CCN-CERT

BP/25

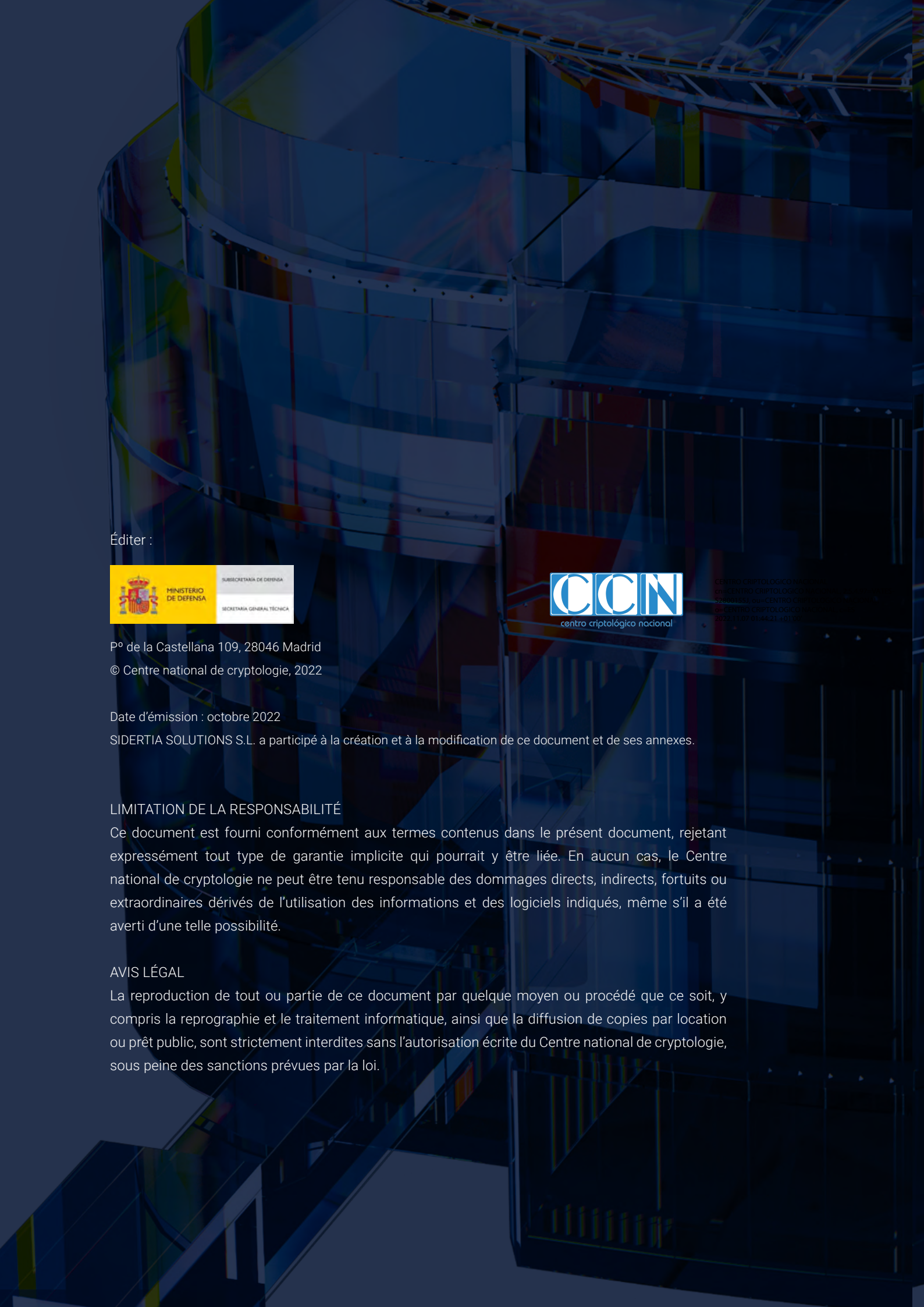
Recommandations de sécurité pour les bases de données Db2 sur zOS

RAPPORT DE BONNES PRATIQUES

FÉVRIER **2022**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Éditer :

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

Pº de la Castellana 109, 28046 Madrid

Date d'émission : octobre 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.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en tant que 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. Il se charge également de la coordination au niveau public de l'État, des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

Tout cela, dans le but ultime de parvenir à un cyberespace plus sûr et plus fiable, en préservant les informations classifiées (comme indiqué dans l'art. 4. 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 cyberincidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

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

2. Introduction

Les bases de données sont devenues le moteur fondamental des entreprises. Elles stockent en effet, des données sensibles et toutes les données nécessaires à la gestion des organisations allant des noms des clients, aux prix des produits, en passant par les données temporaires stockées pour les modifications des applications critiques de l'environnement.

Comme il s'agit d'un point d'accès à toutes sortes de cyberattaques, il convient de suivre des directives claires pour éviter de les exposer à des vulnérabilités potentielles.

La nécessité de ce document découle du fait que les meilleures pratiques et les directives doivent être imposées à la mise en œuvre, à la modification et à la maintenance de la base de données.

Le document suivant présente les bonnes pratiques et les meilleures procédures pour une utilisation sécurisée d'IBM Db2 version 12 sur les systèmes Z.

