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 CIEL, veuillez visiter :
coursbacprociel.fr/annales-sujets-et-corriges

Valorisation de la donnée et cybersécurité

Session 2026 • Code sujet : **26-BCP-CIEL-E32** • Durée : **3 heures** • Coefficient : **3**

Sommaire

Cliquez sur une partie pour y accéder directement

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

2. Valorisation des données et développement (3 questions) **Page 5**

3. Analyse d'incident et durcissement des accès (3 questions) **Page 7**

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

Sujet officiel (PDF) : https://coursbacprociel.fr/assets/annales/bac-pro-ciel/Valorisation de la donnée et cybersécurité/2026/Bac Pro CIEL - Valorisation de la donnée et cybersécurité - Session 2026 - 1-Sujet.pdf

1. Architecture réseau et adressage

Dans le réseau segmenté de l'Atelier Logistique des Rives, le routeur R1 assure le routage inter-VLAN et l'accès à un réseau distant. À partir de la topologie et du plan d'adressage, il faut vérifier l'adressage IPv4 et IPv6 puis compléter la table de routage.

Question 1.1. Pour PC-LOG, à partir de l'adresse IPv4 indiquée dans le DT 1, donner l'adresse réseau, l'adresse de diffusion et la première adresse utilisable du sous-réseau, puis préciser si le poste appartient au VLAN 10, 20 ou 99.

PC-LOG utilise l'adresse **192.168.10.25/24**. Avec un masque /24, les trois premiers octets définissent le réseau : 192.168.10.0/24. L'adresse de diffusion est 192.168.10.255 et la première adresse utilisable est 192.168.10.1. Le plan d'adressage rattache PC-LOG au **VLAN 10**.

> ✓ RÉPONSE À RETENIR
>
> Réseau : 192.168.10.0/24 ; diffusion : 192.168.10.255 ; première adresse utilisable : 192.168.10.1 ; VLAN 10.

Question 1.2. Pour les VLAN 10 et 20, proposer les deux préfixes IPv6 /64 à utiliser dans le préfixe du DT 1. Préciser l'adresse de passerelle IPv6 de chaque VLAN en appliquant la convention d'attribution indiquée dans le DT 1.

Le DT 1 attribue un /64 à chaque VLAN et utilise son numéro comme identifiant de sous-réseau dans le préfixe 2001:db8:42::/48. Les préfixes sont donc 2001:db8:42:10::/64 pour le VLAN 10 et 2001:db8:42:20::/64 pour le VLAN 20. La passerelle est la première adresse d'hôte, terminée par ::1.

> ✓ RÉPONSE À RETENIR
>
> VLAN 10 : 2001:db8:42:10::/64, passerelle 2001:db8:42:10::1. VLAN 20 : 2001:db8:42:20::/64, passerelle 2001:db8:42:20::1.

Question 1.3. Compléter dans le DR 1 les entrées manquantes de la table de routage de R1. Pour le réseau du serveur distant, indiquer le préfixe de destination et le prochain saut ; pour les réseaux directement connectés, indiquer l'interface de sortie appropriée. La route par défaut est déjà présente.

Les réseaux des VLAN 10, 20 et 99 sont directement connectés aux sous-interfaces correspondantes de R1. Le réseau 172.16.0.0/30 est connecté à G0/1. Le réseau distant 10.50.0.0/16 est atteint via 172.16.0.1, également par G0/1. La route par défaut fournie reste inchangée.

Destination	Prochain saut	Interface de sortie
192.168.10.0/24	Directement connecté	G0/0.10
192.168.20.0/24	Directement connecté	G0/0.20
192.168.99.0/24	Directement connecté	G0/0.99
172.16.0.0/30	Directement connecté	G0/1
10.50.0.0/16	172.16.0.1	G0/1

Table de routage de R1 complétée

Destination	Prochain saut	Interface de sortie
192.168.10.0/24	Directement connecté	G0/0.10
192.168.20.0/24	Directement connecté	G0/0.20
192.168.99.0/24	Directement connecté	G0/0.99
172.16.0.0/30	Directement connecté	G0/1
10.50.0.0/16	172.16.0.1	G0/1
0.0.0.0/0	172.16.0.1	G0/1

✓ RÉPONSE À RETENIR

Routes directement connectées : G0/0.10, G0/0.20, G0/0.99 et G0/1. Réseau 10.50.0.0/16 : prochain saut 172.16.0.1, sortie G0/1.

2. Valorisation des données et développement

Le responsable informatique souhaite obtenir le nombre d'équipements actifs par site à partir d'une base relationnelle. Il demande aussi un outil Python qui compte les événements d'authentification échoués, avec des tests automatisés et un commentaire d'utilisation.

Question 2.1. Rédiger une requête SQL affichant, pour chaque site possédant au moins un équipement actif, le nom du site et le nombre d'équipements actifs. Utiliser une jointure entre les tables du DT 2, filtrer les équipements actifs, regrouper par site et trier par nom de site dans l'ordre croissant.

