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 CPH, veuillez visiter :
bacprocph.fr/annales-sujets-et-corriges

Bac Pro CPH

Épreuve E4 : Culture scientifique et technologique, capacité C4.2

Session 2026 • Code sujet : **26-BCP-CPH-E4** • Durée : **120 minutes** • Coefficient : **1**

Sommaire

Cliquez sur une partie pour y accéder directement

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

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

3. Cybersécurité et analyse des événements (4 questions) **Page 7**

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

Sujet officiel (PDF) : https://bacprocph.fr/assets/annales/bac-pro-cph/Informatique/2026/Bac Pro CPH - Informatique - Session 2026 - 1-Sujet.pdf

1. Architecture réseau et adressage

L'exploitation horticole Les Serres de la Plaine sépare les postes administratifs, les équipements de serre et les serveurs en VLAN. À partir de la topologie et du plan d'adressage du DT 1, il faut interpréter le rôle des équipements et vérifier des paramètres IPv4 et IPv6.

Question 1.1. À partir de la topologie du DT 1, indiquez le rôle du commutateur SW1 et celui du routeur R1. Expliquez en une phrase pourquoi les capteurs de serre sont placés dans un VLAN différent des postes administratifs.

SW1 commute les équipements locaux et transporte les VLAN 10, 20 et 30 vers R1 sur une liaison trunk. **R1** route les paquets entre ces trois VLAN et utilise le pare-feu comme prochain saut pour la route par défaut. Placer les capteurs dans le VLAN 20 sépare leur trafic de celui des postes administratifs. Cette segmentation limite les communications entre groupes et facilite l'application de règles de sécurité adaptées à chaque usage.

> ✓ **RÉPONSE À RETENIR**
>
> SW1 commute les équipements et transporte les VLAN ; R1 route entre les VLAN. Le VLAN 20 sépare les capteurs des postes administratifs.

Question 1.2. Pour le réseau IPv4 192.168.10.0/27 du VLAN 10, donnez le masque en notation décimale pointée, l'adresse de diffusion et la plage d'adresses utilisables pour les équipements. Indiquez si l'adresse 192.168.10.14 appartient à cette plage.

Le préfixe **/27** laisse 5 bits pour les adresses hôtes, soit 32 adresses dans le bloc. Le masque correspondant est **255.255.255.224**. Pour le réseau 192.168.10.0/27, l'adresse réseau est 192.168.10.0 et l'adresse de diffusion est 192.168.10.31. Les adresses utilisables par les équipements vont donc de 192.168.10.1 à 192.168.10.30. Comme 192.168.10.14 est comprise dans cette plage, elle peut être attribuée à un équipement.

> ✓ **RÉPONSE À RETENIR**
>
> Masque : 255.255.255.224 ; diffusion : 192.168.10.31 ; plage utilisable : 192.168.10.1 à 192.168.10.30. 192.168.10.14 est utilisable.

Question 1.3. Complétez dans le DR 1 la table de routage simplifiée de R1. Pour chaque réseau de destination, inscrivez l'interface de sortie correspondante. Pour la route par défaut, indiquez le prochain saut fourni par le DT 1.

Chaque réseau de destination directement raccordé à R1 utilise son interface logique correspondante : G0/0.10 pour le VLAN 10, G0/0.20 pour le VLAN 20 et G0/0.30 pour le VLAN 30. Pour la route par défaut, le prochain saut est le pare-feu, à l'adresse 192.168.30.2. Comme ce pare-feu se trouve sur le VLAN 30, la sortie s'effectue par G0/0.30. Ces valeurs sont reportées dans le tableau du DR 1.

DR 1 complété : table de routage

Destination	Interface de sortie	Prochain saut
192.168.10.0/27	G0/0.10	Réseau directement connecté
192.168.20.0/27	G0/0.20	Réseau directement connecté
192.168.30.0/28	G0/0.30	Réseau directement connecté
0.0.0.0/0	G0/0.30	192.168.30.2

✓ RÉPONSE À RETENIR

VLAN 10 : G0/0.10 ; VLAN 20 : G0/0.20 ; VLAN 30 : G0/0.30. Route par défaut : G0/0.30, prochain saut 192.168.30.2.

Question 1.4. Un capteur du VLAN 20 possède l'adresse IPv6 2001:db8:24:20::45/64. Donnez l'adresse IPv6 de sa passerelle d'après le DT 1 et expliquez pourquoi le préfixe IPv6 du VLAN 10 ne doit pas remplacer celui du VLAN 20 pour joindre cette passerelle.

La passerelle IPv6 du VLAN 20 est **2001:db8:24:20::1**. Le préfixe /64 désigne les 64 premiers bits de l'adresse, qui identifient le réseau. Le capteur et sa passerelle appartiennent donc au même réseau, **2001:db8:24:20::/64**. Le préfixe **2001:db8:24:10::/64** est celui du VLAN 10 : le substituer désignerait un autre réseau, et ne permettrait pas d'identifier correctement la passerelle du capteur.