Au fil des ans, Db2 a reconnu et traité les problèmes de sécurité suivants :

- **Vol de privilèges ou mauvaise gestion**
- **Manipulation d'applications ou de serveurs d'applications**
- **Manipulation de données ou d'enregistrements**
- **Vol de supports de stockage**
- **Accès non autorisé à des objets.**

Il convient de noter que cette tâche reposera fondamentalement sur les **points clés** suivants :

- **Authentification**
- **Autorisation**
- **Intégrité des données**
- **Confidentialité**
- **Intégrité des systèmes**
- **Audit**

Mais ce n'est pas seulement le moteur de la base de données qui doit être pris en compte, il faut aussi octroyer une grande importance à l'environnement dans lequel il est déployé. Ce point sera fondamental pour la sécurité et la gestion des bases de données.

Dans ce document, comme déjà mentionné, l'accent sera mis sur le système d'exploitation z/OS, avec tout ce que peut impliquer le déploiement d'une base de données sur l'un des systèmes les plus sûrs du marché.

3. Bonnes pratiques

Indépendamment de la base de données qui est déployée sur le système d'exploitation z/OS, il y a toujours des directives de sécurité qui doivent être prises en compte.

Le moteur dans lequel la base de données est déployée fournit les blocs de construction pour les communications et l'accès à la base de données, d'où l'importance de la mise à jour et de la maintenance du système d'exploitation lui-même.

Une fois le système d'exploitation installé, il est recommandé de suivre les étapes suivantes dans le but de garantir une bonne pratique :

1. Mise à jour du système d'exploitation dans lequel la base de données est déployée.
2. Application des correctifs et mises à jour recommandés pour remédier aux vulnérabilités.
3. Abonnement aux nouvelles de sécurité concernant le système d'exploitation z/OS et la base de données Db2.
4. Utilisation d'autorisations avec authentifications par les utilisateurs et mot de passe.
5. Critères de sécurité spécifiques recommandés par les fournisseurs de systèmes d'exploitation eux-mêmes.

Le moteur dans lequel la base de données est déployée fournit les blocs de construction pour les communications et l'accès à la base de données, d'où l'importance de la mise à jour et de la maintenance du système d'exploitation lui-même.

4. Vérification de logiciels

Une fois le produit installé ou corrigé, il faut s'assurer que tout a été fait correctement et que le niveau de sécurité est aussi élevé que possible, en tenant compte des recommandations du fabricant pour ses produits.

Il est important, lorsqu'une mise à jour est effectuée, de lire attentivement la documentation fournie afin de savoir ce qu'elle implique et à quoi s'attendre.

Au niveau du logiciel, les actions suivantes doivent être effectuées :

- **Maintenance du produit sur la dernière version.**
- **Maintenance du produit avec le téléchargement de la FL intrinsèque de Db2 et les APAR nécessaires au bon fonctionnement de Db2 et de ses utilitaires.**
- **Mise à jour des correctifs de sécurité et d'évolution du produit.**
- **Vérifier, de temps en temps, les comptes qui ont des privilèges d'utilisateur root, pour voir s'il s'agit des comptes appropriés et pour vérifier s'ils sont réutilisés, clonés ou utilisés de manière inappropriée.**

Il est important, lorsqu'une mise à jour est effectuée, de lire attentivement la documentation fournie afin de savoir ce qu'elle implique et à quoi s'attendre.

- **Vérifier les éventuelles vulnérabilités du logiciel et du système d'exploitation dans lequel il a été déployé.**
- **Si l'on considère qu'une vulnérabilité a été découverte, le fabricant doit en être informé dès que possible avec une description détaillée du problème et des situations où des vulnérabilités ont été découvertes.**
- **Si le fabricant met en ligne un nouveau correctif en raison d'une vulnérabilité et que les personnes chargées de la mise à jour des correctifs n'ont pas effectué l'actualisation, vous devez contacter l'équipe des systèmes pour que le correctif soit appliqué au plus vite.**
- **Nettoyer les fichiers temporaires.**
- **Maintenir à jour les systèmes qui communiquent avec la base de données.**
- **Maintenir à jour le moteur de la base de données.**
- **Maintenir à jour et sécuriser les canaux donnant accès à la base de données est accessible.**

5. Contrôle de l'accès aux données

L'accès aux données peut se faire par le biais d'utilisateurs souhaitant appeler des informations spécifiques, comme les processus dans l'environnement lui-même. C'est-à-dire depuis des terminaux interactifs aux procédures de stockage locales ou distantes, aux utilitaires ou aux transactions CICS ou IMS. Elle peut également provenir d'applications fonctionnant en mode batch, d'applications utilisant le DDF ou le CLI ou de connexions via JDBC.

Pour que tout cela fonctionne correctement, il est recommandé d'utiliser différents utilisateurs et rôles qui peuvent accéder aux données avec différents privilèges de sécurité, ceux-ci devant être octroyés en fonction de l'accès nécessaire à chaque utilisateur ou programme avec une étude préalable de chaque cas d'utilisation.

Les autorisations doivent être données pour chaque vue, table, schéma, objet, etc. Pour ce faire, il sera nécessaire de :

- Définir des règles d'autorisation pour les systèmes Db2.
- Définir les niveaux de sécurité dans les objets Db2.
- Définir les profils d'utilisateurs et les rôles qui peuvent accéder aux données et comment y accéder.

- Garantir la possibilité d'auditer les entrées de données pour vérifier que les règles de sécurité appropriées ont été créées.
- Le système doit toujours être en mesure de connaitre l'origine de la demande ou « qui » fait la demande.
- La création, la modification et la suppression des comptes, des identifiants, des rôles ou des groupes doivent être centralisées dans un rôle unique de l'administrateur de la base de données. En outre, il/elle est chargé(e) d'accréditer les différents niveaux de sécurité comme convenu avec les rôles du système de sécurité.

