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 LA COMPÉTENCE C3 : ADMINISTRER LES RÉSEAUX ET L'INTERNET, NIVEAU 2

SESSION 2026

Durée : 2 h 30

SPÉCIALITÉ / UNITÉ	COEFF
RÉSEAUX ET TÉLÉCOMMUNICATIONS	3,0 (PONDÉRATION INDICATIVE LOCALE)

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 MÉDICAL, SITE PRINCIPAL DE LYON ET AGENCE DE GRENOBLE

Novalys Médical conçoit et distribue des équipements de santé. Son système d'information comprend un réseau local segmenté en VLAN, des serveurs hébergés sur le site de Lyon, une base de données de gestion des incidents et des services hébergés dans un cloud privé. L'agence de Grenoble est reliée au site principal par un réseau opérateur.

Vous intervenez comme technicien(ne) réseaux au sein de l'équipe infrastructure. Il vous est demandé de préparer une évolution du plan d'adressage, de vérifier le routage et les requêtes de suivi d'incidents, puis d'analyser une alerte de sécurité et de proposer des mesures de durcissement.

Le programme national du BUT R&T organise l'évaluation des compétences en contrôle continu intégral. Les indications de durée et de pondération figurant sur ce sujet correspondent aux modalités de cette évaluation. Le présent sujet porte sur la compétence « Administrer les réseaux et l'Internet », niveau 2.

Les documents DT 1 et DT 2 fournissent les données nécessaires. Les réponses sont à rédiger sur la copie et dans les documents réponse lorsque cela est demandé. Toute hypothèse ajoutée doit être explicitement justifiée.

PARTIE 1 : Architecture réseau, adressage et routage (7 points)

Plan d'adressage IPv4 et IPv6, VLAN et routage dynamique

La direction souhaite créer un plan d'adressage cohérent pour les réseaux internes de Lyon et pour le lien intersite. Les besoins en hôtes, les VLAN et la topologie sont fournis dans le DT 1. Pour les sous-réseaux IPv4 ordinaires, une adresse est réservée à l'identifiant réseau et une à la diffusion. Les passerelles doivent utiliser la première adresse hôte disponible de chaque sous-réseau.

Besoins en adressage et paramètres de segmentation

Réseau	VLAN	Nombre maximal d'hôtes	Préfixe IPv6 attribué
Utilisateurs	20	60	2001:db8:24:20::/64
Serveurs	30	50	2001:db8:24:30::/64
Administration	10	25	2001:db8:24:10::/64
Invités	40	12	2001:db8:24:40::/64
Lien Lyon-Grenoble	Sans objet	2 interfaces	2001:db8:24:ff::/64

Données à utiliser pour les questions 1.1 à 1.3, d'après le DT 1.

1.1 (2,5 points) À partir du bloc IPv4 **10.24.0.0/24**, dimensionner les cinq sous-réseaux du tableau du plus grand besoin au plus petit. Pour chacun, donner le préfixe CIDR, le masque décimal, l'adresse réseau, la première et la dernière adresse utilisables ainsi que l'adresse de diffusion. Affecter les sous-réseaux successivement à partir de la plus petite adresse disponible, sans chevauchement.

1.2 (1,5 point) Pour les VLAN 20, 30, 10 et 40, indiquer l'adresse IPv4 de passerelle selon la règle donnée et proposer l'adresse IPv6 de passerelle **::1** dans chaque préfixe attribué. Indiquer également le préfixe IPv6 utilisé pour le lien Lyon-Grenoble et les deux adresses d'interface choisies dans ce préfixe.

1.3 (1,5 point) Le commutateur cœur **SW-LYO** assure le routage inter-VLAN. Préciser les informations nécessaires sur un port d'accès destiné à un poste du VLAN 20 et sur le lien trunk entre SW-LYO et le pare-feu FW-LYO. Indiquer les VLAN autorisés sur ce trunk et expliquer pourquoi le VLAN de gestion ne doit pas être confondu avec le VLAN des utilisateurs.

1.4 (1,5 point) Le routage entre les équipements de couche 3 est assuré par OSPF, aire 0. À partir du DT 1, compléter dans le DR 1 la table de routage de SW-LYO pour le réseau de Grenoble et la route par défaut. Indiquer le prochain saut de chaque route et expliquer brièvement comment le réseau de Grenoble est appris par OSPF.

PARTIE 2 : Exploitation de la base de données des incidents (6 points)

Lecture de schéma relationnel et rédaction de requêtes SQL

Le service informatique suit les incidents dans une base relationnelle. Le schéma, les contraintes et un extrait des données sont fournis dans le DT 2. Les requêtes demandées doivent être écrites en SQL standard. Les colonnes de résultat doivent porter les alias demandés. Aucun résultat hors des données présentes dans l'extrait ne doit être supposé.