✓ RÉPONSE À RETENIR

Passerelle IPv6 : 2001:db8:24:20::1. Le préfixe du VLAN 10 désigne un autre réseau.

2. Base de données et exploitation des relevés

L'application de suivi des cultures enregistre les mesures de température et d'humidité dans les tables relationnelles Capteur et Releve. Le DT 2 fournit le schéma et des relevés du 15 juin 2026 à interroger et analyser.

Question 2.1. Complétez dans le DR 1 la requête SQL afin d'afficher le nom du capteur, la température et l'humidité pour les relevés du 15 juin 2026 dont la température est supérieure à 28 °C. Utilisez les noms de colonnes fournis dans le DT 2.

La requête sélectionne le nom du capteur et les deux mesures. Comme le nom se trouve dans `Capteur`, on relie cette table à `Releve` par leur identifiant commun, puis on applique les critères de date et de température.

Requête de filtrage complétée

Requête SQL de filtrage : question 2.1

```
SELECT Capteur.nom, Releve.temperature, Releve.humidite
FROM Capteur JOIN Releve ON Capteur.id_capteur = Releve.id_capteur
WHERE date_releve = '2026-06-15' AND temperature > 28;
```

Compléter les groupes de points pour sélectionner les relevés demandés.

✓ **RÉPONSE À RETENIR**

```
SELECT Capteur.nom, Releve.temperature, Releve.humidite
FROM Capteur JOIN Releve ON Capteur.id_capteur = Releve.id_capteur
WHERE date_releve = '2026-06-15' AND temperature > 28;
```

Question 2.2. Complétez dans le DR 1 la requête SQL qui relie les tables Capteur et Releve grâce à leur identifiant commun et affiche, pour chaque relevé du 15 juin 2026, le nom du capteur et la température mesurée. Utilisez une jointure explicite avec la clause JOIN.

La jointure explicite associe chaque relevé à son capteur avec la clé étrangère `Releve.id_capteur`. On affiche ensuite le nom du capteur et la température du relevé, en filtrant sur la date demandée.

Requête avec jointure complétée

Requête SQL avec jointure : question 2.2

```
SELECT Capteur.nom, Releve.temperature
FROM Releve JOIN Capteur ON Releve.id_capteur = Capteur.id_capteur
WHERE date_releve = '2026-06-15';
```

✓ **RÉPONSE À RETENIR**

```
SELECT Capteur.nom, Releve.temperature
FROM Releve JOIN Capteur ON Releve.id_capteur = Capteur.id_capteur
WHERE date_releve = '2026-06-15';
```

Question 2.3. **À partir des relevés fournis dans le DT 2, calculez la température moyenne du capteur S02 le 15 juin 2026. Donnez le résultat au dixième de degré Celsius près et indiquez les valeurs utilisées dans le calcul.**

Les relevés de S02 sont de 24 °C et 26 °C. Leur moyenne est $(24 + 26)/2 = 25$, soit 25,0 °C au dixième près.

> ✓ **RÉPONSE À RETENIR**
>
> Température moyenne de S02 : 25,0 °C.

Question 2.4. **Un relevé du capteur S03 affiche une température de 42 °C, alors que les autres relevés de la même zone sont compris entre 21 °C et 25 °C. Indiquez une vérification à effectuer avant d'utiliser cette valeur pour décider d'une intervention sur la culture, puis expliquez brièvement pourquoi cette vérification est nécessaire.**

Contrôler le positionnement et l'état de la sonde, puis vérifier la valeur avec une mesure indépendante dans la même zone. L'écart avec les autres relevés peut signaler une sonde défectueuse ou une erreur de mesure. Cette vérification évite de décider d'une intervention sur la culture à partir d'une donnée potentiellement erronée.

> ✓ **RÉPONSE À RETENIR**
>
> Contrôler la sonde et confirmer la température par une mesure indépendante avant toute intervention.

3. Cybersécurité et analyse des événements

L'administratrice examine des événements de connexion SSH consignés dans le journal système et cherche à renforcer la sécurité des comptes de l'exploitation. Le DT 2 décrit aussi la copie nocturne des relevés vers un espace cloud et les informations disponibles sur les sauvegardes.

Question 3.1. Relevez l'adresse IP à l'origine des tentatives de connexion refusées, le compte visé et leur nombre. Calculez la durée entre la première et la dernière tentative refusée.

Le journal recense quatre connexions SSH refusées depuis **203.0.113.77**, toutes pour le compte **admin**. La première tentative refusée est horodatée à 08:42:03 et la dernière à 08:43:01. En secondes après 08:42:00, cela donne $61 - 3 = 58$ secondes. La durée entre les deux tentatives est donc de 58 secondes.

> ✓ **RÉPONSE À RETENIR**
>
> 203.0.113.77 a effectué 4 tentatives SSH refusées visant admin, sur une durée de 58 s.

Question 3.2. À partir des seules informations du DT 2, expliquez pourquoi ces événements justifient une vérification sans affirmer qu'une intrusion a réussi. Citez un élément du journal qui limite ce que l'on peut conclure.

