RÉPUBLIQUE DU NIGER
Fraternité - Travail - Progrès
MINISTÈRE DU PLAN
INSTITUT NATIONAL DE LA STATISTIQUE
PLATEFORME NATIONALE D'INFORMATION POUR LA NUTRITION

NIGER
RAPPORT DE FORMATION
MAI 2021

NUTRITION

FORMATION À LA GESTION ET SÉCURISATION DES BASES DE DONNÉES EN LIGNE

EuropeAid/139-061/DD/SER/NE - *A2055*

SOFRECO

HC3N
LES NIGERIENS NOURRISSENT LES NIGERIENS

Institut National de la Statistique
NIGER

SIGNALÉTIQUE

OURS

Unité responsable : Plateforme Nationale d'Information pour la Nutrition (PNIN)

Directeur du projet : **ALCHINA KOURGUENI Idrissa**, Directeur Général de l'INS

Chargée du suivi du projet : Mme OMAR Haoua Ibrahim, Secrétaire Générale de l'INS

Coordonnateur : **MAMAN HASSAN Moussa,** Coordonnateur de la Plateforme Nationale d'Information pour la Nutrition (PNIN), Institut National de la Statistique (INS)

Auteur :

Spécialiste des Systèmes d'Information et bases de données, AT-PNIN, SOFRECO : **Alexis CAPO-CHICHI**

Contributeur :

Chef d'Équipe, Statisticien-Analyste, Assistant Technique PNIN (AT/PNIN) : **POIREL Guillaume**

Photos / illustratuions : PNIN

Editeur de la publication : Plateforme Nationale d'Information pour la Nutrition / INS

RÉPUBLIQUE DU NIGER
Fraternité - Travail - Progrès
MINISTÈRE DU PLAN
INSTITUT NATIONAL DE LA STATISTIQUE
PLATEFORME NATIONALE D'INFORMATION POUR LA NUTRITION

NIGER
GUIDE MÉTHODOLOGIQUE
AVRIL 2021

NUTRITION

GUIDE FORMATION EN GESTION ET SÉCURISATION DES BASES DE DONNÉES EN LIGNE

SOFRECO
HC3N
Institut National de la Statistique NIGER

SIGLES ET ABRÉVIATIONS

AT	Assistance Technique
BD	Base de Données
CE	Commission Européenne
DS	Directions Statistiques
ECT	Expertise Court Terme
HC3N	Haut-Commissariat à l'Initiative 3N (« les Nigériens Nourrissent les Nigériens
INS	Institut National de la Statistique
LCD	Langage de Contrôle des Données
LDD	Langage de Définition des Données
LID	Langage d'Interrogation des Données
LMD	Langage de Manipulation des Données
PNIN	Plateformes Nationales d'Information pour la Nutrition
PNSN	Politique Nationale de Sécurité Nutritionnelle
PTFs	Partenaires Techniques et Financiers
SGBDR	Systèmes de Gestion des Base de Données Relationnelles
SGDB	Systèmes de Gestion des Base de Données
SQL	Structured Query Language
TP	Travaux pratiques
UE	Union Européenne

SOMMAIRE

CONTEXTE ET OBJECTIFS DE LA MISSION

1. CONTEXTE DE L'ASSISTANCE TECHNIQUE À LA PNIN

L'initiative « Plateformes Nationales d'Information pour la Nutrition (PNIN) », portée par la Commission Européenne (CE), vise à aider les pays à renforcer leurs systèmes d'information et leurs capacités d'analyse de données pour la nutrition, de manière à mieux étayer les décisions stratégiques auxquelles ils sont confrontés pour prévenir la malnutrition et ses conséquences. L'approche développée par l'initiative PNIN consiste à renforcer les capacités des pays les plus concernés (Bangladesh, Niger, Burkina, Côte d'Ivoire, Guatemala, Éthiopie, Laos, Kenya, Burundi, Zambie) en matière d'exploitation optimale des données et informations existantes en lien avec la nutrition, de manière à ce qu'ils puissent mettre en œuvre des politiques et programmes efficaces et définir des priorités dans l'allocation des ressources avec l'appui des délégations locales de la Commission Européenne.

L'objectif général du programme PNIN est de contribuer à la réduction de toutes les formes de malnutrition à l'horizon 2025 à travers la mise en œuvre de la Politique Nationale de Sécurité Nutritionnelle (PNSN) et ses plans d'action multisectoriels. L'initiative a pour but de produire de l'information liée à la nutrition, puis d'engendrer des besoins et demandes d'informations, de manière à alimenter le débat public et de reformuler des plans d'analyse pour les décideurs, les parties prenantes ou les partenaires de la nutrition.

Du point de vue institutionnel et organisationnel, la plateforme est mise en œuvre par l'Institut National de la Statistique (INS) (bénéficiaire d'une subvention de l'Union Européenne) qui est en charge de développer la partie « offre d'information », grâce à :

- L'organisation de bases des données issues des enquêtes statistiques et autres systèmes de routines dans un entrepôt de données facilement accessible pour les utilisateurs ;
- La conduite des analyses statistiques proprement dites et la mise à disposition de l'information ainsi générée ;
- L'appui aux Ministères sectoriels afin d'améliorer la prise en considération de la statistique « nutrition sensible » à la fois au niveau des processus de collecte, mais surtout de l'analyse et de la diffusion.

Concernant la formulation de la demande, elle est coordonnée par le Haut-Commissat à l'Initiative 3N (« les Nigériens Nourrissent les Nigériens » (HC3N) qui est plus particulièrement responsable :

- De l'organisation des fora de concertation permettant l'émergence des questions relatives à la nutrition ;
- De la communication des résultats des analyses et de leur utilisation à des fins décisionnelles.

Dans ce contexte, une Assistance Technique (AT) internationale intervient en appui à l'INS et au HC3N depuis le démarrage du projet en fin novembre 2017.

Les objectifs spécifiques de l'AT sont au nombre de trois (3) :

- **Objectif spécifique 1** : Créer au sein de l'Institut National de la Statistique une Unité de mission capable de gérer, d'analyser et de diffuser l'information relative à la nutrition ;
- **Objectif spécifique 2** : Créer les capacités, au sein des parties prenantes au Niger, de formuler des questions / demandes en termes d'analyse, d'analyser les données afin de répondre à celles-ci et de mesurer les progrès effectués vers l'atteinte des objectifs nationaux de réduction de la prévalence de sous-nutrition ;

- **Objectif spécifique 3** : Promouvoir, au sein des parties prenantes, la compréhension et l'utilisation de l'analyse générée par les plateformes à des fins décisionnelles et stratégiques.

L'Assistance Technique apporte principalement un appui technique et de renforcement de capacités liés aux résultats attendus du programme et qui doivent être déployés à différents niveaux institutionnels et décisionnels :

- L'appui à l'INS vise à développer, au sein de l'institution, des capacités pérennes d'analyse statistique (aspect méthodologiques, techniques et technologiques en particulier le développement et l'entretien d'entrepôts de données multisectorielles) ;
- L'appui au HC3N vise le renforcement du leadership de cette institution en matière à la fois de réflexion sur les différentes dimensions de la nutrition, mais aussi l'amélioration in fine, de la qualité des politiques de lutte contre la malnutrition ;
- L'appui aux ministères sectoriels impliqués dans la mise en œuvre de l'initiative est destiné à fournir des outils permettant une meilleure prise en considération de l'information statistique dans la programmation et le suivi des actions de lutte contre la malnutrition.

Dans le cadre de l'atteinte de l'objectif 1 du programme PNIN « Créer au sein de l'Institut National de la Statistique une Unité de mission capable de gérer, d'analyser et de diffuser l'information relative à la nutrition » et plus particulièrement dans le souci de pouvoir collecter et traiter les données des Directions Statistiques (DS) des Ministères clés, l'AT PNIN a mobilisé une Expertise Court Terme (ECT) pour la formation en gestion/sécurisation des bases de données en ligne.

2. CONTEXTE DE LA MISSION DE FORMATION

Lors de la phase d'élaboration du programme, puis de démarrage du projet, le besoin de renforcement des capacités pour la gestion de bases de données et la sécurisation des bases de données en ligne a été souligné, que ce soit au niveau de l'INS ou de certaines Directions Statistiques (DS) sectorielles.

Les différents producteurs d'informations sont amenés à mettre en place des Systèmes de Gestion des Base de Données (SGDB) en lignes afin de faciliter l'accès à leurs données aux utilisateurs de plus en plus nombreux. Beaucoup d'initiatives poussées par les autorités nigériennes et les Partenaires Techniques et Financiers (PTFs) visent à accroitre l'accès aux informations statistiques. Ainsi, la plupart des Directions Statistiques ont commencé à déployer des SGDB.

La mise en place de bases de données en ligne doit s'accompagner de mesures pour la sécurisation des données. Clés de voûte de beaucoup d'institutions, les bases de données reposent souvent sur des produits clés en main dont les vulnérabilités sont souvent mal connues des différents services qui les utilisent. Ainsi, la sécurité et la bonne maîtrise du système de gestion de base de données (SGBD) sont devenues indispensables.

3. OBJECTIFS DE LA MISSION

Les objectifs spécifiques de la mission de formation de l'Expert Court-Terme (ECT) peuvent être regroupés en deux (2) catégories :

1. Savoir assurer la gestion d'un SGDB et plus spécifiquement :

- Savoir paramétrer un SGDB ;
- Avoir une connaissance des fonctionnalités d'un SGDB ;
- Avoir une connaissance sur les types de SGDB existants ;
- Être en mesure de spécifier les caractéristiques des données : types de données, structure des données contenues dans la base de données, règles de cohérence et relations (primaires et étrangères) ;
- Savoir paramétrer les autorisations d'accès sous forme de requêtes ;
- Maîtriser la gestion des utilisateurs et le paramétrage des accès par IP ;
- Connaître les opérations les plus courantes et les options de sécurisation des données ;
- Maîtriser les différents types de requêtes SQL CRUD (Create, Read, Update, Delete).

2. Assurer la sécurisation des bases de données en lignes et plus spécifiquement :

- Connaitre la méthode et la nature des accès afin de définir une politique de sécurité adaptée ;
- Être en mesure de faire une analyse de la sécurité en amont ;
- Connaître les failles les plus fréquemment rencontrées depuis les 10 dernières années : prise de contrôle à distance du SGBDR par le réseau, mauvaise installation du système d'exploitation (socle du SGBDR), utilisation abusive de privilèges admin, mots de passes codés en dur dans des fichiers systèmes non chiffrés, attaque par déni de service ;
- Connaître les solutions adéquates afin d'assurer la sécurisation des SGDB : stratégie de sauvegarde et de restauration, blocage des comptes génériques, fixation d'un nombre limité d'authentifications infructueuses, interdiction de réutiliser un mot de passe déjà utilisé par le passé ;
- Assurer la supervision de la sécurité et connaître les outils d'écoute et d'analyse du trafic réseau pour chiffrer les flux de données ;
- Présenter les différents protocoles de chiffrement ainsi que leurs forces et faiblesses.

DÉROULEMENT DE LA MISSION

1. INTRODUCTION

L'ensemble de la mission s'est déroulé en deux (2) phases :

Phase 1 (travail à distance de 5 jours) : Préparation de la formation dont l'élaboration du rapport de démarrage comprenant : 1/ Une proposition de plan de formation ; 2/ Un exposé en vidéo-projection d'animation des sessions (les modules sont résumés sur des fiches de présentation Microsoft PowerPoint) ; 3/ exercices pratiques ; 4/ supports techniques. Cette étape suit une première réunion tenue à l'INS et permet d'évaluer le contenu à développer à l'intention des participants. Elle s'effectue en collaboration avec l'équipe AT long-terme PNIN et l'Institut National de la Statistique du Niger.

Phase 2 qui s'est déroulée du 19 Avril au 23 Avril 2021 à Niamey. Outre des représentants de l'INS, la formation a concerné des représentants du HC3N, des Ministères de l'Education, de l'Hydraulique et de l'Assainissement, de l'Environnement et de Développement Durable, de l'Agriculture et de l'Elevage et de l'Education Primaire. La liste des participants est donnée en annexe 1.

La formation est orientée vers un public d'administrateurs de bases de données en charge des sauvegardes, des restaurations de données et de la sécurité des bases de données donc supposé avoir des connaissances en méthodes de conception de base de données (Merise, UML) et en langage SQL (Structured Query Language), le langage standard pour les traitements de bases de données le plus populaire.

Une partie de la formation a été consacrée aux aspects théoriques, dont certains ont été ensuite mis en application lors d'exercices pratiques. Pour pouvoir en profiter pleinement, chaque participant disposait d'un ordinateur portable.

2. PREMIÈRE JOURNÉE (19/04/2021)

La séance d'ouverture de la formation a été présidée par la Secrétaire Générale de l'INS, Mme OMAR Haoua Ibrahim et en présence du coordinateur de la PNIN, MAMAN HASSAN Moussa et du Chef de Mission de l'Assitance Technique M. POIREL Guillaume.

