré puisqu'il ne confère pas de droits sur les données.

Les limites du jeu de données sont fixées par :

* le programme (source de données)
* un ensemble de navires, calculé par :
  + un (ou des) lieu(x) +/- exceptions navires
  + transitivité dans le cas de droits sur des personnes (ne concerne que les privilèges *consultation* ou *validation*) : le jeu de données est le même que celui de la personne source.

Seuls les navires rattachés au programme *SIH*, et dont le type est indiqué ci-dessous, sont pris en compte :

* Navire de pêche professionnel ;
* Navire informel ;
* Navire scientifique.

Cette liste est modifiable simplement, en utilisant les constantes d’exploitation incluses dans la fonction (cf 3.1.2).

Selon le type de privilège, les droits accordés sont différents. Le type de droit est défini par les champs de la table PERSON\_SESSION\_VESSEL :

* READ\_DATA : accès en lecture
* WRITE\_DATA: accès en écriture
* READ\_VESSEL permet de donner l'accès aux informations du navire (caractéristiques et armateurs – les données d’immatriculation sont toujours visibles). Actuellement, cette valeur est toujours à 1.
* VALIDATE\_DATA permet de donner l'accès à la validation des données.

Le tableau suivant dresse un résumé des correspondances.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Privilège** | **READ\_DATA** | **WRITE\_DATA** | **READ\_VESSEL** | **VALIDATE\_DATA** |
| **Gestion des programmes stratégies** | N/A | N/A | N/A | N/A |
| **Saisie** | 1 | 1 | 1 | 0 |
| **Consultation** | 1 | 0 | 1 | 0 |
| **Validation** | 1 | 1 | 1 | 1 |
| **Qualification** | 1 | 0 | 1 | 0 |

Remplissage des autres colonnes :

* PROGRAM\_FK : Programme sur lequel s’applique le privilège ;
* OBJECT\_TYPE\_FK : Rempli avec le nom de la table tête de grappe, issu de la table ACQUISITION\_LEVEL (récupéré à partir des niveaux d’acquisition trouvés des stratégies applicables du programme) ;
* UPDATE\_DATE : mise à jour automatiquement par le système. Ce champ est mis à jour uniquement en cas de nouveau privilège ou de privilège modifié : le but est de minimiser le nombre de lignes récupérées par la synchronisation Allegro.

Note 1 : concernant la gestion particulière des données de prédocumentation déclaratives déclaratives (SIH-ACTIPRED), on peut imaginer d’affecter automatiquement des droits de consultation dessus, lors de l’affectation de droits de saisie sur les calendriers d’activité (SIH-ACTIFLOT). (cf mantis évolution #[0018649](https://forge.ifremer.fr/mantis/view.php?id=18649))

Note 2 : Attention, le statut des navires n’est pas pris en compte (comme dans l’ancienne procédure de calcul des droits). Il est en effet normal de ne pas en tenir compte, afin de pouvoir consulter ou modifier les données historiques sur un navire devenu obsolète.

### Privilèges sur des personnes

Si une personne référencée est spécifiée pour un privilège, alors d’éventuels lieu (PROGRAM2PERSON.LOCATION\_FK) ou exceptions sont ignorés. Le niveau de privilège est celui donné à l’utilisateur (ex : consultation, validation), tandis que le jeu de données est calculé à partir des droits de la personne référencée (ex : observateur).

Il est à noter que les droits de supervision ne sont pas transitifs : si une personne référencée est elle-même superviseur, ces droits de supervision ne seront pas remontés dans le calcul du remplissage.

Evolution : S.Bocande propose de mettre en œuvre une récursivité complète de la gestion des droits sur les personnes (ex : pouvoir superviser une personne A qui supervise une personne B, et avoir les droits sur A et B). (cf mantis évolution #[0018651](https://forge.ifremer.fr/mantis/view.php?id=18651)).

Note : la période d’ouverture de droits prise en compte est celle du superviseur et non celle de la personne supervisée. Un membre de l’équipe projet qui supervise un non-membre peut donc potentiellement avoir plus de droits que la personne supervisée.

### Privilèges par lieu(x)

En règle générale les lieux sont des quartiers d'immatriculation (QIM) ou des lieux de niveau supérieur.

