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 CAEHSCF, veuillez visiter :
bacprocaehscf.fr/annales-sujets-et-corriges

BAC PRO CAEHSCF • CORRIGÉ DÉTAILLÉ

Évaluation des compétences numériques : Informatique et réseaux

Session 2026 • Code sujet : **26-BCP-CAEH-EP1** • Durée : **2 heures** • Coefficient : **1**

Sommaire

Cliquez sur une partie pour y accéder directement

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

2. Base de données et exploitation des réservations (4 questions) **Page 5**

3. Cybersécurité, analyse de journaux et durcissement (4 questions) **Page 7**

4. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 9**

Sujet officiel (PDF) : https://bacprocaehscf.fr/assets/annales/bac-pro-caehscf/Informatique/2026/Bac Pro CAEHSCF - Informatique - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

L'établissement Les Quatre Pattes utilise un réseau local segmenté en VLAN pour l'administration, les soins, les visiteurs et la gestion réseau. Le candidat analyse les plans d'adressage IPv4 et IPv6, vérifie la configuration d'un poste et complète une table de routage vers le prestataire.

Adressage IPv4 du VLAN 20

Question 1.1. Pour le VLAN 20, indiquer le masque IPv4 en notation décimale pointée, l'adresse de diffusion et le nombre maximal d'adresses IPv4 utilisables par des hôtes.

Le plan indique le réseau VLAN 20 **192.168.10.64/26**. Le préfixe /26 laisse 32 - 26 = 6 bits pour les hôtes, donc le masque est **255.255.255.192**. Le bloc comprend 2^6 = 64 adresses, de 192.168.10.64 à 192.168.10.127. L'adresse la plus élevée est l'adresse de diffusion. En retirant l'adresse réseau et l'adresse de diffusion, le sous-réseau permet d'attribuer au maximum 62 adresses aux hôtes.

> ✓ **RÉPONSE À RETENIR**
>
> Masque : 255.255.255.192 ; diffusion : 192.168.10.127 ; maximum : 62 hôtes.

Vérification d'une configuration IPv4

Question 1.2. Déterminer si l'adresse IPv4 192.168.10.90/26 appartient au sous-réseau du VLAN 20 et si la passerelle 192.168.10.65 est cohérente avec le plan d'adressage. Justifier la réponse.

Le plan associe le VLAN 20 au réseau **192.168.10.64/26**, dont les adresses vont de 192.168.10.64 à 192.168.10.127. L'adresse 192.168.10.90 se trouve dans cette plage et n'est ni l'adresse réseau ni l'adresse de diffusion : c'est une adresse d'hôte valide. La passerelle indiquée, **192.168.10.65**, est bien celle attribuée au VLAN 20 dans le plan. Les deux paramètres sont donc cohérents.

> ✓ **RÉPONSE À RETENIR**
>
> 192.168.10.90 appartient au VLAN 20 ; 192.168.10.65 est sa passerelle cohérente.

Adressage IPv6 du VLAN 30

Question 1.3. Indiquer le préfixe IPv6 du VLAN 30 et proposer une adresse IPv6 d'hôte valide dans ce préfixe, différente de l'adresse réseau et de l'adresse de passerelle 2001:db8:4a10:30::1.

Le plan attribue au VLAN 30 le préfixe **2001:db8:4a10:30::/64**. Une adresse valide de ce sous-réseau conserve les quatre premiers groupes du préfixe et complète les bits d'hôte. Elle doit être différente de l'adresse réseau, dont la partie hôte est nulle, ainsi que de l'adresse de passerelle `2001:db8:4a10:30::1`. L'adresse `2001:db8:4a10:30::2` respecte ces conditions.

✓ RÉPONSE À RETENIR

Préfixe : 2001:db8:4a10:30::/64 ; exemple d'hôte : 2001:db8:4a10:30::2.

Routage statique

Question 1.4. Compléter le document réponse DR 1 avec une route statique vers le réseau de gestion 192.168.50.0/24 en indiquant le prochain saut 198.51.100.1. Indiquer également la route par défaut vers ce même prochain saut.

