UNIVERSITÉ DE NANTES

MIAGE NANTES

Gestion d’un carnet de contact et d’un calendrier d’entreprise

Sécurité du SI

TP

Maxime Henaff

Lucas Détré

1. Introduction

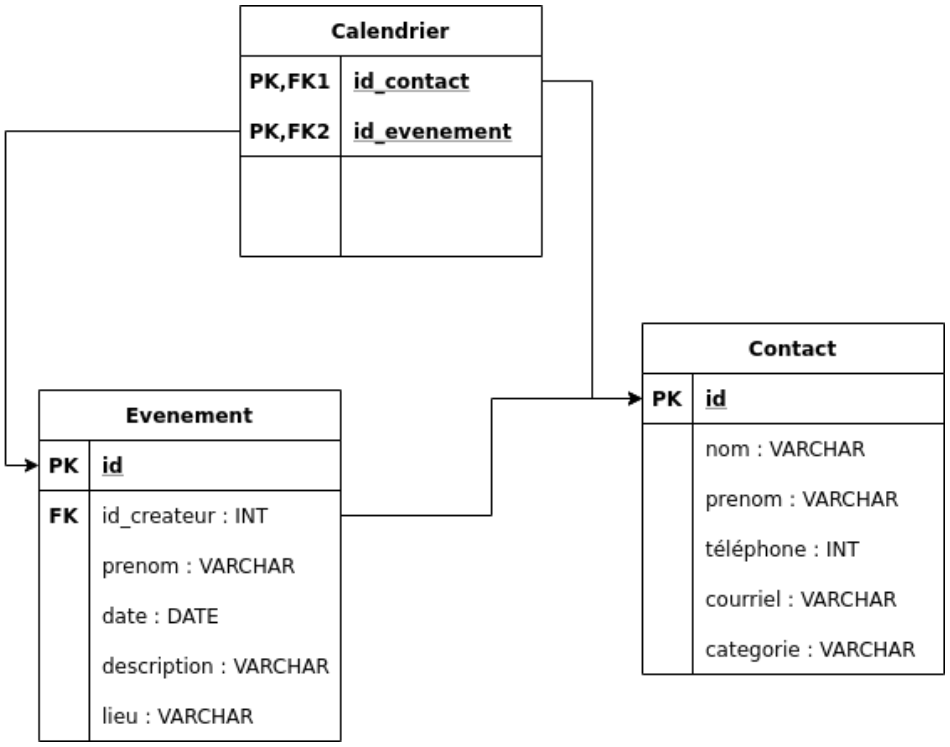
Pour ce projet nous avons choisi d'implémenter un système de calendrier d'entreprise complet, comprenant à la fois la gestion des événements, la gestion du calendrier et la gestion des contacts.

Ce système nécessite des droits d'accès particuliers afin de permettre une notion d'imperméabilité des données. En effet, il ne semble pas pertinent de permettre à des clients de mettre à jour les données de contact de leurs interlocuteurs potentiels. De la même façon, il n'est pas sérieux de permettre aux commerciaux de supprimer des événements auxquels ils ne sont même pas conviés.

Cette politique de contrôle d'accès a pour visée d'empêcher les actions malveillantes ou non intentionnelles des utilisateurs du système en ne leur accordant des privilèges que sur un certain nombre de données bien délimité.

Ce rapport a pour objectif de décrire le système que nous avons mis en place ainsi que les différents éléments qui composent la politique de sécurité. Nous parlerons des tables, des rôles ainsi que des limitations sur les différents privilèges grâce aux Virtual Private Databases (VPD) d'Oracle.

2. Description des tables



a. Table Contact

La table Contact a pour but de référencer les différentes personnes utilisant le calendrier partagé ainsi que leurs informations de contact (numéro de téléphone, adresse de courriel). Ces personnes sont catégorisées en fonction de leur rôle dans l'organisation (Commercial, Client, Informaticien).

b. Table Evenement

La table Événement permet de définir des événements (date, heure, lieu, description…). Chaque événement est créé par un contact (id_createur) qui aura alors des droits particuliers sur celui-ci.

c. Table Calendrier

La table calendrier permet de lier les contacts aux événements. Cela permet de pallier la contrainte de la table événements qui ne prend pas en compte la liste des participants à un événements.

