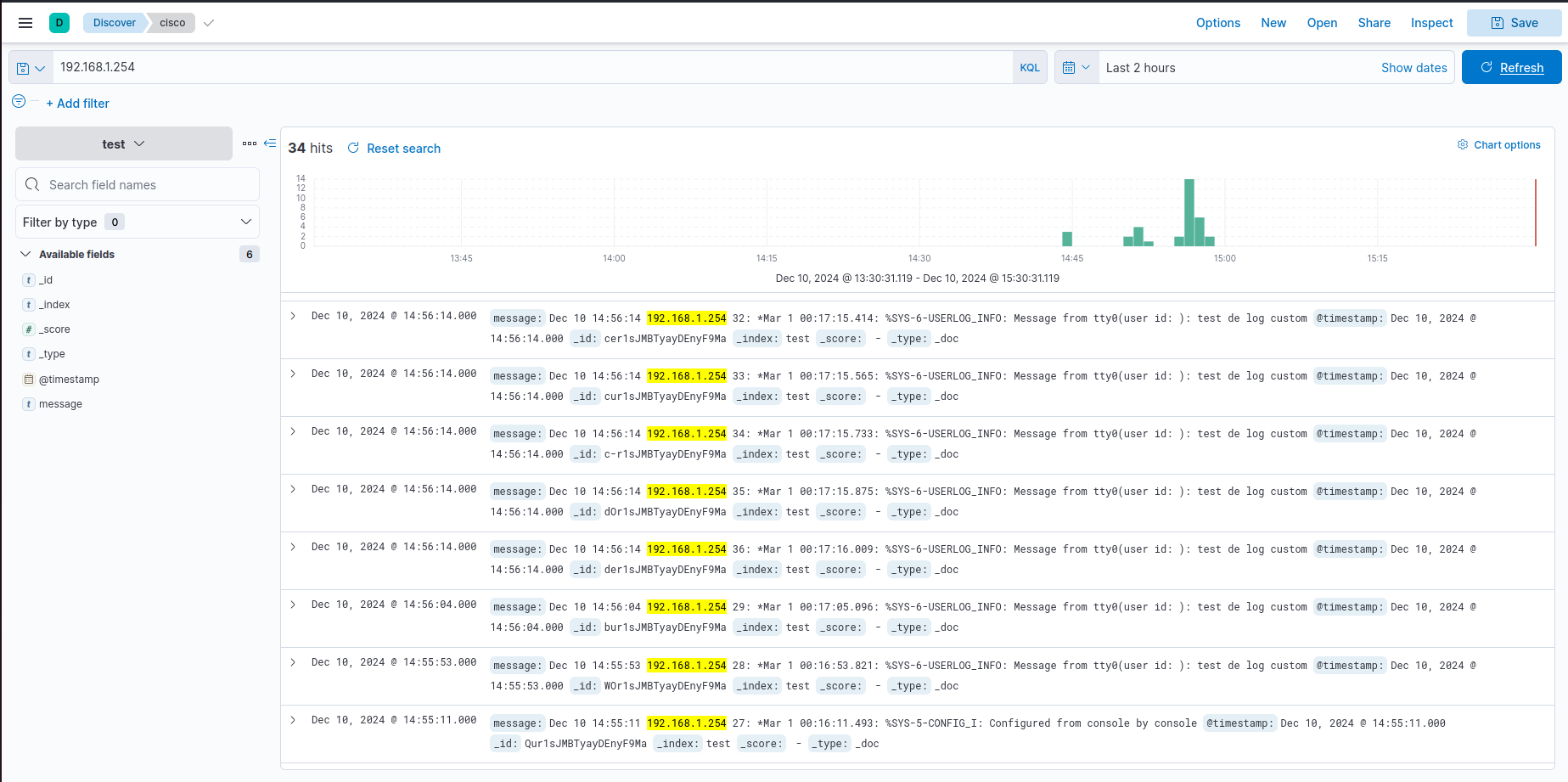
Analyse cisco



### **Résumé des types de logs :**

1. **%SYS-5-RELOAD** :
   1. Description : redémarrage de l'équipement, exécuté via la console.
   2. Exemple : Dec 10 14:58:10.000 - Reload requested by console.
2. **%SYS-5-CONFIG\_I** :
   1. Description : Modifications de la configuration effectuées via la console.
   2. Exemple : Dec 10 14:58:01.000 - Configured from console by console.
3. **%LINK-3-UPDOWN** et **%LINEPROTO-5-UPDOWN** :
   1. Description : Changements d'état des interfaces (FastEthernet).
   2. Exemples :
      1. Dec 10 14:57:39.000 - Interface FastEthernet0/2, changed state to up.
      2. Dec 10 14:51:32.000 - Interface FastEthernet0/3, changed state to down.
4. **%SYS-6-USERLOG\_INFO** :
   1. Description : Logs personnalisés générés depuis l'interface utilisateur (tty0).
   2. Exemple : test de log custom.
5. **%SYS-6-LOGGINGHOST\_STARTSTOP** :
   1. Description : Activation des logs envoyés à un serveur distant.
   2. Exemple : Logging to host 192.168.1.100 port 514 started.

### **Analyse détaillée :**

1. **Événements critiques :**
   1. Un redémarrage manuel est visible (%SYS-5-RELOAD) à **14:58:10**, probablement pour appliquer des modifications ou corriger une anomalie.
2. **Changements fréquents d'état des interfaces :**
   1. L'interface FastEthernet0/2 oscille entre les états **UP** et **DOWN** plusieurs fois en l'espace d'une minute (entre 14:57:34 et 14:57:39). Cela pourrait indiquer :
      1. Une instabilité réseau.
      2. Des tests effectués sur cette interface.
   2. L'interface FastEthernet0/3 passe en **DOWN** à **14:51:32** après avoir été en **UP**, ce qui pourrait signaler un problème ou une désactivation manuelle.
3. **Logs utilisateur personnalisés :**
   1. Plusieurs logs identiques contenant test de log custom ont été enregistrés à **14:56:16**, afin de tester la fonctionnalité de journalisation. Ces messages ne semblent pas critiques.
4. **Connexion à un serveur de logs distant :**
   1. Un serveur de journalisation a été configuré (192.168.1.100) à **14:44:08**, ce qui pourrait indiquer une centralisation des journaux pour un suivi ou une analyse à long terme.