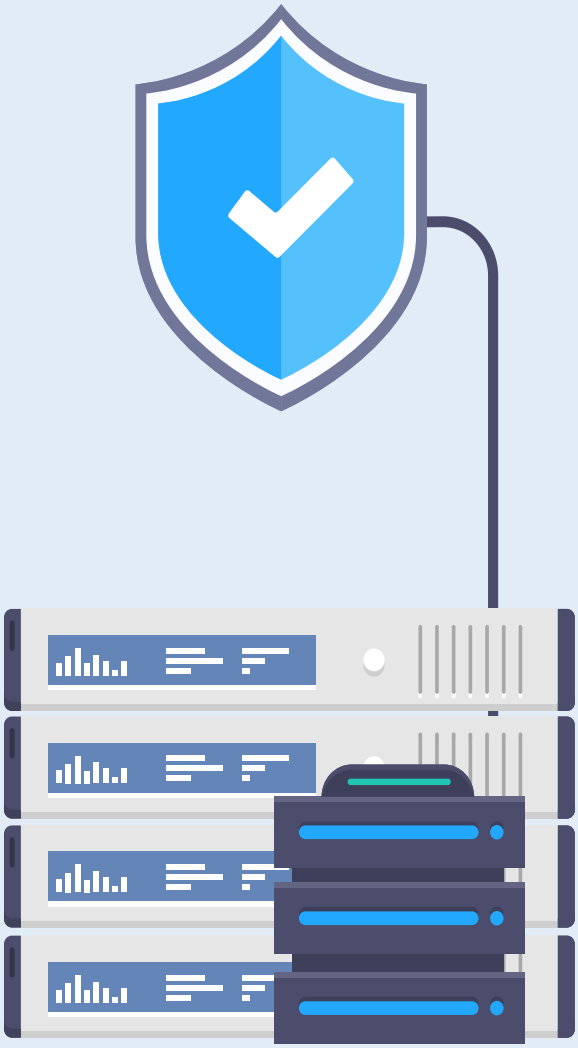
CCN-CERT

BP/22



Recommandations de sécurité pour la base de données Oracle 19C

RAPPORT DE BONNES PRATIQUES

MAI 2022

cn-cert centro criptológico nacional
CCN centro criptológico nacional

Edition:

Date d'émission: mai de 2022

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux termes contenus dans le présent document, rejetant expressément tout type de garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et des logiciels indiqués, même s'il a été averti d'une telle possibilité.

AVIS JURIDIQUE

Avant-propos

Dans un monde de plus en plus complexe et globalisé, dans lequel les technologies de l'information et de la communication (TIC) jouent un rôle extrêmement important, nous devons être conscients que la bonne gestion de la cybersécurité est un défi collectif que nous devons nécessairement relever. Il est nécessaire d'assurer la protection des capacités économiques, technologiques et politiques de notre pays, surtout lorsque la prolifération des attaques ciblées et le vol d'informations sensibles sont une réalité indéniable.

Il est donc essentiel de se tenir au courant des menaces et des vulnérabilités liées à l'utilisation des nouvelles technologies. La connaissance des risques qui pèsent sur le cyberespace doit servir à mettre en œuvre avec des garanties les mesures, tant procédurales que techniques et organisationnelles, qui permettent de créer un environnement sûr et fiable.

La loi 11/2002 du 6 mai 2002, qui réglemente le Centre national d'intelligence (CNI), confie au Centre national d'intelligence l'exercice des fonctions relatives à la sécurité des technologies de l'information et à la protection des informations classifiées, tout en confiant à son secrétaire d'État directeur la responsabilité de diriger le Centre national de cryptologie (CCN).

Sur la base de la connaissance et de l'expérience du CNI en matière de menaces et de vulnérabilités en termes de risques émergents, le Centre réalise, par l'intermédiaire du Centre national de cryptologie, régi par le décret royal 421/2004 du 12 mars, diverses activités directement liées à la sécurité des TIC, visant la formation de personnel expert, l'utilisation de technologies de sécurité appropriées et l'application de politiques et de procédures de sécurité.

Nous devons être conscients que la bonne gestion de la cybersécurité est un défi collectif que nous devons nécessairement relever.

Précisément, cette série de documents CCN-STIC reflète clairement le travail que cet organisme réalise en matière de mise en œuvre de la sécurité, en permettant l'application de politiques et de procédures, puisque les guides ont été élaborés avec un objectif clair : améliorer le degré de cybersécurité des organisations, conscients de l'importance d'établir un cadre de référence dans ce domaine pour soutenir le personnel de l'administration dans l'accomplissement de la difficile tâche de sécurisation des systèmes TIC dont ils ont la charge.

Avec cette série de documents, le Centre National de Cryptologie, conformément à ses missions et à ce qui est reflété dans le Décret Royal 3/2010 réglementant le Schéma National dans le domaine de l'administration électronique, contribue à améliorer la cybersécurité espagnole et à maintenir les infrastructures et les systèmes d'information de toutes les administrations publiques avec des niveaux de sécurité optimaux. Tout ceci a pour but de générer la confiance et des garanties dans l'utilisation de ces technologies, en protégeant la confidentialité des données et en garantissant leur authenticité, leur intégrité et leur disponibilité.

Mai 2022

Paz Esteban López

Secrétaire d'État
Directeur du Centre National de Cryptologie

Index

1. À propos du CCN-CERT, Certificat Gouvernemental National

CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN.

Le **CCN-CERT** est la capacité de réponse aux incidents de sécurité informatique du Centre National de Cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT Gouvernemental National Espagnol** et ses fonctions sont définies dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma national de sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de **contribuer à l'amélioration de la cybersécurité espagnole,** en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est chargé de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyber-incidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

2. Principes fondamentaux de la sécurité des bases de données

Les systèmes de gestion de bases de données fonctionnent sur des plates-formes et des systèmes d'exploitation spécifiques qui leur fournissent les éléments fondamentaux de communication et d'accès.

On peut donc dire que le modèle de sécurité d'un système de gestion de base de données, d'un point de vue simplifié, se divise en ces deux **domaines d'action:**

L'étendue de la plate-forme où le service est exécuté

L'environnement et les capacités fournis par le gestionnaire de base de données lui-même

Le produit Oracle 19c est un gestionnaire de base de données relationnelle généraliste, ce qui signifie qu'il peut être utilisé dans de multiples environnements et applications, et qu'il peut être déployé sur des serveurs Unix, Linux et Microsoft Windows.

Dans tous les cas, il sera important de ne pas perdre de vue les aspects de sécurité qui sont configurés au niveau du système d'exploitation, tels que les utilisateurs, les services, les communications et les protocoles, ainsi que ceux qui sont configurés dans l'environnement Oracle 19c, tels que les processus d'autorisation et le contrôle d'accès aux données résidant dans les différentes bases de données.

L'authentification est le processus par lequel **un système vérifie l'identité d'un utilisateur.** Dans Oracle 19c, ce processus est effectué en dehors de l'environnement de l'application, par le biais d'un module d'authentification. Grâce aux différents modules qu'incorpore Oracle 19c, il est possible d'utiliser des protocoles d'authentification tels que LDAP, OS, TNS, Kerberos, par SID ou nom de service.

L'authentification est le processus par lequel un système vérifie l'identité d'un utilisateur.

Pour activer et configurer les **différentes méthodes d'authentification,** voir le guide:

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-authentication.html

Kerberos peut être implémenté comme indiqué via le lien suivant:

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-kerberos-authentication.html

L'application de la sécurité sur le moteur de la base de données Oracle 19c fait partie d'une série de tâches qui doivent être effectuées en permanence. Oracle est un moteur de base de données bien connu et ses comptes d'utilisateurs, ports, chemins de fichiers et paramètres par défaut dans une installation peuvent constituer une menace sérieuse pour la sécurité d'une organisation.

Cette nouvelle version d'Oracle offre un certain nombre d'améliorations et de fonctionnalités concernant l'indexation automatique grâce à des algorithmes d'apprentissage automatique et ajoute un point d'amélioration sur la stabilité grâce à la redirection DML d'Active Data Guard en termes de sauvegardes.

Active Data Guard est un modèle d'architecture de haute disponibilité qui permet de prévenir les pertes de données en mode synchrone ou asynchrone.

Les fonctionnalités d'Oracle (Active) Data Guard dans Oracle Database 19c renforcent son objectif stratégique de prévention des pertes de données, de haute disponibilité, d'élimination des risques et d'augmentation du retour sur investissement en permettant la mise en place de systèmes actifs de reprise après sinistre hautement fonctionnels, faciles à déployer et à gérer. Pour ce faire, il fournit l'infrastructure logicielle de gestion, de surveillance et d'automatisation permettant de créer et de maintenir une ou plusieurs bases de données de secours synchronisées qui protègent les données Oracle contre les pannes, la corruption des données, les erreurs humaines et les catastrophes.

Active Data Guard utilise la simplicité de la réplication physique. Grâce à son intégration avec Oracle, il assure une isolation unique entre les bases de données primaires et de secours pour offrir le plus haut niveau de protection contre la perte de données. Active Data Guard prend en charge les systèmes synchrones (perte de données garantie nulle) et asynchrones (perte de données quasi nulle).

Active Data Guard utilise la simplicité de la réplication physique, son intégration avec Oracle fournissant une isolation unique entre les bases de données primaires.

Pour maintenir une haute disponibilité des applications critiques, les administrateurs de bases de données peuvent choisir un basculement manuel ou automatique au cas où, pour une raison quelconque, le système primaire deviendrait indisponible. Active Data Guard est une option sous licence pour Oracle Database Enterprise Edition. Toutes les capacités qui sont explicitement nommées "Active Data Guard" nécessitent une licence Active Data Guard. Toutes les fonctionnalités explicitement désignées comme "Data Guard" sont incluses dans Oracle Enterprise Edition, aucune licence optionnelle n'est requise. Active Data Guard est un superset de Data Guard et hérite de toutes les capacités de Data Guard.

L'un des grands avantages d'Active Data Guard 19c est l'amélioration de la capacité à effectuer des lectures intensives hors ligne sur des applications en attente. Il est désormais possible d'effectuer des opérations DML occasionnelles sur la base de données de secours, ce qui en fait une base de données de rapports entièrement fonctionnelle. Cela permet d'optimiser le retour sur investissement car la base de données primaire est utilisée de manière optimale et les ressources du système de reprise après sinistre sont utilisées de manière optimale.

Vous pouvez obtenir plus d'informations sur Oracle Active Data Guard 19c en cliquant sur le lien suivant:

Lien: https://www.oracle.com/technetwork/database/availability/dg-adg-technical-overview-wp-5347548.pdf

En ce qui concerne la traçabilité et la croissance soudaine que chacune des tables Oracle peut avoir en fonction des besoins de chaque organisation, des tables partitionnées hybrides ont été mises en œuvre permettant la gestion d'une table entre les partitions à l'intérieur de la base de données et également à l'extérieur de la base de données, dans le cas externe avec un accès en lecture.

