

SAE 5.Cyber.03 - R5.Cyber.11

Supervision d'une Machine Ubuntu

Flavien Marchand

Sommaire

Sommaire	1
AuditBeat	2
Les informations sur les machines connectées	3
Les informations sur les connexions	4
Les informations sur les utilisateurs	5
Les informations sur les processus	5
Les informations sur les sockets	6
Les informations sur les paquets	7

AuditBeat

Grâce à Auditbeat nous avons dans le Dashboard Elastic les différents dashboards.

Dashboards

Search...

Recently updated ▾

Tags ▾

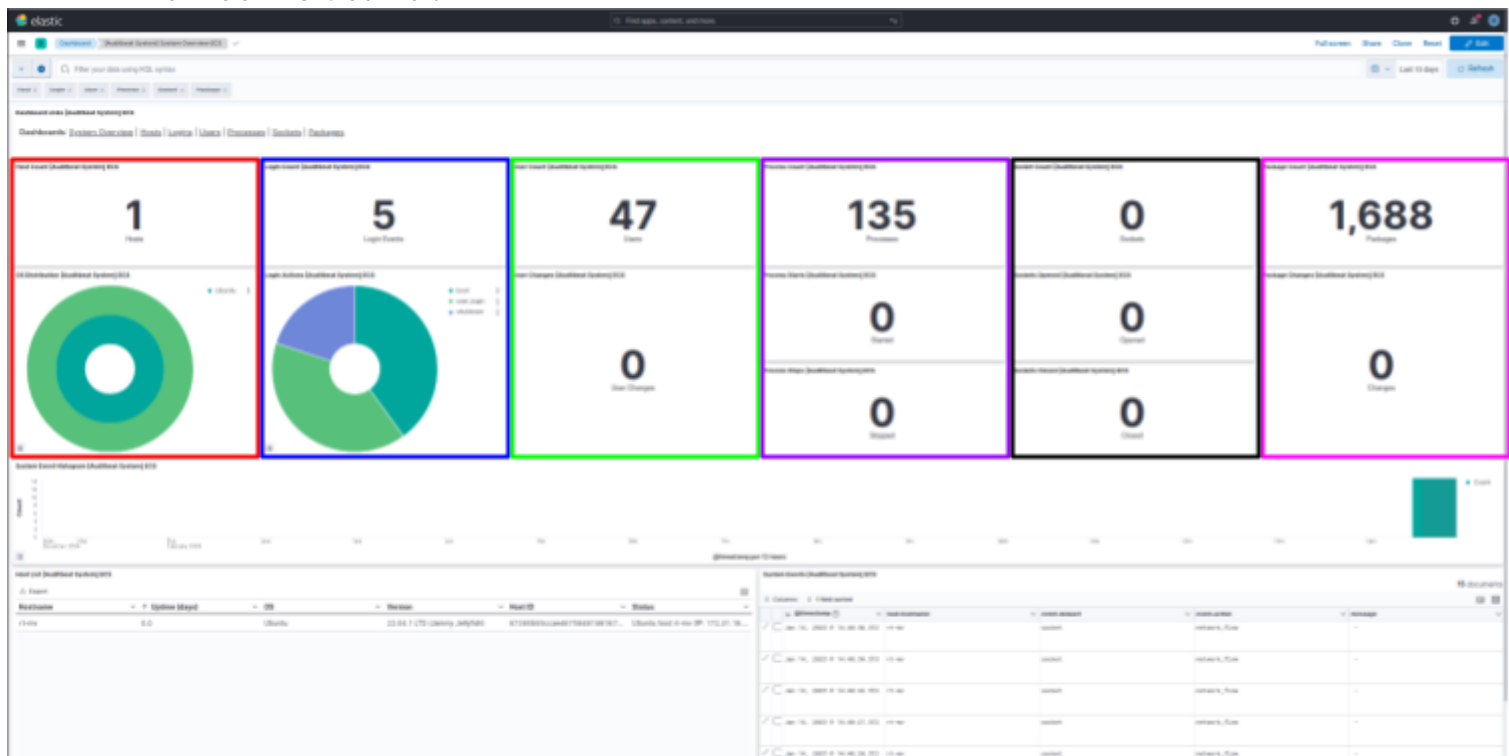
Create dashboard

☐ Name, description, tags	Last updated ▾	Actions
☐ [Auditbeat System] Host Dashboard ECS System Hosts	22 minutes ago	✎
☐ [Auditbeat Auditd] Overview ECS Summary of Linux kernel audit events.	22 minutes ago	✎ 🔍
☐ [Auditbeat System] User Dashboard ECS System Users	22 minutes ago	✎ 🔍
☐ [Auditbeat File Integrity] Overview ECS Monitor file integrity events.	22 minutes ago	✎ 🔍
☐ [Auditbeat System] Socket Dashboard ECS System Sockets	22 minutes ago	✎ 🔍
☐ [Auditbeat Auditd] Executions ECS Overview of kernel executions	22 minutes ago	✎ 🔍
☐ [Auditbeat Auditd] Sockets ECS Summary of socket related syscall events.	22 minutes ago	✎ 🔍
☐ [Auditbeat System] Process Dashboard ECS System Processes	22 minutes ago	✎ 🔍
☐ [Auditbeat System] System Overview ECS Overview of System Information.	22 minutes ago	✎ 🔍