5.1 Autorisation selon identifiant d'utilisateur

L'une des façons d'analyser les entrées Db2 est de passer par l'identifiant de l'utilisateur principal ou primaire, donnant des privilèges de Db2 à ces utilisateurs.

Il est recommandé d'utiliser un identifiant primaire unique pour chaque système/personne qui veut accéder aux données, et un identifiant secondaire qui sera associé au primaire et auquel seront associées différentes couches de sécurité. Il s'agit de l'un des moyens d'identification des autorisations d'accès de chaque utilisateur à grande échelle. Accorder à un ID le privilège d'exécuter un plan ou un paquet peut fournir un ensemble de privilèges finement détaillé et peut éliminer la nécessité d'accorder d'autres privilèges séparément.

Il est recommandé d'utiliser un identifiant primaire unique pour chaque système/ personne qui veut accéder aux données, et un identifiant secondaire qui sera associé au primaire et auquel seront associées différentes couches de sécurité.

5.2 Autorisation selon le rôle

En outre, il est recommandé de créer des rôles d'utilisateur où les privilèges peuvent être garantis à ce niveau. Ce regroupement créé pour catégoriser les utilisateurs ou les identifiants aidera à la création de profils de sécurité par regroupement de types de poste dans la base de données.

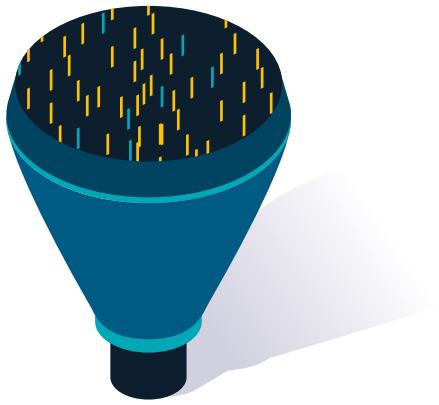
Parmi les rôles que l'on peut trouver, il y a certains rôles de base et communs qui doivent être pris en compte et créés en conséquence (ce ne sont pas les seuls rôles qui peuvent être utilisés, mais ils sont le minimum recommandé).

- **Rôle d'administrateur de la sécurité :**
  ce sont les responsables de la sécurité, en plus des comptes d'utilisateurs, des audits à effectuer ou de la gestion des clés de chiffrement.

- **Rôle d'administrateur de base de données :**
  implique un large éventail de tâches, depuis la génération de la base de données, la mise à jour du logiciel, le contrôle des performances, le démarrage et l'arrêt de la base de données, et même la création des sauvegardes nécessaires de la base de données. Ces utilisateurs doivent avoir des privilèges d'administration et de modification de la base de données.

  Il s'agit d'un rôle qui ne devrait être attribué qu'aux administrateurs, et qui, une fois la base de données créée, devrait être révoqué pour tous, à l'exception des administrateurs réels qui conservent le rôle.

  Ce rôle doit être revu périodiquement pour vérifier que les identifiants associés à ce rôle sont corrects.



- **Rôle d''utilisateur pour usage des données :**
  ce rôle convient aux utilisateurs chargés de l'usage et de l'exploitation des données commerciales. Ces utilisateurs ont généralement un accès en lecture seule.

- **Rôle d'administrateur de l'application :**
  il peut s'agir de comptes qui ne disposent que des privilèges permettant de mettre à jour et de corriger l'application.

- **Rôle de l'application :**
  cette catégorie pourrait englober les comptes d'identifiants provenant d'applications externes ou internes qui ont besoin de visualiser des données. Dans ce cas, ils ont généralement un accès en lecture et en écriture aux tables ou aux données nécessaires à leur application.

- **Rôle des utilisateurs réguliers de la base de données :**
  il s'agit notamment d'identifiants ayant un accès restreint à leurs données, tables, vues et objets spécifiques.

5.3 Accès basé sur la propriété

La propriété d'un objet s'accompagne d'un ensemble de privilèges connexes sur l'objet. Db2 fournit des contrôles séparés pour la création et la propriété des objets.

Si vous voulez empêcher les utilisateurs d'obtenir des privilèges implicites à partir de la propriété de l'objet, vous pouvez faire d'un rôle Db2 le propriétaire de l'objet. Pour ce faire, vous devez créer l'objet dans un contexte de confiance défini avec la clause ROLE AS OBJECT OWNER AND QUALIFIER.

5.4 Accès multiniveau

Également connu sous le nom d›accès multicouche, il permet de classer les utilisateurs et les rôles avec des niveaux de sécurité. Ces couches sont basées sur une hiérarchie de niveaux de sécurité plutôt que sur des catégories de sécurité.

Ce mode d'accès est encore renforcé par l'utilisation de la fonctionnalité de sécurité multiniveau propre à z/OS pour empêcher les utilisateurs non autorisés d'accéder à des classifications auxquelles ils ne devraient pas avoir accès.

S'il est utilisé au niveau des lignes, vous pouvez définir des politiques de sécurité très strictes pour les objets Db2 et effectuer des contrôles de sécurité au niveau des lignes. Ces contrôles permettent de visualiser quels utilisateurs sont autorisés à voir, modifier ou effectuer toute autre action sur des lignes de données.

L'utilisation de cet accès à plusieurs niveaux est recommandée pour les données très sensibles.

5.5 Accès externe

Vous pouvez contrôler l'accès à Db2 en utilisant une routine de sortie fournie par Db2 ou une routine de sortie que vous écrivez.

Si votre installation utilise l'une des routines de sortie d'autorisation de contrôle d'accès, vous pouvez l'utiliser pour contrôler la vérification et l'authentification des autorisations, au lieu d'utiliser d'autres techniques et méthodes.

