SÉCURITÉ DES BASES DE DONNÉES SOUS ORACLE

SÉCURITÉ DES DONNÉES

- La sécurité de l'information est vitale.
- Elle conditionne l'activité économique des entreprises et la confiance dans les organismes publics
- La divulgation volontaire ou accidentelle de données financières ou privées peut avoir des conséquences fâcheuses sur le plan
  - Economique, commercial et…juridique
  - 25 % des incidents sont le fait de personnels internes
  - 50 % sont consécutifs à des pertes ou des vols de matériels divers

SÉCURITÉ DES SI UNE AFFAIRE DE RISQUES

L 'analyse des risques conduit généralement à considérer 5 objectifs de sécurité de l'information

- **Sa confidentialité**
- **Son intégrité**
- **Son utilisation conforme aux règles**
- **Sa disponibilité**
- **La traçabilité de son utilisation**

CONFIDENTIALITÉ

Empêcher la consultation de données sensibles par des personnes non autorisées

- Qui a accès?
- Quels sont les mécanismes de contrôle d'accès ?
- Qui des utilisateurs à super privilèges ?

❑ Les données sont-elles protégées par du chiffrement:

- Lors de leur stockage ?
- Durant leurs mouvements ?
- …

INTÉGRITÉ

❑ Prévenir la modification des données par des personnes non autorisées

- ❑ Qui peut modifier l'information ?
- ❑ Quels contrôles sont en place pour limiter les accès ? Pour donner les accès ?
- ❑ Quels sont les mécanismes permettant de vérifier si l'information a été changée ?
- ❑ Quels moyens sont utilisés par les applications pour contrôler la cohérence des informations ?

❑• …

TRAÇABILITÉ / CONFORMITÉ

Permettre de garder la trace des actions effectuées sur les systèmes, à des fins de prévention, de dissuasion et d'audit des incidents

- ❑ **Qui a accédé ?**
- ❑ **Quelle information sur l'activité est capturée ?**
- ❑ **Comment sont protégés les référentiels d'audit ?**
- ❑ **Une exploitation systématique des audits est-elle en place ?**
- ❑ **…**

LA SÉCURITÉ DES BD

- Le piratage des BD est partout

→ trouver de nouvelles manières de sécuriser les données.

- La plupart des données sensibles sont stockées dans les SGBD
  - Oracle, Microsoft SQL Server, IBM DB2 ou Sybase
- Les SGBD, cibles favorits des criminels.

Exemple

- les attaques par injections SQL ont grimpé de 134 % en 2008
- plusieurs centaines de milliers par jour
- **60 % des entreprises sont à la traîne pour appliquer les patchs de sécurité**

LES HUIT ÉTAPES DE LA SÉCURISATION DES BD

1. Détection et reconnaissance
2. Évaluer les vulnérabilités des configurations
3. Renforcer la sécurité
4. Auditer les changements
5. Surveiller l'activité de la base de données (DAM)
6. Auditer
7. Authentification, contrôle des accès et gestion des habilitations
8. Cryptage

HUIT ETAPES DE SÉCURITÉ

1. **Détection et reconnaissance**

- **On ne sécurise que ce que l'on connaît.**
- **Disposer d'une bonne cartographie des ressources sensibles (instances de bases de données, données sensibles).**
- **Automatiser la reconnaissance car l'emplacement des données sensibles ne cesse de changer**
  - nouvelles applications ou applications modifiées,
  - fusions et acquisitions, etc.

HUIT ETAPES DE SÉCURITÉ

2. **Évaluer les vulnérabilités et les configurations**

- S'assurer de la sûreté et l'absence de failles
  - Vérifier la manière dont la base de données est installée dans le système d'exploitation
    - par exemple, les privilèges pour les fichiers et les exécutables de configuration de la base de données
  - Vérifier les options de configuration au sein de la base de données elle-même
    - par exemple, au bout de quel nombre d'échecs de connexion un compte finira par être verrouillé, ou quels privilèges ont été affectés aux tables critiques).
  - vérifier que les versions de base de données que vous exécutez ne comportent pas de vulnérabilités connues.