De plus amples informations sont disponibles sur le lien suivant:

Lien: https://oracle-base.com/articles/19c/hybrid-partitioned-tables-19c

L'autorisation est le processus qui consiste à déterminer si un utilisateur authentifié a accès aux informations et aux autorisations qu'il demande. Ce processus s'effectue entièrement dans Oracle 19c, en consultant les permissions associées à une identité spécifique. En ce sens, il existe différents types de permissions qui peuvent être accordées.

- **Autorisations primaires:** celles qui sont accordées directement à l'identifiant d'autorisation.
- **Autorisations secondaires:** celles qui sont accordées aux groupes et aux rôles dont un identifiant d'autorisation est membre.
- **Permis publics:** ceux qui sont accordés à l'entité PUBLIC.
- **Autorisations basées sur le contexte:** celles qui sont accordées à un rôle de contexte de confiance.

Ces autorisations peuvent être accordées à des utilisateurs de différents niveaux ou catégories:

- **Autorisation au niveau du système:** il s'agit des autorités qui effectuent les tâches d'administration. Il y a plusieurs utilisateurs avec des rôles différents.
- L'utilisateur SYS est l'administrateur du système. Son mot de passe doit être modifié par rapport au mot de passe par défaut du fabricant. Il n'est pas conseillé de créer des objets dans son schéma.
- L'utilisateur SYSTEM chargé du contrôle du système a le rôle de DBA et doit également changer son mot de passe par défaut. Dans son schéma, des tables et des vues d'administration peuvent être créées.
- Les utilisateurs SYSBACKUP, SYSDG, SYSKM et SYSRAC sont automatiquement créés lors de l'installation pour faciliter l'administration.
- L'utilisateur SYSBACKUP facilite les opérations de sauvegarde et de récupération d'Oracle Recovery Manager (RMAN) à partir de RMAN ou de SQL * Plus.
- L'utilisateur SYSDG facilite les opérations de Data Guard. L'utilisateur peut effectuer des opérations avec Data Guard Broker ou avec l'interface de ligne de commande DGMGRL.

- L'utilisateur SYSKM facilite les opérations du keystore de cryptage transparent des données.
- L'utilisateur SYSRAC facilite les opérations Oracle Real Application Clusters (Oracle RAC) en se connectant à la base de données via l'agent Clusterware à l'aide d'utilitaires Oracle RAC tels que SRVCTL.
- Le privilège administratif SYSRAC ne peut pas être accordé aux utilisateurs de la base de données et n'est pas pris en charge dans un fichier de mots de passe. Le privilège administratif SYSRAC est uniquement utilisé par l'agent Oracle Clusterware Oracle pour se connecter à la base de données en utilisant l'authentification du système d'exploitation.

Les utilisateurs qui ont reçu le privilège système CREATE USER peuvent créer des comptes d'utilisateur, y compris des comptes d'utilisateur à utiliser comme utilisateurs proxy. Le privilège système CREATE USER étant un privilège puissant, un administrateur de base de données ou un administrateur de sécurité est généralement le seul utilisateur qui dispose de ce privilège système. Si vous souhaitez créer des utilisateurs qui disposent du privilège de création d'utilisateur, vous pouvez inclure la clause WITH ADMIN OPTION dans l'instruction GRANT.

- **Autorisation au niveau de la base de données:** Oracle 19c dispose de 79 rôles prédéfinis lors de l'installation. La définition de ces derniers se trouve dans le lien suivant:

  Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-privilege-and-role-authorization.html

  Indépendamment de ceux-ci, d'autres rôles peuvent être générés à l'aide de l'instruction create role, auxquels peuvent ensuite être attribuées des autorisations spécifiques. Par conséquent, un audit des permissions dans la base de données doit être dynamique et ne pas se limiter aux seuls rôles et permissions générés dans une installation. Le fournisseur propose au moins 30 vues de gestion des rôles pour faciliter ces tâches. Les autorités disposant d'autorisations d'octroi et de révocation de privilèges peuvent attribuer et révoquer des autorisations aux utilisateurs et aux rôles.

- **Autorisation au niveau de l'objet:** L'autorisation au niveau de l'objet implique la vérification des privilèges lorsqu'une opération spécifique est effectuée sur un objet spécifique.

Autorisation basée sur le contenu: les vues constituent un moyen d'autoriser l'accès basé sur le contenu. Les vues permettent de contrôler quelles colonnes ou lignes d'un tableau peuvent être lues par des utilisateurs spécifiques. D'autre part, Oracle, par le biais d'Oracle Label Security, permet de contrôler l'accès à des lignes spécifiques (étiquetées) d'une base de données. Avec Oracle Label Security en place, les utilisateurs ayant différents niveaux de privilèges se voient automatiquement accorder (ou exclure) le droit de visualiser ou de modifier les lignes de données étiquetées. Le guide de l'administrateur d'Oracle Label Security décrit comment utiliser Oracle Label Security pour protéger les données sensibles. Il explique les concepts de base de la sécurité basée sur les étiquettes et fournit des exemples pour montrer comment elle est utilisée.

Un autre élément important pour définir la sécurité d'un gestionnaire de base de données est le cryptage, tant pour les données en transit que pour les données au repos. Oracle 19c offre différentes options de cryptage et de transport des données, qui sont abordées plus loin dans ce document.

Les informations de cette section peuvent être complétées à partir du lien suivant.

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/admin/getting-started-with-database-administration.html

3. Mise en œuvre d'une base de données sécurisée

Cette section fournit des recommandations sur l'installation du produit Oracle 19c orientées vers la plupart des cas d'utilisation possibles de chaque organisation en fonction du système.

Les commandes décrites ci-dessous doivent être adaptées à l'environnement et au système sur lequel elles sont exécutées, en tenant compte des exigences minimales fixées par le fabricant.

Les étapes décrites ci-dessous sont destinées à être répétées après avoir effectué une mise à niveau logicielle sur le moteur de base de données Oracle 19c.

Pour installer Oracle 19c, vous devez d'abord installer les prérequis nécessaires en utilisant la commande suivante:

```
dnf install et https://yum.oracle.com/repo/
OracleLinux/OL8/baseos/latest/x86_64/getPackage/
oracle-database-preinstall-19c-1.0-1.el8.x86_64.rpm
```

Après avoir exécuté la commande, le système produira une fenêtre de sortie semblable à l'image suivante:

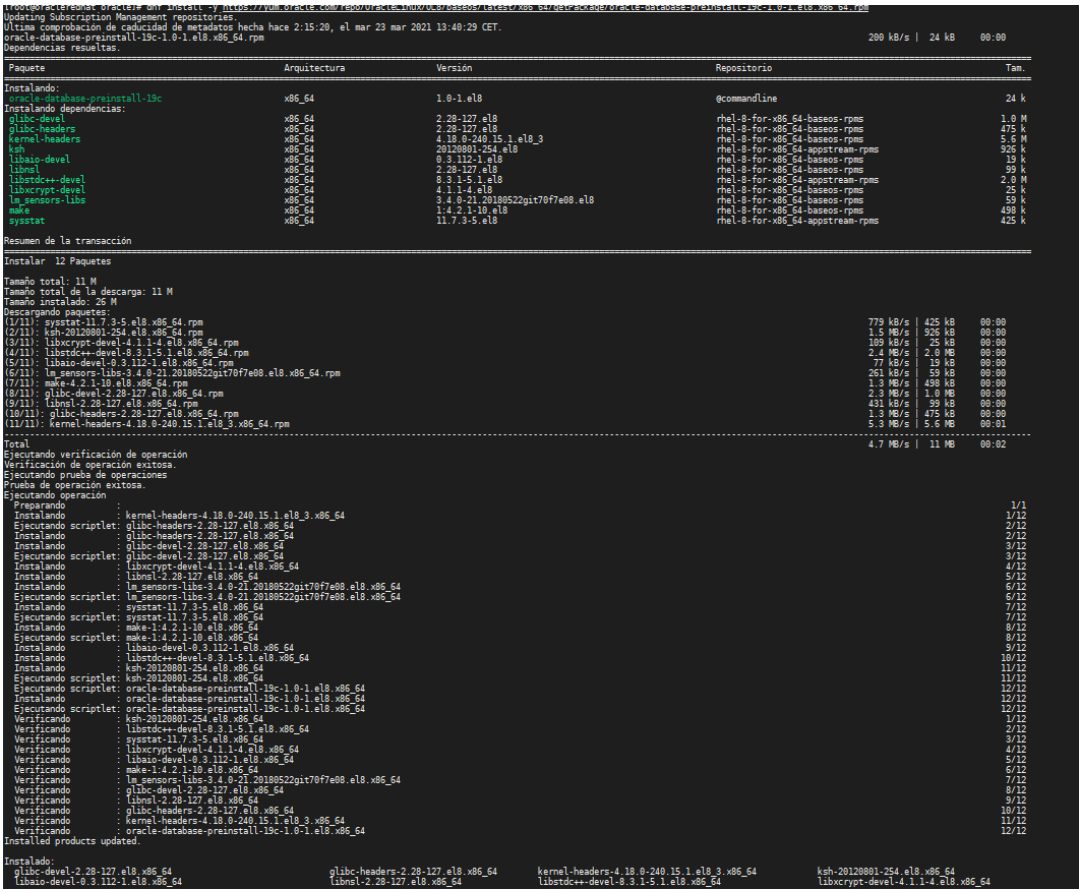


Illustration 1 - Commande d'installation Oracle Conditions préalables

Une fois terminé, vous devez télécharger le logiciel d'installation Oracle et l'installer avec la commande suivante:

```
rpm -i oracle-database-ee-19c-1.0-1.x86_64.rpm
```

Après avoir exécuté la commande, le système renvoie des informations similaires à celles qui suivent:

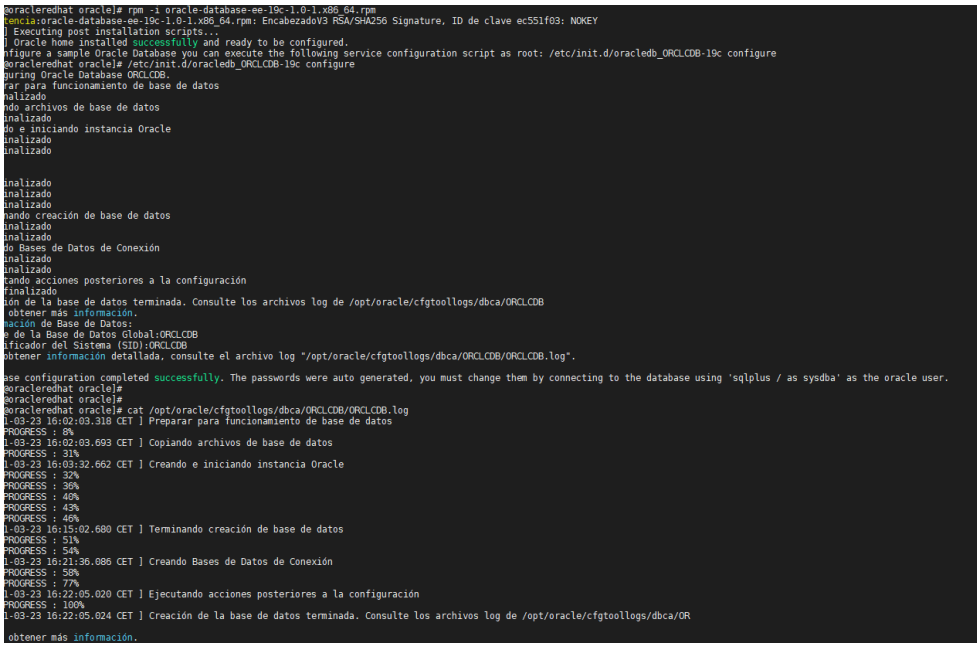


Illustration 2 - Commande du logiciel d'installation Oracle

Note: Vous trouverez de plus amples informations sur l'installation dans le document du fabricant intitulé **"database-installation-guide-linux.pdf"**. Veuillez noter que certains documents du vendeur peuvent nécessiter une connexion à votre plateforme.

