Cognos BI

Gestion de la sécurité & bonnes pratiques

Sommaire

1 – Aperçu de Cognos BI

2 – La sécurité dans Cognos BI

3 – Modéliser la sécurité

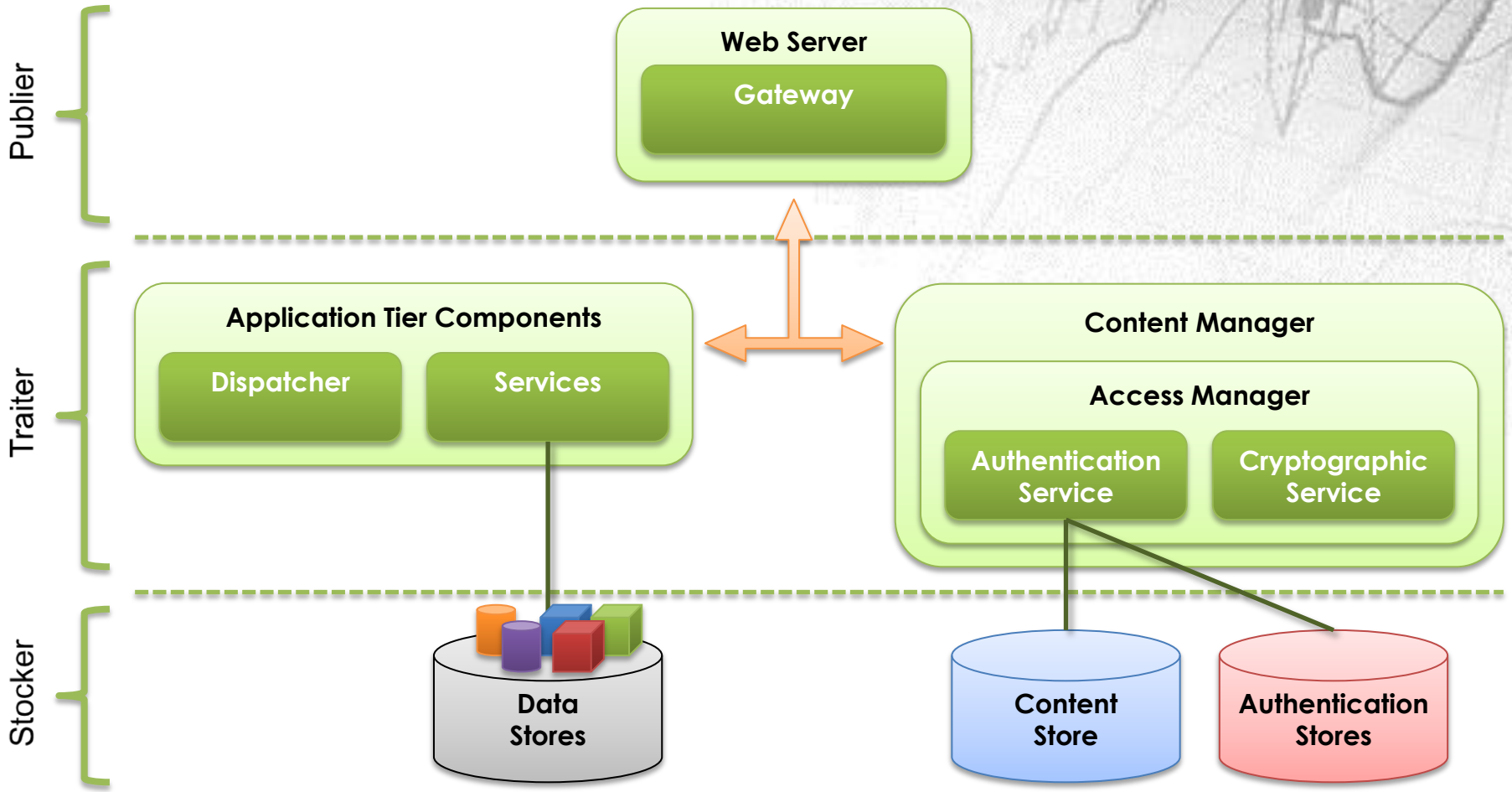
4 – Maintenance

Bi2B

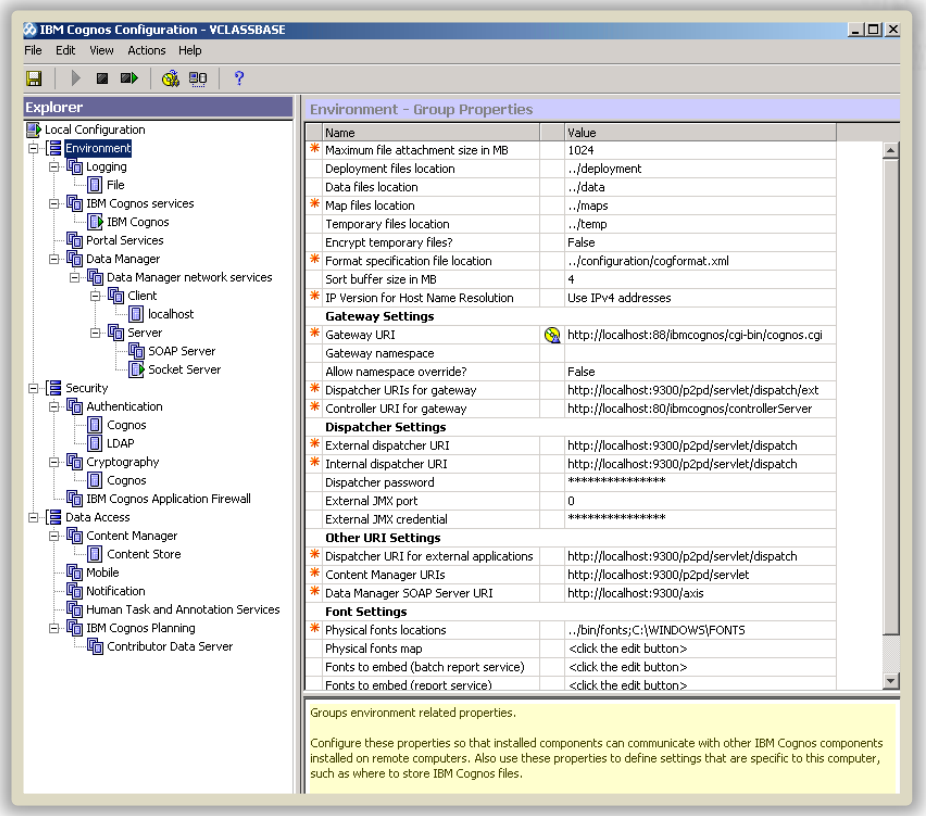
Pilot your performance

Aperçu de Cognos BI

Aperçu de Cognos BI : Architecture



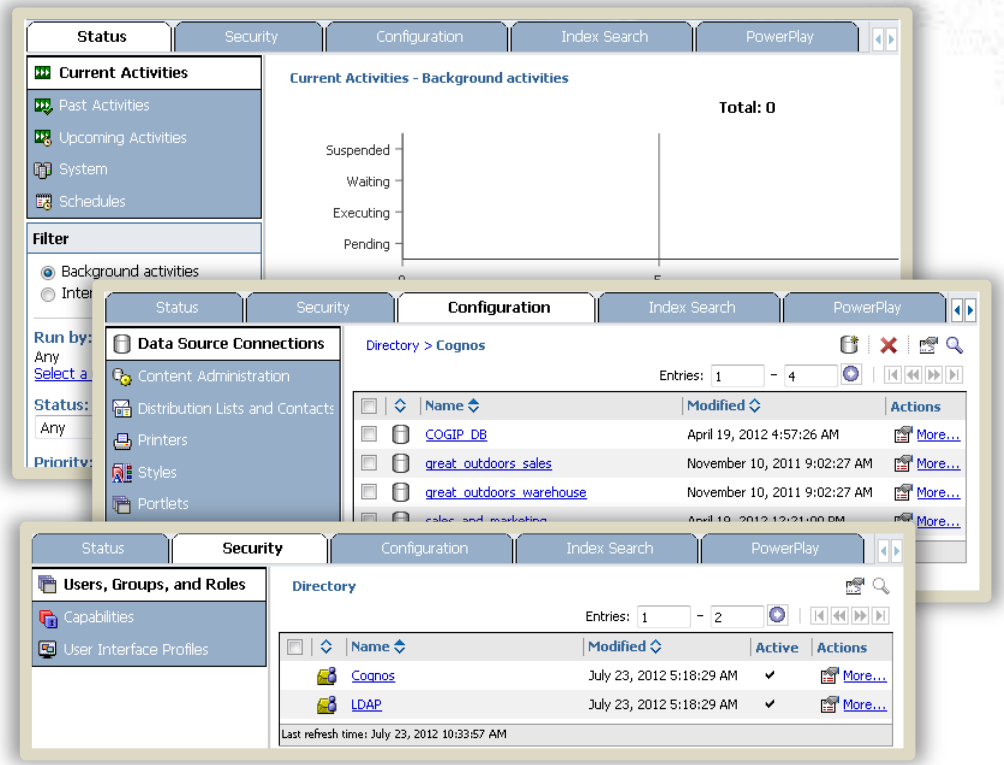
Aperçu de Cognos BI : Cognos Configuration



Cognos configuration permet de définir les composants côté serveur, notamment :

- Variables d'environnement.