Schéma relationnel de suivi des incidents

Table	Colonnes et contraintes
equipement	id INT PRIMARY KEY; nom VARCHAR(40); site VARCHAR(20); vlan INT
incident	id INT PRIMARY KEY; equipement_id INT; date_heure TIMESTAMP; severite VARCHAR(10); statut VARCHAR(12); description VARCHAR(120)

Extrait du DT 2. La clé étrangère incident.equipement_id référence equipement.id.

2.1 (2 points) Écrire une requête SQL qui affiche, pour chaque incident de sévérité **HAUTE** encore au statut **OUVERT**, l'identifiant de l'incident, sa date et heure, le nom de l'équipement et son site. La requête doit utiliser une jointure entre les deux tables et trier les résultats du plus récent au plus ancien.

2.2 (2,5 points) Écrire une requête SQL qui donne, pour chaque site, le nombre d'incidents de sévérité **HAUTE** enregistrés dans l'extrait du DT 2. Le résultat doit contenir les colonnes **site** et **nb_incidents_haute**. Inclure également les sites pour lesquels ce nombre est nul et trier le résultat par nom de site. Compléter la requête dans le DR 1.

2.3 (1,5 point) À partir des lignes fournies dans le DT 2, indiquer le nombre d'incidents ouverts de sévérité HAUTE au site de Lyon. Justifier le résultat par les filtres appliqués aux tables **incident** et **equipement**.

PARTIE 3 : Analyse d'incident et durcissement de la sécurité (7 points)

Analyse de journaux, diagnostic réseau et mesures de sécurité

Le centre de supervision a détecté une activité inhabituelle sur le serveur de fichiers FS-LYO. Les extraits de journaux système, de pare-feu et de capture réseau figurent dans le DT 2. Les horodatages sont exprimés en heure locale synchronisée par NTP. Les adresses IP concernées sont celles indiquées dans les documents techniques.

Éléments de la capture réseau

Heure	Source	Destination	Protocole ou port	Information observée
09:14:02	10.24.0.131	10.24.0.66	TCP/22	SYN
09:14:02	10.24.0.131	10.24.0.66	TCP/22	SYN retransmis
09:15:11	10.24.0.131	10.24.0.66	TCP/445	SYN
09:15:11	10.24.0.131	10.24.0.66	TCP/445	RST, ACK en réponse

Extrait de capture réalisé sur le VLAN serveurs, d'après le DT 2.

3.1 (2 points) En vous appuyant sur les événements syslog et les paquets de la capture, reconstituer la chronologie de l'incident en trois étapes au minimum. Identifier l'équipement source, le serveur visé, les services sollicités et les éléments qui permettent de qualifier l'activité d'anormale.

3.2 (2 points) La capture montre un SYN vers TCP/22 sans réponse visible, puis une tentative vers TCP/445 suivie d'un RST, ACK. Expliquer ce que permettent de conclure ces observations et préciser une limite de l'analyse d'une capture réalisée sur un seul point du réseau.

3.3 (1,5 point) Proposer une règle de filtrage qui autorise l'administration SSH du serveur FS-LYO uniquement depuis le poste d'administration **10.24.0.130**, tout en interdisant aux postes utilisateurs l'accès SSH et SMB aux serveurs. Indiquer les adresses, les protocoles ou ports et l'ordre logique des règles. Le pare-feu applique une politique implicite de refus.

3.4 (1,5 point) Formuler trois mesures complémentaires de durcissement adaptées à l'incident. Les propositions doivent couvrir au moins deux domaines parmi la gestion des comptes, la journalisation et la supervision, le cloisonnement réseau, la sécurisation des postes et la réponse à incident. Pour chaque mesure, préciser brièvement le risque qu'elle réduit.

DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

DT 1 : TOPOLOGIE, PLAN D'ADRESSAGE ET PARAMÈTRES DE ROUTAGE

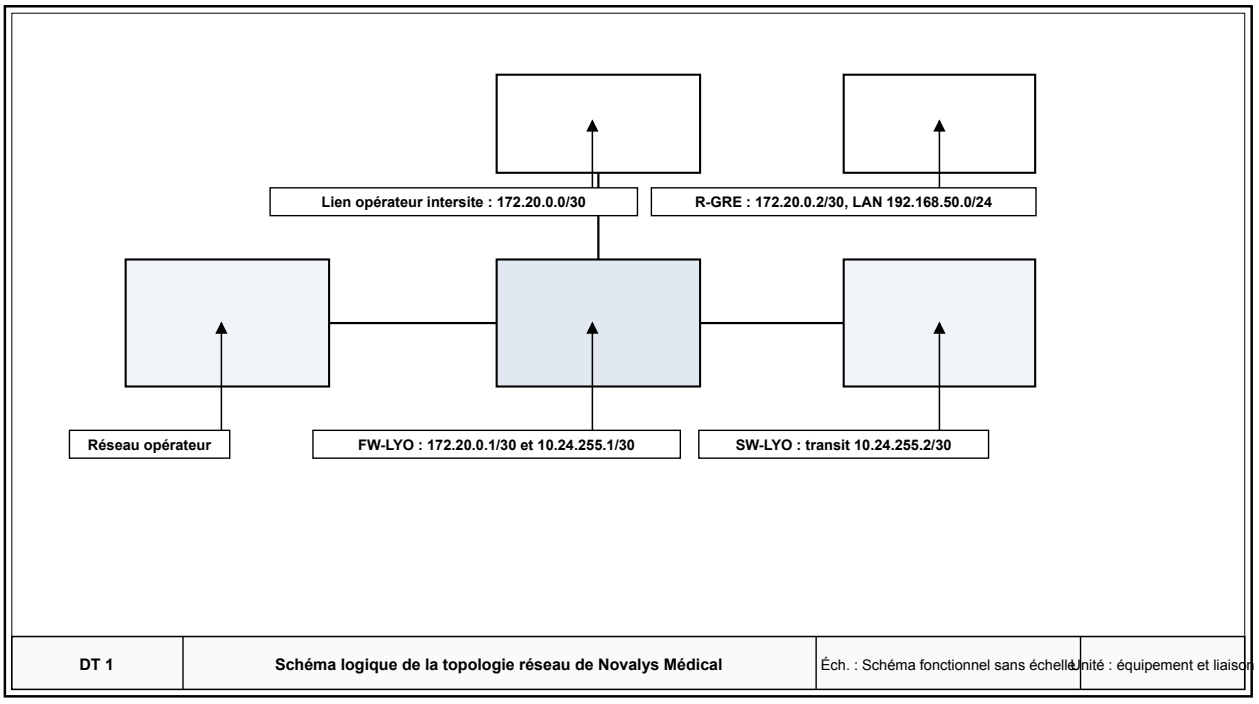
Topologie. Le site de Lyon comprend un pare-feu FW-LYO relié au réseau opérateur, un commutateur cœur de couche 3 SW-LYO et des commutateurs d'accès. Le site de Grenoble comprend le routeur R-GRE et un réseau local. Le lien opérateur entre les sites utilise le réseau IPv4 **172.20.0.0/30** : FW-LYO possède l'adresse **172.20.0.1/30** et R-GRE l'adresse **172.20.0.2/30**. Le lien de transit entre FW-LYO et SW-LYO utilise **10.24.255.0/30** : FW-LYO est en **10.24.255.1/30** et SW-LYO en **10.24.255.2/30**.

Réseaux IPv4 existants hors du nouveau plan à dimensionner. Le réseau de Grenoble est **192.168.50.0/24**, passerelle **192.168.50.1**, annoncée par R-GRE dans OSPF. Le bloc réservé au nouveau plan interne de Lyon est **10.24.0.0/24**. Les besoins en hôtes et les VLAN sont indiqués dans la partie 1. Les préfixes IPv6 des VLAN et du lien intersite sont également fournis dans cette partie.

Routage. SW-LYO et R-GRE participent à OSPF, aire 0. FW-LYO relaie le trafic entre le réseau opérateur et le transit de Lyon, mais n'annonce pas le réseau de Grenoble dans OSPF. SW-LYO utilise FW-LYO comme prochain saut pour sa route par défaut. Pour les questions, le coût OSPF du chemin vers Grenoble est le plus faible par le lien SW-LYO, FW-LYO puis le réseau opérateur. La route par défaut est configurée sur SW-LYO avec le prochain saut **10.24.255.1**.

VLAN. VLAN 10 : administration; VLAN 20 : utilisateurs; VLAN 30 : serveurs; VLAN 40 : invités. Le trunk entre SW-LYO et FW-LYO doit transporter les VLAN 10, 20, 30 et 40. Le VLAN de gestion des équipements est le VLAN 10. Le bloc IPv4 destiné au nouveau plan ne comprend pas les réseaux de transit décrits ci-dessus.

Pour un sous-réseau IPv4 ordinaire de préfixe /p, le nombre total d'adresses est égal à 2^{32-p}. Pour le dimensionnement demandé, réserver l'adresse réseau et l'adresse de diffusion.



