CCN-CERT

BP/23

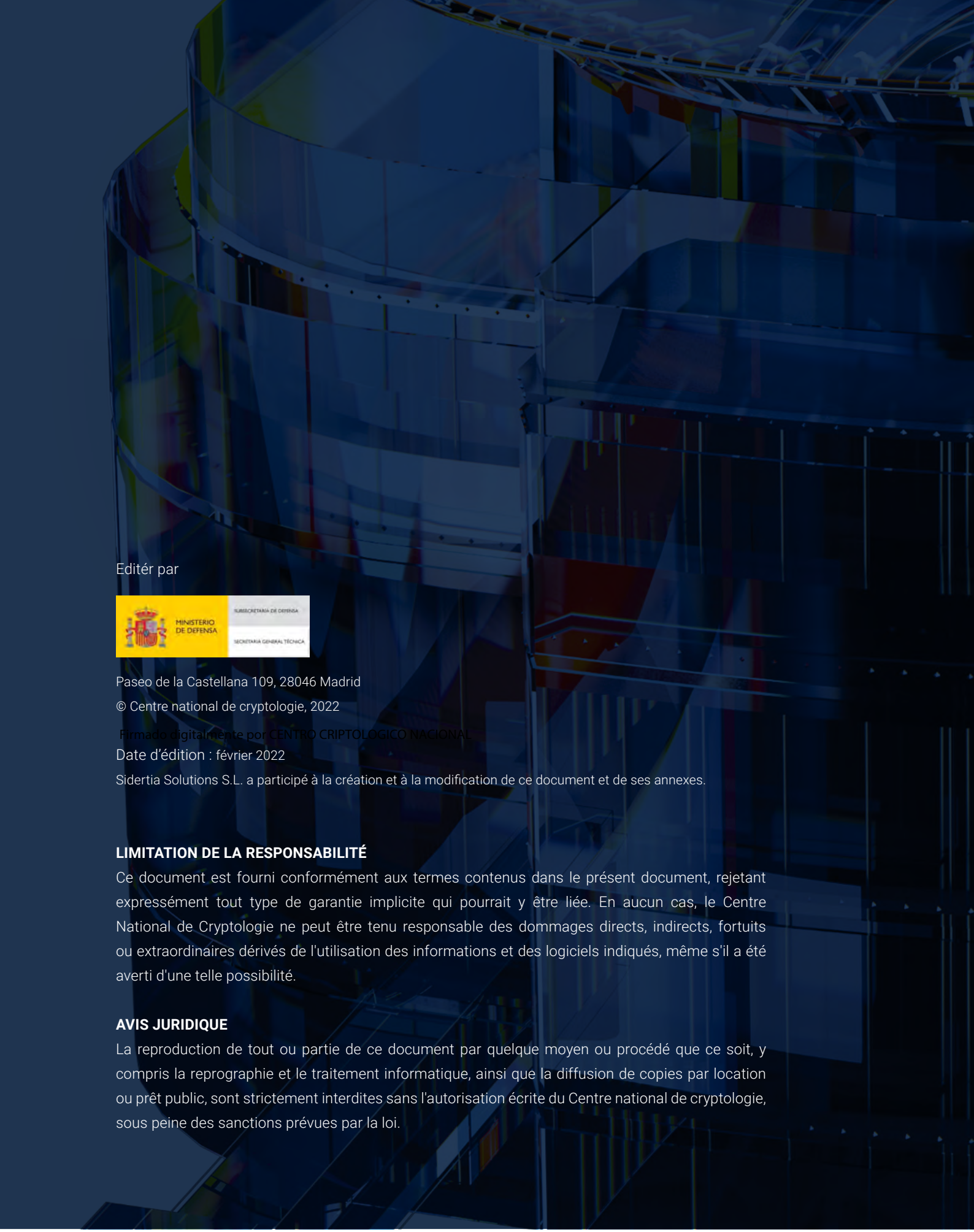
Recommandations en matière de sécurité pour les bases de données DB2

RAPPORT DE BONNES PRATIQUES

OCTOBRE **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Editér par

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

Firmado digitalmente por CENTRO CRIPTOLOGICO NACIONAL

Date d'édition : février 2022

Sidertia Solutions S.L. a participé à la création et à la modification de ce document et de ses annexes.

Index

1. À propos du CCN-CERT, Certificat gouvernemental national

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.

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie

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 responsable 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 :

1. L'étendue de la plate-forme sur laquelle le service est exécuté.
2. L'environnement et les capacités fournis par le gestionnaire de base de données lui-même..

Le produit IBM DB2 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 DB2, tels que les processus d'autorisation et le contrôle d'accès aux données résidant dans les différentes 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.

L'authentification est le processus par lequel un système vérifie l'identité d'un utilisateur. Dans DB2, ce processus est effectué en dehors de l'environnement de l'application, par le biais d'un module d'authentification. Grâce aux différents modules que DB2 intègre, il est possible d'utiliser des protocoles d'authentification tels que LDAP et Kerberos. L'authentification de l'utilisateur est généralement effectuée par le système d'exploitation ou par un serveur externe.

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

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 IBM DB2, en consultant les permissions associées à une identité spécifique. En ce sens, il existe différents types de permissions qui peuvent être accordées.