HUIT ETAPES DE SÉCURITÉ

3. Renforcer la sécurité

- **L'évaluation des vulnérabilités donne souvent lieu à un ensemble de préconisations spécifiques.**
- **C'est la première étape dans le renforcement de la sécurité de la base de données.**
- **Ce renforcement comporte d'autres éléments qui impliquent de supprimer toutes les fonctions et toutes les options inutilisées**

HUIT ETAPES DE SÉCURITÉ

4. Auditer les changements

- **Une fois avoir une configuration renforcée (« gold »), il faut surveiller en permanence la sécurité de la BD**
- **Utiliser des outils d'audit**
  - Comparent des instantanés des configurations
    - au niveau du système d'exploitation,
    - Au niveau de la BD
  - Alertent immédiatement l'administrateur lorsqu'intervient un changement susceptible d'affecter la sécurité de la base de données

HUIT ETAPES DE SÉCURITÉ

5. Surveiller l'activité de la base de données (Database Monitoring:DAM)

- La surveillance en temps réel de l'activité de la base de données est fondamentale pour limiter les risques
- Permet de détecter immédiatement les intrusions et les mauvaises utilisations
- La DAM peut ainsi vous alerter sur des comportements inhabituels d'accès, indices potentiels d'une attaque par injection SQL, de modifications non autorisées de données financières, de hausse du niveau des privilèges sur des comptes ou de modifications de la configuration exécutées via des commandes SQL.
- Certaines technologies de DAM proposent une surveillance des couches applicatives, ce qui vous permet de détecter les fraudes effectuées via des applications multiniveau comme PeopleSoft, SAP et Oracle e-Business Suite, plutôt que via des connexions directes à la base de données

HUIT ETAPES DE SÉCURITÉ

6. Auditer

- Des traces de contrôle sécurisées et incontestables doivent être générées et maintenues pour toutes les activités de base de données qui ont un impact sur la sécurité, sur l'intégrité des données ou sur la consultation de données sensibles
- La plupart des organisations recourent à une forme ou à une autre d'audit manuel, en utilisant les possibilités natives de journalisation offertes par leur base de données

→ Complexité, Coût opérationnels

HUIT ETAPES DE SÉCURITÉ

6. Auditer

- Complexité, Coût opérationnels
- mobilisation excessive des temps système
- non-étanchéité des responsabilités (il est facile aux administrateurs de base de données d'altérer les journaux)
- besoin d'acquérir et de gérer des capacités de stockage considérables pour traiter les quantités massives d'informations de transactions non filtrées.

Heureusement, une nouvelle classe de solutions DAM a fait son apparition.

Ces solutions permettent d'effectuer des audits granulaires

- indépendants des systèmes de bases de données
- avec un impact minimal sur les performances tout en réduisant les coûts opérationnels, via l'automatisation, la centralisation des règles SGBD et des référentiels d'audit, le filtrage et la compression.

HUIT ETAPES DE SÉCURITÉ

7. Authentification, contrôle des accès et gestion des habilitations

Les données et les utilisateurs ne sont pas tous créés égaux.

- L'ADM doit
  - Authentifier les utilisateurs
  - Garantir la responsabilité plénière de chacun de ces utilisateurs
  - Gérer les privilèges afin de limiter l'accès aux données.
- Il doit veiller au respect de ces privilèges, même en ce qui concerne les utilisateurs de la base de données disposant du maximum de privilèges.
- Il doit également prévoir une procédure formelle d'audit dans laquelle il examinera régulièrement des rapports d'habilitation (aussi appelés rapports d'attestations des droits utilisateurs).

HUIT ETAPES DE SÉCURITÉ

8. Cryptage

- Le cryptage rend impossibles à lire les données sensibles, ce qui empêche les attaquants d'accéder à des données non autorisées depuis l'extérieur de la base.
- Le cryptage doit intervenir à plusieurs niveaux.
- Les données en transit doivent être cryptées pour empêcher toute indiscrétion au niveau réseau et tout accès lors de l'envoi des données au client de base de données.
- Mais les données résidentes doivent elles aussi être cryptées, pour empêcher leur extraction par un attaquant, même si ce dernier parvient à accéder aux fichiers.