Réseaux internes de Lyon à créer

VLAN	Fonction	Nombre maximal d'hôtes	Bloc IPv6
20	Utilisateurs	60	2001:db8:24:20::/64
30	Serveurs	50	2001:db8:24:30::/64
10	Administration	25	2001:db8:24:10::/64
40	Invités	12	2001:db8:24:40::/64
Sans objet	Lien Lyon-Grenoble à adresser dans le bloc réservé	2 interfaces	2001:db8:24:ff::/64

DT 2 : EXTRAITS DE LA BASE DE DONNÉES ET JOURNAUX D'INCIDENT

Schéma relationnel. La table **equipement** contient les colonnes **id** (clé primaire), **nom**, **site** et **vlan**. La table **incident** contient les colonnes **id** (clé primaire), **equipement_id** (clé étrangère vers equipement.id), **date_heure**, **severite**, **statut** et **description**. Les valeurs de site sont « Lyon » et « Grenoble »; les valeurs de severite sont « HAUTE », « MOYENNE » et « BASSE »; les valeurs de statut sont « OUVERT » et « CLOS ».

Extrait syslog et pare-feu. Les journaux sont horodatés le 12 mars 2026 et les adresses sont en IPv4. Le poste d'administration autorisé est **10.24.0.130**. Le poste concerné est **10.24.0.131**. Le serveur de fichiers FS-LYO est **10.24.0.66**. La politique du pare-feu est un refus implicite si aucune règle d'autorisation ne correspond.

Extrait des équipements

id	nom	site	vlan
1	FS-LYO	Lyon	30
2	DB-LYO	Lyon	30
3	PC-ADM-01	Lyon	10
4	PC-USER-17	Lyon	20
5	FW-LYO	Lyon	10
6	FS-GRE	Grenoble	30

Extrait des incidents

id	equipement_id	date_heure	severite	statut	description
501	1	2026-03-12 09:14:02	HAUTE	OUVERT	Tentatives de connexion SSH
502	1	2026-03-12 09:15:11	HAUTE	OUVERT	Tentative SMB refusée
503	2	2026-03-12 08:52:30	MOYENNE	OUVERT	Latence base de données
504	4	2026-03-12 09:18:20	BASSE	CLOS	Échec de connexion au partage
505	6	2026-03-12 09:20:05	HAUTE	OUVERT	Compte de service verrouillé
506	1	2026-03-12 09:32:40	HAUTE	CLOS	Analyse antivirus terminée

Extrait syslog et journal du pare-feu

Heure	Source	Équipement ou service	Événement
09:14:02	10.24.0.131	FS-LYO	sshd : plusieurs tentatives de connexion avec des comptes différents
09:14:19	10.24.0.131	FS-LYO	sshd : authentification refusée, compte inexistant
09:15:11	10.24.0.131	FW-LYO	Connexion TCP vers 10.24.0.66:445 refusée par la règle inter-VLAN
09:16:03	10.24.0.131	SW-LYO	Port d’accès du VLAN 20 actif; adresse MAC non répertoriée dans l’inventaire du poste
09:19:44	10.24.0.131	Serveur de supervision	Alerte : hausse du nombre de connexions vers les serveurs du VLAN 30

Extrait de capture réseau

Heure	Source	Destination	Protocole ou port	Information observée
09:14:02	10.24.0.131	10.24.0.66	TCP/22	SYN
09:14:02	10.24.0.131	10.24.0.66	TCP/22	SYN retransmis, aucune réponse visible dans l’extrait
09:15:11	10.24.0.131	10.24.0.66	TCP/445	SYN
09:15:11	10.24.0.66	10.24.0.131	TCP/445	RST, ACK

NE RIEN ÉCRIRE DANS CETTE PARTIE

DR 1 : Document réponse à rendre avec la copie : questions 1.4 et 2.2 **À RENDRE AVEC LA COPIE**

Compléter directement les tableaux ci-dessous. Pour la question 1.4, indiquer le préfixe de destination, la source d'apprentissage ou le type de route et le prochain saut. Pour la question 2.2, compléter la requête SQL en respectant les alias et le tri demandés.

Table de routage de SW-LYO à compléter

Destination	Type ou source de la route	Prochain saut	Interface de sortie
192.168.50.0/24	.....	.....	Lien de transit vers FW-LYO
0.0.0.0/0	.....	.....	Lien de transit vers FW-LYO

Requête SQL de comptage des incidents de sévérité HAUTE par site

Requête à compléter
SELECT e.site, ... AS nb_incidents_haute
FROM equipement AS e ...
.....
.....

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.