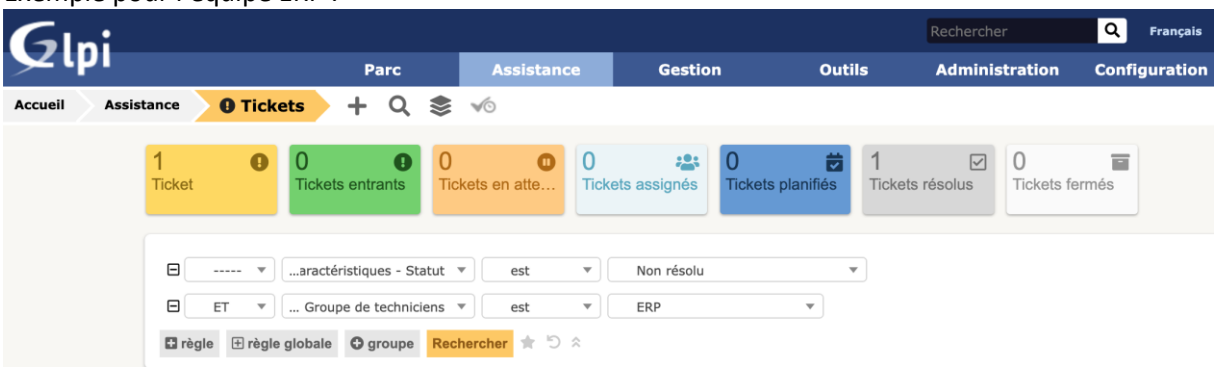
GLPI : simulation gestion d'incidents/demandes

Utilisation des filtres pour une équipe

L'équipe « Service Desk » est l'équipe de première ligne, qui traite tous les tickets qui arrivent des utilisateurs.
Ses membres voient donc tous les tickets d'incident « Non-résolu » et non-attribué à un groupe ou un technicien.

Les autres équipes doivent, elles, voir uniquement les tickets non résolus qui leur sont attribués.
Pour cela, elles utilisent les filtres, dans le menu Assistance Tickets, afin de ne voir que les tickets dont le statut est « non résolu » et « Attribué à – Groupe de techniciens » est égal à leur équipe.
Exemple pour l'équipe ERP :



Urgence, impact et priorité

Un utilisateur, lorsqu'il créé de lui-même un ticket d'incident, va indiquer l'urgence de son problème.
Par défaut, le ticket est créé avec un impact « Moyen ».
C'est le rôle de l'équipe « Service Desk » d'ajuster le niveau de d'urgence après avoir échangé avec l'utilisateur et de calibrer le bon niveau d'impact.
Ainsi, le niveau de « Priorité » est automatiquement calculé et permet de prioriser les tickets les uns par rapport aux autres.

Revoir le document-cours sur ITIL, partie « Gestions d'incident ».

Simulation de la gestion d'incident

Par groupe de 3, utiliser l'application GLPI d'une des personnes du groupe

Maintenant que GLPI est installé et paramétré pour votre organisation GSB, vous allez simuler ensemble les scénarios de gestion d'incident décrits ci-dessous :

Scénario 1 :

Un utilisateur, alors connecté chez lui sur sa box avec son PC professionnel, a cliqué sur une pièce jointe reçue dans un email de phishing (hammeçonnage). Son PC a alors été « crypto-verrouillé » avec une demande de rançon affichée sur sa page de login.

De retour au bureau, il ouvre un ticket d'incident (depuis le PC d'un collègue) pour faire part de son problème et le qualifié de très urgent.

Le Service Desk analyse la situation, ajuste le niveau d'urgence à « moyenne » (ça n'est qu'un utilisateur impacté) et décide du niveau d'impact (« haut »), et escalade le ticket à l'équipe RSSI.

Un expert en sécurité rappelle l'utilisateur et valide avec lui que le PC n'a pas été connecté au réseau après la « contamination » par ce ransomware. Il informe l'utilisateur qu'il ne doit en aucun cas brancher son PC à un réseau, et que celui-ci sera réinstallé par l'équipe « Postes Clients ».
Le ticket est escaladé à l'équipe « Postes Clients », qui prend contact avec l'utilisateur pour organiser la récupération et la réinstallation du PC.
Une fois la réinstallation effectuée, l'équipe informe l'utilisateur de la mise à disposition de son nouveau PC et clos l'incident.

Scénario 2 :

Un utilisateur rencontre le problème suivant : il n'arrive pas à se connecter à une application web « RH-2028 » en cours de développement, afin de faire les quelques tests que l'équipe projet lui a demandé de faire.
Ce n'est pas très urgent ni critique, mais il est bloqué.
Il ouvre un ticket d'incident sans changer le niveau d'urgence par défaut.

L'équipe Service Desk le rappelle et valide avec lui la reproductibilité du problème. L'urgence est ajustée à « haute » et l'impact à «très haut » vu les pertes potentielles de chiffre d'affaire. Sans solution dans la base de connaissance, le ticket est escaladé à l'équipe « Web Apps ».

L'équipe « Web Apps » analyse le problème, et observe que c'est le serveur d'authentification qui n'est pas joignable. Le ticket est escaladé à l'équipe « Systèmes et Réseaux ».

Le ticket est pris en charge et après analyse, le technicien décide de redémarrer le service d'authentification sur le serveur LDAP. Après quelques vérifications, il considère que ce service technique est de nouveau opérationnel.

Il renvoie le ticket à l'équipe « Web Apps » qui valide que la connexion à l'application web « RH-2028 » est fonctionnelle et clos le ticket.