* Les droits seront donnés sur tous les navires ayant été immatriculés sous ce lieu, et ceci de manière hiérarchique. (ex : France donnera les droits sur toutes les données du programme liées aux navires immatriculés dans des quartiers français). A ces droits s’ajoutent ou se soustraient des exceptions navires (PROGRAM2PERSON\_EXCEPTIONS)
* Si le lieu n’est pas spécifié, alors le jeu de données est lié à tous les navires, sauf exceptions
  + Si au moins une exception d’inclusion est définie, alors les droits porteront uniquement sur les données liées aux navires définis comme exceptions d’inclusion.
  + En cas d’exceptions d’exclusion uniquement, les droits portent sur toutes les données moins celles des navires « exceptions ».

### Héritage du droit des services

Le fonctionnement des privilèges par service est le même que pour les personnes, à la différence des droits de supervision. Le calcul ne se fait qu’à partir de la paire programme/lieu (il n’y a pas d’exceptions d’inclusion / exclusion de navires).

La fonction de remplissage ignore alors les privilèges hérités du service (ou de la société) de la personne si aucun lieu n’est défini.

De plus les droits ne viennent que du service direct, il n’y a pas de notion d’héritage hiérarchique, dans un sens ou dans l’autre. Dans le cas d’une hiérarchie A>B>C, une personne du service C n’aura pas les droits définis pour les services B ou A. L’outil d’administration ne permettant pas encore la gestion hiérarchique des droits entre services, ce point pourra être réévalué en même temps.

### Règles de correspondances périodes d'immatriculations – périodes d'ouverture de droits

Les ouvertures de droits sur les données portent sur des périodes qui dépendent :

* des périodes d'immatriculation des navires inclus dans les privilèges (suivant le lieu défini)
* de la visibilité de la personne
  + membre de l'équipe projet (profil ALLEGRO\_SUPER\_UTILISATEUR): période plus longue (15 ans)
  + non-membre de l’équipe projet (profil ALLEGRO\_UTILISATEUR) : période courte (3 ans)

Ainsi les navires qui ne sont plus immatriculés pendant la période visible par l'utilisateur ne seront pas inclus dans les droits.

La période d'ouverture des droits demande obligatoirement une date de fin (PERSON\_SESSION\_VESSEL.END\_DATE\_TIME). Dans le cas où une période d'immatriculation n'est pas bornée, la date de fin pour l'ouverture des droits est affectée au 1er janvier 2100 (note : le choix de 2100 plutôt que *null* a été fait pour l’optimisation des indexes qui se basent sur la date de fin).

La règle de définition des périodes d'ouverture de droits est la suivante :

***Les droits ne seront ouvert que sur les intervalles de temps où périodes d'immatriculation et visibilité de la personne se recouvrent.***

Note sur l’optimisation de périodes :

Notons que dans le cas de droits liés à un lieu, les périodes ne sont pas optimisées afin de ne pas rallonger les temps de calcul : en cas de périodes d'immatriculation continues, elles ne seront pas groupées en une seule et il y aura donc une ligne PERSON\_SESSION\_VESSEL par période.

En revanche, si le privilège sur les données d’un navire n’est pas lié au lieu d’immatriculation du navire, alors toutes ses périodes d’immatriculations sont agrégées en une seule période les recouvrant toutes, et ceci même en cas de trous dans les périodes.

Le tableau suivant détaille 5 cas de figure.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Cas 1 | Cas 2 | Cas 3 | Cas 4 | Cas 5 |
| Période de visibilité |  |  |  |  |  |
| Période d'immatriculation |  |  |  |  |  |

* Cas 1

PERSON\_SESSION\_VESSEL .START\_DATE\_TIME = 01/01/[année courante – période de visibilité]

PERSON\_SESSION\_VESSEL .END\_DATE\_TIME = date de fin de la période d'immatriculation

* Cas 2

PERSON\_SESSION\_VESSEL .START\_DATE\_TIME = date de début de la période d'immatriculation

PERSON\_SESSION\_VESSEL .END\_DATE\_TIME = nvl(date de fin de la période d'immatriculation,01/01/2100)

* Cas 3

PERSON\_SESSION\_VESSEL .START\_DATE\_TIME = date de début de la période d'immatriculation

PERSON\_SESSION\_VESSEL .END\_DATE\_TIME =  date de fin de la période d'immatriculation

* Cas 4

Le navire n’apparaît pas dans PERSON\_SESSION\_VESSEL

* Cas 5

PERSON\_SESSION\_VESSEL .START\_DATE\_TIME = 01/01/[année courante – période de visibilité]

PERSON\_SESSION\_VESSEL .END\_DATE\_TIME =  nvl(date de fin de la période d'immatriculation,01/01/2100)

### Cas des portefeuilles volumineux

**ATTENTION :**

Dans le cas d’un utilisateur ayant des privilèges sur des personnes, si le nombre de personnes référencées est trop élevé, le calcul transitif des droits peut prendre trop de temps.