La jointure associe chaque équipement à son site par `site_id = id`. Le filtre `actif = 1` exclut OLD-PC, puis le regroupement compte les équipements actifs de chaque site. La jointure interne écarte automatiquement les sites sans équipement actif. Le tri croissant affiche Romans avant Valence.

```
SELECT s.nom, COUNT(e.id) AS nombre_equipements_actifs
FROM site AS s
JOIN equipement AS e ON e.site_id = s.id
WHERE e.actif = 1
GROUP BY s.id, s.nom
ORDER BY s.nom ASC;
```

✓ RÉPONSE À RETENIR

Romans : 1 équipement actif ; Valence : 2 équipements actifs.

Question 2.2. Dans le fichier analyse.py fourni sur le poste, écrire la fonction compter_echecs(lignes). Le paramètre lignes est une liste de dictionnaires comportant les clés event et user. La fonction retourne le nombre de dictionnaires dont la valeur de event est exactement LOGIN_FAIL ; une liste vide doit produire 0. Ajouter un commentaire décrivant le rôle de la fonction.

La fonction compte uniquement les dictionnaires dont la valeur associée à `event` est exactement `LOGIN_FAIL`. La clé `user` fait partie des données reçues, mais n'intervient pas dans ce comptage.

1. Ajouter cette fonction et son commentaire dans `analyse.py` :
2. La somme est nulle si aucune ligne ne correspond, notamment pour une liste vide.

```
def compter_echecs(lignes):
    """Compte les événements d'authentification LOGIN_FAIL."""
    return sum(1 for ligne in lignes
               if ligne["event"] == "LOGIN_FAIL")
```

✓ RÉPONSE À RETENIR

La fonction retourne le nombre de valeurs `LOGIN_FAIL` ; pour une liste vide, elle retourne 0.

Question 2.3. Tester la fonction avec les quatre événements du DT 2 et avec une liste vide, indiquer les deux résultats attendus, ajouter au fichier un test automatisé pour chacun de ces cas et rédiger un court commentaire d'utilisation précisant les données attendues par la fonction.

Les données de test sont des dictionnaires contenant les clés `event` et `user`. Les événements à compter doivent porter exactement la valeur `LOGIN_FAIL`.

- Dans les quatre événements du DT 2, trois ont cette valeur.
- La liste vide vérifie le cas limite demandé.
- Les assertions ci-dessous automatisent les deux vérifications dans `analyse.py`.

```
# Utilisation : liste de dictionnaires avec les clés event et user.
evenements = [
    {"event": "LOGIN_FAIL", "user": "admin"},
    {"event": "LOGIN_FAIL", "user": "admin"},
    {"event": "LOGIN_SUCCESS", "user": "admin"},
    {"event": "LOGIN_FAIL", "user": "tech01"},
]
assert compter_echecs(evenements) == 3
assert compter_echecs([]) == 0
```

✓ RÉPONSE À RETENIR

Quatre événements : 3 échecs. Liste vide : 0.

3. Analyse d’incident et durcissement des accès

Les journaux de SRV-APP montrent plusieurs échecs de connexion au compte admin depuis une même adresse IP, suivis d’une authentification réussie, puis d’une autre connexion réussie depuis une adresse interne. Il faut reconstituer les faits, proposer deux réglages SSH dans l’environnement de test et communiquer l’incident ainsi que les mesures de suivi.

Question 3.1. À partir des horodatages, des adresses IP et des comptes présents dans le DT 2, reconstituer la chronologie des événements. Indiquer les éléments qui justifient de signaler l’événement comme suspect et distinguer les faits observés de votre interprétation.

Faits observés : le 12/02/2026 à 08:14:02, 08:14:09 et 08:14:17, l’adresse 203.0.113.45 échoue trois fois avec le compte admin. À 08:16:31, cette même adresse obtient une connexion réussie avec ce compte. À 08:22:04, 192.168.20.35 se connecte avec le compte tech01. Les journaux sont présentés dans l’ordre chronologique et utilisent l’heure locale du site.

Interprétation : les échecs répétés suivis d’une réussite depuis la même adresse constituent un comportement suspect, potentiellement une compromission du compte admin. La connexion interne ultérieure est un événement distinct à vérifier, sans preuve qu’elle soit liée.

> **✓ RÉPONSE À RETENIR**
>
> Événement suspect : trois échecs du compte admin depuis 203.0.113.45, suivis d’une réussite depuis la même adresse à 08:16:31.

Question 3.2. Dans le fichier de configuration SSH de l’environnement de test, proposer et appliquer deux réglages adaptés pour réduire le risque d’accès non autorisé. Pour chaque réglage, indiquer brièvement l’effet recherché. Vérifier la syntaxe de la configuration avec l’outil disponible avant de proposer son rechargement.