5.6 Accès au niveau de l'utilisateur

Lorsque vous créez un utilisateur qui doit se connecter avec un mot de passe, l'administrateur de la base de données vous envoie un mot de passe temporaire que vous devez modifier la première fois que vous vous connectez au système. Le changement de mot de passe doit s'accompagner des directives suivantes :

- Le mot de passe ne doit pas contenir de mots tels que : USER, ADMINS, PUBLIC, GUESTS, ni aucun mot réservé de SQL.
- Si vous utilisez TSO, RACF ou l'une des autres applications de sécurité qui peuvent être connectées, vous devrez suivre les directives définies par chacune de ces applications de sécurité, car les mots de passe devront suivre les directives, telles que la longueur, de chacun de ces systèmes.
- Pour qu'un mot de passe soit fiable et sûr, il est recommandé :

1.	Au moins 12 caractères et pas plus de 15 caractères.
2.	Alterner entre les lettres majuscules et minuscules.
3.	Contenir au moins un numéro.
4.	Contenir au moins un caractère spécial (! # # $ $ % & ' ( ) * + , - . / : ; < = > ? @ ^ _).
5.	Ne pas contenir le nom de l'utilisateur ou tout autre nom de rôle.
6.	Ne pas contenir de dates de naissance, en général, des dates.
7.	Déterminer une limite du nombre de tentatives de connexion avec un mauvais mot de passe.
8.	Il doit être possible de verrouiller un utilisateur après un certain nombre de tentatives infructueuses (la limite des tentatives ne doit pas être supérieure à six).
9.	Fixer une limite de temps pour les sessions externes qui expirent dans le but de clôturer le système (la limite de temps recommandée est de 90 minutes, mais il convient d'étudier le cas de chacune des applications ou de chacun des utilisateurs effectuant cette session).
10.	Les mots de passe doivent être renouvelés au moins tous les trois mois. Il est recommandé de créer des rappels au niveau de l'utilisateur.

6. Accès au sous-système Db2

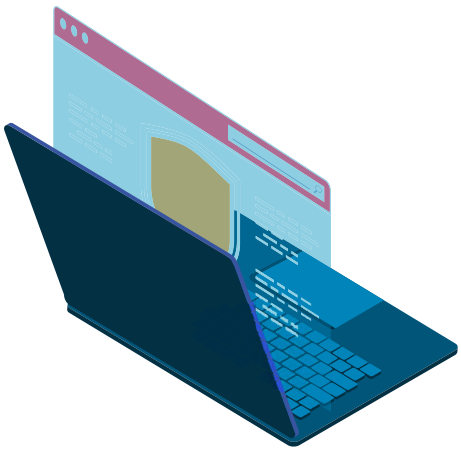
L'accès à un sous-système Db2 externe peut être contrôlé avec des produits tels que RACF.

6.1 Contrôle d'accès avec le programme RACF

Les avantages du contrôle de l'entrée des sous-systèmes avec RACF seront mentionnés ci-dessous :

- Identifier et vérifier l'identifiant associé au processus qui tente d'entrer.
- Connecter les identifiants aux rôles et groupes enregistrés dans RACF. La base de données de sécurité qui est appliquée sur z/OS.
- Auditer les différentes tentatives d'accès aux ressources protégées.

Il est recommandé d'utiliser l'accès aux bases de données par RACF tant que le système est opérationnel dans le même sous-système où se trouve la base de données.



6.2 Contrôle d'accès avec IMS Terminal Security

IMS Terminal Security vous permet de contrôler et de limiter les entrées d'un code de transaction à un LTERM ou à des groupes de LTERMS dans le système. Pour protéger un programme particulier, vous devez autoriser l'introduction d'un code de transaction dans la liste des LTERMS. Vous pouvez également associer chaque LTERM à une liste de codes de transaction qu'un utilisateur peut saisir à partir de ce LTERM.

Ce code sera celui qui est transmis à Db2 comme identifiant et qui est enregistré.

L'utilisation de ce produit est recommandée, à condition qu'il soit installé sur un système de fonctionnement du moteur.

6.3 Contrôle d'accès avec sécurité par code de transaction CICS

La sécurité du code de transaction CICS fonctionne avec RACF pour contrôler quelles transactions et quels programmes peuvent accéder à Db2. L'option peut être activée ou désactivée dans les opérations de liaison pour limiter l'accès à des sous-systèmes CICS spécifiques.

L'utilisation de ce produit est recommandée lorsque des transactions CICS sont utilisées pour les appels de base de données et qu'il est mis en œuvre dans le système.

6.4 Appels locaux et distants

6.4.1 Les appels des systèmes locaux

Le logon TSO pourrait être utilisé pour se connecter aux systèmes internes.

Si vous exécutez Db2 avec TSO et que vous utilisez l'identifiant TSO comme identifiant Db2 principal, c'est TSO lui-même qui vérifie si l'identifiant a accès ou non.

L'utilisation du logon TSO est recommandée pour tous les utilisateurs qui ont accès par ce système. Il est également recommandé d'attribuer l'utilisateur TSO comme identifiant principal et de continuer à maintenir un identifiant secondaire pour l'application des couches de sécurité.

Après avoir effectué ces actions, l'ID d'autorisation peut à nouveau utiliser les services d'un système de sécurité externe.

NOTE :

Les mots de passe utilisés par ces identifiants doivent suivre les mêmes conseils qu'un utilisateur TSO.