Dans son discours de bienvenue, Mme OMAR Haoua Ibrahim a resitué la formation « Dans le cadre du programme PNIN », avec un souci de mieux répondre et dans de meilleures conditions aux besoins de compétences dans le domaine de la gestion et de la sécurisation des bases données et ainsi renforcer les compétences de l'INS, du Haut-Commissariat à l'I3N et des Directions Statistiques sur les moyens à mettre en œuvre et les pratiques à assurer afin de sécuriser leurs bases de données. Mme OMAR Haoua Ibrahim a parlé également de l'aspect documentation et partage de connaissances et n'a pas oublié de remercier l'Union Européenne (UE) pour son appui financier.

Ensuite chaque participant, au cours d'un tour de table, a eu l'occasion de se présenter. Enfin, l'AT Long terme a pris la parole pour rappeler les objectifs de la formation.

Après une présentation du chronogramme de la formation par le formateur, les participants ont suggéré une modification au vu du contexte de carême en cours. Le chronogramme amandé de formation est donné en annexe 2.

La fin de la matinée et l'après-midi sont consacrés au premier module de la formation relatif aux concepts, définitions et principes des SGBD, à répondre à quelques questions techniques précises

et à approfondir certains concepts à travers des questions-réponses et illustrations. Le contenu a abordé, principalement, les points suivants :

- Ce qu'est un SGBD et une Base de Données (BD) ;
- Connaitre les objectifs, les fonctionnalités d'un SGDB et les types de SGDB existants ;
- Savoir les caractéristiques des données : types de données, structure des données contenues dans une base de données, règles de cohérence et relations ;
- Structures d'une base de données relationnelle.

3. DEUXIÈME JOURNÉE (20/04/2021)

La deuxième journée est consacrée au deuxième module de formation en commençant par des travaux dirigés d'installation et de configuration sur chaque ordinateur des participants le SGBD MySQL version 5.7.

Les différentes manières d'utiliser MySQL sont ensuite exposées. Néanmoins il a été recommandé aux participants l'utilisation de la ligne de commande au lieu des interfaces graphiques pour deux (2) principales raisons :

- Premièrement, parce que l'on souhaite que les participants puissent vraiment connaître et maitriser les commandes. En effet, les interfaces graphiques permettent de faire pas mal de choses, mais une fois lancés, les participants seront amenés à effectuer des choses subtiles et compliquées. Il ne serait pas étonnant qu'il leur soit obligatoire d'écrire eux-même leurs requêtes ;
- Ensuite, parce qu'il est fort probable que les participants désirent utiliser MySQL en combinaison avec un autre langage de programmation (si ce n'est leur but immédiat, cela viendra probablement un jour). Or, dans du code PHP (ou Java, ou Python, etc.), on ne va pas écrire « Ouvre PhpMyAdmin et clique sur le bon bouton pour que je puisse insérer une donnée dans la base ». On va devoir écrire en dur, « coder » les requêtes. Il faut donc que que les participants sachent comment faire.

Le principe général de l'interface de commande en ligne, le langage SQL (Structured Query Language), considéré comme le langage d'accès standard et normalisé, destiné à interroger ou à manipuler une base de données relationnelle a été présenté.

Les règles générales à retenir et les conventions syntaxiques concernant le SQL ont été présentées et expliquées avec des d'exemples pour illustrer.

Les instructions SQL qui constituent l'aspect LDD (Langage de Définition des Données) ont été ensuite présentées. Il s'agit notamment de savoir comment déclarer une table avec ses éventuels index et contraintes, comment afficher la structure d'une table. Ses instructions ont été ponctuées par des exemples.

4. TROISIÈME JOURNÉE (21/04/2021)

Les participants ont effectué des travaux pratiques, sous forme d'exercices, sur l'ensemble des instructions SQL constituant l'aspect LDD présentées la veille.

La fin de la matinée est consacrée aux instructions SQL qui constituent l'aspect LMD (Langage de Manipulation des Données).

Il s'agit des instructions SQL suivantes :

- L'insertion d'enregistrements : INSERT ;
- La modification de données : UPDATE ;
- La suppression d'enregistrements : DELETE (et TRUNCATE).

Après la présentation de ces instructions SQL, les participants ont effectué des exercices pratiques sur ces dernières.

Dans l'après-midi, les instructions SQL de modification structurelle et comportementale d'une table ont été présentées et expliquées, ensuite suivi des travaux pratiques d'exercices effectués par les participants.

La fin de l'après midi a été consacrée aux instructions SQL constituant l'aspect LID (Langage d'Interrogation des Données), l'aspect le plus connu du langage SQL qui concerne l'extraction des données par requêtes (nom donné aux instructions SELECT). Les participants ont effectué également quelques exercices sur ces instructions. Vu le temps de formation, il a été recommandé aux participants de se référer à des sites web afin d'approfondir les multitudes d'options existantes (une cinquantaine) qui peuvent être combinées avec l'instruction SELECT.

5. QUATRIÈME JOURNÉE (22/04/2021)

La matinée est consacrée aux instructions SQL qui constituent l'aspect LCD (Langage de Contrôle des Données). Les aspects du langage SQL qui concernent le contrôle des données et des accès sont abordés :

- La gestion des utilisateurs qui manipuleront des bases de données dans lesquelles se trouvent des objets tels que des tables, index, séquences, vues, procédures, etc. ;
- La gestion des privilèges qui permettent de donner des droits sur la base de données (privilèges système) et sur les données de la base (privilèges objet) ;
- La gestion des bases de données ;
- Les accès à distance et l'utilisation du dictionnaire des données (base de données « information_schema » de MySQL).

Après avoir brièvement présenté les concepts liés à la compréhension des aspects du LCD, une étude de cas a été présentée sur laquelle toutes les instructions SQL constituant le LCD ont été illustrées. Ensuite les participants ont effectué des travaux pratiques sur ces instructions.

Le deuxième module a été conclu par une brève revue de l'ensemble des instructions SQL pour interagir avec MySQL, donnant lieu à des échanges et des recommandations pratiques, tels que :

- Se servir d'interface graphique pour générer des commandes SQL de base et la faire évoluer ;
- L'utilisation régulière des instructions SQL facilite leur mémorisation. Et surtout ne pas chercher à les apprendre par cœur ;
- Ecrire toujours des instructions SQL normalisées pour éviter des désagréments lors d'une mise à niveau de votre application …

Le dernier module de la formation a débuté en fin d'après-midi et s'est poursuivi le lendemain. Il a été consacré à la présentation de différents concepts, bonnes pratiques liées à la sécurisation des bases de données en ligne.

6. CINQUIÈME JOURNÉE (23/04/2021)

La sécurité des bases de données est un domaine complexe, polymorphe, pour lequel il n'existe pas encore d'étude intégrée et homogène. Il n'existe pas encore de solution globale ni de recettes clé en main. Il a été présenté aux participants :

- Les concepts et enjeux liés à la sécurité des bases de données en ligne ;
- La méthode et la nature des accès à une base de données en ligne ;
- Les critères fondamentaux, connus sous le nom de D.C.I.P., de la sécurité de l'information ;
- Quelques failles/vulnérabilités les plus fréquemment rencontrées ;
- Quelques solutions adéquates afin d'assurer la sécurisation des SGDB ;
- Supervision de la sécurité et quelques outils d'écoute et d'analyse du trafic réseau ;
- Différents protocoles de chiffrement ainsi que leurs forces et faiblesse, notamment le protocole HTTPS/TLS.

Cette présentation a donné lieu à beaucoup d'échanges et des conseils pratiques. Il y a eu une forte demande des participants pour la présentation et l'explication de long en large de l'importance du fichier « .htaccess » de configuration du server Apache.

« .htaccess » désigne un type de fichier utilisé par le logiciel libre Apache HTTP Server. Ce dernier fait tourner plus de la moitié des serveurs d'Internet. Ces fichiers permettent de personnaliser la configuration d'Apache principalement pour gérer la confidentialité et la sécurité.

En effet, un fichier « .htaccess », placé dans un répertoire va agir sur le répertoire où il se trouve ainsi que sur tous ses sous-répertoires. Il va pouvoir autoriser ou interdire l'accès à certains fichiers. Il donne aussi la possibilité, que ce soit pour un fichier, un répertoire ou encore un sous-répertoire, de bloquer les utilisateurs qui ne se sont pas authentifiés grâce à un mot de passe. Essentiels à la sécurité d'un site internet et du serveur, les fichiers .htaccess sont des outils puissants qui doivent être manipulés avec précaution par les gestionnaires / développeurs avertis.

ÉVALUATION DE LA FORMATION

A la fin de la formation, le questionnaire d'évaluation à remplir par les participants a été distribué. Il était composé de cinq (5) parties. Les questionnaires ont été remplis par les 13 participants, les résultats présentés ici sont basés sur ces réponses.

1. OBJECTIFS DE LA FORMATION

Cette première partie du questionnaire est composée de trois (3) questions, dont deux (2) questions auxquelles on peut répondre par quatre (4) choix (Pas du tout ; Un peu ; Moyennement ; Beaucoup). Les résultats sont présentés ci-dessous.

Objectifs de formations	Pas du tout	Un peu	Moyennement	Beaucoup
1. Cette formation a-t-elle globalement répondu à vos attentes	0%	0%	**54%**	46%
2. Pensez-vous avoir acquis des connaissances utiles pour votre travail actuel	0%	0%	**54%**	46%

A la question à laquelle on demande des commentaires particuliers sur les objectifs de la formation, on ne dénombre que trois (3) commentaires particuliers :

- « Objectifs de la formation clairement définis » ;
- « Plus de pratiques pour le module 3 » ;
- « Formation très importante, faire bénéficier plus d'acteurs sectoriel, par exemple deux (2) personnes par secteur au lieu d'un ».

La moitié des participants (46 %) a jugée que la formation avait répondu « beaucoup » à leurs attentes et l'autre motié des participants (54 %) a jugée que la formation avait répondu « moyennement » à leurs attentes. De façon générale, les participants estiments qu'ils ont acquis des connaissances utiles pour leur travail actuel (46 % « beaucoup » et 54 % « moyennement »).

2. CONTENU DE LA FORMATION

La deuxième partie du questionnaire est composée de vingt-quatre (24) questions, dont 19 questions auxquelles on peut répondre par 4 choix (Faible ; Passable ; Correct ; Dense). Les résultats sont présentés ci-dessous.

Objectifs de formations	Faible	Passable	Correct	Dense
Le programme annoncé a été respecté ?	0%	0%	38%	62%
Le contenu était équilibré (équilibre entre les thèmes, les sessions) ?	0%	0%	46%	54%
Ouverture, présentation de la formation	0%	0%	77%	23%
Base de données et SGBD - Concepts, définition et fonctionnalités	0%	0%	77%	23%
Typologie et panorama des SGBD les plus courants	0%	8%	77%	15%
Structure des bases de données relationnelles	0%	8%	77%	15%

Travaux d'installation et configuration de MySQL	0%	23%	62%	15%
Types de données dans MySQL	0%	15%	77%	8%
Langage de Définition des Données (LDD)	0%	8%	85%	8%
Langage de Manipulation des Données (LMD)	0%	23%	77%	0%
Langage d'Interrogation des Données (LID)	0%	23%	69%	8%
Langage de Contrôle des Données (LCD) - Gestion des utilisateurs	0%	23%	54%	23%
Langage de Contrôle des Données (LCD) - Attributions de droits	0%	15%	62%	23%
Langage de Contrôle des Données (LCD) - Révocation de droits	0%	31%	54%	15%
Accès distant à une base de données MySQL	0%	38%	54%	8%
Généralités et critères fondamentaux de sécurité de l'information	0%	23%	69%	8%
Notion de vulnérabilité, menace et attaque	0%	15%	69%	15%
Failles de sécurité les plus fréquemment rencontrés	0%	15%	69%	15%
Solutions adéquates pour assurer la sécurisation des SGBD	0%	23%	62%	15%
Supervision de la sécurité et les outils d'écoute du trafic réseau	17%	25%	50%	8%
Protocoles de chiffrement	17%	17%	58%	8%

De façon général le programme de formation annoncé a été respecté (« beaucoup » pour 62 % des participants et « moyennement » par 38 % des participants). Le contenu de la formation a été estimé « équilibré ». La session d'introduction a été « moyennement » appréciée par 77 % des participants et « beaucoup » apprécié par 23 % des paricipants. Ces évaluations sont dans les même proportions sur les sessions relatives à la présentation des Systèmes de Gestion de Bases de Données (SGBD), la session sur les types de SGDB les plus courants et la présentation de la structure des Bases de Données Relationnelles (BDR).

Malgré l'absence de diffultés techniques sur l'installation et la configuration de MySQL sur les postes de travail des participants, cette session a été moins appréciée. Les participants ont en effet été plus intéressés par la mise en œuvre, l'utilisation d'un SGBD que par les aspects d'installlation qui reste néanmoins une étape incontournable avant les exercices pratiques. Alors que les sessions sur les types de données dans MySQL et le Langage de Définition des Données (LDD) ont été très appréciées, les sessions sur le Langage de Manipulation des Données (LMD), le Langage d'Interrogation des Données (LID) et le Langage de Contrôle des Donnée (LCD) pour la révocation des droits ont été moins appréciées en raison peut-être du niveau de difficulté.

