

# MOOC Supervision de Réseaux et Services

Transcription Interview 2  
Cyril Delaballe et Shifteh Salehi, Orange  
Equipe Supervision de Services

Bonjour, Cyril Delaballe, responsable de la supervision des services. Bonjour, Shifteh Salehi, je suis responsable opérationnelle de la supervision de services.

## Présentation de l'équipe

Par supervision des services, on entend la supervision des services de tous nos clients grand public et pro, comme l'Internet, la télévision, le mail, le mobile, le banking. Tous les services d'Orange. Cette salle à Paris fonctionne 24 heures sur 24, 7 jours sur 7. Elle est managée par huit responsables opérationnels de supervision (ROS) et des équipes de superviseurs. En tout, ils sont une quarantaine. Il y a deux types de supervision : (1) une supervision plus technique, où on supervise les équipements. Les équipements du coeur de réseau mobile, et aussi les plateformes de services. Et (2) une supervision des services, qui est une supervision de bout en bout où on regarde le fonctionnement de nos services, tel que le perçoivent nos clients. Par exemple, si je prends le cas d'un incident télévision. Une incidence sur la télévision peut avoir différentes origines. Ça peut être le diffuseur, ça peut être sur notre plateforme de la télévision, ça peut être depuis le décodeur. Nous regardons le service tel que le perçoit le client.

## Objectifs de la supervision

Le rôle de la supervision des services d'Orange France est de superviser tous les services qu'Orange France propose à ses clients sur tous les domaines : Voix sur IP, Internet, Mobile et la TV. On classe les différentes classes de services : service premium, standard et light. En fait, on classe les services en terme d'importance pour nos clients. Par exemple, pour une chaîne TV, une chaîne à forte audience pour nos clients est considérée comme un service premium, qui est supervisé 24 heures sur 24. Les services standard sont supervisés en heures ouvrables, de 8h à 18 h, ou 20 h. Les services light sont supervisés via nos partenaires externes ou via la remontée des plateaux clients. Nous avons différents moyens de détection des incidents chez nous. Le principal est via un système d'alarmes. Les alarmes sont remontées via les robots et les sondes. Les robots sont les serveurs qui simulent l'utilisation d'un service par le client. Par exemple, le robot teste une chaîne TV toute la journée, comme les chaînes principales, les chaînes de live. S'il tombe sur un écran noir, une absence de son, ou une image figée, il nous remonte une alarme. Les sondes sont les scripts qui analysent l'efficacité du trafic en temps réel. Sur un dépassement de seuil, ils remontent une alarme. Par exemple, nous avons des sondes qui sont installées directement dans les box des clients et qui nous remontent une alarme sur une efficacité faible ou nulle. Le deuxième moyen de détection des incidents pour nous, c'est grâce à notre support niveau 3. En fait, ce sont les cas compliqués et complexes des clients qui n'ont pas pu être résolus par le support niveau 1 et niveau 2, qui sont remontés au niveau 3. Le niveau 3 effectue une corrélation entre les différentes signalisations unitaires des clients et nous envoie une suspicion d'incidents collectifs. Nous pouvons également superviser les services via nos

partenaires externes. Notre diffuseur télé peut nous envoyer une notification d'incidents sur une anomalie sur sa chaîne. Nous pouvons également recevoir des tickets par la DRCGP, la direction de la relation client grand public ou par les réseaux sociaux. Finalement, peu importe les moyens de détection des incidents, la première étape pour nous consiste à les reproduire. Ici dans la salle, on a tous les bancs de tests nécessaires pour effectuer un test vue client. On peut se mettre dans la peau réellement de nos clients. Nous avons par exemple pour la télévision les différents accès télé. Nous avons les différentes box ADSL, fibre, accès satellite. Nous avons les différents forfaits mobiles. Nous avons les smartphones, les téléphones plus anciens pour effectuer un test pour le service mobile. Nous avons les différents accès pour effectuer un test webmail ou un test web. Le rôle ici dans la supervision est qu'une fois qu'on a détecté l'incident, le superviseur effectue un test au service. Il faut qu'il constate le problème parce que tout simplement le robot peut se tromper. Par exemple, le robot peut prendre une image figée pour une image fixe, et nous remonter une alarme. Dans ce cas, le superviseur effectue le test. Si l'incident est avéré, on ouvre un ticket. On active les différents pôles concernés. On informe en parallèle le carrefour de l'information, qui gère la communication de l'information vers le management, vers le plateau client, mais également vers les abonnés et les exploitants qui gèrent les équipements. Ensuite, nous sommes le pilote de rétablissement de l'incident. C'est à dire que tant que l'incident n'est pas résolu, on ne clôt pas le ticket, car nous avons les moyens de vérifier le retour de service chez nous.

