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

BACHELOR UNIVERSITAIRE DE TECHNOLOGIE

RÉSEAUX ET TÉLÉCOMMUNICATIONS

ÉVALUATION DE COMPÉTENCE : C2, ASSISTER L'ADMINISTRATEUR DU RÉSEAU

SESSION 2026

Durée : 2 heures

SPÉCIALITÉ / UNITÉ	COEFF
RÉSEAUX ET TÉLÉCOMMUNICATIONS	3,0 INDICATIF

Moyens de calculs et matériel autorisés :

L'usage de calculatrice avec mode examen actif est autorisé. L'usage de calculatrice sans mémoire, « type collège », est autorisé.

Aucun document ou matériel autorisé en dehors de ceux fournis avec le sujet.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 8 pages numérotées de 1/8 à 8/8.

Les documents réponses en fin de sujet sont à rendre avec la copie.

DOSSIER SUJET

MISE EN SITUATION PROFESSIONNELLE ET CONSIGNES GÉNÉRALES : NOVALYS SERVICES, AGENCE DE LYON, RHÔNE

Novalys Services dispose d'un réseau local segmenté, d'un commutateur de niveau 3, d'un pare-feu, de postes clients et de serveurs hébergeant notamment une base de données de suivi des incidents. Vous assistez l'administratrice réseau lors d'une opération de diagnostic et de documentation.

Le référentiel national du BUT Réseaux et Télécommunications situe « Assister l'administrateur du réseau » au niveau 1 de la compétence « Administrer les réseaux et l'Internet ». Les modalités d'évaluation relèvent de l'établissement. Pour cette évaluation, la durée retenue est de 2 heures et le coefficient indicatif est de 3,0.

Les réponses doivent être justifiées lorsque cela est demandé. Les adresses IPv4 sont exprimées en notation décimale pointée et en préfixe CIDR. Les documents DT 1 et DT 2 sont à utiliser pour répondre. Complétez le document réponse DR 1 et rendez-le avec la copie.

PARTIE 1 : ARCHITECTURE, ADRESSAGE ET ROUTAGE (7 points)

Configuration de base du réseau local et identification d'un dysfonctionnement

À partir du DT 1, vous préparez l'ajout d'un réseau invité et vérifiez la cohérence du plan d'adressage et du routage. Le réseau invité doit pouvoir accueillir 24 postes clients simultanément, en plus de sa passerelle. Le bloc attribué à ce VLAN est 192.168.40.0/24.

1.1 (2 points) Déterminez le plus petit préfixe IPv4 permettant d'attribuer une adresse à 24 postes clients et à une passerelle. Donnez le masque décimal, l'adresse réseau, l'adresse de diffusion et la plage d'adresses utilisables du premier sous-réseau correspondant, en partant de 192.168.40.0.

1.2 (2 points) Le VLAN 20 utilise le préfixe IPv6 2001:db8:1200:20::/64 et la passerelle 2001:db8:1200:20::1. Un poste reçoit l'adresse 2001:db8:1200:20::25/64. Indiquez si le poste appartient au sous-réseau de la passerelle et justifiez. Donnez également l'adresse de réseau IPv6 correspondant à ce poste.

1.3 (1,5 point) Complétez dans le DR 1 les routes directement connectées du commutateur de niveau 3 pour les VLAN 10, 20, 30 et 40, ainsi que sa route par défaut vers le pare-feu. Pour le VLAN 40, utilisez le sous-réseau calculé à la question 1.1 et la première adresse utilisable comme passerelle.

1.4 (1,5 point) Un poste du VLAN 20 peut joindre sa passerelle mais ne peut pas joindre 192.168.30.10, serveur du VLAN 30. En vous appuyant sur le DT 1, citez deux vérifications pertinentes à effectuer sur le commutateur ou le poste client avant de conclure à une panne du serveur. Pour chacune, précisez le résultat attendu.

PARTIE 2 : EXPLOITATION DES DONNÉES ET AUTOMATISATION (6 points)

Interrogation d'une base relationnelle et traitement élémentaire de journaux

La base de données de suivi contient les tables **Devices** et **Incidents** décrites dans le DT 2. Les dates sont stockées au format ISO 8601. Les requêtes demandées doivent fonctionner sur les données décrites, sans modifier le contenu de la base.

