Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour consulter tous nos sujets d'annales et corrigés du Bac Pro GMNF, veuillez visiter :
bacprogmnf.fr/annales-sujets-et-corriges

Épreuve E4 : Culture scientifique et technologique

Session 2026 • Code sujet : **26-BACPRO-GMNF-E4** • Durée : **2 heures** • Coefficient : **4**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Architecture réseau, adressage et routage (4 questions) **Page 3**

2. Base de données relationnelle et requêtes SQL (4 questions) **Page 6**

3. Cybersécurité, analyse des journaux et sécurisation des accès (3 questions) **Page 8**

4. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 11**

Sujet officiel (PDF) : https://bacprogmnf.fr/assets/annales/bac-pro-gmnf/Informatique/2026/Bac Pro GMNF - Informatique - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

Le Syndicat mixte des marais de la Rive utilise quatre VLAN pour séparer l'administration, les agents de terrain, les équipements et les serveurs. À partir de la topologie et du plan d'adressage, il faut vérifier des paramètres IPv4 et IPv6, compléter la table de routage de R1 et expliquer une communication inter-VLAN.

Question 1.1. Pour le VLAN 20, indiquez le masque IPv4 en notation décimale pointée, l'adresse de diffusion, la première et la dernière adresse utilisables ainsi que le nombre d'adresses utilisables. Justifiez vos réponses à partir du préfixe fourni dans le DT 1.

Le préfixe /26 correspond au masque 255.255.255.192. Il reste 6 bits pour les hôtes, soit 64 adresses dans le bloc. Le réseau 10.24.20.0/26 va de .0 à .63 : .0 est l'adresse réseau et .63 l'adresse de diffusion. Les 62 adresses utilisables vont donc de .1 à .62.

Élément	Valeur
Masque	255.255.255.192
Adresse de diffusion	10.24.20.63
Première adresse utilisable	10.24.20.1
Dernière adresse utilisable	10.24.20.62
Nombre d'adresses utilisables	62

✓ RÉPONSE À RETENIR

Masque : 255.255.255.192 ; diffusion : 10.24.20.63 ; plage utilisable : 10.24.20.1 à 10.24.20.62, soit 62 adresses.

Question 1.2. Le terminal de terrain T-07 a reçu les adresses IPv4 10.24.20.45/26 et IPv6 2001:db8:24:20::45/64. Indiquez le VLAN auquel il appartient et ses deux passerelles par défaut à configurer. Précisez, pour chaque adresse, l'élément du plan d'adressage qui permet de conclure.

L'adresse IPv4 10.24.20.45/26 appartient au réseau 10.24.20.0/26, attribué au VLAN 20. Le plan d'adressage donne pour ce VLAN la passerelle IPv4 10.24.20.1. L'adresse IPv6 2001:db8:24:20::45/64 appartient au préfixe 2001:db8:24:20::/64 du VLAN 20 ; la passerelle IPv6 correspondante est 2001:db8:24:20::1. Les deux adresses confirment que T-07 est raccordé au VLAN 20.

✓ RÉPONSE À RETENIR

VLAN 20 ; passerelles par défaut : 10.24.20.1 et 2001:db8:24:20::1.

Question 1.3. Complétez dans le DR 1 la table de routage du routeur R1. Pour les quatre réseaux locaux, indiquez l'interface de sortie correspondant au VLAN. Pour la route par défaut, renseignez le prochain saut et l'interface de sortie à partir des données de liaison WAN figurant dans le DT 1.

Chaque réseau local est directement connecté à l'interface logique de R1 associée à son VLAN. Pour la route par défaut, le DT 1 indique le prochain saut Internet 198.51.100.9 et l'interface WAN G0/1. Reportez ces interfaces et ces valeurs dans le DR 1.

Destination	Prochain saut	Interface de sortie
10.24.10.0/27	Directement connecté	G0/0.10
10.24.20.0/26	Directement connecté	G0/0.20
10.24.30.0/27	Directement connecté	G0/0.30
10.24.40.0/28	Directement connecté	G0/0.40
0.0.0.0/0	198.51.100.9	G0/1

DR 1 complété : interfaces et route par défaut

Table de routage à compléter

Destination	Prochain saut	Interface de sortie
10.24.10.0/27	Directement connecté	G0/0.10
10.24.20.0/26	Directement connecté	G0/0.20
10.24.30.0/27	Directement connecté	G0/0.30
10.24.40.0/28	Directement connecté	G0/0.40
0.0.0.0/0	198.51.100.9	G0/1

À compléter à partir du document DT 1

✓ **RÉPONSE À RETENIR**

Interfaces locales : G0/0.10, G0/0.20, G0/0.30 et G0/0.40. Route par défaut : 198.51.100.9 via G0/1.