A. **Autorisations primaires :** celles qui sont accordées directement à l'identifiant d'autorisation.

B. **Autorisations secondaires :** celles qui sont accordées aux groupes et aux rôles dont un identifiant d'autorisation est membre.

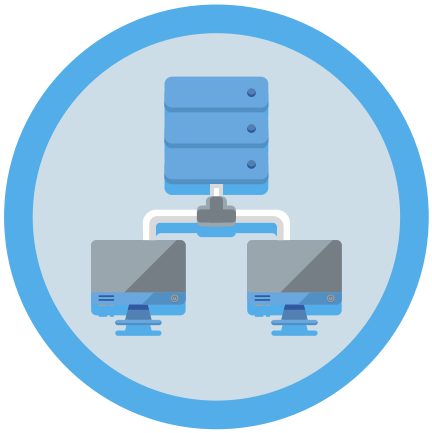
C. **Permis publics :** ceux qui sont accordés à l'entité PUBLIC.

D. **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 :

E. **Autorisation au niveau du système :** Les autorités d'administration du système (SYSADM), de contrôle du système (SYSCTRL), de maintenance du système (SYSMAINT) et de supervision du système (SYSMON) fournissent divers degrés de contrôle sur les fonctions au niveau de l'instance. Il s'agit d'un moyen de regrouper les privilèges et de contrôler les actions telles que les opérations de maintenance et autres tâches pour les instances, les bases de données et les objets de base de données.

F. **Autorisation au niveau de la base de données :** Les autorités administrateur de la sécurité (SECADM), administrateur de la base de données (DBADM), contrôle d'accès (ACCESSCTRL), accès aux données (DATAACCESS), administrateur SQL (SQLADM), administrateur de la gestion de la charge de travail (WLMADM), chargement de données dans une table (LOAD) et connexion à une base de données (CONNECT), fournissent divers degrés de contrôle au sein de la base de données.



G. **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.

H. **Autorisation basée sur le contenu :** les vues constituent un moyen d'autoriser l'accès basé sur le contenu. Les vues vous permettent de contrôler quelles colonnes ou lignes d'un tableau peuvent être lues par des utilisateurs spécifiques. Le contrôle d'accès basé sur les étiquettes (LBAC), quant à lui, détermine quels utilisateurs ont le droit de lire et d'écrire des lignes et des colonnes individuelles..

Un autre élément important pour définir la sécurité d'un gestionnaire de base de données est le cryptage, tant des données en transit que des données au repos. BD2 propose différentes options de cryptage des données.

Pour le cryptage des données au repos, les options suivantes sont disponibles :

- Cryptage natif de DB2 pour crypter les bases de données et les images de sauvegarde.
- Solution IBM InfoSphere Guardium Data Encryption pour chiffrer les données du système d'exploitation sous-jacent et les fichiers de sauvegarde.
- Le système de fichiers chiffrés AIX (EFS) pour chiffrer les données du système d'exploitation et les fichiers de sauvegarde.

Pour chiffrer les données en transit entre les clients DB2 et les bases de données, il est recommandé d'utiliser le support TLS natif inclus dans DB2 pour les communications inter-bases de données :

- Clients et serveurs DB2.
- Nœuds primaires et de secours dans un environnement DB2 HADR.
- Des clients DB2 et un serveur de fédération DB2.

NOTE :

Le type d'authentification DATA_ENCRYPT est déprécié et pourrait être supprimé dans une prochaine version. Pour crypter les données en transit entre les clients et les bases de données DB2, il est recommandé d'utiliser le support TLS (Transport Layer Security) du système de base de données DB2. En outre, DATA_ENCRYPT et SERVER_ENCRYPT utilisent des algorithmes faibles qui ne sont pas compatibles avec les directives du CCN-STIC et ne doivent pas être utilisés.

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

Au cours du processus d'installation de la base de données DB2, un ID utilisateur, un groupe et un mot de passe sont créés. Ces valeurs sont créées par défaut si elles ne sont pas modifiées pendant l'installation. Selon la plate-forme où DB2 est installé, différentes valeurs sont créées :

A. **Systèmes d'exploitation UNIX et Linux :** L'assistant d'installation crée, par défaut, l'utilisateur "dasusr" pour le DAS, "db2inst" pour le propriétaire de l'instance et "db2fenc" comme utilisateur clôturé. Il est recommandé de spécifier des noms d'utilisateurs différents de ceux créés par défaut.
Si un utilisateur par défaut existe déjà, l'assistant d'installation ajoute un numéro de 1 à 99 au nom par défaut, jusqu'à ce qu'un ID utilisateur qui n'existe pas encore puisse être créé.

.

B. **Systèmes d'exploitation Microsoft Windows :** par défaut, l'assistant d'installation crée un seul nom d'utilisateur : l'utilisateur (db2admin) pour l'utilisateur DAS, le propriétaire de l'instance et les utilisateurs délimités. Il est recommandé de modifier ce paramètre par défaut et de spécifier des noms d'utilisateur différents pour chaque rôle. Contrairement aux systèmes d'exploitation Linux et UNIX, aucune valeur numérique n'est ajoutée à l'ID utilisateur..

