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 CGEH, veuillez visiter :
bacprocgeh.fr/annales-sujets-et-corriges

Mobilisation des technologies de l’informatique et du multimédia

Session 2026 • Code sujet : **26-BCP-CGEH-EP1** • Durée : **3 heures** • Coefficient : **Aucun coefficient d’épreuve autonome**

Sommaire

Cliquez sur une partie pour y accéder directement

1. **Architecture réseau, adressage et routage** (5 questions) — **Page 3**

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

3. **Cybersécurité, analyse d’incident et durcissement** (4 questions) — **Page 8**

4. **Ce qu’il faut retenir & Questions fréquentes (FAQ)** (Synthèse & Q&A Examen) — **Page 10**

Sujet officiel (PDF) : https://bacprocgeh.fr/assets/annales/bac-pro-cgeh/Informatique/2026/Bac Pro CGEH - Informatique - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

L'Écurie des Trois Chênes organise son réseau local en trois VLAN pour l'administration, les équipements de l'écurie et les invités. À partir des besoins en adresses IPv4, du préfixe IPv6 et de la topologie fournie, il faut compléter le plan d'adressage et décrire le routage inter-VLAN.

Partie 1

Question 1.1. Pour chacun des trois VLAN, indiquez le nombre minimal de bits nécessaires pour les adresses d'hôtes et le préfixe CIDR correspondant. Justifiez brièvement votre choix en tenant compte des deux adresses réservées du sous-réseau IPv4.

Il faut choisir le plus petit nombre de bits d'hôtes h pour lequel $2^h - 2$ couvre le besoin, car les adresses réseau et de diffusion ne sont pas attribuables. Pour le VLAN 10, 6 bits donnent 62 adresses utilisables, donc un préfixe /26. Pour le VLAN 20, 5 bits donnent 30 adresses, donc /27. Pour le VLAN 30, 4 bits donnent 14 adresses, donc /28. Dans chaque cas, le préfixe est égal à $32 - h$.

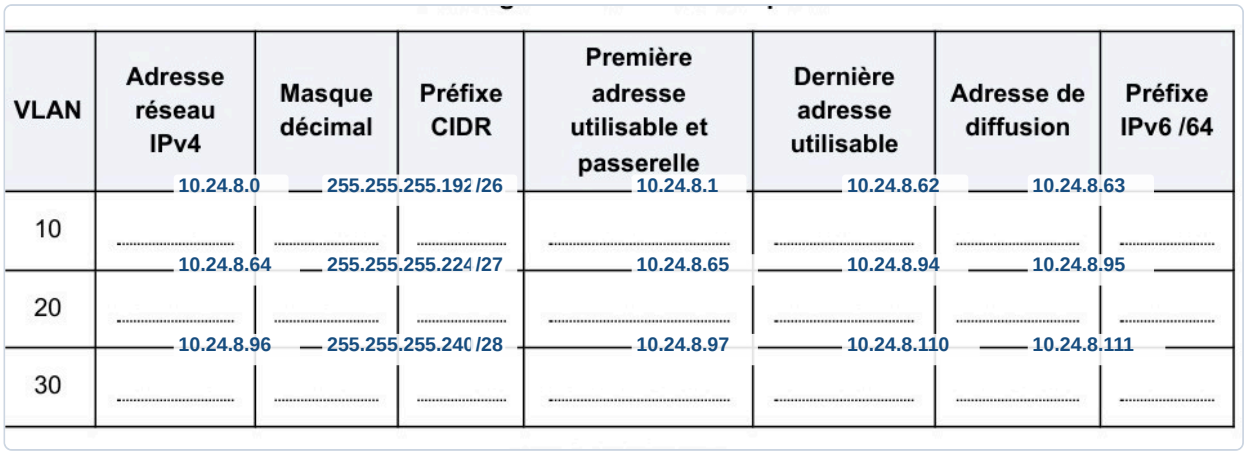
> ✓ **RÉPONSE À RETENIR**
>
> VLAN 10 : 6 bits d'hôtes, /26 ; VLAN 20 : 5 bits, /27 ; VLAN 30 : 4 bits, /28.

Question 1.2. En appliquant une allocation VLSM du plus grand besoin au plus petit, proposez pour chaque VLAN l'adresse réseau, le masque décimal, la première adresse utilisable, la dernière adresse utilisable et l'adresse de diffusion. Utilisez uniquement des blocs appartenant au réseau 10.24.8.0/24, sans chevauchement, et reportez vos résultats dans le DR 1.