- Espaces-noms d'authentification.
- Paramètres SSO.
- Connection au Content Store.
- Définition du logging de l'audit.
- Paramètres email.

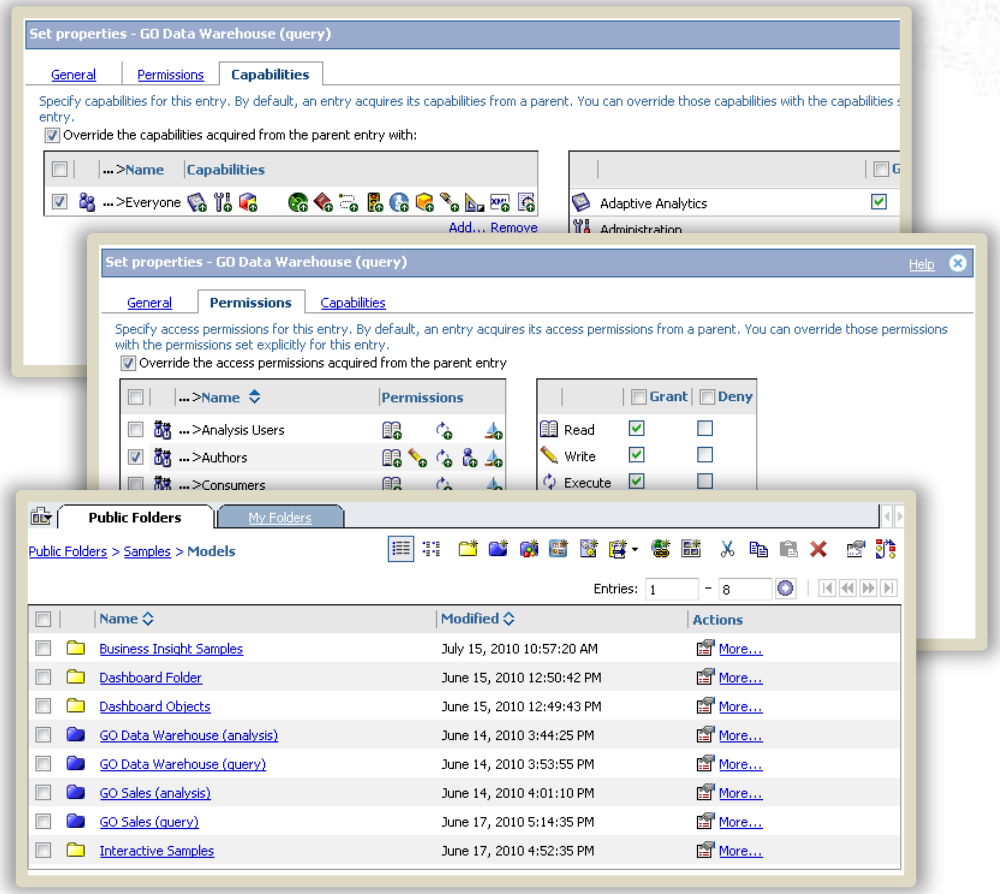
Aperçu de Cognos BI : Cognos Administration



Cognos Administration permet de :

- Contrôler l'état du portail.
- Définir les associations de sécurité.
- Gérer les profils utilisateur.
- Définir les connexions aux sources de données.
- Importer & exporter le contenu du portail.
- Définir les propriétés d'index et de recherche.

