

Rapport – Incident Général

IG-2025-01-28-001

Début de l'incident : 28/01/2025 à 15h28

Fin de l'incident : 28/01/2025 à 20h30

Résumé de l'incident

Service(s) impacté(s) : Téléphonie IP et services SIP / Webex

Impact Client : Plus d'appels entrants / sortants

Cause : Kernel Oops / Défaut logiciel de routage

Déroulement

Date	Heure	Description
28/01/2025	15h28	Remontées d'alertes anormalement élevées sur plusieurs machines VOIP chez notre fournisseur
28/01/2025	15h30	Ouverture d'un ticket Opérateur chez notre fournisseur
28/01/2025	15h32	Les techniciens NOC commencent à traiter l'incident et premiers appels Clients pour signaler l'incident
28/01/2025	15h35	L'incident est escaladé auprès des équipes VOIP, une cellule de crise est montée avec notre fournisseur
28/01/2025	15h35	Les équipes de notre fournisseur étudient des remontées d'alertes sur un taux anormal d'appels par machine générant une saturation de notre plaque VOIP.
28/01/2025	15h35	Nos trunks d'interconnexion vers nos transitaires sont également saturés et nous observons des appels en anomalie rejetés en code SIP erreur 500
28/01/2025	15h40	Confirmation du NOC : tous nos autres services sont fonctionnels : DATA / Mobile / hébergement / transit / VISIP. La partie réseau est mise hors de cause.
28/01/2025	15h40	Nos indicateurs ne permettent pas d'identifier la cause des rejets des appels, une étude de l'ensemble des briques de la plaque voix est lancée. Toute l'équipe infra VOIP de notre fournisseur arrive en renfort.
28/01/2025	15h42	Les équipes étudient les dernières actions de provisionning de trunk afin de rechercher une anomalie. Cette piste sera refermée à 18h30
28/01/2025	16h00 – 17h30	L'ensemble des contrôles sur les proxys SIP ont été réalisés, aucun changement d'état n'est constaté, ils sont donc mis hors de cause. Le contrôle des médias gateways est réalisé, le trafic constaté est élevé (les appels sont rejoués de multiples fois automatiquement) mais cohérent avec l'incident en cours.

		Le service M.A.N (mécanisme d'authentification de numéros) ne présente pas de défaut, il est écarté des investigations. Par précaution, un ticket a été ouvert chez notre transitaire principal
28/01/2025	18h00	Les services en charge du routage sont identifiés comme étant potentiellement à l'origine du défaut, le redémarrage des machines a commencé.
28/01/2025	19h00	Fin de redémarrage des machines qui ne permet pas un retour au fonctionnement nominal.
28/01/2025	19h30	Détection d'une trace « Kernel défaut » (Kernel Oops)
28/01/2025	19h30	Isolation du châssis en défaut. Isolation de plaque VOIP de l'extérieur afin d'abaisser la charge du trafic de manière à pouvoir retrouver un fonctionnement normal.
28/01/2025	19h55	Retour à la normal du service, les appels entrants / sortants refonctionnent. Nos équipes poursuivent les vérifications
28/01/2025	20h30	L'incident est résolu, fin des opérations

Analyse Post-Incident

Le default Kernel Oops logiciel sur une des machines de routage a perturbé l'intégrité du système sans pour autant la rendre visible en anomalie sur la supervision. Lors de la vérification initiale, nos équipes n'ont pas détectées le défaut. L'expertise des logs liés au service n'ont pas permis d'identifier l'incident ; ce n'est que lors d'une étude approfondie des logs Kernel que l'anomalie a été confirmée.

A date, la supervision surveille les matériels, les services, les logs applicatifs mais le défaut reflète un manque de surveillance des logs Kernel. Ceci explique le délai anormalement long de résolution de l'incident.

La problématique du Kernel Oops est issue de montées en versions logicielles en lien avec la mise en place de M.A.N. Une mise à jour est planifiée cette nuit, le 29/01 sans impact client.

À la suite de l'incident du 10/12 nous avons mandaté un cabinet externe avec une forte expérience en réseaux télécoms pour réaliser un audit approfondi de nos infrastructures et de nos processus. Cet audit est en cours. Cette démarche s'inscrit dans notre engagement à tirer les enseignements nécessaires et à renforcer la résilience et la performance de notre réseau. Nous vous partagerons les conclusions et les plans d'actions associés.



SAS ITELIA
1361 Route de Bagnols
30290 Laudun L'Ardoise

Notre NOC évolue avec l'intégration de l'analyse avancée des logs Kernel. Grâce à une corrélation approfondie des événements réseaux et systèmes, nous renforcerons notre capacité à détecter les anomalies en amont, à anticiper les dégradations de service et à optimiser la remédiation des incidents.

Soyez assurés de notre engagement total à offrir un service de qualité. Nous restons à votre disposition pour toutes questions ou clarifications.