PLACE DE LA SÉCURITÉ DES BD DANS LE SI

Budgets Sécurité vont d'abord

- **à l'achat de système de sécurité (firewalls, IDS, ...)**
- **à la formation**
- **à la sécurisation des applications**

→ le SGBD est le parent pauvre de la sécurité

CONTRAINTES SUR LA SÉCURITÉ

Rôle du DBA

- maintenir le SGBD
- gérer les comptes, les applications, ...
- pas de formation sécurité : ne peut pas « imaginer » les attaques possibles

Mises à jour des systèmes

- 80% des serveurs de BD meurent avec le système et le SGBD initial: (Informix 7.2, Oracle 7.2, ...)
- Marchent encore, mais pas de patchs
- Conséquence : de nombreuses failles système et applicatives ne sont JAMAIS corrigées

Criticité des applications : Arrêts impossibles

- La sécurité passe en dernier

CONTRAINTES SUR LA SÉCURITÉ

Le SGBD est souvent un composant

- installé par ou avec un logiciel tiers
  - ERP (SAP, Lawson) DataMining
  - Gestion de parc (SMS, ...)
  - Pour SQL Server : 223 Applications recensées en 2003
- Géré via ce logiciel tiers
- Dans une version limitée
- Dans un mode d'installation par défaut

→Sa configuration de sécurité est bien souvent encore plus obscure !

- personne ne veut/peut prendre la responsabilité de modifier le paramétrage

TYPES D'ATTAQUES

Attaques sur le SGBD lui même

- failles connues classiques (buffer overflows, bugs d'autentification, injections SQL dans les procédures stockées, ...)
- failles dans les applications associées: serveurs Web d'administration, applications Web, serveurs LDAP, démons snmp, programmes setuid root installés par le SGBD, ...

Mauvaises configurations

- modes d'authentification dégradés (.rhosts, OPS$... ...)
- mots de passe par défaut

Interception de mots de passe

- par écoute du réseau
- par lecture de fichiers de configuration sur disque

TYPES D'ATTAQUES

Attaques sur les applicatifs

- Injection SQL sur les applications Web
- détournement des requêtes effectuées par un ERP
- autorisations trop larges

Attaques sur l'OS via le SGBD

- écriture/lecture de fichiers, exécution de commandes
  - la base de données tourne avec des privilèges différents
  - contournement de la politique de sécurité
    - 'safe_mode' de PHP
    - chroot
- critique chez les hébergeurs Web mutualisés
  - load data infile '/web/data/a/anotheruser/db.param' INTO hack ...

FAILLES : COMPTES ET MOTS DE PASSES

- Mots de passe par défaut

Oracle 8 : SYSTEM/MANAGER et SYS/CHANGE_ON_INSTALL ?

  - 80% des installations ne les changent pas
  - Permet d'accéder à tous l'environnement à distance
  - Permet d'écrire des procédures stockées appelant le système

- Mots de passe des comptes applicatifs
  - appli/appli
- Comptes par défaut installés par Oracle ...
- Possession des tables, privilèges DBA attribués abusivement, ..

VULNÉRABILITÉ SOUS ORACLE

Multiples vulnérabilités découvertes en permanence

  - 25 vulnérabilités en un seul jour
  - Principalement liées aux extensions (mod_plsql, ...)
  - Beaucoup de problèmes liées aux procédures stockées nécessaires au fonctionnement du système...
  - Exemple: gain des privilèges via le compte CTXSYS

Produit difficile à patcher

La suppression des comptes par défaut, une installation minimalisée permet de réduire beaucoup de problèmes

VULNÉRABILITÉ SOUS ORACLE

Problème le plus évident: utilisation d'une fonctionnalité dangereuse: « remote_os_authent»

- **remote_os_authent : permet à un utilisateur de se connecter en utilisant son compte OS.**
- **Oracle fait confiance au client pour authentifier l'utilisateur**

Si le réseau n'est pas sécurisé, une tiers personne pourra intercepter la communication et se connecte.

SÉCURITÉ EN ENVIRONNEMENT WEB

Typiquement utilisé pour « dynamiser » les sites Web

- **Contenu mobile (publications)**
- **Commerce électronique / Notion de compte**

Risques principaux sur la base de données :

Injection SQL

- **Compromission de la base depuis une autre machine compromise**
  - Les bases de données sont souvent moins durcies
    - Comptes oracle/oracle
    - Systèmes d'exploitation non configurés pour la sécurité
- **Déni de service**

ATTAQUE PAR INJECTION SQL?