☐ [Auditbeat System] Login Dashboard ECS System Logins	22 minutes ago	✎ 🔍
☐ [Auditbeat System] Package Dashboard ECS System Packages	22 minutes ago	✎ 🔍

Rows per page: 20 ▾

< 1 >

Dans le dashboard System Overview ECS, on y retrouve toutes les informations sur la machine Ubuntu :



Les informations sur les machines connectées

- Le nombre de machines connectées
- Le système d'exploitation des machines connectées

Les informations sur les connexions

- Le nombre de connexions
- Le type de connexions (démarrage, arrêt, connexion utilisateur)

Les informations sur les utilisateurs

- Le nombre d'utilisateurs enregistrés
- Le nombre de changements d'utilisateurs

Les informations sur les processus

- Le nombre de processus
- Le nombre de processus démarrés depuis le démarrage d'auditbeat
- Le nombre de processus arrêtés depuis le démarrage d'auditbeat

Les informations sur les sockets

- Le nombre de sockets
- Le nombre de processus ouverts depuis le démarrage d'auditbeat
- Le nombre de processus fermés depuis le démarrage d'auditbeat

Les informations sur les paquets

- le nombre de paquets installés sur les machines connectées
- le nombre de changement de paquets sur les machines connectées

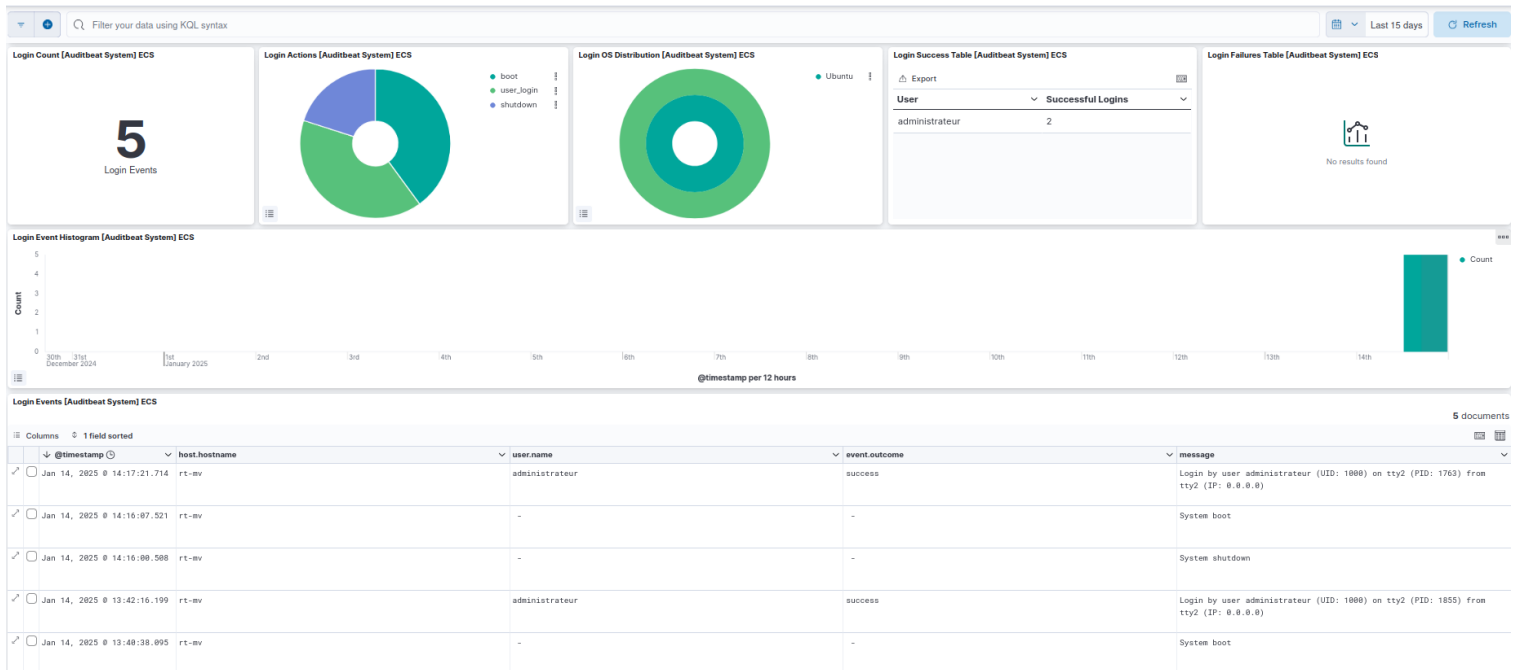
Les informations sur les machines connectées



