Guide d’Administration

Version 7.2

Date : Février 2025

Classification : Non classifié

Rédacteur : Team IKare

Bienvenue

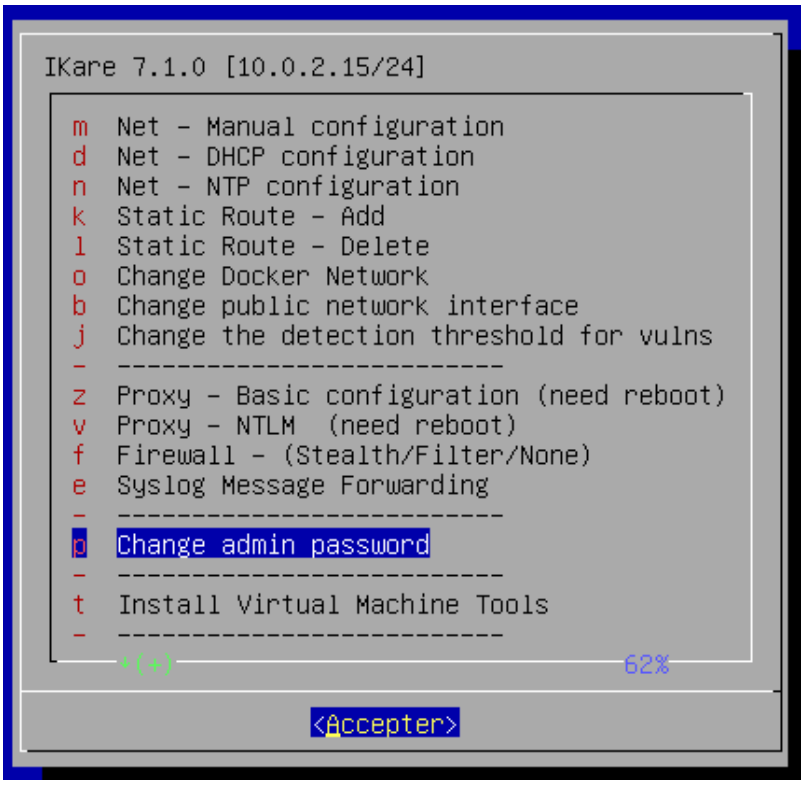
Ce guide vous accompagne dans l'administration et le paramétrage de votre logiciel Ikare. Ikare est un outil qui automatise la mise en place des meilleures pratiques de sécurité et du management des vulnérabilités.

1. Administration

1.1 Paramétrage système

Les paramètres systèmes se gèrent depuis la console d'IKare. Elle est accessible directement depuis le terminal d'IKare ou depuis une connexion SSH.

Le menu d'administration ci-dessous apparaît :



Les options qui sont proposées dans le menu d'administration sont les suivantes :

Menu	Description
Net - Manual Configuration	Paramétrage de l'interface réseau en mode manuel
Net - DHCP Configuration	Paramétrage de l'interface réseau en mode DHCP (IP dynamique)
Net - NTP Configuration	Paramétrage du serveur de temps NTP (Network Time Protocol)
Static Route – Add	Ajout d'une route statique pour permettre à IKare d'accéder à des réseaux nécessitant un routage
Static Route – Delete	Supprime une route statique de l'interface réseau
Change Docker Network	Change l'interface réseau interne du service docker
Change public network interface	Change l'interface réseau publique de la VM
Change the detection thresold for vulns	Change le seuil de qualité de détection des vulnérabilités IKare
Proxy - Basic Configuration	Paramétrage d'un relais HTTP
Proxy – NTLM	Paramétrage d'un relais HTTP NTLM (authentification Windows)
Firewall	Paramétrage du pare-feu IKare
Syslog Message Forwarding	Permet à IKare d'exporter les alertes de sécurité vers un serveur Syslog distant. Les protocoles TCP et UDP sont supportés.
Change admin password	Changement du mot de passe de l'administrateur console
Install Virtual Machine Tools	Permet d'installer les paquets nécessaires à l'utilisation des fonctionnalités
Import certificates	Permet d'importer les certificats SSL de la machine
Test Network Connectivity	Lancement d'un test de connectivité réseau
Ikare license register	Enregistrer la clef de licence d'Ikare
Reload Vulnerabilities database	Recharger la base de vulnérabilité
Change IKare update mode	Change la politique d'installation des mises à jour d'IKare (manuelle ou automatique)
Check & run updates	Vérifie et installe les mises à jour d'IKare
Reboot	Redémarrage du serveur IKare
Shutdown	Arrêt du serveur IKare
Quit	Déconnexion du compte admin

Veillez à appliquer les modifications des notes 1 et 2 ci-dessous.

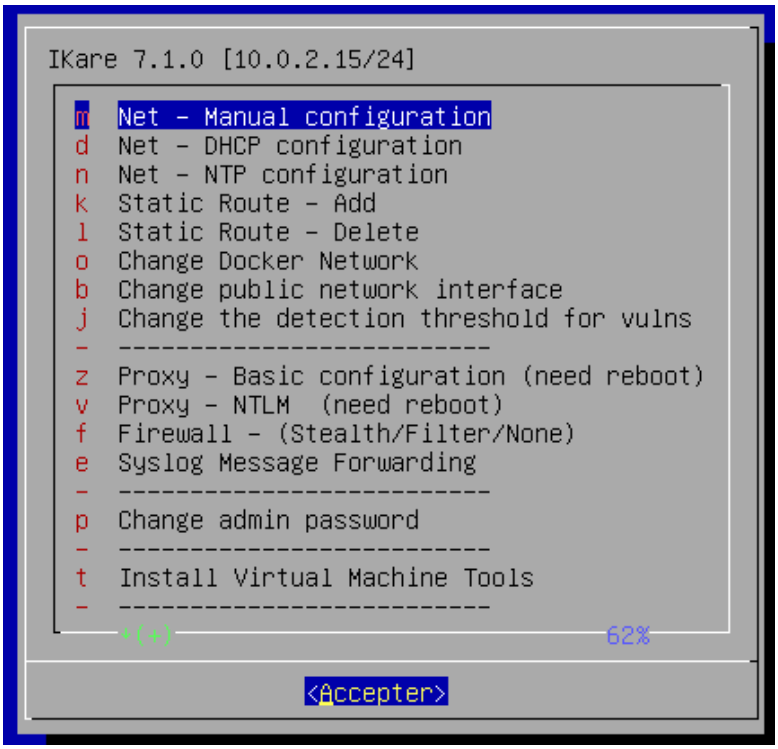
ℹ️ **Note 1 :** Pour des raisons de sécurité, il est impératif de changer le mot de passe admin.

ℹ️ **Note 2 :** Les certificats présents sur le serveur IKare sont autosignés par ITrust. Vous devez les remplacer par des certificats délivrés par une autorité de certification.

1.2 Administration d'une sonde

Dans le cas d'une licence multisondes, les paramètres système de la sonde se gèrent depuis la console d'administration de celle-ci. Tout comme la console d'administration d'IKare, elle est disponible directement depuis le terminal ou à travers une connexion SSH.

Le compte d'administration est "**admin**", le mot de passe par défaut est "**IkareCh4ng3!**". Le menu d'administration ci-dessous apparaît :



La majorité des items sont communs avec la console d'administration d'un serveur et ne sont pas repris ci-dessous.

Menu	Description
Register IKare Probe	Enregistrement de la sonde vers le serveur
Import CA file	Permet d'importer le certificat SSL du CA de la machine

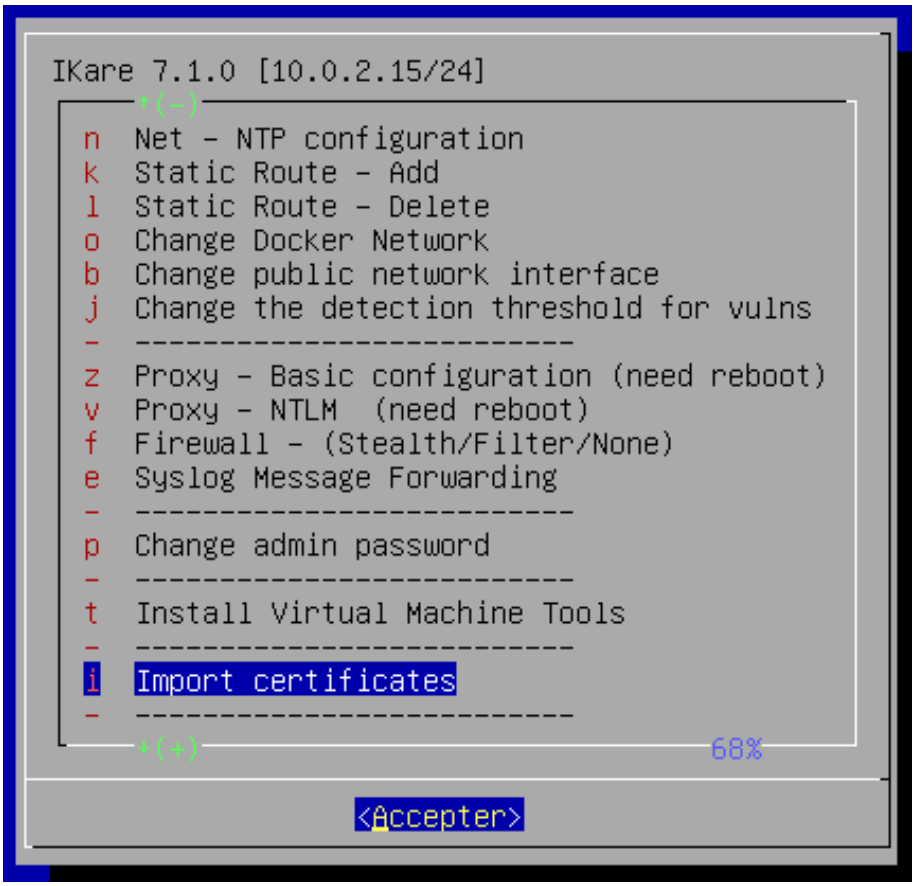
ℹ️ **Note 1 :** Pour des raisons de sécurité, il est impératif de changer le mot de passe admin.

1.3 Changement des certificats

Les certificats embarqués par IKare sont des certificats auto-signés qu'il faut changer dans la mesure du possible. Depuis le menu SSH admin, vous pouvez directement importer dans IKare vos propres certificats.

1.3.1 Imports des certificats sur un IKare Master

Pour cela, sélectionnez l'entrée "**Import certificates**" dans le menu et suivez les instructions.



Si vous souhaitez importer vos propres certificats, vous devez générer vos certificats SSL avec 4096 bits d'encryptage (clé RSA, au format PEM) et définir dans le certificat les informations suivantes pour IKare : Country, State, Organization, FQDN, adresse mail et un Subject Name incluant la machine IKare (wildcard sur un domaine de votre organisation ou le nom DNS de la machine IKare ou son IP lorsqu'elle est fixe).

Lors de l'importation de vos certificats dans IKare, vous devez appliquer les règles suivantes :

- Import du certificat : insérez le contenu base64 du certificat
  - Il doit commencer par la chaine : -----BEGIN CERTIFICATE-----
  - Et se terminer par la chaine -----END CERTIFICATE-----

- Import de la clé privée : insérez le contenu base64 de la clé privée
    - Elle doit commencer par la chaine : -----BEGIN RSA PRIVATE KEY-----
    - Et se terminer par la chaine -----END RSA PRIVATE KEY-----

- Import du certificat de l'autorité de certification (CA) : vous devez importer l'ensemble de la chaine de certification (il faut éventuellement importer tous les certificats intermédiaires jusqu'au certificat racine du CA. Dans le cas où le certificat CA contient une chaine de certification, insérez les certificats dans l'ordre du premier certificat intermédiaire et terminez par le certificat racine).

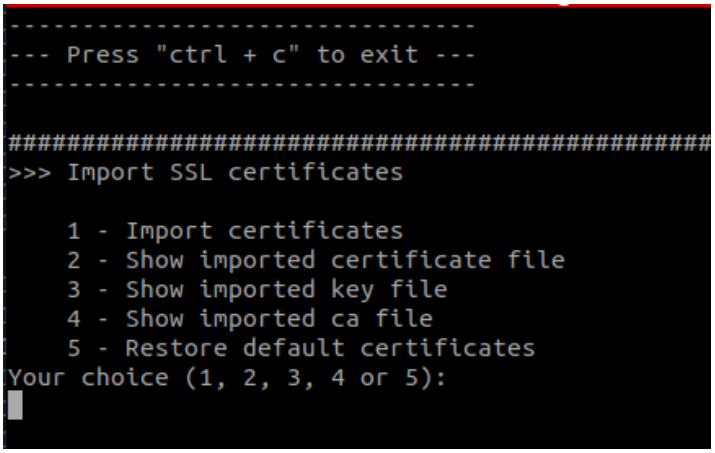
- Chaque certificat ajouté doit commencer par la chaine : -----BEGIN CERTIFICATE-----
- Et se terminer par la chaine -----END CERTIFICATE-----

ℹ️ **Note** : Pour vérifier si votre certificat CA est un intermédiaire ou un racine, vous pouvez exécuter la commande :

'openssl x509 -text -noout -in <ca_cert_file.pem>'

Si les CN de la partie "**Issuer**" et "**Subject**" sont identiques, il s'agit d'un certificat racine. Sinon, il s'agit d'un certificat intermédiaire, il est donc nécessaire d'ajouter également le certificat CA ayant comme partie "**Subject**" la valeur de la partie "**Issuer**" du certificat intermédiaire (et ainsi de suite pour atteindre le certificat racine).

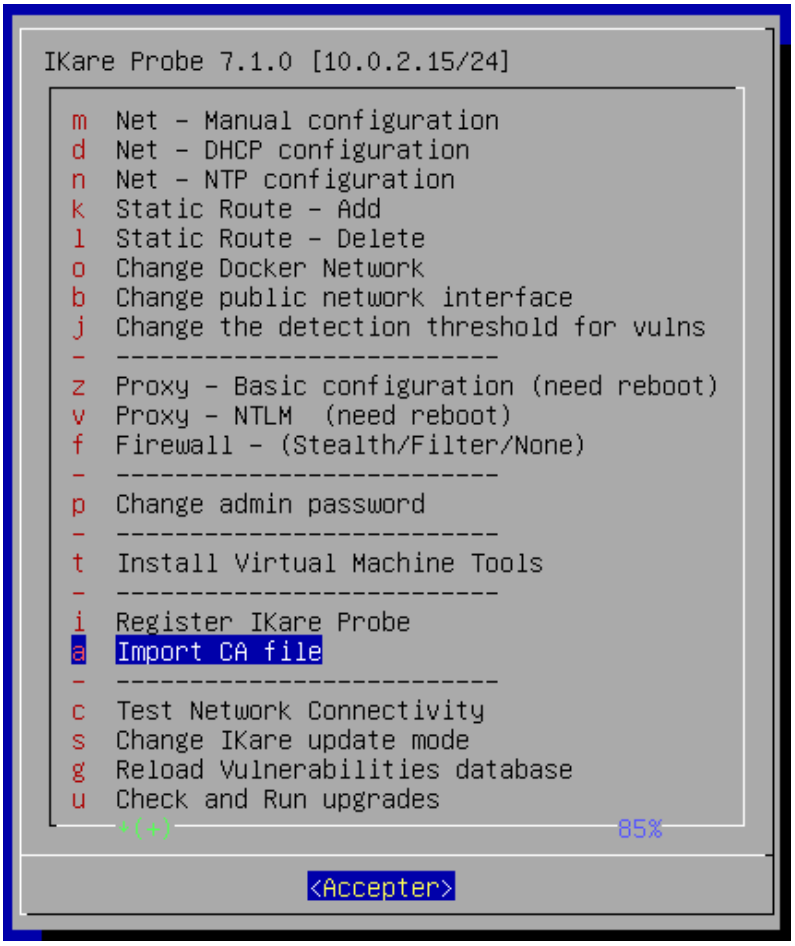
Vous pouvez vous procurer ce certificat racine auprès de l'autorité ayant délivré le certificat pour votre organisation.



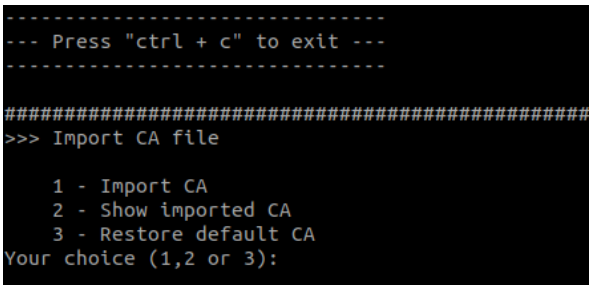
🆘 En cas de problème lors de cette configuration, le support ITrust peut vous aider dans le déploiement de vos propres certificats.

1.3.2 Imports des certificats sur une sonde IKare

Pour cela, sélectionnez l'entrée "**Import CA file**" dans le menu et suivez les instructions.



Si vous avez généré vos propres certificats et que vous les avez importés sur votre IKare Master, il est nécessaire d'importer le certificat de l'autorité de certification (CA) sur votre sonde IKare. Vous devez importer, comme décrit dans le paragraphe ci-dessus la chaine complète de certification de votre CA.

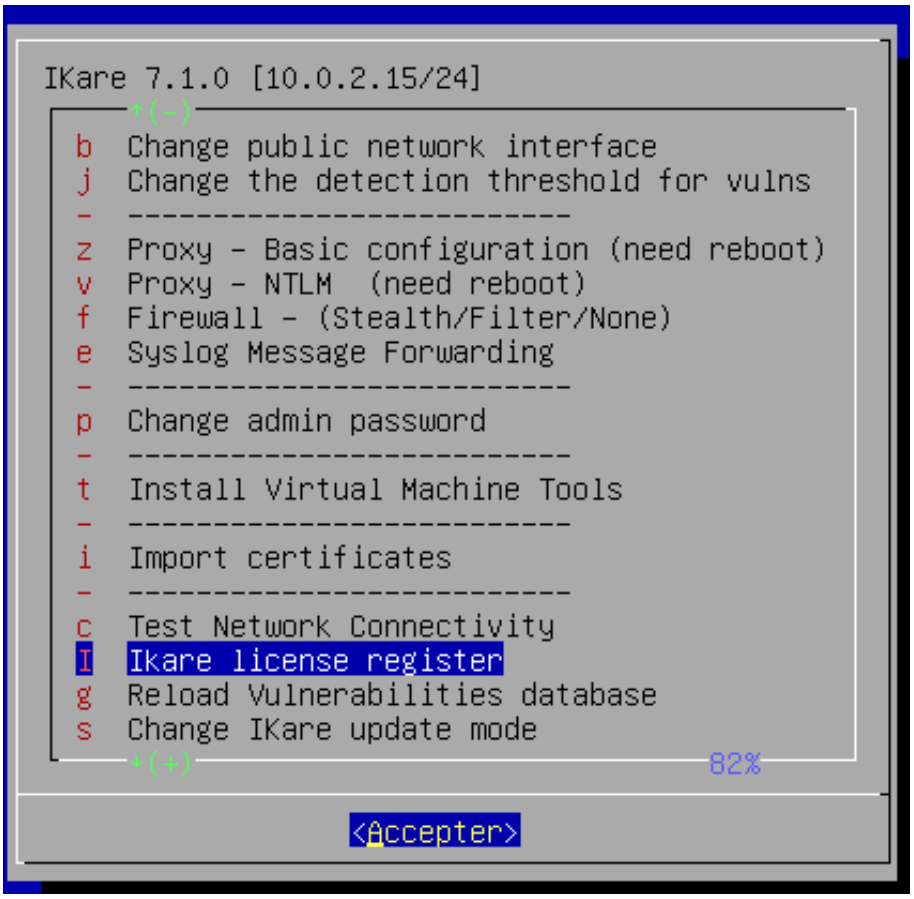


SOS En cas de problème lors de cette configuration, le support ITrust peut vous aider dans le déploiement de vos propres certificats.

1.4 Connexion Web

1.4.1 Prérequis

IMPORTANT: En premier lieu, veuillez entrer le numéro de licence qui vous a été fourni par mail.



Pour cela, sélectionnez l'entrée "**Ikare license register**" dans le menu et rentrez le numéro et cliquez sur entrée.

1.4.2 Interface Web

L'interface utilisateur est accessible depuis votre navigateur avec l'URL du serveur IKare :

https://aaa.bbb.ccc.ddd Note : L'adresse IP d'IKare est accessible sur la console ou en haut du menu d'administration.

IKare a été validé avec les navigateurs suivants :

- Microsoft Edge (13.10122 ou supérieur)
- Mozilla Firefox (31.0 ou supérieur)
- Google Chrome (38.0.2125 ou supérieur)

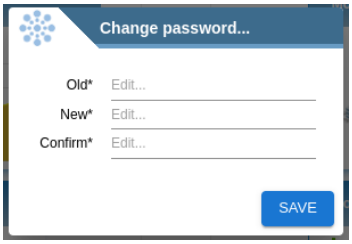
Pour utiliser l'interface web d'IKare, il est nécessaire :

- D'avoir JavaScript activé
- D'autoriser un cookie de session

1.4.3 Connexion

Le compte par défaut est "**admin**" et son mot de passe est "**admin**".

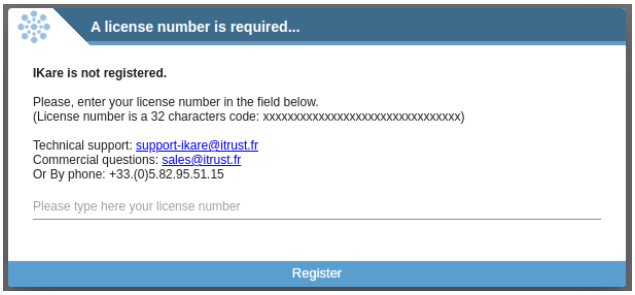
ℹ️ **Note** : Il vous sera demandé de changer le mot de passe par défaut lors de votre première connexion.