2.1 (2,5 points) Écrivez une requête SQL qui affiche, pour chaque incident de priorité « haute » encore ouvert, son identifiant, sa date, le nom de l'équipement concerné et sa localisation. Utilisez une jointure entre les deux tables et triez le résultat de la date la plus récente à la plus ancienne.

2.2 (1,5 point) Écrivez une requête SQL qui donne, pour chaque équipement, le nombre total d'incidents enregistrés, y compris les équipements qui n'ont aucun incident. Le résultat doit afficher le nom de l'équipement et le nombre d'incidents, puis être trié par nombre décroissant.

2.3 (2 points) Le DT 2 contient un extrait de journal système. Proposez une commande Bash utilisant **grep** pour afficher uniquement les lignes comportant le marqueur **AUTH_FAIL**, puis une commande permettant de compter ces lignes. Indiquez le nombre de lignes correspondant à ce marqueur dans l'extrait fourni.

PARTIE 3 : DIAGNOSTIC DE SÉCURITÉ ET MESURES DE DURCISSEMENT (7 points)

Analyse de journaux, signalement d'incident et sécurisation des accès

Une alerte signale des échecs répétés d'authentification sur un serveur. Vous analysez les événements du DT 2 avant de rédiger un signalement à l'administratrice réseau. Toute conclusion doit être appuyée par un élément observable dans les journaux ou les configurations fournis.

3.1 (2,5 points) Relevez dans l'extrait de journal les éléments qui permettent de caractériser l'incident : service visé, adresse IP source, nombre d'échecs observés et période concernée. Présentez ces éléments sous forme d'un signalement synthétique.

3.2 (2 points) Le journal indique que les tentatives proviennent d'une adresse qui n'apparaît pas dans le plan d'adressage interne. Expliquez pourquoi cette observation ne suffit pas, à elle seule, à démontrer que l'adresse est malveillante. Citez deux vérifications à effectuer pour confirmer l'origine et l'impact des tentatives.

3.3 (2,5 points) Proposez trois mesures de durcissement adaptées à la situation, dont au moins une mesure sur le compte ou l'authentification et une mesure sur l'exposition réseau du service. Pour chaque mesure, indiquez le risque qu'elle réduit et veillez à ne pas préconiser une action susceptible de couper sans contrôle l'accès d'administration légitime.

DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

DT 1 : TOPOLOGIE ET PLAN D'ADRESSAGE DU SITE DE LYON

Le commutateur de niveau 3 SW-L3 assure le routage inter-VLAN. Il est relié au pare-feu FW-01 par un lien de transit. Le pare-feu assure l'accès à Internet. Les interfaces de passerelle des VLAN sont configurées sur SW-L3. Les postes des VLAN 10 et 20 obtiennent leur configuration IPv4 par DHCP. Les serveurs du VLAN 30 utilisent des adresses statiques.

Le lien entre SW-L3 et SW-ACC1 transporte les VLAN 10, 20, 30 et 40 en 802.1Q. Les ports d'accès des postes sont configurés dans le VLAN correspondant à leur service.

Topologie logique et liaisons

Équipement ou liaison	Rôle ou extrémités	Informations utiles
FW-01	Pare-feu et accès Internet	Interface de transit : 192.168.254.1/30
SW-L3	Commutateur de niveau 3	Interface de transit : 192.168.254.2/30
FW-01 vers SW-L3	Lien de transit routé	Réseau 192.168.254.0/30
SW-L3 vers SW-ACC1	Lien de commutation 802.1Q	VLAN 10, 20, 30 et 40 autorisés
SW-ACC1	Commutateur d'accès des postes	Ports utilisateurs configurés en mode accès
VLAN 10	Administration	192.168.10.0/24 ; passerelle 192.168.10.1
VLAN 20	Utilisateurs	192.168.20.0/24 ; passerelle 192.168.20.1
VLAN 30	Serveurs	192.168.30.0/24 ; passerelle 192.168.30.1
VLAN 40	Invités	Bloc disponible 192.168.40.0/24 ; passerelle à définir

