support@itelia.fr 04 66 90 55 90

SAS ITELIA
1361 Route de Bagnols
30290 Laudun L'Ardoise

Rapport – Incident Général
IG-2024-12-10-001

Début de l'incident : 10/12/2024 à 14:58	**Fin de l'incident : 10/12/2024 à 23:30**

Résumé de l'incident

Service(s) impacté(s) : Trunk SIP (Téléphonie IP) / Liens Internet / Solutions 4G avec IP Fixe

Impact Client : Plus d'accès total aux services ci-dessus

Cause : Erreur humaine chez notre fournisseur

Déroulement

Date	Heure	Description
10/12/2024	14h58	Remontées d'alertes anormalement élevées sur tout notre réseau.
10/12/2024	15h05	Ouverture d'un ticket Opérateur chez notre fournisseur
10/12/2024	15h08	Une cellule de crise est montée en interne et chez notre fournisseur, mobilisant l'ensemble des services techniques.
10/12/2024	15h15	Nous réalisons des vérifications sur différentes machines afin de poser un premier diagnostic.
10/12/2024	15h30	Les premières investigations de notre fournisseur indiquent que certaines machines en POP et Routeurs intégrateurs sont fonctionnelles.
10/12/2024	15h40	À la suite des différents retours des équipes, nous orientons nos investigations vers notre coeur en fabric IP.
10/12/2024	15h50	Nous n'observons aucune coupure physique et réseau entre les différents équipements de routage de notre infrastructure de type Fabric IP.
10/12/2024	16h00	Des alertes d'insuffisance mémoires sont identifiées sur les routeurs satellites de notre fournisseur Une première tentative de désengorgement d'apprentissage révèle un délai de retour fonctionnel trop long. (Leaf).
10/12/2024	16h15	Le nombre de routes BGP qui apparaissent sur les équipements de notre fournisseur sont très anormalement élevées. Un défaut de filtrage des routes est identifié en amont et corrigé.
10/12/2024	16h30	Une première tentative de désengorgement d'apprentissage révèle un délai de retour fonctionnel trop long.
10/12/2024	16h40	Un test de **shutdown logiciel** permet de réduire le délai de rétablissement.
10/12/2024	16h50	Cette dernière solution est ensuite validée, notre fournisseur procède au déploiement de la solution. Cette méthode a été généralisée sur environ 50 routeurs, machine par machine.

10/12/2024	17h00	Le déploiement de la solution sur les premières baies de notre fournisseur permet de remonter des services.
10/12/2024	17h10	La solution est déployée sur l'ensemble des baies, certains de nos services Data sont remontés en dégradé (ADSL / FTTH Orange, FTTB Altitude Covage Axione) 70 % des services sont de nouveau fonctionnels.
10/12/2024	17h30	Des incohérences dans les clusters de routeurs intégrateurs virtuels sont détectés, nécessitant une vérification et un rééquilibrage communautaire.
10/12/2024	17h35	Une partie du parc ADSL Orange remonte. Une équipe prend en charge la vérification de l'ensemble de nos troncs collectes DATA. Les administrateurs VOIP poursuivent le contrôle et la remise en conformité de la plaque VOIP
10/12/2024	18h05	90% des collectes DATA sont rétablies.
10/12/2024	18h30	50% du rééquilibrage communautaire sur le cluster de routeurs intégrateurs est réalisé.
10/12/2024	19h15	L'ensemble de la plaque VOIP, le SI et des services adjacents ont été contrôlés, le service est nominal.
10/12/2024	21h00	L'ensemble des collectes DATA sont fonctionnelles, un défaut subsiste sur une porte de collecte Axione. L'équilibrage communautaire sur le cluster de routeurs intégrateurs est terminé. Le service est nominal.
10/12/2024	23h30	Le défaut sur la collecte Axione est corrigé ainsi que différentes anomalies sur certaines VISP.

Analyse Post-Incident

Une enquête interne a été lancée chez notre fournisseur
Les premiers éléments confirment qu'il ne s'agit pas d'un acte de malveillance. Cependant, deux manquements ont été identifiés :

Non-respect du processus CAB (Change Advisory Board)
Absence de prévenances AD HOC pour ce type d'opération.

Afin d'éviter la reproduction d'un tel incident, notre fournisseur prévoit :

- Une évaluation de la chaîne managériale
- Une revue immédiate des processus internes, accompagnée d'un renforcement des contrôles d'accès aux machines cœurs de réseau.

De notre côté, nous allons lancer les actions suivantes :

- Réflexion sur la séparation des Backups 4G chez un autre fournisseur