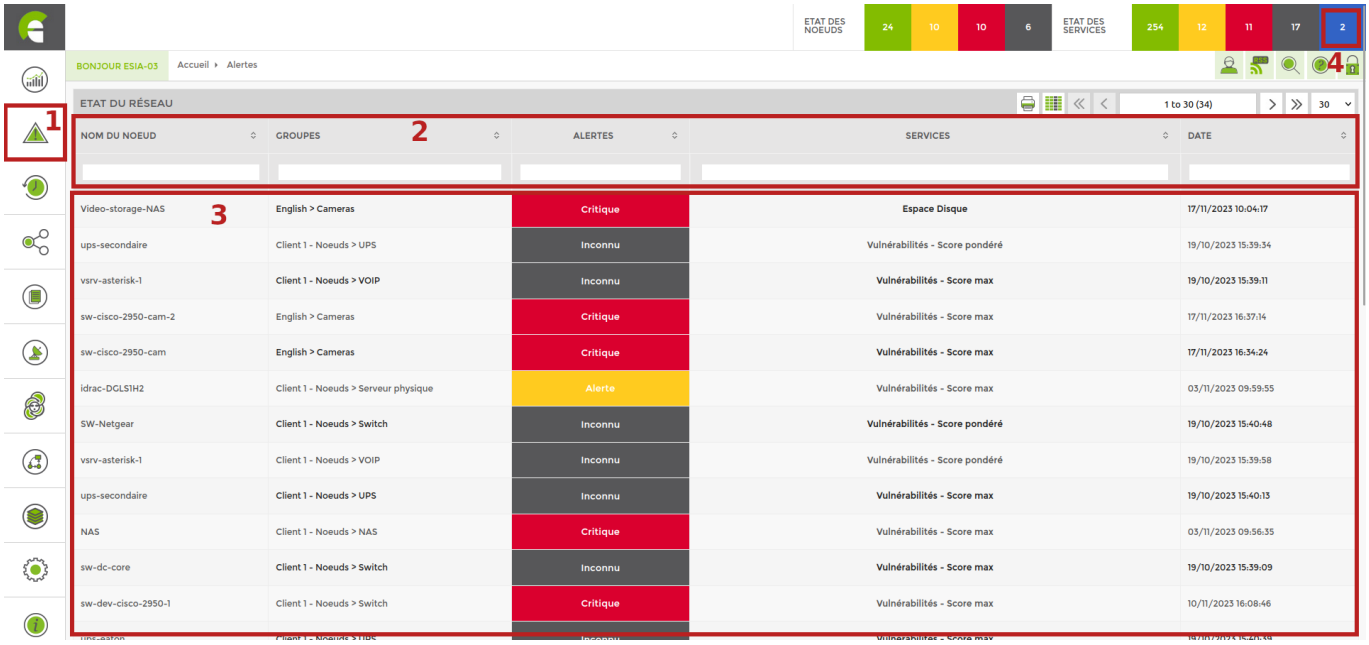
Tableau des alertes et sa widget

Pour accéder au tableau des alertes, cliquez sur le menu “Alertes” à gauche. Un grand tableau s'affiche comme si dessous.

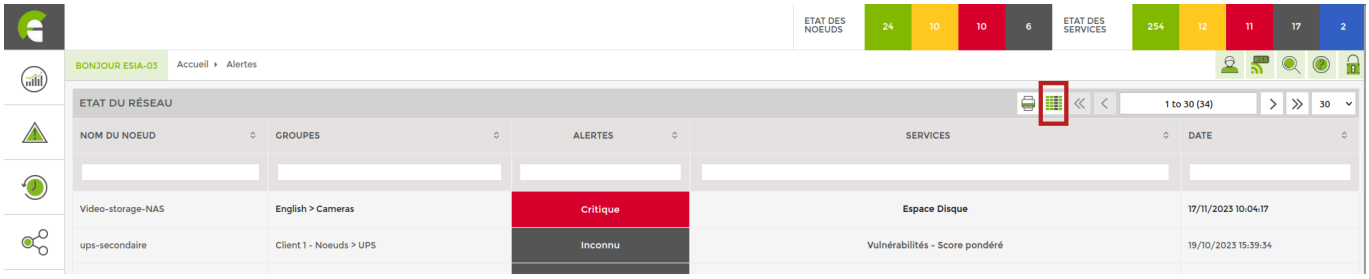
1. Boutons d'accès
2. “tablesorter”: champs de recherche par colonne (voir “Mots-clés dans les champs de recherche”)
3. Liste des erreurs impactées par la priorité (voir chapitre).
4. Affiche les erreurs acquittées