En raison de la nouvelle version d'Oracle, il existe deux nouvelles options lors de la création d'une base de données pendant l'installation. Par conséquent, les options suivantes doivent être prises en considération en fonction des besoins de l'organisation:

NON-CDB

Base de données similaire aux versions précédentes 9.x, 10.x ou 11.x

CDB

Base de données conteneur pour le stockage de bases de données enfichables.

Cette base de données CDB permet l'option "multitenant" de la version 19c, qui permet de créer plusieurs bases de données "pluggables" sur ce conteneur, en partageant les métadonnées contenues dans la base de données du conteneur ou "CDB".

La création d'une CBD n'est guère différente de la création d'une autre base de données dans les versions précédentes.

Au démarrage, le DBCA offre les options suivantes, comme indiqué ci dessous:

- **Créez une CDB ainsi qu'une base de données enfichable ("PDB").**
- **Créer un CBD en mode avancé, ce qui permet de créer le CBD vide.**

Par conception, vous pouvez rapidement connecter une PDB à une CDB, déconnecter la PDB de la CDB, puis connecter cette PDB à une autre CDB. Vous pouvez également cloner les PDB tant qu'elles sont disponibles.

Vous trouverez de la documentation sur les différentes architectures dans les liens suivants:

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/18/rilin/deciding-between-multitenant-container-databases-and-non-cdbs-in-oracle-rac.html

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/multi/introduction-to-the-multitenant-architecture.html

3. Mise en œuvre d'une base de données sécurisée

Après l'installation du produit ou l'application d'un correctif au produit, il convient de vérifier l'état de la solution et d'examiner la documentation du fabricant, car il se peut que des objets précédemment bastionnés doivent l'être ou que de nouveaux objets existent après l'installation.

Au niveau du logiciel, les tâches de conformité suivantes doivent être effectuées régulièrement:

- Maintenez la version du moteur à jour.
- Maintenez à jour les versions de tout logiciel supplémentaire au moteur, par exemple Apex ou tout autre produit susceptible de modifier ou d'incorporer des objets du serveur de base de données. Il existe plusieurs produits qui permettent d'ajouter des rôles, des autorisations, des paquets, etc. À ce stade, la sécurité du moteur de la base de données doit être réexaminée.
- Vérifiez que les comptes utilisateurs **ORA_DBA** ne sont pas root dans le système d'exploitation.
- Passez en revue les vulnérabilités de chaque composant de l'installation. Les vulnérabilités connues (CVE) par composant (CPE) peuvent être consultées sur des portails tels que le NIST.
- Si des vulnérabilités sont publiées et n'ont pas été corrigées par Oracle, il convient de le signaler aux responsables de la sécurité.
- Nettoyer les fichiers temporaires après l'installation d'un produit ou d'un patch (TMP_DIR, TMPDIR, TEMP, TMP...).

4. Configuration sécurisée de la base de données

Voici des recommandations pour renforcer la sécurité de la base de données Oracle 19c une fois le processus d'installation terminé.

4.1 Contrôle d'accès

La conception de contrôles d'accès appropriés, adaptés aux besoins de l'exploitation des données par les utilisateurs et les outils, est essentielle pour réduire les risques d'exfiltration ou d'accès non autorisé. La plupart des menaces entrent dans cette catégorie et sont minimisées ou éliminées par le maintien de contrôles stricts.

L'accès à une instance ou à une base de données nécessite l'authentification de l'utilisateur. Oracle fournit différents protocoles d'authentification comme indiqué au point 2 du document.

Il est recommandé d'utiliser des mécanismes d'authentification forte tels que SERVER, LDAP ou Kerberos et d'éviter d'utiliser l'authentification CLIENT, notamment dans les environnements où la sécurité du client ne peut être garantie.

Il est recommandé de suivre le principe du moindre privilège, selon lequel seuls les utilisateurs sont autorisés à accéder aux informations et à effectuer les actions dont ils ont réellement besoin, ce qui minimise la surface d'exposition.

La conception de contrôles d'accès appropriés, adaptés aux besoins de l'exploitation des données par les utilisateurs et les outils, est essentielle pour réduire les risques d'exfiltration ou d'accès non autorisé.

Il est recommandé d'examiner et, si nécessaire, de révoquer les autorisations des utilisateurs ou des groupes qui n'en ont pas besoin.

Dans les scénarios où des données sensibles sont stockées, il est recommandé, outre la **révision des privilèges**, d'établir des contrôles d'accès granulaires tels que cellule, colonne ou ligne, afin d'empêcher l'accès aux données sensibles à partir d'environnements non fiables, voir la section 4.4.1 du présent document pour l'application.

Par défaut, un DBA a **accès à toutes les tables** de son instance de base de données. Il s'agit d'un risque, surtout si le compte a été violé ou si ces privilèges sont utilisés de manière abusive. Il est recommandé de révoquer les privilèges d'accès aux données du DBA s'il n'a pas réellement besoin d'accéder aux données.

Il est recommandé de vérifier que l'accès PUBLIC n'a été accordé à aucune base de données.

Un utilisateur non autorisé peut accéder aux informations résidant dans les tables du système si celles-ci n'ont pas été correctement protégées.

Il est recommandé d'examiner et de protéger les tables et les vues importantes du système, telles que les conteneurs de code plsql: les objets **All_source, dba_source** ou **ALL_OBJECTS , DBA_OBJECTS.** Il recommande également d'attribuer les privilèges par le biais d'un modèle de rôle, en évitant l'attribution directe aux utilisateurs. N'oubliez pas d'attribuer ensuite des rôles à des utilisateurs spécifiques ou concrets qui pourront identifier qui fait quoi.

En outre, il est recommandé d'utiliser les contrôles du système d'exploitation pour empêcher les administrateurs du système d'exploitation d'obtenir un accès trop important.

D'autre part, **il est recommandé d'attribuer les autorisations DBA uniquement par le biais d'un rôle, et de contrôler l'accès à ce rôle par le biais de contextes de confiance.** Cela permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.

Il est également recommandé de révoquer le privilège de créer des bases de données pour tous les utilisateurs, à l'exception de l'utilisateur DBA.

L'écouteur est l'un des composants les plus susceptibles de faire l'objet d'attaques, principalement des attaques par déni de service distribué (DDoS). Pour cette raison, les composants de ce service doivent être sécurisés et audités.

Il recommande également d'attribuer les privilèges par le biais d'un modèle de rôle, en évitant l'attribution directe aux utilisateurs.

Les recommandations suivantes concernent la configuration de la sécurité du service.

a. **Des mesures de sécurité doivent être appliquées sur l'accès aux fichiers de service: lsnrctl, listener.ora, sqlnet.ora** et **tnslnsr. lsnrctl** et **tnslnsr** sont des exécutables qui doivent avoir des permissions 0700.

Sur la base de ces fichiers, l'accès au service doit être configuré de manière sécurisée. Le nom du SID par défaut doit être modifié, permettant uniquement les authentifications locales pour l'administration.

Les étapes suivantes peuvent être suivies pour configurer ces paramètres:

```
LOCAL_OS_AUTHENTICATION_ = ON , ADMIN_RESTRICTIONS_
LISTENER=ON
```

Les commandes d'audit suivantes peuvent être exécutées sur le service pour détecter les éventuelles attaques par force brute qu'il pourrait recevoir:

```
set current_listener <nom de l'écouteur>
set  log_directory  <oracle_home  path>/network/
admin
set log_file <nom du sid>.log
set log_status on
sauvegarder_config
```

Les autorisations d'accès aux services doivent également être vérifiées, en utilisant un nom unique pour chaque service. L'audit des auditeurs doit être activé pour vérifier les valeurs par rapport aux drapeaux suivants afin d'identifier d'éventuelles attaques en direct.

Message
TNS-01169
TNS-01189
TNS-01190
TNS-12508
ORA-12525
ORA-28040
ORA-12170

b. **Il est conseillé de mettre en place une journalisation des paquets réseau.**

Dans le fichier "Listener.ora", les paramètres suivants doivent être définis comme étant au moins le niveau de journal suivant:

- "SEC_PROTOCOL_ERROR_TRACE_ACTION" pour "TRACE", "LOG o "ALERT"
- "SEC_PROTOCOL_ERROR_FURTHER_ACTION" par "DROP,3".

c. **Les ports par défaut du fabricant doivent être édités et modifiés en éditant le fichier "Listener.ora" ou en utilisant l'utilitaire "Netmgr".**

- Listener TNS port par défaut 1521, 1522.
- Port par défaut 1575 du serveur de noms Oracle.
- Port 1630 par défaut d'Oracle Connection Manager - connexions clients.
- Port 1830 par défaut d'Oracle Connection Manager - connexions administratives.
- Le port 2483 est le port par défaut de la TNS dans le protocole TCP/IP.
- Le port 2484 par défaut de la TNS dans le protocole TCP/IP avec SSL.

d. **Le paramètre "INBOUND_CONNECT_TIMEOUT" doit être fixé à 60 dans les fichiers ".ora" pour prévenir les attaques DDoS.**

e. **L'entrée dans le fichier "Sqlnet.ora" des listes blanches et noires d'IP et de plages ayant accès au serveur (Valid Node Checking) doit être configurée.**

Vous pouvez prendre les valeurs d'exemple suivantes :

```
tcp.validnode_checking = oui
tcp.invited_nodes = (x.x.x.x | nom, x.x.x.x | nom)
tcp.excluded_nodes=( x.x.x.x | nom, x.x.x.x | nom)
```

f. **Le trafic SQL entre les clients et le serveur doit être crypté.**

Dans le fichier **"Sqlnet.ora",** les entrées requises doivent être configurées comme obligatoires:

```
SQLNET.ENCRYPTION_SERVER = [accepted | rejected |
requested | required ]
SQLNET.ENCYRPTION_TYPES_SERVER = (nom de l'algorithme)
```

Du côté du client, les entrées **requises** doivent être configurées comme obligatoires:

```
SQLNET.ENCRYPTION_CLIENT = [ accepted | rejected |
requested | required ]
SQLNET.ENCYRPTION_TYPES_CLIENT = ( nom de l'algorithme
)
```

La configuration peut être vérifiée avec la commande:

```
SELECT NETWORK_SERVICE_BANNER À PARTIR V$SESSION_
CONNECT_INFO;
```

Remarque: vous trouverez de plus amples informations sur les paramètres de sécurité ci-dessus dans les liens suivants:

https://www.integrigy.com/files/Integrigy_Oracle_Listener_TNS_Security.pdf

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/keeping-your-oracle-database-secure.html

4.2 Audit

L'audit est un élément fondamental pour renforcer la sécurité d'un environnement informatique, en particulier dans les environnements multi-utilisateurs, où il est nécessaire de connaître les actions effectuées par chacun des utilisateurs.