Au cours du processus d'installation de la base de données DB2, un ID utilisateur, un groupe et un mot de passe sont créés

Comme indiqué ci-dessus, DB2 peut utiliser les mécanismes d'authentification propres au système d'exploitation pour authentifier les utilisateurs. Par conséquent, il est fortement recommandé de spécifier des exigences d'authentification forte au niveau du système d'exploitation.

Sur les systèmes d'exploitation Linux et UNIX, les mots de passe non définis sont traités comme NULL et tout utilisateur sans mot de passe sera considéré comme ayant un mot de passe NULL. Du point de vue du système d'exploitation, il s'agit d'une correspondance et l'utilisateur sera validé et pourra se connecter à la base de données.

Par défaut, la méthode de communication pour l'exécution des commandes dans les environnements de bases de données partitionnées sur les systèmes d'exploitation Linux et UNIX est basée sur l'outil "rsh". Cet outil transmet les mots de passe en texte non crypté sur le réseau, ce qui peut représenter un risque pour la sécurité.

Il est recommandé de configurer la variable de registre DB2RSHCMD pour définir le chemin d'accès à l'exécutable SSH afin d'améliorer la sécurité dans tout type d'environnement.

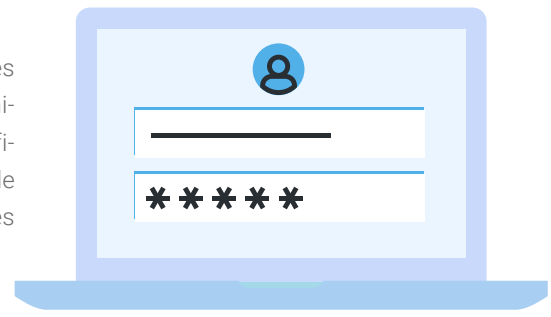
```
# db2set DB2RSHCMD=/usr/bin/ssh -i
```

Il est également conseillé d'examiner et de modifier les privilèges par défaut qui ont été accordés aux utilisateurs lors de l'installation. Par défaut, le processus d'installation accorde les privilèges d'administration du système (SYSADM) aux utilisateurs suivants sur chaque système d'exploitation :

A. **Sur les systèmes d'exploitation Linux et UNIX,** les privilèges SYSADM sont accordés à tout utilisateur valide appartenant au groupe primaire du propriétaire de l'instance..

B. **Sur les systèmes Microsoft Windows,** les privilèges SYSADM sont accordés aux membres du groupe Administrateurs locaux et du compte LocalSystem.

Si l'énumération des groupes a été configurée (LOCAL ou DOMAIN), les privilèges SYSADM seront également appliqués au groupe des administrateurs sur le contrôleur de domaine où les utilisateurs sont définis. La variable d'environnement DB2_GRP_LOOKUP vous permet de contrôler la façon dont DB2 effectue l'énumération des groupes sur les systèmes Windows.



Il est recommandé de créer des identifiants d'utilisateur propriétaire d'instance spécifiques à chaque instance, en l'ajoutant uniquement en tant que membre du groupe qui possède l'instance et en ne l'utilisant dans aucun autre groupe. Cela permet de mieux contrôler le nombre d'utilisateurs et de groupes qui peuvent modifier l'instance.

Par défaut, lors de l'installation, la sécurité étendue est activée sur tous les produits DB2 installés sous Windows. Dans ce cas, le programme d'installation crée deux nouveaux groupes DB2ADMNS et DB2USERS. Les membres du groupe DB2ADMNS bénéficient également des privilèges SYSADM.

Les privilèges attribués à chaque groupe d'utilisateurs lors de l'utilisation de la sécurité étendue de Windows sont indiqués ci-dessous.

PRIVILEGE	DB2ADMNS	DB2USERS	MOTIV
Agir en tant que partie du système d'exploitation (SeTcbPrivilege)	Y	N	Connexion de l'utilisateur
Générer des audits de sécurité (SeSecurityPrivilege)	Y	N	Manipulation des journaux d'audit et de sécurité
Prendre la propriété de fichiers ou d'autres objets (SeTakeOwnershipPrivilege)	Y	N	Modifier les ACL des objets
Augmenter la priorité d'ordonnancement (SeIncreaseBasePriorityPrivilege)	Y	N	Modifier la mémoire de travail des processus
Sauvegarde des fichiers et des répertoires (SeBackupPrivilege)	Y	N	Manipulation du profil et du registre (nécessaire pour exécuter certaines routines de manipulation du registre et du profil utilisateur : LoadUserProfile, RegSaveKey(Ex), RegRestoreKey, RegReplaceKey, RegLoadKey(Ex))
Restaurer les fichiers et les répertoires (SeRestorePrivilege)	Y	N	Manipulation du profil et du registre (nécessaire pour exécuter certaines routines de manipulation du registre et du profil utilisateur : LoadUserProfile, RegSaveKey(Ex), RegRestoreKey, RegReplaceKey, RegLoadKey(Ex))
Déboguer les programmes (SeDebugPrivilege)	Y	N	Manipulation de jetons (requis pour certaines opérations de manipulation de jetons et utilisé dans l'authentification et l'autorisation)