VLAN	Adresse réseau	Masque décimal	Préfixe	Première adresse utilisable	Dernière adresse utilisable	Diffusion
10	10.24.8.0	255.255.255.192	/26	10.24.8.1	10.24.8.62	10.24.8.63
20	10.24.8.64	255.255.255.224	/27	10.24.8.65	10.24.8.94	10.24.8.95
30	10.24.8.96	255.255.255.240	/28	10.24.8.97	10.24.8.110	10.24.8.111

L'allocation suit l'ordre décroissant des besoins : 64 adresses pour le VLAN 10, 32 pour le VLAN 20 et 16 pour le VLAN 30. Les blocs sont alignés sur leurs frontières, contenus dans 10.24.8.0/24 et sans chevauchement. La première adresse utilisable de chaque plage est réservée à la passerelle.

DR 1 complété : adressage IPv4



✓ RÉPONSE À RETENIR

VLAN 10 : 10.24.8.0/26 ; VLAN 20 : 10.24.8.64/27 ; VLAN 30 : 10.24.8.96/28.

Question 1.3. Attribuez à chacun des VLAN 10, 20 et 30 un préfixe IPv6 /64 distinct pris dans le préfixe fourni. Indiquez chaque préfixe dans une notation IPv6 valide.

Le préfixe du site est 2001:db8:24::/48. Chaque sous-réseau demandé doit être un /64 distinct appartenant à ce préfixe. On utilise ici les identifiants de sous-réseau 1, 2 et 3 dans le quatrième groupe hexadécimal. Ces trois préfixes sont valides, distincts et peuvent être inscrits dans la colonne IPv6 du DR 1.

- VLAN 10 : 2001:db8:24:1::/64
- VLAN 20 : 2001:db8:24:2::/64
- VLAN 30 : 2001:db8:24:3::/64

DR 1 complété : préfixes IPv6

VLAN	Adresse réseau IPv4	Masque décimal	Préfixe CIDR	Première adresse utilisable et passerelle	Dernière adresse utilisable	Adresse de diffusion	Préfixe IPv6 /64
10	.....	.....	.....	.....	.....	.....	2001:db8:24:1::/64
20	.....	.....	.....	.....	.....	.....	2001:db8:24:2::/64
30	.....	.....	.....	.....	.....	.....	2001:db8:24:3::/64

✓ RÉPONSE À RETENIR

VLAN 10 : 2001:db8:24:1::/64 ; VLAN 20 : 2001:db8:24:2::/64 ; VLAN 30 : 2001:db8:24:3::/64.

Question 1.4. À partir des sous-réseaux IPv4 proposés, attribuez à chaque VLAN sa passerelle en choisissant la première adresse utilisable. Complétez ensuite dans le DR 1 les trois routes directement connectées de R1, en indiquant pour chacune le réseau de destination, le préfixe et l'interface VLAN de sortie précisée dans le DT 1.

Le DT 1 associe les VLAN 10, 20 et 30 aux sous-interfaces G0/0.10, G0/0.20 et G0/0.30. Pour chaque VLAN, la passerelle est la première adresse utilisable du sous-réseau. Les routes directement connectées reprennent le réseau et son préfixe, avec la sous-interface correspondante en sortie.

1. VLAN 10 : passerelle 10.24.8.1 ; réseau 10.24.8.0/26 via G0/0.10.
2. VLAN 20 : passerelle 10.24.8.65 ; réseau 10.24.8.64/27 via G0/0.20.
3. VLAN 30 : passerelle 10.24.8.97 ; réseau 10.24.8.96/28 via G0/0.30.

DR 1 complété : routes de R1

Entrées de routage directement connecté de R1

Réseau de destinatio 10.24.8.0	Préfi /26	Interface de sortie
10.24.8.64	/27	G0/0.10
10.24.8.96	/28	G0/0.20
		G0/0.30

✓ RÉPONSE À RETENIR

Passerelles : 10.24.8.1, 10.24.8.65, 10.24.8.97. Routes : 10.24.8.0/26 via G0/0.10 ; 10.24.8.64/27 via G0/0.20 ; 10.24.8.96/28 via G0/0.30.