1.4.4 Licence

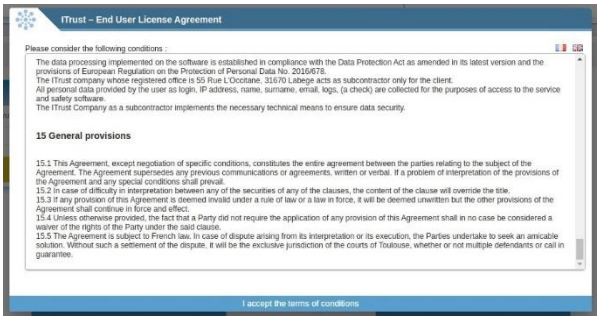
Lors de la toute première connexion à IKare, un numéro de licence vous est demandé pour enregistrer le produit. Le numéro de licence vous est fourni lors de l'inscription en ligne.

ℹ️ **Note :** Une connexion internet vers le serveur license.itrust.fr sur le port 443 est nécessaire pour utiliser IKare.



1.4.5 Conditions de ventes et d'utilisation

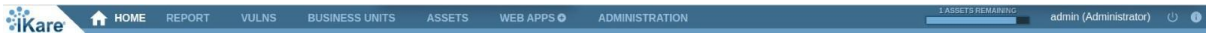
Chaque utilisateur de type '**administrateur**' doit lire et accepter les conditions générales de vente d'IKare lors de sa première connexion.



Chaque utilisateur doit lire et accepter les **conditions générales d'utilisation** d'IKare lors de sa première connexion.

1.4.6 Présentation de l'interface

Après connexion, IKare affiche l'interface utilisateur avec un bandeau de navigation :



Ce bandeau regroupe différentes sections :

- L'onglet **HOME** (vue par défaut lors de la connexion à l'interface) : indicateurs synthétisant les données
- L'onglet **REPORT** : tableau de bord représentant la répartition des vulnérabilités
- L'onglet **VULNS** : vue des vulnérabilités actives sur IKare
- L'onglet **BUSINESS UNITS** : tableau de bord représentant les Business Units, ou groupes
- L'onglet **ASSETS** : vue des équipements découverts et supervisés par IKare
- L'onglet **WEB APPS** : vue des applications web supervisées par IKare
- L'onglet **ADMINISTRATION** : administration de l'interface web IKare
- Un récapitulatif de l'utilisation de la licence
- L'utilisateur connecté et un bouton de déconnexion
- Un accès au changelog et aux nouveautés techniques

Vous trouverez également en pied de page une sélection de petits drapeaux afin de vous permettre de choisir la langue souhaitée. Vous avez le choix entre Anglais et Français.

1.5 Connexion API

L'API est accessible par l'URL https://user:password@aaa.bbb.ccc.ddd:port/api/v2 Vous pouvez retrouver sa documentation dans la partie licence ou à l'adresse https://aaa.bbb.ccc.ddd/doc

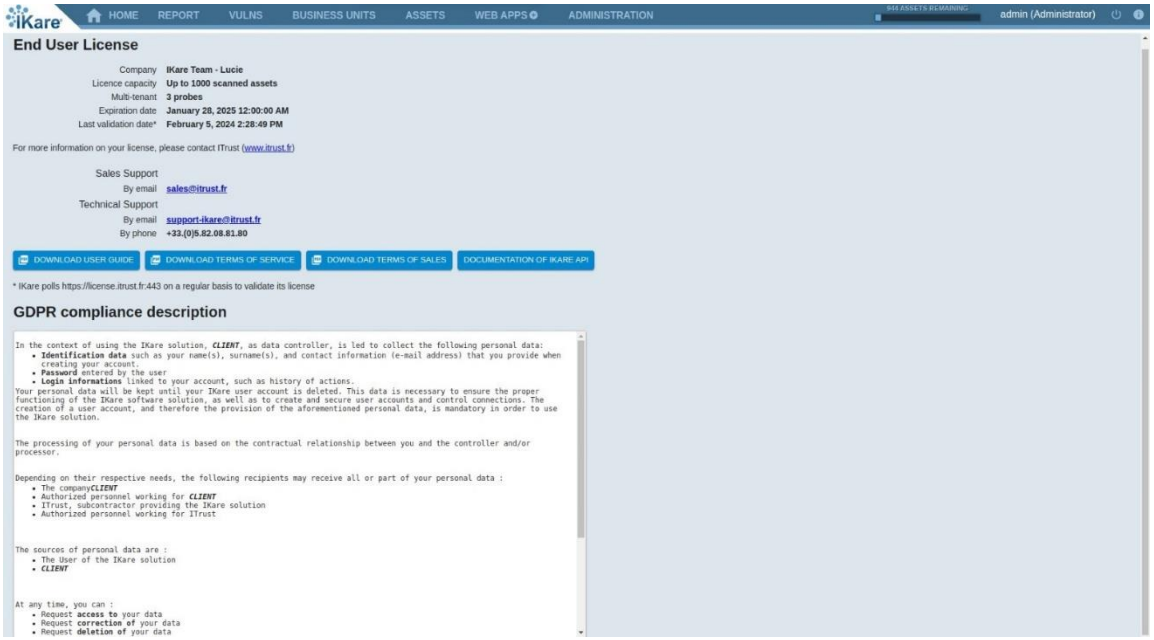
ℹ️ **Note :** Il peut y avoir des problèmes de connexion, dans le cas où le mot de passe contient des "%".

1.6 Administration

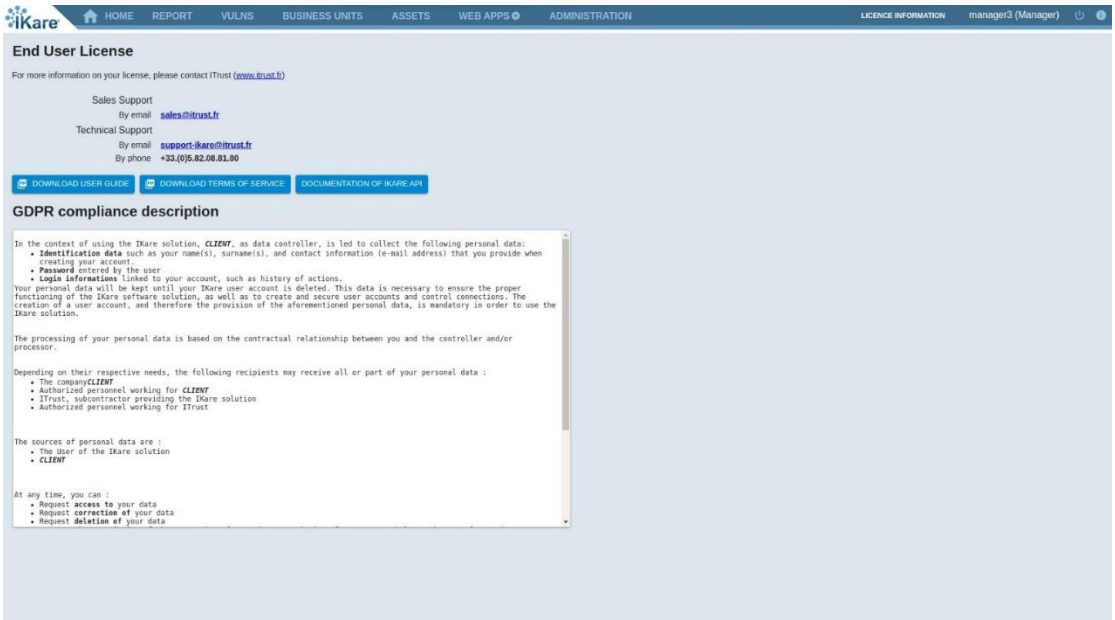
1.6.1 Licence

En cliquant sur l'indicatif de la licence dans le bandeau supérieur, les informations de la licence s'affichent en fonction du rôle de l'utilisateur.

→ Pour un utilisateur "**administrateur**", le détail de la licence est complet :

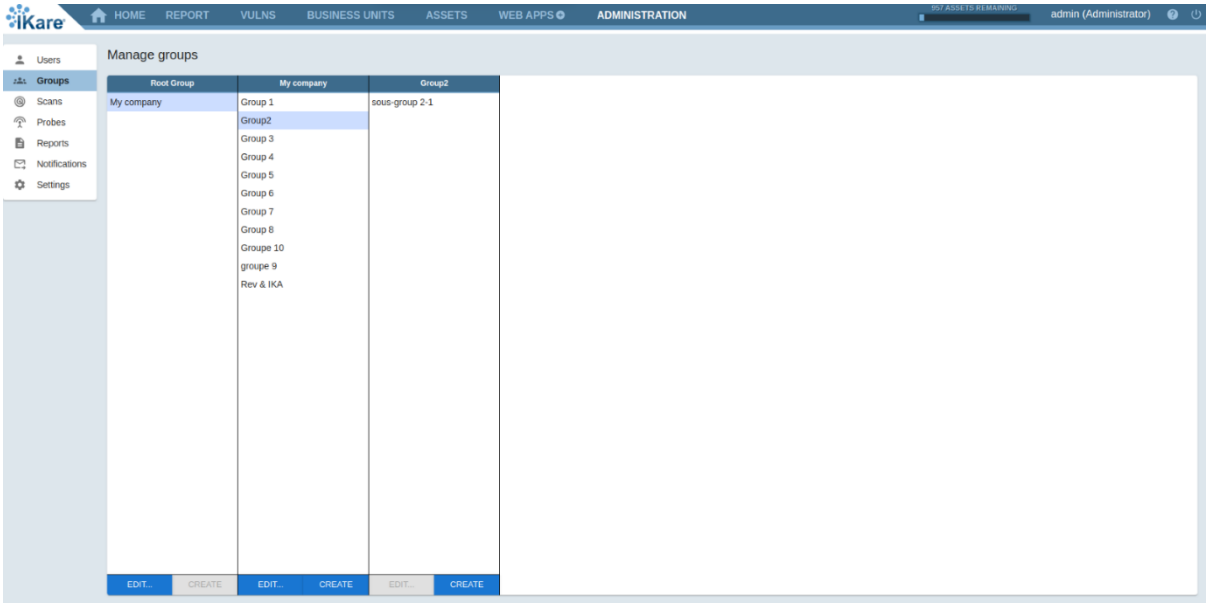


→ Pour un utilisateur "**manager**", "**opérateur**" ou simple "**utilisateur**", le détail de la licence est restreint aux informations suivantes :

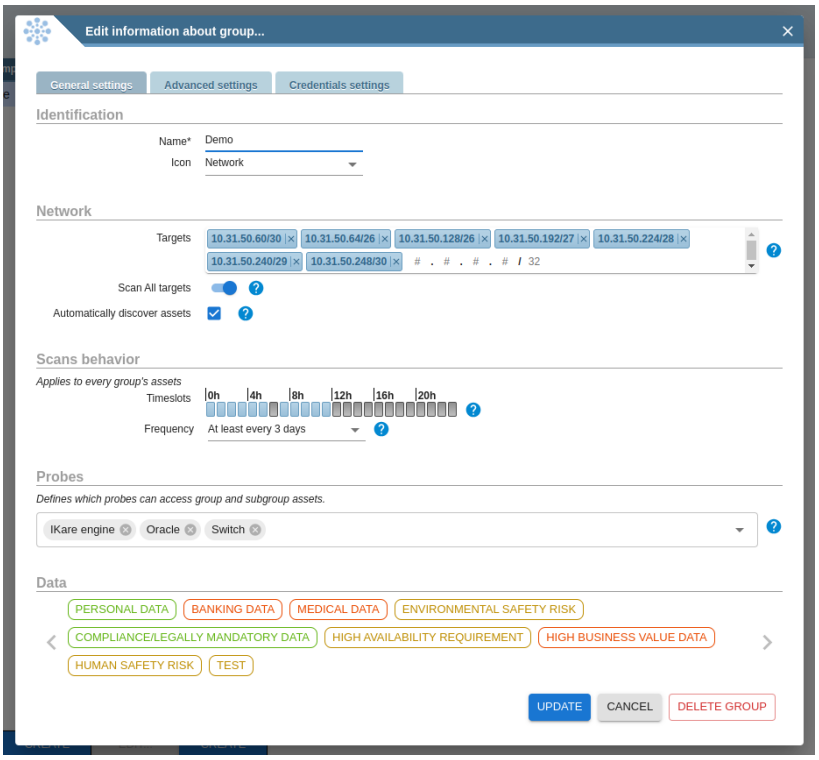


1.6.2 Groupes

Dans cette section vous pouvez définir et gérer vos Business Units (groupes d'équipements).



Les groupes peuvent être modifiés via le bouton "**EDIT**" ou en double cliquant sur leur nom.

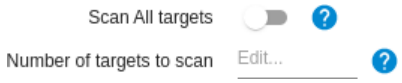


Configurations générales

Les informations suivantes sont configurables :

- **Name** : le nom du groupe (nom affiché dans l'onglet Business Units)
- **Icon** : l'icône affichée pour le groupe dans l'onglet Business Units
- **Targets** : définition des cibles à superviser (adresses IP ou masques réseau)

  ℹ️ **Note** : IKare accepte les listes de réseaux ou adresses séparées par des symboles.
- **Scan All targets** : possibilité de limiter le nombre d'équipements scannés dans le groupe. Par défaut, tous les équipements du groupe peuvent être scannés. En désactivant ce paramètre, un nouveau champ apparait afin de permettre la saisie du nombre d'équipements maximums qui seront scannées dans le groupe. (Number of targets to scan)



- **Automatically discover assets :** découverte automatique des cibles

ℹ️ **Note** : Pour qu'une cible apparaisse dans l'interface et soit scannée, elle doit au moins être découverte dans un des groupes (ou sous-groupe) la contenant.

- **Timeslots** : définit les tranches horaires pendant lesquelles IKare peut scanner les équipements
- **Frequency** : définit la fréquence de scan des équipements

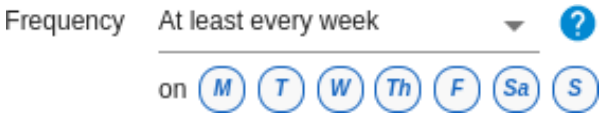
ℹ️ **Note** : les paramètres timeslots et frequency sont hérités des groupes parents. Un groupe fils ne peut que réduire les timeslots. Un groupe fils ne peut que réduire le délai entre deux scans.

Le moteur de planification d'IKare s'organise pour scanner les cibles dans le temps et la fréquence impartis. Dans le cas où il y aurait trop de cibles pour la fréquence choisie, les cibles ignorées seront scannées en priorité dès qu'une plage sera disponible.

Il est possible d'affiner les jours de scans autorisés lorsque la fréquence de scan est définie entre une fois par semaine et une fois par mois.

Cas : une fois par semaine / une fois toutes les 2 semaines

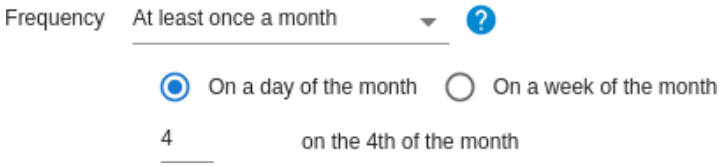
Lorsque la fréquence est définie sur un scan une fois par semaine (ou une fois toutes les deux semaines), il est possible de sélectionner le ou les jours pendant lesquels les scans pourront se lancer :



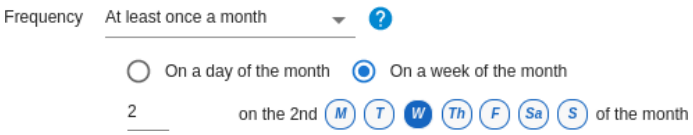
Cas : une fois par mois

Lorsque la fréquence est définie sur un scan une fois par mois, il est possible de sélectionner une configuration plus précise sur le déclenchement des scans en spécifiant :

- Un jour donné dans le mois



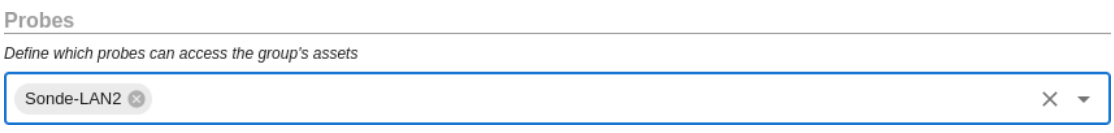
- Un jour donné dans une des semaines du mois (Exemple : 2ème mercredi du mois)



ℹ️ **Note 1 :** Il est possible de laisser les cibles d'un groupe vide et déclarer les cibles directement dans ses sous-groupes. Les cibles sont néanmoins héritées des groupes parents.

ℹ️ **Note 2 :** Si une cible d'un sous-groupe ne fait pas partie des cibles du ou de l'un des groupes parents, celle-ci n'est pas enregistrée.

Dans le cas d'une licence multisondes, il est également nécessaire de configurer les sondes qui auront accès au groupe sélectionné pour permettre la découverte et le scan des machines concernées.



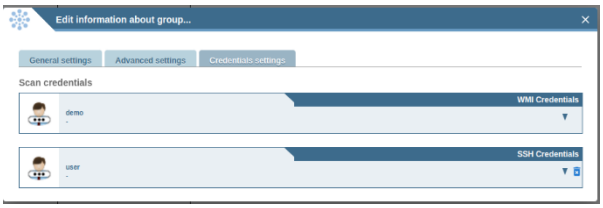
Le nom de ces sondes est auto-complété.

ℹ️ **Note** : Il est possible de laisser les sondes d'un groupe vides et déclarer les cibles directement dans ses sous-groupes. Les sondes sont néanmoins héritées des groupes parents.

Enfin, vous avez la possibilité de sélectionner des types de données (tags), afin de pondérer la note de vos équipements présents dans le groupe, selon le type de données qu'il contient.

Configurations d'identifiant de scan

Dans cet onglet de configuration ("**Credentials settings**"), il est possible de définir des identifiants afin d'effectuer des scans authentifiés sur les équipements présents dans le groupe.



Chaque groupe peut posséder un identifiant WMI (de la forme identifiant/mot de passe) et/ou un identifiant SSH (de la forme identifiant/mot de passe ou identifiant/clé privée).

Dans le cas d'un identifiant Active Directory, celui-ci peut prendre la forme "**username@domain**" ou "**domain\username**".

Dans le cas d'un identifiant SSH avec clé privée, il est nécessaire que la clé privée enregistrée dans IKare soit une clé RSA au format PEM.

Voici des exemples de génération de clé privée / publique en utilisant les outils openssl / ssh-keygen. L'identifiant sur la machine à scanner est appelé user dans les exemples ci-dessous :

- Génération de la paire de clé privée / publique :
  - Clé privée : openssl genrsa -out private-key.pem 2048
  - Clé publique associée : openssl rsa -in private-key.pem -pubout -out public-key.pem

ℹ️ **Note 1 :** C'est le contenu du fichier private-key.pem qu'il est nécessaire d'enregistrer sur l'interface d'IKare

- Enregistrement de la clé publique sur la machine scannée :
  - ssh-keygen -i -m PKCS8 -f public-key.pem >> /home/user/.ssh/authorized_keys

ℹ️ **Note 2 :** Si vous disposez d'une clé SSH de type RSA générée avec avec ssh-keygen, vous pouvez la transformer au format PEM en utilisant les commandes suivantes :

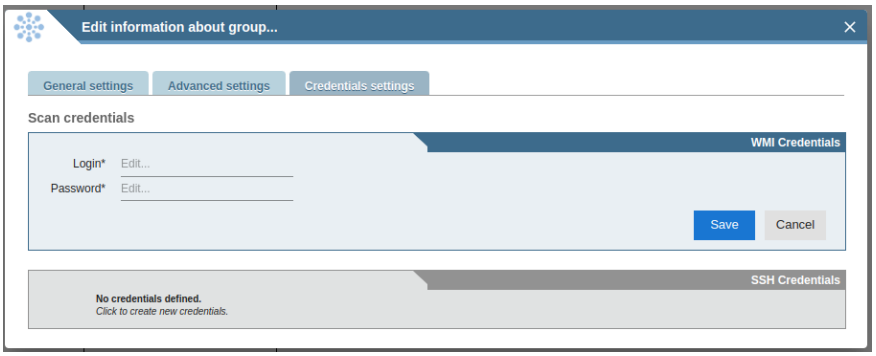
→ Copie de votre clé privée RSA générée avec keygen : cp id_rsa private-key.pem

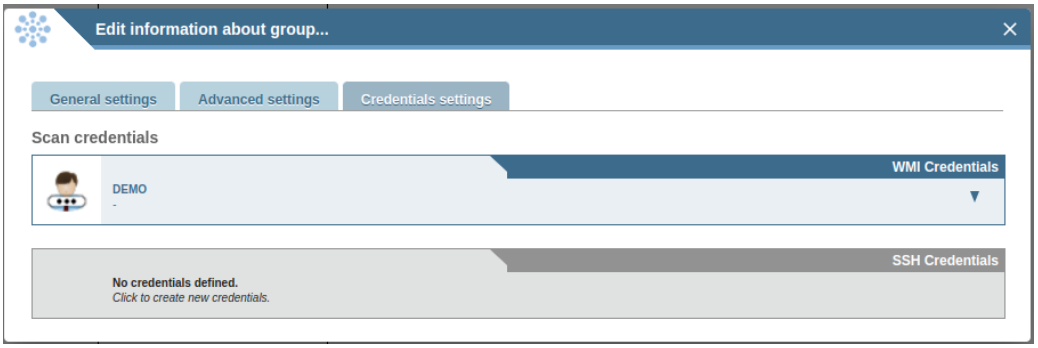
- Transformation de votre clé privée en PEM : ssh-keygen -p -N "" -m pem -f private-key.pem Le comportement de ces vignettes est le suivant :
- Si un identifiant est défini sur le groupe actuel, alors ce dernier y sera affiché.