En revanche la session sur le Langage de Contrôle des Données (LCD) pour les attributions des droits a été plus apprécié. Compte tenu de temps imparti à la formation et de la fatigue (période de ramadan et journée continue), les dernières sessions ont été moins bien évaluées (17 % de « pas du tout » satisfait pour les aspects liés à la supervision de la sécurité et des outils d'écoute du trafic réseau et la session sur les protocoles de chiffrement.

	Trop court	Correcte	Trop longue
Pour son contenu, la durée de la formation est ?	**62%**	38%	0%
Évaluation et clôture de la formation	0%	**83%**	17%

De façon générale, la formation a été évaluée « trop courte » par 62 % des participants. Aussi, quatre (4) commentaires particuliers ont été effectués concernant le contenu de la formation :

- « Il faut plus de séances pratiques » ;
- « Contenu globalement satisfaisant, cependant le temps imparti était trop court » ;
- « Plus de détails pour le module 3 » ;
- « Bonne initiative pour la sécurisation des données ».

3. PÉDAGOGIE UTILISÉE

La troisième partie du questionnaire est composée de cinq (5) questions dont une question à laquelle on peut répondre par 3 choix (Pas assez détaillées ; Suffisamment détaillées ; Trop détaillées). Ainsi, 85 % des participants estiments que les présentations et le guide étaient « suffisament » détaillés et 15 % « trop » détaillés.

	Pas assez détaillées	Suffisamment détaillées	Trop détaillées
Les présentations/guide de formation étaient-ils ?	0%	85%	15%

Enfin 69 % des participants pensent que la durée des présentations était « correcte » ; 23 % « trop courte » et «8 % « trop longue ».

	Trop courte	Correcte	Trop longue
La durée des présentations était-elle ?	23%	69%	8%

La majorité des participants (69 %) estiment que le nombre d'exemples et d'exercices était assez nombreux. Cependant, 23 % des participants auraient voulu avoir plus d'exemples et exercices et 8% ont trouvé qu'il y en avait « trop ». Enfin l'ensemble des participants évalue le nombre d'échanges entre participant suffisament nombreux.

	Pas assez nombreux	Suffisamment nombreux	Trop nombreux
Les exemples/exercices/travaux pratiques données étaient-ils ?	23%	**69%**	8%
Les échanges entre participants étaient-ils ?	0%	**100%**	0%

On dénombre cinq (5) commentaires particuliers sur la pédagogie utilisée :

- « Temps insuffisant, il fallait donner des exercices de maison à la fin de chaque séance » ;
- « Plus de temps devrait être accordé aux séances pratiques. La durée de ce genre de formation devrait être de deux semaines » ;
- « Le formateur est à la hauteur de la tâche » ;
- « Le formateur s'est bien adapté au rythme des participants qui sont en jeûne » ;
- « Malheureusement le temps n'avait pas permis de détailler certaines choses, mais on sait que l'animateur est à la hauteur ».

Dès le début de la formation et à travers la présentation des participants, nous avons constaté des niveaux de connaissance très contrastés : certains participants sont informaticiens spécialistes de la gestion de bases de données et d'autres participants n'avaient pas de notions dans le domaine. Ceci résulte également de la différence des Systèmes d'Information entre les Secteurs Clés de la PNIN.

4. ACCUEIL ET LOGISTIQUE

La quatrième partie du questionnaire est composée de trois (3) questions sur l'accueil et la logistique. Les résultats sont présentés ci-dessous.

	Faible	Moyen	Bien
Le confort de la salle était-il ?	0%	**77%**	23%
La qualité des repas était-elle ?	0%	38%	**62%**

Le confort de la salle a été globalement apprécié (77 % des participants l'évaluent « moyen » et 23 % « bien ») de même que la qualité des repas jugée « bien » par 62 % des participants et « moyen » par 38 %.

Quant aux commentaires particuliers sur l'accueil et la logistique, on en dénombre cinq (5) :

- « Bon dans l'ensemble » ;
- « Les sauts du disjoncteur ont perturbé les présentations » ;
- « Salle de formation chaude pendant les trois premiers jours » ;
- « Premier jour de formation Jus offert de mauvaise qualité. Retard observé lors de la troisième journée » ;
- « Climatisation ne donne pas bien ».

5. EVALUATION GLOBALE DE LA FORMATION PAR LES PARTICIPANTS

Dans l'ensemble, 23 % des participants ont apprécié « moyennement » la formation et **77% l'on « bien » apprécié**.

RECOMMANDATIONS

A l'issue de la formation en gestion/sécurisation des bases de données en ligne deux (2) types de recommandations ont été effectuées :

- Recommandations portant sur l'organisation de la formation ;
- Recommandations portant sur l'usage qui peut en être fait par les participants.

1. ORGANISATION DE LA FORMATION

1.1 PROFIL DES PARTICIPANTS, PÉRIODE ET DURÉE DE LA FORMATION

Les thèmes abordés, au cours de la formation, méritaient d'y consacrer plus de temps, les Travaux pratiques (TP) auraient pu être faits en laissant d'avantage d'autonomie plutôt que de passer à la correction après que le temps imparti au TP soit épuisé.

Mais vu le programme dans le temps imparti, il n'était pas possible de se le permettre au risque de ne pas couvrir l'ensemble du programme prévu dans les délais de cinq (5) jours.

La période de jeûn a certainement négativement influencé la concentration et l'efficacité des participants surtout les après-midis de formation.

Le deuxième module, très pratique, méritait à lui seul une semaine de formation surtout qu'il a été constaté que dix (10) participants sur treize (13) participants sont à leur vrai premier contact avec le langage SQL, contrairement aux prérequis de la formation.

Le groupe de particpants n'était pas homogène et les participants n'avaient pas toujours le même rythme entraînant des temps d'attente pour la majorité.

1.2 ORGANISATION MATÉRIELLE

Les conditions matérielles sont parfaitement adaptées au déroulement de la formation et ne soulèvent aucune remarque particulière.

2. EXPLOITATION PRATIQUE DES MÉTHODES ET TECHNIQUES PRÉSENTÉES

2.1 ÉLABORER UN PLAN INTERNE DE TRANSFERT DE COMPÉTENCES

Suivre une formation, c'est bien. Utiliser ce qu'on a appris sur son lieu de travail, c'est mieux. Et partager ses nouvelles compétences avec ses collègues pour qu'ils les intègrent dans leurs habitudes de travail, c'est le must.

Une formation bien conçue ne se termine pas lorsqu'on sort de la salle de formation, explique Nicolas Lefèvre, associé en charge de PwC's Academy. La formation, pour « être 100 % efficace, se poursuit une fois de retour à son poste de travail, avec la mise en place des compétences acquises ».

Ce **processus de transfert de compétences** peut se réaliser à travers quelques actions assez simples à mettre en place. Citons par exemple **l'organisation de sessions de « learn and lunch »** en interne où ceux qui ont assisté à la formation viennent partager ce qu'ils ont appris. Il est également possible d'inciter les managers à organiser des temps de partage des acquis de formation durant des « **team meetings** ». On peut également créer sur l'intranet de l'Institut National de la Statistique et des Secteurs **des communautés d'apprentissage** où les participants

peuvent partager les supports de cours reçus et proposer à tout collègue intéressé de lui expliquer les contenus.

Néanmoins la transmission de compétences est un processus qui demande du temps et qui ne s'improvise pas. Voici quelques clefs pour un transfert de compétences réussi :

- **S'assurer que le détenteur de compétences est volontaire pour transmettre** son expertise, et **vérifier que le récepteur est enclin à la recevoir** et à se former. Il est recommandé de faire en sorte que le partage de savoirs s'effectue dans les deux (2) sens ;
- **Encadrer le transfert de compétences avec un dispositif méthodologique** clair et précis ;
- **Planifier, coordonner, encadrer** et avoir un outil de suivi de la transmission de compétences ;
- **Former** si nécessaire **le détenteur de compétences à la transmission de son savoir** ;
- **Informer les parties prenantes sur la réorganisation induite par le transfert de compétences**. Une nouvelle organisation du temps de travail est souvent nécessaire pour permettre aux détenteurs de compétences d'enseigner dans les centres de formation interne ou d'animer les outils collaboratifs visant à partager leur expertise (intranet, réseaux sociaux d'entreprise, forums, partages d'écran, de fichiers, etc.) ;
- Organiser le suivi de l'utilisation des méthodes par les participants.

Le toolkit de formation en gestion et sécuration des bases de données en lignes (guide, présentations, exercices) **sera posté sur le Portail de la PNIN** d'ici la fin de l'année 2021 et pourra ainsi s'inscire dans le cadre du renfrocement des capacités en plus de la formation effectuée.

ANNEXES

1. ANNEXE 1 : LISTE DES PARTICIPANTS À LA FORMATION DES FORMATEURS (7-9 AVRIL 2021

Prénoms et Noms	Structure	Téléphone	Email
Abdoul karim HAROUNA ISSA	ENSTAT/INS	96 74 19 94	habdoulkarim@ins.ne
Abdoul Nasr ADAMOU GADO	ENSTAT/INS	96 24 09 64	agado@ins.ne
Abdoul wahidou Assoumane ALP	DI/INS	80 72 87 69	awahid@ins.ne
ALMOUSTAPHA THEODORE YATTA	PNIN/INS	99 45 40 83	atyatta@ins.ne
Amadou ALOU	DI/INS	96 96 49 05	aalou@ins.ne
Amadou BACHIR	HC3N/DSEC	96 96 23 40	abachir@yahoo.com
Assoumane Alparissou Abdoul Wahidou	DI/INS	80 72 87 69	awahid@ins.ne
Bassirou MAHAMADOU .M	DI/INS	96 50 19 96	bmahamadou@ins.ne
CAPO-CHICHI ALEXIS	Formateur	88 66 47 71	info@caagi.com
Gondah Neino	DS/MAG/EL	99 56 71 03	gondahn@yahoo.fr
Mamane Ibro	DIGBD/DGRE	96 17 16 74	mamaneibro@gmail.com
Mme Haboubacar Aminata Diallo	DS/MSP	90 40 46 45	minatousalim@yahoo.fr
Mme Hadiza Alhadji Cissé	DS/MAGEL	96 87 06 64	hadizacisseali@gmail.com
Tanko Hamani Mohamet	DS/MEP	96 87 03 52	Tankohani2@yahoo.fr
YAHOU Harissou	DS/ME/LCD	96 48 22 67	Yharissou2000@yahoo.fr

2. ANNEXE 2 : CHRONOGRAMME DE LA FORMATION

Lundi 19/04/2021	
9h00-9h15	**Installation des participants**
9h15-9h30	Tour de table : Présentation et recueil des attentes des participants
9h30-10h00	Rappel du cadre et des objectifs de la formation (Chef de mission AT PNIN)
10h00 -10h10	**Pause**
10h10-13h00	Présentation du programme et de la méthodologie de travail. Questions des Participants, questions pratiques **Module 1 : Les SGBD - définition, principes et architecture** Base de données et SGBD, Fonctions essentielles et fonctions induites d'un SGBD, Architecture d'un SGBD, Le fonctionnement, Typologie des SGBD (Exposé du formateur)
13h00-14h00	**Pause - Déjeuner**
14h00-16h00	**Module 1 : Les SGBD - définition, principes et architecture** ▪ Base de données et SGBD, Fonctions essentielles et fonctions induites d'un SGBD, Architecture d'un SGBD, Le fonctionnement, Typologie des SGBD (Exposé du formateur) ▪ Questions des participants concernant les concepts ▪ Réponses, compléments et approfondissement

Mardi 20/04/2021	
9h00-9h15	**Installation des participants**
9h15-10h00	**Module 2 : SQL pour MySQL** ▪ Travaux dirigés et questions – réponses : Installation de MySQL, Configuration de base ▪ Réponses, compléments et approfondissement
10h00 -10h10	**Pause**
10h10-13h00	**Module 2 : SQL pour MySQL** ▪ Principes de base des bases de données relationnelles ▪ Connexion et déconnexion au client MySQL, Syntaxe SQL et premières commandes ▪ Exemples d'application ▪ Les types de données ▪ Questions, réponses, compléments, approfondissement
13h00-14h00	**Déjeuner**
14h00-16h00	**Module 2 : SQL pour MySQL** ▪ Langage de Définition des Données ▪ Questions, réponses, compléments, approfondissement

Mercredi 21/04/2021	
9h00-9h15	**Installation des participants**
9h15-10h00	**Module 2 : SQL pour MySQL** ▪ Travaux pratiques : exercices sur le LDD
10h00 -10h10	**Pause-café**
10h10-13h00	**Module 2 : SQL pour MySQL** ▪ Langage de Manipulation des Données, exemples d'application et exercices ▪ Questions – réponses – approfondissement et compléments

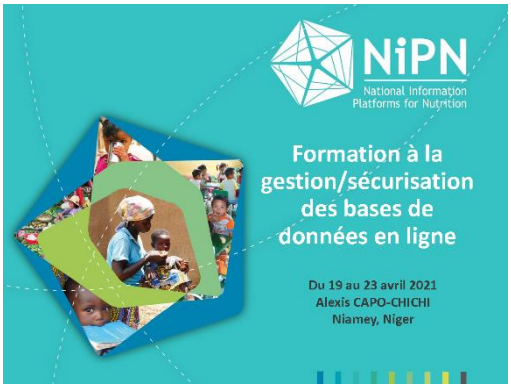
13h00-14h00	**Déjeuner**
14h00-16h00	**Module 2 : SQL pour MySQL** ▪ Modifications Structurelles et comportementales des tables, exemples d'application et exercices ▪ Langage d'Interrogation des Données, exemples d'application et exercices ▪ Questions – réponses – approfondissement et compléments

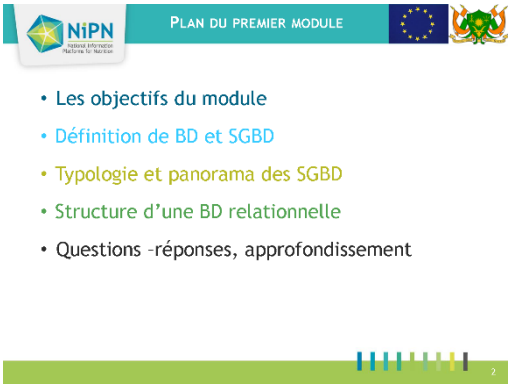
Jeudi 22/04/2021	
9h00-9h15	**Installation des participants**
9h15-10h00	**Module 2 : SQL pour MySQL** ▪ Langage de Contrôle des Données, illustrations par des exemples
10h00 -10h10	**Pause-café**
10h10-13h00	**Module 2 : SQL pour MySQL** ▪ Langage de Contrôle des Données Etude de cas, Questions – réponses – approfondissement et compléments
12h30-14h00	**Déjeuner**
14h00-16h00	**Module 2 : SQL pour MySQL** Langage de Contrôle des Données : Exercices, Questions – réponses – approfondissement et compléments **Module 3 : Sécurisation des bases de données** ▪ Concepts, enjeux et introduction aux critères D.I.C.P.

