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 en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

BTS SIO

BTS Services informatiques aux organisations, option solutions d'infrastructure, systèmes et réseaux

Session 2026 • Code sujet : **26-BTS-SIO-E7** • Durée : **4 heures** • Coefficient : **4**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Segmentation réseau, adressage IPv4 et IPv6, routage (3 questions) **Page 3**

2. Analyse des traces d'authentification VPN et requête SQL (3 questions) **Page 5**

3. Traitement de l'incident et durcissement des accès (4 questions) **Page 7**

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

Sujet officiel (PDF) : https://coursbtssio.fr/assets/annales/bts-sio/E6 - Cybersécurité des services informatiques (spécifique à l'option)/2026/BTS SIO - E6 - Cybersécurité des services informatiques (spécifique à l'option) - Session 2026 - 1-Sujet.pdf

1. Segmentation réseau, adressage IPv4 et IPv6, routage

NORDALIM organise son réseau local en trois VLAN dédiés aux utilisateurs, aux serveurs et à l'administration. À partir de l'architecture et des capacités indiquées, il faut dimensionner les sous-réseaux, compléter les routes de SW-L3 et proposer les passerelles IPv6.

Question 1.1. Pour chacun des trois VLAN du DT 1, déterminez le plus petit préfixe IPv4 permettant d'accueillir le nombre minimal d'adresses indiqué, passerelle comprise. Complétez le DR 1 avec le préfixe, l'adresse réseau, l'adresse de diffusion et la passerelle, en utilisant des sous-réseaux distincts du bloc 10.20.0.0/24. (3 points)

La capacité demandée comprend la passerelle : il faut donc 50, 25 et 10 adresses utilisables. Les plus petits sous-réseaux adaptés sont /26, /27 et /28, qui offrent respectivement 62, 30 et 14 adresses utilisables. L'affectation ci-dessous utilise les premières plages disponibles du bloc 10.20.0.0/24. La première adresse utilisable de chaque plage est réservée à la passerelle.

VLAN	Préfixe	Adresse réseau	Adresse de diffusion	Passerelle
10	/26	10.20.0.0	10.20.0.63	10.20.0.1
20	/27	10.20.0.64	10.20.0.95	10.20.0.65
30	/28	10.20.0.96	10.20.0.111	10.20.0.97

DR 1 complété : plan d'adressage IPv4

VLAN	Nombre minimal d'adresses	Préfixe CIDR	Adresse réseau	Adresse de diffusion	Passerelle
10	50	/26	10.20.0.0	10.20.0.63	10.20.0.1
20	25	/27	10.20.0.64	10.20.0.95	10.20.0.65
30	10	/28	10.20.0.96	10.20.0.111	10.20.0.97

✓ RÉPONSE À RETENIR

VLAN 10 : 10.20.0.0/26, diffusion 10.20.0.63, passerelle 10.20.0.1. VLAN 20 : 10.20.0.64/27, diffusion 10.20.0.95, passerelle 10.20.0.65. VLAN 30 : 10.20.0.96/28, diffusion 10.20.0.111, passerelle 10.20.0.97.

Question 1.2. Complétez dans le DR 1 la table de routage du commutateur de couche 3 : indiquez les trois routes directement connectées correspondant aux VLAN et la route par défaut vers le pare-feu, avec les interfaces et l'adresse du pare-feu données dans le DT 1. (2 points)

Les trois réseaux des VLAN sont directement connectés aux interfaces virtuelles correspondantes de SW-L3. La route par défaut envoie le trafic sans route plus spécifique vers FW-01, joignable sur le réseau de transit 172.16.0.0/30. L'adresse de SW-L3 sur ce transit est 172.16.0.2/30 et celle du pare-feu est 172.16.0.1/30.

1. Destination 10.20.0.0/26 : directement connecté, VLAN 10.
2. Destination 10.20.0.64/27 : directement connecté, VLAN 20.

3. Destination 10.20.0.96/28 : directement connecté, VLAN 30.
4. Destination 0.0.0.0/0 : prochain saut 172.16.0.1, liaison vers FW-01.

DR 1 complété : routes de SW-L3

Destination	Préfixe	Prochain saut	Interface ou VLAN
10.20.0.0	/26	Directement connecté	VLAN 10
10.20.0.64	/27	Directement connecté	VLAN 20
10.20.0.96	/28	Directement connecté	VLAN 30
0.0.0.0	/0	172.16.0.1	Liaison vers FW-01

✓ RÉPONSE À RETENIR

Routes connectées : 10.20.0.0/26, 10.20.0.64/27 et 10.20.0.96/28. Route par défaut : 0.0.0.0/0 via 172.16.0.1.