En filtrant sur un événement donné, nous obtenons la liste des participants à cet événement. A l'inverse, en filtrant sur un contact, nous obtenons l'ensemble des événements auxquels ce contact est ou a été convié.

d. Vue d'ensemble

En plus des différentes tables décrites ci-dessus, nous avons mis en place une vue d'ensemble qui permet de regrouper les informations de manière plus compréhensible et globale. Cette vue consiste à la fusion du calendrier avec, à la fois, les informations des contacts et les informations des événements. Le résultat est trié sur les événements afin de pouvoir identifier rapidement les différents participants d'un événement et d'accéder aux détails de cet événement en une seule requête.

3. Description des rôles

Afin de structurer les différents privilèges des utilisateurs nous avons mis en place différents rôles correspondant à la fonction des différents acteurs de l'entreprise. Les utilisateurs ayant accès au système informatique peuvent être rangés en 4 catégories de rôles :

a. Les clients

Rôle le plus restrictif, un client ne possède que des droits en lecture sur les différentes tables. De plus, il ne peut lire que les données qui le concerne directement, à savoir : ses informations de contact, ses événements et son calendrier d'événement.

b. Les informaticiens

Ce rôle inclut les différents privilèges donnés aux clients auxquels s'ajoutent la mise à jour sur la table contact, l'insertion sur les tables calendrier et évènement afin de pouvoir créer des réunions, et la suppression sur la table réunion pour les annuler.

c. Les commerciaux

Ce rôle permet les mêmes actions que le rôle informaticien tout en permettant des actions supplémentaires. En effet, le métier de commercial peut nécessiter d'ajouter des nouveaux contacts lors de la prospection de clients. Le rôle commercial inclut ce droit. De plus, le commercial peut accéder à la vue d'ensemble du calendrier en lecture car il peut avoir besoin d'une vue globale des différentes réunions pour éviter de trop solliciter certains clients par exemple.

d. Les administrateurs

Ce rôle, attribué à un informaticien de l'entreprise, permet d'avoir les pleins droits sur toutes les tables et aussi d'accéder à la vue d'ensemble de l'organisation. C'est lui qui est sollicité par les différents acteurs pour effectuer les opérations exceptionnelles qui ne sont pas prévues par les rôles.

4. Les restrictions supplémentaires (VPD)

Les rôles ne sont pas suffisants pour assurer la bonne confidentialité des données. Par exemple, le client ne devrait pas pouvoir accéder à l'ensemble des contacts de l'entreprise, seulement le sien.

Nous avons par conséquent mis en place des VPD dans notre système afin de limiter les différentes requêtes des utilisateurs. Au total nous avons cinq VPD actives dans notre système. Ces VPD se basent toutes sur le rôle de l'utilisateur afin de garder un ensemble simple et cohérent.

Nous résumons ici les limitations imposées par chacune des VPD, par défaut, si un rôle n'est pas mentionné, c'est qu'il n'est pas limité par la VPD en question. Les informations sont à ajouter aux restrictions données par les différents rôles.

Ainsi, la première VPD limite la **sélection** sur les **contacts**. Les clients ne peuvent se sélectionner qu'eux-mêmes et les informaticiens ne peuvent pas sélectionner les clients.

Une seconde VPD va limiter la **mise à jour** des **contacts**. L'informaticien ne peut mettre à jour que sa propre fiche de contact alors que le commercial peut mettre à jour sa propre fiche et les fiches clients.

La troisième VPD limite la **sélection** sur le **calendrier**. Les clients et les informaticiens ne peuvent voir que leur propre calendrier (la liste des événements auxquels ils sont conviés).

La quatrième VPD limite la **suppression** dans le **calendrier**. Les informaticiens ne peuvent ainsi que supprimer leur propre participation à une réunion.