PRIVILEGE	DB2ADMNS	DB2USERS	MOTIV
Gérer l'audit et le journal de sécurité (SeAuditPrivilege)	Y	N	Générer des entrées d'audit
Se connecter en tant que service (SeServiceLogonRight)	Y	N	Exécution de DB2 en tant que service
Accéder à cet ordinateur depuis le réseau (SeNetworkLogonRight)	Y	N	Autoriser les informations d'identification du réseau (permet à l'administrateur de la base de données DB2 d'utiliser l'option LOGON32_LOGON_NETWORK pour s'authentifier, ce qui a des implications sur les performances)
Usurper l'identité d'un client après authentification (SeImpersonatePrivilege)	Y	N	Impersonnalisation du client (nécessaire pour Windows afin de permettre l'utilisation de certaines API pour usurper l'identité des clients DB2 : ImpersonateLoggedOnUser, ImpersonateSelf, RevertToSelf, etc.)
Verrouiller les pages en mémoire (SeLockMemoryPrivilege)	Y	N	Prise en charge des grandes pages de mémoire
Créer des objets globaux (SeCreateGlobalPrivilege)	Y	Y	Privilège permettant de créer des objets globaux dans une session Terminal Services (requis sous Windows)
Impersonate a client after authentication (SeImpersonatePrivilege)	Y	N	Suplantación de cliente (necesario para que Windows permita el uso de determinadas API para hacerse pasar por clientes DB2: ImpersonateLoggedOnUser, ImpersonateSelf, RevertToSelf, etc.)
Lock pages in memory (SeLockMemoryPrivilege)	Y	N	Soporte de páginas grandes de memoria
Create global objects (SeCreateGlobalPrivilege)	Y	Y	Privilegio para crear objetos globales en una sesión de Terminal Services (requerido en Windows)

Enfin, dans tous les cas, lors de l'installation, il est recommandé d'utiliser des mots de passe forts, conformes aux politiques de sécurité de l'organisation.

4. Configuration sécurisée de la base de données

Les recommandations suivantes permettent de renforcer la sécurité de la base de données DB2 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. DB2 fournit différents types d'authentification. Le type d'authentification utilisé est stocké dans le fichier de configuration sur le serveur et est configuré lors de la création de l'instance. Chaque instance peut avoir son propre type d'authentification pour accéder au serveur et aux bases de données fonctionnant sur cette instance.

- 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.

- 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, en plus de l'examen des privilèges, de mettre en place des contrôles d'accès granulaires tels que le contrôle d'accès par ligne et par colonne (RCAC) et le contrôle d'accès par étiquette (LBAC), afin d'empêcher l'accès aux rôles sensibles depuis des environnements non fiables.
- 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 de passer en revue et de protéger les tables importantes du système, telles que les tables de transit, d'exception, de réplication SQL, de clonage et de requêtes matérialisées (MQT).
- Il est recommandé d'attribuer des privilèges par le biais d'un modèle de rôle, en évitant l'attribution directe aux utilisateurs.
- 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.
- 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 vous permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
- Il est recommandé de révoquer le privilège de créer des bases de données pour tous les utilisateurs, à l'exception de l'utilisateur DBA.

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

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.

L'audit DB2 génère et conserve des preuves d'audit pour une série d'événements prédéfinis de la base de données. Les journaux générés sont stockés dans un fichier journal d'audit et leur analyse peut 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 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.

L'administrateur du système (qui a l'autorisation SYSADM) peut utiliser l'outil "db2audit" pour configurer l'audit au niveau de l'instance, ainsi que pour contrôler quand ces informations d'audit sont collectées.

L'audit est un élément fondamental pour renforcer la sécurité d'un environnement informatique, en particulier dans les environnements multi-utilisateurs

L'outil "db2audit" peut également être utilisé pour archiver les journaux d'audit des bases de données et des instances, ainsi que pour extraire les données d'audit des journaux archivés de tout type.

L'administrateur de sécurité (qui a l'autorité SECADM dans une base de données) peut utiliser des politiques d'audit en plus de la fonction SQL AUDIT pour configurer et contrôler les exigences d'audit pour une base de données individuelle.

L'administrateur de la sécurité peut utiliser les routines d'audit suivantes pour effectuer les tâches spécifiées :

- **La procédure stockée SYSPROC.AUDIT_ARCHIVE archive les enregistrements d'audit.**
- **La fonction de la table SYSPROC.AUDIT_LIST_LOGS vous permet de localiser les enregistrements qui vous intéressent**
- **La procédure stockée SYSPROC.AUDIT_DELIM_EXTRACT extrait les données dans des fichiers délimités pour les analyser.**

Du point de vue des informations d'audit générées, DB2 identifie les différents événements dans différentes catégories :

A. **Audit (AUDIT).** Génère des journaux lorsque la configuration de l'audit est modifiée ou lorsque le journal d'audit est consulté.