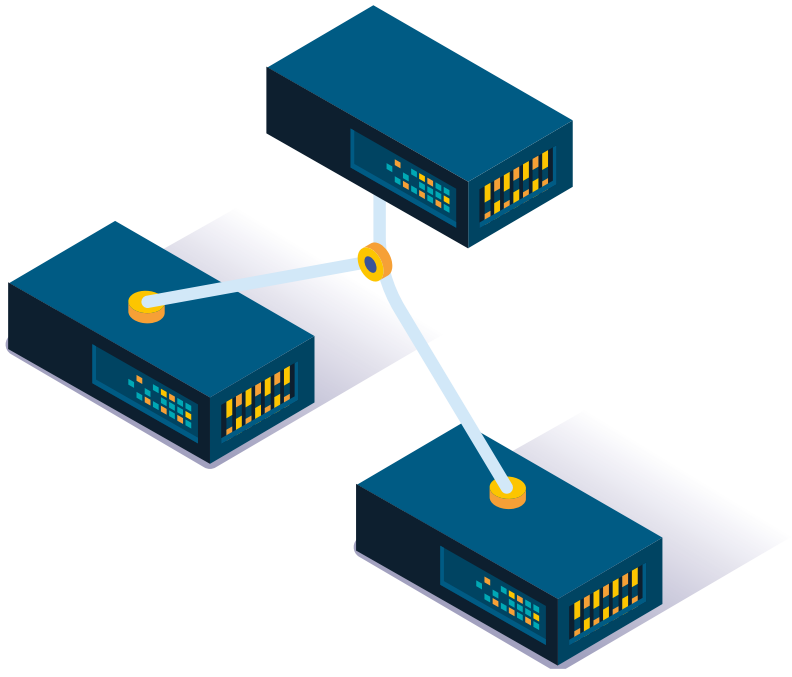
6.4.2 Les appels de systèmes à distance

L'utilisation de systèmes de sécurité capables de gérer, de maintenir et d'auditer ces entrées est recommandée.

Si un système de sécurité tel que RACF est déployé sur le moteur, ce système doit être utilisé pour l'accès externe car, grâce à ses fonctionnalités, il est capable de valider plusieurs contrôles de sécurité avant de pouvoir entrer dans le système.

Les tâches suivantes sont recommandées pour un moteur déployé sur un système de sécurité RACF :

- Vérifier un ID associé à une demande à distance et vérifier l'ID avec un mot de passe.
- Générer un « PassTicket » du côté du demandeur. Cela évite d'envoyer des mots de passe sur le réseau.
- Vérifier un ticket Kerberos si votre environnement distribué utilise Kerberos pour gérer l'accès des utilisateurs et effectuer leur authentification.
- Authentifier les entrées avec la base de données de communication Db2 (CDB). Il s'agit simplement de tables dans le catalogue Db2 qui sont utilisées pour établir des conversations avec des systèmes distants.



7. Audit

L'audit des accès et des permissions sera un élément clé d'une bonne configuration de sécurité dans le cadre de la mise en œuvre de Db2 12 sur z/OS.

Il tentera de surveiller toute entrée provenant à la fois des utilisateurs et des applications et de les différencier afin que les examinateurs de cet audit soient en mesure de distinguer les menaces communes ou les entrées communes.

La surveillance tente de répondre à des questions telles que : quelles sont les données sensibles nécessitant une autorisation, qui est autorisé à accéder aux données, qui a accédé aux données, qui tente d'obtenir des privilèges pour accéder aux données, quelles sont les tentatives d'accès non autorisé ?

Le catalogue Db2 contient des informations critiques d'authentification et d'autorisation. Ces informations constituent la principale piste d'audit pour le sous-système Db2. Vous pouvez récupérer les informations des tables du catalogue en émettant des requêtes SQL.

La plupart des tables du catalogue décrivent des objets Db2, tels que des tables, des vues, des tablespaces, des packages et des plans. D'autres tables, notamment celles dont le nom contient la chaîne « AUTH », contiennent les enregistrements de tous les privilèges et autorisations accordés. Chaque notice de catalogue d'une subvention contient les informations suivantes :

L'audit des accès et des permissions sera un élément clé d'une bonne configuration de sécurité dans le cadre de la mise en œuvre de Db2 12 sur z/OS.

☑ **Nom de l'objet**	☑ **Type de privilège**	☑ **ID recevant le privilège**	☑ **ID accordant le privilège**	☑ **Date d'attribution**

7. Audit

La piste d'audit Db2 peut vous aider à surveiller et à suivre tous les accès à vos données protégées. Les journaux d'audit fournissent une autre trace importante pour le sous-système Db2. Vous pouvez utiliser la piste d'audit pour enregistrer les informations d'accès suivantes :

- Modifications des ID d'autorisation
- Modifications de la structure des données, telles que la suppression d'une table.
- Modifications des valeurs des données, telles que la mise à jour ou l'insertion d'enregistrements.
- Tentatives d'accès par des identifiants non autorisés
- Résultats des déclarations GRANT et REVOKE
- Attribution de tickets de sécurité Kerberos aux IDs
- Autres activités intéressant les auditeurs

Il devrait être possible d'auditer au niveau des instances ainsi qu'au niveau des bases de données, les recommandations à suivre sont les suivantes :

- Activer Db2 trace pour pouvoir écrire dans les journaux.
- Avant de l'activer, il ne sauvegardera pas les anciennes données. Il sera nécessaire de prendre en compte le nettoyage des bûches de temps en temps.
- Choisir les éléments à auditer. Il est recommandé d'activer les catégories d'événements tels que les connexions, les modifications, les suppressions, etc. le cas échéant, mais il faudra activer les événements pour pouvoir voir toutes les informations dans les traces.