Question 1.4. Un poste du VLAN 20 doit accéder au serveur de base de données du VLAN 40. Indiquez le chemin logique suivi par les paquets et expliquez le rôle du routeur R1 dans cette communication.

Le poste envoie les paquets à sa passerelle du VLAN 20, 10.24.20.1. Ils transitent par SW1 et le trunk jusqu'à l'interface G0/0.20 de R1. R1 route ensuite les paquets vers le VLAN 40 par G0/0.40 ; SW1 les transmet à DB1. Les réponses empruntent le chemin inverse. R1 assure donc la communication entre les deux réseaux IP distincts.

✓ RÉPONSE À RETENIR

Poste VLAN 20 → SW1 → R1 (G0/0.20 vers G0/0.40) → SW1 → DB1, VLAN 40. R1 assure le routage inter-VLAN.

2. Base de données relationnelle et requêtes SQL

La base relationnelle du syndicat conserve les observations de faune et relie les espèces, les sites et les observations par des identifiants. À partir du schéma, des extraits de tables et des règles de nommage, il faut identifier les clés, rédiger des requêtes SQL et expliquer l'intérêt des identifiants pour la cohérence des données.

Question 2.1. À partir du schéma relationnel du DT 2, identifiez la clé primaire de la table Observation et les deux clés étrangères de cette table. Pour chacune des deux clés étrangères, nommez la table référencée.

Rôle dans Observation	Colonne	Table référencée
Clé primaire	id_observation	Aucune
Clé étrangère	id_espece	Espece
Clé étrangère	id_site	Site

La clé primaire identifie chaque observation de manière unique. Les clés étrangères établissent les liens entre Observation, Espece et Site, conformément au schéma relationnel du DT 2.

✓ RÉPONSE À RETENIR

Clé primaire : `id_observation`. Clés étrangères : `id_espece` vers `Espece` et `id_site` vers `Site`.

Question 2.2. Rédigez une requête SQL qui affiche, pour les observations réalisées depuis le 1er mai 2026 inclus, la date d'observation, le nom de l'espèce, le nom du site et l'effectif. La requête doit relier les tables Observation, Espece et Site à l'aide de leurs clés.

La requête relie les tables avec les clés indiquées dans le schéma : `Observation.id_espece` à `Espece.id_espece`, et `Observation.id_site` à `Site.id_site`. Le filtre >= inclut le 1er mai 2026 et toutes les dates ultérieures. Les quatre colonnes demandées sont sélectionnées.

✓ RÉPONSE À RETENIR

```
SELECT Observation.date_obs, Espece.nom_espece, Site.nom_site, Observation.effectif
FROM Observation
JOIN Espece ON Observation.id_espece = Espece.id_espece
JOIN Site ON Observation.id_site = Site.id_site
WHERE Observation.date_obs >= '2026-05-01';
```

Question 2.3. Rédigez une requête SQL qui affiche, pour chaque espèce observée sur le site dont l'identifiant est 3, le nom de l'espèce et la somme des effectifs observés. Le résultat doit être regroupé par espèce et présenté par somme décroissante des effectifs.

Le filtre retient uniquement les observations du site 3. La jointure permet d'afficher le nom de l'espèce associée à chaque identifiant. `SUM` calcule le total des effectifs et le regroupement par identifiant et nom rassemble les observations de chaque espèce.

1. Regrouper les lignes par espèce.
2. Trier les sommes par ordre décroissant.

✓ RÉPONSE À RETENIR

```
SELECT Espece.nom_espece, SUM(Observation.effectif) AS somme_effectifs
FROM Observation
JOIN Espece ON Observation.id_espece = Espece.id_espece
WHERE Observation.id_site = 3
GROUP BY Espece.id_espece, Espece.nom_espece
ORDER BY somme_effectifs DESC;
```

Question 2.4. Indiquez pourquoi l'identifiant de l'espèce est enregistré dans la table Observation plutôt que de répéter le nom de l'espèce dans chaque ligne. Donnez un avantage lié à la cohérence des données.

`id_espece` est une clé étrangère qui renvoie à l'espèce enregistrée dans `Espece`. L'identifiant évite de répéter le nom dans chaque observation. Si le nom change, il est modifié une seule fois dans la table Espece, ce qui limite les variantes et les erreurs de saisie.

✓ RÉPONSE À RETENIR

L'identifiant évite les répétitions et garantit que chaque observation renvoie à une espèce existante, avec un nom cohérent dans la base.