Question 1.5. Décrivez le chemin logique des paquets lorsqu'un poste du VLAN 10 doit joindre le serveur du VLAN 20. Nommez l'équipement qui réalise le routage entre les VLAN et expliquez pourquoi le commutateur d'accès ne peut pas, à lui seul, acheminer ce trafic entre ces sous-réseaux dans la configuration fournie.

Le poste du VLAN 10 détecte que le serveur du VLAN 20 est dans un autre sous-réseau. Il envoie le paquet à sa passerelle par défaut, sur G0/0.10 de R1, en passant par SW1. R1 consulte sa table de routage, puis transmet le paquet vers le VLAN 20 par G0/0.20 et SW1, qui le remet au serveur.

R1 assure le routage inter-VLAN grâce à ses sous-interfaces. Dans cette configuration, SW1 commute les trames au niveau 2 et sépare les VLAN ; aucune fonction de routage entre ces sous-réseaux n'y est indiquée.

✓ RÉPONSE À RETENIR

Le paquet passe par SW1 jusqu'à R1, qui le route vers le VLAN 20 ; SW1 le transmet ensuite au serveur. R1 réalise le routage inter-VLAN.

2. Base de données relationnelle et requêtes SQL

La base relationnelle de l'écurie contient les tables Client, Cheval et Pension, dont le schéma, les relations et des exemples de données figurent dans le dossier technique. Les questions portent sur les pensions en cours au 15 mai 2026, l'agrégation des tarifs journaliers et la sécurisation des requêtes SQL.

Partie 2

Question 2.1. Écrivez une requête SQL qui affiche, pour les pensions en cours au 15 mai 2026, le nom du cheval, le nom du client et le tarif journalier. Une pension est en cours si sa date de début est antérieure ou égale à cette date et si sa date de fin est NULL ou postérieure ou égale à cette date. La requête doit relier correctement les trois tables.

La requête relie chaque pension à son cheval et à son client avec les clés étrangères du schéma. Les deux conditions de dates sélectionnent les pensions commencées au plus tard le 15 mai 2026 et encore actives ce jour-là. La condition sur la date de fin doit rester entre parenthèses pour appliquer correctement le OU.

```
SELECT Cheval.nom_cheval, Client.nom_client, Pension.tarif_journalier
FROM Pension
JOIN Cheval ON Pension.id_cheval = Cheval.id_cheval
JOIN Client ON Pension.id_client = Client.id_client
WHERE Pension.date_debut <= '2026-05-15'
  AND (Pension.date_fin IS NULL
       OR Pension.date_fin >= '2026-05-15');
```

✓ RÉPONSE À RETENIR

Afficher le cheval, le client et le tarif de chaque pension en cours au 15 mai 2026.

Question 2.2. Écrivez une requête SQL qui donne, pour chaque client ayant au moins une pension en cours au 15 mai 2026, son nom et la somme des tarifs journaliers de ses pensions en cours. Utilisez une fonction d'agrégation, regroupez les résultats par client et excluez les clients dont la somme est inférieure à 40 euros.

```
SELECT Client.nom_client, SUM(Pension.tarif_journalier) AS total_journalier
FROM Client
JOIN Pension ON Pension.id_client = Client.id_client
WHERE Pension.date_debut <= '2026-05-15'
  AND (Pension.date_fin IS NULL
       OR Pension.date_fin >= '2026-05-15')
GROUP BY Client.id_client, Client.nom_client
HAVING SUM(Pension.tarif_journalier) >= 40;
```

Le filtre de dates, placé dans WHERE, sélectionne les pensions à inclure avant le calcul des sommes. GROUP BY rassemble ces pensions par client. HAVING s'applique ensuite aux groupes et conserve les clients dont le total atteint au moins 40 euros par jour. Le regroupement par identifiant et par nom distingue correctement les clients.

✓ RÉPONSE À RETENIR

Sommer les tarifs des pensions en cours par client et retenir les totaux supérieurs ou égaux à 40 euros par jour.

Question 2.3. **Expliquez le principe d'une requête paramétrée permettant de remplacer la date inscrite directement dans la requête par une valeur transmise par l'application. Indiquez en quoi cette méthode réduit le risque d'injection SQL par rapport à la concaténation directe d'une chaîne saisie par l'utilisateur.**

Une requête paramétrée remplace la date écrite dans le SQL par un marqueur, par exemple `?`. L'application prépare la requête, puis transmet la date, telle que `2026-05-15`, séparément. Le moteur SQL traite cette valeur comme une donnée et non comme une instruction. À l'inverse, la concaténation directe d'une saisie peut modifier le texte SQL et y introduire des commandes malveillantes.