Sur le Hosts dashboard, on voit bien que l'on a 1 host de connecté à elastic via auditbeat, on voit depuis combien de temps cette machine est démarrée et son OS.

On y retrouve dans la section host List le hostname de la machine, la version d'Ubuntu, son ID et le statut de la machine (si elle est up ou down)

Les informations sur les connexions



Sur le Login Dashboard, on voit le nombre d'événements de connexion qu'il y a eu sur la machine Ubuntu, le premier graphique montre le type d'action de connexion qui ont été effectués, dans mon cas boot, user_login et shutdown.

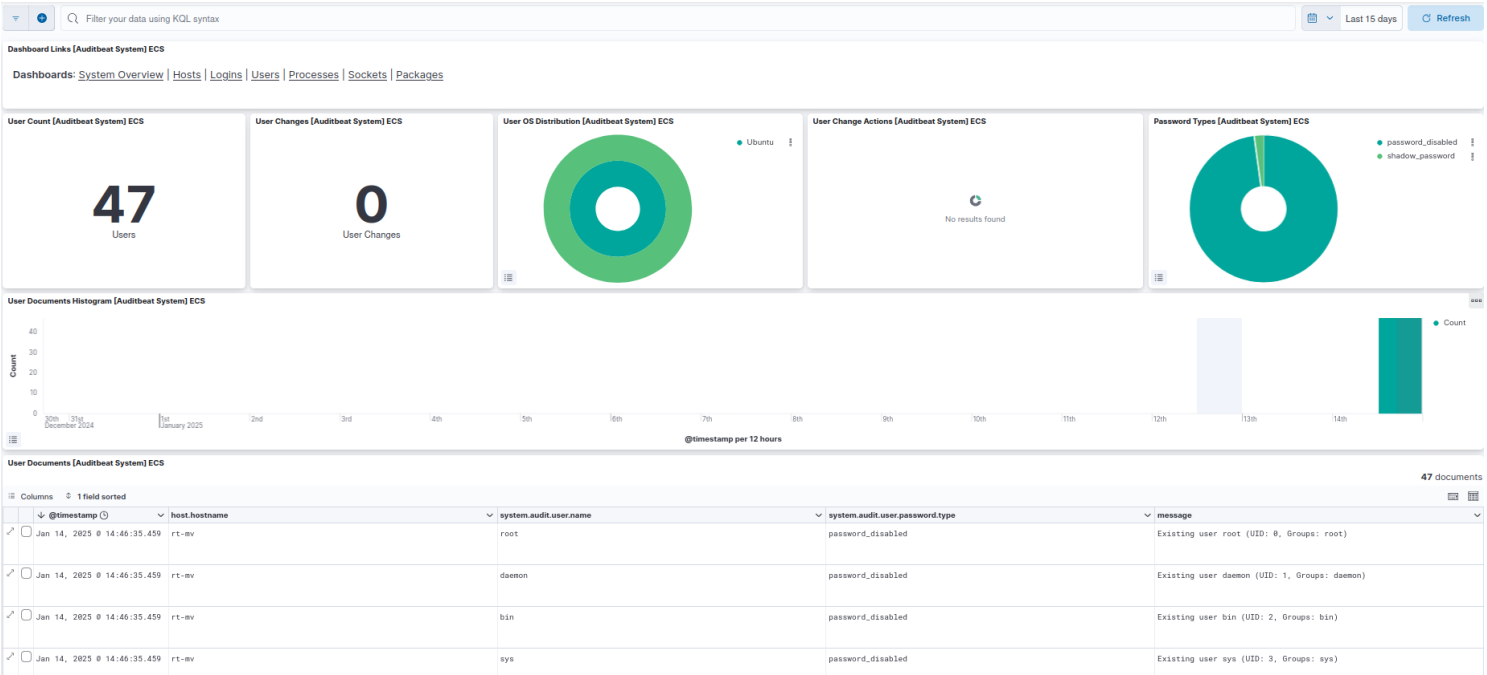
Le second graphique montre l'OS qui est Ubuntu, avec la distribution 22.04.1 LTS [Jammy Jellyfish].

