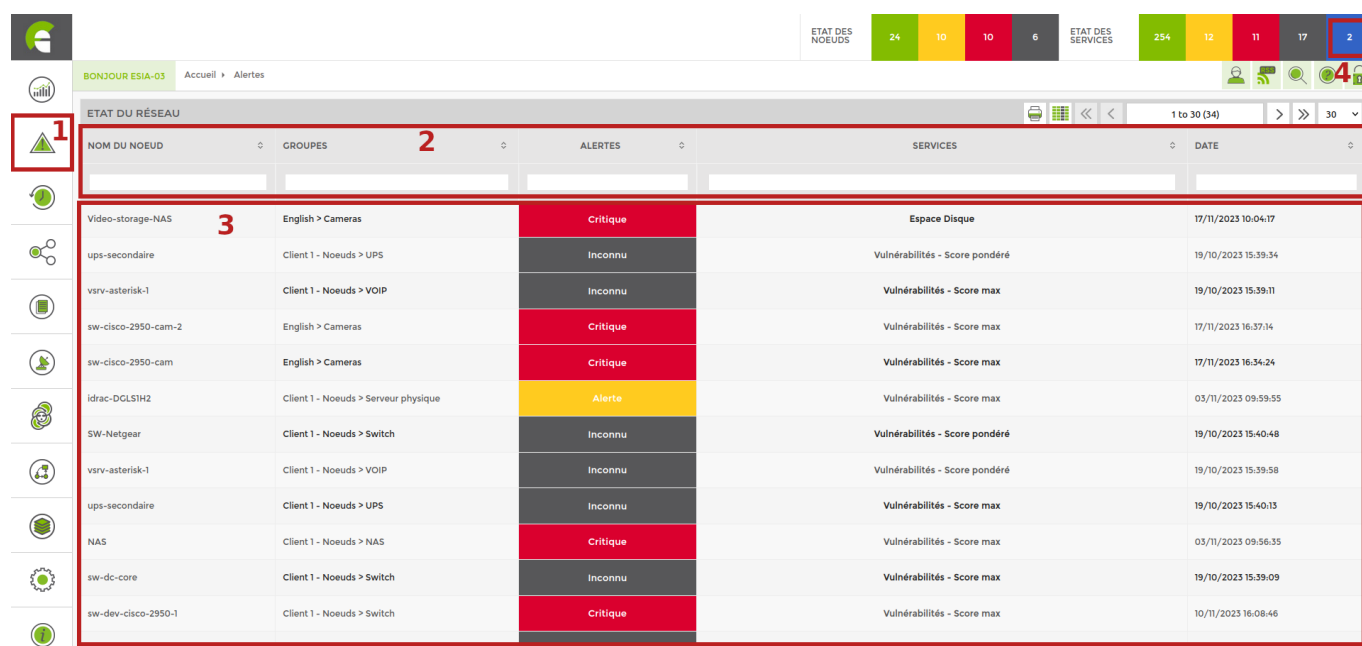


Tableau des alertes et sa widget

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

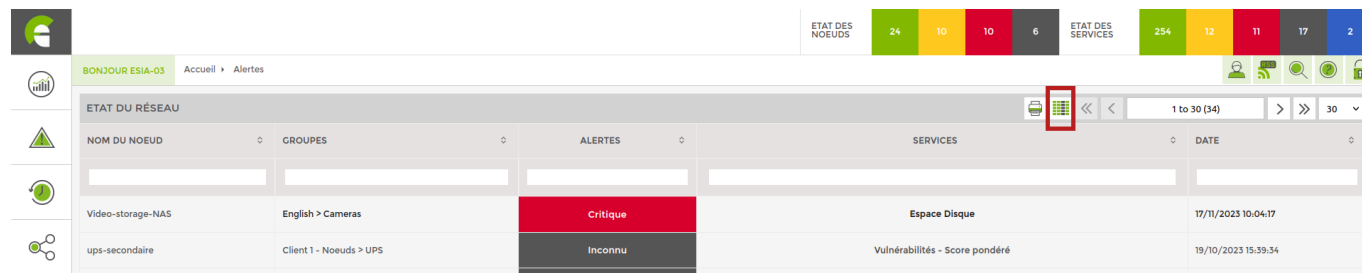


NOM DU NOEUD	GROUPE	ALERTES	SERVICES	DATE
Video-storage-NAS	English > Cameras	Critique	Espace Disque	17/11/2023 10:04:17
ups-secondaire	Client 1 - Noeuds > UPS	Inconnu	Vulnérabilités - Score pondéré	19/10/2023 15:39:34
vsvr-asterisk-1	Client 1 - Noeuds > VOIP	Inconnu	Vulnérabilités - Score max	19/10/2023 15:39:11
sw-cisco-2950-cam-2	English > Cameras	Critique	Vulnérabilités - Score max	17/11/2023 16:37:14
sw-cisco-2950-cam	English > Cameras	Critique	Vulnérabilités - Score max	17/11/2023 16:34:24
ldrac-DGLSIH2	Client 1 - Noeuds > Serveur physique	Alerte	Vulnérabilités - Score max	03/11/2023 09:59:55
SW-Netgear	Client 1 - Noeuds > Switch	Inconnu	Vulnérabilités - Score pondéré	19/10/2023 15:40:48
vsvr-asterisk-1	Client 1 - Noeuds > VOIP	Inconnu	Vulnérabilités - Score pondéré	19/10/2023 15:39:58