## Méthodes et outils

Nous avons deux outils principaux de supervision. Le premier est l'outil de supervision des services. C'est un outil via lequel on peut remarquer une interruption ou une perturbation de service. Toutes les alarmes sur nos outils sont liées à une fiche consignes dans laquelle est indiquée le processus spécifique de test demandé, mais également les différents pôles concernés. Le superviseur suit cette fiche, effectue son test. Si l'incident est avéré, il informe le pôle concerné. Sauf que dans certains cas, une fois qu'on active le pôle concerné, aucune anomalie n'est remarquée par le pôle. Dans ce cas, la valeur ajoutée est que nous avons accès à une chaîne de soutien qui est accessible par tous, via laquelle on peut voir, pour un service donné, tous les pôles et toutes les équipes concernées par un service. Dans ce cas, si le premier pôle ne voit aucune anomalie sur ses équipements, on active d'autres pôles. On peut ouvrir un pont technique pour ramener tous ces pôles et discuter entre eux. Ensuite, tout est tracé dans une fiche dans une fiche de suivi, qui est une sorte de mains courantes. Comme l'équipe travaille en 3x8, il est important de tracer tout en détails, pour que l'équipe qui remplace l'équipe précédente puisse avoir accès en détails à tout ce qui s'est passé avant. Ensuite, on devient le pilote de rétablissement de l'incident. Dans une journée très chargée où on a beaucoup d'alarmes, le ROS peut être amené à prioriser les différents incidents, donc via notre référentiel, comme nous avons les incidents relatifs aux services premium, standard et light, on peut prioriser la résolution d'un tel incident par rapport à par rapport à d'autres. On peut également escalader vers les différents services, afin de connaître quel est le dysfonctionnement, puis mettre en ligne l'information. Le deuxième moyen de superviser, chez nous, est un outil de supervision technique, qu'on appelle TMC. Toutes les alarmes qu'on reçoit sur cet outil sont également liées à une fiche consignes. L'activité sur ces études est assez simple. Ce sont les alarmes sur un dysfonctionnement logiciel ou matériel, comme par exemple, on peut avoir une alarme

sur un disque dur qui est plein, le fichier de logs qui est plein, ou le CPU qui est à 100%. Dans ce cas, sur cet outil, on crée un ticket via un outil de ticketing. D'ailleurs, pour toutes les alarmes, nous utilisons le même outil de ticketing, un outil commun de ticketing chez Orange, qui est disponible pour toutes les équipes chez Orange. On crée un ticket, puis on active le pôle. Comme sur certaines alarmes, dans cet outil, l'activité est assez simple, nous avons un mécanisme d'automatisation. On enregistre les alarmes, ensuite un ticket est créé automatiquement, et est envoyé vers le pôle. L'identifiant de l'équipe concernée est tagué sur ce ticket, puis le ticket est envoyé. Cela nous permet de ne pas perdre de temps pour nos superviseurs, et de se consacrer à d'autres incidents plus urgents.

## Métiers liés

Il y a deux types de métiers. (1) Les métiers temps réel. Dans les métiers temps réel, il y a le responsable opérationnel de supervision (ROS), qui est le manager opérationnel de la salle de supervision. Il suit l'activité de ses superviseurs. En cas d'incidents très graves, il peut procéder à une escalade. Il est là en soutien puisque tout n'est pas obligatoirement bien processé. Il est là en soutien à ses superviseurs. Le deuxième métier temps réel, ce sont les superviseurs, qui sont là pour prendre en compte les alarmes et déclencher les bons intervenants. Et, on a un troisième rôle, qui est l'incident management, donc une équipe dédiée en heures ouvrées au rétablissement des incidents, et en heures non ouvrées, ce sont les ROS qui reprennent ce rôle-là, et puis, il y a une deuxième catégorie de métiers, pour faire fonctionner cette supervision, ce sont (2) les métiers non temps réel. Ce sont les responsables performances supervision, qui sont là pour faire le lien entre la salle temps réel et le reste de l'entreprise. Quand on constate un dysfonctionnement dans nos outils, dans nos fiches consignes, dans la salle temps réel, c'est remonté à ces responsables performances supervision, qui vont le prendre en compte et le traiter avec les différentes personnes, les exploitants externes. Il y a aussi un autre métier, qui est la partie outils, on va dire les soutiens outils, pour faire fonctionner cette salle de supervision on a besoin de beaucoup d'outils, que ce soit pour nos bancs de test, mais aussi nos outils d'alarmer, la configuration de ces outils. Le dernier intervenant, ce sont les exploitants, donc les experts niveau 2 et niveau 3, qu'on peut déclencher suite à la détection d'une alarme.

## Autres

Un autre partenaire, ce sont toutes les autres supervisions. On peut être amené à contacter, selon la nature de l'incident, la supervision des réseaux, la supervision des infrastructures, ou même nos collègues du système d'information.