Question 1.3. À partir du préfixe IPv6 attribué dans le DT 1, proposez un sous-réseau IPv6 /64 pour chacun des trois VLAN, en conservant le numéro de VLAN comme valeur du quatrième groupe hexadécimal. Indiquez également pour chaque VLAN l'adresse IPv6 de passerelle attendue, définie comme la première adresse du sous-réseau. (2 points)

Le préfixe /56 fixe les 56 premiers bits, soit les trois premiers groupes et les deux premiers chiffres hexadécimaux du quatrième groupe : 12. Pour former chaque /64, on conserve ce 12 et on ajoute l'identifiant du VLAN en hexadécimal dans les deux derniers chiffres du quatrième groupe : 10 devient 0a, 20 devient 14 et 30 devient 1e. La première adresse attribuée à la passerelle est ici l'adresse du sous-réseau suivie de ::1.

1. VLAN 10 : sous-réseau 2001:db8:4a10:120a::/64, passerelle 2001:db8:4a10:120a::1.
2. VLAN 20 : sous-réseau 2001:db8:4a10:1214::/64, passerelle 2001:db8:4a10:1214::1.
3. VLAN 30 : sous-réseau 2001:db8:4a10:121e::/64, passerelle 2001:db8:4a10:121e::1.

✓ RÉPONSE À RETENIR

Passerelles : VLAN 10, 2001:db8:4a10:120a::1 ; VLAN 20, 2001:db8:4a10:1214::1 ; VLAN 30, 2001:db8:4a10:121e::1.

2. Analyse des traces d'authentification VPN et requête SQL

Les journaux du VPN de NORDALIM recensent des authentifications refusées et acceptées, avec horodatages UTC et adresses IP sources. Il faut compter les refus sur une période définie, rédiger une requête SQL d'audit et distinguer les faits établis des éléments qui nécessitent des vérifications complémentaires.

Question 2.1. À partir des lignes du DT 2 comprises entre 08:00:00 inclus et 08:10:00 exclu le 12 mars 2026, comptez les événements dont le résultat est « REFUSE », regroupés par adresse IP source. Présentez le résultat pour chaque adresse IP présente dans l'extrait et identifiez celle qui atteint le seuil de cinq refus. (2 points)

La fenêtre étudiée va du 12 mars 2026 à 08:00:00 inclus au même jour à 08:10:00 exclu. On compte uniquement les lignes dont le résultat est « REFUSE », puis on les regroupe par adresse IP source.

Adresse IP source	Nombre de refus
203.0.113.77	6
198.51.100.24	2

Les six refus de 203.0.113.77 sont aux horaires 08:01:12, 08:02:04, 08:03:19, 08:05:33, 08:06:40 et 08:07:52. Les deux refus de 198.51.100.24 sont à 08:04:26 et 08:07:11. L'événement « ACCEPTE » est exclu du comptage. Seule 203.0.113.77 atteint le seuil demandé.

> ✓ **RÉPONSE À RETENIR**
>
> Sur la période étudiée, 203.0.113.77 totalise 6 refus et 198.51.100.24 en totalise 2. Le seuil de cinq refus est atteint par 203.0.113.77.

Question 2.2. Rédigez une requête SQL à partir de la table auth_event décrite dans le DT 2. Elle doit filtrer les dates et heures demandées, ne retenir que les événements « REFUSE », regrouper les résultats par adresse IP source et ne restituer que les adresses comptant au moins cinq refus. (2,5 points)

La borne basse est incluse avec « >= » et la borne haute est exclue avec « < ». Le filtre de date et d'heure limite les lignes au 12 mars 2026, de 08:00:00 à 08:10:00. Le filtre sur result élimine les événements acceptés. Le regroupement porte uniquement sur src_ip, puis HAVING applique le seuil après le comptage.

```
SELECT src_ip, COUNT(*) AS nombre_refus
FROM auth_event
WHERE event_time >= TIMESTAMP '2026-03-12 08:00:00'
  AND event_time < TIMESTAMP '2026-03-12 08:10:00'
  AND result = 'REFUSE'
GROUP BY src_ip
HAVING COUNT(*) >= 5;
```

> ✓ **RÉPONSE À RETENIR**
>
> La requête ne restitue que 203.0.113.77, avec 6 événements « REFUSE » dans la fenêtre demandée.