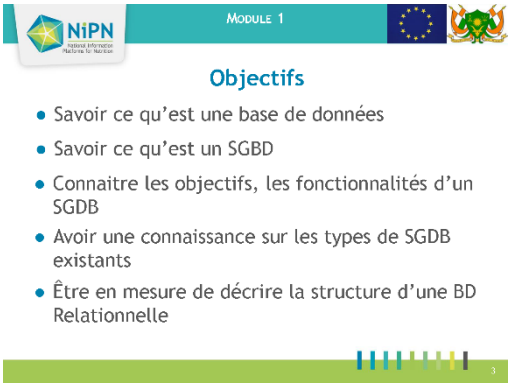
Vendredi 23/04/2021	
9h00-9h15	**Installation des participants**
9h15-10h00	**Module 3 : Sécurité des bases de données** ▪ Quelques failles/vulnérabilités les plus fréquemment rencontrées ; ▪ Quelques solutions adéquates afin d'assurer la sécurisation des SGDB
10h00 -10h10	**Pause-café**
10h10-13h00	**Module 3 : Sécurité des bases de données** ▪ Quelques solutions adéquates afin d'assurer la sécurisation des SGDB ▪ Supervision de réseau et les outils d'écoutes et d'analyse du trafic réseau
13h00-14h00	**Déjeuner**
14h00-15h30	▪ Protocoles de chiffrement ▪ Récapitulatif des journées de formation et recommandations ▪ Questions ouvertes et discussion
15h30-16h00	▪ Evaluation de la formation ▪ Clôture

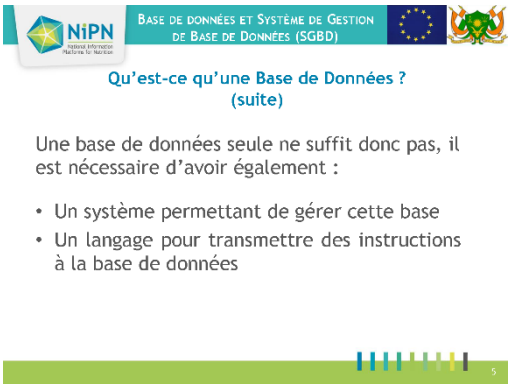
3. PRÉSENTATIONS EFFECTUÉES

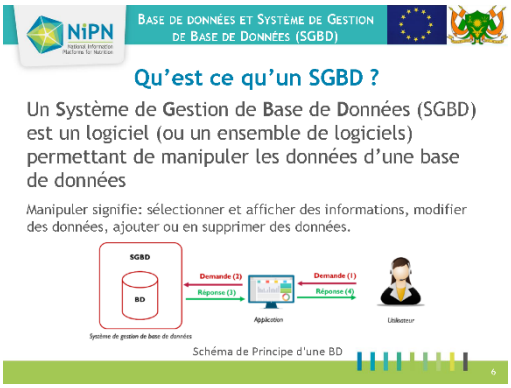
3.1 MODULE 1











BASE DE DONNÉES ET SYSTÈME DE GESTION DE BASE DE DONNÉES (SGBD)

Les objectifs d'un SGBD (Suite)

Exemple du Principe d'indépendance logique

Les données d'un hôpital : médecins, malades, chambres, ... ;

- Application n°1 : Suivi des malades (Nom, N° SS, N° Chambre, Médecin) ;
- Application n°2 : Données d'un médecin (Nom, N°SS, N° Chambre, Thérapie) ;
- Application n°3 : Gestion du personnel : les médecins (Nom, Grade, Spécialité, Salaire).

9

BASE DE DONNÉES ET SYSTÈME DE GESTION DE BASE DE DONNÉES (SGBD)

Les fonctionnalités d'un SGBD

- Définition des données : on parle de Langage de définition des données (DDL) - (conforme à un modèle de données)
- Manipulation des données : Interrogation, Mise à jour : Insertion, suppression, modification : on parle de Langage de manipulation des données (DML) - (langage de requête déclaratif)
- Contrôle des données : Contraintes d'intégrité, Contrôle des droits d'accès, Gestion de transactions : on parle de Langage de contrôle des données (DCL)

10

TYPOLOGIE ET PANORAMA DES SGBD

Types de SGBD

Il y a différentes façons de classer les SGBD, en voici une reposant sur des aspects pratiques :

- SGBD relationnel (SGBDR)
- SGBD NoSQL
- SGBD in-Memory
- Autres SGBD: SGBD pour les données XML/RDF, SGBD orientés objets, systèmes hiérarchiques ou réseaux

11

TYPOLOGIE ET PANORAMA DES SGBD

Types de SGBD (suite)

Selon leur construction et les possibilités qu'ils offrent:

- Relationnel (SGBDR)
- Hiérarchique, réseau
- Orienté objet et objet-relationnel
- A base de XML ou RDF
- Mixte
- Centralisé ou distribué
- Embarqué
- Spatial

12

TYPOLOGIE ET PANORAMA DES SGBD

Paradigme client/serveur

Quand la base de données se trouve sur un serveur qui ne sert qu'à ça, et pour interagir avec cette base de données, il faut utiliser un logiciel "client" qui va interroger le serveur et transmettre la réponse que le serveur lui aura donnée.

La plupart des SGBD sont basés sur un modèle Client/serveur

13

TYPOLOGIE ET PANORAMA DES SGBD

Panorama des SGBD existants

Nom SGBD	Année	Editeur	Caractéristiques	SQL	Licence
Microsoft Access	1992	Microsoft	Relationnel, pour particuliers et groupes de travail	Oui	Propriétaire
Microsoft SQL Server	1989	Microsoft	Entreprises, groupes de travail, particuliers, relationnel, distribué	Oui	Propriétaire
MySQL	1995	Oracle Corporation et MySQL AB	Centralisé, embarqué, distribué, pour entreprises, groupes de travail et particuliers, relationnel	Oui	GPL
Oracle Database	1979	Oracle Corporation	Entreprises, groupes de travail, particuliers, relationnel, spatial, distribué	Oui	Propriétaire
Oracle NoSQL Database	2011	Oracle Corporation	NoSQL	Non	Propriétaire
CouchDB	2010	CouchBase	NoSQL orientée documents	Non	Apache 2.0
Db2 (IBM)	1983	IBM	Pour entreprises, groupes de travail, particuliers	Oui	Propriétaire
IBM Informix	1981	IBM	Pour entreprises, groupes de travail, distribue	Oui	Propriétaire

14

TYPOLOGIE ET PANORAMA DES SGBD

Panorama des SGBD existants (suite)

Nom SGBD	Année	Editeur	Caractéristiques	SQL	Licence
MariaDB	2009	Monty Program AB	Pour entreprises, groupes de travail, particuliers	Oui	GPL
Sybase ASE	1987	Sybase Inc	Pour entreprises, groupes de travail, Relationnel	Oui	Propriétaire
MongoDB	2007	MongoDB	NoSQL orientée documents	Non	
PostgreSQL	1985	PostgreSQL Global Development Group	Entreprises, groupes de travail, particuliers, relationnel, distribué, Objets, Spatial	Oui	BSD
Firebird	1981	Firebird Corporation	Relationnel, centralisé, embarqué, pour groupes de travail et entreprises	Oui	MPL 1.1 (d) et IBM Public License
SQLite	2000	D. Richard Hipp	Système de gestion de base de données embarqué, moteur de base de données relationnelle accessible par le langage SQL	Oui	Domaine Publique

15

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Eléments structurants une base de données

Selon le modèle relationnel, une base de données est composée de :

- Tables
- Colonnes
- Lignes
- Clés primaires
- Clés étrangères
- Contraintes d'intégrité

16

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Table

Une **table** est un ensemble de données relatives à un même sujet (ou entité) et structurées sous forme de tableau.

Dans une base de données relationnelle, la table constitue la structure la plus importante car la manipulation des données se fait toujours à travers les tables : création, sélection, modification et suppression

Code article	Désignation article	Prix unitaire	Quantité en stock
V10	Vis 50x3	40	2500
V20	Vis 20x2	20	1300
B100	Boulon 90x15	450	100
C60	Clou 60x2	5	5000

Example de table article

17

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Colonne

Dans une table, une colonne correspond à une propriété élémentaire de l'objet décrit par cette table.

Un autre terme utilisé également pour désigner une colonne est celui d'« attribut» ou de « champ »

Nom de la table : Article
Description : Détail des articles commercialisés

Nom colonne	Description	Type de données	Taille	Obligatoire	Valeur par défaut	Valeurs autorisées
Code_art	Code de l'article	Chaîne de caractères	20	Oui		
Des_art	Désignation de l'article	Chaîne de caractères	50	Oui		
PU	Prix unitaire de l'article	Numérique	8,3	Non		> 0
Qte_stok	Quantité en stock	Numérique	4	Non	0	>= 0

Description des colonnes de la table article

18

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Ligne

Une table est composée horizontalement d'un ensemble de lignes. Une ligne correspond à une occurrence du sujet représenté par la table. On dit aussi qu'elle correspond à un objet du monde réel.

Un autre terme utilisé également pour désigner une ligne est celui de l' « enregistrement » ou de « n-uplet ».

19

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Clé primaire

La clé primaire d'une table est une colonne ou un groupe de colonnes permettant d'identifier de façon unique chaque ligne de la table

Remarques:

- Chaque table doit comporter une et une seule clé primaire
- Dans certains cas, dans une même table on peut avoir deux ou plusieurs colonnes qui peuvent jouer le rôle de clé primaires
- Les colonnes qui constituent la clé primaire sont obligatoires
- Pour distinguer une colonne qui fait partie de la clé primaire des autres colonnes, on la souligne, ou on la met en gras

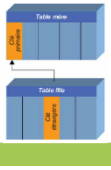
20

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Relations entre tables - clé étrangère

Pour que la base de données constitue une représentation fidèle du ou des domaines concernés, les liens entre les sujets du monde réel doivent se retrouver dans la base de données.

Un lien entre deux tables A et B est représenté par l'ajout dans la table B d'une nouvelle colonne correspondant à la clé primaire de la table A. Cette nouvelle colonne est appelée **clé étrangère**.



21

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Relations entre tables - clé étrangère

Supposons qu'en plus de la table « Article », nous avons une table « Commande » qui décrit les commandes reçues par le magasin. Dans cet exemple, nous admettons l'hypothèse qu'une commande ne concerne qu'un seul article.

Articles

Code article	Désignation article	Prix unitaire	Quantité en stock
V10	Vis 50x3	40	200
V20	Vis 20x2	20	1300
B100	Boulon 90x15	450	100
C60	Clou 60x2	5	5000

N° Commande	Date de commande	Code article#	Quantité commandée
100	03/03/2006	V10	500
101	15/04/2006	B100	30
102	17/04/2006	V10	120

22

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Contrainte d'intégrité -Intégrité référentielle

La cohérence et l'intégrité des données, dans une base de données, sont assurées à l'aide d'un ensemble de règles dites **contraintes d'intégrité**.

Les principaux types de contraintes d'intégrité sont :

- **Les contraintes de domaines:** Ce sont des contraintes appliquées à des colonnes. Elles permettent de fixer le caractère obligatoire ou pas d'une colonne et les règles de validité des valeurs qui peuvent être prises par cette colonne
- **Les contraintes d'intégrité de tables:** Elles permettent d'assurer que chaque table a une clé primaire
- **Les contraintes d'intégrité référentielles:** Elles permettent de s'assurer que les valeurs introduites dans une colonne figurent dans une autre colonne en tant que clé primaire.