1. Préparer la requête avec un marqueur de paramètre.
2. Associer à ce marqueur la date fournie par l'application.

> **✓ RÉPONSE À RETENIR**
>
> Transmettre la date comme paramètre séparé évite de l'interpréter comme du code SQL.

Question 2.4. **Dans la requête de la question 2.2, précisez le rôle des clauses GROUP BY et HAVING. Distinguez le filtrage des lignes avant agrégation du filtrage des groupes après agrégation.**

Clause	Rôle dans la requête	Moment du filtrage
WHERE	Sélectionne les pensions en cours	Avant l'agrégation
GROUP BY	Rassemble les pensions par client	Forme les groupes à sommer
HAVING	Garde les groupes dont la somme atteint 40 euros	Après l'agrégation

WHERE filtre les lignes individuelles avant le calcul de `SUM`. GROUP BY constitue un groupe pour chaque client. HAVING filtre ensuite ces groupes selon leur somme de tarifs journaliers. Il ne remplace donc pas WHERE : les deux clauses interviennent à des étapes différentes de la requête.

> **✓ RÉPONSE À RETENIR**
>
> WHERE filtre les lignes avant calcul ; GROUP BY forme les groupes ; HAVING filtre les groupes après agrégation.

3. Cybersécurité, analyse d’incident et durcissement

Le serveur de gestion de l’écurie fournit une application web et est accessible en SSH. Le DT 2 décrit sa configuration de sécurité et présente des événements consignés le 15 mai 2026, à analyser avant de proposer des actions immédiates, des mesures de durcissement et une règle de sauvegarde.

Partie 3

Question 3.1. Relevez deux indices justifiant l’ouverture d’un incident de sécurité et construisez une chronologie concise des événements observés entre 08:41 et 08:44. Indiquez un élément à vérifier avant de conclure qu’une compromission a effectivement eu lieu.

Deux indices d’alerte : trois échecs SSH rapprochés visant *admin*, puis une connexion réussie de *gestion* depuis la même adresse et l’ajout d’un compte local par sudo.

Heure	Événement observé
08:41:02, 08:41:05, 08:41:09	Trois échecs d’authentification pour admin depuis 198.51.100.27
08:43:16	Connexion réussie pour gestion depuis cette adresse
08:44:03	Ajout d’un compte local par gestion

Ces faits justifient l’ouverture d’un incident, sans prouver à eux seuls une compromission. Vérifier si l’adresse source correspond à un salarié autorisé et si la connexion, puis la création du compte, étaient légitimes.

> ✓ **RÉPONSE À RETENIR**
>
> Incident à investiguer : échecs SSH, connexion réussie et création d’un compte. Vérifier l’autorisation de la source et l’origine de l’action avant de conclure à une compromission.

Question 3.2. Proposez deux actions immédiates et proportionnées à mener sur le serveur et les comptes concernés, en expliquant en une phrase l’objectif de chacune. N’effacez pas les journaux avant leur conservation.

1. Copier immédiatement les journaux et préserver les éléments de preuve dans un emplacement protégé, avant toute modification du serveur. Cela conserve les traces nécessaires à l’analyse.
2. Après cette conservation, désactiver le compte local nouvellement créé et interrompre les sessions SSH suspectes. Vérifier la légitimité de ces accès, puis révoquer ou renouveler les identifiants concernés si nécessaire, afin de limiter un accès non autorisé sans bloquer d’emblée tous les salariés partageant *gestion*.

> ✓ **RÉPONSE À RETENIR**
>
> Préserver les journaux, puis désactiver le compte ajouté et interrompre les sessions suspectes en vérifiant leur légitimité.

Question 3.3. Proposez quatre mesures de durcissement adaptées à la configuration SSH et au compte d’administration décrits dans le DT 2. Les mesures doivent couvrir au moins deux thèmes parmi l’authentification, la réduction de la surface d’exposition, la gestion des privilèges et la surveillance.