Aperçu de Cognos BI : Cognos Connection



Cognos Connection permet de :

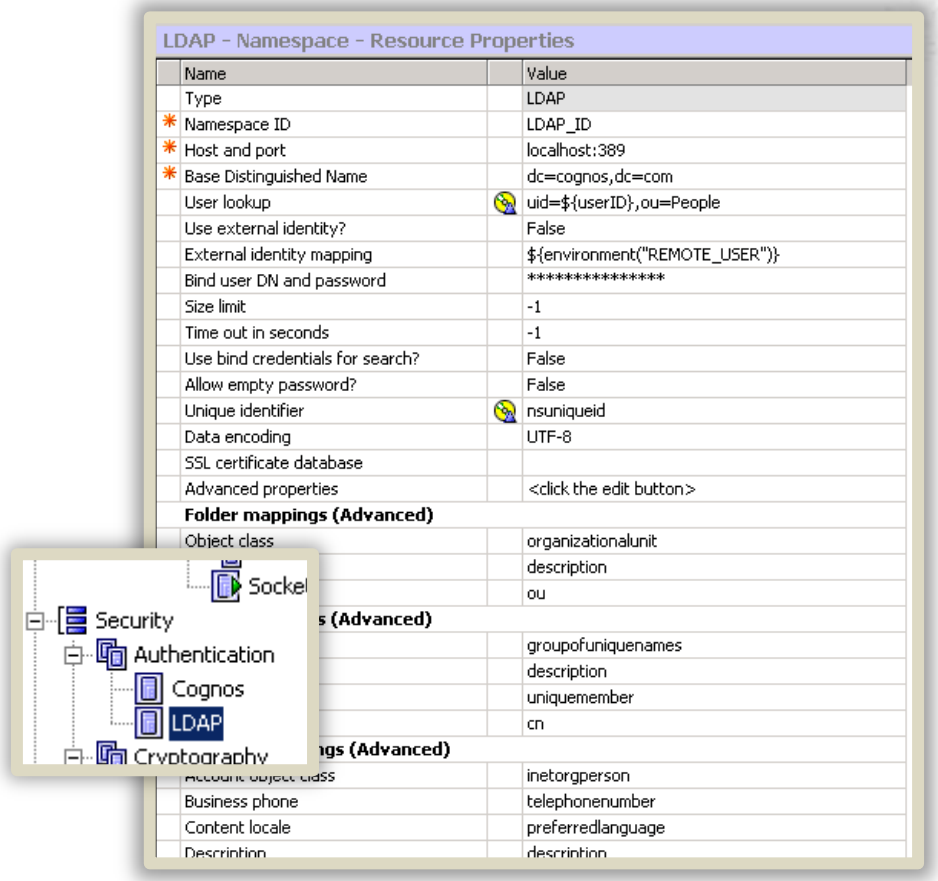
- Naviguer dans le contenu Cognos.
- Voir / Exécuter / Editer les objets Cognos.
- Exécuter les studios de reporting.
- Définir les permissions sur les objets
  - Lecture
  - Ecriture
  - Exécution
  - Définition des règles
  - Passage.
- Définir des fonctions autorisées à l'intérieur d'un dossier.

Bi2B

Pilot your performance

2 La sécurité dans Cognos BI

La sécurité dans Cognos BI : Les espaces-noms



- Cognos BI fournit un espace-nom local permettant de gérer des groupes et rôles spécifiques à l'application.
- Cognos BI ne fournissant pas de composant permettant la gestion d'utilisateurs, il est nécessaire de paramétrer au moins un annuaire externe (LDAP) afin de gérer des comptes utilisateurs.
- Le paramétrage des annuaires externes est effectué dans Cognos Configuration.
- Cognos BI est compatible avec l'ensemble des technologies d'annuaire du marché: OpenLDAP, ApacheDirectory, Active Directory, solution spécifique, etc.

La sécurité dans Cognos BI : Cognos Access Manager ID (CAMID)

Chaque utilisateur est identifié dans Cognos BI grâce à un identifiant unique, basé sur les propriétés suivantes :

- **L'ID d'espace nom :** L'ID d'espace-nom est défini dans Cognos Configuration. Il peut être différent du nom de l'espace-nom qui est présenté dans l'écran d'authentification aux utilisateurs. Il est important de noter que si l'ID d'espace-nom devait être modifié, Cognos considèrerait cela comme un nouvel espace-nom et l'ensemble des profils et objets utilisateurs deviendrait inaccessible car restant attachés à l'ancien ID.

- **La propriété nsuniqueid :** La propriété nsuniqueid doit être renseignée dans la configuration de l'espace-nom avec un attribut de l'annuaire externe utilisé, lequel doit être un identifiant unique pour chaque objet de l'annuaire. Cet attribut est totalement géré par l'annuaire et Cognos n'y accède qu'en lecture seule.

- **Le type d'objet :** Utilisé dans le CAMID via un caractère. Par exemple, ce caractère vaut "u" pour un utilisateur et "g" pour un groupe.

Pour un annuaire dont l'ID serait "LDAP_ID" et un utilisateur nommé "David Smith" avec une propriété nsuniqueid valant "smithd", le CAMID résultant serait :