La journalisation des actions indésirables ou des accès non autorisés aux données et leur analyse ultérieure améliorent les niveaux de contrôle de l'accès aux données et la prévention des accès non autorisés, des accès malveillants ou des erreurs de configuration.

La **surveillance** de l'accès des utilisateurs individuels et des applications, y compris les actions d'administration du système, peut fournir un enregistrement historique de l'activité sur vos systèmes de base de données.

Oracle 19c audit génère et conserve des preuves d'audit pour une série d'événements prédéfinis de la base de données. Les enregistrements générés dans un fichier ou un tableau de journal d'audit et leur analyse peuvent révéler des schémas d'utilisation qui permettraient d'identifier une mauvaise utilisation du système. Une fois identifiées, des mesures peuvent être prises pour réduire ou éliminer cette mauvaise utilisation du système. La commande create audit policy peut être utilisée pour générer le journal de l'événement à auditer. Vous pouvez également définir les actions à auditer sur l'objet, comme la lecture d'une table ou l'exécution d'une fonction. Vous pouvez passer en revue tous les objets auditables et sur quelles actions dans le lien:

Vous pouvez définir les actions à auditer sur l'objet, comme la lecture d'une table ou l'exécution d'une fonction.

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/sqlrf/CREATE-AUDIT-POLICY-Unified-Auditing.html

La fonction d'audit permet d'auditer au niveau de l'instance ainsi qu'au niveau de la base de données individuelle, toutes les activités étant enregistrées indépendamment dans des journaux séparés pour chacune d'elles.

Il convient de noter que si vous souhaitez auditer et/ou bastionner les accès aux enregistrements d'une table, vous devez vérifier que tous les accès aux vues, aux vues matérialisées, aux synonymes ou aux éventuelles sorties de fichiers via des ETL basés sur les enregistrements de cette table sont également audités et/ou bastionnés.

En outre, Oracle 19c intègre des outils de filtrage, des politiques de sécurité et des audits sur toutes les requêtes entrantes et sortantes du moteur de base de données avec **"AVDF Oracle Audit Vault"** et **"Database Firewall"**. Les politiques doivent être générées à l'aide du WASS (Web Application Acceleration and Security Policy) avant que les règles Oracle WAF puissent être créées.

Dans le cas où l'une des bases de données est en développement continu, l'application de la méthodologie OSSA pour l'application de la sécurité dans les bases de données en construction et en test doit être envisagée.

Une fois que les politiques du WASS ont été configurées, les règles du WAF doivent être créées avec les paramètres suivants comme recommandations standard:

- **Règles d'accès.** Les valeurs **ALLOW, DETECT**, et **BLOCK** de la politique WASS doivent être configurées.
- **AddressRateLimiting.** Limitation du nombre total de demandes pour une adresse IP.
- **CachingRules.** Règles de mise en cache pour l'accès à une application web.
- **Captchas.** Configuration de captchas pour empêcher l'accès par des robots.
- **CustomProtectionRules.** OCIDs règles de blocage et actions autorisées.

- **DeviceFingerprintChallenge.** Règles de refus d'énumération des moteurs par des bots utilisant des techniques d'empreinte digitale.
- **GoodBots.** Liste blanche des bots ayant accès au serveur web.
- **Défi de l'interaction humaine.** Liste des interactions humaines telles que les mouvements de la souris, les temps de réaction, le défilement des pages, etc. pour identifier les bots.
- **JsChallenge.** Liste des options de configuration des requêtes Javascript pour le blocage des bots.
- **Origine.** Clé de conteneur au sein des Origines définies dans la Politique WASS.
- **Groupes d'origine.** Groupe d'origine de l'objet d'origine à consulter défini dans le WASS.
- **Règles de protection.** Liste des règles de protection et leur description.
- **ProtectionSettings.** Liste des options à appliquer aux ProtectionRules.
- **ThreatFeeds.** Actions à appliquer lorsque du trafic malveillant est détecté.
- **Listes blanches.** Liste blanche des adresses IP qui peuvent passer à travers le Pare-feu.

4.3 Mesures de protection des communications

Le fabricant permet de crypter les communications au niveau du socket ou de la couche de transport (TLS). Les **avantages et les inconvénients de chaque option peuvent être examinés** sur le lien suivant:

Lien: https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html

Oracle Database fournit un chiffrement et une intégrité natifs du réseau de données pour garantir la sécurité des données lorsqu'elles circulent sur le réseau.

Oracle Database prend en charge l'algorithme de chiffrement AES (Advanced Encryption Standard) de la norme FIPS (Federal Information Processing Standard). Un cryptage triple DES est également possible.

Les algorithmes que le fabricant marque pour le cryptage réseau natif comme étant dépréciés et ne devant pas être utilisés sont les suivants: **DES, DES40, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 et RC4_256.** Les algorithmes améliorés dans cette version avec le correctif 2118136.2 sont : AES128, AES192 et AES256.

Pour renforcer la sécurité du cryptage réseau natif, les fichiers sql.ora sur les clients doivent être configurés en supprimant les entrées suivantes si et seulement si elles existent :

```
SQLNET.ENCRYPTION_TYPES_CLIENT

SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
```

Les fichiers sql.ora sur les serveurs doivent être configurés en supprimant les entrées suivantes si et seulement si elles existent:

```
SQLNET.ENCRYPTION_TYPES_SERVER

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
```

Le fichier sql.ora doit être configuré sur le serveur avec les paramètres:

```
SQLNET.ENCRYPTION_SERVER = OBLIGATOIRE

SQLNET.ENCRYPTION_TYPES_SERVER = (AES256)

SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA512)

SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS = FALSE
```

Chaque client doit être configuré dans le fichier sql.ora avec les entrées suivantes:

```
SQLNET.ENCRYPTION_CLIENT = OBLIGATOIRE

SQLNET.ENCRYPTION_TYPES_CLIENT = (AES256)

SQLNET.CRYPTO_CHECKSUM_CLIENT = OBLIGATOIRE

SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (SHA512)

SQLNET.ALLOW_WEAK_CRYPTO = FALSE
```

Note: Vous trouverez de plus amples informations dans les liens suivants:


https://ittutorial.org/oracle-19c-network-encryption/


https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/release-changes.html


https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/configuring-transparent-data-encryption.html


https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html

4.4 Mesures de protection des informations

Les mesures de protection de l'information comprennent à la fois celles qui sont configurées ou mises en œuvre dans l'environnement du serveur de base de données et dans l'environnement du système d'exploitation qui fait fonctionner le serveur.

Oracle 19c vous permet de générer des clés de cryptage et de crypter vos bases de données. Il vous permet également de crypter des objets spécifiques tels que des tableaux, des colonnes de tableaux ou des cellules. Il est de la responsabilité de l'organisation de connaître et de sécuriser les données les plus sensibles. Cela dépend du contenu informatif des différentes bases de données. Toutes les données n'ont pas la même criticité et il appartient à l'organisation de catégoriser d'abord les informations, puis d'en sécuriser l'accès en fonction de la sensibilité des données.

Les vues d'administration des objets chiffrés ainsi que les permissions de ces objets doivent être revues. Seuls les administrateurs doivent être en mesure d'exécuter **"Select"** sur ces vues. Les permissions peuvent être attribuées avec la commande **"GRANT SELECT ON view TO user"** ;

Les vues qui donneront des informations sur les objets cryptés sont les suivantes:

Voir
TOUTES_LES_COLONNES_CRYPTÉES
DBA_ENCRYPTED_COLUMNS
COLONNES_CRYPTÉES_ DE_L'UTILISATEUR
DBA_TABLESPACE_USAGE_METRICS
V$CLIENT_SECRETS
V$DATABASE_KEY_INFO
V$ENCRYPTED_TABLESPACES
V$ENCRYPTION_KEYS
V$ENCRYPTION_WALLET
V$WALLET

a. L'option "Generate Encryption Keys" doit être considérée dans le moteur avec la commande:

```
ADMINISTER KEY MANAGEMENT CREATE KEY [USING TAG 'tag']
[FORCE KEYSTORE]
IDENTIFIED BY [EXTERNAL STORE | keystore_password]
[WITH BACKUP [USING 'backup_identifier']];
```

b. Les bases de données Oracle doivent être cryptées avec la commande suivante.

```
ALTER TABLESPACE SYSTEM ENCRYPTION Type ENCRYPT
OPTIONS;
```

c. La clé peut être activée avec la commande suivante:

```
ADMINISTRER LA GESTION DES CLÉS CRÉER UNE CLÉ EN UTILISANT UNE BALISE
OPTIONS ;
```

Le dictionnaire d'objets du moteur de la base de données est l'une des sources courantes d'attaques contre le moteur de la base de données. Si un attaquant obtient l'accès au moteur de la base de données, il peut ajouter ou modifier des objets de la base de données. Il est nécessaire de savoir quels objets et avec quel code, le cas échéant, sont des objets légitimes de la base de données. Il est également essentiel de faire l'inventaire des dates auxquelles les objets ont été créés et modifiés.

Oracle 19c dispose d'objets d'apprentissage automatique qui créent automatiquement des index pour optimiser les performances du moteur. Les objets indexés doivent donc être exclus de l'analyse de l'inventaire.

- **Contrôler l'inventaire des objets. Chaque fois qu'il y a un changement ou une mise à niveau du développement à la production, le contenu objet du moteur, ainsi que son code "PLSQL", doivent être documentés et datés.**

- **Les permissions des synonymes du moteur doivent être vérifiées. Il est important de vérifier la sécurité du synonyme créé.**

- **Comme au point précédent, l'accès et le contenu des vues matérialisées doivent être sécurisés.**

Oracle permet d'accéder à d'autres serveurs de bases de données en les reliant. La sécurité de ces accès et de leurs données exposées doit faire l'objet de la même attention que celle des données propres au moteur Oracle.

Les applications génèrent souvent des tables temporaires à partir du code. Par conséquent, l'utilisation de "Global Temporary" est recommandée, afin que l'accès à ces données ne soit possible qu'à partir de la connexion active qui les génère et que la table soit détruite à la fin de l'exécution du code "PLSQL".

L'utilisation de "Global Temporary" est recommandée, afin que l'accès à ces données ne soit possible qu'à partir de la connexion active plutôt que de la connexion générale.