B. **Contrôle des autorisations (CHECKING).** Génère des journaux pendant le contrôle d'autorisation des tentatives d'accès ou de manipulation des objets ou fonctions de la base de données DB2

C. **Gestion des objets (OBJMAINT).** Génère des enregistrements lors de la création ou de la libération d'objets de données et lors de la modification de certains objets

D. **Maintenance de sécurité (SECMAINT).** Génère des enregistrements lorsque :

1. Les privilèges d'objet ou les autorisations de base de données sont accordés ou révoqués
2. Des labels de sécurité ou des exemptions sont accordés ou révoqués.
3. L'autorisation de groupe, l'autorisation de rôle ou le remplacement ou la restriction des attributs d'une politique de sécurité LBAC est modifiée
4. Le privilège SETSESSIONUSER est accordé ou révoqué
5. Vous modifiez l'un des paramètres de configuration : SYSADM_GROUP, SYSCTRL_GROUP, SYSMAINT_GROUP ou SYSMON_GROUP

E. **Administration du système (SYSADMIN).** Génère des journaux lorsque des opérations nécessitant une autorisation SYSADM, SYSMAINT ou SYSCTRL sont effectuées

F. **Validation de l'utilisateur (VALIDATE)**. Génère des journaux lors de l'authentification des utilisateurs ou de la récupération des informations de sécurité du système.

G. **Contexte de l'opération (CONTEXT).** Génère des enregistrements pour montrer le contexte de l'opération lorsqu'une opération de base de données est effectuée. Cette catégorie permet une meilleure interprétation du fichier journal d'audit.

H. **EXECUTER.** Génère des journaux pendant l'exécution des instructions SQL.

Pour chaque catégorie, des politiques d'audit peuvent être générées pour enregistrer les échecs, les succès ou les deux. L'activation de toutes les catégories et de tous les événements peut entraîner une surdéclaration et un nombre élevé d'enregistrements.

Pour chaque catégorie, des politiques d'audit peuvent être générées pour enregistrer les échecs, les succès ou les deux

- 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.
- Il est recommandé de créer un rôle AUDITOR et d'accorder les privilèges nécessaires pour lire et gérer les événements d'audit.
- Il est recommandé de contrôler l'accès au rôle AUDITOR par le biais de contextes de confiance. Cela permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
- 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.
- Il est recommandé de faire appel à un service centralisé de piste d'audit.
- 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.
- Il est recommandé d'auditer toutes les actions du DBA.
- Il est recommandé d'auditer l'accès des utilisateurs, en particulier ceux qui ont accès à des données sensibles.
- Il est recommandé d'auditer tous les accès aux tables importantes.
- Si un accès direct aux tables MQT (Materialised Query Tables) est nécessaire, il est recommandé d'activer l'audit granulaire de tous les accès SQL à ces tables.
- Il est recommandé d'auditer toutes les tentatives de création de bases de données.

4.3 Mesures de protection des communications

Db2 utilise le protocole TLS (Transport Layer Security) pour transmettre en toute sécurité les données entre les serveurs et les clients.

Pour protéger les données en transit avec le plus haut degré de fiabilité sur tous les réseaux utilisant TCP/IP, il est recommandé d'activer l'utilisation de TLS 1.2 ou supérieur et de limiter l'utilisation de SSL, TLS 1.0 ou TLS 1.1.

Il est recommandé d'utiliser des jeux d'algorithmes de chiffrement robustes approuvés par le Centre national de cryptologie.

Pendant la négociation du protocole TLS, le client et le serveur négocient la suite de chiffrement à utiliser pour échanger des données. Une suite de chiffrement est un ensemble d'algorithmes utilisés pour assurer l'authentification, le chiffrement et l'intégrité des données.

Db2 utilise GSKit fonctionnant en mode FIPS pour fournir le support TLS. GSKit prend en charge les suites de chiffrement suivantes :

ENSEMBLES D'ALGORITHMES SUPPORTÉS PAR GSKIT	
TLS_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Pendant la négociation, DB2 sélectionne automatiquement le jeu de chiffres le plus puissant supporté par le client et le serveur.

Si le serveur ne doit accepter qu'un ou plusieurs jeux de chiffres spécifiques, le paramètre de configuration "ssl_cipherspecs" peut être défini :

- L'une des valeurs ci-dessus.
- Une combinaison de valeurs, en séparant chaque valeur par une virgule, sans espace..
- Nul. Dans ce cas, l'algorithme disponible le plus puissant sera sélectionné.

Il est recommandé de vérifier que vous disposez d'une version récente de DB2 où les algorithmes de cryptage basés sur 3DES ont été désactivés. Si ce n'est pas le cas, il est recommandé de supprimer les ensembles d'algorithmes suivants de la liste des valeurs dans "ssl_cipherspecs" :

- TLS_RSA_WITH_3DES_EDE_CBC_SHA.
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA.
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA.

REMARQUE :

Ces algorithmes sont désactivés à partir des versions suivantes : Db2 V10.5 FP9, Db2 V11.1.2.2 et Db2 V11.5.0.0.

Pour activer TLS 1.2 dans DB2, il est recommandé d'utiliser des certificats émis par une autorité de certification de confiance.

La base de données DB2 utilise le port 523 pour le serveur d'administration DB2 (DAS), qui est utilisé par les outils de la base de données DB2. 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.

En outre, pour les environnements de bases de données partitionnées et les environnements Db2 pureScale, si la variable de registre DB2_FIREWALL_PORT_RANGE est définie, il est recommandé de n'autoriser que les connexions dans la plage de ports spécifiée entre les membres d'une même instance DB2.