Si un temps de calcul trop long est détecté (> 30s, paramétrable dans la fonction), par la suite les droits de l’utilisateur seront pré-calculés à intervalles réguliers en tâche de fond en cas de changements. Une procédure PL/SQL permet ce calcul (P\_FILL\_BIG\_PERSON\_SESION).

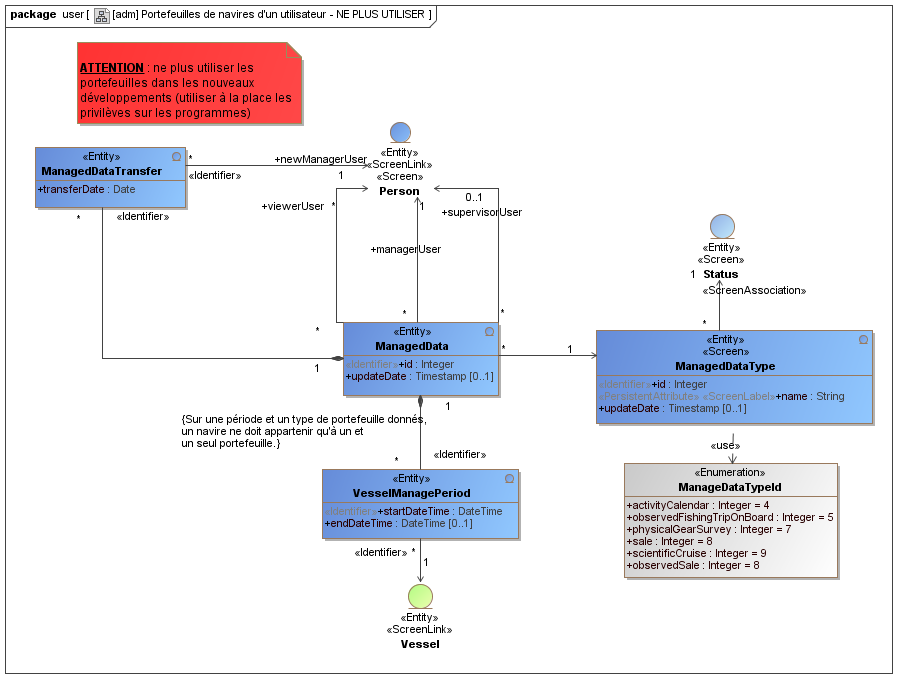
**=>** Il faut implémenter le lancement de cette procédure en tache de fond (par exemple en définissant un *cron)*.

Toutefois, en cas de demande de modification des droits urgente, le calcul peut être lancé manuellement par l'outil d'administration.

Action Ifremer : mettre en œuvre en œuvre une tache récurrente pour le lancement des portefeuilles volumineux (P\_FILL\_BIG\_PERSON\_SESION).