23

STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Représentation de la structure d'une BD

Il s'agit de donner un formalisme permettant de représenter de façon homogène tous ces concepts que us venons devoir.

Un schéma de base de données représente la configuration logique de tout ou partie d'une base de données relationnelle.

La structure d'une base de données peut être représentée selon deux formalismes :

- Représentation textuelle
- Représentation graphique

24

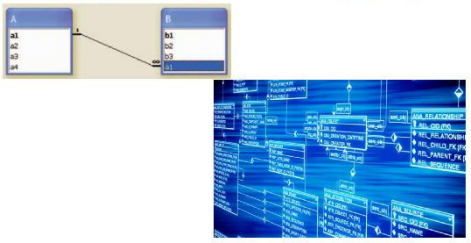
STRUCTURE DE BASE DE DONNÉES RELATIONNELLE

Exemple de représentation textuelle

A (a1, a2, a3, a4)
B (b1, b2, b3, a1#)

25

Exemple de représentation graphique



26

MODULE 1

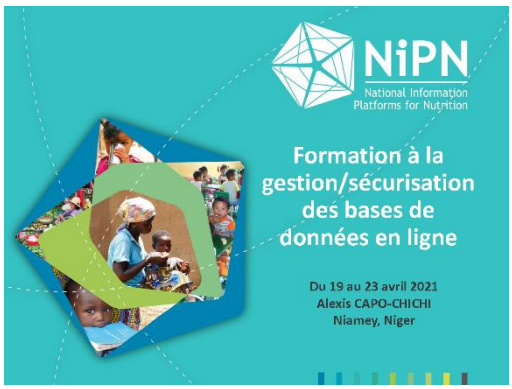
Questions-Réponses, approfondissement

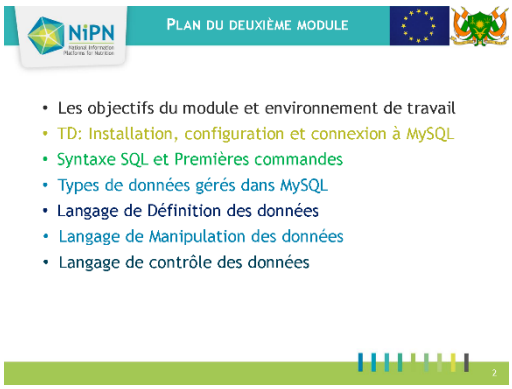
27

Merci de votre attention

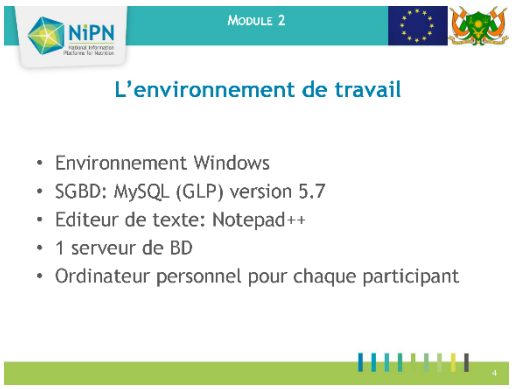
PNiN
Plateformes nationales d'information pour la nutrition

3.2 MODULE 2

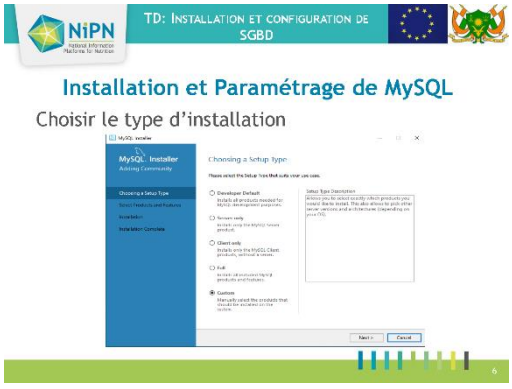

NiPN
National Information Platforms for Nutrition
Formation à la gestion/sécurisation des bases de données en ligne
Du 19 au 23 avril 2021
Alexis CAPO-CHICHI
Niamey, Niger

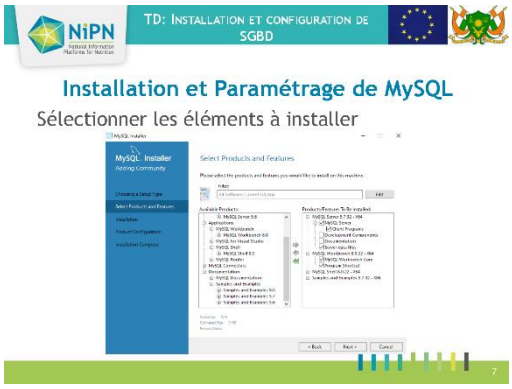

NiPN
PLAN DU DEUXIÈME MODULE
Les objectifs du module et environnement de travail
TD: Installation, configuration et connexion à MySQL
Syntaxe SQL et Premières commandes
Types de données gérés dans MySQL
Langage de Définition des données
Langage de Manipulation des données
Langage de contrôle des données
2

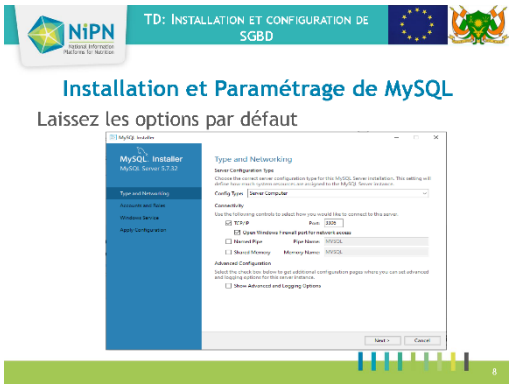

NiPN
MODULE 2
Objectifs
Savoir Installer et paramétrer MySQL
Maîtriser les commandes SQL de définition de données
Maîtriser les commandes SQL de manipulation des données (opérations CRUD)
Maîtriser la gestion des utilisateurs et des privilèges par les commandes SQL
Savoir configurer les accès à distant
Connaître les opérations les plus courantes et les options de sécurisation des données
3


NiPN
MODULE 2
L'environnement de travail
Environnement Windows
SGBD: MySQL (GLP) version 5.7
Editeur de texte: Notepad++
1 serveur de BD
Ordinateur personnel pour chaque participant
4


NiPN
TD: INSTALLATION ET CONFIGURATION DE SGBD
Installation et Paramétrage de MySQL
Téléchargement du programme d'installation
Lancer l'installation
Choisir le type d'installation
Sélectionner les éléments à installer
Laissez les options par défaut
Choisir un mot de passe pour l'utilisateur par défaut de MySQL, l'utilisateur "root"
Ajouter le chemin vers MySQL aux dossiers explorés par l'invite de commande de Windows.
5

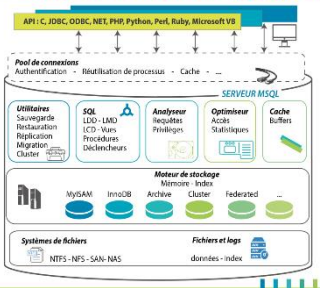

NiPN
TD: INSTALLATION ET CONFIGURATION DE SGBD
Installation et Paramétrage de MySQL
Choisir le type d'installation
MySQL Installer
Choosing a Setup Type
6


NiPN
TD: INSTALLATION ET CONFIGURATION DE SGBD
Installation et Paramétrage de MySQL
Sélectionner les éléments à installer
MySQL Installer
Select Products and Features
7


NiPN
TD: INSTALLATION ET CONFIGURATION DE SGBD
Installation et Paramétrage de MySQL
Laissez les options par défaut
MySQL Installer
Type and Networking
8

TD: INSTALLATION ET CONFIGURATION DE SGBD

Fonctionnalités de MySQL 5.7



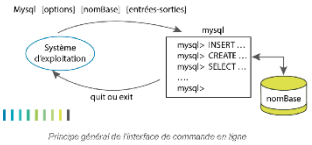
9

INTERFACE DE COMMANDE

Utilisation à MySQL

Il existe plusieurs manières d'utiliser MySQL

- Utilisation en **ligne de commande**
- Utilisation d'**interface graphique**



Principe général de l'interface de commande en ligne

10

SYNTAXE SQL ET LES PREMIÈRES COMMANDES

Le Langage SQL

Le langage SQL (Structured query language) peut être considéré comme le langage d'accès standard et normalisé, destiné à interroger ou à manipuler une base de données relationnelle.

Il a fait l'objet de plusieurs normes ANSI/ISO.

Les instructions SQL sont regroupées en catégories en fonction de leur utilité et des entités manipulées.

11

SYNTAXE SQL ET LES PREMIÈRES COMMANDES

Catégories des instructions SQL

Nous pouvons distinguer cinq catégories:

- Un langage de définition de données (LDD)
- Un langage de manipulation de données (LMD)
- Un langage de contrôle de données (LCD)
- Un langage de contrôle des transactions (LCT)
- Et d'autres modules

12

SYNTAXE SQL ET LES PREMIÈRES COMMANDES

Catégories des instructions SQL

Langage de Définition de Données (LDD) :

Langage orienté au niveau de la structure de la base de données. Le LDD permet de créer modifier, supprimer des objets

Par exemple: créer une table, créer une colonne, modifier une clé; un index, etc.

13

SYNTAXE SQL ET LES PREMIÈRES COMMANDES

Catégories des instructions SQL

Langage de Manipulation de Données (LMD) :

L'ensemble des commandes concernant la manipulation des données dans une base de données. Le LMD permet la sélection, l'ajout, la suppression et la modification de lignes

Par exemple: ajouter un enregistrement; afficher un ensemble d'enregistrement; modifier une ligne de données, etc.

14

SYNTAXE SQL ET LES PREMIÈRES COMMANDES

Catégories des instructions SQL

Langage de Contrôle de Données (LCD) :

L'ensemble des commandes pour contrôler l'accès aux données d'une base de données.

Exemple: Attribution de droits, révocation de droits, etc.

15

SYNTAXE SQL ET LES PREMIÈRES COMMANDES

Catégories des instructions SQL

Langage de Contrôle des Transactions (LCT) :

L'ensemble des commandes utilisé pour le contrôle transactionnel dans une base de données, c'est-à-dire les caractéristiques des transactions, la validation et l'annulation des modifications.

16

Catégories des instructions SQL

Autres modules:

Ils sont destinés notamment à écrire des routines (procédures, fonctions ou déclencheurs) et interagir avec des langages externes.

17

CRUD ?

Le terme « CRUD » est étroitement lié avec la gestion des données. Plus précisément, CRUD est un acronyme des noms des quatre opérations de base de la gestion de la persistance des données et applications :

- Create (créer) ;
- Read ou Retrieve (lire) ;
- Update (mettre à jour) ;
- Delete ou Destroy (supprimer).

CRUD-Operation	SQL	RESTful HTTP	XQuery
Create	INSERT	POST, PUT	insert
Read	SELECT	GET, HEAD	copy/modify/return
Update	UPDATE	PUT, PATCH	replace, rename
Delete	DELETE	DELETE	delete

18

Syntaxe

Avant d'aller plus loin, voici quelques règles générales à retenir concernant le SQL qui, comme tout langage informatique, obéit à des règles syntaxiques très strictes :

- **Fin d'une instruction:** pour signifier à MySQL qu'une instruction est terminée, il faut mettre le caractère « ; »
- **Commentaires:** ce sont des parties de code qui ne sont pas interprétées. les commentaires sont introduits par -- (deux tirets, la norme). MySQL déroge un peu à la règle SQL et accepte deux syntaxes : -- et #
- **Chaînes de caractères:** lorsque vous écrivez une chaîne de caractères dans une commande SQL, il faut absolument l'entourer de guillemets simples (donc des apostrophes). MySQL permet également l'utilisation des guillemets doubles, mais ce n'est pas le cas de la plupart des SGBDR

```
SELECT 'Salut l'ami'; -- Pas bien !
SELECT 'Salut l\'ami'; -- Bien !
```

19

Conventions

- **Mots-clés:** Une convention largement répandue veut que les commandes et mots-clés SQL soient écrits complètement en majuscules
- **Noms de bases, de tables et de colonnes:** les noms de bases, tables et colonnes seront écrits en minuscule pour les différencier des mots-clés.
- **Options facultatives:** On utilise des crochets [ ] pour indiquer ce qui est facultatif. La même convention est utilisée dans la documentation officielle MySQL (et dans beaucoup d'autres documentations d'ailleurs)

20

TP: Les premières commandes

Utilisateur « root » et création d'un utilisateur

1. Ouvrez le fichier « premierPas.sql » qui se trouve dans le répertoire Exemples SQL, à l'aide du bloc-notes (ou d'un éditeur de texte de votre choix)
2. Changez « util » par le nom de l'utilisateur à créer (modifiez aussi le nom de la base). Vous pouvez changer le mot de passe si vous voulez. Enregistrez ce fichier dans un de vos répertoires.