Dans la configuration SSH du serveur de test, ajouter deux directives :

```
PermitRootLogin no
MaxAuthTries 3
```

La première interdit les connexions SSH directes au compte root ; la seconde limite le nombre de tentatives d’authentification par connexion. Vérifier que l’accès d’administration nécessaire reste possible, puis contrôler la syntaxe avec `sudo sshd -t`. Si le contrôle ne renvoie aucune erreur, le rechargement peut être proposé, par exemple avec `sudo systemctl reload ssh` ou le nom du service disponible dans l’environnement.

> **✓ RÉPONSE À RETENIR**
>
> Réglages : `PermitRootLogin no` et `MaxAuthTries 3`. Exécuter `sshd -t` sans erreur avant tout rechargement du service SSH.

Question 3.3. **Rédiger dans le compte rendu fourni un message professionnel de 5 à 8 lignes à destination du responsable informatique. Présenter l'incident suspect, citer au moins deux éléments observés dans les journaux, indiquer les mesures immédiates proposées et préciser une action de suivi. Ajouter une phrase en anglais technique demandant à un technicien distant de préserver les journaux et de ne pas supprimer les traces.**

Bonjour,
Le 12 février, SRV-APP a enregistré une activité suspecte sur le compte admin.
Trois échecs depuis 203.0.113.45 entre 08:14:02 et 08:14:17 ont été suivis d'une réussite à 08:16:31.
Je propose de désactiver l'accès SSH direct à root et de limiter à trois les tentatives par connexion.
Après contrôle syntaxique, appliquer ces réglages et vérifier l'accès d'administration autorisé.
Préserver les journaux, examiner l'activité du compte admin et contrôler les connexions ultérieures.
Please preserve the logs and do not delete or alter any traces.

> **✓ RÉPONSE À RETENIR**
>
> Compte rendu : signaler l'activité suspecte du compte admin, sécuriser SSH, préserver les journaux et vérifier les connexions ultérieures.

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

Bilan de l'épreuve : Cette sous-épreuve E32 du bac professionnel CIEL, session 2026, code 26-BCP-CIEL-E32, dure 3 heures et a un coefficient 3. Le cas de l'Atelier Logistique des Rives mobilise l'adressage et le routage, les requêtes SQL, le développement et les tests Python, puis l'analyse de journaux, le durcissement SSH et la communication professionnelle sur un incident suspect.

Notions-clés, formules & règles à maîtriser

- Pour un sous-réseau IPv4, l'adresse réseau s'obtient par application du masque ; l'adresse de diffusion met tous les bits hôte à 1.
- Un préfixe IPv6 /64 conserve les 64 premiers bits ; ici, le numéro du VLAN identifie le sous-réseau et la passerelle se termine par ::1.
- En SQL, relier site.id à equipement.site_id, filtrer actif = 1, regrouper par site et compter les équipements.
- Une route vers un réseau directement connecté utilise l'interface associée ; une route vers un réseau distant indique le prochain saut.

Points de vigilance & attentes du jury

- Vérifier le masque avant de calculer les adresses réseau, diffusion et première adresse utilisable.
- Respecter la convention IPv6 donnée et associer chaque préfixe et passerelle au bon VLAN.
- Respecter les noms de champs SQL et compter uniquement les événements dont event vaut exactement LOGIN_FAIL.
- Dans l'analyse d'incident, séparer faits et interprétations ; vérifier la syntaxe SSH avant de proposer un rechargement.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment calculer les adresses principales d'un sous-réseau IPv4 ?

Appliquez le masque à l'adresse IP pour obtenir l'adresse réseau. Pour l'adresse de diffusion, mettez tous les bits hôte à 1. La première adresse utilisable est généralement l'adresse réseau augmentée de 1.

Q : Comment construire la requête SQL pour compter les équipements actifs par site ?

Reliez equipement.site_id à site.id, filtrez les lignes où actif vaut 1, puis regroupez par site. Comptez les équipements de chaque groupe et triez les résultats sur le nom du site en ordre croissant.

Q : Comment organiser les trois heures de l'épreuve ?

Répartissez le temps selon les points attribués aux trois parties : 7, 6 et 7 points. Gardez une marge pour vérifier les calculs, compléter le DR 1, tester les fichiers demandés et relire le compte rendu.

Q : Que doit montrer une réponse solide sur l'incident et les réglages SSH ?

Présentez les événements datés et les données des journaux comme des faits, puis formulez séparément leur interprétation. Pour chaque réglage SSH, indiquez l'effet recherché et vérifiez la syntaxe avant de proposer le rechargement.

Sujet officiel associé (PDF) : https://coursbacprociel.fr/assets/annales/bac-pro-ciel/Valorisation de la donnée et cybersécurité/2026/Bac Pro CIEL - Valorisation de la donnée et cybersécurité - Session 2026 - 1-Sujet.pdf
Ressources Bac Pro CIEL : 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.