Ensuite on voit la Login Success Table, qui montre les utilisateurs et leur nombre de connexions réussies.

Puis on voit la Login failure Table, qui dans mon cas est vide, mais qui montrera les utilisateurs avec leur nombre d'erreurs de connexions.

La section Login Events montre en détails les événements de connexions.

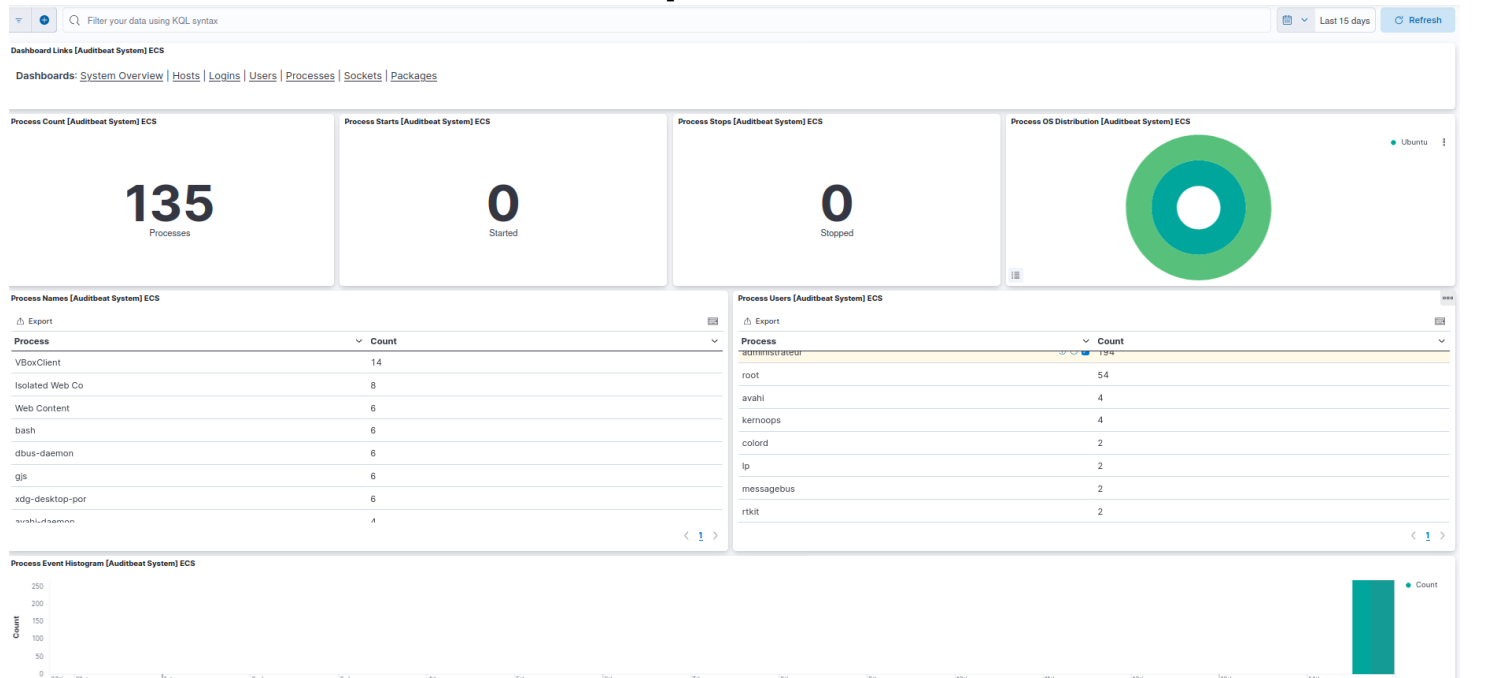
Les informations sur les utilisateurs



Sur le User Dashboard, on voit le nombre d'utilisateur existants sur la machine, le nombre de changement d'utilisateur, l'OS, le User Change Action qui