- Populaire sur les applications web
- Les applications web donne la possibilité de saisie d'information via des formulaires
- Souvent cette entrée d'utilisateur est utilisé littéralement dans la construction d'une requête SQL soumise à une base de données.

Exemple

- SELECT * FROM Produit WHERE Nom='Nom produit saisie';

❑ Une attaque par injection SQL consiste à placer des instructions SQL dans la saisie de l'utilisateur

EXEMPLES (WIKIPÉDIA)

- En février 2002, Jeremiah Jacks révèle une faille de sécurité sur le site de Guess.com exploitable par une attaque d'injection SQL et permettant **d'obtenir les coordonnées de plus de 200 000 personnes y compris leurs numéros de cartes de crédit avec la date d'expiration**
- Le 1er novembre 2005, un jeune pirate utilise l'injection SQL pour s'introduire dans le site d'information taïwanais consacrée à la sécurité informatique et **s'empare des données de la base client**
- Le 29 mars 2006, un pirate s'attaque par une injection SQL au site officiel du tourisme indien appartenant au gouvernement3.
- En janvier 2008, **des dizaines de milliers de PC sont infectées par une injection SQL automatique** exploitant une faille de sécurité de Microsoft SQL Server.
- Le 13 avril 2008 survient le **vol de 10 597 numéros de sécurité social américains**
- Le 17 août 2009, le département de la justice américaine identifie l'américain Albert Gonzales et deux russes comme les auteurs du **vol de 130 millions de numéros de cartes de crédit grâce à une attaque par injection SQL**

EXEMPLES (WIKIPÉDIA)

- Le 24 juillet 2010, des attaques par injection SQL simultanées de Japon et de Chine parviennent a pénétrer la société NeoBeat qui gère des supermarchés sur internet et **volent 12 191 données de cartes bancaires**.
- Le 8 novembre 2010, un pirate roumain appelé TinKode utilise une attaque par injection SQL pour **paralyser le site de la Royal Navy en Angleterre**
- Le 11 avril 2011, l'ensemble du réseau Barracuda est victime d'une attaque par injection SQL. **Identifiants et adresses emails des employés sont détournés**
- Le 1er juin 2011, le groupe appelé LulzSec est accusé d'une attaque par injection SQL contre le site de Sony. Au moins **1 million de clients se font voler coupons, clés d'activation et mot de passe**
- En juillet 2012, Yahoo rapporte le **vol de données de plus de 450 000 clients**.
- Le 16 janvier 2014, Orange France est victime d'une attaque, **les pirates dérobent noms, prénoms, adresses, emails et numéros de téléphone de 3 % de la clientèle de l'opérateur soit 800 000 personnes13**

EXEMPLE D'UNE ATTAQUE PAR INJECTION SQL

Recherche d'un produit:

yyyy' OR 'x' = 'x

Cette entrée est mis directement dans l'instruction SQL dans l'application Web:

- $query = "SELECT * FROM Produit WHERE Nom = '" . $_POST['prod_search'] . "'";

La requete suivante sera créée:

- SELECT * FROM Produit WHERE Nom = 'yyyy' OR 'x' = 'x'
- L'attaquant a maintenant réussi , il a la base de données entière à retourner.

PLUS GRAVE

Si le hacker touche à la table utilisateur

SELECT * FROM users WHERE name='admin' and

password='xxx' or 'x'='x'

Il récupère la table Users entière!!!!

AUTRES EXEMPLES

Qu'est-ce qui se passe si le hacker a saisis :

- blabla'; DROP TABLE Produit; --

Résultat en SQL:

- SELECT * FROM Produit WHERE Nom = 'blabla'; DROP TABLE Produit; --'
- Notons comment le commentaire (--) élimine l'apostrophe finale

Peut causer la suppression de toute la base de données

- Dépend de la connaissance du nom de la table
- Ceci est parfois exposé à l'utilisateur dans le code de débogage appelé lors d'une erreur de base de données
- Il faut Utiliser les noms de tables non-évidentes, ne jamais les exposer à l'utilisateur

Habituellement la destruction de données n'est pas votre plus grande peur

- faible motivation économique
- Il faut faire des sauvegardes périodiques

AUTRES POSSIBILITÉ D'ATTAQUE

En utilisant des injections SQL, les hackers peuvent:

- **Ajouter des données dans la BD**
  - Se fait en ajoutant un ordre INSERT INTO dans la requête SQL
  - Pourrait être ambarrassant de se retrouver entrain de vendre des produits non désirés sur un site d'e-commerce : armes, produits interdits, etc.
- **Modifier des données présentes dans la BD**
  - Se fait par l'injection de l'ordre : UPDATE
  - Peut engendrer des incohérences dans la BD
  - Désinformation
- **Accéder à un autre système par l'obtention du mot de son passe**

PROTECTION CONTRE LES INJECTIONS

Utiliser les fonctions prévues pour protéger les chaines

- **De nombreuses attaques peuvent être contrecarrées en modidfiant les apostrophe**
  - ' → \' et " → \"
  - mysql_real_escape_string() est la fonction préférée.

PROTECTION CONTRE LES INJECTIONS

Vérifier la syntaxe de la chaine entrée pour la valider

- **Plusieurs classes d'entrées ont des langages ou expressions régulières**
  - Addresses émails, dates, numéros de téléphone, etc.
  - Vérifier que l'entrée appartient au langage (expression régumlière)
  - Il faut exclure les appostrophes, les points-virgule, etc.

Limiter la taille des zones de saisie

- **Beaucoup d'injections SQL dépendent de la taille des zones de saisie**

AUTRES DÉFENSES

Parser la chaine de requêtes pour éliminer des combinaison de mots indésirables contenant des ordres SQL

- **INSERT, DROP, etc.**
- **Vérifier la syntaxe SQL pour voir que la chaine est valide ou non**

Limiter les autorisations de base de données et séparer les utilisateur

- **Si l'accès nécessite une lecture seulement, il faut se connecter avec un utilisateur ayant uniquement les privilèges SELECT**
- **Ne jamais se connecter comme DBA dans une application web**

AUTRES DÉFENSES

Configurer les rapports d'erreurs de la BD

- **Les messages d'erreurs par défaut donnent souvent des informations exploitables par les hackers (noms des tables, noms des attributs, etc.)**
- **Configurer le SGBD pour que ces informations ne soient jamais affichées à l'utilisateur**

ORACLE

- D'une manière générale, la gestion de la sécurité est le parent pauvre des administrateurs de système.
- Dès lors qu'un serveur héberge les données de l'entreprise, ce n'est plus une machine de test, sa sécurité doit être renforcée et faire l'objet d'une attention pointilleuse.

ORACLE DATABASE VAULT

Pourquoi faire ?

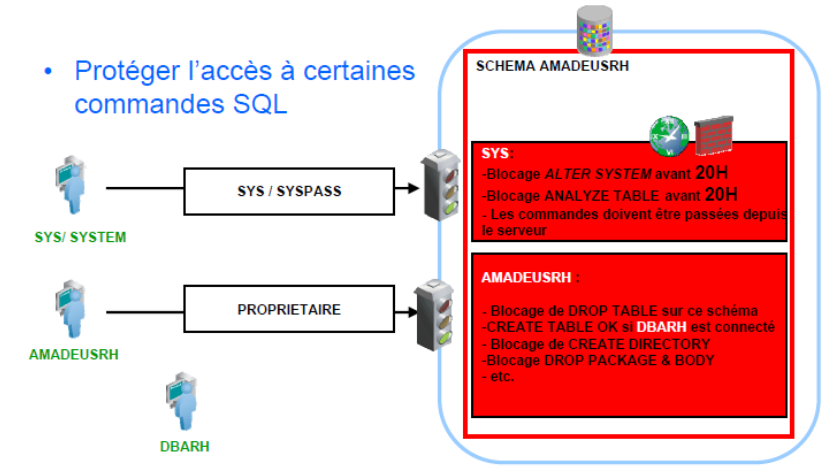
- Protéger les données des accès par les personnes disposant de privilèges exceptionnels
- …et n'ayant pas de droits d'accès octroyés par leur fonction dans l'entreprise

Bénéfices attendus

- Permettre aux responsables d'application de prendre des engagements quant à la sécurité de leurs données
- Garantir une séparation stricte des responsabilités

EXEMPLE DE SÉCURITÉ ORACLE

- Protéger l'accès à certaines commandes SQL



ORACLE AUDIT VAULT

Pourquoi faire ?