- La trace d'audit utilise l'ID primaire pour garder la trace des modifications et des entrées qui sont faites, il est donc recommandé que l'ID primaire soit compréhensible et visible pour savoir qui est la personne qui entre (et utiliser l'ID secondaire pour superposer les niveaux de sécurité en fonction des privilèges).

- Générer des rapports quotidiens et hebdomadaires sur les traces acquises dans lesquels les éléments suivants peuvent être définis :
  - **Consommation de données sensibles.**
  - **Des privilèges plus élevés à différents ID**
    (Il est recommandé de surveiller les ID ayant des autorisations spéciales et de contrôler soigneusement les ID ayant des privilèges sur les données confidentielles. Vous pouvez consulter le catalogue Db2 pour déterminer quels ID ont des privilèges et des autorisations à un moment donné).
  - **Échecs de connexion et nombre de tentatives**
    (si vous avez des données sensibles, utilisez toujours la piste d'audit de classe 1).

- Il est recommandé de créer un rôle d'auditeur qui est la personne ayant accès à ces données et pouvant les examiner.

- Il est recommandé que les rapports générés ne puissent pas être modifiés par le reste des utilisateurs, pas même par l'auditeur. En outre, ils ne doivent pas être supprimés sans une opération spéciale.

- Il est recommandé d'auditer toutes les actions de l'administrateur de la base de données (chargé de donner ou de retirer des privilèges aux autres rôles).

- Il est recommandé que l'accès aux données sensibles fasse l'objet d'un audit spécifique.

- Il est recommandé d'utiliser un type de système capable d'alerter si nécessaire. Un système de type SIEM qui peut générer des alarmes de sécurité.

Il est recommandé que les rapports générés ne puissent pas être modifiés par le reste des utilisateurs, pas même par l'auditeur. En outre, ils ne doivent pas être supprimés sans une opération spéciale.

8. La protection des communications

Pour protéger davantage les accès à la base de données, il est recommandé d'agir sur les canaux de communication avec la base de données.

- Il est recommandé d'utiliser des certificats émis par une autorité de certification de confiance et d'utiliser des algorithmes de cryptage approuvés par le Centre national de cryptologie.
- Il est recommandé d'utiliser des outils de gestion des vulnérabilités, dans lesquels des analyses régulières des menaces sont prévues.
- Le déploiement de Db2 sur z/OS prend en charge les protocoles TLS 1.0, SSL 3.0 et SSL 2.0.

9. Cryptage

La recommandation prévoit que les données les plus sensibles de la base de données doivent être cryptées. Pour ce faire, les recommandations fournies par le Centre national de cryptologie (CCN) dans ses documents de référence sur Db2 peuvent être suivies.

Db2 est déjà prêt à crypter de manière transparente les données au repos, telles que les journaux, les catalogues, les répertoires, les tableaux et les index. La recommandation est d'utiliser la fonctionnalité propre à Db2 pour protéger ces données au repos.

Si DFSMS est utilisé, il est recommandé d'étendre ses fonctions afin qu'il puisse crypter les données dans Db2. De cette façon, le cryptage peut être optimisé en utilisant le matériel intrinsèque de la Z. (Disponible dans zOS 2.2, RACF ou ICIS ou autre système de sécurité).

Avant de pouvoir utiliser le cryptage des ensembles de données DFSMS z/OS pour chiffrer les ensembles de données Db2, assurez-vous que votre système répond aux exigences suivantes :

- Le système d'exploitation est z/OS 2.2 ou supérieur. Pour z/OS 2.2, les PTFs pour APAR OA50569 et APAR OA53951 doivent être appliqués.
- Le matériel nécessaire est installé.
- ICSF et RACF ou systèmes de sécurité équivalents.
- L'ID utilisateur de la tâche Db2 initiée et tout ID utilisateur qui doit lire ou écrire dans un jeu de données crypté a la permission d'utiliser toutes les balises de clé qui sont utilisées pour protéger les jeux de données Db2.
- Toute balise de clé utilisée pour protéger les ensembles de données Db2 est définie sur tous les membres d'un groupe

La recommandation prévoit que les données les plus sensibles de la base de données doivent être cryptées. Pour ce faire, les recommandations fournies par le Centre national de cryptologie (CCN) dans ses documents de référence sur Db2 peuvent être suivies.

d'échange de données et sur tout système de sauvegarde qui peut lire ou écrire à partir d'un ensemble de données crypté.

- Tout identifiant d'utilisateur requis pour exécuter l'un des utilitaires indépendants est autorisé à utiliser les balises clés servant à protéger les ensembles de données Db2.

- Mises à jour des prérequis pour que votre produit de sécurité prenne en charge le cryptage des ensembles de données z/OS.

En outre, et dans le cadre du système d'exploitation z/OS, les données peuvent être sécurisées grâce à l'utilisation de RACF dont il a été question plus haut dans ce document.

Si vous souhaitez transporter des données d'un système à un autre, les copier, créer de nouvelles bases de données ou les partager avec d'autres systèmes, vous devez tenir compte des éléments suivants :

- Si les données sont sensibles et qu'il est nécessaire de les partager, il faut créer un canal sécurisé qui utilise le cryptage des données en transit, et les autorisations nécessaires doivent être en place pour traiter les données en toute sécurité à destination.

- Si les données ne sont pas sensibles, il est néanmoins recommandé de créer un canal sécurisé pour le partage des données et, si possible, de disposer de clés de cryptage pour les données en transit.

- En cas de reprise après sinistre, si les données doivent être accessibles sur un autre site physique, les clés ICSF et les profils RACF doivent être configurés de la même manière que sur le site source. La même règle s'applique aux sites proxy et source Db2 dans l'environnement de la solution de disponibilité continue GDPS® zéro perte de données.