3. Cybersécurité, analyse des journaux et sécurisation des accès

Le journal du serveur de base de données présente une connexion SSH acceptée depuis le réseau d'administration et plusieurs échecs d'authentification depuis une autre adresse, avec des comptes différents. Il faut distinguer les événements, proposer des protections conformes aux règles d'accès et décrire les premières vérifications et actions à mener.

Question 3.1. Analysez l'extrait du journal. Identifiez l'événement suspect en précisant l'adresse source, le service visé et les indices qui permettent de le repérer. Distinguez cet événement de la connexion légitime également présente dans l'extrait.

Les événements suspects sont les trois échecs d'authentification SSH du 12 mai, entre 08:16:31 et 08:16:38, depuis **203.0.113.77**. La même source tente deux fois le compte « admin », puis « root » : ces échecs rapprochés et le changement de compte évoquent des essais d'accès. Le journal ne permet pas de vérifier si cette source appartient au VPN autorisé. La connexion de m.roux est distincte : elle est acceptée depuis **10.24.10.12**, dans le réseau d'administration 10.24.10.0/27, puis se termine par une déconnexion. L'adresse suspecte est un exemple réservé à la documentation dans le sujet.

Échecs SSH à examiner

Horodatage	Service	Adresse source	Compte	Événement
2026-05-12 08:14:02	sshd	10.24.10.12	m.roux	Connexion acceptée
2026-05-12 08:16:31	sshd	203.0.113.77	admin	Échec d'authentification
2026-05-12 08:16:34	sshd	203.0.113.77	admin	Échec d'authentification
2026-05-12 08:16:38	sshd	203.0.113.77	root	Échec d'authentification
2026-05-12 08:19:10	sshd	10.24.10.12	m.roux	Déconnexion

3 échecs, 2 comptes

✓ RÉPONSE À RETENIR

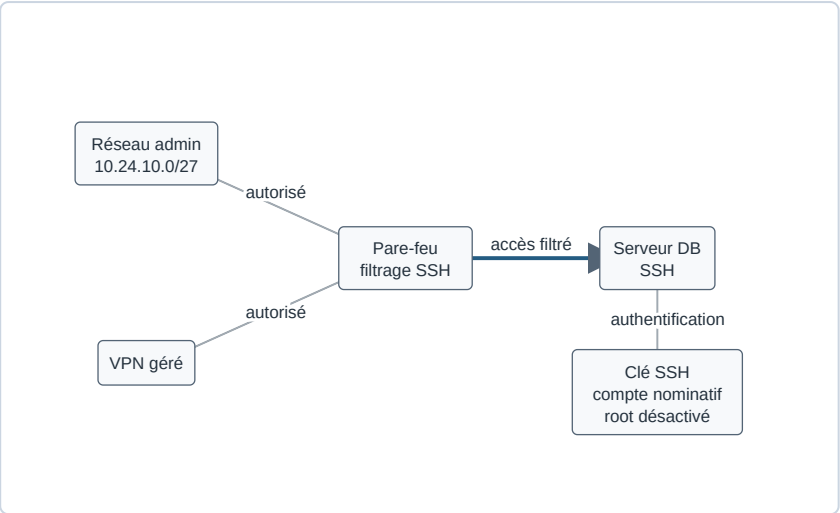
Suspect : trois échecs SSH depuis 203.0.113.77 sur admin puis root. Légitime : connexion acceptée de m.roux depuis 10.24.10.12.

Question 3.2. Proposez deux mesures techniques complémentaires permettant de réduire le risque d'accès non autorisé au serveur par SSH. Pour chaque mesure, indiquez le risque qu'elle réduit. Vos propositions doivent être compatibles avec les règles d'accès données dans l'introduction de la partie 3.

Deux mesures complémentaires respectent la règle d'accès SSH depuis le réseau d'administration ou le VPN géré et avec des comptes nominatifs du personnel informatique :

- Filtrer SSH au pare-feu pour n'autoriser que 10.24.10.0/27 et les adresses du VPN : cela réduit les tentatives provenant d'autres réseaux.
- Imposer l'authentification par clé et désactiver les mots de passe ainsi que la connexion directe de root : cela réduit les risques de mots de passe devinés ou volés et d'accès privilégié non autorisé.

Accès SSH autorisé et protections



Les sources autorisées passent le filtre ; l'accès SSH exige une clé et un compte nominatif.

✓ RÉPONSE À RETENIR

Limiter SSH au réseau d'administration et au VPN, puis exiger une clé sur les comptes nominatifs et désactiver la connexion directe de root.

Question 3.3. Décrivez les premières actions à engager après la détection de ces échecs d'authentification : conservation des éléments utiles, vérification de l'état du serveur et traitement de l'adresse source. Précisez pourquoi il convient de vérifier les journaux avant de conclure à une compromission.