La route vers le réseau de gestion distant indique comme destination **192.168.50.0/24**. Son prochain saut est **198.51.100.1**, le routeur du prestataire, et l'interface de sortie est WAN. La route par défaut utilise le préfixe `0.0.0.0/0` et le même prochain saut. Elle oriente vers le prestataire tout trafic qui ne correspond pas à une route plus spécifique. Les deux prochains sauts sont reportés dans les cellules prévues du DR 1.

Table de routage DR 1 complétée

Table de routage de R1

Destination	Préfixe	Prochain saut	Action ou interface
Réseau de gestion distant	192.168.50.0/24	198.51.100.1	WAN
Route par défaut	0.0.0.0/0	198.51.100.1	WAN

✓ RÉPONSE À RETENIR

192.168.50.0/24 via 198.51.100.1, WAN ; 0.0.0.0/0 via 198.51.100.1, WAN.

2. Base de données et exploitation des réservations

La pension utilise une base relationnelle composée des tables Animal, Client et Sejour pour suivre les réservations. Le candidat doit expliquer les relations entre les tables et rédiger ou compléter des requêtes SQL sur les séjours confirmés, le nombre d'animaux par espèce et les montants.

Clé étrangère et intégrité relationnelle

Question 2.1. Expliquer le rôle de la clé étrangère id_animal dans la table Sejour, préciser avec quelle clé primaire elle est reliée et citer une incohérence que cette relation permet d'éviter.

Une clé étrangère établit un lien entre une ligne et un enregistrement d'une autre table. Ici, `Sejour.id_animal` doit correspondre à une valeur existante de la clé primaire `Animal.id_animal`. Cette contrainte d'intégrité référentielle garantit que chaque séjour est rattaché à un animal identifié dans la base. Elle évite, par exemple, d'enregistrer une réservation avec un identifiant d'animal qui n'existe pas dans la table `Animal`.

> ✓ **RÉPONSE À RETENIR**
>
> `Sejour.id_animal` référence la clé primaire `Animal.id_animal` et empêche d'associer un séjour à un animal inexistant.

Requête SQL sur les séjours confirmés

Question 2.2. Compléter la requête du document réponse DR 1 afin d'afficher le nom de l'animal, le nom du client et les dates de début et de fin des séjours dont le statut est « confirmé ». Classer les résultats du plus récent au plus ancien selon date_debut.

La jointure entre `Animal` et `Sejour` associe chaque séjour à son animal grâce à `id_animal`. La jointure avec `Client` utilise ensuite `id_client`. Le filtre conserve les séjours confirmés. Enfin, le tri décroissant sur `date_debut` place les dates les plus récentes en premier. Les colonnes sélectionnées sont celles indiquées dans le document réponse.

Requête complétée dans le DR 1

Requête SQL à compléter

Élément	Réponse du candidat
Requête	SELECT Animal.nom, Client.nom_client, Sejour.date_debut, Sejour.date_fin FROM Animal JOIN Sejour ON ... JOIN Client ON ... WHERE Sejour.statut = 'confirmé' ORDER BY ...;

Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :

```
SELECT Animal.nom, Client.nom_client, Sejour.date_debut, Sejour.date_fin
FROM Animal JOIN Sejour ON Animal.id_animal = Sejour.id_animal
JOIN Client ON Sejour.id_client = Client.id_client
WHERE Sejour.statut = 'confirmé'
ORDER BY Sejour.date_debut DESC;
```

✓ RÉPONSE À RETENIR

```
SELECT Animal.nom, Client.nom_client, Sejour.date_debut, Sejour.date_fin
FROM Animal JOIN Sejour ON Animal.id_animal = Sejour.id_animal
JOIN Client ON Sejour.id_client = Client.id_client
WHERE Sejour.statut = 'confirmé'
ORDER BY Sejour.date_debut DESC;
```

Comptage par espèce

Question 2.3. Rédiger une requête SQL affichant, pour chaque espèce présente dans la table Animal, le nombre d'animaux. Nommer la colonne de résultat nombre_animaux et classer les résultats par nombre décroissant.