pour moi est vide, et le Password Types qui donne des informations sur le type de mot de passe des utilisateurs de la machine (password_disabled ou shadow_password).

La section User Documents montre les détails de chaque utilisateur (username, password_type, message avec l'uid et le groupe de l'utilisateur).

Les informations sur les processus

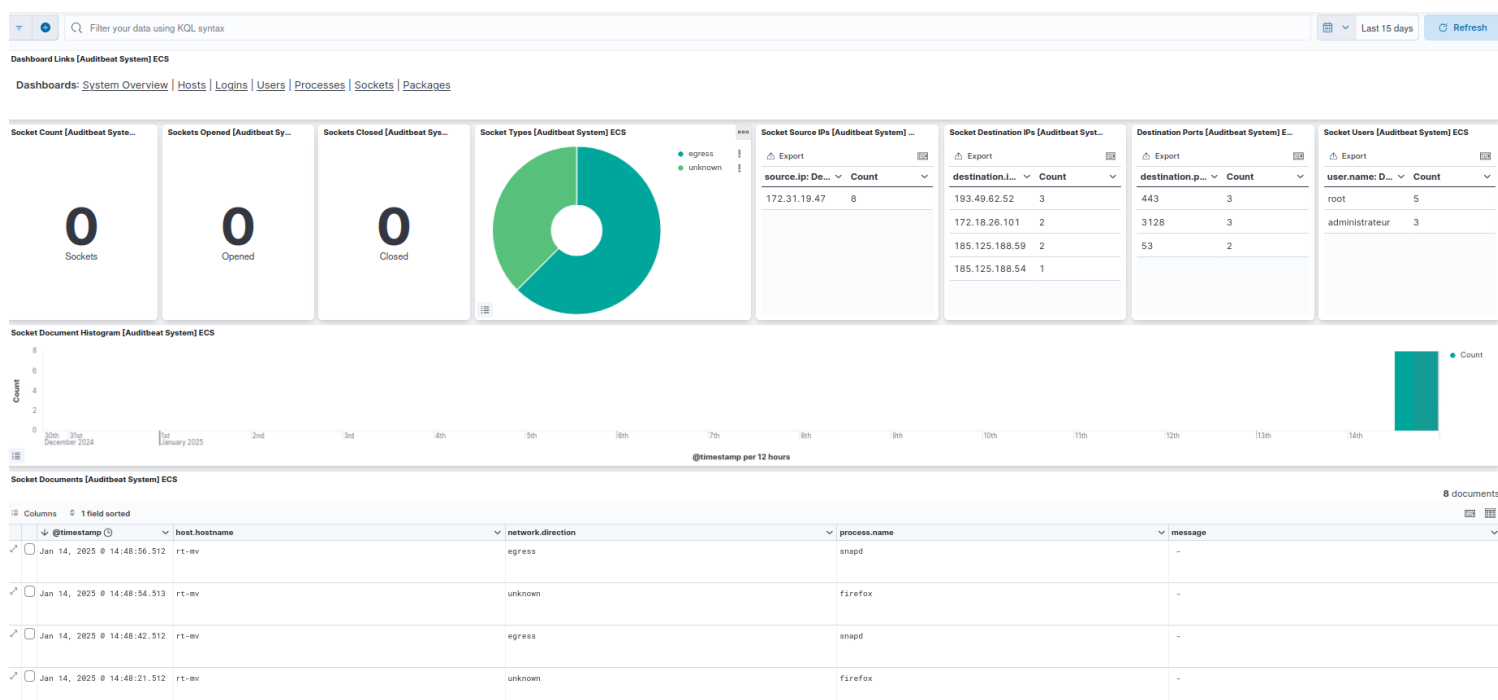


Sur le Process Dashboard, on voit le nombre de processus existant sur la machine, le nombre de processus démarrés et arrêtés depuis le lancement de auditbeat et l'OS.