La sécurité doit être examinée pour les demandes d'incorporation de classes Java ou d'autres objets autres que ceux incorporés par le fabricant. Oracle autorise l'incorporation de classes non techniques qui peuvent compromettre la sécurité du produit.

La sécurité de tous les objets conteneurs de code "PLSQL" développés pour le fonctionnement des applications, tels que les procédures stockées, les fonctions et les paquets, doit être examinée. Les objets conteneurs (procédures, fonctions et packages) pour l'exécution dynamique de SQL, comme execute immmediate, sont particulièrement sensibles. Si ces objets n'ont pas été paramétrés correctement, ils peuvent faire l'objet d'attaques SQL dynamiques.

Le code de tous les objets du conteneur "PLSQL" développés pour le fonctionnement des applications: procédures stockées, fonctions et packages doit être crypté. De cette façon, un utilisateur qui modifie l'objet ne pourra pas voir son contenu. Les vues **"all_source"** et/ou **"dba_source"** peuvent être utilisées pour visualiser rapidement le code de ces objets.

Les comptes d'utilisateurs par défaut constituent un vecteur d'attaque évident pour la solution. Ils doivent donc répondre à certains critères de sécurité afin de minimiser leur exposition et leur exploitation éventuelle.

Il est recommandé que la sécurité des comptes utilisateurs réponde aux critères suivants.

- **Séparation des privilèges et exposition minimale : les autorisations ne doivent être accordées qu'aux objets auxquels l'accès doit être accordé.**
- **Une attention particulière doit être portée aux privilèges accordés avec la clause "ANY" qui accorde des privilèges à tous les objets du même type. Dans Oracle 19c, il existe 148 instructions d'affectation de permission d'objet possibles qui incluent une telle clause ANY. En outre, il existe 84 autres commandes d'attribution d'autorisations génériques possibles qui accordent une autorisation à un ensemble d'objets.**

Voici les directives recommandées pour la sécurité des mots de passe des comptes utilisateurs:

- Contenir au moins **12 caractères.**
- Incluez des lettres **majuscules,** au moins deux.
- Contenir au moins **deux** lettres **minuscules.**
- Contenir au moins **deux chiffres.**
- Contenir au moins **deux** caractères **spéciaux**.

Les comptes d'utilisateurs par défaut constituent un vecteur d'attaque évident pour la solution.

- **Ne contiennent pas le nom de l'utilisateur.**

- Définissez les paramètres suivants.

  - **PASSWORD_REUSE_TIME**: Nombre de jours pendant lesquels un mot de passe ne peut être réutilisé.

  - **PASSWORD_REUSE_MAX**: Nombre de mots de passe qui doivent être utilisés avant que le premier mot de passe puisse être réutilisé.

- En plus des mots de passe, il est recommandé de configurer les éléments suivants :

  - **PASSWORD_LIFE_TIME**: paramètre définissant le nombre de jours avant l'expiration du mot de passe.

  - **PASSWORD_GRACE_TIME:** Le paramètre définissant le nombre maximum de jours après l'expiration du mot de passe que l'utilisateur doit changer son mot de passe à l'expiration avant que toutes les connexions soient refusées.

- Blocage du compte. Il est recommandé de configurer les variables :

  - **FAILED_LOGIN_ATTEMPTS:** Nombre de tentatives de connexion échouées autorisées avant que le compte de l'utilisateur ne soit verrouillé.

  - **PASSWORD_LOCK_TIME:** Nombre de jours pendant lesquels un compte sera verrouillé après une série de tentatives de connexion infructueuses.

- Il est particulièrement intéressant de limiter à environ 90 minutes la durée de la session pour les comptes non-serveurs.

- Les comptes d'utilisateurs qui ne sont pas des serveurs d'applications peuvent être bloqués après **deux tentatives infructueuses.**

- Temps de **déconnexion en cas d'inactivité 20 minutes** pour les comptes de serveurs non applicatifs.

- **Nombre de tentatives** de connexion échouées avant le verrouillage du compte **égal ou inférieur à 6.**

- Durée de vie maximale d'un mot de passe avant d'être obligé de le changer: **180 jours.**

- Modifier le **compte SYS :**

  Ce compte peut effectuer toutes les fonctions administratives. Toutes les tables et vues de base (sous-jacentes) du dictionnaire de données de la base sont stockées dans le schéma SYS. Ces tables et vues de base sont essentielles au fonctionnement de la base de données Oracle.

  Pour maintenir l'intégrité du dictionnaire de données, les tables du schéma SYS sont uniquement manipulées par la base de données.

  En revanche, ils ne doivent jamais être modifiés par un utilisateur ou un administrateur de la base de données. Aucune table ne doit être créée dans le schéma SYS. L'utilisateur SYS dispose du privilège SYSDBA, qui lui permet d'effectuer des tâches administratives de haut niveau, telles que la sauvegarde et la récupération.

  Les mots de passe peuvent être modifiés à l'aide de la commande suivante:

```
ALTER USER SYS IDENTIFIÉ PAR “nouveau mot de passe”
```

Remarque: les nouveaux mots de passe doivent répondre aux exigences de complexité minimale.

- Modifier le **compte SYSTEM.**

  Ce compte peut effectuer toutes les fonctions administratives, à l'exception de la sauvegarde et de la récupération, et de la mise à jour de la base de données. Il est vrai que ce compte peut être utilisé pour effectuer des tâches administratives quotidiennes, mais Oracle recommande fortement la création de comptes utilisateurs nommés pour administrer la base de données Oracle afin de permettre le suivi de l'activité de la base.

  Vous pouvez changer le mot de passe de l'utilisateur SYSTEM de "SQLPLUS" comme suit:

  ```
  ALTER USER SYSTEM IDENTIFIÉ PAR "nouveau mot de passe";
  ```

  Remarque: les nouveaux mots de passe doivent répondre aux exigences de complexité minimale.

- Il est recommandé de configurer des comptes d'utilisateurs spécifiques pour les serveurs d'applications.

- Les comptes utilisateurs doivent être nominatifs afin de garantir la traçabilité des différentes actions exécutées dans le moteur. Il ne faut pas utiliser de comptes génériques associés aux différents rôles, mais plutôt des comptes qui identifient de manière unique l'auteur de tout changement.

- Il est souhaitable de disposer d'un certificat d'utilisateur pour chaque compte ayant accès au moteur.

- L'établissement d'une authentification à deux facteurs au moteur de base de données pour les comptes de serveurs d'applications, avec des identifiants tels que Google Authenticator ou d'autres réseaux sociaux (Social Sign-In Authentication), est recommandé pour les serveurs d'applications où un nombre indéterminé d'utilisateurs se connecteront.

4. Configuration sécurisée de la base de données

Souvent, après une installation, les bases de données à exploiter sont restaurées et des scripts sont exécutés qui peuvent modifier les autorisations associées aux comptes d'utilisateurs, aux rôles, aux autorisations de lecture, à la modification, à la suppression d'objets, etc.

Par conséquent, avant et après la restauration d'une base de données dans le moteur, les vues suivantes du dictionnaire doivent être vérifiées.

- Tous les rôles existants **"DBA_ROLES"** doivent être vérifiés pour les nouveaux rôles.
- Les utilisateurs associés à ces rôles **"DBA_TAB_PRIVS"** doivent être vérifiés.
- Les privilèges système associés aux rôles système et à leurs comptes associés **"DBA_SYS_PRIVS"** doivent être vérifiés.
- Les utilisateurs de l'APEX doivent être pris en compte.

  Note: APEX est l'interface web pour la gestion des espaces de travail. Un utilisateur "ADMIN" est généré avec le même mot de passe que le compte système. Le mot de passe de ce compte doit être revu et modifié conformément aux exigences de complexité minimale.
- Les comptes d'utilisateurs doivent être associés à des types ou à des rôles. Les rôles ou types de comptes minimums définis par le fabricant sont les suivants :
- **Utilisateurs réguliers de bases de données:** ils sont généralement limités à leur schéma contenant leurs tables, vues, index et procédures stockées. Si des pirates s'introduisent dans leurs comptes, ils pourraient non seulement visualiser/mettre à jour les données du schéma de l'utilisateur, mais aussi accéder aux objets d'autres schémas auxquels l'utilisateur peut être autorisé à accéder.

Comptes d'application: Il s'agit des comptes de base de données utilisés pour exécuter vos applications, tant commerciales que personnelles. Ces comptes sont similaires aux comptes d'utilisateurs de base de données ordinaires, mais comme les applications doivent fonctionner 24 heures sur 24 et 7 jours sur 7, leurs mots de passe sont souvent stockés sur plusieurs serveurs intermédiaires. La compromission de ces comptes de base de données peut entraîner une perte de données pour l'ensemble de l'application, y compris les données de l'utilisateur final.

Administrateurs des demandes: Ces comptes sont utilisés pour administrer, corriger et mettre à jour votre application, et ont donc un accès complet à toutes les données et procédures stockées utilisées pour l'application.

Analystes de données ou utilisateurs de business intelligence: ces utilisateurs ont généralement un accès illimité en lecture au schéma de l'application sans passer par les contrôles d'accès au niveau de l'application.

Administrateurs de bases de données (DBA): ils sont responsables d'une grande variété de tâches liées aux bases de données, notamment la gestion des performances, le diagnostic et le réglage, la mise à niveau et l'application de correctifs, le démarrage et l'arrêt de la base de données et la sauvegarde de celle-ci. Leur accès hautement privilégié à la base de données leur donne également accès à toute donnée sensible contenue dans la base de données (dossiers personnels, dossiers médicaux, dossiers financiers de l'entreprise, etc.), bien que cet accès ne soit pas nécessaire pour effectuer les tâches de DBA. Les administrateurs de bases de données ont accès à la gestion des comptes et ont donc souvent la confiance de leur organisation. Ces comptes d'utilisateurs sont souvent la cible d'attaques.

Administrateurs de sécurité: de nombreuses organisations ont des administrateurs de bases de données spécialisés qui ont également la responsabilité d'administrateurs de sécurité, notamment la gestion des comptes d'utilisateurs, la gestion des clés de cryptage et la gestion des audits.

Oracle recommande de ne générer en aucun cas un compte associé à la fois au rôle de DBA et au rôle d'administration de la sécurité. **Deux comptes nominatifs différents** doivent être générés si les informations d'identification des deux rôles doivent être données à la même personne physique, afin d'améliorer la gestion de la séparation des rôles.

Tous les comptes doivent être affectés par défaut à des espaces de travail autres que "SYSTEM".

- Les comptes d'utilisateurs affectés aux serveurs d'applications **ne doivent pas avoir de quotas.**

- L'accès aux objets appartenant à **"SYS"** (objets de l'administrateur système), **"DBA_"** (objets de l'administrateur de base de données), **"USER_"** (rôle de l'utilisateur et tables de permissions) doit être vérifié et seuls les comptes appartenant aux profils **"SYS"** ou **"DBA"** doivent avoir accès à ces objets. Si, par la suite, un accès en compte à un objet particulier est nécessaire, cela doit être analysé et documenté.