- Sinon la vignette apparait grisée, signifiant qu'aucun identifiant n'a été défini.

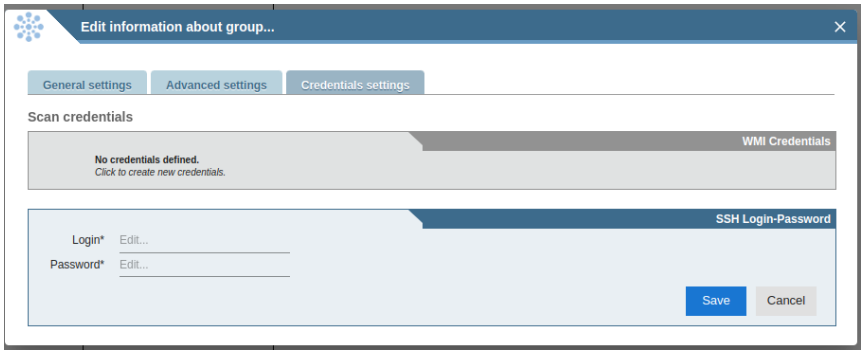
Si aucun identifiant n'a été défini sur le groupe actuel, alors il est possible d'en créer un. Pour cela, il suffit de cliquer sur la vignette correspondant au type voulu (WMI ou SSH). Un formulaire apparaitra, dans lequel vous pourrez saisir les informations demandées.

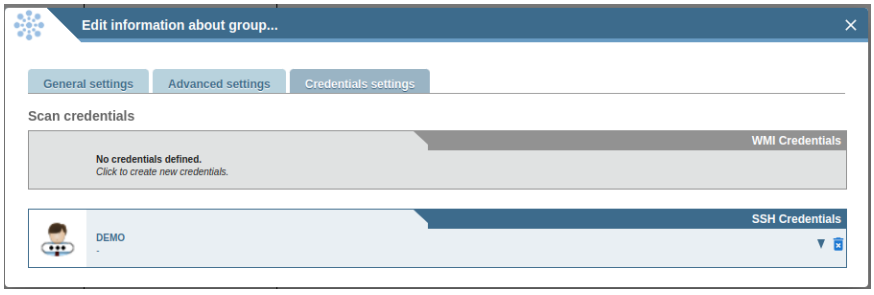
- Enregistrement d'identifiants WMI :





- Enregistrement d'identifiants SSH :



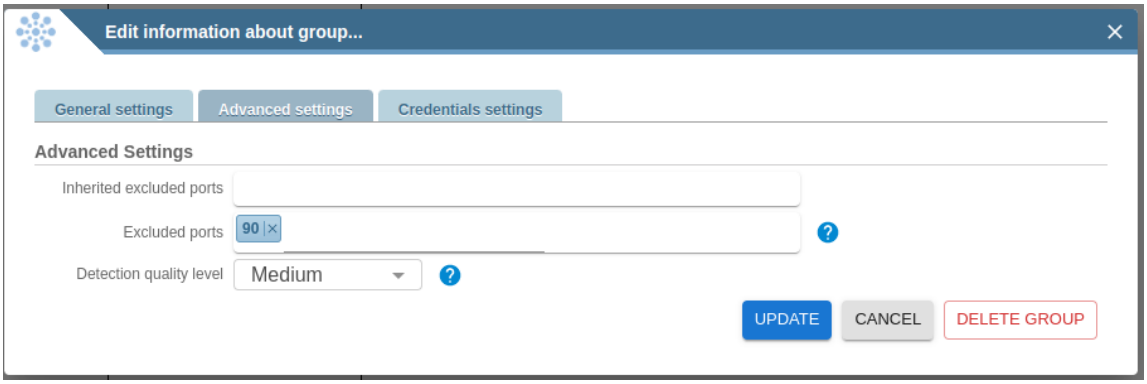


Si un identifiant est défini sur le groupe actuel, il n'est plus possible de créer un nouvel identifiant pour le type concerné. Il faut au préalable supprimer l'identifiant avant de pouvoir effectuer cette action. Pour cela, il suffit de cliquer sur l'icône représentant une corbeille.

ℹ️ **Note :** Il est possible de définir les identifiants utilisés par les scans authentifiés directement sur les équipements (Voir 3.2. Assets – Présentation détaillée – Onglet Settings).

Configurations avancées

Dans cet onglet de configuration (“**Advanced settings**”), il est possible de définir des configurations avancées de scan pour les équipements du groupe.

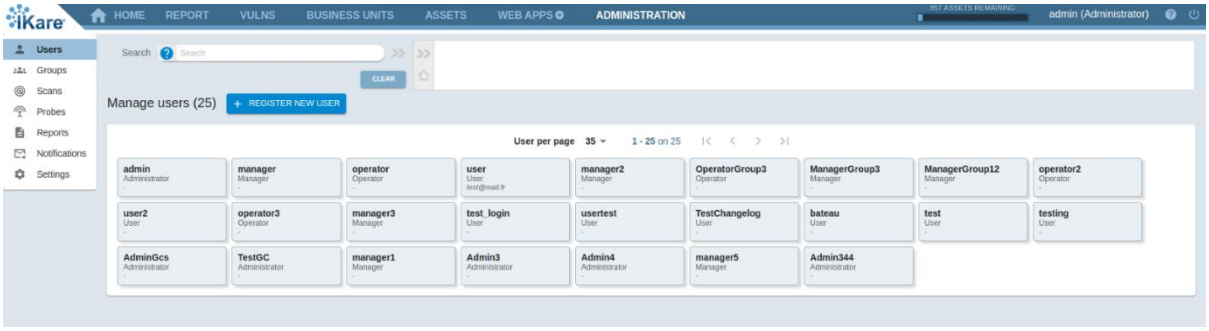


- **Excluded ports** : possibilité de définir des ports et/ou plages de ports à exclure lors de la réalisation des scans sur les équipements du groupe. Les plages de ports doivent être saisies avec le séparateur - entre le premier port à exclure et le dernier. Exemple : 22-55 (=> Exclusion des ports 22 à 55)
- **Detection quality level** : possibilité de définir le niveau de qualité de détection minimal à prendre en compte dans la remontée des vulnérabilités sur les équipements du groupe. Par défaut, IKare remonte toutes les vulnérabilités détectées, qu’elles aient une qualité de détection faible, moyenne ou forte. En sélectionnant un seuil dans la liste déroulante (Low [par défaut], Medium ou High), IKare ne fera remonter que les vulnérabilités ayant une qualité de détection égale ou supérieure à la valeur sélectionnée

ℹ️ **Note :** Le champ **Inherited excluded ports** affiche les ports / plages de ports qui ont été exclus dans le groupe parent du groupe courant.

1.6.3 Utilisateurs

Dans cette section, vous pouvez définir et administrer les utilisateurs d'IKare:



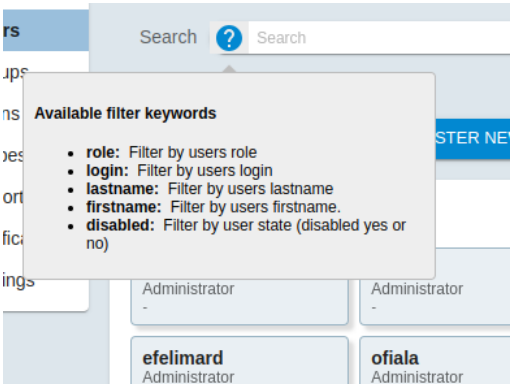
Bandeau supérieur

Le bandeau supérieur de l'administration des utilisateurs permet de filtrer et d'accéder rapidement aux informations souhaitées :

Une pagination des utilisateurs est disponible pour afficher un nombre convenable d'utilisateurs sur une page.

Recherche

Ce champ permet de filtrer les utilisateurs en fonction de mots clés prédéfinis et de sauvegarder des vues.



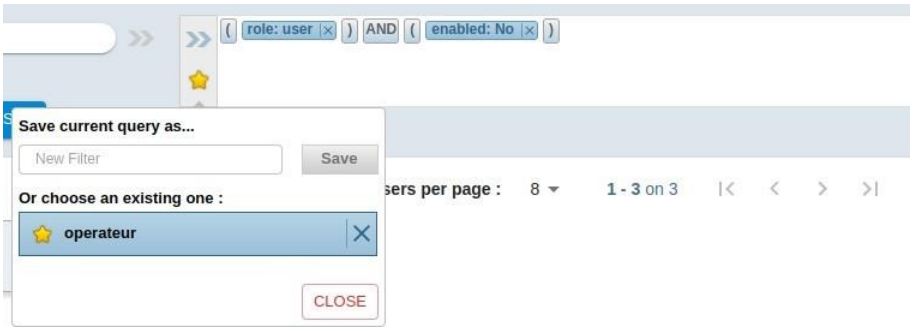
Les mots clés possibles sont :

- **role** : Rechercher par rôle d'utilisateur (administrateur, manager, opérateur, utilisateur)
- **login** : Rechercher par nom d'utilisateur (le caractère joker * peut être utilisé)
- **lastname** : Rechercher par nom de famille (le caractère joker * peut être utilisé)
- **firstname** : Rechercher par prénom (le caractère joker * peut être utilisé)
- **enabled** : Rechercher en fonction de l'état des utilisateurs (actif ou non)

Une fois complet, le schéma de recherche est ajouté dans le champ de droite qui représente les filtres actifs. Si plusieurs schémas de recherche sont ajoutés, ils se complètent selon la règle suivante :

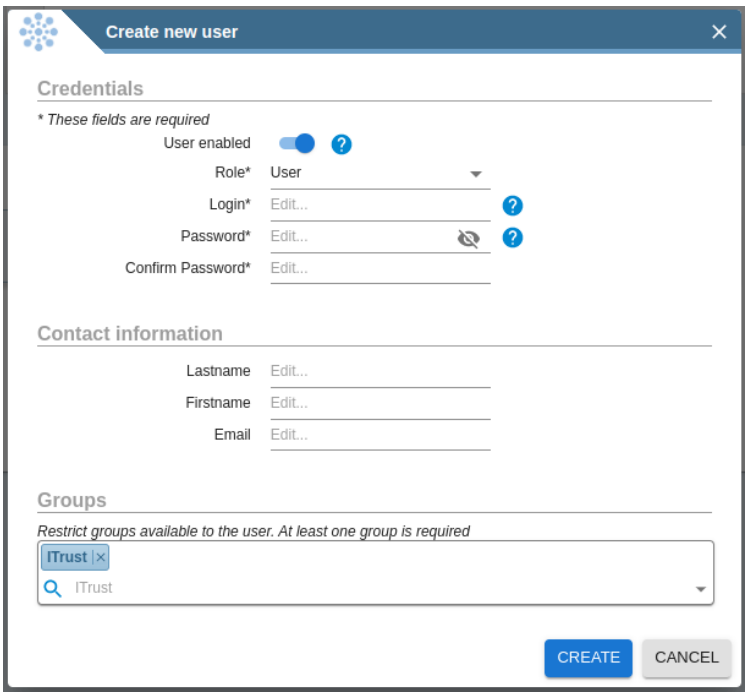
- 2 schémas avec des mots clés différents sont liés par un ET
- 2 schémas avec le même mot clé sont liés par un OU

Les filtres qui vous conviennent, peuvent être sauvegardés sous forme de vue que vous pouvez retrouver avec l'étoile :



Création d'un nouvel utilisateur

Pour créer un nouvel utilisateur, cliquez sur le bouton "**register new user**". Pour éditer un utilisateur existant, cliquez sur sa vignette.



Les informations suivantes sont configurables :

- Etat : Etat de l'utilisateur (User enabled)

ℹ️ **Note :** L'utilisateur ne pourra se connecter à l'interface web d'IKare que s'il est actif

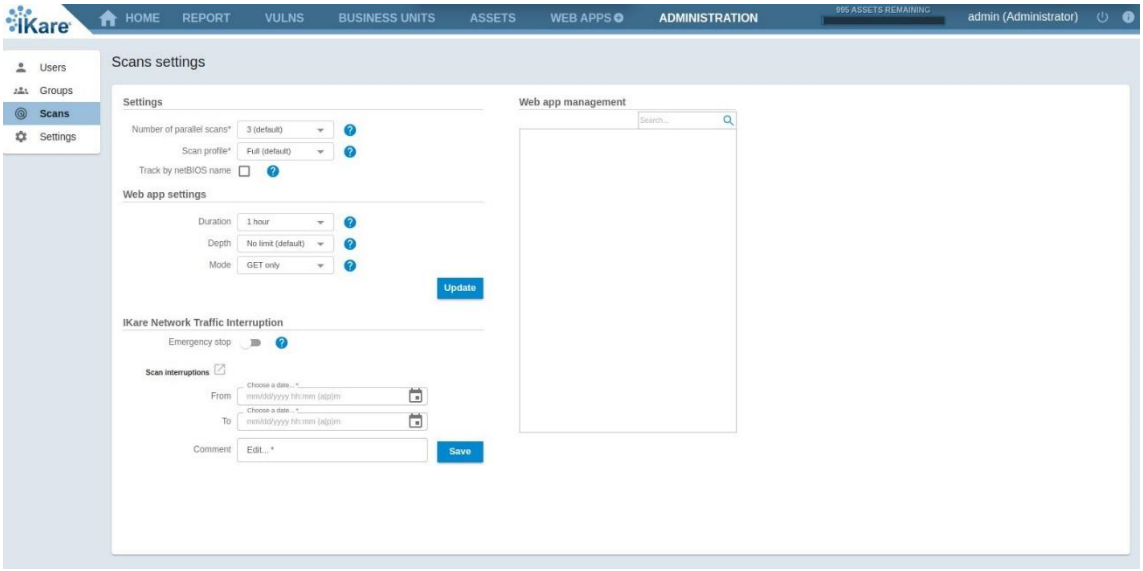
- Rôle : rôle de l'utilisateur

ℹ️ **Note :** Les ACLS sont définies comme suit :

- **Administrator :** il a tous les droits sur IKare (gestion de la licence, des mises à jour, des groupes et des utilisateurs).
- **Manager :** il est responsable d'un groupe (gestion du groupe, des sous-groupes, des utilisateurs et des équipements), mais ne peut pas modifier son groupe racine.
- **Operator :** il peut gérer des équipements (déclencher ou arrêter un scan, renommer un équipement ou ignorer une vulnérabilité).
- **User :** il peut consulter IKare (consultation de l'interface et génération du rapport).
- **Login :** nom utilisé pour se connecter
- **Password :** mot de passe du compte
- **Lastname :** [optionnel] nom de l'utilisateur
- **Firstname :** [optionnel] prénom de l'utilisateur
- **Email :** [optionnel] adresse courriel de l'utilisateur
- **Groups :** groupes auxquels l'utilisateur a accès. Les groupes sont auto-complétés.

1.6.4 Scans

Dans cette section, vous pouvez définir les paramètres de scans d'IKare.



Note 1 : Seul un administrateur peut accéder à cette page.

Note 2 : Les parties "Settings" et "Webapp scan settings" ne sont pas disponibles dans le cas d'une licence multisondes, la configuration se fait au niveau de chaque sonde dans la partie "Probes".

Pour la partie "**Settings**", les informations suivantes sont configurables :

- **Number of parallel scans** : Nombre de scans qui s'exécuteront en parallèle (3 par défaut)
- **Scan profile** : Profondeur du scan (nombre de ports scannés)
- **Track by Netbios :** Activer le tracking par NETBIOS, permettant de suivre les changements d'IP d'une machine identifiée par son nom NETBIOS

Le champ "**Scan profile**" peut contenir les valeurs suivantes :

- **Light** (100 TCP ports and 10 UDP ports)
- **Standard** (1000 TCP ports and 30 UDP ports)

Note : Cette option est à privilégier pour les scans au travers d'un firewall ou pour les scans externes

- **Full - default** (65535 TCP ports and 69 UDP ports)

ℹ️ **Note :** Cette option est à privilégier pour auditer les équipements internes et identifier les services suspects

La partie "**Web app settings**" vous permet de paramétrer les scans qui seront effectués sur les applications web supervisées.

- **Duration** : Durée maximale d'un scan
- **Depth** : Profondeur maximale du scan. Par exemple, une profondeur de 2 résultera en un scan sur uniquement 2 niveaux de l'application web (i.e. la page d'accueil et une page accessible depuis la page d'accueil)
- **Mode** : Type de requête qui sera utilisé lors du scan d'une application web (GET uniquement, conseillé pour une application en production ou GET + POST, conseillé pour une application en cours de recette).

Pour finir, la partie "**Web app management**" vous permettra de gérer facilement des applications web dans IKare. Il s'agit de toutes les applications répertoriées, non archivées. Il est alors possible d'en ajouter de nouvelles ou d'en supprimer (elles seront alors archivées). Le champ de recherche vous permettra de repérer rapidement l'application désirée.

Pour ajouter une application web, il est nécessaire que l'équipement l'hébergeant soit connu d'IKare. Dans le cas contraire, se référer à la section 2.4.1.

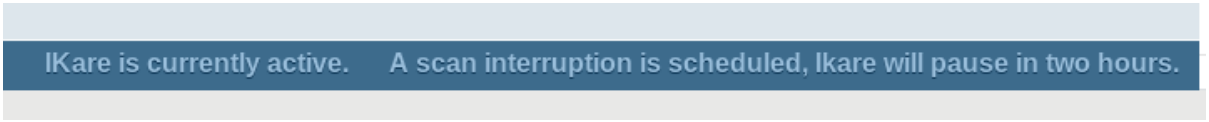
Dans la partie "**Ikare Network Traffic Interruption**", il vous est possible de programmer une période durant laquelle aucun scan ne sera effectué et où le processus de découverte d'IKare sera suspendu. Pour cela, les informations suivantes doivent être renseignées :

- **From** : Date et heure du début de l'interruption
- **To** : Date et heure de la fin de l'interruption
- **Comment** : Commentaire optionnel détaillant la raison de l'interruption

ℹ️ **Note :** Lors de la création d'une interruption, la durée est définie à 24 heures par défaut.

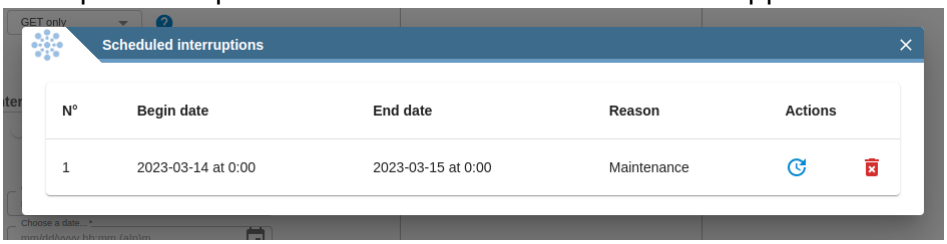
Il est également possible d'activer le "**Troubleshooting mode**" qui correspond à une interruption de scan immédiate, tant que ce mode est actif. (Il est à noter que si certains scans sont en cours lors de l'activation de ce mode, ces derniers seront annulés et marqués comme erronés).

Une fois l'interruption programmée, un indicateur apparaitra dans le pied de page :



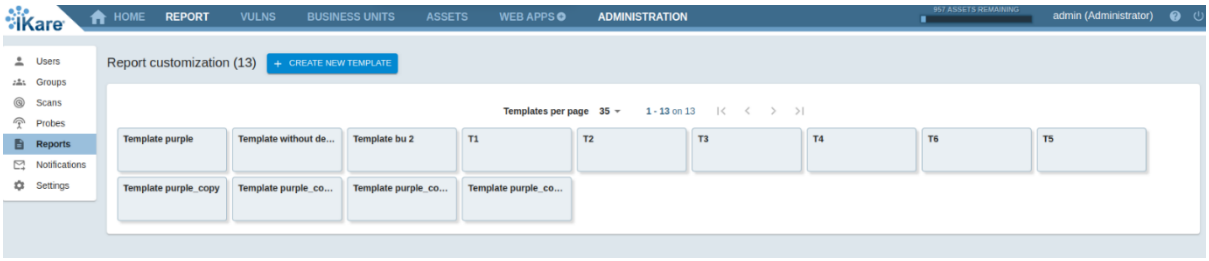
Vous pouvez programmer plusieurs interruptions de scan à l'avance. Vous retrouverez toutes les interruptions programmées en cliquant sur le bouton suivant situé à côté de "**Scan interruptions**" :

Vous pourrez à partir d'ici éditer le commentaire ou supprimer une interruption.