Pour obtenir un effectif distinct pour chaque espèce, regroupez les lignes de `Animal` avec `GROUP BY espece`. La fonction `COUNT(*)` compte les animaux dans chaque groupe. L'alias `nombre_animaux` donne à la colonne le nom exigé. Le tri décroissant sur cet alias place en tête l'espèce ayant le plus grand nombre d'animaux.

✓ RÉPONSE À RETENIR

```
SELECT espece, COUNT(*) AS nombre_animaux
FROM Animal
GROUP BY espece
ORDER BY nombre_animaux DESC;
```

Total des séjours confirmés

Question 2.4. Rédiger une requête SQL utilisant la fonction SUM pour calculer le montant total des séjours confirmés du client dont id_client vaut 12. Nommer la colonne de résultat total_confirme.

La table `Sejour` contient les colonnes `montant`, `id_client` et `statut`. La fonction `SUM` additionne les montants des lignes qui respectent les deux conditions : le client a l'identifiant 12 et le séjour est confirmé. L'alias `total_confirme` nomme la colonne renvoyée par la requête.

✓ RÉPONSE À RETENIR

```
SELECT SUM(montant) AS total_confirme
FROM Sejour
WHERE id_client = 12 AND statut = 'confirmé';
```

3. Cybersécurité, analyse de journaux et durcissement

Les journaux du serveur font apparaître des échecs SSH, une connexion réussie au compte admin, l'exécution d'une commande avec privilèges élevés et une connexion sortante vers l'adresse source. Le candidat reconstitue l'incident, propose des mesures immédiates et de durcissement, puis définit un filtrage pour le VLAN visiteurs.

Chronologie et indices de suspicion

Question 3.1. Reconstituer la chronologie de l'incident à partir des journaux, relever deux indices qui rendent la connexion suspecte et expliquer pourquoi l'adresse 203.0.113.77 doit être traitée avec prudence dans ce contexte.

Le 14 mai 2026, deux échecs d'authentification SSH visant `admin` surviennent à 21:14:02 et 21:14:08 depuis `203.0.113.77`. Une connexion réussit à 21:14:15, puis le compte admin exécute une commande avec privilèges élevés à 21:16:41. À 21:18:03, le serveur établit une connexion sortante vers cette même adresse sur TCP 443. Les échecs suivis d'une réussite et l'usage de privilèges élevés sont deux indices suspects. De plus, l'adresse appartient à une plage réservée aux exemples documentaires : elle ne permet pas d'identifier une origine réelle fiable.

> **✓ RÉPONSE À RETENIR**
>
> Échecs SSH, connexion réussie, commande privilégiée, puis trafic sortant vers la même adresse. L'adresse étant réservée à la documentation, son origine réelle n'est pas identifiable.

Mesures immédiates et préservation des éléments d'analyse

Question 3.2. Indiquer deux mesures immédiates permettant de limiter l'incident et de préserver les éléments utiles à son analyse. Justifier chacune en lien avec les informations des journaux.

Prendre immédiatement deux mesures complémentaires. Isoler le serveur du réseau sans l'éteindre si possible : cela limite les échanges potentiellement malveillants après l'accès privilégié et la connexion sortante vers TCP 443. Préserver ensuite les journaux d'authentification et du pare-feu, ainsi que les éléments volatils pertinents, en réalisant une copie protégée. Ces traces documentent les échecs SSH, la connexion réussie, l'usage de `sudo` et le trafic vers l'adresse suspecte ; elles sont essentielles à l'analyse de l'incident.

> **✓ RÉPONSE À RETENIR**
>
> Isoler le serveur sans l'éteindre et préserver, copier de façon sécurisée les journaux ainsi que les éléments utiles à l'analyse.

Durcissement des accès SSH

Question 3.3. Proposer deux mesures de durcissement des accès SSH adaptées au serveur de gestion. La réponse doit inclure une mesure d'authentification et une mesure limitant l'exposition du service.

Imposer une authentification SSH par clé et désactiver l'authentification par mot de passe ; désactiver également la connexion directe de `root`. Pour limiter l'exposition du service, autoriser SSH uniquement depuis le réseau d'administration, ou depuis un VPN dédié, et refuser les autres sources au pare-feu. Ces mesures réduisent le risque de nouvelles tentatives et empêchent qu'un accès soit possible depuis des réseaux non autorisés, comme l'accès suspect observé depuis une adresse inconnue.