- Garder la trace de certaines actions effectuées sur les bases de données

Bénéfices attendus

- Progressivement mettre en place une architecture solide de règles d'audit des bases
- Collecter systématiquement en lieu sûr, les évènements produits par les sources d'audit
- Analyser les évènements remontés
- Faciliter la gestion du cycle de vie des données d'audit

ORACLE AUDIT VAULT

Deux types d'audit existent

❑Standard

- Pour auditer tout ce qui peut s'imaginer!
- Les ordres DDL et DML. A privilégier pour tout ce qui est DDL et utilisation de privilèges

❑*'Fine Grained'*

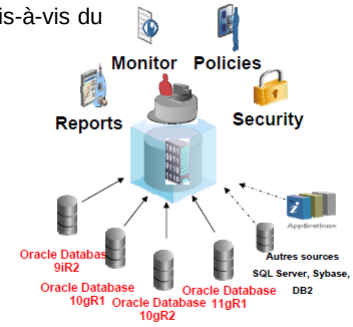
- *Permet de réduire la volumétrie de* l'audit en ciblant les conditions de déclenchement sur des conditions précises

❑ Ou stocker l'audit?

- Dans la base cible ou sur des fichiers externes

AUDITER LA BD

- Collecte & Consolidation les données d'Audit
  - Oracle 9i Release 2 et postérieures
  - Autres SGBD (SQLServer, Sybase, DB2)
- Définition des politiques d'Audit sur les bases cibles dans un référentiel central
- Provisionning des politiques d'Audit vers les cibles
- Comparaison des politiques mises en place vis-à-vis du référentiel
- Simplification du reporting pour conformité
  - • Etats prédéfinis
  - • Etats personnalisables
- Détecte et prévient les menaces internes
- Alertes d'Activité suspectes



EXEMPLE

Etats prédéfinis

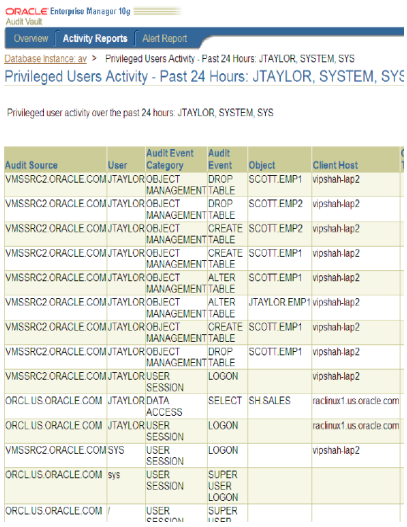
- **Activité des utilisateurs privilégiés**
- **Accès à des données sensibles**
- **Attribution de droits à des rôles**
- **Activité DDL**
- **Login/logout**

Etats liés aux utilisateurs

- **Quels utilisateurs privilégiés accèdent aux données financières ?**
- **Quelles données peuvent être accédées par un user 'A' dans différentes base de données ?**
- **Qui accède à des données sensibles ?**

Etats personnalisés

- **Oracle BI Publisher, Application**
- **Express, Outils Tiers**


ORACLE Enterprise Manager 10g
Audit Vault
Overview | Activity Reports | Alert Report
Database Instance: av > Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS
Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS
Privileged user activity over the past 24 hours: JTAYLOR, SYSTEM, SYS

Audit Source	User	Audit Event Category	Audit Event	Object	Client Host
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	JTAYLOR.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	JTAYLOR	DATA ACCESS	SELECT	SH.SALES	raclinux1.us.oracle.com
ORCL.US.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		raclinux1.us.oracle.com
VMSSRC2.ORACLE.COM	SYS	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	sys	USER SESSION	SUPER USER LOGON		
ORCL.US.ORACLE.COM	/	USER	SUPER		

ORACLE CHIFFREMENT

Pourquoi faire ?