Appliquer quatre mesures directement liées aux faiblesses relevées dans la configuration :

- Restreindre SSH aux postes ou réseaux d’administration autorisés et le bloquer depuis le réseau invité.

- Désactiver l’authentification SSH par mot de passe et utiliser des clés individuelles protégées, avec une authentification multifacteur si disponible.
- Interdire la connexion SSH directe de *admin* et remplacer le compte partagé *gestion* par des comptes nominatifs.
- Limiter sudo aux seules commandes nécessaires et centraliser les journaux hors du serveur, avec des alertes sur les échecs d’authentification et les créations de comptes.

> **✓ RÉPONSE À RETENIR**
>
> Restreindre SSH, renforcer l’authentification, supprimer les accès directs et partagés, limiter sudo et centraliser la surveillance.

Question 3.4. Indiquez une règle essentielle de sauvegarde permettant de limiter l’impact d’un chiffrement malveillant qui toucherait à la fois les postes et le serveur connecté au réseau local.

Conserver au moins une copie de sauvegarde hors ligne ou immuable, inaccessible en écriture depuis les postes et le serveur du réseau local. La sauvegarde actuellement montée en écriture en permanence pourrait être chiffrée avec les systèmes connectés. Protéger aussi son accès avec des identifiants distincts et vérifier régulièrement qu’une restauration des données est possible.

> **✓ RÉPONSE À RETENIR**
>
> Garder une sauvegarde hors ligne ou immuable, inaccessible en écriture depuis le réseau local, et tester sa restauration.

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

Bilan de l'épreuve : Cette évaluation de formation contextualisée du baccalauréat professionnel Conduite et Gestion de l'Entreprise Hippique, session 2026, code 26-BCP-CGEH-EP1, dure trois heures et n'a pas de coefficient autonome. Dans le contexte de l'Écurie des Trois Chênes, elle évalue l'adressage IPv4 et IPv6 et le routage, les requêtes SQL sur les pensions, puis l'analyse d'incident et les mesures de cybersécurité.

Notions-clés, formules & règles à maîtriser

- Le nombre d'adresses utilisables d'un sous-réseau IPv4 est 2^h - 2, où h est le nombre de bits réservés aux hôtes.
- En VLSM, allouez d'abord les blocs les plus grands, puis vérifiez leurs bornes et l'absence de chevauchement.
- Une pension est en cours à une date si date_debut <= date et si date_fin IS NULL ou date_fin >= date.
- Une sauvegarde déconnectée ou immuable limite le risque qu'un chiffrement malveillant atteigne aussi les copies de sauvegarde.

Points de vigilance & attentes du jury

- Distinguez les adresses réseau et de diffusion des adresses attribuables aux hôtes.
- Vérifiez que les blocs VLSM restent dans 10.24.8.0/24 et ne se chevauchent pas.
- Reliez les tables SQL par leurs clés et traitez explicitement les dates de fin NULL.
- Séparez les faits observés des hypothèses et conservez les journaux avant toute intervention.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment déterminer rapidement le préfixe IPv4 adapté à un VLAN ?

Cherchez le plus petit nombre de bits h tel que 2^h - 2 couvre le nombre d'hôtes demandé. Le préfixe CIDR vaut 32 - h, car les adresses réseau et de diffusion ne sont pas attribuables.

Q : Comment distinguer WHERE et HAVING dans une requête avec une somme ?

WHERE sélectionne les pensions avant le calcul des sommes. GROUP BY rassemble les lignes par client, puis HAVING filtre les groupes selon leur somme, par exemple en ne conservant que ceux dont le total atteint 40 euros.

Q : Comment organiser le temps et tenir compte du barème de cette épreuve ?

L'épreuve dure trois heures et répartit 20 points entre trois parties : 7 pour le réseau, 7 pour SQL et 6 pour la cybersécurité. Prévoyez du temps pour compléter et rendre le DR 1.

Q : Quels critères faut-il privilégier dans les réponses de cybersécurité ?

Appuyez chaque constat sur le journal ou la configuration et distinguez-le d'une hypothèse. Proposez des mesures adaptées aux éléments fournis et conservez les journaux avant toute intervention.

Sujet officiel associé (PDF) : https://bacprocgeh.fr/assets/annales/bac-pro-cgeh/Informatique/2026/Bac Pro CGEH - Informatique - Session 2026 - 1-Sujet.pdf
Ressources Bac Pro CGEH : 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.