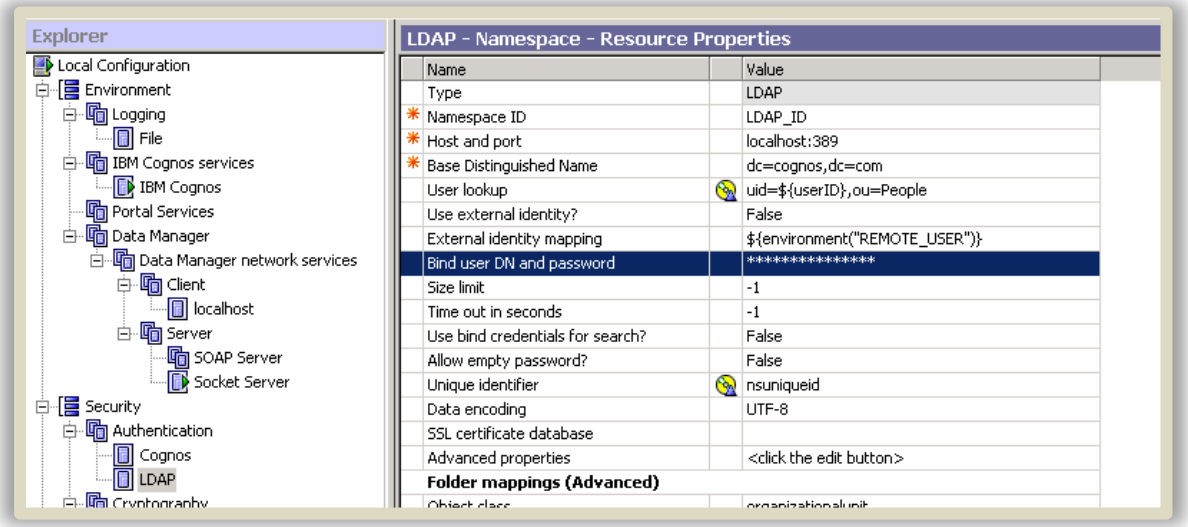
```
CAMID("LDAP_ID:u:smithd")
```

La sécurité dans Cognos BI : Single-signon

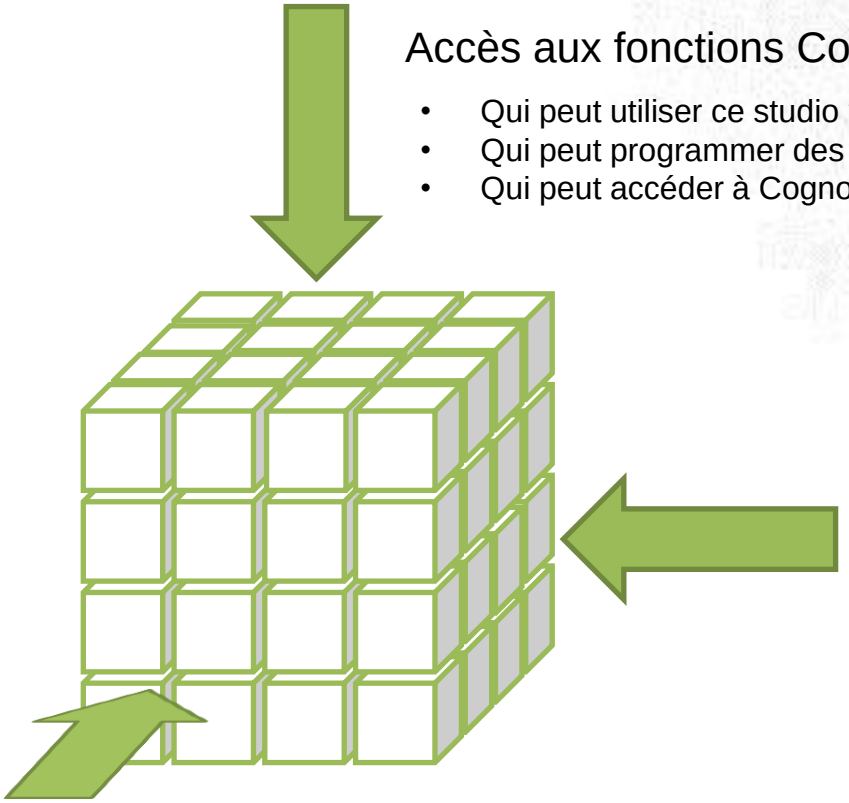
Cognos BI fournit deux manières d'activer l'authentification automatique (Single-signon) des utilisateurs :

- **Utilisation de Kerberos SSO :** Aucune configuration n'est nécessaire côté Cognos BI. Néanmoins, le compte utilisé pour accéder à l'annuaire externe dans Cognos Configuration (propriété "bind user DN and password") doit posséder les droits de délégation Kerberos au niveau de l'annuaire.

- **Utilisation de variables d'environnement :** Les informations d'identification sont transmises par une application tierce et stockées dans une variable d'environnement sur les machines clientes. Dans Cognos Configuration, la propriété "use external identity mapping" doit être renseignée en fonction de la variable à récupérer.



La sécurité dans Cognos BI : Axes de sécurisation



Accès aux fonctions Cognos

- Qui peut utiliser ce studio ?
- Qui peut programmer des exécutions de rapports ?
- Qui peut accéder à Cognos Administration ?

Accès aux données métiers

- Qui peut voir cette donnée élémentaire ?
- Qui peut voir ces valeurs de données ?

Accès au contenu Cognos

- Qui peut voir ce rapport ?
- Qui peut éditer cette propriété ?
- Qui peut utiliser ce package ?

La sécurité dans Cognos BI : Groupes, Rôles & Comptes utilisateurs

Cognos BI fournit deux types d'objets permettant de gérer la sécurité, qui sont techniquement identiques mais utilisés selon des objectifs différents :

- Les rôles sont en général utilisés pour gérer l'accès aux différentes fonctionnalités du portail et pour organiser les utilisateurs selon un axe technique.

- Les groupes sont en général utilisés pour gérer l'accès au contenu Cognos Bi et pour organiser les utilisateurs selon un axe métier.

- Les comptes représentent les utilisateurs, uniques par leurs identifiants d'authentification. Chaque compte possède un profil configurable et un espace personnel dans lequel l'utilisateur peut stocker ses objets Cognos. Le profil est créé lors de la première connexion de l'utilisateur.

Les appartenances aux groupes et rôles dans Cognos BI sont cumulatives. Ainsi, un utilisateur membre du groupe "RH Manager" et du groupe "France" cumulera les droits définis pour ces deux groupes.

La sécurité dans Cognos BI : Rôles & Groupes par défaut

Cognos BI fournit quatre groupes et rôles par défaut qui ne peuvent être supprimés :

- **Administrateurs système :** Tous les utilisateurs membres de ce rôle ont accès à l'ensemble des objets et fonctionnalités du portail et ce, quelle que soit la sécurité définie par ailleurs.

- **Tous les utilisateurs authentifiés :** Ce groupe représente l'ensemble des utilisateurs qui se sont connectés au portail au moins une fois. En pratique, cela correspond à tous les utilisateurs qui possèdent un profil.

- **Tous :** Ce groupe représente l'ensemble des utilisateurs pouvant potentiellement accéder d'une manière ou d'une autre au portail Cognos Connection. En pratique, cela correspond à l'ensemble des comptes accessibles par Cognos dans les espaces-noms paramétrés à l'aide de Cognos Configuration.

- **Anonyme :** Il s'agit du seul compte utilisateur pouvant exister dans l'espace-nom local de Cognos BI. Si l'accès anonyme est autorisé dans Cognos Configuration, ce compte représente l'ensemble des utilisateurs accédant au portail Cognos Connection et ne s'étant pas encore authentifiés. Ce compte n'a pas d'utilité si l'accès anonyme est désactivé dans Cognos Configuration.

- Les autres groupes et rôles par défaut peuvent être supprimés (bien que ce ne soit pas recommandé) et fournissent un axe technique basique donnant accès aux différentes fonctionnalités du portail.

La sécurité dans Cognos BI : Permissions

La sécurité Cognos BI étant extrêmement fine, absolument tous les objets Cognos peuvent posséder des permissions spécifiques. Pour chaque objet, les permissions définies s'appliquent à l'objet en question ainsi qu'à ses descendants, sauf en cas de permission spécifique définie sur les descendants. Les permissions peuvent être autorisées, interdites ou indéfinies et sont les suivantes :

- **Lecture** : Permet de voir l'objet.

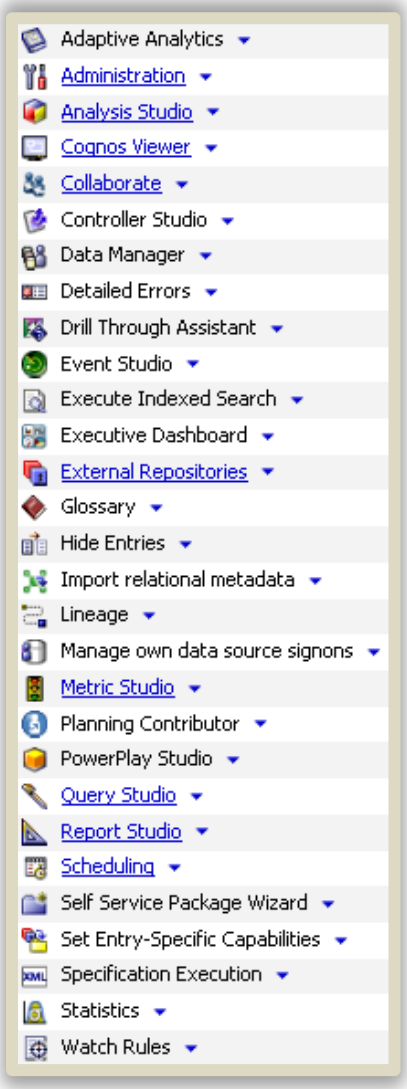
- **Ecriture** : Permet d'éditer les propriétés de l'objet.