- Protéger les données lors de leur transport
- Protéger les données lors de leur stockage

Bénéfices attendus

- Assurer la protection contre des attaques physiques sur les fichiers
- Protéger les flux réseau
- Se couvrir de la perte ou du vol de supports
- physiques

PROTÉGER LES FLUX *ORACLENET*

Chiffrement et scellement avec des algorithmes

- standard *(RC4, 3DES, AES & MD5, SHA-1)*

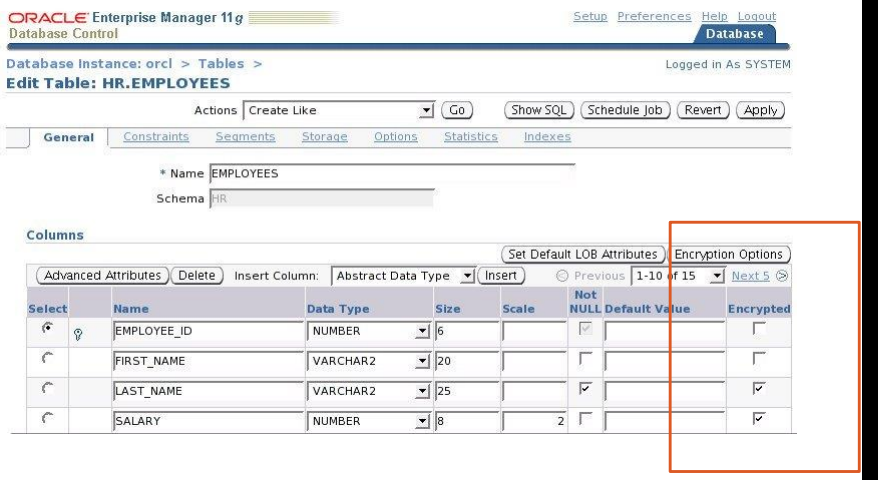
Chiffrement et scellement simple

- Paramétrage du réseau *OracleNet*
- Négociation des algorithmes au moment de la connexion

Utilisation de TCPS

- Paramétrage du réseau *OracleNet et utilisation de* certificats. SSL V2 / V3

EXEMPLE



OPTION AVANCÉE CHIFFREMENT DES TABLES SPACE

Chiffrement de toutes les données

- Chiffre les fichiers bases de données
- en entier sur l'OS
- Algorithme standard AES 128

Efficacité maximale

- Haute performance
- Intégration avec Oracle Data Compression

Pas d'impact applicatif

TABLESPACE ENCRYPTION : PERFORMANCE

Les blocks de données sont chiffrés / déchiffrés au niveau des E/S Oracle

- **Très Haute Performance (1-2% overhead environ)**
- **Tous types de données supportés**
- **Transparence Complete**

Test dans un contexte Peoplesoft

- **Des tests récent utilisant des tablespaces chiffrés dans un contexte applicatif sous PeopleSoft Applications n'ont pas montré des pertes de performance significatives**

QUELQUES CONSEILS

1. Ne communiquer les mots de passe à personne
2. Changer régulièrement le mot de passe
3. Éviter d'inscrire le mot de passe sur des Post-it collés sur l'écran.
4. Une enveloppe de sécurité scellée contenant les mots de passe des systèmes sera maintenue à jour et accessible aux personnes accréditées.
5. L'accès à cette enveloppe devra être lui aussi sécurisé.
6. Pour le moindre soupçon, il faut changer le mot de passe.
7. Pour les utilisateurs occasionnels, il faut créer des accès temporaires à fermer après leur départ.

SÉCURITÉ ORACLE : BEST PRACTICES

1. Installer seulement ce qui est nécessaire
2. Verrouiller ou supprimer les comptes par défaut
3. Changer les mots de passe par défaut
4. Changer les mots de passe pour les comptes administrateurs
5. Changer les mots de passe par défaut à tous les utilisateurs
6. Forcer la gestion des mots de passe
7. Sécuriser les transactions en batch (batch jobs)
8. Gérer l'accès aux rôles sysdba et sysoper
9. Activer oracle data dictionary protection
10. Suivre le principe du privilège minimum

SÉCURITÉ ORACLE : BEST PRACTICES

1. Limiter les privilèges Public
2. Authentifier les utilisateurs
3. Restreindre l'accès via le système d'exploitation
4. Sécuriser oracle listener
5. Sécuriser les procédures externes
6. Vérifier les adresses IP
7. Crypter les trafic réseau
8. Appliquer tous les patchs de sécurité