Colonnes cachées

Par défaut, certaines colonnes ne sont pas affichées afin de limiter la taille de chaque ligne et de s'adapter à toutes les tailles d'écrans.

Au besoin vous pouvez afficher les colonnes qui sont cachées par défaut via le bouton “Afficher/masquer les colonnes” situé en haut à droite. Voir l'image ci-dessous dans l'encadré rouge:



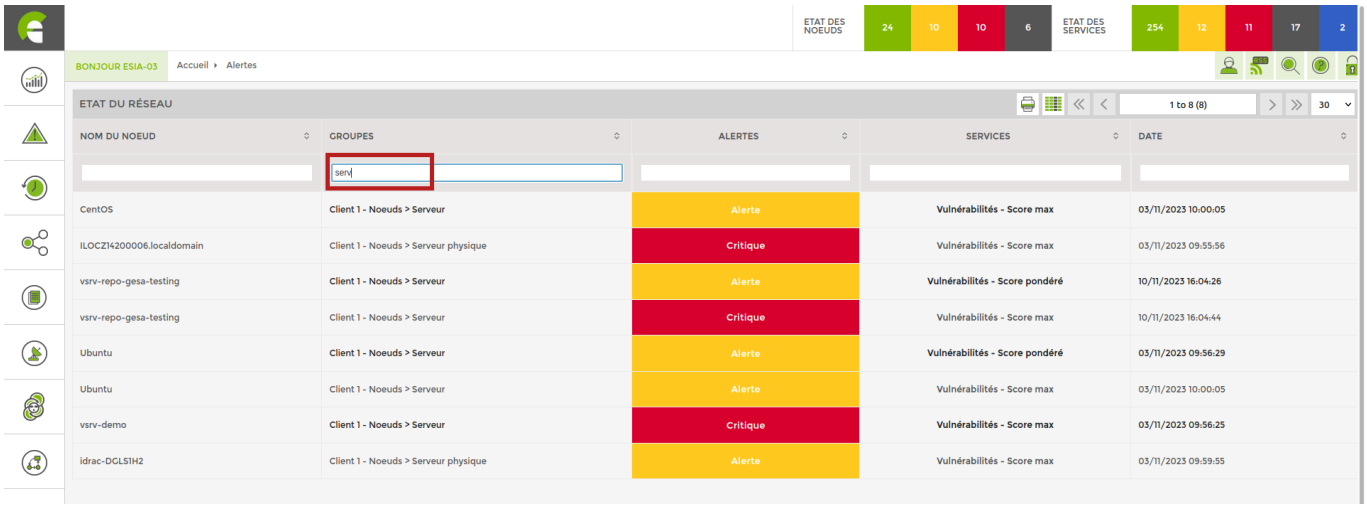
Le menu apparaît juste en dessous, décochez la case “Auto” pour pouvoir sélectionner les colonnes que vous souhaitez afficher ou cacher.

Les colonnes suivantes sont cachées par défaut:

- Adresse IP
- Type de nœud
- Description du nœud
- Nom technique du service
- Message de l'erreur

Mots-clés dans les champs de recherche

Vous pouvez faire une recherche basique comme par exemple filtrer sur les groupes contenant les lettres “serv”. Et vous aurez un affichage comme ceci.