21

TP: Les premières commandes

Connexion au serveur / vérification de la version

Dans une fenêtre de commande Windows, lancez l'interface en ligne en connectant l'utilisateur « root » avec le mot de passe que vous avez donné lors de l'installation.

```
mysql --user=root -p
```

Une fois connecté, par copier-coller (en effectuant un clic droit dans la fenêtre de commande MySQL), exécutez une à une les différentes instructions (création de la base, de l'utilisateur, des privilèges et déconnexion de root)

Pour tester votre connexion, lancez la commande suivante qui se connecte au serveur sur la base bdutil, sous l'utilisateur util.

```
mysql --user=util --host=localhost -p --database=bdutil
```

Vérification de la version

```
mysql --version
```

22

Pour décrire les colonnes d'une table, MySQL fournit les types prédéfinis suivants :

- **Caractères** (CHAR, VARCHAR, TINYTEXT, TEXT, MEDIUMTEXT, LONGTEXT) ;
- **Valeurs numériques** (TINYINT, SMALLINT, MEDIUMINT, INT, INTEGER, BIGINT, FLOAT, DOUBLE, REAL, DECIMAL, NUMERIC, et BIT) ;
- **Date/heure** (DATE, DATETIME, TIME, YEAR, TIMESTAMP) ;
- **Données binaires** (BLOB, TINYBLOB, MEDIUMBLOB, LONGBLOB) ;
- **Énumérations** (ENUM, SET).

23

Opérations diverses sur une table

Pour pouvoir créer une table dans votre base, il faut que vous ayez reçu le privilège CREATE. La syntaxe SQL simplifiée est la suivante :

```
CREATE [TEMPORARY] TABLE [IF NOT EXISTS] [nomBase.]nomTable
    ( colonne1 type1
            [NOT NULL | NULL] [DEFAULT valeur1] [COMMENT 'chaine1']
     [, colonne2 type2
            [NOT NULL | NULL] [DEFAULT valeur2] [COMMENT 'chaine2'] ]
     [CONSTRAINT nomContrainte1 typeContrainte1] ...)
     [ENGINE= InnoDB | MyISAM | ...];
```

24

Opérations diverses sur une table

Exemple de création de table

Compagnie

comp	nrue	rue	ville	nomComp

Instruction SQL	Commentaires

`CREATE TABLE bdsoutou.Compagnie`
`(comp CHAR(4),`
`nrue INTEGER(3),`
`rue CHAR(20),`
`ville CHAR(15) DEFAULT 'Paris'`
`COMMENT 'Par defaut : Paris',`
`nomComp CHAR(15) NOT NULL);`
	La table contient cinq colonnes (quatre chaînes de caractères et un numérique de trois chiffres). La colonne `ville` est commentée.
	La table inclut en plus deux contraintes :
	• `DEFAULT` qui fixe *Paris* comme valeur par défaut de la colonne `ville` ;
	• `NOT NULL` qui impose une valeur non nulle dans la colonne `nomComp`.

Opérations diverses sur une table

Contraintes

```
CONSTRAINT nomContrainte
UNIQUE (colonne1 [,colonne2]...)
PRIMARY KEY (colonne1 [,colonne2]...)
FOREIGN KEY (colonne1 [,colonne2]...)
REFERENCES nomTablePere [(colonne1 [,colonne2]...)]
                [ON DELETE {RESTRICT | CASCADE | SET NULL | NO ACTION}]
                [ON UPDATE {RESTRICT | CASCADE | SET NULL | NO ACTION}]
CHECK (condition)
```

- La contrainte `UNIQUE` impose une valeur distincte au niveau de la table (les valeurs nulles font exception à moins que `NOT NULL` soit aussi appliquée sur les colonnes).
- La contrainte `PRIMARY KEY` déclare la clé primaire de la table. Un index est généré automatiquement sur la ou les colonnes concernées. Les colonnes clés primaires ne peuvent être ni nulles ni identiques (en totalité si elles sont composées de plusieurs colonnes).
- La contrainte `FOREIGN KEY` déclare une clé étrangère entre une table enfant (child) et une table père (parent). Ces contraintes définissent l'intégrité référentielle
- La contrainte `CHECK` impose un domaine de valeurs ou une condition simple ou complexe entre colonnes (exemple : `CHECK (note BETWEEN 0 AND 20)`, `CHECK (grade='Copilote' OR grade='Commandant')`)

Contraintes: Par exemple deux tables reliées à créer

Pilote

brevet	nom	nbHVol	compa

Compagnie

comp	nrue	rue	ville	nomComp

Tables	Contraintes

`CREATE TABLE Compagnie`
`(comp CHAR(4), nrue INTEGER(3),`
`rue CHAR(20), ville CHAR(15) DEFAULT 'Paris'`
`COMMENT 'Par defaut : Paris',`
`nomComp CHAR(15) NOT NULL,`
`CONSTRAINT pk_Compagnie PRIMARY KEY(comp));`
	Deux contraintes en ligne et une contrainte nommée de clé primaire.

`CREATE TABLE Pilote`
`(brevet CHAR(4), nom CHAR(15) NOT NULL,`
`nbHVol DECIMAL(7,2), compa CHAR(4),`
`CONSTRAINT pk_Pilote PRIMARY KEY(brevet),`
`CONSTRAINT ck_nbHVol`
`CHECK(nbHVol BETWEEN 0 AND 20000),`
`CONSTRAINT un_nom UNIQUE (nom),`
`CONSTRAINT fk_Pil_compa_Comp`
`FOREIGN KEY (compa)`
`REFERENCES Compagnie(comp));`
	Une contrainte en ligne et quatre contraintes nommées :
	• Clé primaire
	• NOT NULL
	• CHECK (nombre d'heures de vol compris entre 0 et 20 000)
	• UNIQUE (homonymes interdits)
	• Clé étrangère

Opérations diverses sur une table

Index

```
CREATE [UNIQUE | FULLTEXT | SPATIAL] INDEX nomIndex
    [USING BTREE | HASH]
    ON nomTable (colonne1 [(taille1)] [ASC | DESC],...) ;
```

- `UNIQUE` permet de créer un index qui n'acceptera pas les doublons.
- `FULLTEXT` permet de bénéficier de fonctions de recherche dans des textes (flot de caractères).
- `SPATIAL` permet de profiter de fonctions pour les données géographiques.
- `ASC` et `DESC` précisent l'ordre (croissant ou décroissant).

Créons deux index sur la table `Pilote`.

Instruction SQL	Commentaires

`CREATE UNIQUE INDEX idx_Pilote_nom`
`USING BTREE`
`ON Pilote (nom(15) DESC);`
	Index *B-tree*, ordre décroissant sur les trois premiers caractères du nom des pilotes.

`CREATE INDEX idx_Pilote_compa`
`USING BTREE`
`ON Pilote (compa);`
	Index *B-tree*, ordre croissant sur la colonne clé étrangère compa.

Opérations diverses sur une table

Structure d'une table

`DESCRIBE` (écriture autorisée `DESC`) est une commande qui vient de SQL*Plus d'Oracle et qui a été reprise par MySQL. Elle permet d'extraire la structure brute d'une table ou d'une vue.

```
DESCRIBE [nomBase.] nomTableouVue [colonne] ;
```

Résultat	Commentaires

`mysql> DESCRIBE Pilote;`
`+---+---+---+---+---+---+`
`| Field | Type | Null | Key | Default | Extra |`
`+---+---+---+---+---+---+`
`| brevet | char(4) | NO | PRI | | |`
`| nom | char(15) | YES | UNI | NULL | |`
`| nbHVol | double(7,2) | YES | | NULL | |`
`| compa | char(4) | YES | MUL | NULL | |`
`+---+---+---+---+---+---+`
	Les clés primaires sont `NOT NULL` (désignées par `PRI` dans la colonne `Key`).
	Les uniques sont désignées par `UNI` dans la colonne `Key`.
	Les occurrences multiples possibles sont désignées par `MUL` dans la colonne `Key`.
	Les contraintes `NOT NULL` nommées (définies via les contraintes `CHECK`) n'apparaissent pas.
	La colonne `Extra` indique notamment les séquences (`AUTO_INCREMENT`).

`mysql> DESCRIBE Compagnie;`
`+---+---+---+---+---+---+`
`| Field | Type | Null | Key | Default | Extra |`
`+---+---+---+---+---+---+`
`| comp | char(4) | NO | PRI | | |`
`| nrue | int(3) | YES | | NULL | |`
`| rue | char(20) | YES | | NULL | |`
`| ville | char(15) | YES | | Paris | |`
`| nomComp | char(15) | NO | | | |`
`+---+---+---+---+---+---+`	

Opérations diverses sur une table

Suppression d'une table

```
DROP [TEMPORARY] TABLE [IF EXISTS]
    [nomBase.] nomTable1 [,[nomBase2.]nomTable2,...]
    [RESTRICT | CASCADE]
```

- `TEMPORARY` : pour supprimer des tables temporaires. Les transactions en cours ne sont pas affectées. L'intérêt limité de `TEMPORARY` peut être un peu moins d'ouvrir qu'on ne décrit par accidentellement une table non temporaire.
- `IF EXISTS` : permet d'éviter qu'une erreur se produise si la cible n'existe pas.
- `RESTRICT` et `CASCADE` ne sont pas encore opérationnels. Le premier permettra de vérifier qu'aucun autre élément n'utilise la table (vue, déclencheur, etc.). Le second répercutera la suppression à tous les éléments référencés.

Avec `CASCADE` (pas encore opérationnel)	Les « fils » puis les « pères »
`DROP TABLE Compagnie CASCADE;` `DROP TABLE Pilote;`	`DROP TABLE Pilote;` `DROP TABLE Compagnie;`

Opérations diverses sur une table

Renommer une table

L'instruction `RENAME` renomme une ou plusieurs tables ou vues. Il faut posséder le privilège `ALTER` et `DROP` sur la table d'origine, et `CREATE` sur la base.

```
RENAME [nomBase.]ancienNomTable TO [nomBase.] nouveauNomTable
       [,[nomBase.] ancienNom2 TO [nomBase.]nouveauNom2] ;
```

Exemple

Commande RENAME	Commande ALTER TABLE
`RENAME Pilote TO Navigant;`	`ALTER TABLE Pilote RENAME TO Navigant;`

Opérations diverses sur une table

Modification structurelle d'une table - Ajout de colonne

Considérons la table suivante que nous allons faire évoluer:

```
CREATE TABLE Pilote
    (brevet VARCHAR(4), nom VARCHAR(20));
INSERT INTO Pilote
    VALUES ('PL-1', 'Agnès Labat');
```

Pilote

brevet	nom
PL-1	Agnès Labat

Le script suivant ajoute trois colonnes à la table `Pilote`. La première instruction insère la colonne `nbHVol` en l'initialisant à `NULL` pour tous les pilotes (ici il n'en existe qu'une seule). La deuxième commande ajoute deux colonnes initialisées à une valeur non nulle. La colonne `ville` ne sera jamais nulle.

```
ALTER TABLE Pilote ADD (nbHVol DECIMAL(7,2));
ALTER TABLE Pilote
      ADD (compa VARCHAR(4)  DEFAULT 'AF',
           ville VARCHAR(30) DEFAULT 'Paris' NOT NULL);
```

Résultats

Pilote

brevet	nom	nbHVol	compa	ville
PL-1	Agnès Labat		AF	Paris

DÉFINITION DES DONNÉES

Opérations diverses sur une table

Modification structurelle d'une table - Renommer colonne

```
ALTER TABLE [nomBase].nomTable CHANGE [COLUMN] ancienNom
      nouveauNom typeMySQL [NOT NULL | NULL] [DEFAULT valeur]
          [AUTO_INCREMENT] [UNIQUE [KEY] | [PRIMARY] KEY]
              [COMMENT 'chaine'] [REFERENCES ...]
        [FIRST|AFTER nomColonne];
```

L'instruction suivante permet de renommer la colonne `ville` en `adresse` en la positionnant avant la colonne `compa` :

```
ALTER TABLE Pilote CHANGE ville adresse VARCHAR(30) AFTER nbHVol;
```

33

DÉFINITION DES DONNÉES

Opérations diverses sur une table

Modification structurelle d'une table - Modifier type colonne

```
ALTER TABLE [nomBase].nomTable MODIFY [COLUMN] nomColonneAmodifier
      typeMySQL [NOT NULL | NULL] [DEFAULT valeur]
          [AUTO_INCREMENT] [UNIQUE [KEY] | [PRIMARY] KEY]
              [COMMENT 'chaine'] [REFERENCES ...]
        [FIRST|AFTER nomColonne];
```

Instructions SQL	Commentaires
`ALTER TABLE Pilote MODIFY compa VARCHAR(6) DEFAULT 'SING';`	Augmente la taille de la colonne `compa` et change la contrainte de valeur par défaut puis insère un nouveau pilote.
`INSERT INTO Pilote (brevet, nom) VALUES ('PL-3', 'Laurent Boutrand');`	
`ALTER TABLE Pilote MODIFY compa CHAR(4) NOT NULL;`	Diminue la colonne et modifie également son type de VARCHAR en CHAR tout en le déclarant NOT NULL (possible car les données contenues dans la colonne ne dépassent pas quatre caractères).
`ALTER TABLE Pilote MODIFY compa CHAR(4);`	Rend possible l'insertion de valeur nulle dans la colonne compa.