Copier et préserver les journaux avec leurs horodatages, puis vérifier les connexions acceptées, les comptes concernés, les sessions actives et les changements récents sur le serveur. Croiser ces éléments avec les journaux réseau et VPN pour établir l'origine des tentatives et rechercher une activité anormale.

Après vérification, bloquer la source à la frontière réseau si elle est confirmée comme malveillante et renforcer la surveillance. Ici, 203.0.113.77 est une adresse d'exemple réservée à la documentation, pas une adresse réelle à bloquer. Des échecs seuls ne prouvent pas une compromission : il faut rechercher une connexion réussie ou d'autres signes d'intrusion avant de conclure.

Journal à conserver et vérifier

Horodatage	Service	Adresse source	Compte	Événement
2026-05-12 08:14:02	sshd	10.24.10.12	m.roux	Connexion acceptée
2026-05-12 08:16:31	sshd	203.0.113.77	admin	Échec d'authentification
2026-05-12 08:16:34	sshd	203.0.113.77	admin	Échec d'authentification
2026-05-12 08:16:38	sshd	203.0.113.77	root	Échec d'authentification
2026-05-12 08:19:10	sshd	10.24.10.12	m.roux	Déconnexion

Échecs SSH

Conserver les horodatages

✓ RÉPONSE À RETENIR

Préserver les journaux, vérifier les connexions et l’état du serveur, puis traiter la source après confirmation. Des échecs seuls ne prouvent pas une compromission.

Ce qu'il faut retenir de ce sujet (Session 2026)

Bilan de l'épreuve : L'épreuve E4 de Culture scientifique et technologique du Bac professionnel Gestion des milieux naturels et de la faune, session 2026, code 26-BACPRO-GMNF-E4, dure 2 heures et compte un coefficient 4. Elle porte sur le système d'information d'un syndicat de marais : réseau VLAN, base d'observations de faune et journaux SSH. Les compétences évaluées concernent l'adressage, le routage, SQL et la cybersécurité.

Notions-clés, formules & règles à maîtriser

- Un préfixe IPv4 /26 correspond au masque 255.255.255.192 et à 64 adresses, dont 62 utilisables dans un sous-réseau classique.
- Une route directement connectée utilise l'interface associée au réseau ; une route par défaut dirige le trafic inconnu vers un prochain saut.
- Une clé étrangère relie une table à la clé d'une autre table et contribue à la cohérence des données reliées.
- En SQL, WHERE filtre les lignes, GROUP BY forme les groupes et ORDER BY trie les résultats selon une valeur calculée.

Points de vigilance & attentes du jury

- Vérifier le masque, les bornes utilisables et l'adresse de diffusion en distinguant les adresses réseau et de diffusion.
- Reporter exactement les interfaces, passerelles et noms de tables ou de colonnes fournis dans les documents.
- Pour une requête agrégée, relier les tables, filtrer le site, regrouper par espèce et trier la somme demandée.
- Distinguer les connexions conformes aux règles des échecs suspects et proposer des mesures compatibles avec les accès autorisés.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment calculer le nombre d'adresses utilisables dans un réseau IPv4 ?

Pour un préfixe /26, il reste 6 bits pour les hôtes : 2^6 donne 64 adresses au total. Dans un sous-réseau classique, on retire l'adresse réseau et l'adresse de diffusion, soit 62 adresses utilisables.

Q : Comment construire une requête SQL qui totalise les observations par espèce ?

Reliez Observation à Espece avec id_espece, filtrez le site avec WHERE, regroupez par espèce avec GROUP BY et calculez SUM(effectif). Utilisez ensuite ORDER BY sur cette somme pour afficher les résultats dans l'ordre décroissant demandé.

Q : Comment gérer le temps pour cette épreuve de deux heures ?

Les trois parties valent respectivement 7, 7 et 6 points. Répartissez le temps en conséquence, gardez un moment pour compléter le DR 1, puis relisez les requêtes SQL et les justifications avant de rendre la copie.

Q : Quels critères faut-il respecter pour analyser les connexions SSH ?

Relevez l'adresse source, le service et les indices des échecs, puis comparez-les aux règles d'accès et à la connexion légitime. Les mesures proposées doivent réserver SSH aux comptes nominatifs venant du réseau d'administration ou du VPN.

Sujet officiel associé (PDF) : https://bacprogmnf.fr/assets/annales/bac-pro-gmnf/Informatique/2026/Bac Pro GMNF - Informatique - Session 2026 - 1-Sujet.pdf
Ressources Bac Pro GMNF : Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.