Inventaire des équipements et des liaisons du site

Extraits de configuration et de routage

Équipement	Extrait
SW-L3	ip routing activé ; VLAN 10 : 192.168.10.1/24 ; VLAN 20 : 192.168.20.1/24 ; VLAN 30 : 192.168.30.1/24
SW-L3	Route statique : 0.0.0.0/0 via 192.168.254.1
FW-01	Route vers les réseaux internes via 192.168.254.2
SW-L3 vers SW-ACC1	Trunk 802.1Q ; VLAN 10, 20 et 30 autorisés
Poste VLAN 20	IPv4 : 192.168.20.45/24 ; passerelle : 192.168.20.1 ; DNS : 192.168.30.53
Serveur applicatif	IPv4 : 192.168.30.10/24 ; passerelle : 192.168.30.1
VLAN 20 en IPv6	Préfixe : 2001:db8:1200:20::/64 ; passerelle : 2001:db8:1200:20::1

État relevé lors du diagnostic

DT 2 : BASE DE SUIVI DES INCIDENTS ET EXTRAIT DE JOURNAL SYSTÈME

La base est relationnelle. La clé primaire de **Devices** est **device_id**. La clé primaire de **Incidents** est **incident_id**. Le champ **Incidents.device_id** référence **Devices.device_id**. Les valeurs possibles de **status** sont « ouvert » et « clos ».

Extrait du journal de sécurité de **srv-auth-01**, le 18 juin 2026, heure locale du site :

Table Devices

device_id	name	location
1	SW-L3	Baie réseau
2	SW-ACC1	Bureau utilisateurs
3	srv-auth-01	VLAN serveurs
4	srv-app-01	VLAN serveurs

Extrait complet des équipements concernés

Table Incidents

incident_id	device_id	created_at	priority	status	description
501	3	2026-06-18 08:42:00	haute	ouvert	Échecs d'authentification SSH
502	2	2026-06-18 08:10:00	moyenne	clos	Perte temporaire de lien
503	4	2026-06-17 16:25:00	haute	ouvert	Service applicatif indisponible
504	1	2026-06-16 11:05:00	basse	clos	Port inutilisé à vérifier

Extrait complet des incidents enregistrés

Extrait du journal de sécurité

Horodatage	Source	Message
2026-06-18 08:41:12	203.0.113.77	sshd[4102]: AUTH_FAIL user=admin
2026-06-18 08:41:35	203.0.113.77	sshd[4110]: AUTH_FAIL user=admin
2026-06-18 08:42:01	203.0.113.77	sshd[4118]: AUTH_FAIL user=admin
2026-06-18 08:43:16	198.51.100.24	sshd[4126]: AUTH_OK user=netadmin
2026-06-18 08:44:03	203.0.113.77	sshd[4134]: AUTH_FAIL user=admin
2026-06-18 08:45:10	203.0.113.77	sshd[4142]: AUTH_FAIL user=admin

Les lignes sont présentées dans l'ordre chronologique

NE RIEN ÉCRIRE DANS CETTE PARTIE

DR 1 : Tableau de routage à compléter, questions 1.1 et 1.3 — **À RENDRE AVEC LA COPIE**

Complétez les cellules contenant « ... ». Pour les routes directement connectées, indiquez l'interface logique ou le VLAN de sortie. Pour la route par défaut, indiquez le prochain saut.

Plan d'adressage du VLAN 40

Élément	Valeur
Préfixe CIDR	.....
Masque décimal	.....
Adresse réseau	.....
Adresse de diffusion	.....
Plage d'adresses utilisables	.....

À compléter à la question 1.1

Table de routage de SW-L3

Destination	Type de route	Prochain saut ou interface de sortie
192.168.10.0/24	Directement connectée	.....
192.168.20.0/24	Directement connectée	.....
192.168.30.0/24	Directement connectée	.....
.....	Directement connectée	.....
0.0.0.0/0	Route par défaut	.....

Routes attendues après ajout du VLAN 40

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

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.