Question 2.3. **Expliquez ce que l'analyse des traces permet d'établir et ce qu'elle ne permet pas de conclure à elle seule, sachant qu'un événement « ACCEPTE » suit les refus pour le même compte et la même adresse IP. Citez deux vérifications complémentaires à effectuer pour déterminer si le compte ou des ressources internes ont été compromis. (1,5 point)**

Les traces établissent six refus puis une connexion VPN acceptée pour svc-backup depuis 203.0.113.77 à 08:08:41 UTC, sans second facteur. À 08:11:03, le même compte ouvre une session SMB vers FS-01. Cette succession rend probable un usage non autorisé du compte, mais ne prouve ni l'identité de l'auteur ni la consultation ou la copie de fichiers.

Deux vérifications complémentaires :

- Examiner les journaux d'accès et les événements de fichiers de FS-01 pour déterminer quelles ressources ont été consultées, modifiées ou copiées.
- Corréler les journaux VPN, système et réseau pour rechercher les actions du compte et d'éventuels accès inhabituels à d'autres ressources.

> **✓ RÉPONSE À RETENIR**
>
> La connexion VPN suivie d'un accès SMB rend probable l'usage indu du compte, sans établir la consultation ou la copie de données.

3. Traitement de l’incident et durcissement des accès

Les traces indiquent des échecs successifs de connexion au VPN, puis une authentification réussie du compte technique svc-backup sans second facteur et une session SMB vers FS-01. Il faut qualifier l’incident, proposer des mesures de confinement et de durcissement, préserver les éléments d’analyse et prendre en compte les données à caractère personnel.

Question 3.1. Reconstituez la chronologie des faits observables dans le DT 2. Qualifiez l’événement de sécurité le plus probable et indiquez les éléments disponibles qui justifient cette qualification. (2 points)

Le 12 mars 2026, l’adresse 203.0.113.77 provoque six refus VPN pour `svc-backup`, de 08:01:12 à 08:07:52 UTC. À 08:08:41, l’authentification VPN de ce compte est acceptée, sans second facteur. À 08:11:03, le compte ouvre une session SMB vers FS-01. Cette succession fait suspecter des tentatives de devinette du mot de passe suivies d’un accès frauduleux ou d’une compromission du compte. Les journaux ne prouvent ni l’identité de l’auteur ni la consultation ou la copie de fichiers.

> **✓ RÉPONSE À RETENIR**
>
> Suspicion de compromission de `svc-backup` : six refus VPN, puis une connexion acceptée et une session SMB vers FS-01.

Question 3.2. Présentez, dans un ordre cohérent, quatre mesures immédiates à prendre pour contenir l’incident et préserver les éléments nécessaires à son analyse. Pour chaque mesure, indiquez brièvement son objectif. (2 points)

1. Préserver les journaux VPN, FW-01 et FS-01 en conservant l’export d’origine en lecture seule et en documentant les copies : garantir leur intégrité pour l’analyse.
2. Révoquer la session VPN de `svc-backup`, désactiver temporairement le compte et renouveler son secret : empêcher une nouvelle connexion.
3. Bloquer la source suspecte et restreindre les accès VPN et SMB ; isoler FS-01 si le risque de propagation le justifie : limiter l’activité malveillante.
4. Examiner les copies des journaux et les traces de FS-01, puis corréler les événements : déterminer les actions réalisées et le périmètre touché.

> **✓ RÉPONSE À RETENIR**
>
> Préserver les journaux, neutraliser le compte, limiter les accès suspects et analyser FS-01.

Question 3.3. Proposez quatre mesures de durcissement des accès au VPN et aux serveurs, couvrant au minimum l’authentification, les privilèges et la surveillance. Reliez chaque mesure au risque qu’elle réduit. (2 points)

Quatre mesures réduisent les risques d’intrusion et de propagation :

- Exiger le MFA pour tout accès VPN et supprimer les exceptions : limite l’usage d’un mot de passe volé.

- Interdire l’accès VPN interactif aux comptes de service et gérer leurs secrets de façon sécurisée : réduit leur détournement.
- Appliquer le moindre privilège et limiter les flux VPN aux serveurs nécessaires : réduit l’impact d’un compte compromis.
- Centraliser et surveiller les journaux VPN et serveurs, avec alertes sur les échecs répétés et connexions atypiques : accélère la détection.