La cinquième et dernière VPD permet de limiter la **sélection** sur la liste des **événements**. Ainsi, les clients ne peuvent accéder qu'aux détails des événements présents dans leur calendrier. Les informaticiens et les commerciaux quant à eux peuvent accéder aux détails des événements présents dans leurs calendriers ainsi qu'aux détails des événements qu'ils ont créés. Cette VPD intègre ainsi une **contrainte sur le contenu d'une autre table.**

5. Synthèse de la politique de sécurité

L'ensemble des accès donnés aux différents rôles et des limitations mises en place grâce aux VPD sont synthétisées dans le tableau ci-dessous :

Rôle \ Table	Contact	Calendrier	Evenement	Vue (jointure des 3 tables)
Client	**Sélection** sur son identifiant *VPD1* *F1*	**Sélection** sur son identifiant *VPD3* *F3*	**Sélection** sur les événements présents dans son calendrier *VPD5* *F5*	**Aucun droit**
Informaticien	**Sélection** sur commerciaux et informaticiens *VPD1* *F1* **Mise à jour** sur son identifiant *VPD2* *F2*	**Sélection** sur son identifiant *VPD3* *F3* **Suppression** sur son identifiant *VPD4* *F4* **Insertion**	**Sélection** sur les événements présents dans son calendrier, ou créés *VPD5* *F5* **Insertion**	**Aucun droit**
Commercial	**Sélection** *VPD1* *F1* **Mise à jour** sur son identifiant et sur les clients *VPD2* *F2* **Insertion**	**Sélection** *VPD3* *F3* **Suppression** *VPD4* *F4* **Insertion**	**Sélection** sur les événements présents dans son calendrier, ou créés *VPD5* *F5* **Insertion**	**Sélection**
Admin	**Pleins droits**	**Pleins droits**	**Pleins droits**	**Sélection**

6. Retours sur la mise en place de cette politique de sécurité

Ce projet a été pour nous l'occasion d'éprouver les capacités d'un certain nombre de fonctionnalités de contrôle d'accès d'Oracle. Les VPD nous ont permis de définir pour **une même table** plusieurs **types de contrôle sur différents types d'action**. Les VPD nous ont permis également de **conditionner** la contrainte **sur le contenu d'une autre table** à l'aide de **requêtes imbriquées** et d'ainsi faire preuve d'une plus grande précision dans notre politique de contrôle d'accès.

Toutefois, nous avons également pu faire face à un certain nombre de problèmes ou blocages liés à ces **VPD** notamment sur les **boucles** qui peuvent êtres générées à cause des VPD. Au départ nous souhaitions conditionner la sélection sur calendrier au contenu de la table événement (voir le contenu du calendrier pour les événements que l'utilisateur a créé par exemple). Le problème était que la sélection sur la table événement était elle aussi conditionnée au contenu de la table calendrier. Cela créait une boucle infinie qui générait des erreurs lors de l'accès au système. Nous avons résolu ce problème simplement en cassant la boucle grâce à une modification de la politique de sécurité pour la table calendrier.

Nous avons également fait face à un **problème d'héritage de rôle**. En effet, certains rôles définis plus haut sont plus restrictifs que d'autres et peuvent fonctionnellement s'imbriquer les uns dans les autres.
Ainsi, le rôle Commercial par exemple est simplement un rôle Informaticien auquel on ajoute le droit d'insertion sur la table contact et le droit de lecture sur la vue d'ensemble du système. De la même façon, tous les rôles "héritent" du rôle client ayant uniquement accès aux tables en lecture.
Dans le faits, l'héritage entre les rôles (affectation d'un rôle à un autre rôle) ne fonctionnait pas pour nous, ni pour nos camarades à notre connaissance. Nous nous sommes résolus à supprimer cet héritage et à dupliquer l'affectation des privilèges communs à chacun des rôles.

Nous avons fait le choix de créer un script (*lancement_demo.sql*) qui permet de rafraîchir les données (destruction puis génération de la base, des données, des vues, des rôles, des contextes et des vpd) puis de se connecter en tant que différents types d'utilisateurs pour tester notre politique de contrôle d'accès. Ce script permet, pas à pas, de vérifier le bon fonctionnement de notre base selon la politique définie dans ce rapport.