ups-secondaire	Client 1 - Noeuds > UPS	Inconnu	Vulnérabilités - Score max	19/10/2023 15:40:13
NAS	Client 1 - Noeuds > NAS	Critique	Vulnérabilités - Score max	03/11/2023 09:56:35
sw-dc-core	Client 1 - Noeuds > Switch	Inconnu	Vulnérabilités - Score max	19/10/2023 15:39:09
sw-dev-cisco-2950-1	Client 1 - Noeuds > Switch	Critique	Vulnérabilités - Score max	10/11/2023 16:08:46

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:



NOM DU NOEUD	GROUPE	ALERTES	SERVICES	DATE
Video-storage-NAS	English > Cameras	Critique	Espace Disque	17/11/2023 10:04:17
ups-secondaire	Client 1 - Noeuds > UPS	Inconnu	Vulnérabilités - Score pondéré	19/10/2023 15:39:34

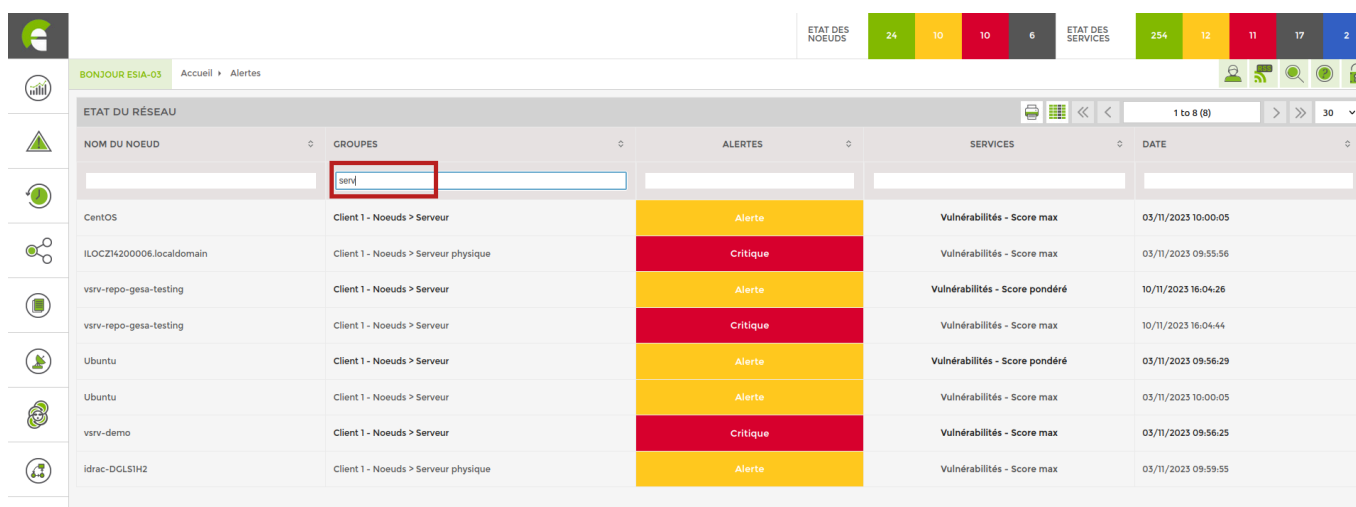
Le menu apparaît juste en dessous, décochez la case “Auto” pour pouvoir sélectionner les colonnes que vous souhaitez afficher ou cacher.

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.