Si cette variable de registre n'est pas définie, les connexions doivent être autorisées sur tous les ports non privilégiés entre les membres d'une même instance DB2. Les ports non privilégiés ont des numéros de port supérieurs ou égaux à 1024.

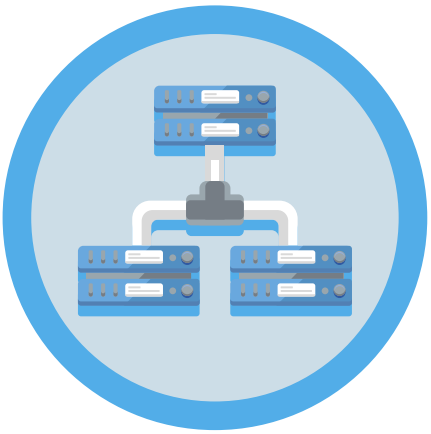
4.4 Mesures de protection des informations

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.

4.4.1 Contrôler l'accès en ligne et en colonne (RCAC)

À partir de la version 10.1 de DB2, la prise en charge de la configuration du contrôle d'accès aux lignes et aux colonnes (RCAC) est ajoutée comme couche supplémentaire de sécurité des données. Le RCAC contrôle l'accès à une table au niveau des lignes, des colonnes ou des deux et peut être utilisé pour compléter le modèle de privilège de la table.

Grâce à cette fonction, vous pouvez vous assurer que les informations sont protégées de manière adéquate et que les utilisateurs n'ont accès qu'au sous-ensemble de données dont ils ont besoin pour accomplir leurs tâches et se conformer aux règles et réglementations spécifiques.



Avantages du RCAC :

A. Le CCR respecte le principe du "besoin de savoir".

B. Aucun utilisateur de la base de données n'est intrinsèquement exempté des règles de contrôle d'accès aux lignes et aux colonnes.

C. Même les autorités de niveau supérieur, telles que les utilisateurs ayant l'autorité DATAACCESS, ne sont pas exemptées de ces règles.

D. Seuls les utilisateurs disposant du pouvoir d'administrateur de sécurité (SECADM) peuvent administrer les contrôles d'accès aux lignes et aux colonnes d'une base de données.

E. Les données de la table sont protégées quelle que soit la manière dont on accède à la table via SQL.

F. Les applications, les outils d'interrogation improvisés et les outils de rapport sont tous soumis aux règles du CCR. L'application est centrée sur les données.

G. Aucun changement d'application n'est nécessaire pour profiter de cette couche supplémentaire de sécurité des données.

Le modèle de sécurité basé sur le RCAC se concentre sur qui accède à quelles informations, et non sur un ensemble statique de permissions. Les ensembles de résultats pour une même requête changent en fonction du contexte dans lequel la requête a été demandée et aucun avertissement ou erreur n'est renvoyé.

Il est recommandé de concevoir et d'utiliser des politiques RCAC dans des 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.

Le modèle de sécurité basé sur le RCAC se concentre sur qui accède à quelles informations, et non sur un ensemble statique de permissions

4.4.2 Contrôle d'accès par étiquette (LBAC)

Le contrôle d'accès basé sur les étiquettes (LBAC) est un modèle de sécurité qui est principalement destiné aux applications gouvernementales ou aux applications dont les niveaux de classification sont connus, car il exige que les données et les utilisateurs soient classés à l'aide d'un ensemble fixe de règles qui sont mises en œuvre.

LBAC augmente considérablement le contrôle que vous avez sur les personnes qui peuvent accéder aux données, vous permettant de décider exactement qui a accès en écriture et qui a accès en lecture aux lignes et colonnes individuelles.

En revanche, le RCAC est un modèle de sécurité à usage général destiné principalement aux clients commerciaux. Toute organisation peut utiliser le RCAC pour créer ses propres règles de sécurité, ce qui permet une plus grande flexibilité.

Une politique de sécurité LBAC comprend ces informations :

A. Quels composants d'étiquettes de sécurité sont utilisés dans les étiquettes de sécurité qui font partie de la politique.

B. Quelles sont les règles utilisées pour comparer les composants de l'étiquette de sécurité.

C. Lesquels de certains comportements facultatifs sont utilisés lors de l'accès aux données protégées par la politique.

D. Quels sont les labels de sécurité et les exceptions supplémentaires à prendre en compte lors de l'application de l'accès aux données protégées par la politique de sécurité.

Chaque table protégée doit être associée à une et une seule politique de sécurité. Les lignes et les colonnes de cette table ne peuvent être protégées que par des étiquettes de sécurité qui font partie de cette politique de sécurité et tout accès aux données protégées suit les règles de cette politique.

Le contrôle d'accès basé sur les étiquettes (LBAC) est un modèle de sécurité qui est principalement destiné aux applications gouvernementales ou aux applications dont les niveaux de classification sont connus

Vous pouvez avoir plusieurs politiques de sécurité sur une seule base de données, mais vous ne pouvez pas avoir plus d'une politique de sécurité protégeant une table donnée.

LBAC est recommandé au niveau du registre lors du traitement d'informations sensibles ou classifiées liées à des entités gouvernementales.