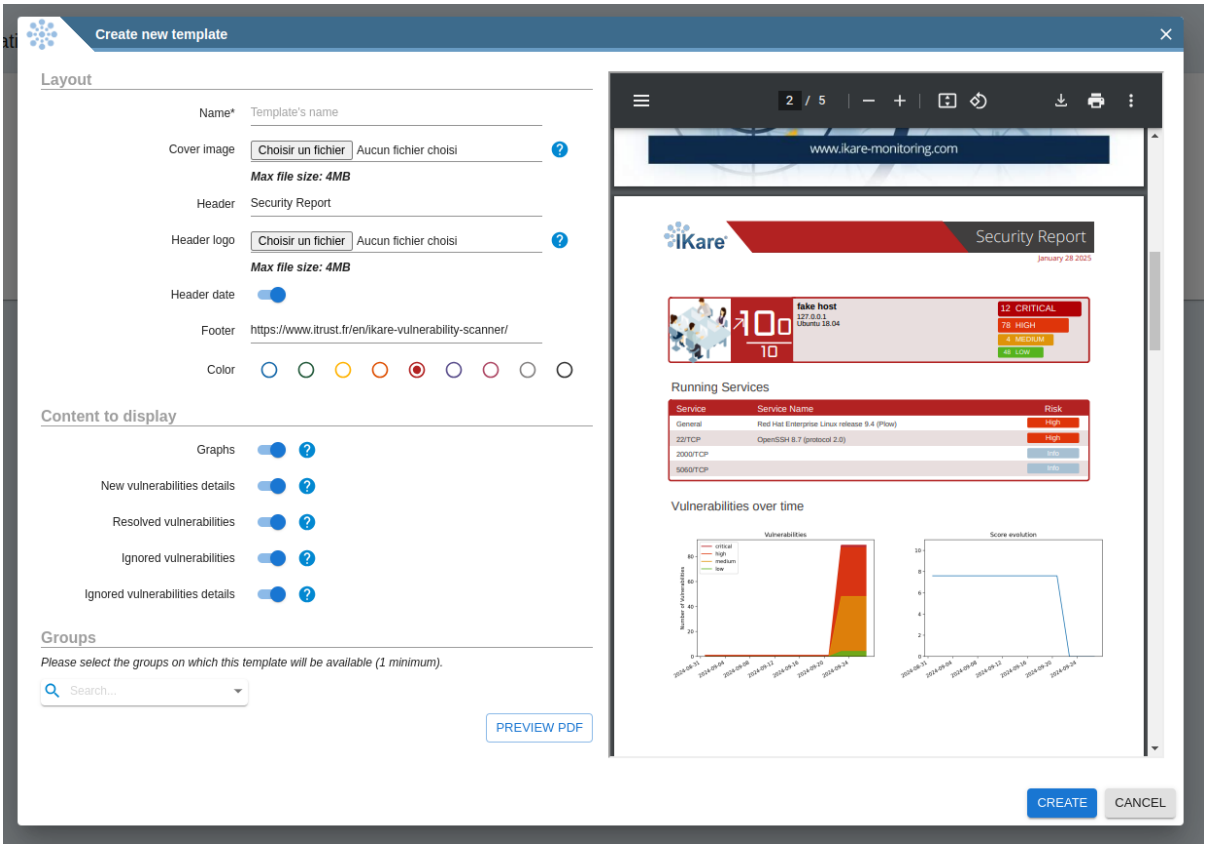


1.6.5 Rapport

ℹ️ **Note 1** : Seul un administrateur ou un manager peut accéder à cette page.



Vous pouvez désormais créer des modèles de rapports personnalisés adaptés aux besoins de votre organisation et les assigner à des groupes spécifiques. Cela permet une gestion plus ciblée et efficace des rapports.



Vous pouvez gérer les paramètres suivants :

- **Name** : Le nom du template
- **Cover image** : La page de garde
- **Header** : Le titre qui sera présent dans l'en-tête de chaque page
- **Header logo** : Le logo dans l'en-tête de chaque page
- **Header date** : La date présente dans l'en-tête

- **Footer** : Texte présent dans le pied de page
- **Color** : La couleur du rapport
- **Graphs** : Présence ou non des graphiques dans le rapport
- **New vulnerabilities details :** La présence ou non du détail des nouvelles vulnérabilités dans le rapport
- **Resolved vulnerabilities :** La présence ou non des vulnérabilités résolues dans le rapport
- **Ignored vulnerabilities** : La présence ou non des vulnérabilités ignorées
- **Ignored vulnerabilities details** : La présence ou non du détail des vulnérabilités ignorées
- **Groups** : Sélection des groupes qui pourront utiliser le template
- **Preview PDF :** Permet d'avoir un aperçu du rapport final

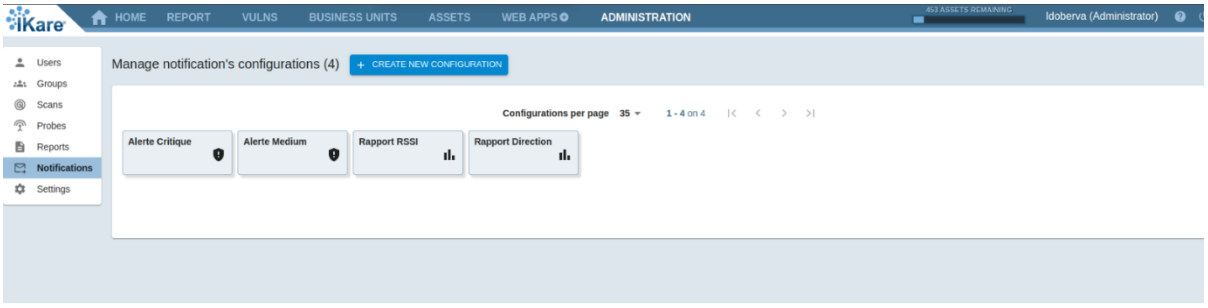
Les utilisateurs des différents groupes n'auront accès qu'aux templates configurés pour leur groupe.

1.6.6 Notification

ℹ️ **Note 1** : Seul un administrateur et un manager peut accéder à cette page.

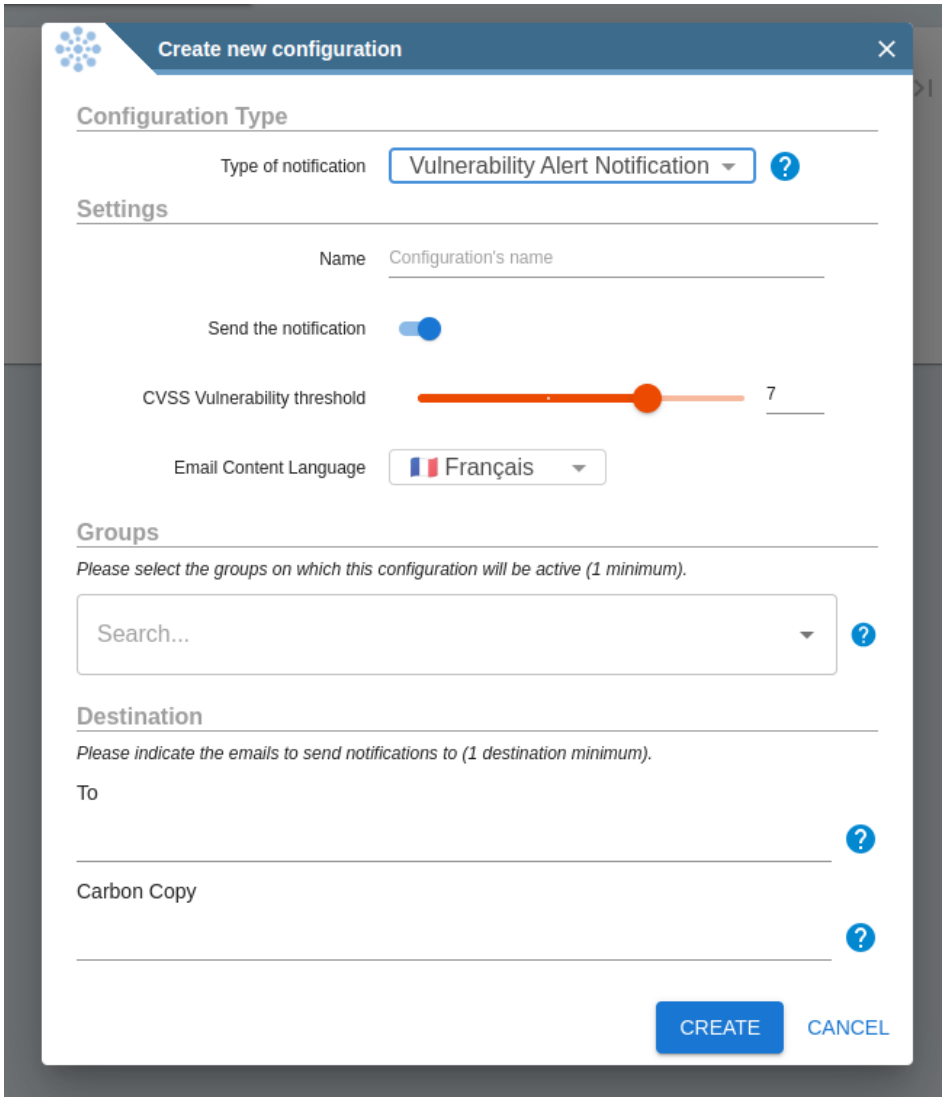
Des notifications par mail peuvent être configurés :

- Les administrateurs et les managers peuvent programmer des alertes par groupe avec des listes de diffusion configurables.
- Les rapports peuvent être envoyés périodiquement pour des groupes, assets ou webapps spécifiques.



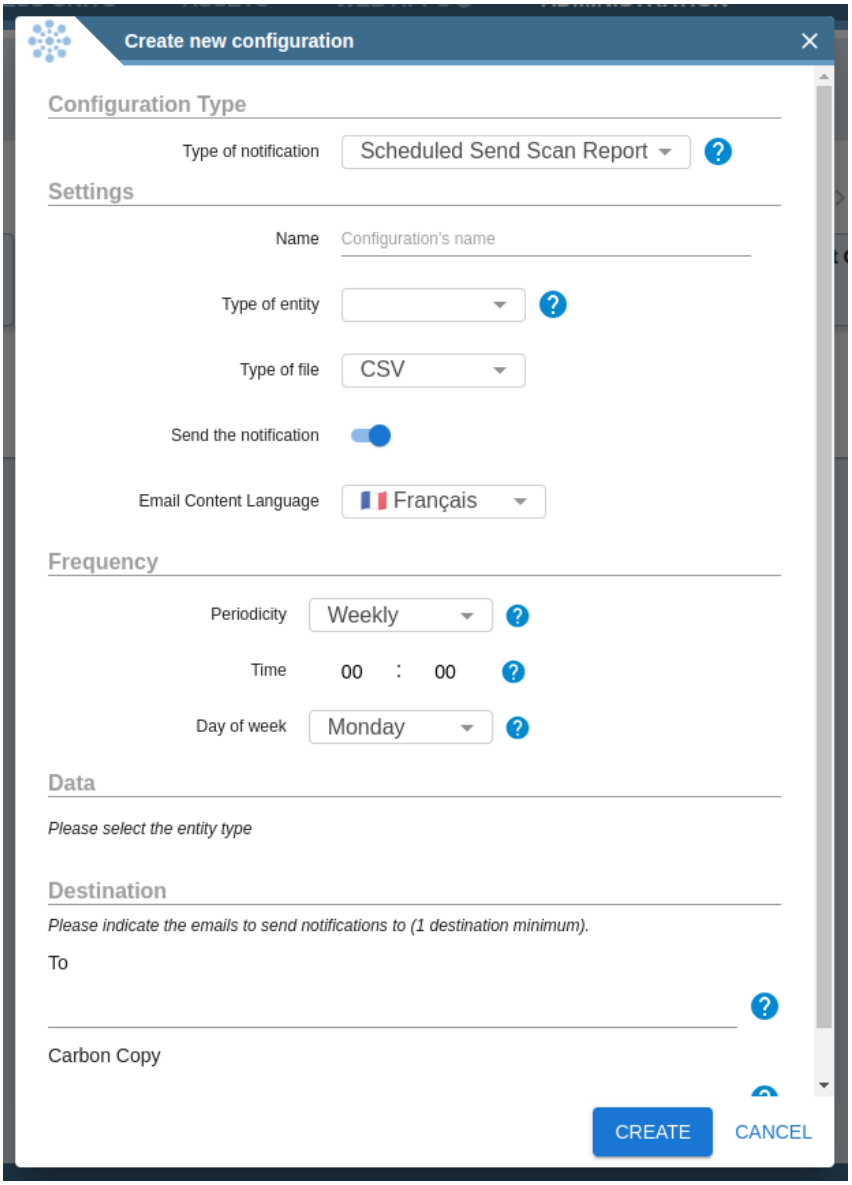
Alertes

Les alertes permettent d'être prévenu par mail, lors de la découverte d'une nouvelle vulnérabilité en fonction du seuil configuré :



- **Type of notification** : Le type de notification ici pour les alertes "Vulnerability Alert Notification"
- **Name** : Nom de la notification
- **Send the notification :** Activation ou non de la notification
- **CVSS Vulnerability threshold :** Seuil de criticité à partir duquel l'alerte sera envoyé
- **Email Content Language** : La langue de l'email
- **Groups :** Le groupe surveillé
- **To :** La liste des adresses emails qui recevront l'alerte
- **Carbon Copy :** La liste des adresses emails en copie

Rapport



- **Type of notification** : Le type de notification ici pour les alertes “Scheduled Send Scan Report”
- **Name :** Nom de la notification
- **Type of entity :** Le type rapport qui sera envoyé (Groupe, Asset, Webapp)
- **Type of file :** Le format du rapport (CSV, PDF, JSON)
- **Send the notification :** Activation ou non de la notification
- **Email Content Language :** La langue de l’email
- **Frequency :** La fréquence à laquelle le mail sera envoyé
- **Data :** Le groupe ou l’asset ou la webapp dont le rapport sera envoyé
- **To :** La liste des adresses emails qui recevront l’alerte
- **Carbon Copy** : La liste des adresses emails en copie

1.6.7 Paramètres

ℹ **Note 1 :** Seul un administrateur peut accéder à cette page.

Paramètres globaux

Dans cette section, vous pouvez définir les paramètres généraux d'IKare.

Configuration des contacts RGPD

Les informations suivantes sont configurables :

- **Company name** : [optionnel] personnalisation du nom de l'organisation ayant souscrit une licence IKare
- **DPO mail contact** : [optionnel] personnalisation de l'adresse email d'un contact référent au sein de l'organisation concernant la protection des données personnelles

ℹ **Note 2** : Les champs ci-dessus (Company name et DPO mail contact) sont utilisés dans la personnalisation de la notice RGPD accessible dans la description de la licence IKare (Voir 2.6.1. Administration – Licence)

Paramètres des tags

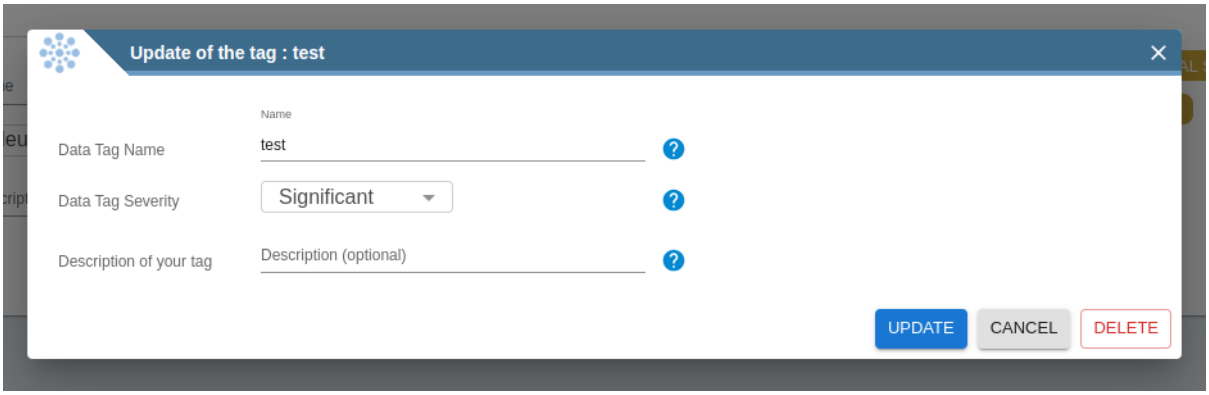
Vous pouvez gérer la création ou la modification de nouveau Tags. Ces tags vous permettent de spécifier le type de données qui peut être présent dans vos groupes ou sur vos équipements directement. En fonction de leur sévérité, une pondération sera appliquée sur vos équipements et diminuera leur note.

- **Data Tag Name** : Le nom du tag que vous voulez créer
- **Data Tag Severity** : La sévérité que vous voulez appliquer
    - *Neutral* : N'applique aucune pondération, utile pour simplement étiqueter un groupe ou un équipement
    - *Minor* : Ajouter une pondération mineure
    - *Significant* : Ajouter une pondération plus significative
    - *Major* : Ajouter une pondération majeure
    - *Critical* : Ajouter une pondération critique
- **Description of your tag** : [optionnel] Vous pouvez noter une courte description de votre tag qui s'affichera au survol de celui-ci

Les Tags par défaut ne sont pas modifiables et s'affichent en gris. S'affichent ensuite les tags que vous aurez rajoutés. Une couleur est appliquée en fonction de sa sévérité.

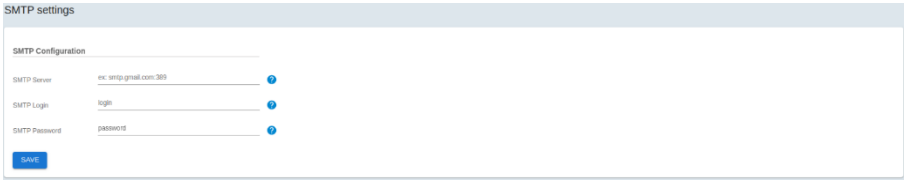
Vous pouvez modifier un tag en cliquant sur l'icône en forme de crayon situé sur les tags

Une fenêtre s'ouvrira avec un formulaire qui reprend les champs précédents, vous permettant de faire les modifications souhaitées.



Paramètres SMTP

Vous pouvez configurer un serveur smtp afin de recevoir des alertes ou des rapports de scan par mail.



- **SMTP Server** : l'adresse de votre serveur smtp
- **SMTP Login** : le login de votre serveur smtp
- **SMTP Password** : le mot de passe de votre serveur

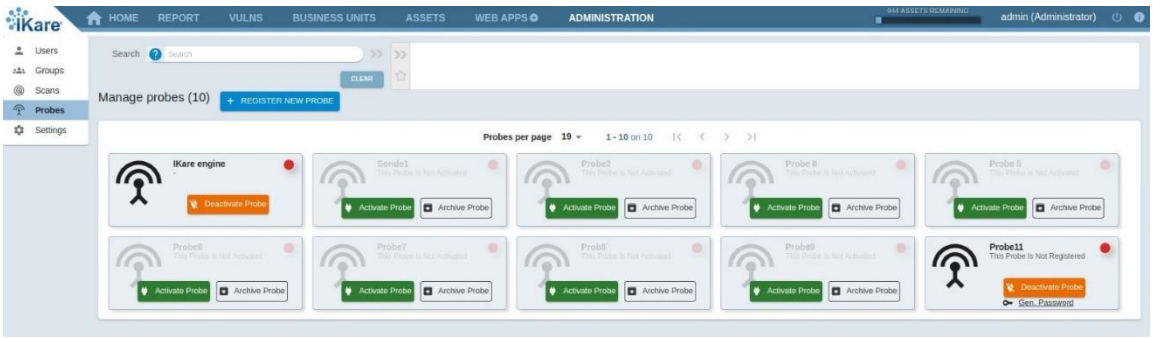
1.6.8 Sondes

Cette section n'est disponible qu'à partir du moment où vous disposez d'une licence multisondes. Dans cette section vous pouvez gérer les paramètres de scans des différentes sondes.

Seuls les administrateurs peuvent accéder à cette section de configuration.

Bandeau supérieur

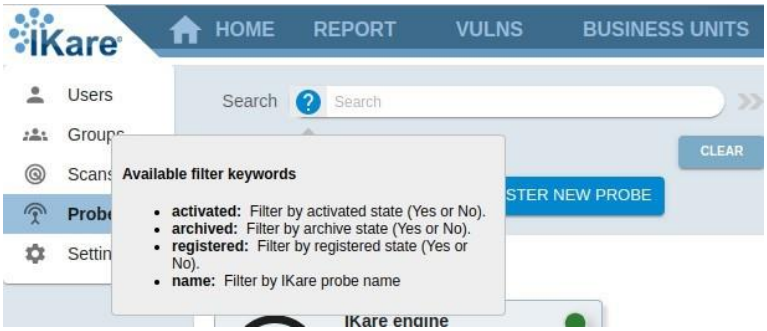
Le bandeau supérieur de l'administration des sondes permet de filtrer et d'accéder rapidement aux informations souhaitées :



Une pagination des sondes est disponible pour afficher un nombre convenable de sondes sur une page.

Recherche

Ce champ permet de filtrer les sondes en fonction de mots clés prédéfinis et de sauvegarder des vues.