Résultat

CHAR(4) NULL possible Défaut 'SING'

Pilote				
brevet	nom	nbHVol	adresse	compa
PL-1	Agnès Labat		Paris	AF
PL-2	Laurent Boutrand		Paris	SING

34

DÉFINITION DES DONNÉES

Opérations diverses sur une table

Modification structurelle d'une table - Supprimer colonne

```
ALTER TABLE [nomBase].nomTable DROP
  ( [COLUMN] nomColonne | PRIMARY KEY
    | INDEX nomIndex | FOREIGN KEY nomContrainte )
```

```
ALTER TABLE Pilote DROP COLUMN adresse;
```

35

DÉFINITION DES DONNÉES

Modifications comportementales sur une table

Les mécanismes d'ajout, de suppression, d'activation et de désactivation de contraintes

- Ajout de contraintes
- Suppression de contraintes
- Désactivation des contraintes
- Réactivation des contraintes
- Contraintes différées

36

DÉFINITION DES DONNÉES

Modifications comportementales sur une table

Pour pouvoir créer une table dans votre base, il faut que vous ayez reçu le privilège CREATE. La syntaxe SQL simplifiée est la suivante :

Exemples de création, suppression de tables, renommage, modifications structurelles de table

Exercices: 1 à 6

37

MANIPULATION DES DONNÉES

Langage de Manipulation des Données

SQL propose trois instructions pour manipuler des données :

- L'insertion d'enregistrements : INSERT ;
- La modification de données : UPDATE ;
- La suppression d'enregistrements : DELETE (et TRUNCATE).

Exemples de manipulation des données

Exercices: Exo 7.5.2.1 à Exo 7.5.2.4

38

INTERROGATION DES DONNÉES

C'est l'aspect le plus connu du langage SQL qui concerne l'extraction des données par requêtes. Une requête permet de rechercher des données dans une ou plusieurs tables ou vues, à partir de critères simples ou complexes.

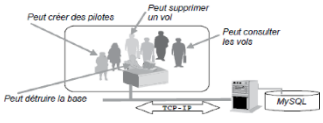
Exemples de d'interrogation de données

Exercices: Exo 8.2.4.1 à Exo 8.2.4.6

39

CONTRÔLE DES DONNÉES

les aspects du langage SQL qui concernent le contrôle des données et des accès



- La gestion des utilisateurs ;
- La gestion des privilèges qui permettent de donner des droits sur la base de données (privilèges système) et sur les données de la base (privilèges objet) ;
- La gestion des vues ;
- L'utilisation du dictionnaire des données (base de données information_schema).

40

CONTRÔLE DES DONNÉES

Gestion des utilisateurs

Les types d'utilisateurs, leurs fonctions et leur nombre peuvent varier d'une base à une autre. On peut classifier les utilisateurs de la manière suivante :

- Le DBA (DataBase Administrator).
- L'administrateur réseau (qui peut être le DBA) se charge de la configuration des couches client pour les accès distants.
- Les développeurs qui conçoivent et mettent à jour la base.
- Les administrateurs d'application qui gèrent les données manipulées par la ou les applications. Pour les petites et les moyennes bases, le DBA joue ce rôle.
- Les utilisateurs qui se connectent et interagissent avec la base à travers les applications ou à l'aide d'outils (interrogations pour la génération de rapports, ajouts, modifications ou suppressions d'enregistrements).

Tous seront des utilisateurs (au sens MySQL) avec des privilèges différents.

41

CONTRÔLE DES DONNÉES

Gestion des utilisateurs

Exemples, création, suppression, modification d'utilisateurs

42

CONTRÔLE DES DONNÉES

Gestion de base de données

Pour pouvoir créer une base de données, vous devez posséder le privilège CREATE sur la nouvelle base (ou au niveau global pour créer toute table).

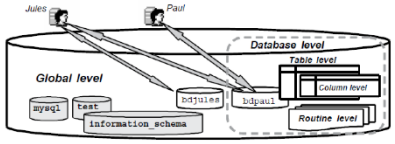
Exemples, création, suppression, modification, utilisation de base de données

43

CONTRÔLE DES DONNÉES

Gestion des privilèges

Un privilège (sous-entendu utilisateur) est un droit d'exécuter une certaine instruction SQL (on parle de privilège système), ou un droit relatif aux données des tables situées dans différentes bases (on parle de privilège objet).



Niveaux de privilège

44

CONTRÔLE DES DONNÉES

Révocation de privilèges

La révocation d'un ou de plusieurs privilèges est réalisée par l'instruction REVOKE. Pour pouvoir révoquer un privilège, vous devez détenir (avoir reçu) au préalable ce même privilège avec l'option WITH GRANT OPTION.

```
REVOKE privilège [ (col1 [, col2...])] [,privilège2 ... ]
ON [ {TABLE | FUNCTION | PROCEDURE} ]
{nomTable | * | *.* | nomBase.*}
FROM utilisateur [,utilisateur2 ... ];
```

45

CONTRÔLE DES DONNÉES

Accès distant

La table mysql.host est utilisée conjointement avec mysql.db et concerne les accès distants. Cette table n'est employée que pour les prérogatives au niveau database, indépendamment des utilisateurs.

Caractère	Signification pour `mysql.db`		Signification pour `mysql.host`	
	colonne `Host`	colonne `Db`	colonne `Host`	colonne `Db`
%	toute machine	toute base	toute machine	toute base
`' '` (chaîne vide)	consultez la table `mysql.host`	toute base	toute machine	toute base

Exemple de configuration

46

CONTRÔLE DES DONNÉES

Les vues

Pour pouvoir créer une vue dans une base, vous devez posséder le privilège CREATE VIEW et les privilèges en SELECT des tables présentes dans la requête de définition de la vue.

Exemples de vues

47

CONTRÔLE DES DONNÉES

Dictionnaire des données

Le dictionnaire des données (metadata ou data dictionary) est une partie majeure d'une base de données MySQL qu'on peut assimiler à une structure centralisée.

Le dictionnaire des données contient :

- La définition des tables, vues, index, séquences, procédures, fonctions et déclencheurs ;
- La description de l'espace disque alloué et occupé par chaque objet ;
- Les valeurs par défaut des colonnes (DEFAULT) ;
- La description des contraintes d'intégrité référentielle (de vérification à venir) ;
- Le nom des utilisateurs de la base ;
- Les privilèges pour chaque utilisateur ;
- Des informations d'audit (accès aux objets) et d'autre nature (commentaires, par exemple).

Exemples d'utilisation du dictionnaire

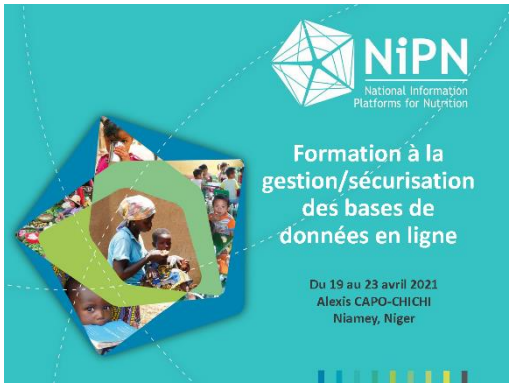
48

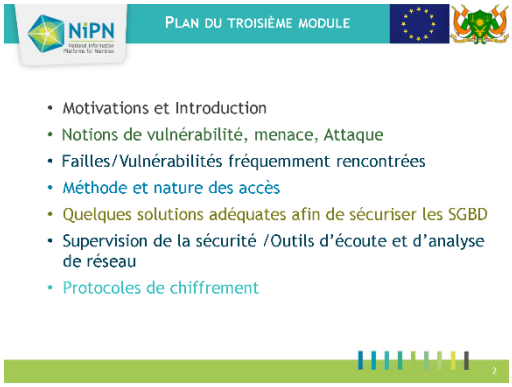
Exercices: Exo 9.7.5.1 à Exo 9.7.5.5

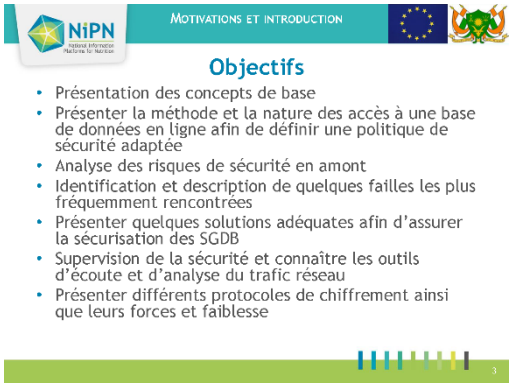
Merci de votre attention

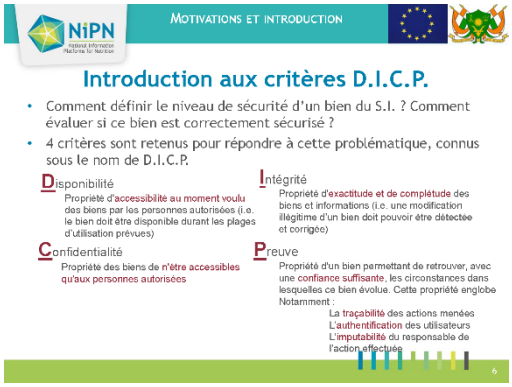
PNiN
Plateformes nationales d'information pour la nutrition

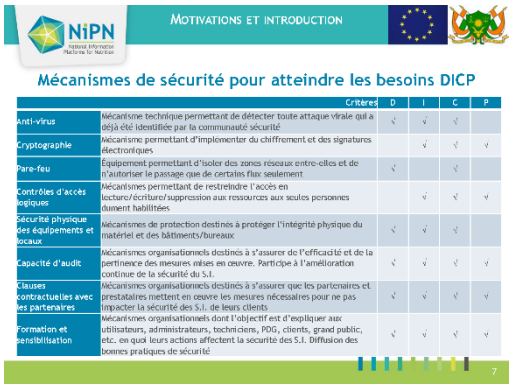
3.3 MODULE 3



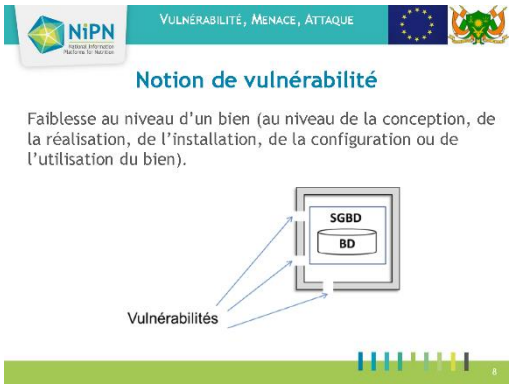






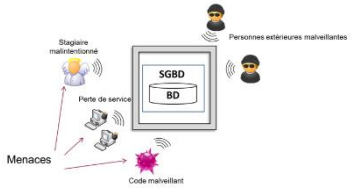


	Critères	D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	√	√	√	
Cryptographie	Mécanisme permettant d'implementer du chiffrement et des signatures électroniques		√	√	√
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	√		√	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées		√	√	√
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux	√	√	√	
Capacité d'audit	Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.	√	√	√	√
Clauses contractuelles avec les partenaires	Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients	√	√	√	√
Formation et sensibilisation	Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I. Diffusion des bonnes pratiques de sécurité	√	√	√	√



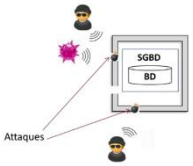
Notion de menace

Cause potentielle d'un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



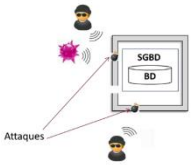
Notion d'attaque

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.

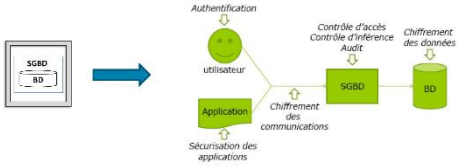


Notion d'attaque

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.



Protections contres les attaques



Synthèse

Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif zéro inatteignable

Failles de sécurité: Applications web

Chaque année OWASP publie un classement qui récence les failles de sécurité les plus critiques. Voici le classement 2017 :

1. Injection.
2. Authentification cassée.
3. Exposition de données sensibles.
4. Entités externes XML (XXE).
5. Contrôle d'accès cassé.
6. Mauvaise configuration de la sécurité.
7. Scripts intersites (XSS).
8. Désérialisation non sécurisée.
9. Utilisation de composants avec des vulnérabilités connues.
10. Journalisation et surveillance insuffisantes.

Failles de sécurité: Bases de données

1. Abus de privilège excessif
2. Abus de privilège légitime
3. Elévation de privilège
4. Exploitation de failles des bases de données vulnérables ou mal configurées
5. Injection SQL
6. Faiblesse de l'audit natif
7. Déni de service
8. Vulnérabilités des protocoles de communication des bases de données
9. Copies non autorisées de données sensibles
10. Exposition de données de sauvegarde

Solutions adéquates de sécurisation des SGBD

1. Changer le mot de passe par défaut
2. Refuser les connexions distantes
3. Supprimer les comptes inutiles
4. Supprimer la base de données d'exemple
5. Activer les logs et les externaliser
6. Exécuter le service avec un compte de service
7. Restreindre les privilèges des utilisateurs
8. Chiffrer les données stockées
9. Appliquer les patchs de l'éditeur

Supervision de la sécurité

La supervision réseau fait référence à la surveillance du bon fonctionnement des réseaux informatiques et des services informatiques connectés sur ces réseaux.