LBAC au niveau du registre est recommandé lorsque les affirmations suivantes sont vraies :

A. Le degré de classification des données est connu.

B. La classification des données peut être représentée par une ou plusieurs étiquettes de sécurité LBAC.

C. Les règles d'autorisation peuvent être liées aux composants de l'étiquette de sécurité.

Le LBAC au niveau de la colonne vertébrale est recommandé lorsque :

A. Il est nécessaire de protéger les colonnes sensibles contre les accès non autorisés des propriétaires de la table ou même du DBA.

B. Il est nécessaire de protéger des tables entières contre tout accès non autorisé aux propriétaires de la table ou même au DBA. Dans ce cas, vous attribuerez une étiquette de sécurité à toutes les colonnes de la table, puis vous attribuerez l'étiquette de sécurité à un rôle et vous assignerez ce rôle uniquement aux utilisateurs qui doivent accéder aux informations de la table.

Les points suivants doivent être pris en compte avant de mettre en œuvre un modèle de sécurité basé sur LBAC :

A. LBAC n'autorisera jamais l'accès à des données qui sont interdites par un contrôle d'accès discrétionnaire.

B. Les politiques LBAC limitent uniquement l'accès aux données protégées. Ils n'ont aucun effet sur les données non protégées.

C. Les politiques LBAC ne sont pas vérifiées lorsque vous supprimez une table ou une base de données, même si la table ou la base de données contient des données protégées.

D. Les politiques LBAC ne sont pas vérifiées lors de la sauvegarde des données. Si un utilisateur peut exécuter une sauvegarde d'une table, les lignes qui sont sauvegardées ne sont en aucun cas limitées par la protection LBAC des données. De plus, les données sur le support de sauvegarde ne sont pas protégées par LBAC. Seules les données de la base de données sont protégées.

E. LBAC ne peut pas être utilisé pour protéger l'un des types de tableaux suivants :

1. Une table de mise en scène.
2. Une table dont dépend une table de mise à disposition.
3. Un tableau dactylographié.

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.

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.

5. Glossaire

L'authentification : est le processus par lequel un système vérifie l'identité d'un utilisateur. Dans DB2, ce processus est effectué en dehors de l'environnement de l'application, par le biais d'un module d'authentification. Grâce aux différents modules que DB2 intègre, il est possible d'utiliser des protocoles d'authentification tels que LDAP et 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 IBM DB2, en consultant les permissions associées à une identité spécifique.

DB2 Native Encryption : Db2 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.

HADR : High Availability Disaster Recovery. DB2 sur Red Hat OpenShift prend en charge la reprise après sinistre à haute disponibilité (HADR) pour protéger la base de données contre la perte de données. HADR fournit une solution de haute disponibilité aux pannes partielles et complètes

du site en répliquant les modifications d'une base de données source, appelée base de données primaire, vers des bases de données cibles, appelées bases de données de secours.

DB2 Federation Server : Un système fédéré est un type particulier de système de gestion de base de données (SGBD) distribué qui consiste en une instance de base de données agissant comme un serveur fédéré, une base de données agissant comme une base de données fédérée, une ou plusieurs sources de données et des clients (utilisateurs et applications) accédant à la base de données et aux sources de données. Un système fédéré sert de base sur laquelle une ou plusieurs solutions de virtualisation des données peuvent être construites. Dans un système fédéré, une seule instruction SQL peut accéder à des données réparties entre plusieurs sources de données.

Utilisateur clôturé : L'utilisateur clôturé est un type d'utilisateur utilisé pour exécuter des fonctions définies par l'utilisateur (UDF) et des procédures stockées en dehors de l'espace d'adressage utilisé par la base de données DB2. L'utilisateur par défaut est db2fenc1 et le groupe par défaut est db2fadm1.

DAS : Serveur d'administration DB2. Le serveur d'administration DB2 (DAS) est un point de contrôle qui sert uniquement à faciliter les tâches sur les instances de base de données DB2. Vous devez disposer d'un DAS en fonctionnement si vous souhaitez utiliser des outils tels que le Centre de réplication ou le Centre de développement. DB2 Administration Server (DAS) a été déprécié et pourrait être supprimé dans une prochaine version. DAS n'est pas pris en charge dans les environnements Db2 pureScale.

RSH : protocole permettant l'exécution à distance de commandes de console pour l'administration d'une base de données DB2. L'utilisation de rsh n'est pas recommandée en raison de l'utilisation d'algorithmes de cryptage faibles.

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.

Sécurité étendue : option d'installation qui est activée par défaut lorsque DB2 est installé sur des systèmes d'exploitation Windows. Cette option d'installation crée deux groupes de sécurité (DB2ADMNS et DB2USERS) au niveau du système d'exploitation et leur accorde des privilèges contrôlés.

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.

MQT : Materialized Query Tables. Les Materialised Query Tables (MQTs) sont des tables dont la définition est basée sur le résultat d'une requête. Les tables MTQ mettent en cache les résultats d'une requête et lorsque la requête est réexécutée, le moteur de base de données peut renvoyer les données de la table de requête matérialisée pour améliorer les performances. Les données consistent en des résultats pré-calculés à partir des tables spécifiées dans la définition de la table de consultation matérialisée.