- Les permissions des rôles sur le catalogue "**SELECT_CATALOG_ROLE", "EXECUTE_CATALOG_ROLE", "DELETE_CATALOG_ROLE", "RECOVERY_CATALOG_OWNER"** doivent être révisées.

4.4.1 Contrôle d'accès aux lignes et aux colonnes

Les données sensibles peuvent être cryptées au niveau des enregistrements, des colonnes, des lignes et même des cellules.

Il est conseillé de chiffrer les tableaux et/ou les colonnes contenant les données les plus sensibles.

a. Une colonne cryptée peut être générée avec la commande **"ENCRYPT"** dans le "ddl" de la création de la table comme dans l'exemple suivant:

```
CREATE TABLE nom_table
  (campo_a VARCHAR2(11),
  Campo_cifrado VARCHAR2(16) ENCRYPT NO SALT);
```

b. Les procédures “packages”, “fonctions”, “all Source” peuvent être cryptées. Il est donc impossible pour une personne ayant accès au code de l’objet “PLSQL” de voir son code.

La commande suivante peut être utilisée:

```
wrap iname=input_file [ oname=output_file ]
```

c. Considérons l’option de chiffrer les disques, les partitions au niveau du système d’exploitation, avec l’option de chiffrer les données d’une cellule particulièrement sensible avec l’utilitaire **“DBMS_CRYPTO.SQL”** avec le morceau de code suivant.

```
DECLARE
   input_string VARCHAR2(16) := ‘tigertigertigert’
;
    raw_input RAW(128) :=
UTL_RAW.CAST_TO_RAW(CONVERT(input_string,
‘AL32UTF8’, ‘US7ASCII’)) ;
    key_string VARCHAR2(8) := ‘scottsco’ ;
    raw_key RAW(128) :=
UTL_RAW.CAST_TO_RAW(CONVERT(key_string,
‘AL32UTF8’, ‘US7ASCII’)) ;
    encrypted_raw RAW(2048) ;
    Chaîne cryptée VARCHAR2(2048) ;
    décrypté_raw RAW(2048) ;
    chaîne_décryptée VARCHAR2(2048) ;
-- Commencer à tester le cryptage :
BEGIN
   dbms_output.put_line(‘>Chaîne d’entrée : ‘ |||
     CONVERT(UTL_RAW.CAST_TO_VARCHAR2(raw_input),
‘US7ASCII’, ‘AL32UTF8’)) ;
     dbms_output.put_line(‘> ========= BEGIN TEST
Encrypt =========’) ;
    encrypted_raw := dbms_crypto.Encrypt(
        src => raw_input,
        typ => DBMS_CRYPTO.DES_CBC_PKCS5,
        key => raw_key) ;
```

```
         dbms_output.put_line('>Valeur hexagonale
cryptée : ' ||
          rawtohex(UTL_RAW.CAST_TO_RAW(encrypted_
raw))) ;
decrypted_raw := dbms_crypto.Decrypt(
        src => encrypted_raw,
        typ => DBMS_CRYPTO.DES_CBC_PKCS5,
        key => raw_key) ;
    chaîne_décryptée :=
      CONVERT(UTL_RAW.CAST_TO_VARCHAR2(decrypted_
raw), 'US7ASCII', 'AL32UTF8') ;
dbms_output.put_line('>Sortie de chaîne décryptée
: ' |||
        chaîne_décryptée) ;

si input_string = decrypted_string THEN
     dbms_output.put_line('>Stream DES Encyption
and Decryption successful') ;
FIN si ;
dbms_output.put_line('') ;
dbms_output.put_line('> ========= BEGIN TEST Hash
=========') ;
    encrypted_raw := dbms_crypto.Hash(
        src => raw_input,
        typ => DBMS_CRYPTO.HASH_SH1) ;
dbms_output.put_line('>Valeur de hachage de la
chaîne d'entrée : ' |||
          rawtohex(UTL_RAW.CAST_TO_RAW(encrypted_
raw))) ;
dbms_output.put_line('> ========= BEGIN TEST Mac
=========') ;
    encrypted_raw := dbms_crypto.Mac(
        src => raw_input,
        typ => DBMS_CRYPTO.HMAC_MD5,
        key => raw_key) ;
dbms_output.put_line('>Code d'authentification du
message : ' ||
          rawtohex(UTL_RAW.CAST_TO_RAW(encrypted_
raw))) ;
dbms_output.put_line('') ;
dbms_output.put_line('>Fin des tests DBMS_CRYPTO
') ;
FIN ;
/
```

4.4.2 Contrôle d'accès par étiquette

La sécurité basée sur les signatures a été mise en œuvre pour les localisateurs LOB. Les types de données LOB CLOB, NLOB ou BLOB sont utilisés pour stocker des fichiers ou de grands champs de texte d'une capacité maximale de 4 Go.

L'accent doit être mis sur la façon de stocker la clé de signature LOB dans un format crypté, la base de données ou la PDB doit avoir un keystore TDE ouvert. À partir de cette version, il est possible de configurer la sécurité basée sur les signatures pour les localisateurs d'objets volumineux.

Ces clés de signature LOB peuvent être cryptées avec la commande suivante:

```
MODIFIER LE DICTIONNAIRE DE LA BASE DE DONNÉES
CRYPTER LES INFORMATIONS D'IDENTIFICATION
```

Les types de données LOB CLOB, NLOB ou BLOB sont utilisés pour stocker des fichiers ou des champs de texte de grande taille.

Les algorithmes TDE autorisés dans Oracle 19c sont les suivants :

- **Advanced Encryption Standard (AES) 128, 192, 256 bits**
- **Triple Data Encryption Standard (TDES) 168 bits**

Note: De plus amples informations sont disponibles sur le lien suivant:

https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/configuring-transparent-data-encryption.html

Ces mesures de sécurité que l'analyse des privilèges a héritées des versions précédentes.

Remarque: pour plus d'informations sur la sécurité de l'analyse des privilèges, consultez le guide Oracle Database Vault et Oracle Database Security Guide.

https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/index.html

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/index.html

Il est recommandé d'établir des rôles pour accorder et renouveler les privilèges administratifs à partir de n'importe quel schéma. Les groupes SYSOPER et SYSBACKUP peuvent être segmentés selon des schémas définis par l'administrateur.

Les liaisons SASL (Simple Authentication and Security Layer) et TLS (Transport Layer Security) doivent être prises en charge pour les connexions Microsoft Active Directory.

Toujours en ce qui concerne la connectivité Oracle, cette version du produit nécessiterait un chiffrement natif Oracle et une authentification SSL pour les différents utilisateurs connectés simultanément.

Il est recommandé d'utiliser la nouvelle prise en charge de la correspondance partielle des DN (noms de domaine) basée sur les noms d'hôte pour la correspondance des certificats de serveur, ce qui ajoute une authentification à deux facteurs entre le client et le serveur.

D'autre part, les options d'audit seront établies sur les instructions SQL de haut niveau. Une telle fonction d'audit unifié des déclarations de niveau supérieur correspond à un audit des modifications du dictionnaire d'objets exécutées par les utilisateurs, ce qui permet d'auditer les activités des utilisateurs de niveau supérieur (ou utilisateurs directs) dans la base de données, mais sans collecter de données d'audit sur les activités des utilisateurs indirects. Cela ajoute une couche supplémentaire de sécurité lors de la recherche de traces d'incidents éventuels.

Dans cette version du produit, Oracle Native Encryption et l'authentification SSL seraient nécessaires pour plusieurs utilisateurs connectés simultanément.

Remarque: vous trouverez de plus amples informations dans les guides de sécurité dont les liens figurent ci-dessous:

https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/

En fonction des données stockées dans la base de données de chaque moteur, Oracle 19c dispose de services d'auto-analyse basés sur l'intelligence artificielle et les modèles de données associés à la configuration régionale de l'installation. L'outil recherche des données telles que les noms, les cartes de crédit, les salaires, les montants, les adresses personnelles, etc. et permet d'y accéder de manière sécurisée.

Bien souvent, les administrateurs de bases de données ne disposent pas des informations nécessaires sur les données les plus sensibles de chaque base de données pour sécuriser correctement ces informations. Le composant Oracle 19c "Label Security" permet la classification des données au niveau des lignes et fournit une médiation d'accès, prête à être utilisée en fonction de la classification des données et de l'autorisation du label utilisateur ou de l'autorisation de sécurité.

Le logiciel Oracle Label Security" est installé par défaut, mais n'est pas automatiquement activé. Vous pouvez activer Oracle Label Security dans SQL* Plus ou en utilisant Oracle Database Configuration Assistant (DBCA).

L'administrateur par défaut de Oracle Label Security est l'utilisateur **"LBACSYS".** Pour administrer "Oracle Label Security", vous pouvez utiliser un ensemble de packages "PL/SQL" et de fonctions distinctes au niveau de la ligne de commande ou "Oracle Enterprise Manager Cloud Control". Pour plus d'informations sur les politiques "Oracle Label Security", vous pouvez vous reporter à **"ALL_SA_*", "DBA_SA_*", "SA_*"** ou **"USER_SA_".**

Les objets et utilitaires permettant de catégoriser les données sont les suivants:

Paquet	Objectif
SA_SYDBA	Pour créer, modifier et supprimer les politiques de sécurité Oracle tag.
SA_COMPONENTS	Définir les niveaux, compartiments et groupes de politiques.
SA_LABEL_ADMIN	Pour effectuer des fonctions administratives standard de politique de balises, telles que la création de balises.
SA_POLICY_ADMIN	Pour appliquer des stratégies aux schémas et aux tables.
SA_USER_ADMIN	Gérez les autorisations des utilisateurs pour les niveaux, les partages et les groupes, ainsi que les privilèges des unités de programme. Également pour gérer les privilèges des utilisateurs.
SA_AUDIT_ADMIN	Gérez les autorisations des utilisateurs pour les niveaux, les partages et les groupes, ainsi que les privilèges des unités de programme. Également pour gérer les privilèges des utilisateurs.
SA_SESSION	Gérez les autorisations des utilisateurs pour les niveaux, les partages et les groupes, ainsi que les privilèges des unités de programme. Également pour gérer les privilèges des utilisateurs.
SA_UTL	Pour configurer les options d'audit des tâches administratives et de l'utilisation des privilèges.

"Enterprise Manager fournit un environnement graphique pour la découverte et la catégorisation des données sensibles.

Les informations contenues dans les bases de données doivent être catégorisées et documentées, quel que soit le niveau des paramètres de sécurité appliqués. Il faut savoir quelles informations sont stockées, où et dans quelle mesure elles sont sensibles.

4.5 Politiques de sauvegarde

Parfois, une mauvaise politique de protection des sauvegardes permet un accès non autorisé à des données qui ne sont plus protégées par la sécurité du serveur.

Si les données stockées dans les sauvegardes ne sont pas protégées, il est possible d'y accéder directement à partir du service de sauvegarde.

Il est recommandé de crypter tous les fichiers de sauvegarde et les images d'archive, quel que soit le support sur lequel ils sont stockés.