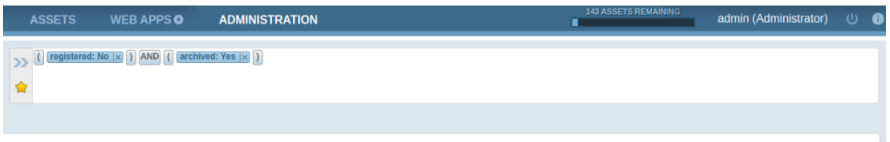


Les mots clés possibles sont :

- **activated** : Rechercher par statut d'activation d'une sonde (activée ou non)
- **archived** : Rechercher par statut d'archive d'une sonde (archivé ou non)
- **registered** : Rechercher par état d'enregistrement d'une sonde (enregistrée ou non)
- **name** : Rechercher par nom d'utilisateur (le caractère joker * peut être utilisé)

Une fois complet, le schéma de recherche est ajouté dans le champ de droite qui représente le filtre actif. Si plusieurs schémas de recherche sont ajoutés, ils se complètent selon la règle suivante :

- 2 schémas avec des mots clés différents sont liés par un ET
- 2 schémas avec le même mot clé sont liés par un OU



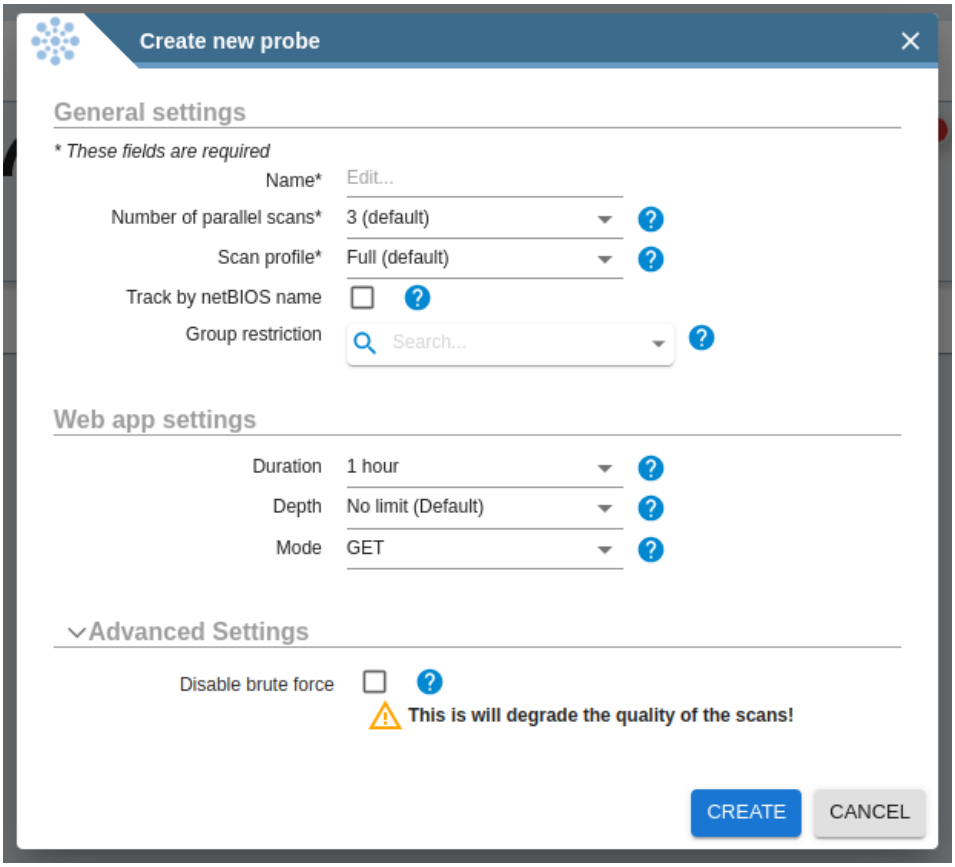
Les filtres qui vous conviennent, peuvent être sauvegardés sous forme de vue que vous pouvez retrouver avec l'étoile :

Création d'une nouvelle sonde

Pour créer une nouvelle sonde, cliquez sur le bouton "**Register new probe**". Pour activer une sonde, cliquez sur le bouton "**Activate probe**".

Pour éditer une sonde existante, cliquez sur sa vignette.

ℹ️ **Note :** Il n'est possible d'activer les sondes que dans les limites qu'autorise votre licence.



Pour la partie "**General settings**", les informations suivantes sont configurables :

- **Name** : Nom de la sonde à afficher
- **Number of parallel scans** : Nombre de scans qui s'exécuteront en parallèle
- **Scan profile** : Profondeur du scan (Nombre de ports)
- **Track by Netbios** : Activer le tracking par Netbios
- **Group restriction** : Restreindre l'utilisation de la sonde à un ou plusieurs groupes

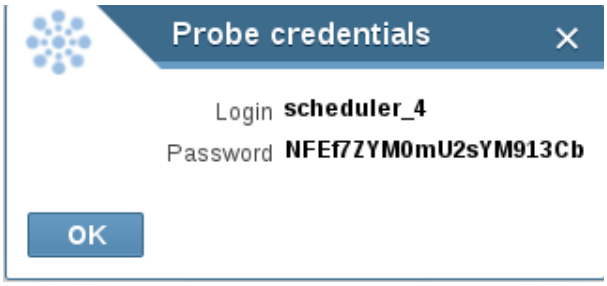
Pour la partie “**Web app settings**”, les informations suivantes sont configurables :

- **Duration** : Durée maximale d’un scan
- **Depth** : Profondeur maximale du scan. Par exemple, une profondeur de 2 résultera en un scan sur uniquement 2 niveaux de l’application web (i.e. la page d’accueil et une page accessible depuis la page d’accueil)
- **Mode** : Type de requête HTTP qui sera utilisé lors du scan d’une application web (HTTP GET uniquement, conseillé pour une application en production ou HTTP GET + POST, conseillé pour une application en cours de recette).

Pour la partie “**Advanced Settings**”, les informations suivantes sont configurables :

- **Disable brute force** : Désactivation du test de connexion de 300 logins/passwords

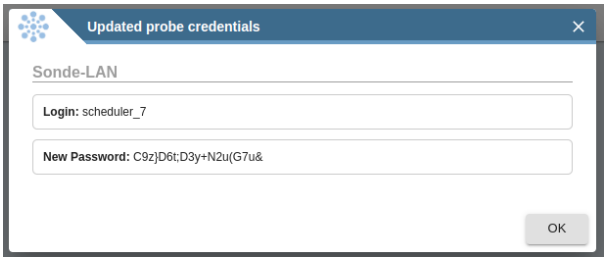
Il est nécessaire d’enregistrer une sonde auprès du serveur IKare afin que cette dernière réalise les scans. Il faut pour cela renseigner les éléments fournis au moment de sa création dans la console d’administration d’une sonde au menu “Register New Probe”.



1.6.9 Actions sur la sonde

Pour chaque sonde il est possible d'effectuer certaines actions. Si la sonde est déjà active :

- **Deactivate probe** : Désactiver la sonde sélectionnée
- **Gen. password** : Générer un nouveau mot de passe aléatoire pour la sonde



Note : Il n'est pas possible de régénérer le mot de passe de la première sonde

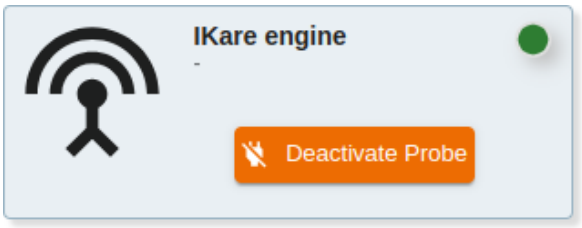
Si la sonde n'est pas encore active :

- **Activate probe** : Activer la sonde sélectionnée
- **Archive Probe :** Archiver la sonde sélectionnée

Si la sonde est archivée :

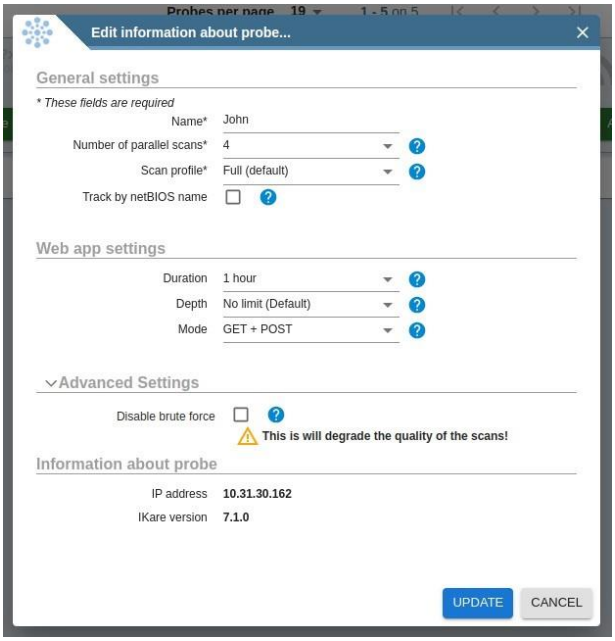
- **Restore probe** : Restaurer la sonde sélectionnée

Vous avez également en haut à droite de chaque sonde une indication sur son état :



- **Vert** : La sonde communique bien avec l'IKare Master
- **Orange :** la connexion entre votre Ikare master et la sonde a été interrompue entre 1 et 24h
- **Rouge :** Dernière connexion à IKare Master il y a plus d'un jour

Lorsque vous cliquez sur une sonde vous aurez accès à ses informations et vous pourrez les modifier :



Vous retrouverez les mêmes parties que lors de la création d'une sonde.

Vous aurez également :

La partie "**Advanced Settings**" :

- **Disable bruteforce** : Désactiver le brute-force lors des scans

La partie "**Information about probe**" :

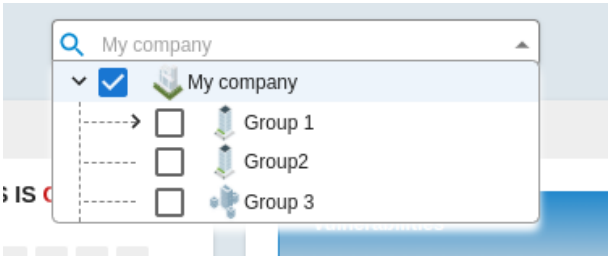
- **IP address :** l'ip de votre sonde
- **IKare version** : la version de votre sonde

2. Utilisation

2.1 Page d'accueil

IKare possède une page d'accueil recensant les indicateurs les plus courants pour surveiller votre infrastructure. Elle est divisée en 4 sections majeures.

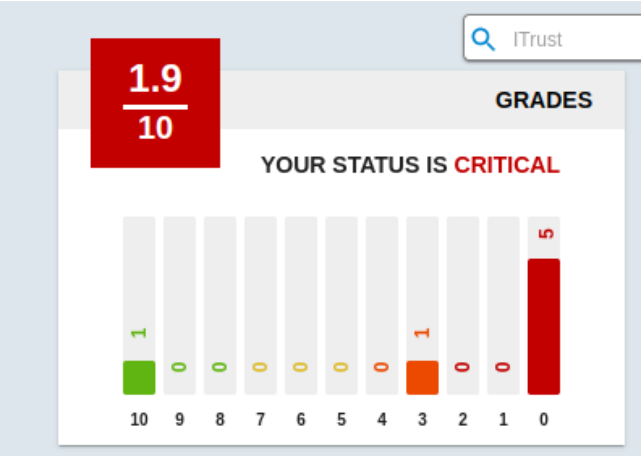
Vous pouvez filtrer l'affichage en sélectionnant un groupe souhaité :



2.1.1 Grades

Cette section résume le niveau global de la sécurité de votre/vos réseaux configurés sur IKare.

La section affiche le nombre d'équipements pour chaque note, ainsi que la note générale du réseau surveillé. Le tout en fonction des groupes configurés pour l'utilisateur.



2.1.2 Network Health

Cette section décrit le niveau de sécurité actuel et vise à déterminer rapidement le niveau de risque sur le réseau.

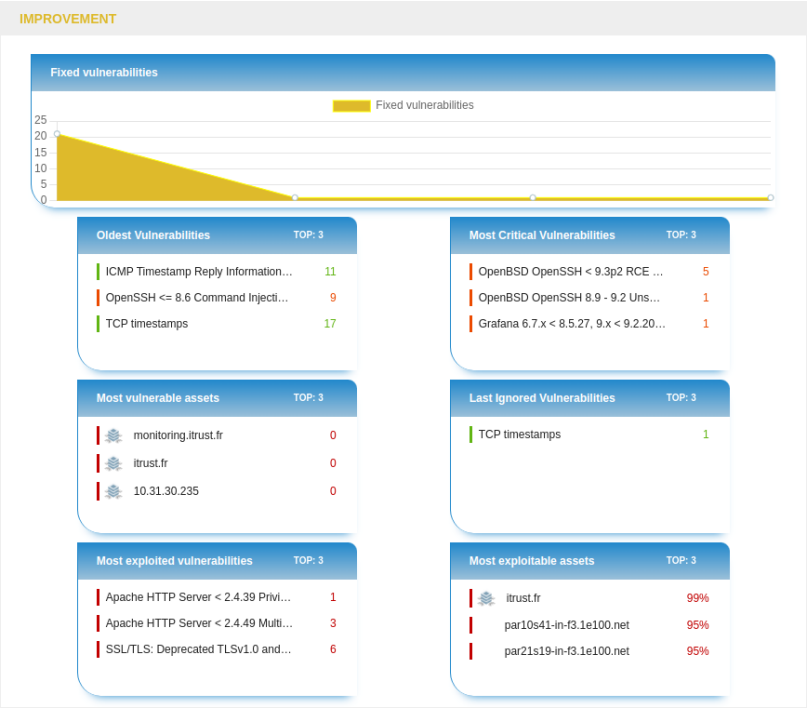
La section **Vulnerabilities** présente le nombre actuel de vulnérabilités découvertes pour chaque criticité. Le graphique affiche un historique dans le temps du nombre de vulnérabilités découvertes pour les 30 derniers jours.

La section **Data Security** affiche la note moyenne des équipements pour chaque tag configuré.

Pour finir, la section **Assets supervised,** vous présente le pourcentage de couverture du réseau découvert, c'est-à-dire le ratio entre les équipements découverts et le nombre d'équipement analysés. Le deuxième graphique expose le pourcentage d'analyses authentifiées.

2.1.3 Improvement

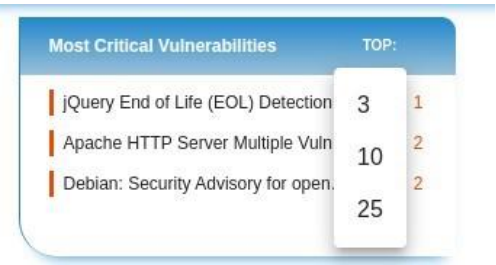
Cette section permet de suivre les récentes progressions du niveau de sécurité des réseaux supervisés.



Le graphique **Fixed vulnerabilities** permet de suivre le nombre de vulnérabilités résolues par semaine.

Les sections **Oldest Vulnerabilities, Most Critical Vulnerabilities, Last Ignored Vulnerabilities** et **Most exploited vulnerabilities** affichent respectivement, les 3 vulnérabilités découvertes les plus vieilles, les 3 vulnérabilités les plus critiques (en fonction de la note de la vulnérabilité), les 3 dernières vulnérabilités ignorées et les 3 vulnérabilités les plus susceptibles d'être exploitées (en fonction de sa notation EPSS). Pour chaque vulnérabilité, le nombre de machines impactées est affiché.

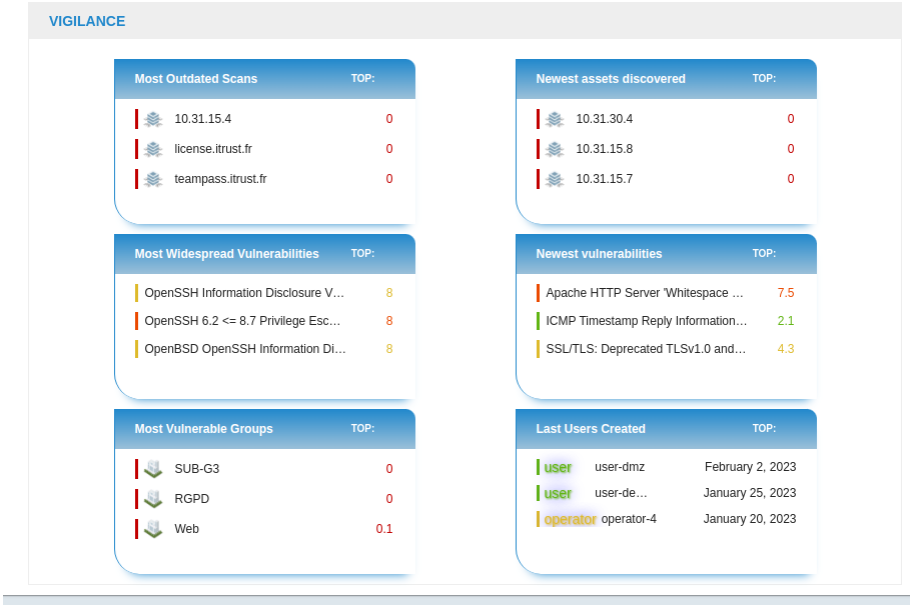
Les sections **Most Vulnerable Assets** et **Most exploitable Assets** affichent respectivement les 3 équipements les plus vulnérables de votre réseau, avec leur note et les 3 équipements avec des failles les plus susceptibles d'être exploitées basées sur le score EPSS. Vous pouvez également cliquer sur l'un des équipements pour afficher sa page de détails.



Vous avez la possibilité de modifier le nombre de vulnérabilités à afficher dans ces sections. Les valeurs possibles sont 3 (par défaut), 10 et 25.

2.1.4 Vigilance

Cette section permet de suivre les activités suspectes afin d'agir de manière urgente. Elle peut être branchée avec un SIEM pour ajouter de nouveaux événements de sécurité dans ses règles.



La section **Most outdated scan** vous montre les équipements qui n'ont pas été analysés depuis longtemps. Elle s'appuie sur la date du dernier scan réalisé, et affiche les 3 équipements dont le dernier scan est le plus vieux.

La section **Newest assets discovered** affiche les 3 derniers équipements découverts. La barre sur le côté affichera si l'analyse est activée ou non (en vert l'analyse est active, en rouge inactive).

Les sections **Most Widespread Vulnerabilities** et **Newest Vulnerabilities** montrent respectivement les vulnérabilités qui ont été détectées sur le plus d'équipements, ainsi que les 3 dernières vulnérabilités détectées. Dans chaque section, le nombre d'équipements impactés est affiché. Vous pouvez cliquer sur l'équipement pour afficher son détail.

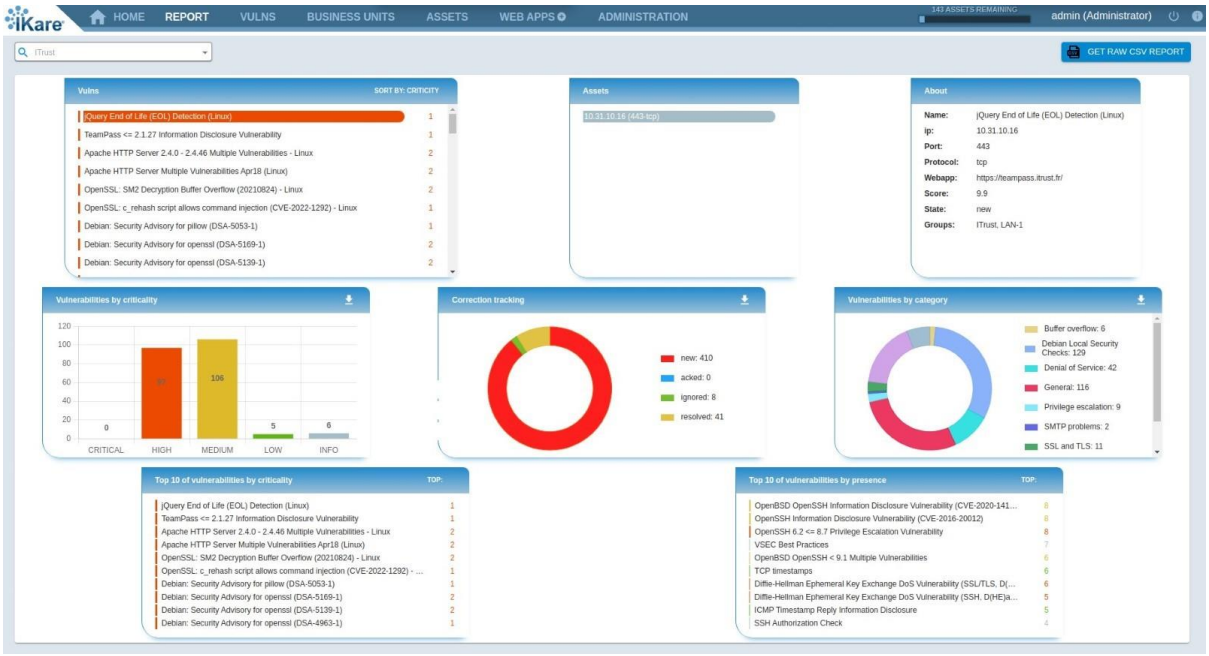
La section **Most Vulnerable Groups** affiche les 3 groupes ayant les notes les plus faibles. Vous pouvez cliquer sur le groupe pour afficher son détail.

Pour finir, la section **Last User Created** vous affichera les 3 derniers utilisateurs créés, leur rôle et leur date de création.

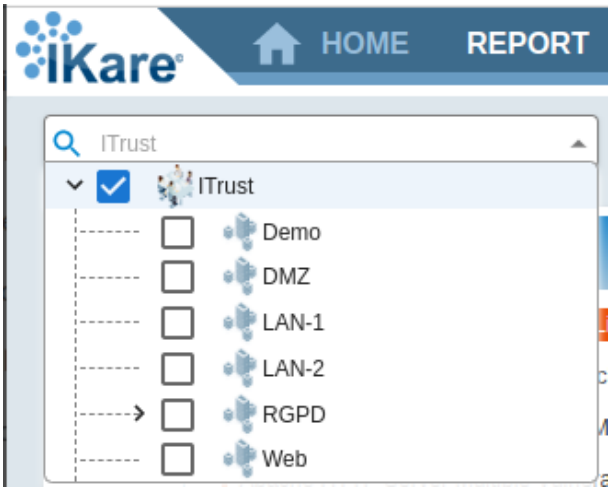
Vous avez également la possibilité de modifier le nombre d'éléments à afficher dans ces sections. Les valeurs possibles sont 3 (par défaut), 10 et 25.

2.2 Report Page

Cette section expose une vue d'ensemble des vulnérabilités découvertes par équipements et groupes supervisés au sein de votre réseau.