- **Exécution** : Permet d'exécuter l'objet (s'il est exécutable).

- **Définition des règles** : Permet de changer les permissions de l'objet.

- **Passage** : Ne permet pas de voir l'objet mais autorise l'accès direct aux descendants de l'objet.

La sécurité dans Cognos BI : Fonctions



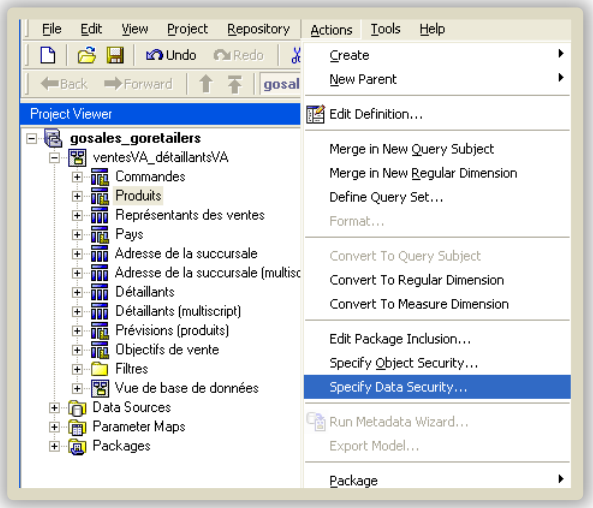
- Les fonctions Cognos BI sont utilisées pour définir l'accès aux différentes fonctionnalités du portail. Certaines fonctions possèdent des sous-fonctions afin de gérer les droits plus finement.
- Une fonction est autorisée lorsqu'une permission de type "Exécution" est définie sur celle-ci. Pour autoriser seulement une sous-fonction sans autoriser la fonction parente, une permission de type "Passage" doit être définie sur la fonction parente.
- Les permissions possibles sur les fonctions reprennent le modèle Cognos détaillé précédemment. Néanmoins, les permissions de type "Lecture" et "Ecriture" ne sont d'aucune utilité pour ce type d'objet.
- Les fonctions peuvent de plus être redéfinies pour chaque dossier dans Cognos Connection. Ces surcharges spécifiques sont définies en éditant les propriétés des dossiers en question.
- L'analyse de l'accès aux différentes fonctions de Cognos BI permet de déduire pour chaque utilisateur le type de licence commerciale effectivement consommé.

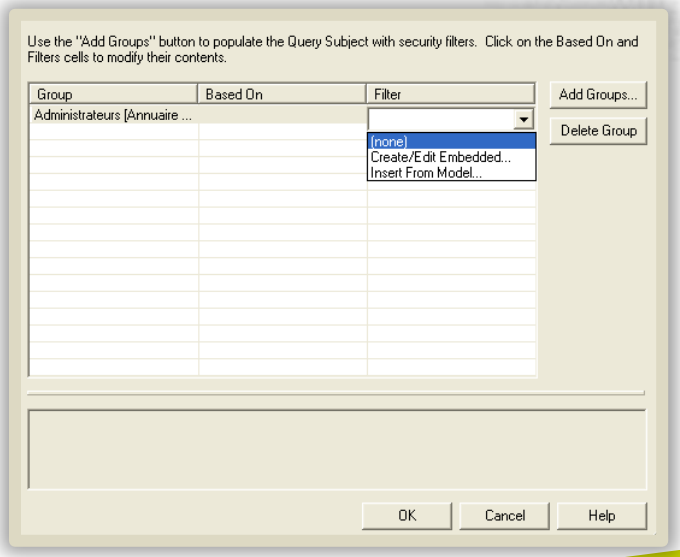
La sécurité dans Cognos BI : Accès au données

Les groupes & rôles Cognos BI peuvent être utilisés pour définir une sécurité sur l'accès aux données, durant l'accès aux bases de données relationnelles métiers. Cette sécurisation est effectuée durant la phase de modélisation, dans Framework Manager. La sécurité peut être utilisée de deux manières :

- D'une part pour définir l'accès aux différentes données élémentaires d'un package publié sur le portail.
- D'autre part pour spécifier des filtres de sécurité qui seront appliqués automatiquement aux requêtes effectuées en base de données.

Dans le cas de bases de données OLAP (cubes) telles que les Powercubes, la sécurité doit être gérée par le moteur OLAP. Etant donné que toutes les technologies OLAP ne sont pas capables de travailler avec des groupes et rôles Cognos, la mise en place de la sécurité peut s'avérer assez complexe.