Il est recommandé de veiller à ce que la restauration de toute sauvegarde nécessite un accès contrôlé à la clé de chiffrement et fasse l'objet d'un audit, tant pour l'accès que pour la restauration elle-même.

Les pratiques recommandées par le fabricant de la sauvegarde doivent être maintenues.

Des sauvegardes régulières sont recommandées. Au moins une sauvegarde incrémentielle doit être générée quotidiennement et conservée pendant sept jours. Une sauvegarde incrémentielle hebdomadaire doit également être générée le dimanche et conservée pendant quatre semaines. Une sauvegarde incrémentielle doit également être générée chaque premier jour du mois, les douze derniers mois étant conservés. Une sauvegarde annuelle doit également être générée et conservée pendant cinq ans.

Les sauvegardes doivent être stockées à des endroits autres que l'emplacement physique du serveur de production.

Des tests de récupération périodiques sont recommandés, ainsi que des exercices périodiques de reprise après sinistre.

Une sauvegarde incrémentielle quotidienne doit être générée et conservée pendant sept jours.

5. Autres considérations

Voici quelques bonnes pratiques générales, quelle que soit la version du produit. Le fabricant incorpore la documentation du produit qui a été référencée dans ce document et complète les informations de ce document. Certaines des fonctionnalités du fabricant peuvent nécessiter l'achat de licences distinctes du moteur de base de données lui-même. Les captures d'écran intégrées dans ce document ont été réalisées sur un système d'exploitation Rhell 8. Par conséquent, la sortie à l'écran de certaines étapes peut ne pas correspondre exactement à celle d'une autre version du système d'exploitation.

Il est recommandé d'activer la redirection Active Data Guard.

Oracle 19c intègre cette fonctionnalité supplémentaire en tant que base de données miroir de reprise après sinistre. En outre, la base de données en miroir peut être utilisée pour l'exploration de données en mode lecture, comme l'exploration de rapports ou d'autres processus avec accès en lecture et refus d'écriture. Les transactions de lecture peuvent être redirigées vers le miroir. Cela permet d'avoir une sauvegarde en temps réel dans un emplacement physique différent de celui de la base de données originale.

Oracle 19c intègre des tables de partitionnement hybride qui peuvent résider physiquement à des endroits différents du reste des tables. Le partitionnement hybride doit être appliqué aux tables qui doivent résider dans un emplacement physique en appliquant des paramètres de sécurité plus élevés sur les accès physiques où ces tables résident.

Il est recommandé de stocker les données sur des systèmes de disques redondants RAID 1 ou 5 par exemple.

Il est recommandé de répliquer les fichiers log et redo log dans des emplacements physiquement différents. Il s'agit de fichiers qui stockent les modifications du journal des transactions qui sont particulièrement sensibles à l'analyse des modifications de données.

Dans le cas où l'une des bases de données est en développement continu, l'application de la méthodologie OSSA pour l'application de la sécurité dans les bases de données en construction et en test doit être envisagée.

- **Il est recommandé de générer des alarmes (politiques IAM) de consommation et d'utilisation du moteur de BD.**
- **Il est recommandé de chiffrer les disques au niveau du contrôleur.**
- **Il est recommandé de documenter les procédures de modification du moteur de BD ainsi que les différentes tâches d'administration.**
- **Il est recommandé de mettre en place des clusters à haute disponibilité.**
- **Il est recommandé d'effacer magnétiquement les disques anciens ou endommagés ayant contenu des informations critiques avant de les jeter définitivement.**
- **Il est recommandé de vérifier les permissions des fichiers du moteur de base de données et des chemins de sauvegarde.**

6. Glossaire

L'authentification: est le processus par lequel un système vérifie l'identité d'un utilisateur. Dans Oracle 19c, ce processus est effectué en dehors de l'environnement de l'application, par le biais d'un module d'authentification. Grâce aux différents modules qu'Oracle intègre, il est possible d'utiliser des protocoles d'authentification tels que LDAP, OS, TNS ou Kerberos. L'authentification de l'utilisateur est généralement effectuée par le système d'exploitation ou par un serveur externe.

Autorisation: processus consistant à déterminer si un utilisateur authentifié a accès aux informations et aux autorisations demandées. Ce processus s'effectue entièrement dans Oracle 19c, en consultant les permissions associées à une identité spécifique.

Oracle 19c Native Encryption: Oracle 19c Native Encryption offre une capacité de cryptage intégrée pour protéger les images de sauvegarde des bases de données et les fichiers clés des bases de données contre tout accès non autorisé lorsqu'ils se trouvent sur un support de stockage externe. Le cryptage est un élément clé de la protection des données hors ligne.

TLS: Transport Layer Security est un protocole de communication dont l'objectif principal est d'assurer la confidentialité et l'intégrité des données entre deux applications en communication. Le protocole est composé de deux couches: le protocole d'enregistrement TLS et le protocole de poignée de main TLS. Pendant la négociation TLS, un algorithme de clé publique est utilisé pour échanger de manière sécurisée des signatures numériques et des clés de chiffrement entre un client et un serveur. Les informations d'identité et la clé sont utilisées pour établir une connexion sécurisée pour la session entre le client et le serveur. Une fois la session sécurisée établie, la transmission des données entre le client et le serveur est chiffrée à l'aide d'un algorithme symétrique, tel que l'AES.

Active Data Guard: est l'une des solutions de réplication des bases de données d'Oracle. Oracle Active Data Guard est une évolution de la précédente avec des améliorations en matière de disponibilité, de performance et de protection.

Oracle Label Security : est une fonctionnalité qui enregistre et applique les autorisations d'accès aux données en fonction des codes de projet, des régions ou des classifications de données. Ces contrôles réduisent

le risque d'accès non autorisé aux données sensibles et contribuent à démontrer la conformité aux réglementations.

AVDF: Oracle Audit Vault and Database Firewall est une solution de surveillance et de filtrage de l'activité des bases de données. Il intègre des agents de collecte de données d'audit, un pare-feu de base de données, des outils d'analyse et de rapport.

Global Temporary: type de table Oracle dont le caractère temporaire peut être défini au niveau de la transaction (les données existent pendant l'exécution de la transaction) ou de la session (les données existent pendant la durée de la session). Les données d'une table temporaire sont uniques à la session Oracle qui l'utilise.

Apprentissage automatique: Oracle Machine Learning est une fonctionnalité offerte dans le produit SQL Developer du fournisseur qui découvre des modèles et peut fournir des informations sur les données stockées.

OUI: Oracle Universal Installer. Oracle Universal Installer, outil d'installation des logiciels Oracle.

DBCA: DataBase Computer Assistant. Logiciel qui facilite la création de bases de données Oracle. Nécessite l'installation du logiciel de gestion de base de données Oracle.

DBUA: DataBase Computer Assistant. Assistant pour la mise à jour des bases de données.

CDB: Base de données conteneur d'objets, qu'il s'agisse de schémas, d'autres objets de schémas ou d'autres objets.

PDB: Base de données enfichable qui se comporte comme un conteneur dans l'architecture CDB, elle compose une collection d'objets indépendants d'autres pdbs avec leurs propres fichiers de données.

OPatch: utilitaire basé sur Java qui permet l'application et le retour en arrière des correctifs aux logiciels Oracle.

Oracle Enterprise Manager: est une plateforme de gestion qui fournit un tableau de bord unique pour gérer toutes les bases de données Oracle.

SSH: Secure Shell (SSH) est un protocole permettant d'établir une connexion à distance sécurisée et d'autres services réseau sécurisés

sur un réseau non sécurisé. SSH peut être utilisé comme base pour un certain nombre de services réseau sécurisés, car il offre un chiffrement robuste, une authentification du serveur et une protection de l'intégrité. Il assure également la compression des données. SSH est utilisé pendant l'installation pour configurer les nœuds membres du cluster, et SSH est utilisé après l'installation par les assistants de configuration, Oracle Enterprise Manager, Opatch et d'autres fonctionnalités.

RCAC: Row and Column Access Control (contrôle d'accès aux lignes et aux colonnes). Il permet de contrôler l'accès à une table au niveau des lignes, des colonnes ou des deux. Il peut être utilisé pour compléter le modèle de privilège de table, en garantissant que les informations sont protégées de manière adéquate et que les utilisateurs n'ont accès qu'au sous-ensemble de données nécessaire à l'exécution de leurs tâches professionnelles et au respect de règles et réglementations spécifiques.

LBAC: Label Based Access Control. Il s'agit d'un modèle de sécurité principalement destiné aux applications gouvernementales ou aux applications dont le degré de classification est connu, car il exige que les données et les utilisateurs soient classifiés à l'aide d'un ensemble fixe de règles qui sont mises en œuvre.

DBA: Administrateur de base de données.

MV: Materialized View. Une vue matérialisée dans Oracle est un objet de base de données qui contient les résultats d'une requête. Ils sont des copies locales de données situées à distance ou sont utilisés pour créer des tableaux récapitulatifs basés sur des agrégations de données d'une table. Les vues matérialisées, qui stockent des données basées sur des tables distantes, sont également connues sous le nom d'instantanés. Le moteur de base de données peut renvoyer les données d'une vue matérialisée pour améliorer les performances. Les données consistent en des résultats pré-calculés à partir des tables spécifiées dans la définition de la vue matérialisée.

FIPS: Federal Information Processing Standards. La publication 140-2 des Federal Information Processing Standards (FIPS) est une norme du gouvernement américain qui définit les exigences de sécurité minimales pour les modules cryptographiques dans les produits de technologie de l'information, comme défini dans la section 5131 de l'Information Technology Management Reform Act de 1996.

7. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NUM.	MESURE	MOTIF
MISE EN ŒUVRE SÉCURISÉE	1	Sur les systèmes Unix ou Linux, il est recommandé de spécifier des noms d'utilisateurs différents de ceux créés par défaut.	Évitez d'utiliser les noms par défaut pour planifier des attaques sur la base de données.
	2	Sur les systèmes Windows, il est recommandé de modifier ce paramètre par défaut et de spécifier des noms d'utilisateur différents pour chaque rôle.	Évitez d'utiliser les noms par défaut pour planifier des attaques sur la base de données.
	3	Il est recommandé de créer des identifiants de propriétaire d'instance spécifiques à chaque instance, en l'ajoutant uniquement en tant que membre du groupe de propriétaires d'instance et en ne l'utilisant dans aucun autre groupe.	Il permet un meilleur contrôle du nombre d'utilisateurs et de groupes qui peuvent modifier l'instance.
	4	Pendant l'installation, il est recommandé d'utiliser des mots de passe forts, conformes aux politiques de sécurité de l'organisation.	Réduit au minimum les possibilités d'attaques par force brute.

7. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NUM.	MESURE	MOTIF
CONTRÔLE D'ACCÈS	5	Il est recommandé d'utiliser des mécanismes d'authentification et de communication forts tels que SERVER, LDAP TLS ou Kerberos et d'éviter d'utiliser l'authentification CLIENT, notamment dans les environnements où la sécurité du client ne peut être garantie.	Améliorer la sécurité et la fiabilité des mécanismes d'authentification.
	6	Il est recommandé de suivre le principe du moindre privilège, selon lequel seuls les utilisateurs sont autorisés à accéder aux informations et à effectuer les actions dont ils ont réellement besoin.	Réduire au minimum la surface d'exposition.
	7	Il est recommandé d'examiner et, si nécessaire, de révoquer les autorisations des utilisateurs ou des groupes qui n'en ont pas besoin.	Réduire au minimum la surface d'exposition.
	8	Dans les scénarios où des données sensibles sont stockées, il est recommandé, en plus de l'examen des privilèges, d'établir des contrôles d'accès granulaires.	Empêcher l'accès aux rôles sensibles depuis des environnements non fiables.
	9	Il est recommandé de révoquer les privilèges d'accès aux données du DBA s'il n'a pas réellement besoin d'accéder aux données.	Par défaut, un DBA a accès à toutes les tables de son instance de base de données. Cela présente un risque, surtout si le compte a été violé ou si ces privilèges sont utilisés de manière abusive.
	10	Il est recommandé de vérifier que l'accès PUBLIC n'a été accordé à aucune base de données.	Réduire au minimum la surface d'exposition.
	11	Il est recommandé de réviser et de protéger les tables et les vues importantes du système telles que ALL_OBJECTS, ALL_SOURCE.	Un utilisateur non autorisé peut accéder aux informations résidant dans les tableaux du système si ceux-ci n'ont pas été protégés de manière adéquate.
	12	Il est recommandé d'attribuer des privilèges par le biais d'un modèle de rôle, en évitant l'attribution directe aux utilisateurs.	Améliorer le contrôle et la maintenance des privilèges d'accès.
	13	Il est recommandé d'utiliser les contrôles d'accès du système d'exploitation.	Empêcher les administrateurs du système d'exploitation d'obtenir un accès trop important.
	14	Il est recommandé d'attribuer les autorisations DBA uniquement par le biais d'un rôle, et de contrôler l'accès à ce rôle par	Permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
	15	Il est recommandé de révoquer le privilège de créer des bases de données pour tous les utilisateurs sauf le DBA.	Réduire au minimum la surface d'exposition.

7. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NUM.	MESURE	MOTIF
AUDIT	16	Il est recommandé d'examiner les besoins en matière de journalisation des événements d'audit et de ne retenir que les événements importants pour l'organisation ou ceux qui sont liés à la sécurité du système.	Contrôler les informations d'audit générées, en évitant les données non pertinentes et les problèmes de stockage qui peuvent entraîner la perte d'éléments probants pertinents.
	17	Il est recommandé de créer un rôle AUDITOR et d'accorder les privilèges nécessaires pour lire et gérer les événements d'audit.	Contrôlez qui peut accéder aux informations d'audit et comment.
	18	Il est recommandé de contrôler l'accès au rôle AUDITOR par le biais de contextes de confiance.	Permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
	19	Il est recommandé que les fichiers d'audit générés ne soient pas copiés, modifiés ou supprimés directement par l'administrateur du système d'exploitation ou par tout autre utilisateur non autorisé de la plate-forme.	Empêchez l'exfiltration de données ou l'accès à des informations d'audit sensibles en contournant les mécanismes de sécurité des bases de données.
	20	Il est recommandé de faire appel à un service centralisé de piste d'audit.	Unification des différentes sources d'audit, facilitant la corrélation des journaux et évitant la perte ou la manipulation des preuves.
	21	Il est recommandé de crypter les enregistrements de création stockés sur disque (données au repos), à la fois sur le serveur de base de données et sur le service de centralisation des journaux, s'il existe.	Empêchez l'exfiltration de données ou l'accès à des informations d'audit sensibles en contournant les mécanismes de sécurité des bases de données.
	22	Il est recommandé d'auditer toutes les actions du DBA.	Conservez une piste d'audit des actions administratives susceptibles de compromettre le système.
	23	Il est recommandé d'auditer l'accès des utilisateurs, en particulier ceux qui ont accès à des données sensibles.	Conserver une piste d'audit des actions des utilisateurs.
	24	Il est recommandé d'auditer tous les accès aux tables importantes.	Conservez une piste d'audit des actions susceptibles de compromettre le système.
	25	Il est recommandé d'auditer les objets du schéma SYS.	Le maintien d'une piste d'audit de ces objets vous permettra de garder la trace des modifications apportées aux objets tels que les tables, les vues, les index, etc.....
	26	Il est recommandé d'auditer toutes les tentatives de création de bases de données.	Conservez une piste d'audit des actions administratives susceptibles de compromettre le système.

7. Tableau récapitulatif des mesures d'amélioration de sécurité

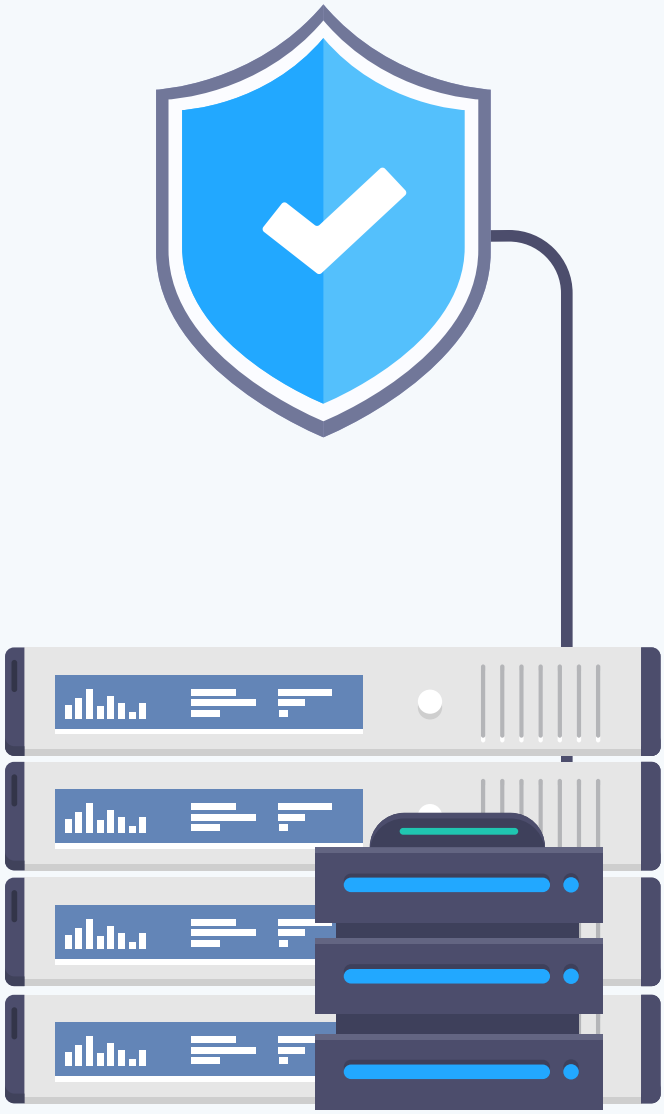
CHAMP	NUM.	MESURE	MOTIF
PROTECTION DES COMMUNICATIONS	27	Il est recommandé d'utiliser le cryptage avec les algorithmes sécurisés exposés dans la couche de communication.	Empêcher la capture de données en transit sur le réseau.
	28	Il est recommandé de ne pas chiffrer avec des algorithmes marqués comme obsolètes par le fabricant.	Le fabricant marque les algorithmes suivants comme obsolètes : DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 et RC4_256, et ils ne doivent pas être utilisés.
	29	Il est recommandé d'utiliser des jeux d'algorithmes de chiffrement robustes approuvés par le Centre national de cryptologie.	Empêcher l'exploitation des vulnérabilités des algorithmes faibles ou obsolètes.
	30	Il est recommandé de vérifier que vous disposez d'une version récente d'Oracle 19c.	Les anciennes versions utilisent des algorithmes de cryptage faibles ou vulnérables qui ne doivent pas être utilisés.
	31	Il est recommandé d'installer le patch de support des algorithmes avancés de ce document.	Oracle 19c a le correctif pour 2118136.2installer des chiffrages avancés.
	32	Pour activer TLS 1.2 (SSl 3.0) dans Oracle 19c, il est recommandé d'utiliser des certificats émis par une autorité de certification de confiance.	Il permet de valider correctement la chaîne d'émission du certificat et donc sa confiance.
	33	Il est recommandé de vérifier et de configurer les ports utilisés par toutes les instances du serveur en utilisant le fichier de services pour faire correspondre le nom du service dans le fichier de configuration de l'administrateur de la base de données du serveur à son numéro de port.	Réduisez la surface d'exposition en n'autorisant que les ports de communication nécessaires.
	34	Il est recommandé de configurer le WAF d'Oracle.	Le pare-feu propre au fabricant permet de mettre en place des règles spécifiques adaptées à chaque environnement.
PROTECTION DES INFORMATIONS	35	Il est recommandé de concevoir et d'utiliser des politiques granulaires d'accès aux enregistrements ou aux colonnes (RCAC) dans les environnements où il existe des réglementations ou des normes à respecter et où l'accès aux données doit se faire en fonction du contexte du demandeur.	Respecter le principe du "besoin de savoir".

7. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NUM.	MESURE	MOTIF
PROTECTION DES INFORMATIONS	36	Il est recommandé d'utiliser LBAC au niveau du registre lors du traitement d'informations sensibles ou classifiées liées à des entités gouvernementales.	Respecter le principe du "besoin de savoir".
	37	Il est recommandé d'utiliser LBAC au niveau du registre lorsque les affirmations suivantes sont vraies : – Le degré de classification des données est connu. – La classification des données peut être représentée par une ou plusieurs étiquettes de sécurité LBAC. – Les règles d'autorisation peuvent être liées aux composants de l'étiquette de sécurité.	Respecter le principe du "besoin de savoir".
	38	Le LBAC au niveau de la colonne vertébrale est recommandé lorsque : – Il est nécessaire de protéger les colonnes sensibles contre les accès non autorisés des propriétaires de la table ou même du DBA. – Il est nécessaire de protéger des tables entières contre tout accès non autorisé aux propriétaires de la table ou même au DBA.	Respecter le principe du "besoin de savoir".
	39	Indépendamment des contrôles d'accès mis en place, il est recommandé d'utiliser des mécanismes de cryptage au repos pour les données, les tableaux, les fichiers d'audit et les fichiers de sauvegarde au niveau du système d'exploitation.	Empêcher tout accès non autorisé à des informations sensibles en dehors du champ de protection de la base de données.
BACKUP	40	Il est recommandé de crypter tous les fichiers de sauvegarde et les images d'archive, quel que soit le support sur lequel ils sont stockés.	Empêcher tout accès non autorisé aux sauvegardes.
	41	Il est recommandé de veiller à ce que la restauration de toute sauvegarde nécessite un accès contrôlé à la clé de chiffrement et fasse l'objet d'un audit, tant pour l'accès que pour la restauration elle-même.	Empêchez tout accès non autorisé aux sauvegardes et enregistrez tout accès par le biais de l'audit.

centro criptológico nacional

centro criptológico nacional



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es