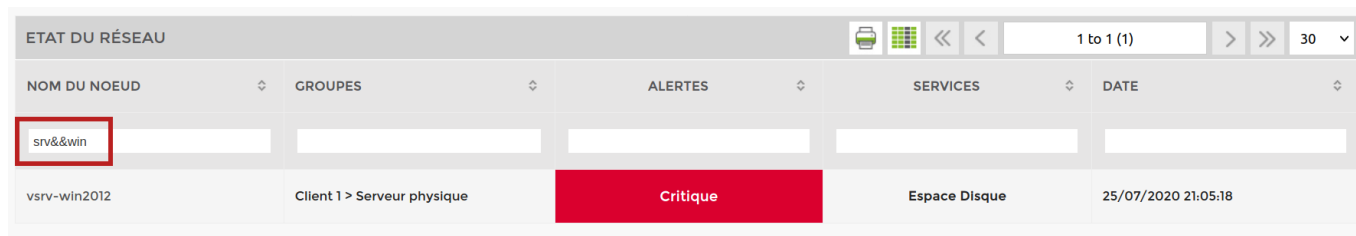
ETAT DU RÉSEAU		ALERTES	SERVICES	DATE
NOM DU NOEUD	GROUPES			
CentOS	Client 1 - Nœuds > Serveur	Alerte	Vulnérabilités - Score max	03/11/2023 10:00:05
ILOCZ14200006.localdomain	Client 1 - Nœuds > Serveur physique	Critique	Vulnérabilités - Score max	03/11/2023 09:55:56
vsvr-repo-gesa-testing	Client 1 - Nœuds > Serveur	Alerte	Vulnérabilités - Score pondéré	10/11/2023 16:04:26
vsvr-repo-gesa-testing	Client 1 - Nœuds > Serveur	Critique	Vulnérabilités - Score max	10/11/2023 16:04:44
Ubuntu	Client 1 - Nœuds > Serveur	Alerte	Vulnérabilités - Score pondéré	03/11/2023 09:56:29
Ubuntu	Client 1 - Nœuds > Serveur	Alerte	Vulnérabilités - Score max	03/11/2023 10:00:05
vsvr-demo	Client 1 - Nœuds > Serveur	Critique	Vulnérabilités - Score max	03/11/2023 09:56:25
idrac-DCL5H2	Client 1 - Nœuds > Serveur physique	Alerte	Vulnérabilités - Score max	03/11/2023 09:59:55

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:

- "!" permet de faire un "NON logique". Par exemple, si je veux filtrer toutes les alertes en éliminant les inconnues. J'écrirais "!inconnu" dans mon filtre.
- "&&" permet 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"
- "||" permet 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":



ETAT DU RÉSEAU		ALERTES	SERVICES	DATE
NOM DU NOEUD	GROUPES			
vsvr-win2012	Client 1 > Serveur physique	Critique	Espace Disque	25/07/2020 21:05:18

Le screen avec "VOIP||té":

ETAT DU RÉSEAU					1 to 2 (2)	30
NOM DU NOEUD	GROUPES	ALERTES	SERVICES	DATE		
	VOIP ité					
Téléphone 2	Voip > Téléphones	Critique	PING	10/07/2020 11:50:43		
VoIP	Voip > Service VOIP	Alerte	Téléphones connectés	27/05/2020 12:43:20		

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.

PARAMÈTRES GÉNÉRAUX		STYLE	
Titre	Alertes en cours	Titre:	
Description		Taille de la police	Aligner
		14	gauche
Durée d'affichage du widget (en secondes)	30	Description:	Couleur de la police
		Taille de la police	Aligner
		12	gauche
			Couleur de la police
PARAMÈTRES		FILTRES	
Afficher les colonnes:		Nom du noeud	
<input type="checkbox"/> Adresse IP		Groupes	
<input type="checkbox"/> Description		Alertes	!inconnu
<input checked="" type="checkbox"/> Groupes		Services	
<input type="checkbox"/> Message			
<input type="checkbox"/> Date			
Autres :			
<input type="checkbox"/> Hiérarchisation des services par noeuds			
Retour	Sauver		

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

ALERTE EN COURS			
NOM DU NOEUD	GROUPE	ALERTE	SERVICES
		Inconnu	
fin-1-syno	web	Alerte	RAID & Disques
sw-cisco-2950-us1	Client 1 > Switch	Critique	PING
XEN2-DEMO	Client 1 > Virtualisation	Critique	PING
vsvr-esia-llnk-era	Client 1 > Serveur virtuel	Critique	PING
PRT-HP-SALLE19	Client 1 > Imprimante	Critique	PING
BCK-Bareos-director	Client 1 > Backup	Critique	BACKUPS Active_Directory
BCK-Bareos-director	Client 1 > Backup	Critique	BACKUPS Client_1
BCK-Bareos-director	Client 1 > Backup	Critique	BACKUPS Git-server

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



).

ETAT DU RÉSEAU				
NOM DU NOEUD	GROUPE	ALERTE	SERVICES	DATE
Housto				
vsvr-Houston	Client 1 > Virtualisation	Critique	PING	07/07/2018 09:10:45

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.

ETAT DES SERVICES				
SERVICE	STATUS	DERNIÈRE EXÉCUTION	INFORMATIONS	ACTION
PING	Critique	27-07-2020 14:59:50	CRITICAL - 10.13.0.1: rta nan, lost 100%	
Mémoire - RAM	Inconnu	27-07-2020 15:00:05	ERROR: netsnmp : No response from remote host "10.13.0.1".	
Espace Disque	Inconnu	27-07-2020 14:58:55	ERROR: Description/Type table : No response from remote host "10.13.0.1".	
Processeur	Inconnu	27-07-2020 14:59:05	ERROR: Description table : No response from remote host "10.13.0.1".	

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

From:

<https://wiki.esia-sa.com/> - **Esia Wiki**

Permanent link:

https://wiki.esia-sa.com/advanced/alert_widget

Last update: **2023/11/21 13:44**