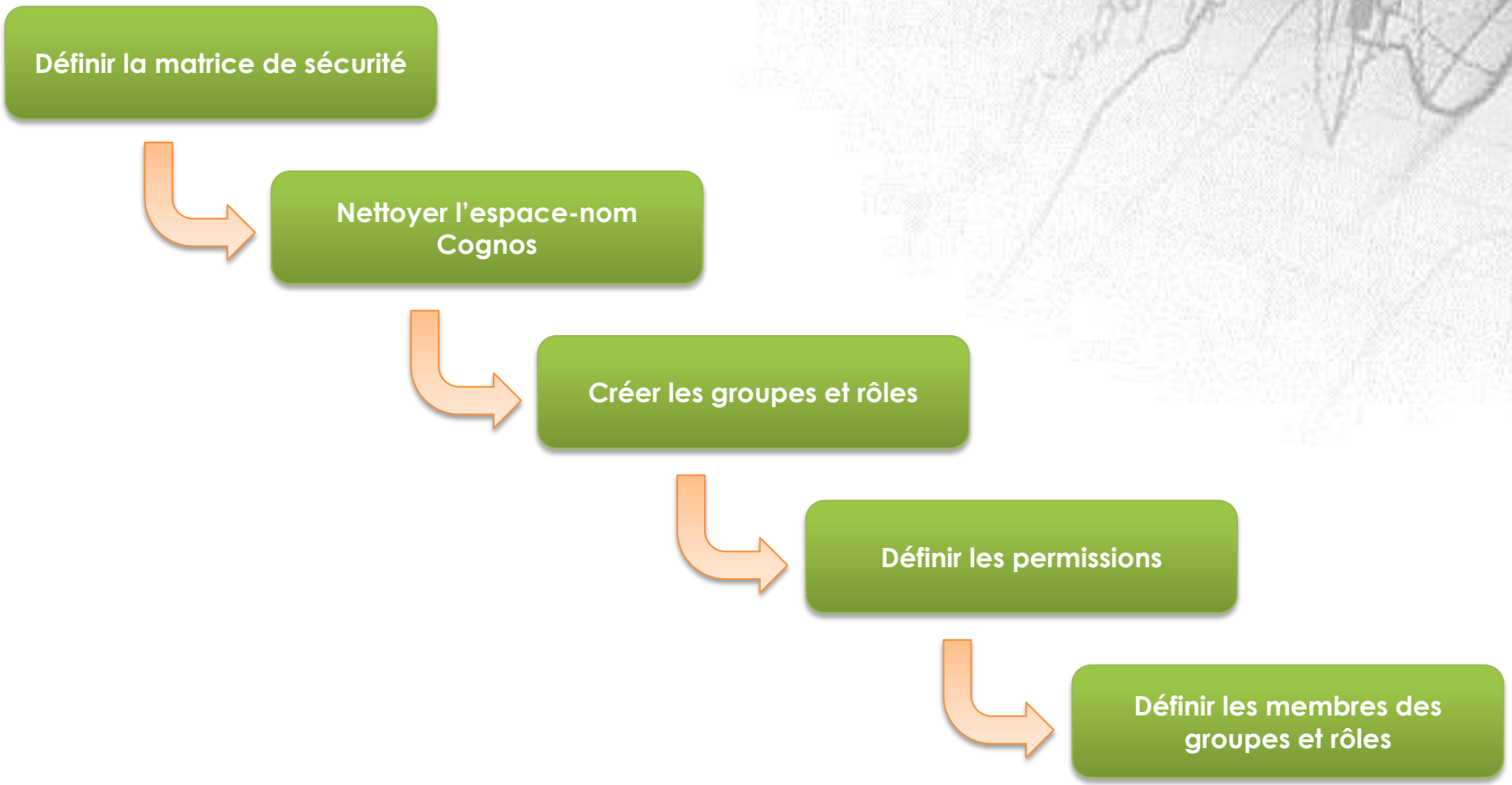


Bi2B

Pilot your performance

3 Modéliser la sécurité

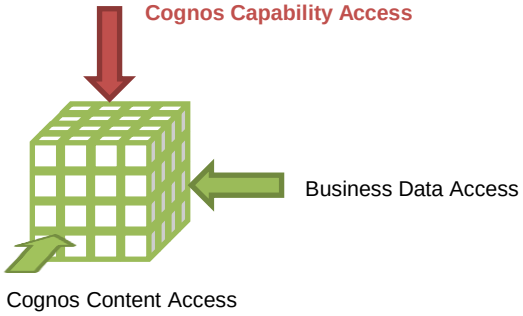
Modéliser la sécurité : Processus



Modéliser la sécurité : Définir la matrice de sécurité

L'axe de sécurité technique

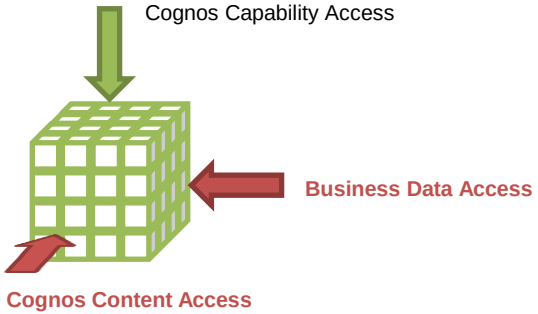
- L'axe de sécurité technique est utilisé pour définir les accès aux différentes fonctions du portail.
- Cet axe est symbolisé par l'utilisation de rôles.
- Généralement, les rôles fournis par défaut dans Cognos BI sont considérés comme suffisants et utilisés tels quels. Dans tous les cas, il est plutôt recommandé de commencer avec ces rôles et d'en ajouter si nécessaire plutôt que de repartir à zéro.
- Etant donné que l'accès aux fonctions détermine le type de licence consommé par les utilisateurs, cet axe de sécurité est généralement maintenu par les équipes informatique.



Modéliser la sécurité : Définir la matrice de sécurité

Le ou les axe(s) de sécurité métier

- Les axes métier sont utilisés pour gérer l'accès au contenu Cognos et aux données de l'entreprise.
- Ces axes sont symbolisés par l'utilisation de groupes.
- Etant donné que les utilisateurs peuvent être mutés voire quitter l'entreprise, il est fortement conseillé de concevoir la liste des groupes de manière à pouvoir gérer l'intégralité des utilisateurs, même si certains groupes ne se retrouvent qu'avec un seul membre. Cela permet d'assurer une bonne stabilité de la sécurité et facilite grandement la maintenance.
- Dans le choix du découpage de la sécurité, la stabilité de ce dernier dans le temps doit être privilégiée afin de faciliter la maintenance.

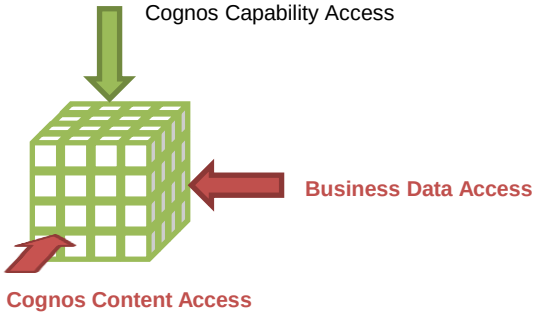


Modéliser la sécurité : Définir la matrice de sécurité

Le ou les axe(s) de sécurité métier -suite-

- Etant donné que les objets à sécuriser sont souvent directement reliés à l'organisation de l'entreprise, les axes de sécurité métiers reprennent fréquemment la même organisation, comme, par exemple, un découpage par entité régionale ou encore par position hiérarchique.

- Un autre aspect à prendre en compte lors de la définition des axes de sécurité métier est l'organisation des dossiers publics qui sera adoptée dans Cognos Connection. La maintenance peut être grandement simplifiée en adoptant des découpages proches de cette organisation, en limitant le nombre d'objets à gérer par la suite pour la définition des permissions.



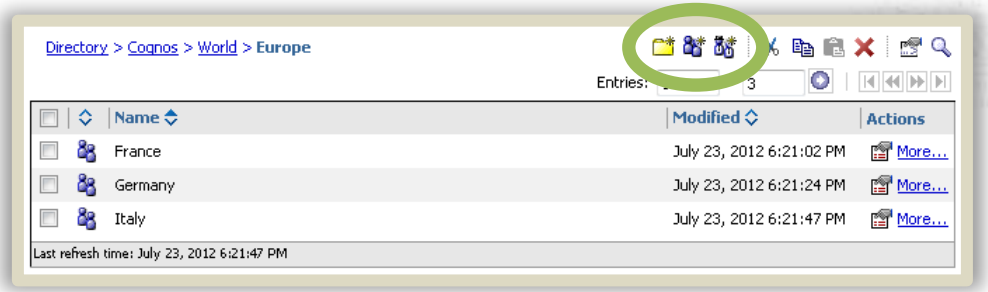
Modéliser la sécurité : Nettoyer l'espace-nom Cognos