> **✓ RÉPONSE À RETENIR**
>
> Authentification par clé, mots de passe SSH et connexion directe de `root` désactivés ; accès SSH limité au réseau d'administration ou au VPN.

Filtrage du VLAN visiteurs

Question 3.4. Indiquer une règle de filtrage réduisant le risque d'accès aux données de l'établissement depuis le VLAN 30. Préciser la source, la destination ou les destinations à protéger et l'action attendue.

Sur R1, filtrer le trafic provenant du VLAN visiteurs, soit `192.168.10.128/27`. Refuser ses connexions vers les réseaux internes des VLAN 10, 20 et 99, notamment vers le serveur de gestion du VLAN 20. Appliquer cette règle avant les autorisations générales, tout en permettant séparément les services nécessaires aux visiteurs, comme l'accès Internet. Cette séparation réduit les possibilités d'accès aux données et aux équipements de l'établissement depuis le réseau invité.

> **✓ RÉPONSE À RETENIR**
>
> Depuis `192.168.10.128/27`, refuser l'accès aux réseaux des VLAN 10, 20 et 99, notamment au serveur du VLAN 20 ; autoriser uniquement les services visiteurs nécessaires.

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

Bilan de l'épreuve : L'épreuve de compétences numériques du baccalauréat professionnel CAEH, session 2026, code 26-BCP-CAEH-EP1, dure deux heures et a un coefficient 1. Elle s'appuie sur le système d'information de la pension Les Quatre Pattes et évalue l'adressage et le routage réseau, l'exploitation d'une base SQL de réservations, ainsi que l'analyse d'un incident de sécurité et les mesures de protection adaptées.

Notions-clés, formules & règles à maîtriser

- Un réseau IPv4 en /26 contient 64 adresses, dont 62 utilisables après exclusion des adresses réseau et de diffusion.
- Une clé étrangère relie une valeur de la table Sejour à une clé primaire existante dans la table référencée.
- Pour compter les animaux par espèce, utiliser COUNT et GROUP BY espece, puis classer avec ORDER BY nombre_animaux DESC.
- Le bloc 203.0.113.0/24 est réservé à la documentation et aux exemples : une adresse de cette plage doit être interprétée avec prudence.

Points de vigilance & attentes du jury

- Vérifier le préfixe, le masque, l'adresse réseau, la diffusion et les adresses d'hôtes avant de valider une configuration IPv4.
- Dans les jointures SQL, relier les clés étrangères aux clés primaires et respecter exactement les noms des tables et colonnes fournis.
- Pour analyser l'incident, replacer les événements dans l'ordre horaire et distinguer confinement du système et préservation des journaux.
- Pour le filtrage du VLAN visiteurs, préciser la source, les destinations protégées et l'action appliquée aux flux.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment déterminer les adresses utilisables d'un réseau IPv4 en /26 ?

Un préfixe /26 laisse 6 bits pour les hôtes, soit 64 adresses. On retire l'adresse réseau et l'adresse de diffusion, ce qui donne 62 adresses utilisables. Pour le VLAN 20, elles vont de 192.168.10.65 à 192.168.10.126.

Q : Comment construire la requête qui compte les animaux par espèce ?

Sélectionnez espece et COUNT(*) AS nombre_animaux depuis Animal, regroupez les lignes avec GROUP BY espece, puis classez avec ORDER BY nombre_animaux DESC. Conservez les noms de tables et colonnes indiqués dans le sujet.

Q : Comment organiser son temps pendant cette épreuve de deux heures ?

Vous pouvez viser environ quarante minutes par partie, en gardant quelques minutes pour vérifier les réponses. Les parties sont indépendantes : commencez par les questions maîtrisées et vérifiez ensuite les calculs, la syntaxe SQL et le report demandé sur DR 1.

Q : Quels éléments rendent une réponse de cybersécurité complète dans ce sujet ?

Appuyez-vous sur l'ordre et le contenu des journaux, proposez des mesures qui limitent l'incident tout en préservant les éléments d'analyse, puis associez au durcissement SSH une authentification renforcée et une réduction de l'exposition du service.

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