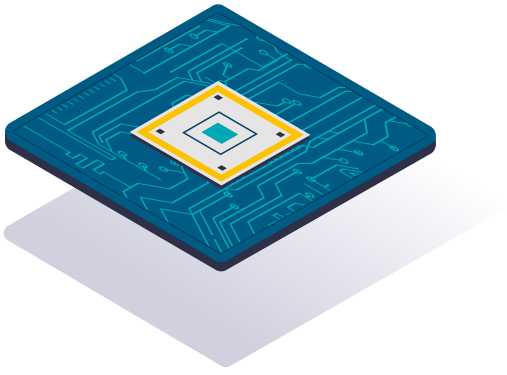
En outre, il est recommandé de crypter :

- **Les données utilisées pour la sauvegarde.**
- **Les images d'archives.**
- **Les données protégées par l'une des lois sur la protection des données.**
- **Les journaux impliquant la modification ou la régénération de commandes.**

10. Politiques de sauvegarde

Certaines bonnes pratiques générales sont décrites, indépendamment du produit ou de la version :

- La restauration de toute sauvegarde nécessite un accès contrôlé à la clé de chiffrement et doit être auditée, tant au niveau de l'accès que de la restauration.
- Il est recommandé d'effectuer des sauvegardes régulières, au moins une copie incrémentielle par jour, et de les conserver pendant au moins sept jours. Il est recommandé de créer une copie incrémentielle sur une base hebdomadaire et de la conserver pendant douze mois, ainsi qu'une copie annuelle à conserver pendant cinq ans.
- Il est recommandé que le stockage de ces copies ne se fasse pas au même endroit physique que le système principal.
- Des tests de restauration périodiques (au moins deux fois par an) sont fortement recommandés pour vérifier que le processus de restauration fonctionne correctement.
- La maintenance et la cohérence des données sont très importantes, il est recommandé d'utiliser l'intégrité référentielle Db2 pour vérifier que la cohérence des données, tant dans les sauvegardes qu'en transit, est fiable et correcte.



10.1. Sauvegarde, récupération et redémarrage

Bien que la haute disponibilité des données soit un objectif pour tous les sous-systèmes de Db2, les pannes imprévues sont difficiles à éviter complètement. Cependant, une bonne stratégie de sauvegarde, de récupération et de redémarrage peut réduire le temps écoulé d'une panne non planifiée.

Pour réduire la probabilité et la durée des pannes non planifiées, vous devez régulièrement sauvegarder et réorganiser vos données afin de maximiser leur disponibilité pour les utilisateurs et les programmes.

De nombreux facteurs affectent la disponibilité des bases de données. Voici quelques points clés à prendre en compte :

- Vous devez comprendre les options des utilitaires tels que COPY et REORG.
  - Récupération des structures en ligne telles que des tablespaces, des partitions, des ensembles de données, une série de pages, une page unique et des index.
  - Récupération des tablespaces et les index en même temps pour réduire le temps de récupération.
  - Avec certaines options de l'utilitaire COPY, vous pouvez lire et mettre à jour un tablespace tout en le copiant.

- Les erreurs d'E/S ont les effets suivants :
  - Les erreurs d'E/S dans une plage de données n'affectent pas la disponibilité du reste des données.
  - Si une erreur d'E/S se produit lorsque Db2 écrit dans le registre, Db2 continue à fonctionner.
  - S'il y a une erreur d'E/S dans l'enregistrement actif, Db2 passe au jeu de données suivant. Si l'erreur se trouve dans l'enregistrement d'archive, Db2 attribue dynamiquement un autre jeu de données.

- Des méthodes documentées de reprise après sinistre sont cruciales en cas de sinistres susceptibles de provoquer un arrêt complet de votre sous-système Db2 local.

- Si Db2 est contraint à un mode d'opération unique pour le jeu de données de démarrage ou les journaux, vous pouvez généralement restaurer le fonctionnement double alors que Db2 est toujours en cours d'exécution. Db2 fournit des méthodes complètes de récupération des données après des erreurs, des défaillances ou même des catastrophes. Il peut récupérer les données dans leur état actuel ou dans un état antérieur. Les unités de données qui peuvent être récupérées sont les espaces de table, les index, les espaces d'index, les partitions et les ensembles de données. Vous pouvez également utiliser les fonctions de récupération pour sauvegarder un sous-système Db2 entier ou un groupe d'échange de données.

- L'élaboration de procédures de sauvegarde et de récupération est essentielle pour éviter les pertes de données coûteuses et fastidieuses. En général, assurez-vous que les procédures suivantes sont mises en œuvre :
  - Création d' un point de cohérence.
  - Restauration du système et des objets de données à un point de cohérence.
  - Sauvegarde et récupération le du catalogue Db2 et de ses données.
  - Rétablissement après l'impact des conditions hors de l'espace.
  - Rétablissement après une panne matérielle ou électrique.
  - Rétablissement après une erreur de composant z/OS.

En outre, votre site doit disposer d'une procédure de récupération sur un site distant en cas de sinistre.

Les problèmes spécifiques nécessitant une récupération peuvent aller d'une erreur inattendue de l'utilisateur à la défaillance d'un sous-système entier. Un problème peut survenir au niveau du matériel ou du logiciel ; le dommage peut être physique ou logique. Voici quelques exemples :

- En cas de panne du système, un redémarrage de Db2 rétablit l'intégrité des données. Par exemple, un sous-système Db2 ou un sous-système attaché peut tomber en panne. Dans un cas comme dans l'autre, Db2 redémarre automatiquement, annule les modifications non validées et termine le traitement des modifications validées.