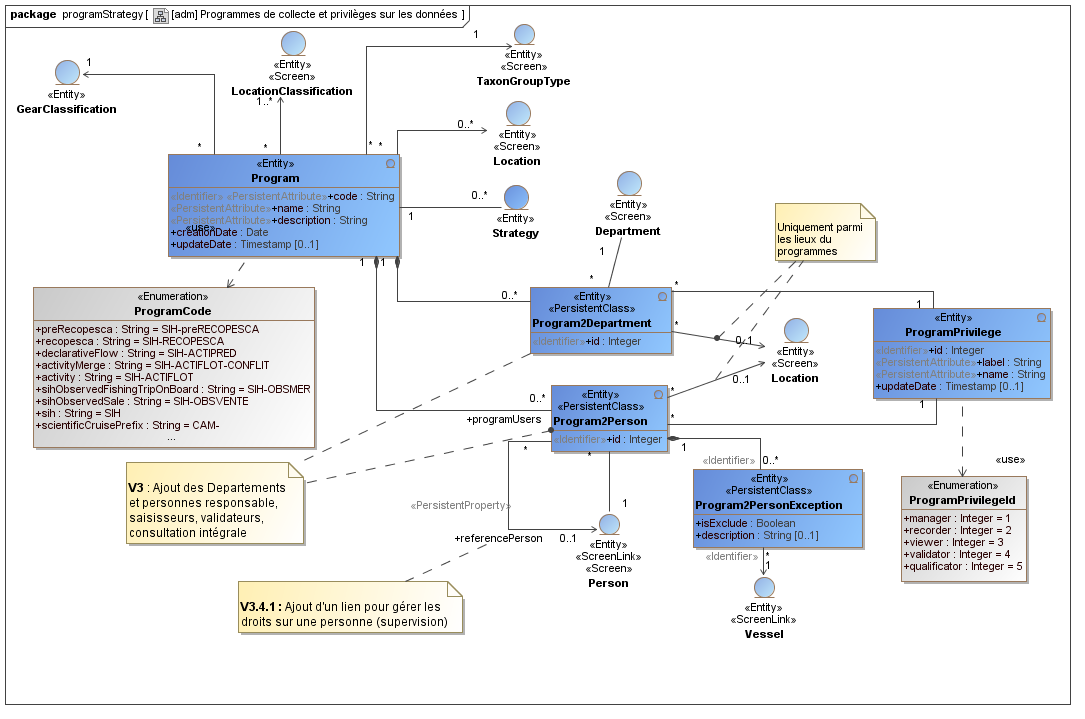
# Annexes

## Modèle de données de l’ancienne gestion des droits par portefeuilles de navires



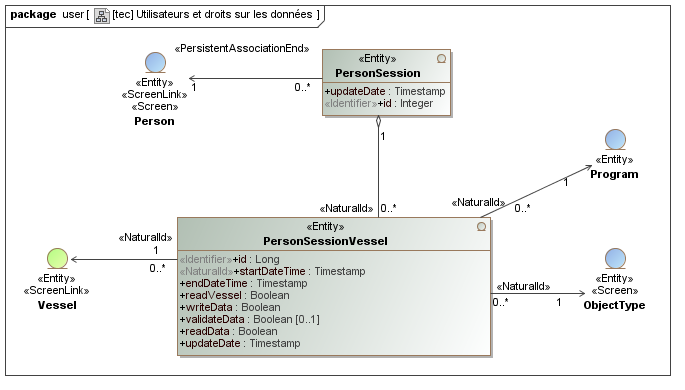
## Modèle de données de la nouvelle gestion des droits

Les tables impactées par la gestion des droits dans l’outil d’administration sont représentées ci-dessous (Program2Person est l’entité centrale).



## Modèle de données des droits Allegro

Les tables impactées par la procédure PL/SQL de remplissage des droits sont représentées ci-dessous.



## Procédure de migration des portefeuilles de navires (pour l'équipe d'exploitation)

Cette section décrit les procédures de migration des portefeuilles de navires dans le cas des programmes fonctionnant par liste restreinte de navire, ou par quartiers d'immatriculation (calendriers d'activité).

Remarque S.Bocande :

Il faut prévoir un cas spécifique pour les valideurs Ifremer (Privilège « validation » - Profil "SIH\_SUPER\_UTILISATEUR" – anciennement « équipe projet »).

Exemple de super-utilisateur :

* Pour OBSMER, deux utilisateurs sont dans ce cas : Olivier Gaudou et Alain Tétard.
* Pour OBSVENTE, il faudra reboucler avec Emilie Leblond. Il nous faut la liste des valideurs Ifremer (Qui valide qui ?) - A défaut, on ne fait rien.
* Pour ces "valideurs Ifremer", il suffit uniquement de leur donner les droits en validation sur les valideurs des sociétés prestataires (OD et groupe EI) et sur tous les utilisateurs IFREMER.

Note : Dans la procédure d'exploitation de création d'un utilisateur, il faudra noter qu'il faut ajouter systématiquement le nouvel utilisateur dans la liste des utilisateurs gérés par les valideurs des sociétés prestataires si extérieur et dans la liste des utilisateurs gérés par les valideurs Ifremer sinon.

### SIH-OBSMER, SIH-OBSVENTE et CAM-CGFS

Pour les programmes **SIH-OBSMER, SIH-OBSVENTE et CAM-CGFS**, dont la gestion est actuellement faite par navire (et non par QIM), il est possible d’exécuter la procédure de migration P\_MIGRATE\_MANAGE\_DATA\_EX , en indiquant l’utilisateur à migrer (paramètre PERSON\_FK).

|  |
| --- |
| execute P\_MIGRATE\_MANAGE\_DATA\_EX( 2 /\*=ID utilisateur à migrer\*/ ); |

Pour migrer tous les utilisateurs d’un seul coup, exécuter la commande suivante :

|  |
| --- |
| DECLARE  CURSOR PERSON\_CURSOR IS  select distinct person\_fk  FROM (  SELECT MANAGER\_PERSON\_FK AS PERSON\_FK FROM MANAGED\_DATA  UNION ALL  SELECT SUPERVISOR\_PERSON\_FK AS PERSON\_FK FROM MANAGED\_DATA  UNION ALL  SELECT PERSON\_FK FROM MANAGED\_DATA2VIEWER\_USER  UNION ALL  SELECT NEW\_MANAGER\_PERSON\_FK AS PERSON\_FK FROM MANAGED\_DATA\_TRANSFER  );  BEGIN  FOR P IN PERSON\_CURSOR LOOP  SIH2\_ADAGIO\_DBA.P\_MIGRATE\_MANAGE\_DATA\_EX(P.PERSON\_FK);  end loop;  END;  / |