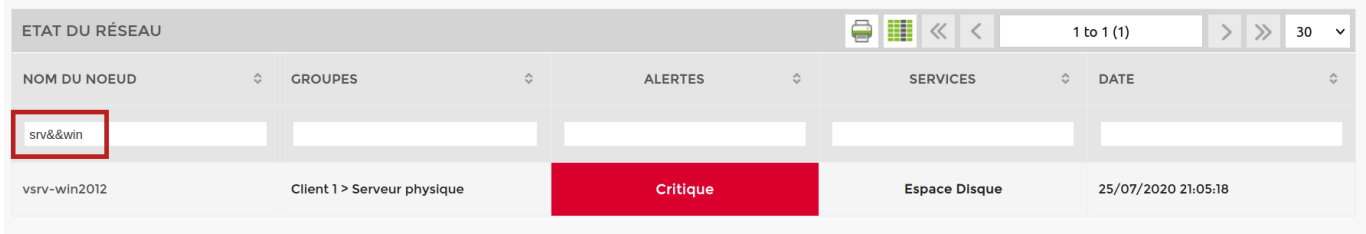


Fonctionnalité existante sur les versions supérieures à 3.2.5.

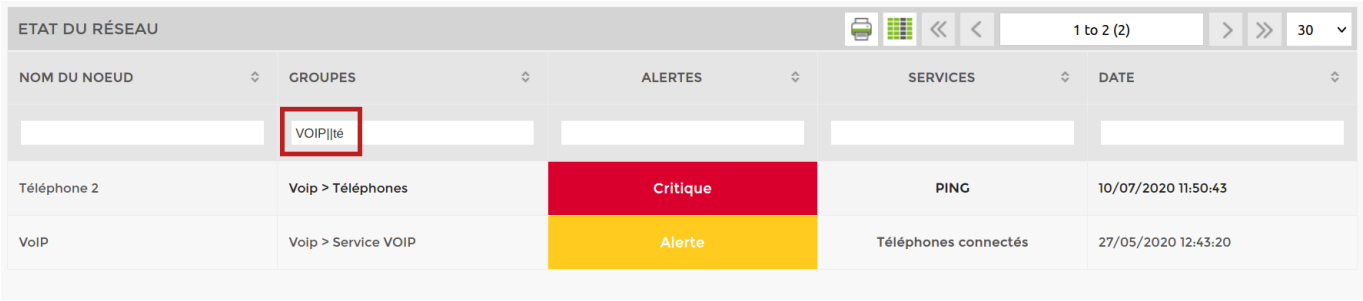
Mais il existe des mots clés qui vous permettent soit de configurer votre widget de tableau de bord ou d'affiner votre recherche. Voici la liste des mots-clés:

- “!” permets de faire un “NON logique”. Par exemple, si je veux filtrer toutes les alertes en éliminant les inconnues. J'écrirais “!inconnu” dans mon filtre.
- “&&” permets de faire un “ET logique”. Par exemple, si je veux afficher les nœuds en erreur contenant à la fois les lettres “srv” et “win”. J'écrirais “srv&&win”
- “||” permets de faire un “OU logique”. Par exemple, si je veux afficher les nœuds en erreur dans les groupes VOIP et téléphone, j'écrirais “VOIP||té”

Le screen avec “srv&&win”:

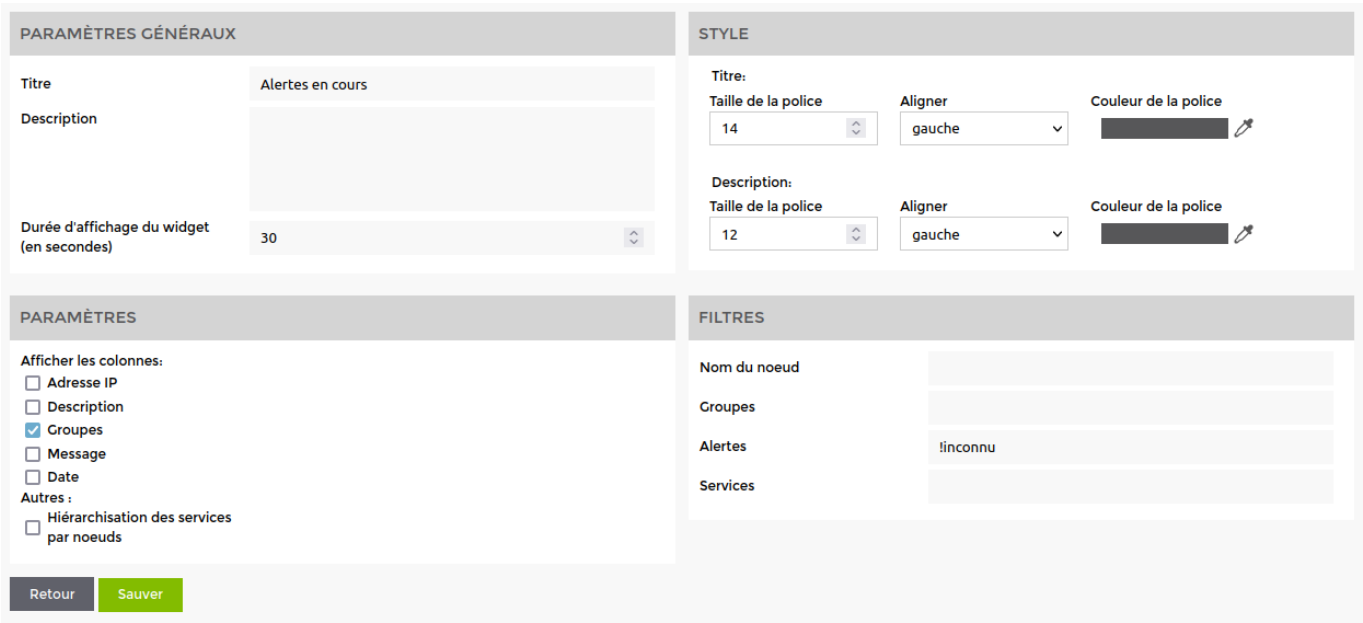


Le screen avec “VOIP||té”:

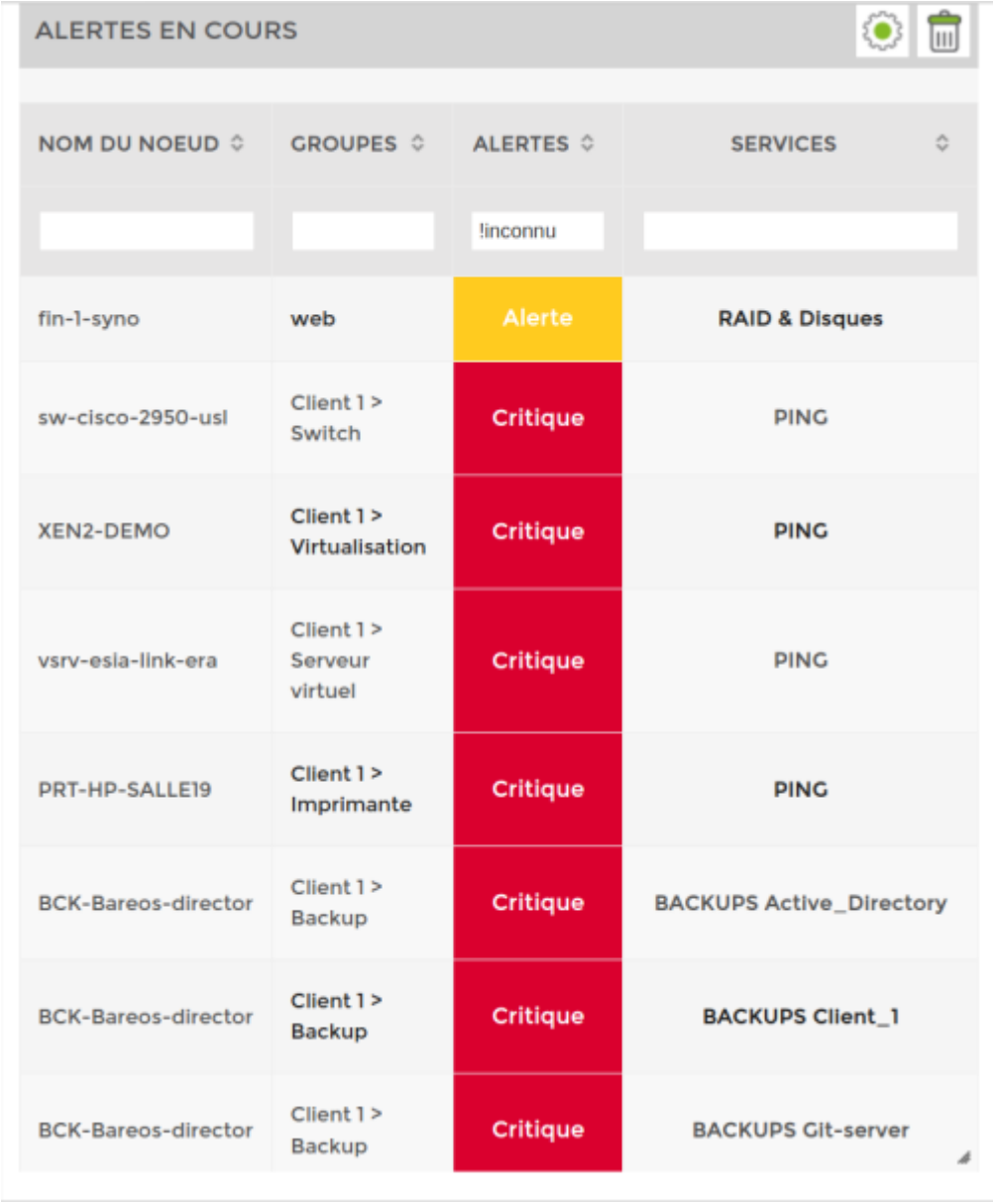


Utilisation sur une widget de tableau de bord

Voici un exemple sur une widget du tableau de bord d' “Alertes en cours”. Il y a une section filtre à droite. Je vais donc filtrer les alertes en éliminant les erreurs de niveau inconnu. Je vais donc indiqué !inconnu dans le filtre des alertes. Comme ci-dessous.



Une fois sauvegardé, vous pouvez constater que le filtre est bien ajouté sur votre widget de tableau de bord.



Hiérarchisation des erreurs

Par défaut, le tableau affiche les erreurs selon la priorité de chaque service. Il y a 7 niveaux disponibles (comme pour le modèle OSI). Cela permet de trier automatiquement les erreurs. Le niveau 1 étant le plus critique.

Par défaut, pour le pattern de supervision Windows ou Linux les priorités des services sont hiérarchisées de la sorte.

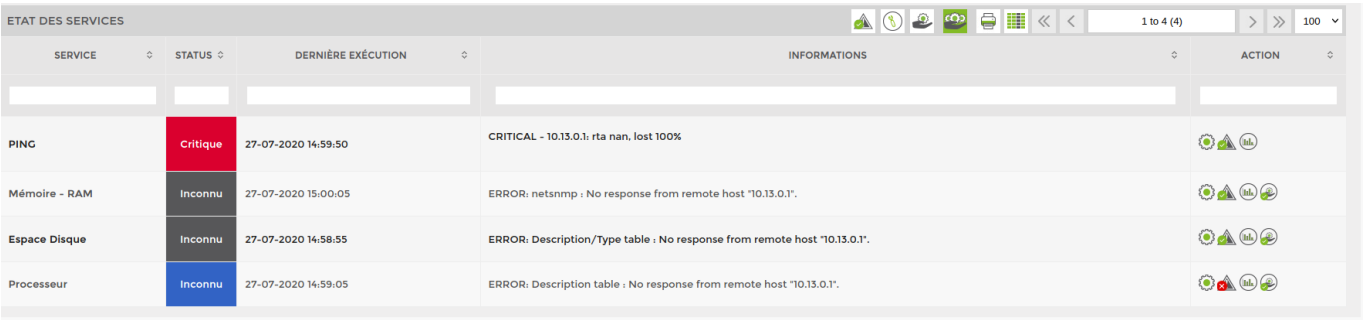
- PING (CHECK_ICMP): niveau 1
- CPU (CHECK_SNMP_LOAD): niveau 2
- RAM (CHECK_SNMP_WINDOWS_MEM: niveau 3
- Espace disque (CHECK_SNMP_WINDOWS_STORAGE): niveau 3