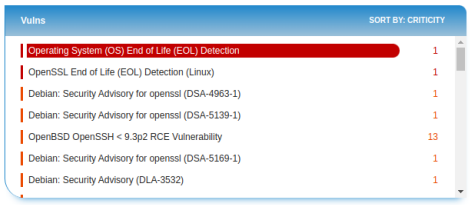
Vous pouvez filtrer l'affichage des différentes sections sur un groupe souhaité :

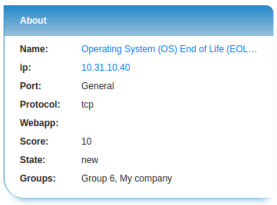


2.2.1 Représentation de l'information

Les différentes sections que contient cette page permettent la navigation à un récapitulatif sur les vulnérabilités par tri :

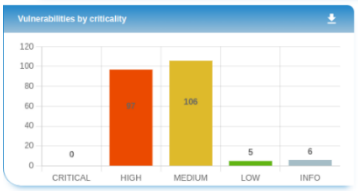
- **Détails d'une vulnérabilité** : la liste des vulnérabilités peut être triée par criticité, date de découverte, par occurrences

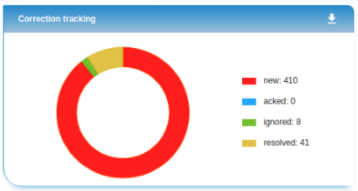


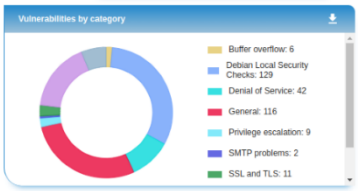


Le clic sur une vulnérabilité (premier tableau : **Vulns**) met à jour la liste des équipements qui remontent cette vulnérabilité (second tableau : **Assets**) ainsi que le détail de la première occurrence de cette vulnérabilité (troisième tableau : **About**)

- **Répartition des vulnérabilités** : les histogrammes suivants présentent la répartition des vulnérabilités par criticité (histogramme **Vulnerabilities by criticity**), par état (histogramme **Correction tracking**) et par catégorie de vulnérabilité (histogramme **Vulnerabilities by category**)

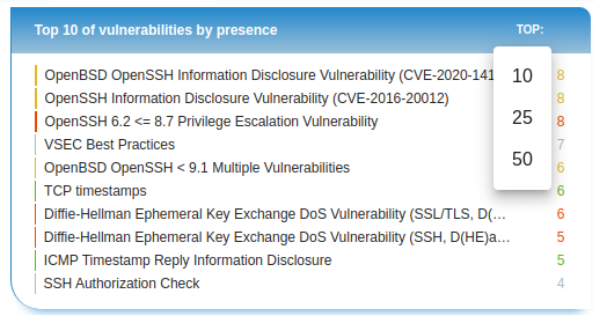




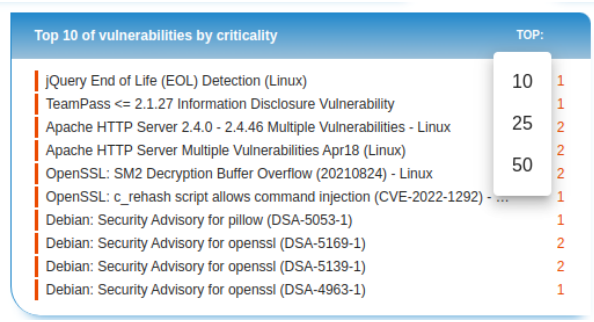


Vous avez la possibilité de télécharger chaque histogramme en cliquant sur la flèche de téléchargement.

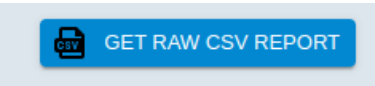
- **Top vulnérabilités** : la liste des vulnérabilités les plus détectées sur vos équipements scannés



- **Vulnérabilités par Criticité/Date/Présence :**



- **Get Raw CSV report :** Générer le rapport CSV synthétisant toutes les vulnérabilités pour le groupe sélectionné



2.3 Business Units

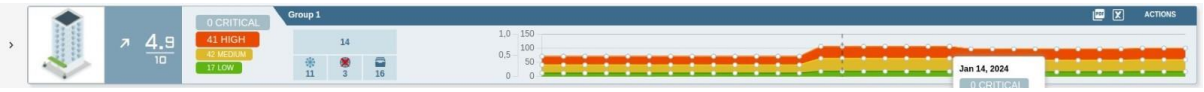
Cette section décrit la vue **BUSINESS UNITS** qui récapitule le niveau de sécurité globale par groupes du système supervisé.

2.3.1 Représentation de l'information

Cette vue montre le récapitulatif des groupes et sous-groupes définis.

ℹ️ **Note** : Par soucis d'ergonomie, seul deux niveaux sont représentés par défaut.

Vous avez la possibilité d'afficher le détail d'un sous niveau en cliquant sur la flèche (>) du niveau souhaité :



Les informations disponibles sont, pour chaque groupe :

- Le nom du groupe
- La note de sécurité sur 10 calculée en fonction de la criticité des vulnérabilités découvertes et du type de données hébergées sur le groupe
- La tendance de la note dans le temps : la flèche monte ou descend en fonction des résultats des scans successifs
- L'indicateur des vulnérabilités découvertes réparties par niveau de risque.
- Le nombre d'équipements découverts dans le groupe

ℹ️ **Note** : Les trois sous catégories correspondent à des raccourcis vers :

- Les équipements scannés par IKare.
- Les équipements découverts mais non activés pour le scan.
- Les équipements archivés.

- Les boutons de téléchargement des rapports (PDF ou CSV)
- Le bouton "**Actions**"

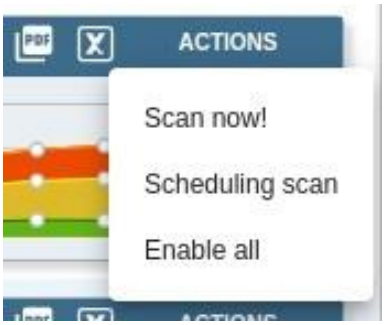
L'histogramme par défaut permet de visualiser l'évolution dans le temps du nombre de vulnérabilités par criticité.

Cette section permet également de visualiser l'évolution dans le temps de la note de chaque groupe (incluant également le nombre d'équipements scannés, désactivés et archivés) en cliquant sur le bouton de droite ci-dessous :

L’histogramme d’évolution de la note des groupes est le suivant :

2.3.2 Actions de groupe

Pour chaque groupe, il est possible d'effectuer certaines actions :



- **PDF report :** Générer le rapport PDF sur l'ensemble des équipements du groupe (icône PDF)
- **CSV report** : Générer le rapport CSV sur l'ensemble des équipements du groupe (icône X)
- **Scan now!** : Relancer un scan immédiat sur un groupe pour s'assurer de la remédiation des vulnérabilités
- **Scheduling scan** : Programmer un scan sur un groupe pour s'assurer de la remédiation des vulnérabilités
- **Enable all** : Autoriser le scan sur l'ensemble des machines découvertes présentes au sein de ce groupe et qui ne sont pas encore actives

ℹ️ **Note 1** : L'action "Scan now!" relance le scan immédiatement sans prise en compte des plages horaires définies pour le groupe.

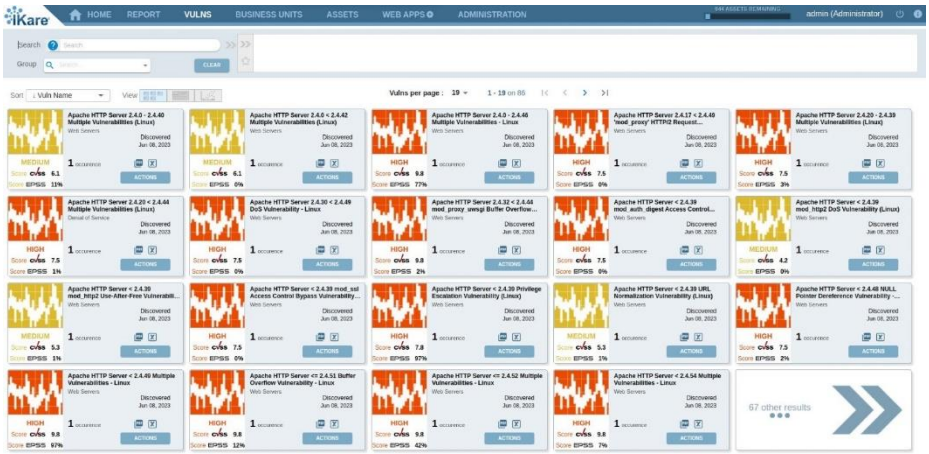
ℹ️ **Note 2** : L'action "Scheduling scan" relance le scan pour le groupe en prenant en compte des plages horaires définies du groupe (les scans s'exécuteront lors de la prochaine plage horaire autorisée du groupe).

ℹ️ **Note 3** : La fonctionnalité "Enable all" entraîne une consommation de jetons de licence comme expliqué dans la partie 3.3.1

ℹ️ **Note 4** : La génération des rapports peut prendre du temps lorsqu'il y a beaucoup de données. Les rapports sont générés en arrière-plan, vous permettant de continuer à naviguer sur la plateforme. Lorsqu'ils sont prêts, ils se téléchargent automatiquement.

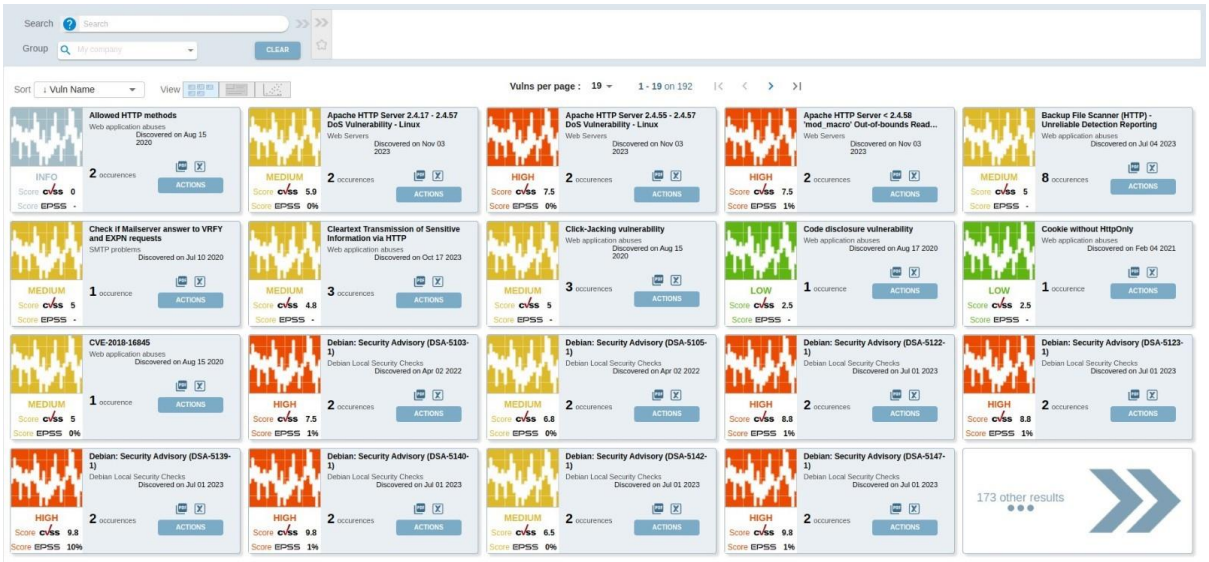
2.4 Vulns

Cette section décrit la vue **VULNS** qui récapitule toutes les vulnérabilités remontées par le logiciel Ikare.



2.4.1 Présentation des vulnérabilités en liste

Cette vue présente l'ensemble des vulnérabilités sous forme de vignettes :



2.4.2 Bandeau supérieur

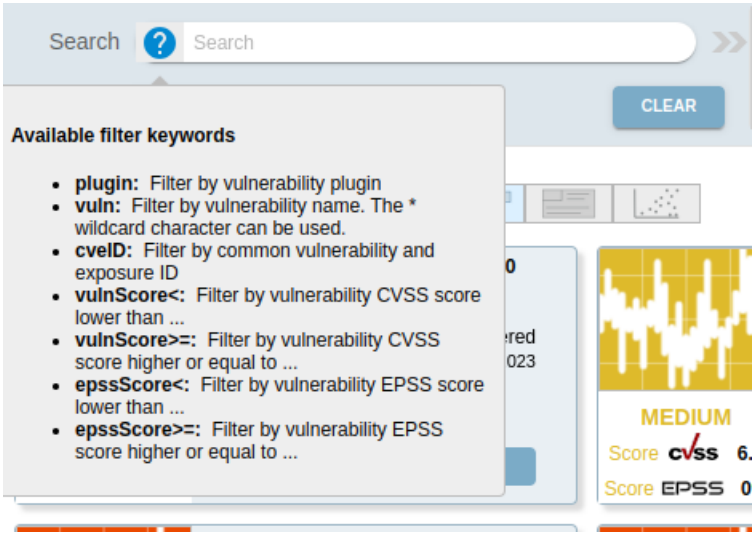
Cette section représente la recherche et le tri des vulnérabilités.

Vous pouvez trier la liste des vulnérabilités par date de découverte, nom de vulnérabilité, score (grade), score EPSS, famille de vulnérabilité, occurrence ou plugin.

Cette section affiche par défaut 19 vulnérabilités par page. Vous pouvez changer de page grâce aux boutons situé au-dessus de la liste des vulnérabilités mais aussi modifier le nombre de vulnérabilités par page à afficher :

Recherche d'une vulnérabilité

Ce bandeau permet de filtrer les vulnérabilités en fonction de mots clés prédéfinis et de sauvegarder des vues :



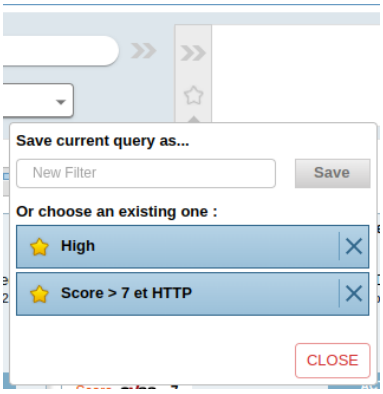
Les mots clés possibles sont :

- **plugin** : Rechercher par numéro de plugin de vulnérabilité (le caractère joker * peut être utilisé)
- **vuln** : Rechercher par nom de vulnérabilité (le caractère joker * peut être utilisé)
- **cveID** : Rechercher par identifiant de CVE (le caractère joker * peut être utilisé)
- **vulnScore** : Rechercher des vulnérabilités ayant un score CVSS supérieur ou inférieur à une valeur CVSS (entre 0 et 10)
- **epssScore** : Rechercher des vulnérabilités ayant un score EPSS supérieur ou inférieur à une valeur EPSS (entre 0% e 100%)

Une fois complet, le schéma de recherche est ajouté dans le champ de droite qui représente le filtre actif. Si plusieurs schémas de recherche sont ajoutés, ils se complètent selon la règle suivante :

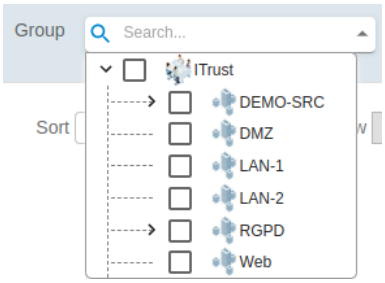
- 2 schémas avec des mots clés différents sont liés par un ET
- 2 schémas avec le même mot clé sont liés par un OU

Les filtres qui vous conviennent peuvent être sauvegardés sous forme de vue que vous pouvez retrouver avec l'étoile :



Groupes

Cette liste permet de filtrer les équipements appartenant à un ou plusieurs groupes (la liste déroulante est un arbre permettant de sélectionner avec les cases à cocher les groupes souhaités) :



Vues

Ces boutons permettent de basculer entre les différentes vues : la vue liste, la vue détaillée ou la vue graphique :

2.4.3 Représentation sous forme de vignettes

Dans cette vue, chaque vulnérabilité est représentée sous forme de vignette contenant les informations suivantes :

- Une image colorée en fonction de la criticité de la vulnérabilité
- La criticité de la vulnérabilité
- Le score CVSS (Common Vulnerability Scoring System) : un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.
- Le score EPSS (Exploit Prediction Scoring System) : probabilité d'exploitation d'une vulnérabilité et met en avant les vulnérabilités qui ont le plus de chance d'être utilisées sur le marché.
- Le nom de la vulnérabilité
- La famille de la vulnérabilité
- La date de la première découverte de la vulnérabilité
- Le nombre d'occurrence (le nombre d'équipements sur lesquels la vulnérabilité a été détectée.)
- Les boutons de téléchargement des rapports de scan en PDF ou CSV
- Le bouton **"Actions"**

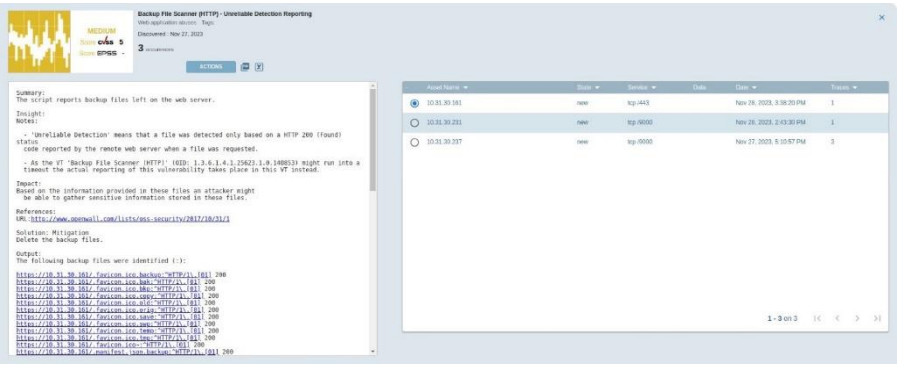
2.4.4 Vue détaillée

En cliquant sur une vulnérabilité vous accèderez à la vue détaillée de celle-ci regroupant les équipements ayant la vulnérabilité, le détail de celle-ci mais aussi d'autres informations comme le service, le statut et la date de découverte.

Vous pouvez cliquer sur un des équipements présents dans la liste ce qui vous redirigera vers l'onglet **ASSETS**, trié avec l'équipement en question.

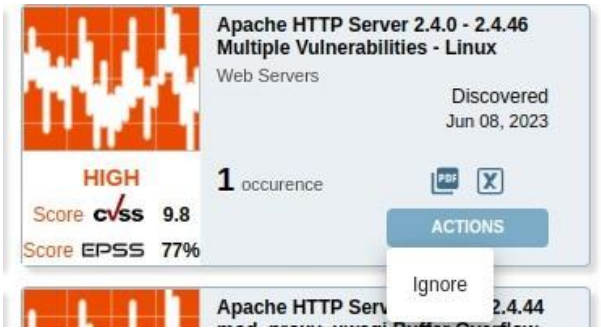
De même pour les tags, si vous avez sélectionné des données dans un groupe, en cliquant sur un des tags cela vous redirigera vers l'onglet **ASSETS** vous retournant ainsi les équipements ayant ce tag.

La croix de fermeture vous permettra de revenir à l'affichage de vos vulnérabilités.

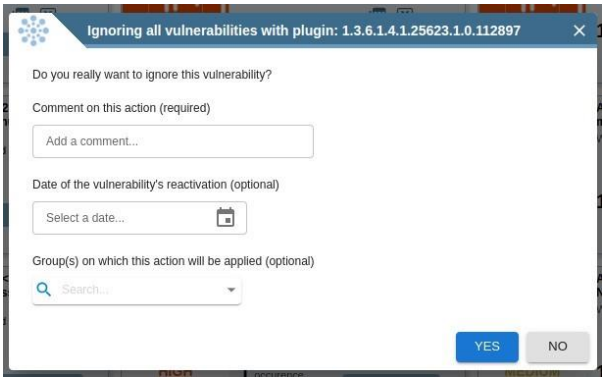


2.4.5 Actions sur une vulnérabilité

Pour chaque vulnérabilité, il est possible d'effectuer certaines actions.



- **PDF report :** Générer le rapport PDF sur la vulnérabilité en cliquant sur l'icône PDF
- **CSV report :** Générer le rapport CSV sur la vulnérabilité en cliquant sur l'icône X
- **Ignore :** Ignorer la vulnérabilité sur toutes les occurrences détectées de celle-ci en cliquant sur le bouton "Actions". Un clic sur l'action Ignore ouvre une fenêtre permettant de :
- **Comment :** Renseigner un commentaire
- **Date of reactivation :** [optionnel] Choisir une date à laquelle la vulnérabilité sera à nouveau prise en compte
- **Groups** : Choisir un groupe sur lequel la vulnérabilité sera ignorée

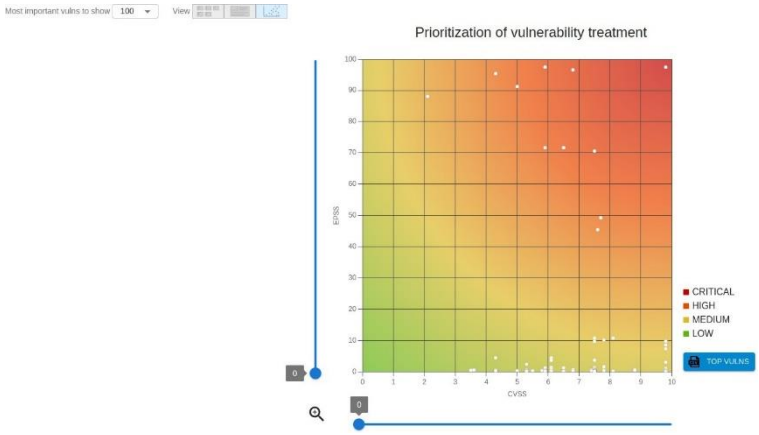


ℹ️ **Note** : l'action d'ignorer une vulnérabilité pour toutes ses occurrences doit être précédée d'une analyse du contexte de chaque occurrence.