### SIH-ACTIPRED, SIH-ACTIFLOT

Pour les programmes des **calendriers d’activité** (SIH-ACTIPRED, SIH-ACTIFLOT)

Mettre à jour le fichier Excel suivant (cf. mantis [#15956](https://forge.ifremer.fr/mantis/view.php?id=15956)) : [quartier\_observateurs-act-v2-nouvelle\_gestion\_droits.xls](https://forge.ifremer.fr/mantis/file_download.php?file_id=12946&type=bug)

Copier le contenu de la colonne “SQL” et l’exécuter sur la base Harmonie-Adagio.

Exemple :

|  |
| --- |
| Execute sih2\_adagio\_dba.P\_FILL\_PRIVILEGE\_BY\_QIM('1541','SIH-ACTIFLOT,SIH-ACTIPRED','YE,LR',2,1);  Execute sih2\_adagio\_dba.P\_FILL\_PRIVILEGE\_BY\_QIM('1521','SIH-ACTIFLOT,SIH-ACTIPRED','BR,MX,CM,DZ,AD',2,1);  Execute sih2\_adagio\_dba.P\_FILL\_PRIVILEGE\_BY\_QIM('1627','SIH-ACTIFLOT,SIH-ACTIPRED','PV,ST,MA,MT,TL,NI',2,1);  Execute sih2\_adagio\_dba.P\_FILL\_PRIVILEGE\_BY\_QIM('1625','SIH-ACTIFLOT,SIH-ACTIPRED','PV',2,1);  (...) |

La procédure P\_FILL\_PRIVILEGE\_BY\_QIM peut également être appelée directement, pour mettre à jour les droits d’un seul utilisateur, à partir d’une liste de QIM :

|  |
| --- |
| Execute sih2\_adagio\_dba.P\_FILL\_PRIVILEGE\_BY\_QIM(  1541 /\*ID de l’utilisateur\*/,  'SIH-ACTIFLOT,SIH-ACTIPRED', /\*Liste des programmes concernés\*/  'YE,LR', /\*Liste des QIM\*/  2, /\*2= observateur, 4= validateur\*/  1 /\*1=remplacer les anciens droits sur les programmes des calendriers d’activité  0=ajouter ces nouveaux droits aux anciens\*/  ); |

Pour les calendriers d’activité, les droits de supervision et de consultation sur le portefeuille d’une autre personne doivent être migrés par une 3ème procédure P\_MIGRATE\_MD\_SUPERVISION.

|  |
| --- |
| execute P\_MIGRATE\_MD\_SUPERVISION( 2 /\*=ID utilisateur à migrer\*/ ); |

Pour migrer tous les utilisateurs d’un seul coup, exécuter la commande suivante :

|  |
| --- |
| DECLARE  CURSOR PERSON\_CURSOR IS  select distinct person\_fk  FROM (  SELECT MANAGER\_PERSON\_FK AS PERSON\_FK FROM MANAGED\_DATA  union all  SELECT SUPERVISOR\_PERSON\_FK AS PERSON\_FK FROM MANAGED\_DATA  UNION ALL  SELECT PERSON\_FK FROM MANAGED\_DATA2VIEWER\_USER  UNION ALL  SELECT NEW\_MANAGER\_PERSON\_FK AS PERSON\_FK FROM MANAGED\_DATA\_TRANSFER  );  BEGIN  FOR P IN PERSON\_CURSOR LOOP  SIH2\_ADAGIO\_DBA.P\_MIGRATE\_MD\_SUPERVISION(P.PERSON\_FK);  end loop;  END;  / |

L’instruction peut également être exécutée dans la même boucle que celle pour OBSMER, OBSVENTE et CAM-CGFS.

### Cas des superviseurs pour les calendriers d'activité

La procédure de migration par QIM ne prend pas en compte les superviseurs des programmes liés aux calendriers d'activité (programmes SIH-ACTIFLO et SIH-ACTIPRED). Il est donc nécessaire de lancer la procédure P\_MIGRATE\_MD\_SUPERVISION pour combler ce manque et ainsi migrer les privilèges de validation et de consultation.