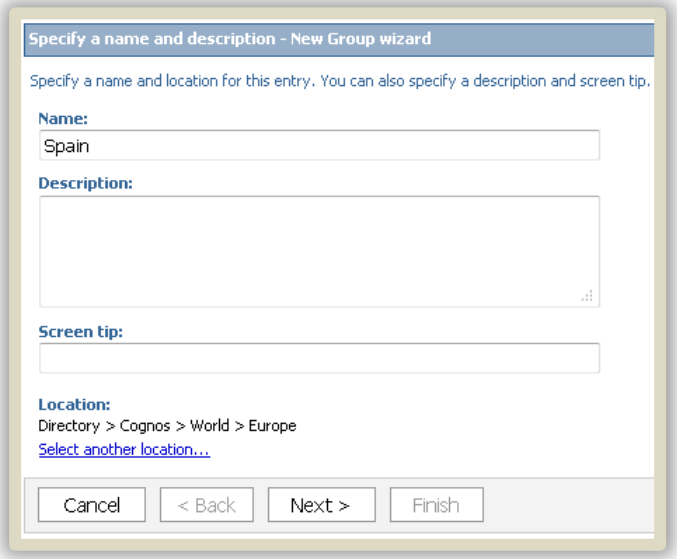
Avant d'implémenter la sécurité précédemment définie et dans le cas d'une installation nouvelle de Cognos BI, il est nécessaire de procéder à un nettoyage de la sécurité définie par défaut afin d'éviter les failles de sécurité.

Le nettoyage se compose des étapes suivantes :

- S'assurer qu'il y ait au moins un utilisateur nommé (non anonyme) membre du groupe "Administrateurs Système ".
- Vérifier l'ensemble des membres des rôles Cognos et supprimer systématiquement, lorsqu'ils sont présents, les membres "Tous les utilisateurs authentifiés", "Tous" et "Anonyme".
- Dans les propriétés de la racine des dossiers publics, vérifier qu'aucun des objets "Tous les utilisateurs authentifiés", "Tous" et "Anonyme" n'a de permission définie.

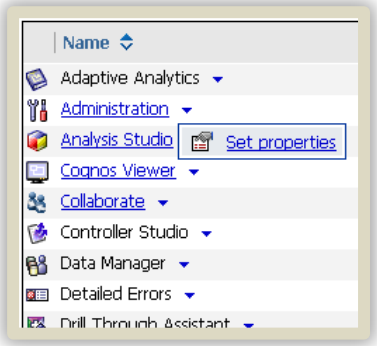
Modéliser la sécurité : Créer les groupes et rôles

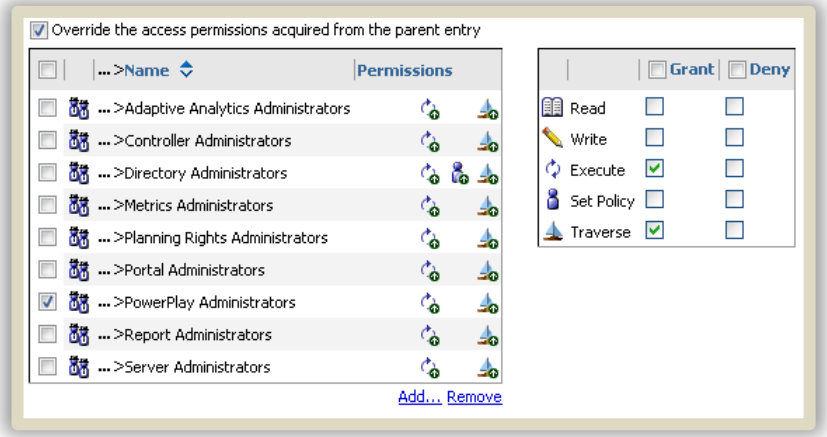




- Les groupes et rôles définis dans la matrice de sécurité doivent être créés dans l'espace-nom local ("Cognos").
- L'objectif dans cette étape est de n'avoir à terme plus que des groupes et des rôles provenant de l'espace-nom local à manipuler lors de la définition des permissions sur les objets Cognos, ce qui facilite la maintenance et la stabilité de la sécurité dans le temps.
- Il est possible d'organiser les groupes et les rôles dans une arborescence de dossiers pour plus de lisibilité.
- La création des groupes et des rôles s'effectue dans l'interface Cognos Administration.

Modéliser la sécurité : Définir les permissions

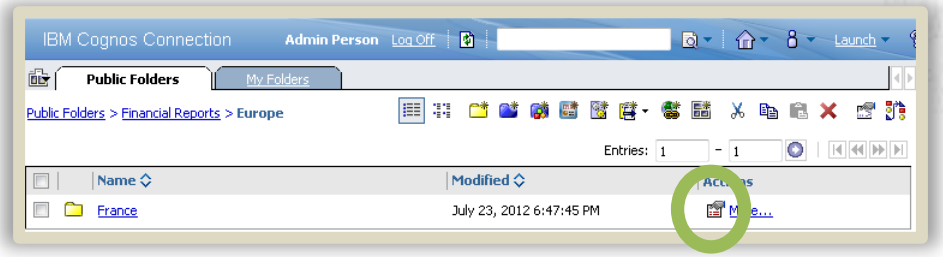


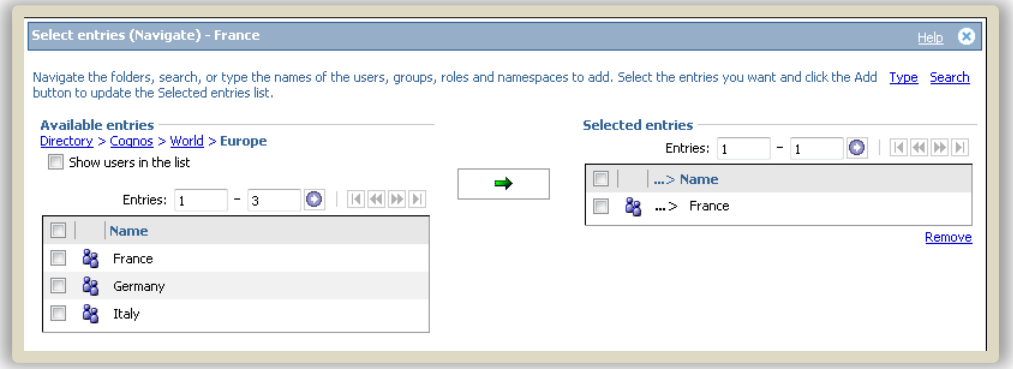


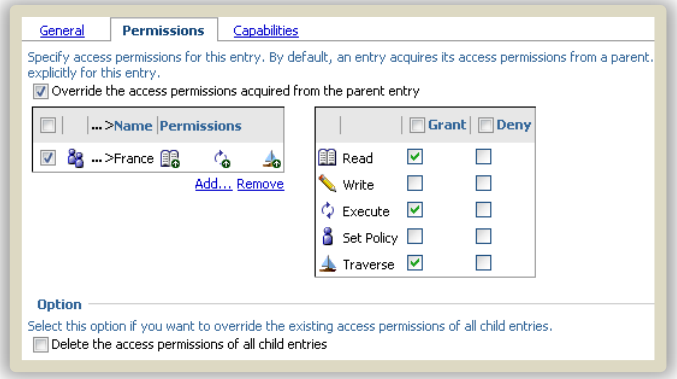
Permissions sur les fonctions

- Chaque rôle de l'axe de sécurité technique doit posséder une permission d'exécution sur les fonctions qui lui sont attribuées.
- La gestion des permissions sur les fonctions est effectuée via l'interface Cognos Administration.
- S'il a été choisi de conserver l'axe de sécurité technique défini par défaut avec l'installation de Cognos BI, cette étape est donc automatiquement réalisée lors de l'initialisation du portail.