2.4.6 Vue graphique

Sur cette vue vous avez accès à un graphique qui vous permet de mettre en évidence les vulnérabilités à corriger en priorité. Ce graphique ce base sur le score **CVSS (Common Vulnerability Scoring System)** et le score **EPSS (Exploit Prediction Scoring System).**

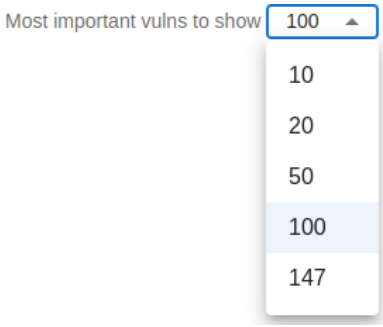
Les vulnérabilités à prioriser se trouveront dans le coin supérieur droit du graphique, car elles possèderont un score CVSS et EPSS élevé.



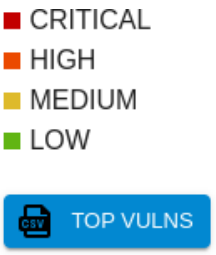
ℹ️ **Note** : Les vulnérabilités à prioriser se trouvent dans le quart supérieur droit.

Vous avez plusieurs actions possibles sur cette vue :

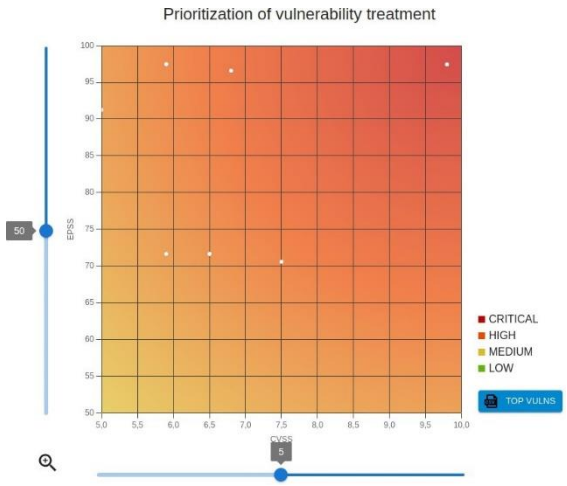
- **Most important vulns to show** : Choisir le nombre de vulnérabilités visible sur le graphique.



- **Légende** : récapitulatif de la signification des couleurs sur le graphique (basé sur la criticité)
- **TOP VULNS :** vous permet de télécharger au format CSV le récapitulatif de toutes les vulnérabilités présentent sur le graphique



- Les sélecteurs à gauche et en bas vous permettent d'effectuer un zoom sur le graphique afin de visualiser rapidement les vulnérabilités à prioriser.



- En passant la souris sur un point, vous pouvez voir certaines informations sur la vulnérabilité : son nom, son score EPSS et CVSS, et sa criticité.

Vous pouvez également cliquer sur le point afin d'obtenir toutes les informations sur la vulnérabilité.

2.5 Assets

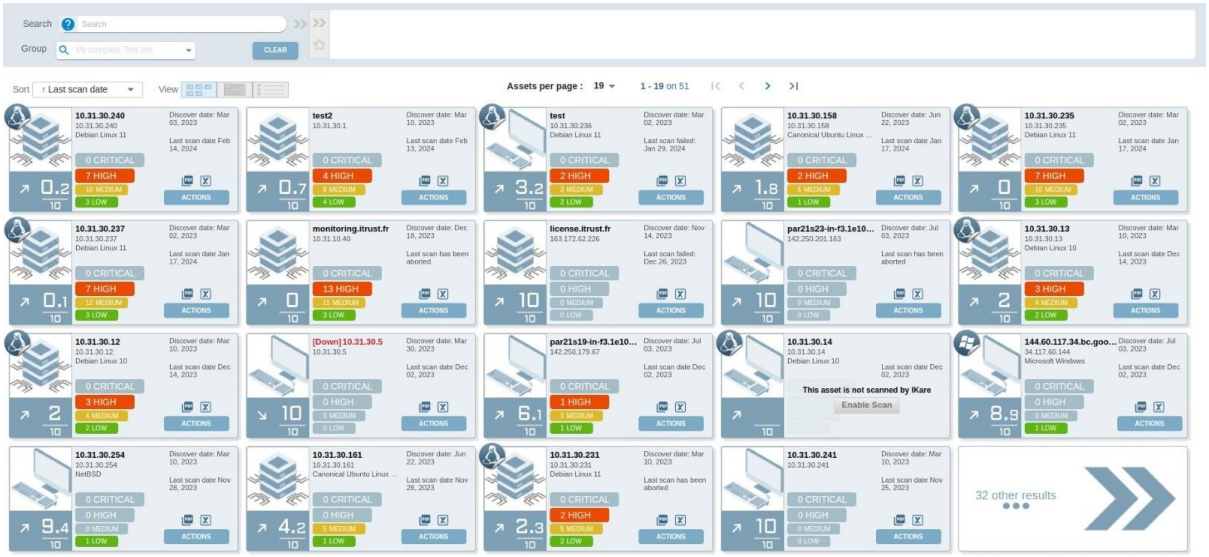
Cette section décrit la vue **ASSETS** qui récapitule le niveau de sécurité globale et détaillé, de chaque équipement supervisé.

2.5.1 Découverte

Dès qu'un équipement est découvert par IKare, il est affiché dans la section **ASSETS** **sans consommer de jeton de licence.**

La découverte d'un équipement se fait automatiquement, dans deux cas différents :

- A l'ajout d'une IP, d'un groupe etc., directement depuis le panneau d'administration.
- Toutes les heures, une découverte se lance afin de vérifier si l'IP d'un équipement a changé et s'il est "UP" (joignable par IKare) ou "DOWN" (injoignable par IKare).

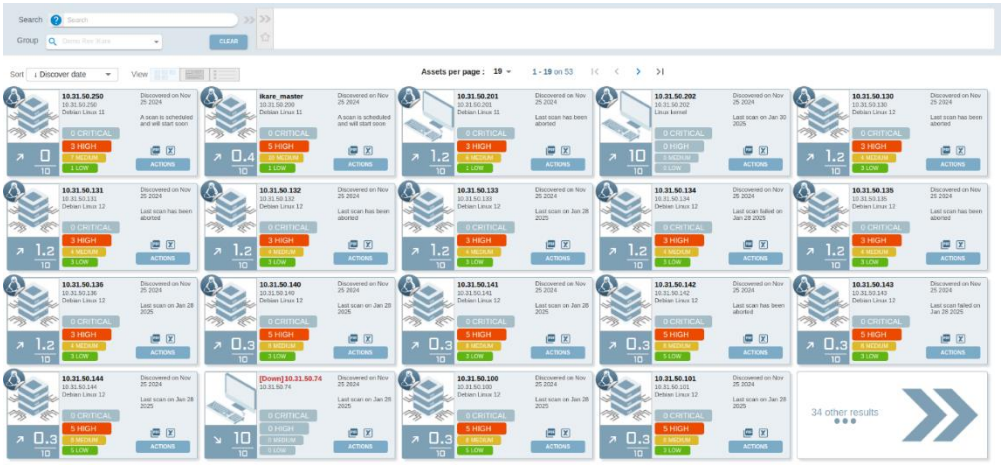


Pour activer la supervision et donc les scans sur cet équipement, il suffit de cliquer sur le bouton **Enable scan**.

Cette activation consomme un jeton de licence.

2.5.2 Présentation des équipements en liste

Cette vue présente l'ensemble des équipements d'un groupe sous forme de vignettes

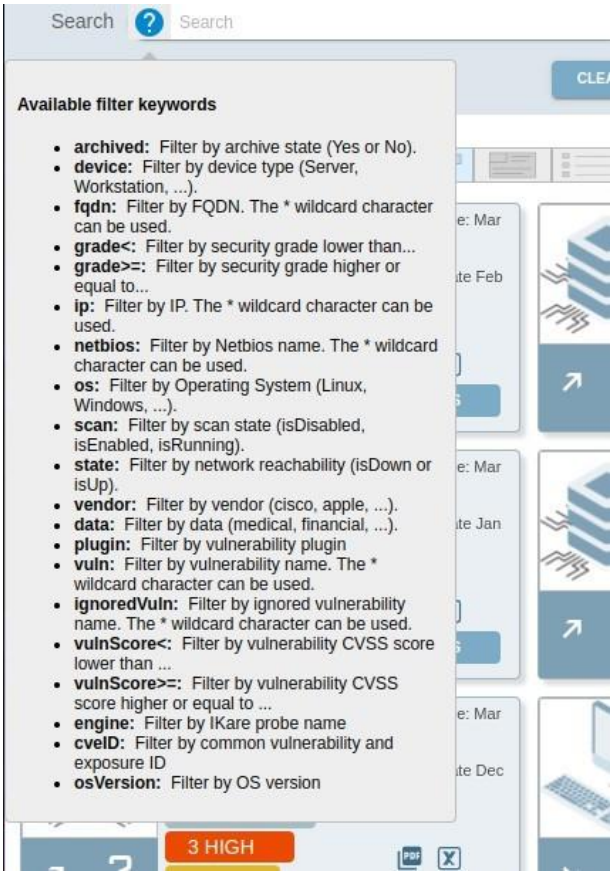


Bandeau supérieur

Le bandeau supérieur de la vue **ASSETS** permet de filtrer et d'accéder rapidement aux informations souhaitées :

Recherche

Ce champ permet de filtrer les équipements en fonction de mots clés prédéfinis et de sauvegarder des vues.



Les mots clés possibles sont :

- **archived** : Rechercher en fonction de l'état des équipements (archivé ou non)
- **device** : Rechercher par type d'équipements (serveur, poste de travail, . . .)
- **fqdn** : Rechercher par nom DNS (le caractère joker * peut être utilisé)
- **grade < ou >= :** Rechercher des équipements en fonction de leur note
- **ip** : Rechercher par adresse IP (le caractère joker * peut être utilisé)

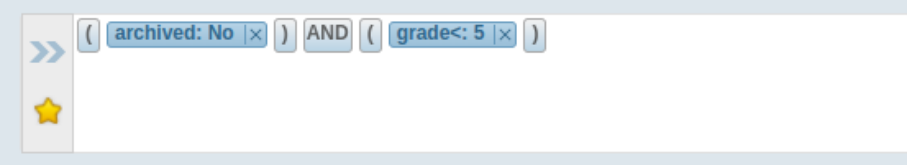
  ℹ️ **Note** : la recherche par IP ou fqdn n'est pas limitée aux entrées existantes.
- **netbios** : Rechercher par nom Netbios (le caractère joker * peut être utilisé)
- **os** : Rechercher par système d'exploitation
- **scan** : Rechercher par état de scan sur un équipement (activé, en cours ou désactivé)
- **state** : Rechercher en fonction de l'état des équipements (éteint ou allumé)
- **vendor** : Rechercher par constructeur (cisco, apple, . . .)
- **data** : Rechercher en fonction du type de données hébergées (médical, bancaire, . . .)
- **plugin** : Rechercher par identifiant de vulnérabilité

- **vuln** : Rechercher en fonction du nom d'une vulnérabilité active (le caractère joker * peut être utilisé)
- **ignoredVuln :** Rechercher en fonction du nom d'une vulnérabilité ignorée (le caractère joker * peut être utilisé)
- **vulnScore < ou >= :** Rechercher des équipements en fonction des notes CVSS d'une de leurs vulnérabilités
- **engine** : Rechercher par nom de sonde IKare associé à l'équipement
- **cveID** : Rechercher par identifiant de CVE
- **osVersion** : Rechercher par version d'OS

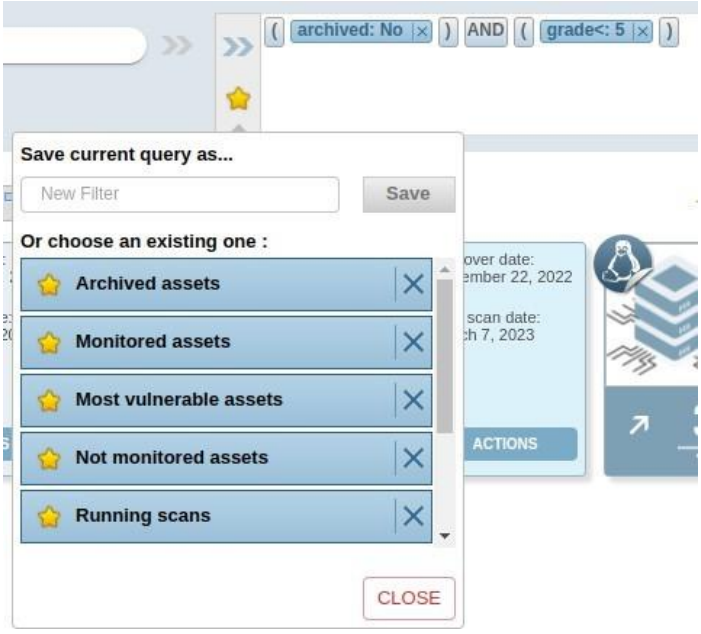
ℹ️ **Note** : La syntaxe de recherche est auto-complétée pour vous guider.

Une fois complet, le schéma de recherche est ajouté dans le champ de droite qui représente les filtres actifs. Si plusieurs schémas de recherche sont ajoutés, ils se complètent selon la règle suivante :

- 2 schémas avec des mots clés différents sont liés par un ET
- 2 schémas avec le même mot clé sont liés par un OU



Les filtres qui vous conviennent peuvent être sauvegardés sous forme de vue que vous pouvez retrouver avec l'étoile :

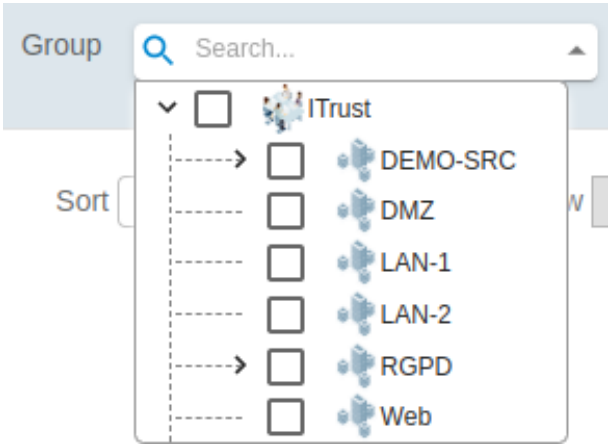


Par défaut, certains filtres sont disponibles :

- **Archived assets** : Lister les équipements archivés
- **Monitored assets** : Lister les équipements activés (via le Enable scan)
- **Most vulnerable assets** : Lister des équipements dont la note est inférieure à 4
- **Not monitored assets** : Lister des équipements découverts et non activés
- **Running scans** : Lister des scans en cours

Groups

Cette liste permet de filtrer les équipements appartenant à un ou plusieurs groupes (la liste déroulante est un arbre permettant de sélectionner avec les cases à cocher les groupes souhaités) :



View

Ces boutons permettent de sélectionner la vue liste, la vue détaillée ou la vue tableau :

2.5.3 Représentation sous forme de vignettes

Dans cette vue, chaque équipement est représenté sous forme de vignette contenant les informations suivantes :

- Un badge représentant le système d'exploitation
- Une icône représentant le type d'équipement
- Le nom de l'équipement (nom DNS, adresse IP ou nom personnalisé)
- L'adresse IP de l'équipement
- Le système d'exploitation
- La note de sécurité sur 10 calculée en fonction de la criticité des vulnérabilités découvertes et des types de données hébergées
- La tendance de la note dans le temps : la flèche monte ou descend en fonction des résultats des scans successifs
- L'indicateur des vulnérabilités découvertes réparties par niveau de risque
- L'indication de date de dernier scan ainsi que la date de découverte de l'équipement
- Les boutons de téléchargement des rapports de scan en PDF ou CSV
- Le bouton **"Actions"**

Lorsqu'un scan est en cours d'exécution, l'icône de l'équipement est mise en arrière-plan et la progression du scan s'affiche (un radar) :

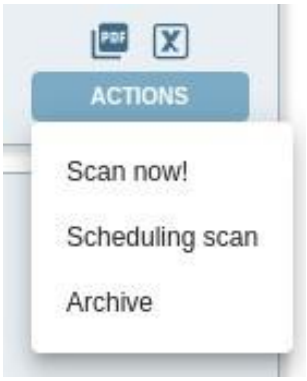
Indication de scan

Sur chaque équipement activé, une indication sur le scan est fournie :

- La date (ou le statut) du dernier scan réalisé sur l'équipement
- Un scan est programmé et va bientôt démarrer
- Un scan est en cours (dans ce cas un radar apparaît sur la vignette)

Actions sur un équipement

Comme pour les groupes, des actions sont disponibles sur un équipement :



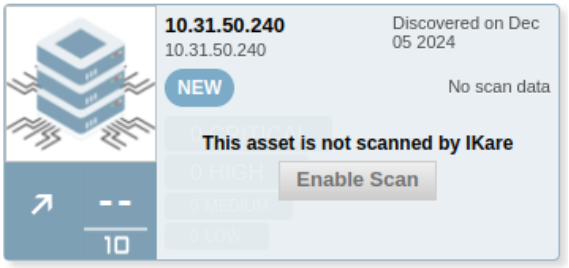
- **PDF report** : Générer le rapport PDF sur l'équipement sélectionné (icône PDF)
- **CSV report** : Générer le rapport CSV sur l'équipement sélectionné (icône X)
- **Scan now!** : Relancer un scan immédiat sur un équipement pour s'assurer de la remédiation de vulnérabilités. (Bouton "Actions")
- **Scheduling scan** : Programmer un scan sur un équipement pour s'assurer de la remédiation de vulnérabilités. (Bouton "Actions")
- **Archive** : Archiver l'équipement et le fait disparaître de l'affichage (Bouton "Actions")

ℹ️ **Note 1** : L'action **"Archive"** libère un jeton de licence. Seuls les "managers" et les "administrateurs" peuvent réaliser cette action

ℹ️ **Note 2** : L'action **"Scan now !"** relance le scan immédiatement sans prise en compte des plages horaires définies pour le groupe. Cette action n'est pas accessible pour les utilisateurs ayant le rôle "user".

ℹ️ **Note 3** : L'action **"Scheduling scan"** relance le scan en prenant en compte des plages horaires définies pour le groupe (le scan s'exécutera lors de la prochaine plage horaire autorisée pour son groupe d'appartenance). Cette action n'est pas accessible pour les utilisateurs ayant le rôle 'user'.

Si l'équipement vient d'être découvert un indicateur "**NEW**" sera affiché :



Si l'équipement n'est pas encore activé vous aurez la possibilité de le faire en cliquant sur le bouton **Enable Scan** :

ℹ️ **Note** : Cette action consommera un jeton de licence

Lorsqu'un équipement est archivé vous aurez la possibilité de :

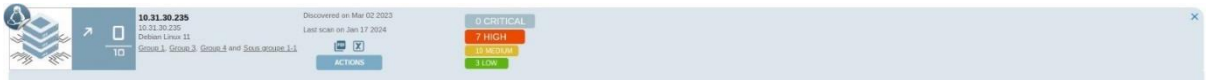
- **Restore** : Restaurer l'équipement (n'active pas les scans sur l'équipement donc ne consomme pas de jeton)
- **Delete** : Supprimer l'équipement et ses données

2.5.4 Présentation détaillée

Pour obtenir la présentation détaillée d'un équipement, il suffit de cliquer sur la vignette correspondante.

Bandeau supérieur

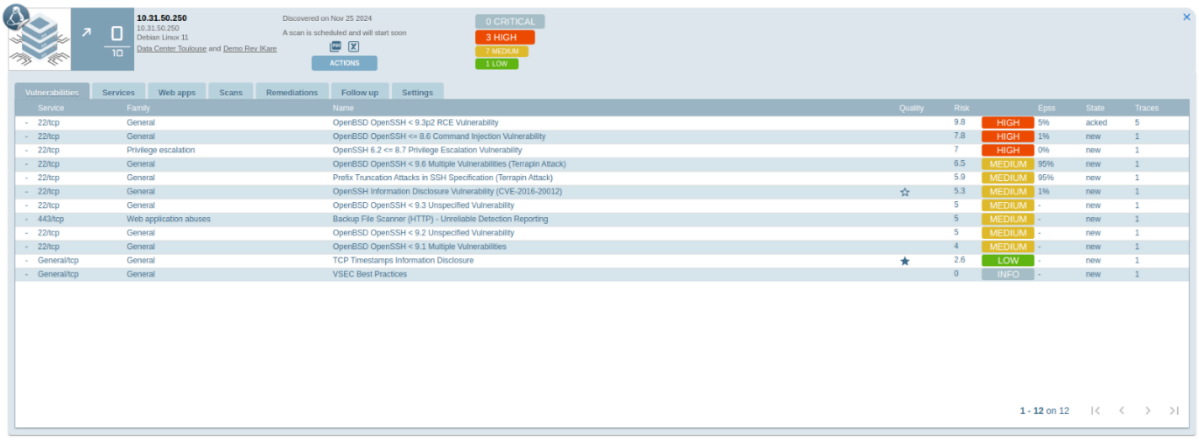
La vue détaillée est constituée d'un bandeau supérieur qui présente toutes les informations présentes sur la vignette, ainsi que les groupes auxquels l'équipement appartient.



ℹ️ **Note 1** : En passant la souris sur un groupe, vous pourrez voir son arborescence (les groupes parents).

ℹ️ **Note 2** : En cliquant sur un groupe vous serez redirigé sur la vue liste, avec le groupe sélectionné.