Dans la section Process Names, on voit les noms des processus et le nombre de processus.

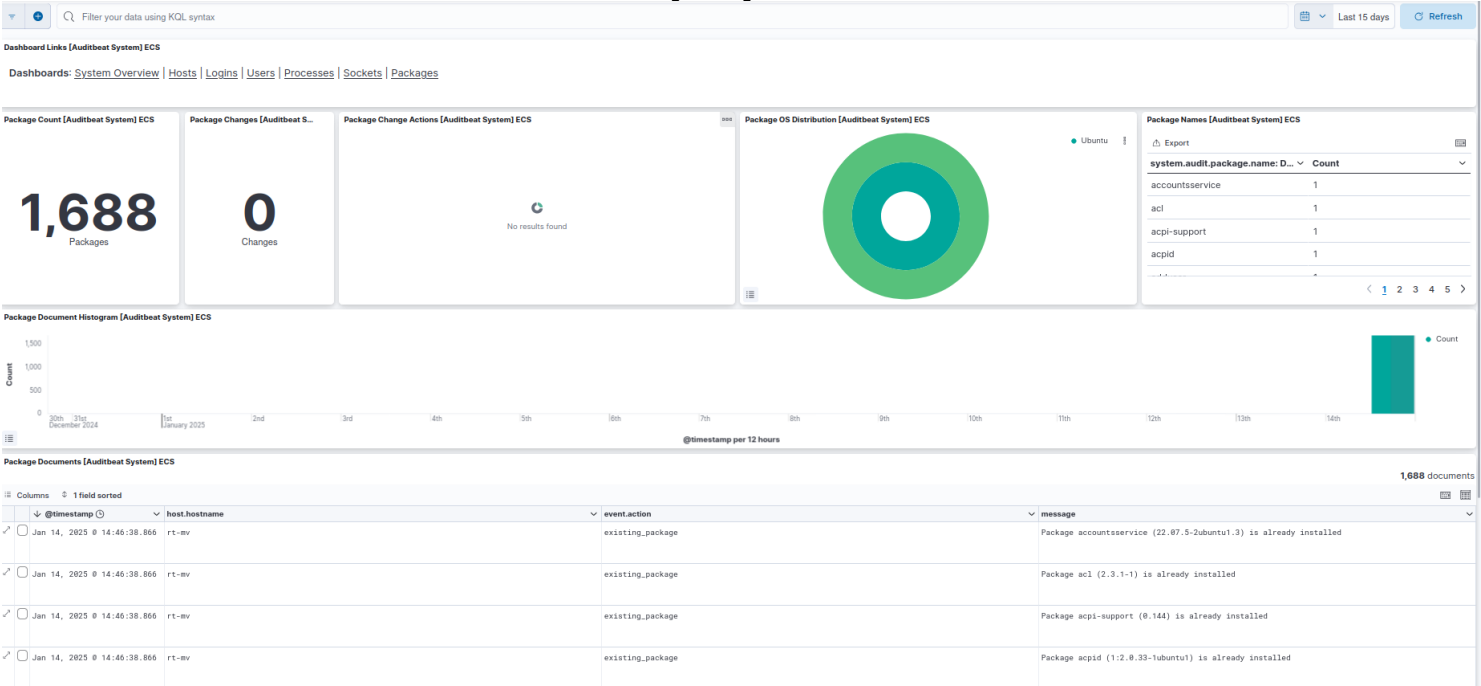
Dans la section Process Users, on voit le nombre de processus existant par utilisateurs.

Les informations sur les sockets



Sur le Socket Dashboard on voit, le nombre de Socket, de socket ouverts et fermés, le type de socket (egress, unknown), IP Source des sockets, l'IP destination des sockets, le port de destination et le nombre de socket par utilisateurs.

Les informations sur les paquets



Sur le Package Dashboard, on voit le nombre de paquets existant sur la machine, le nombre de changement de paquet, l'OS et le nom des paquets.