Enjeux:
- Garantir un niveau de service maximal
- Protéger les systèmes d'information

Comment ça marche ?:
La supervision réseau peut être mise en œuvre sur la base d'analyse de logs, de résultats de commandes et de scripts locaux mais c'est surtout sur la base de protocoles standards comme le protocole snmp que le monitoring des réseaux informatiques fonctionne.

17

Logiciels de supervision de sécurité

CACTI
Il permet de collecter des données de quasiment n'importe élément du réseau, notamment des systèmes de routage et de commutation ainsi que des pare-feux, puis de placer ces données dans des graphiques rigoureux

SPICEWORKS
Il offre de nombreux outils de gestion informatique gratuits, notamment pour la gestion de l'inventaire, le flux de travail du support technique, voire la surveillance Cloud, en plus de la solution de surveillance de réseau. Repose sur des techniques sans agent telles que WMI (pour les machines Windows) et SNMP (pour les systèmes réseau et *nix), cet outil gratuit peut fournir des informations sur de nombreux problèmes de réseau.

18

Outils d'écoute et d'analyse du trafic réseau

WIRESHARK
Wireshark® est un outil d'analyse de paquets open source qui utilise libpcap (*nix) ou winpcap (Windows) pour capturer les paquets et les afficher dans son interface graphique, et fournit de bonnes fonctions de filtrage, de regroupement et d'analyse. Il permet aux utilisateurs de capturer le trafic en temps réel ou de lire des données de lots de paquets et d'analyser les détails microscopiques. Wireshark offre des opportunités illimitées d'analyse de paquets, ce qui en fait une option solide pour les administrateurs réseau, système et de sécurité.

19

Outils d'écoute et d'analyse du trafic réseau

Nmap
Il utilise une fonctionnalité de détection des hôtes sur le réseau qui permet de créer une carte du réseau. Les administrateurs réseau l'apprécient, car il permet de collecter des informations des hôtes relatives au système d'exploitation, aux services ou aux ports exécutés ou ouverts, des informations d'adresse MAC, des noms DNS inversés, etc.
L'évolutivité est la principale raison pour laquelle les administrateurs réseau aiment Nmap. Il peut analyser un seul hôte ou un réseau entier constitué de « centaines de milliers » de machines.

20

Qu'est-ce que le chiffrement ?

Le chiffrement est un terme technique qui désigne la méthode par laquelle les communications (SMS, courriels, appels téléphoniques et vidéo) sont sécurisées afin d'empêcher toute personne autre que le destinataire prévu d'y accéder. Le chiffrement est la manipulation mathématique des informations dans le but de les rendre lisibles uniquement par le ou les destinataires prévus

Nous utilisons quotidiennement l'une des trois méthodes de chiffrement dès que nous utilisons des services connectés :

- Le chiffrement complet des données d'un disque dur ou d'un appareil
- Le chiffrement de bout en bout
- Le chiffrement du transport ou chiffrement de la couche transport (dont l'implémentation la plus courante est le HTTPS avec le protocole TLS ou SSL)

21

Terminologie en cryptographie

- Le **chiffrement** est la transformation d'une information en clair en une information chiffrée, incompréhensible, mais que l'on peut déchiffrer avec une clé pour obtenir l'information en clair originale.
- Un **système de chiffrement** (ou *cryptosystème*, ou encore *chiffre*) est composé d'algorithmes de chiffrement et déchiffrement et d'une clé de chiffrement.
- Un **algorithme de chiffrement** est une fonction qui prend en entrée le texte clair et la clé de chiffrement, transforme le texte par des opérations, et fournit en sortie un texte chiffré.
- **L'algorithme de déchiffrement** est la fonction inverse, qui prend en entrée le texte chiffré et la clé de déchiffrement, transforme ce texte par des opérations, et fournit en sortie le texte clair d'origine.

22

Terminologie en cryptographie (suite)

- La **clé de chiffrement** (ou cryptovariable) est l'information qui permet de transformer un texte clair en texte chiffré en utilisant un algorithme de chiffrement. De même, la clé de déchiffrement est l'information qui permet de transformer un texte chiffré en son texte clair d'origine. L'espace de clé est l'ensemble des valeurs possibles de la clé, c'est une notion importante pour la sécurité d'un algorithme. Si la clé de chiffrement et la clé de déchiffrement sont identiques, on parle de clé secrète et de chiffrement symétrique.
- **Le terme crypter n'existe pas**. En langage informatique le terme crypter n'est pas utilisé car il vient de l'anglicisme. On utilise le terme chiffrer.
- **Le mot décrypter existe** et est à utilisé dans l'opération de déchiffrement lorsque l'on ne possède PAS la clé de déchiffrement. Alors que le terme **déchiffrer** est le mécanisme de déchiffrement en utilisant la clé de déchiffrement.

23

Algorithmes/Protocoles de chiffrement

Les algorithmes symétriques les plus connus sont :
- Le chiffre de césar (Méthode par décalage)
- DES et (Triple DES)
- AES

Les algorithmes asymétriques les plus connus sont :
- RSA
- El-Gamal
- Courbes elliptiques

Les algorithmes hybrides les plus connus sont :
- PGP
- GnuPG
- TLS

Concernant les algorithmes de hachage, les plus connus sont :
- MD5
- SHA-1
- SHA-256

24

PROTOCOLES DE CHIFFREMENT

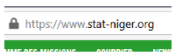
Forces /Faiblesses

Algorithme	Forces	Faiblesses
Symétrique	• Facilité d'intégration • Plus performant	• Moins sécurisé (Par le fait que la clé secrète est facilement transmissible)
Asymétrique	• Clé privée connue que d'un seul acteur • Moins performant (Couteux en ressource, temps de calcul plus élevé) • (RSA demande une clé minimale de 1024/2048 bits) • (Les courbes elliptiques ne nécessitent qu'une clé de 128 bits) • Plus sécurisé	• Complexité à gérer (Utilisation d'une PKI)
Hybride	• Plus performant • Plus sécurisé	• Échange de deux informations (clé symétrique chiffré et message chiffré)

25

PROTOCOLES DE CHIFFREMENT

HTTPS, SSL et TLS



La barre d'adresse d'un navigateur web fournit des informations sur le niveau de sécurité des sites visités. On connaît notamment le petit cadenas qui s'affiche à côté de l'URL, signe que le détenteur du site a adopté le protocole de sécurité HTTPS.
Cette sécurisation des serveurs (et donc des sites web) passe par des algorithmes de chiffrement. Ceux-ci consistent en la génération d'une clé cryptographique qui permet :

26

PROTOCOLES DE CHIFFREMENT

HTTPS, SSL et TLS

Ceux-ci consistent en la génération d'une clé cryptographique qui permet :

- D'assurer la confidentialité des données échangées entre un poste client et un serveur. Dès qu'il est activé, seules ces deux entités peuvent décrypter les informations qui circulent entre elles.
- De garantir l'intégrité des données.
- D'authentifier le serveur web avec lequel l'utilisateur communique. Car une simple clé de chiffrement ne garantit aucunement l'identité de son détenteur !

27

PROTOCOLES DE CHIFFREMENT

HTTPS, SSL et TLS

Pour bénéficier de cette protection, un site web utilise un certificat de chiffrement - un certificat SSL ou TLS - relié au protocole HTTP. Il est délivré par une **Autorité de Certification (AC)**, chacune proposant des niveaux différents de fiabilité.

28

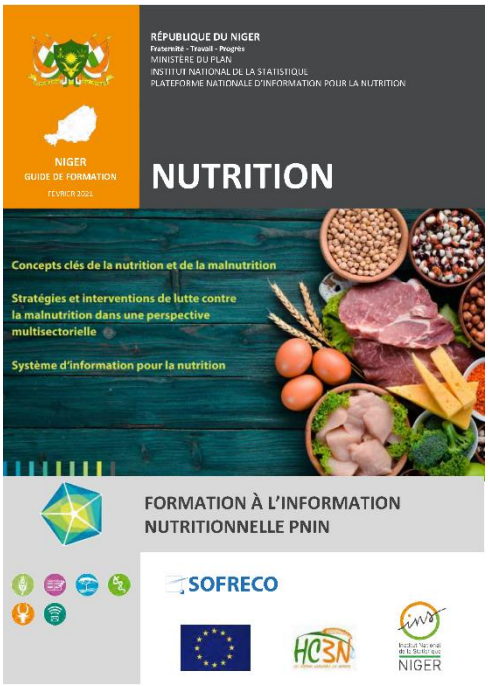
Merci de votre attention

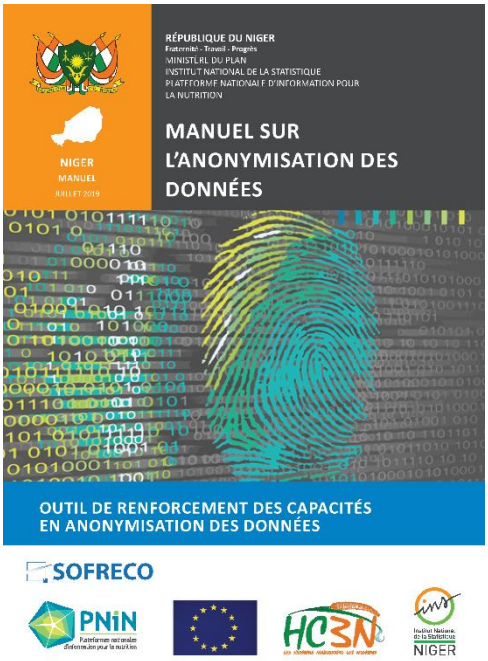
PNiN
Plateformes nationales d'information pour la nutrition

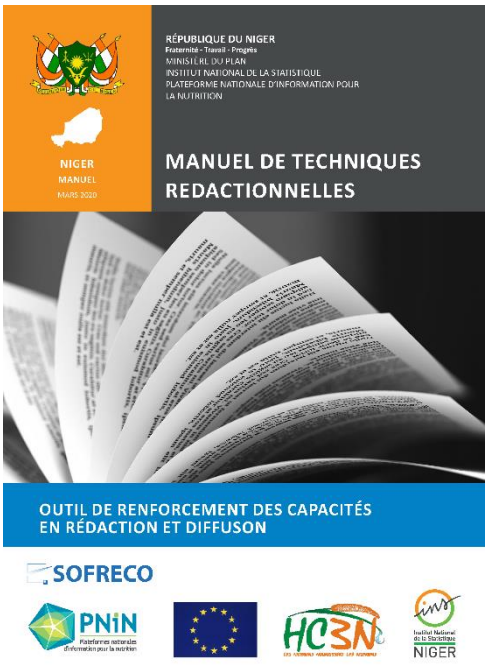
Contacts

Alexis CAPO-CHICHI
E-mail : alexis.capo-chichi@caagi.com
Téléphones:
+226 76 10 07 07 /78 12 47 47
+226 70 23 57 57 (WhatsApp)
+227 88 66 47 71
Skype : live:alexis.capo-chichi

Spécialiste en Système d'Information, Base de données, SIG et NTIC


RÉPUBLIQUE DU NIGER
Fraternité - Travail - Progrès
MINISTERE DU PLAN
INSTITUT NATIONAL DE LA STATISTIQUE
PLATEFORME NATIONALE D'INFORMATION POUR LA NUTRITION
NIGER
GUIDE DE FORMATION
FEVRIER 2021
NUTRITION
Concepts clés de la nutrition et de la malnutrition
Stratégies et interventions de lutte contre la malnutrition dans une perspective multisectorielle
Système d'information pour la nutrition
FORMATION À L'INFORMATION NUTRITIONNELLE PNIN
SOFRECO
HC3N
NIGER


RÉPUBLIQUE DU NIGER
Fraternité - Travail - Progrès
MINISTERE DU PLAN
INSTITUT NATIONAL DE LA STATISTIQUE
PLATEFORME NATIONALE D'INFORMATION POUR LA NUTRITION
NIGER
MANUEL
JUILLET 2019
MANUEL SUR L'ANONYMISATION DES DONNÉES
OUTIL DE RENFORCEMENT DES CAPACITÉS EN ANONYMISATION DES DONNÉES
SOFRECO
PNiN
HC3N
NIGER


RÉPUBLIQUE DU NIGER
Fraternité - Travail - Progrès
MINISTERE DU PLAN
INSTITUT NATIONAL DE LA STATISTIQUE
PLATEFORME NATIONALE D'INFORMATION POUR LA NUTRITION
NIGER
MANUEL
MARS 2020
MANUEL DE TECHNIQUES REDACTIONNELLES
OUTIL DE RENFORCEMENT DES CAPACITÉS EN RÉDACTION ET DIFFUSON
SOFRECO
PNiN
HC3N
NIGER


RÉPUBLIQUE DU NIGER
Fraternité - Travail - Progrès
MINISTERE DU PLAN
INSTITUT NATIONAL DE LA STATISTIQUE
PLATEFORME NATIONALE D'INFORMATION POUR LA NUTRITION
NIGER
MANUEL
JUILLET 2020
MANUEL SUR LES MÉTHODES D'ANALYSES
OUTIL DE RENFORCEMENT DES CAPACITÉS EN ANALYSE DES DONNÉES
SOFRECO
PNiN
HC3N
NIGER


SOFRECO