Cette nomenclature de base s'explique de la façon suivante: Si le ping ne répond pas, c'est que le nœud est injoignable donc pas la peine d'afficher le reste. Si la charge CPU est à 100%, il est normal

que les requêtes SNMP échouent et le problème a traité est la charge processeur. Si SNMP n'est pas configuré, on n'affiche que la ligne du CPU. Il n'est donc pas nécessaire d'afficher les autres erreurs qui feraient doublon.

Exemple: mon serveur Houston qui a un problème de PING (noté l'utilisation d'un filtre de recherche 🙂).

Si je cliques dessus, je peux pourtant voir qu'il y a 4 services en erreurs. Le ping + les 3 services SNMP de base. Dans l'exemple ci dessous, le service “Processeur” a été acquitté.



Le Ping ayant la plus haute priorité (1 par défaut), le tableau d'alerte a éliminé l'ensemble des erreurs de niveau supérieur.

Si vous souhaitez modifier les priorités des services sur un nœud, vous pouvez vous baser sur le tuto suivant: Appliquer des services sur vos nœuds

Cas pratique: un serveur ESIA

Prenons un serveur Esia classique, nous avons une partie liée au matériel qui sera supervisée par le pattern Linux qui a les priorités de services de base comme ceci :

- PING (CHECK_ICMP): niveau 1
- CPU (CHECK_SNMP_LOAD): niveau 2
- RAM (CHECK_SNMP_LINUX_MEM: niveau 3
- Espace disque (CHECK_SNMP_LINUX_STORAGE): niveau 3

J’ajouterais le service testant les IO disques (CHECK_SNMP_LINUX_IO). Je lui mettrais la priorité de niveau 4 car si mes IO sont saturées ma base de données risque d’être KO ou mon serveur apache très lent. Nous considérons donc que la priorité en dessous de 4 est vient d’un problème « matériel ».

Pour la partie logiciel, voici la liste des processus fonctionnant sur notre serveur:

- EsiaDaemon
- PostgreSQL

- Apache2

Je vais rajouter les services suivants en partant du plus critique vers le moins ou en partant refaisant la chaîne de dépendance.

- Processus Postgresql (CHECK_SNMP_PROCESS_POSTGRESQL): niveau 5 s'il ne tourne pas Apache et Esia ne sont pas fonctionnels.
- Processus Apache2 (CHECK_SNMP_PROCESS_Apache): niveau 6 s'il ne tourne pas je sais pas accéder à une page WEB.
- Processus EsiaDaemon (CHECK_SNMP_PROCESS_esiaDaemon): niveau 6 pas de supervision s'il ne tourne pas
- HTTP: CHECK_HTTP / CHECK_HTTPS: niveau 7 tentes une connexion à l'interface web et vérifie que j'ai bien un code de retour 200. Donc la connexion DB et PHP sont parfaitement fonctionnels.

Ainsi dès que j'ai une erreur sur mon serveur, j'ai déjà un diagnostic rien qu'en lisant la première ligne dans mon tableau de bord.

Au final, voici la liste de tous les services avec leurs priorités respectives.

- PING (CHECK_ICMP): niveau 1
- CPU (CHECK_SNMP_LOAD): niveau 2
- RAM (CHECK_SNMP_LINUX_MEM: niveau 3
- Espace disque (CHECK_SNMP_LINUX_STORAGE): niveau 3
- IO disque (CHECK_SNMP_LINUX_IO): niveau 4
- Processus Postgresql (CHECK_SNMP_PROCESS_POSTGRESQL): niveau 5
- Processus Apache2 (CHECK_SNMP_PROCESS_Apache): niveau 6
- Processus EsiaDaemon (CHECK_SNMP_PROCESS_esiaDaemon): niveau 6
- HTTP (CHECK_HTTP): niveau 7