Les quatre refus SSH rapprochés provenant de la même adresse justifient de vérifier les journaux et les règles d'accès au serveur. Selon le DT 2, cette adresse n'appartient pas au plan d'adressage local. Toutefois, l'extrait ne contient aucune connexion réussie depuis 203.0.113.77 : il ne prouve donc pas qu'une intrusion a abouti. Le DT 2 précise aussi que les événements ne permettent pas d'identifier la personne à l'origine des tentatives.

> ✓ **RÉPONSE À RETENIR**
>
> Vérifier les tentatives répétées : aucune connexion réussie depuis cette adresse ni identité de leur auteur n'est établie.

Question 3.3. Proposez deux mesures techniques adaptées pour réduire le risque de connexion non autorisée au serveur. Pour chacune, indiquez le risque qu'elle permet de réduire.

Deux mesures techniques réduisent les possibilités d'accès SSH non autorisé :

- Activer l'authentification multifacteur : un mot de passe volé ou deviné ne suffit alors pas, à lui seul, pour ouvrir une session.
- Filtrer les connexions SSH pour n'autoriser que les sources nécessaires et limiter les tentatives répétées : cela réduit l'exposition du serveur aux accès externes et aux essais successifs de mots de passe.

Ces mesures diminuent les risques sans remplacer la surveillance des journaux.

> ✓ **RÉPONSE À RETENIR**
>
> Activer l'authentification multifacteur et limiter l'accès SSH aux sources autorisées, avec blocage des tentatives répétées.

Question 3.4. Le DT 2 indique que les relevés sont copiés chaque nuit vers un espace cloud. Proposez une mesure de protection des identifiants de cet espace et une mesure permettant de vérifier que les sauvegardes pourront être restaurées.

Pour protéger le compte nominatif de l'espace cloud, utiliser un mot de passe robuste et unique, le conserver dans un gestionnaire de mots de passe et activer l'authentification multifacteur. Pour vérifier que les copies nocturnes sont réellement exploitables, réaliser périodiquement un test de restauration à partir d'une sauvegarde, dans un environnement distinct. Contrôler ensuite que les fichiers restaurés sont lisibles et que les relevés attendus sont présents.

> **✓ RÉPONSE À RETENIR**
>
> Protéger le compte cloud par un mot de passe unique et l'authentification multifacteur ; tester régulièrement la restauration.

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

Bilan de l'épreuve : Cette épreuve E4 du baccalauréat professionnel Conduite de productions horticoles, session 2026, porte le code 26-BCP-CPH-E4 et dure 120 minutes, coefficient 1. Dans le contexte des Serres de la Plaine, elle évalue l'adressage réseau, les requêtes SQL et l'analyse des relevés horticoles, ainsi que l'interprétation d'événements de sécurité et la protection des sauvegardes.

Notions-clés, formules & règles à maîtriser

- Un préfixe IPv4 /27 correspond au masque 255.255.255.224 et à des blocs de 32 adresses.
- Les interfaces logiques de R1 relient directement chaque VLAN à son réseau; la route par défaut pointe vers 192.168.30.2.
- Une jointure SQL explicite associe les clés correspondantes avec JOIN et ON.
- La moyenne arithmétique est la somme des valeurs divisée par leur nombre.

Points de vigilance & attentes du jury

- Distinguez l'adresse réseau, l'adresse de diffusion et les adresses utilisables pour un équipement.
- Associez chaque réseau directement connecté à l'interface logique de R1 correspondant à son VLAN.
- Respectez les noms des tables et colonnes, les conditions de date et la syntaxe SQL demandée.
- Rapportez les faits visibles dans le journal sans conclure à une intrusion réussie si elle n'est pas attestée.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment déterminer la plage d'adresses utilisables d'un réseau IPv4 ?

Pour un préfixe /27, le masque est 255.255.255.224 et le bloc contient 32 adresses. Pour 192.168.10.0/27, .0 est l'adresse réseau et .31 l'adresse de diffusion; les équipements utilisent les adresses de .1 à .30.

Q : Comment relier les tables Capteur et Releve dans une requête SQL ?

Utilisez JOIN pour associer les deux tables, puis ON pour faire correspondre Releve.id_capteur à Capteur.id_capteur. Sélectionnez les colonnes demandées et filtrez la date du relevé avec une condition WHERE.

Q : Comment gérer le temps pendant cette épreuve de 120 minutes ?

Répartissez le temps selon les barèmes des trois parties, soit 7, 7 et 6 points. Gardez quelques minutes pour vérifier les calculs, les unités et les réponses à reporter dans le DR 1. La calculatrice n'est pas autorisée.

Q : Que faut-il montrer pour répondre à une question de sécurité fondée sur un journal ?

Appuyez chaque conclusion sur les événements visibles et distinguez les faits de ce qu'ils ne permettent pas d'établir. Une tentative SSH refusée ne prouve pas une intrusion réussie; proposez des mesures adaptées aux risques cités.

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