GSKit : Global Security Kit. DB2 utilise les capacités cryptographiques du Global Security Kit (GSKit) pour chiffrer à la fois les données au repos (chiffrement natif) et les données en transit. Le GSKit est utilisé pour mettre en œuvre les protocoles SSL et TLS qui permettent de sécuriser les communications DB2 sur le réseau.

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.

DB2 pureScale : Un ensemble de technologies IBM qui aident à réduire les risques et les coûts associés à la croissance des solutions de bases de données distribuées en fournissant une capacité extrême et une transparence des applications. L'environnement Db2 pureScale est conçu pour une disponibilité continue et combine plusieurs composants logiciels intégrés dans une solution de base de données hautement disponible. Ces composants sont automatiquement installés et configurés lorsque DB2 pureScale Feature est déployé.

6. Summary table of security enhancement measures

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 configurer la variable de registre DB2RSHCMD pour définir le chemin d'accès à l'exécutable SSH afin d'améliorer la sécurité dans ce type d'environnement.	Par défaut, sur les systèmes d'exploitation Linux et UNIX, DB2 utilise l'outil rsh. Cet outil transmet les mots de passe en clair sur le réseau, ce qui peut constituer un risque pour la sécurité.
	4.	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.
	5.	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.

CHAMP	NUM.	MESURE	MOTIF
CONTRÔLE D'ACCÈS	6.	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.	Améliorer la sécurité et la fiabilité des mécanismes d'authentification.
	7.	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.
	8.	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.
	9.	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.
	10.	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.
	11.	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.
	12.	Il est recommandé de passer en revue et de protéger les tables système importantes telles que les tables Staging, Exception, SQL Replicated, Clone et Materialized Query (MQT).	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.
	13.	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.
	14.	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.

6. Summary table of security enhancement measures

CHAMP	NUM.	MESURE	MOTIF
CONTRÔLE D'ACCÈS	15.	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.	Permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
	16.	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.
AUDIT	17.	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.
	18.	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.
	19.	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.
	20.	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.
	21.	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.
	22.	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.
	23.	Il est recommandé d'auditer toutes les actions du DBA.	Conservez une piste d'audit des actions administratives susceptibles de compromettre le système.

CHAMP	NUM.	MESURE	MOTIF
AUDIT	24.	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.
	25.	Il est recommandé d'auditer tous les accès aux tables importantes.	Conservez une piste d'audit des actions susceptibles de compromettre le système.
	26.	Si un accès direct aux tables MQT (Materialised Query Tables) est nécessaire, il est recommandé d'activer l'audit granulaire de tous les accès SQL à ces tables.	Conservez une piste d'audit des actions susceptibles de compromettre le système.
	27.	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.
PROTECTION DES COMMUNICATIONS	28.	Il est recommandé d'utiliser la prise en charge native de TLS incluse dans DB2 pour les communications entre les utilisateurs : · Clients et serveurs DB2. · Nœuds primaires et de secours dans un environnement DB2 HADR · Des clients DB2 et un serveur de fédération DB2.	Empêcher la capture de données en transit sur le réseau.
	29.	Pour crypter les données en transit entre les clients et les bases de données DB2, il est recommandé d'utiliser le support TLS (Transport Layer Security) du système de base de données DB2.	Le type d'authentification DATA_ ENCRYPT est déprécié et pourrait être supprimé dans une future version. DATA_ENCRYPT et SERVER_ENCRYPT utilisent des algorithmes faibles qui ne sont pas compatibles avec les directives du CCN-STIC et ne doivent pas être utilisés.
	30.	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.
	31.	Il est recommandé de vérifier que vous disposez d'une version récente de DB2 où les algorithmes de cryptage basés sur 3DES ont été désactivés.	Les anciennes versions utilisent des algorithmes de cryptage faibles ou vulnérables qui ne doivent pas être utilisés.

CHAMP	NUM.	MESURE	MOTIF
PROTECTION DES COMMUNICATIONS	32.	Il est recommandé de supprimer les ensembles d'algorithmes suivants de la liste des valeurs dans "ssl_cipherspecs" : · TLS_RSA_WITH_3DES_EDE_CBC_SHA. · TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA. · TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA.	Les jeux d'algorithmes qui utilisent 3DES ou SHA1 sont considérés comme faibles ou vulnérables et ne doivent pas être utilisés.
	33.	Pour activer TLS 1.2 dans DB2, 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.
	34.	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.
	35.	Pour les environnements de bases de données partitionnées et les environnements Db2 pureScale, si la variable de registre DB2_FIREWALL_PORT_RANGE est définie, il est recommandé d'autoriser uniquement les connexions dans la plage de ports spécifiée entre les membres d'une même instance DB2.	Réduisez la surface d'exposition en n'autorisant que les ports de communication nécessaires.
PROTECTION DES INFORMATIONS	36.	Il est recommandé de concevoir et d'utiliser des politiques RCAC dans des 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".
	37.	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".

CHAMP	NUM.	MESURE	MOTIF
PROTECTION DES INFORMATIONS	38.	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".
	39.	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".
	40.	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	41.	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.
	42.	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.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


ccn-cert
centro criptológico nacional
CCN
centro criptológico nacional