Programme de cours
Expertise Dépannage TCP/IP : Diagnostic de Performance et Analyse de Flux Hybrides (Système vs Infrastructure)

Durée :	5 jours soit 35 heures	Référence :	IF-TCPIPDEP2

Public visé :

- Administrateurs systèmes et réseaux
- Ingénieurs support / production / exploitation
- Techniciens réseau expérimentés
- Consultants IT

Pré-requis :

- Maîtriser les fondamentaux TCP/IP (adressage, routage, VLAN…)
- Avoir une expérience pratique des environnements réseau
- Connaissances de base en systèmes (Windows/Linux) recommandées

Objectifs pédagogiques :

À l'issue de la formation, le participant sera capable de :

- **Appliquer** une méthodologie structurée de dépannage multi-couches
- **Identifier** l'origine d'un incident entre réseau, système et applicatif
- **Analyser** des flux réseau et des indicateurs de performance
- **Corréler** des événements issus de différentes sources (logs, métriques, traces)
- **Diagnostiquer** des incidents dans des architectures hybrides (On-Prem / Cloud)

Compétences acquises à l'issue de la formation :

- Diagnostiquer un incident réseau complexe multi-couches
- Isoler une cause racine dans un environnement hybride
- Utiliser les outils avancés d'analyse réseau et système
- Interpréter des captures et métriques de performance
- Structurer une démarche de troubleshooting reproductible

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :
Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr
Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.
Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- AGEFIPH
- FIPHFP
- MDPH de votre département

Programme de cours
Expertise Dépannage TCP/IP : Diagnostic de Performance et Analyse de Flux Hybrides (Système vs Infrastructure)

Description / Contenu

Module 1 : Rappels essentiels & vision moderne du dépannage

- Modèles OSI et TCP/IP (lecture orientée troubleshooting)
- Typologie des incidents (latence, perte, jitter, saturation…)
- Méthodologie structurée (top-down, bottom-up, divide & conquer)
- Notion de **baseline** et d'indicateurs normaux
- Introduction à la notion de **cause racine (Root Cause Analysis)**

TP

- Analyse de scénarios simples de panne (cartographie des symptômes)
- Mise en place d'une baseline réseau simple

Module 2 : Outils modernes de diagnostic (réseau & système)

- Outils OS : ping, traceroute, netstat, ss, iperf
- Analyse de paquets : Wireshark (approche méthodologique)
- Logs systèmes (Linux / Windows)
- SNMP, NetFlow, sFlow
- Introduction à l'**observabilité** (logs, métriques, traces)

TP

- Capture et analyse de flux (latence TCP, retransmissions)
- Analyse croisée : logs système + trafic réseau

Module 3 : Dépannage couche 2 / couche 3 avancé

- VLAN, trunk, STP (boucles, convergence)
- Problèmes de broadcast et tempêtes réseau
- Routage (OSPF, BGP) : erreurs classiques
- NAT, asymétrie de routage
- MTU, fragmentation

TP

- Diagnostic d'une boucle STP
- Analyse d'un problème de routage asymétrique
- Résolution d'un problème MTU

Module 4 : Dépannage des services réseau & dépendances système

- DNS, DHCP : pannes fréquentes
- Résolution de noms et impacts applicatifs
- Interaction client / serveur
- Dépendances réseau ↔ système (ports, sockets, firewall OS)

TP

- Diagnostic d'un problème DNS impactant une application
- Analyse d'un défaut DHCP en environnement multi-VLAN

Module 5 : Dépannage des performances & analyse fine TCP

- Fonctionnement TCP (fenêtre, retransmissions, congestion)
- Analyse de la latence applicative
- QoS et priorisation
- Identification des goulots d'étranglement

TP

- Analyse Wireshark d'un problème de lenteur applicative
- Identification d'un problème de congestion TCP

Module 6 : Dépannage en environnement hybride (On-Prem / Cloud)

- Architectures hybrides (VPN, interco cloud)
- Problèmes typiques (latence, DNS, routage cloud)
- Notions IaaS / PaaS / SaaS (impacts troubleshooting)
- Responsabilités partagées (client vs fournisseur cloud)

TP

- Simulation d'un accès applicatif dégradé via VPN
- Diagnostic d'un problème DNS dans un environnement hybride

Module 7 : Corrélation réseau / système / applicatif

- Méthode pour distinguer :
  - problème réseau
  - problème système
  - problème applicatif
- Corrélation multi-sources :
  - logs applicatifs
  - métriques système
  - flux réseau
- Introduction aux outils APM (Application Performance Monitoring)

TP

- Étude de cas complet : lenteur applicative → identifier si origine réseau ou serveur
- Analyse croisée logs + trafic + CPU

Module 8 : Sécurité & incidents réseau

- ACL, firewall, filtrage
- Détection d'anomalies réseau
- Notions IDS/IPS
- Impact sécurité sur les performances

TP

- Diagnostic d'un blocage lié à une ACL
- Identification d'un trafic suspect

Module 9 : Atelier global de troubleshooting (fil rouge)

- Scénarios réalistes multi-couches
- Approche méthodologique complète
- Travail en équipe (mode NOC / support)

TP

- Diagnostic complet d'une architecture :
- VLAN + routage + DNS + application
- Restitution + justification des choix

Note relative au programme : *Les travaux pratiques et scénarios de dépannage mentionnés sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation constante avec les réalités du marché — notamment l'hybridation des infrastructures (Cloud/On-premise), l'interdépendance des couches Systèmes/Réseaux et l'évolution des outils de Baseline — le contenu pédagogique ainsi que les environnements de TP sont susceptibles d'être ajustés ou mis à jour en fonction des évolutions technologiques.*