Vous pouvez utiliser les fonctions de récupération pour sauvegarder un sous-système Db2 entier ou un groupe d'échange de données.

- Si une défaillance du support se produit (comme un dommage physique à un périphérique de stockage de données), vous pouvez récupérer les données jusqu'au point actuel.

- Si les données sont logiquement endommagées, l'objectif est de récupérer les données à un point dans le temps avant que le dommage logique ne se produise. Par exemple, si Db2 ne peut pas écrire une page sur le disque en raison d'un problème de connectivité, la page présente une erreur logique.

- Si un programme d'application se termine anormalement, vous pouvez utiliser des utilitaires, des journaux et des copies d'images pour récupérer des données à un moment antérieur.

La récupération des objets Db2 nécessite des copies d'image adéquates et des jeux de données de journal fiables. Vous pouvez utiliser un certain nombre d'utilitaires et certaines structures système pour la sauvegarde et la récupération. Par exemple, l'utilitaire REPORT peut fournir certaines des informations nécessaires pendant la récupération. Vous pouvez également obtenir des informations sur l'inventaire du jeu de données de journal à partir du jeu de données de démarrage (BSDS).

11. Glossaire

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.

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.

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.

LDAP : Lightweight Directory Access Protocol (protocole d'accès à un répertoire léger) est un protocole de niveau applicatif qui permet d'accéder à un service de répertoire ordonné et distribué pour rechercher des informations dans un environnement de réseau.

SSL : Secure Sockets Layer, la technologie standard pour assurer la sécurité d'une connexion Internet, ainsi que pour protéger toute information sensible envoyée entre deux systèmes et empêcher les criminels de lire et de modifier les données transférées, y compris les informations qui pourraient être considérées comme personnelles.

Kerberos : protocole d'authentification sur réseau informatique créé par le MIT, qui permet à deux ordinateurs sur un réseau non sécurisé de prouver leur identité l'un à l'autre de manière sûre.

OTP : Mot de passe à usage unique utilisé pour l'authentification.

Authentification par signature sociale : Social Sign-In est une authentification unique pour les utilisateurs finaux. Avec les informations de connexion existantes d'un fournisseur de médias sociaux tel que Facebook, Twitter ou Google, l'utilisateur peut se connecter à un site web tiers au lieu de créer un nouveau compte spécifiquement pour ce site.

AES : Advanced Encryption Standard (AES), est un schéma de chiffrement par blocs adopté comme norme de chiffrement par le gouvernement des États-Unis, créé en Belgique. AES a été annoncé par le National Institute of Standards and Technology (NIST) comme US FIPS PUB 197 (FIPS 197) le 26 novembre 2001 après un processus de normalisation de 5 ans. Elle est devenue une norme effective le 26 mai 2002. Depuis 2006, AES est l'un des algorithmes les plus populaires utilisés en cryptographie symétrique.

DES : Data Encryption Standard (DES) est un algorithme de cryptage, c'est-à-dire une méthode pour crypter des informations, choisi comme norme FIPS aux États-Unis en 1976, et dont l'utilisation s'est largement répandue dans le monde.

Triple DES : En cryptographie, Triple DES est le nom donné à l'algorithme qui effectue le cryptage triple DES.

SHA : Les algorithmes de hachage sécurisés sont une famille de fonctions de hachage cryptographiques publiées par le National Institute of Standards and Technology (NIST) en tant que norme fédérale américaine de traitement de l'information (FIPS).

SIEM : La gestion des informations et des événements de sécurité (SIEM) est un terme de cybersécurité dans lequel les services et les produits logiciels combinent deux systèmes : la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM).

DDoS : En sécurité informatique, une attaque par déni de service, également appelée attaque DoS (Denial of Service), est une attaque sur un système ou un réseau informatique qui rend un service ou une ressource inaccessible aux utilisateurs légitimes.

CVE : Common Vulnerabilities and Exposures (CVE) est une liste d'informations enregistrées sur les vulnérabilités de sécurité connues, dans laquelle chaque référence comporte un numéro CVE-ID, une description de la vulnérabilité, les versions du logiciel qui sont affectées, une solution de contournement possible (le cas échéant) ou la façon de configurer pour atténuer la vulnérabilité et des références à des publications ou à des articles de forum ou de blog où la vulnérabilité a été rendue publique ou son exploitation est démontrée. En outre, un lien direct vers les informations de la base de données sur les vulnérabilités du NIST (NVD), où l'on peut obtenir plus de détails sur la vulnérabilité et son évaluation, est généralement aussi affiché.

NIST : Le National Institute of Standards and Technology (NIST), appelé National Bureau of Standards (NBS) entre 1901 et 1988, est une agence de l'Administration de la technologie du Département du commerce des États-Unis. La mission de cet institut est de promouvoir l'innovation et la concurrence industrielle aux États-Unis grâce aux progrès de la métrologie, des normes et de la technologie, de manière à renforcer la stabilité économique.

RLS : Row-Level Security. La sécurité au niveau des lignes vous permet d'utiliser l'appartenance à un groupe ou le contexte d'exécution pour contrôler l'accès aux lignes d'une table de base de données.

Db2 : Représente le programme sous licence Db2 ou un sous-système Db2 particulier. IBM a renommé DB2 en Db2, et Db2 for z/OS est le nouveau nom de l'offre anciennement connue sous le nom de «DB2 for z/OS».

RACF : Représente les fonctions fournies par le composant RACF de z/OS Security Server.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


cn-cert
centro criptológico nacional
CCN
centro criptológico nacional