Modéliser la sécurité : Définir les permissions



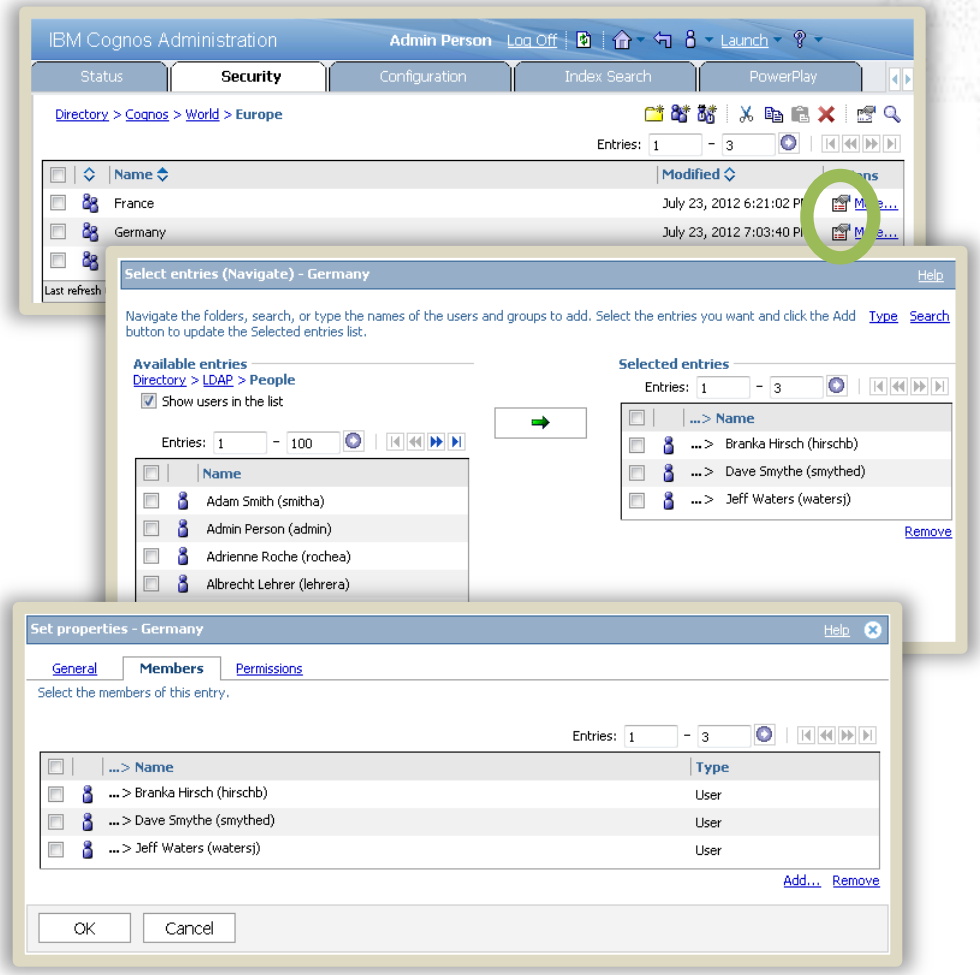




Permissions des dossiers publics

- Chaque groupe des axes de sécurité métier doit posséder les permissions sur les objets qui lui ont été rattachés.
- L'utilisation de l'héritage des permissions permet de limiter le nombre d'objets à éditer.
- Par commodité, les permissions ne sont en général définies que sur les dossiers, qui sont des objets beaucoup plus stables dans le temps que les objets de reporting.
- Il est fortement recommandé de ne jamais utiliser des groupes, rôles ou comptes provenant d'un espace-nom externe durant cette étape car cela rend les permissions quasiment impossible à maintenir proprement.

Modéliser la sécurité : Définir les membres des groupes et rôles



- Cette étape de modélisation de la sécurité est normalement la seule où des objets provenant d'un espace-nom externe sont référencés directement.
- Editer chaque groupe et rôle créé précédemment et ajouter les comptes utilisateurs en tant que membres, selon les droits à mettre en place.

Bi2B

Pilot your performance

4 Maintenance

Maintenance : Maintenance classique

Le processus de définition de la sécurité explicité précédemment permet une maintenance simple de l'environnement Cognos BI, où les tâches principales sont réduites aux suivantes :

- Ajouter et supprimer des membres aux groupes et rôles Cognos afin de refléter les évolutions sur les droits utilisateurs.
- Maintenir les permissions sur les nouveaux dossiers créés dans les dossiers publics, ce qui est simplifié en tirant parti de l'héritage naturel de permissions des objets parents envers leurs descendants.
- Programmer des tâches de maintenances à intervalles réguliers afin de nettoyer le content store des objets obsolètes dans les espaces-noms externes (les références à des objets supprimés dans un espace-nom externe ne sont pas supprimées automatiquement dans Cognos)
- De temps à autre, ajouter un ou plusieurs groupes de sécurité afin de refléter les évolutions des axes de sécurité métier et définir leurs permissions sur les objets concernés dans les dossiers publics.

Maintenance : Audit de la sécurité & BSL Security Manager

Audit de la sécurité

Une base de donnée d'audit peut être paramétrée dans Cognos Connection; elle sera automatiquement renseignée avec l'activité du portail. Des packages d'audit ainsi que divers rapports fournis par l'éditeur sont disponibles et permettent d'analyser ces données.

A noter que la finesse des données d'audit dépend du niveau de logging défini pour chaque sous-service de Cognos, dans Cognos Administration.

BSL Security Manager

BSL Security Manager est un logiciel tiers qui peut être couplé à un portail Cognos. Il est développé par BSL Consulting afin de répondre aux besoins suivants :

- Fournir une interface de gestion de la sécurité plus naturelle et ergonomique.
- Permettre une délégation de la gestion de la sécurité à des administrateurs métiers.
- Fournir une vision en temps réel des licences Cognos consommées.
- Permettre un reporting efficace des droits définis pour chaque utilisateur.