> **✓ RÉPONSE À RETENIR**
>
> MFA obligatoire, comptes de service non interactifs, privilèges et flux limités, surveillance centralisée.

Question 3.4. Si l’analyse établit que des données à caractère personnel ont été consultées ou copiées sans autorisation, indiquez deux actions à engager au titre de la protection des données et précisez à qui elles incombent dans l’entreprise. (1 point)

NORDALIM, en tant que responsable du traitement, doit notifier la CNIL dans les 72 heures après avoir pris connaissance de la violation, sauf si celle-ci est peu susceptible d’engendrer un risque pour les personnes. Si le risque est élevé, l’entreprise doit aussi informer les personnes concernées dans les meilleurs délais. La direction porte ces démarches au nom de l’entreprise ; le délégué à la protection des données conseille et accompagne, sans remplacer le responsable du traitement.

> **✓ RÉPONSE À RETENIR**
>
> NORDALIM notifie la CNIL sous 72 heures si le risque le justifie et informe les personnes si le risque est élevé ; le DPO accompagne ces démarches.

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

Bilan de l'épreuve : L'épreuve E7 de cybersécurité du BTS SIO option solutions d'infrastructure, systèmes et réseaux, session 2026, porte le code 26-BTS-SIO-E7. En quatre heures, coefficient 4, le candidat étudie le réseau et les traces d'incident de NORDALIM. Il mobilise l'adressage et le routage, l'analyse de journaux et SQL, la réponse à incident, le durcissement des accès et la protection des données personnelles.

Notions-clés, formules & règles à maîtriser

- Choisir le plus petit sous-réseau IPv4 dont les adresses attribuables couvrent les équipements requis, en réservant les adresses réseau et de diffusion.
- Une route par défaut utilise le préfixe 0.0.0.0/0 et l'adresse du routeur de sortie comme prochain saut.
- En SQL, filtrer les événements, regrouper par adresse source et utiliser HAVING pour appliquer un seuil au comptage.
- Une authentification acceptée suivie d'une session serveur constitue un indice d'incident, mais ne prouve pas à elle seule un accès aux fichiers.

Points de vigilance & attentes du jury

- Vérifier que chaque sous-réseau IPv4 est distinct, appartient au bloc demandé et couvre le besoin, passerelle comprise.
- Respecter les horodatages UTC et appliquer la borne de début incluse et la borne de fin exclue.
- Distinguer les faits consignés des hypothèses et préserver les journaux originaux en lecture seule.
- Relier chaque mesure de sécurité au risque traité et préciser les responsabilités relatives aux données personnelles.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment choisir le préfixe IPv4 minimal pour un VLAN ?

Comptez les adresses attribuables nécessaires, puis choisissez la plus petite taille de sous-réseau qui les couvre après réservation des adresses réseau et de diffusion. Le préfixe CIDR correspondant indique le nombre total d'adresses du sous-réseau.

Q : Comment construire les sous-réseaux IPv6 /64 à partir du préfixe attribué ?

Un préfixe /56 fixe les 56 premiers bits, dont le premier octet du quatrième groupe. Pour obtenir des /64 distincts, utilisez les bits restants du quatrième groupe comme identifiant de sous-réseau et faites apparaître le numéro VLAN selon la convention demandée.

Q : Comment gérer les quatre heures et le barème de l'épreuve ?

Le sujet répartit les points entre trois parties : 7 points pour le réseau, 6 pour les traces et SQL, et 7 pour le traitement de l'incident. Répartissez le temps entre elles et vérifiez que le DR 1 est rendu avec la copie.

Q : Qu'attend le jury pour justifier la qualification d'un incident ?

Appuyez la qualification sur une chronologie et des faits observables, comme les refus, l'authentification acceptée et la session SMB. Précisez ce que les journaux ne démontrent pas et proposez des vérifications complémentaires adaptées.

Sujet officiel associé (PDF) : https://coursbtssio.fr/assets/annales/bts-sio/E6 - Cybersécurité des services informatiques (spécifique à l'option)/2026/BTS SIO - E6 - Cybersécurité des services informatiques (spécifique à l'option) - Session 2026 - 1-Sujet.pdf
Ressources BTS Services Informatiques aux Organisations : 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.