Onglet ‘Vulnerabilities’



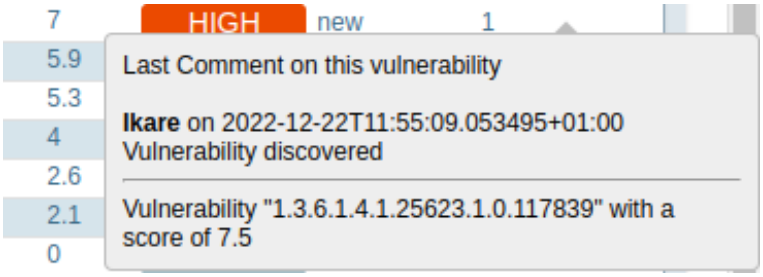
Cet onglet fourni la liste des vulnérabilités détectées sur l’équipement et sur les applications web qu’il héberge avec les informations suivantes :

- Le service impacté par la vulnérabilité avec son port d’écoute

ℹ️ **Note 1** : Dans le cas d’une vulnérabilité appartenant à une application web, l’adresse url sera affichée.

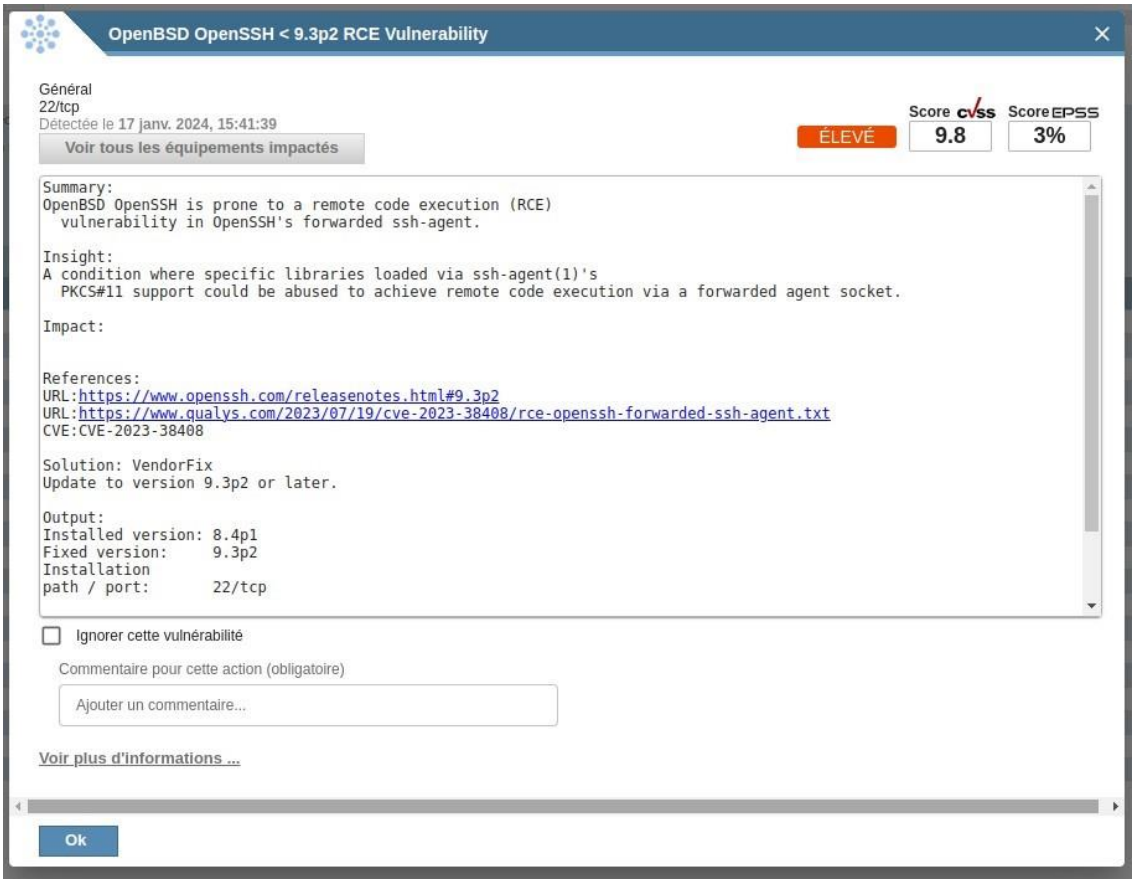
ℹ️ **Note 2** : Dans le cas d’une vulnérabilité applicable à l’équipement dans son ensemble, le service affiché est ‘General/tcp’.

- La famille de la vulnérabilité
- La désignation de la vulnérabilité
- Le niveau de qualité de détection de la vulnérabilité :
  - ***pas d’étoile*** : le niveau de qualité de détection de la vulnérabilité est faible (il se base sur des bannières pouvant ne pas être très fiables)
  - ***une étoile creuse*** : le niveau de qualité de détection de la vulnérabilité est moyen (il se base sur des bannières intéressantes)
  - **une étoile pleine** : le niveau de qualité de détection de la vulnérabilité est élevé (il se base sur des bannières très fiables)
- Le risque associé à la vulnérabilité présenté sous forme de score CVSS et d’indication de criticité
- Le risque d’exploitation de la vulnérabilité présenté avec le score EPSS sous forme de pourcentage
- L’état de la vulnérabilité :
  - ***new*** : vulnérabilité apparue lors du dernier scan
  - ***acked*** : vulnérabilité qui a été ignorée puis réactivée
  - ***ignored*** : vulnérabilité ignorée (cf. ci-après)
- Le nombre de commentaires enregistrés sur la vulnérabilité (en passant la souris sur le nombre, une infobulle affichant le dernier commentaire apparaît)



Détail d'une vulnérabilité

Pour obtenir le détail d'une vulnérabilité, il suffit de cliquer sur la ligne correspondante :



Les informations présentes sont :

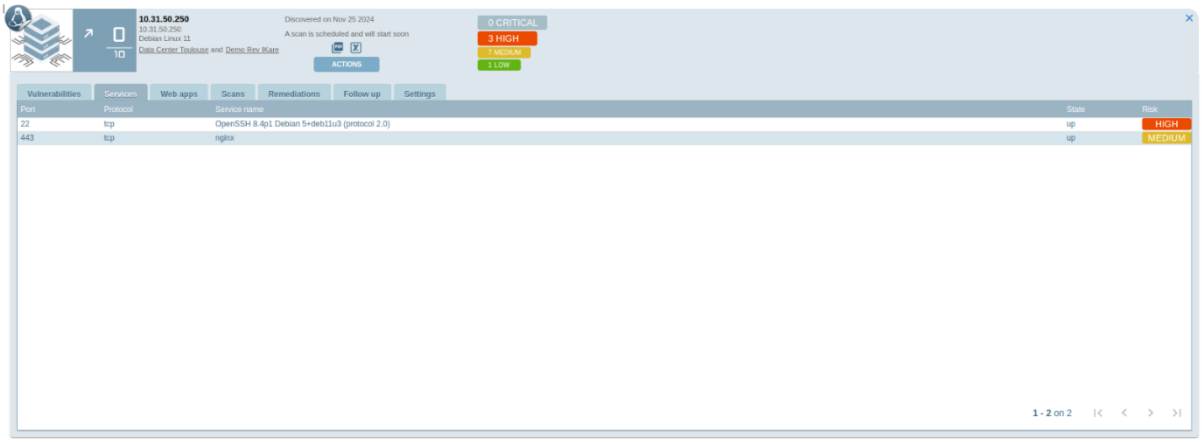
- En titre, la désignation de la vulnérabilité
- Le récapitulatif de la famille, du service et du risque liés à la vulnérabilité
- La date de la première détection de la vulnérabilité.
- La description de la vulnérabilité contenant la solution pour corriger (si disponible), et les références des avis publiant la vulnérabilité.
- L'action "Ignore this vulnerability"

Ignorer une vulnérabilité

Lorsqu'une vulnérabilité est un faux-positif, que le risque est accepté ou qu'une contre mesure rend la vulnérabilité inexploitable, il est possible de l'ignorer. Il suffit de cocher la case dans la description de la vulnérabilité, de renseigner un commentaire expliquant l'action et de valider. Vous pouvez également choisir une date à laquelle la vulnérabilité sera réactivée (optionnel).

La vulnérabilité n'est alors plus prise en compte dans le calcul de la note de sécurité ni dans l'indicatif des vulnérabilités. Néanmoins, cette vulnérabilité apparaît toujours dans l'interface (et dans les rapports) sous forme barrée.

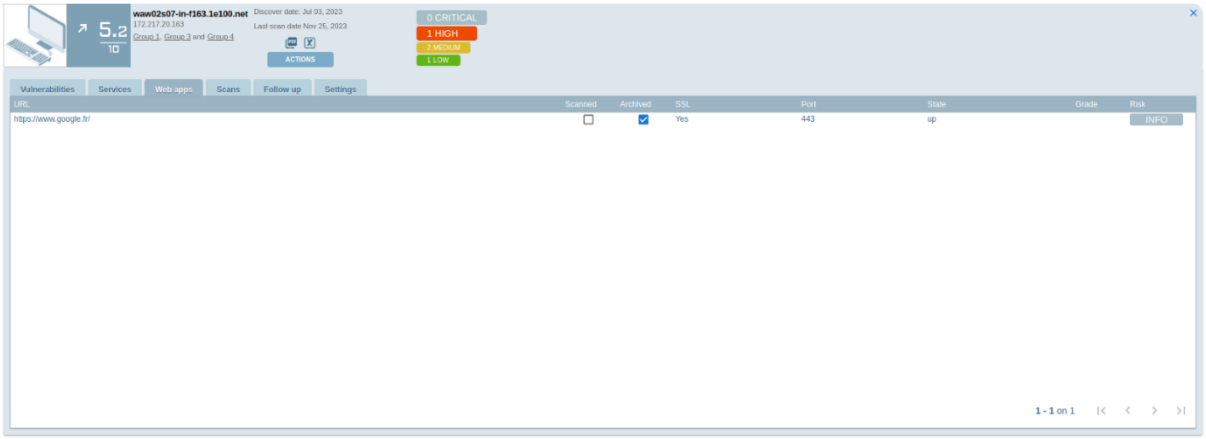
Onglet 'Services'



Cet onglet fourni la liste des services détectés sur l'équipement avec les informations suivantes :

- Le port d'écoute du service
- Le protocole du service
- Le nom et la version du service quand c'est possible
- L'état du service lors du dernier scan (***up***, le service est actif ; ***down***, le service n'est pas accessible)
- L'indication du risque le plus élevé sur le service

Onglet ‘Web apps’

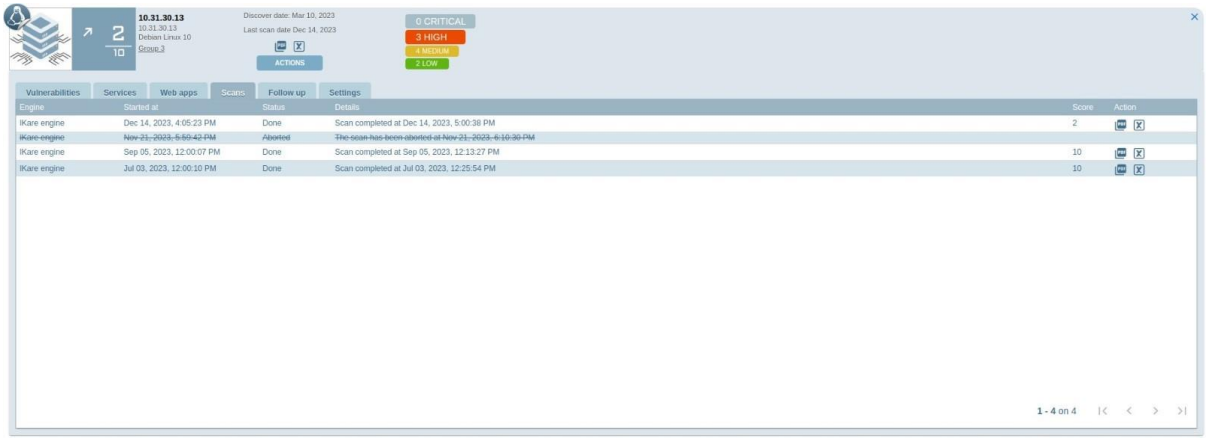


Cet onglet permet de répertorier toutes les applications web supervisées par IKare hébergées sur l’équipement. On peut y retrouver les informations suivantes :

- L’adresse URL de l’application web
- Si cette application web est scannée par IKare
- Si cette application web est archivée
- Si cette application web est en https
- Le port sur lequel l’application écoute
- L’état de l’application
- La note attribuée par IKare à cette application
- La valeur de la plus haute vulnérabilité détectée sur cette application

ℹ️ **Note** : Les vulnérabilités de l’équipement sont aussi présentes sur chaque application qu’il héberge. Il est donc possible que la valeur de la plus haute vulnérabilité d’une application soit en réalité la valeur d’une vulnérabilité de l’équipement.

Onglet ‘Scans’



Cet onglet fournit l’historique des scans sur l’équipement avec les informations suivantes :

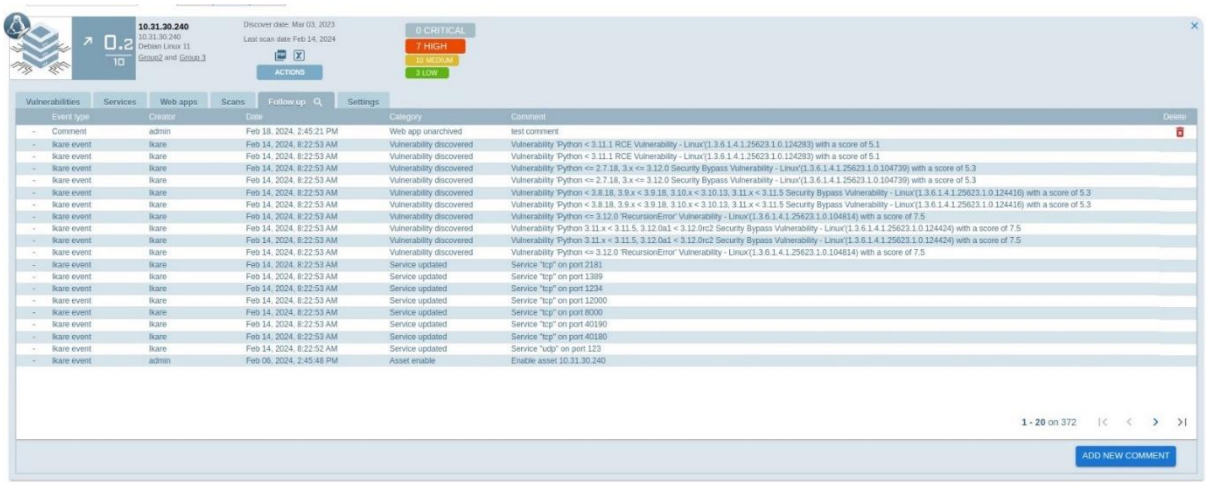
- Le moteur de scan (utile dans le cas d’une architecture multisondes)
- La date de démarrage du scan
- L’état du scan (Réalisé / En attente / En cours / Annulé)
- Les détails du scan
- Les actions possibles sur le scan : Interrompre le scan en cours ou en attente. Télécharger le rapport du scan complet (au format PDF ou CSV)

ℹ️ Note - Il est à noter que la note du scan et la note de l’équipement diffèrent en deux points :

→ Lorsqu’un équipement héberge des applications web, la note de l’équipement tient compte des vulnérabilités découvertes sur les applications web qu’il héberge alors que la note du scan ne concerne que les vulnérabilités effectivement découvertes par le scan

→ De plus, lorsque l’utilisateur ignore des vulnérabilités, la note du scan reste telle qu’elle était au moment du scan alors que la note de l’équipement est recalculée pour prendre en compte le fait que les vulnérabilités ont été ignorées.

Onglet ‘Follow up’



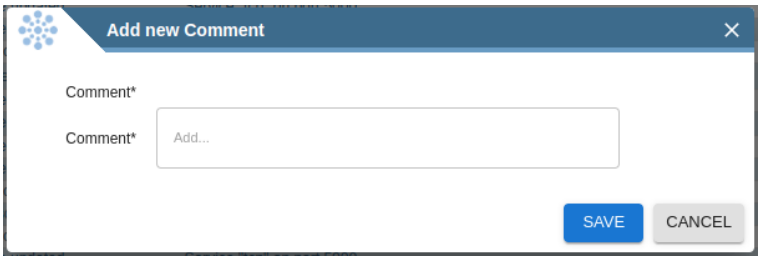
Cet onglet permet de visualiser l’ensemble des événements liés à l’équipement. Un événement peut être la découverte de l’équipement, la découverte/modification/ignorance d’une vulnérabilité, les états des services de l’équipement, les actions réalisées (lancement d’un scan par exemple), etc.

Cet onglet permet également de visualiser et rajouter des commentaires de la part des utilisateurs afin de pouvoir tracer des événements, actions et autres informations permettant de donner des détails sur l’équipement.

Le tableau est constitué des colonnes suivantes :

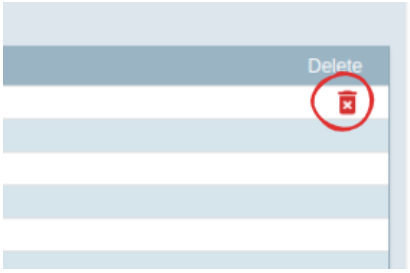
- Le type d’événement : un événement déclenché dans IKare ou un commentaire
- Le créateur de l’événement : Ikare pour tous les événements internes de l’équipement ou le nom de l’utilisateur pour toutes les actions et commentaires saisis
- La date de l’événement
- La catégorie de l’événement
- Le commentaire de l’événement

L’ajout d’un commentaire sur l’équipement s’effectue avec le bouton **“ADD NEW COMMENT”** :

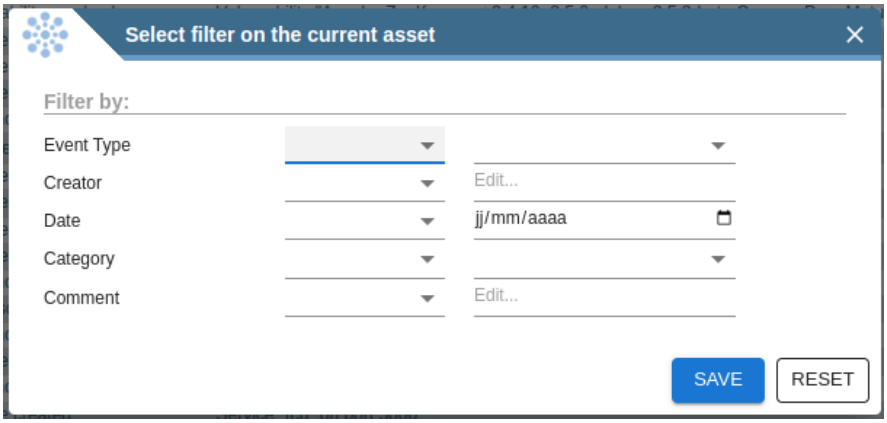


L’utilisateur peut ainsi rédiger le commentaire puis valider celui-ci en cliquant sur le bouton SAVE. Le commentaire apparait directement en début du tableau (étant le dernier événement enregistré sur l’équipement).

Les commentaires peuvent être supprimés si nécessaires :



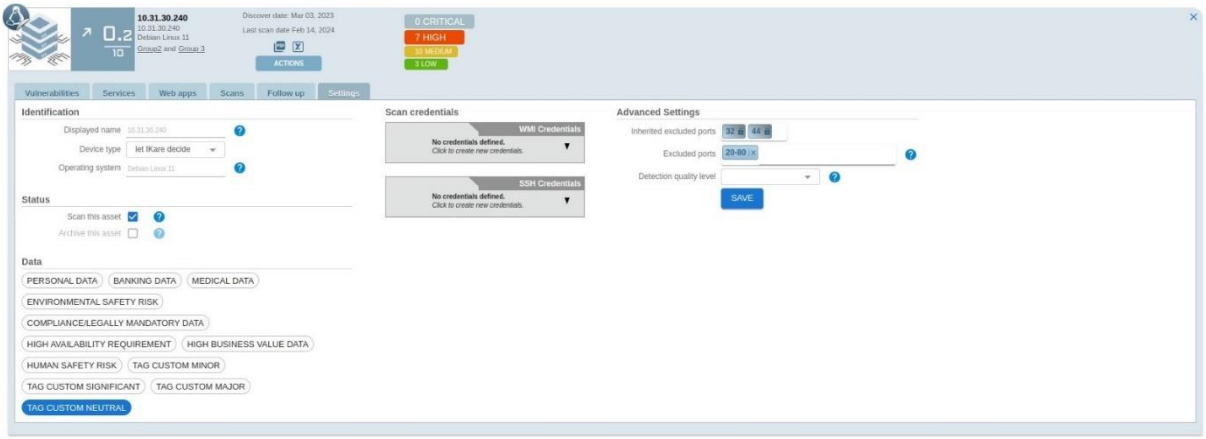
Il est possible de filtrer les événements affichés en cliquant sur la loupe à côté du nom de l'onglet **Follow up**.



Il est donc possible de filtrer en combinant les critères suivants :

- Le type d'événement
- Le créateur de l'événement
- Une date d'événement donnée (inférieur ou supérieure à une date indiquée)
- La catégorie de l'événement
- Le commentaire de l'événement

Onglet ‘Settings’



Cet onglet permet de configurer plusieurs éléments de l’équipement :

Configuration d’identification

→ Le nom affiché de l’équipement (si le nom DNS ou l’adresse IP ne sont pas représentatifs)

→ Le type d’équipement. Ce choix permet de changer l’icône représentant l’équipement et surtout permet d'effectuer des recherches sur certains types.

ℹ️ **Note** : Par défaut IKare définit le type d’équipement en fonction des résultats d’un scan.

→ Le système d’exploitation. Permet d’affiner le système d’exploitation de l’équipement pour les recherches.

ℹ️ **Note** : Par défaut IKare définit le système de l’équipement en fonction des résultats d’un scan. La liste des systèmes possibles est auto-complétée en fonction de la saisie de l’utilisateur.

Configuration de l’état de l’équipement

→ La possibilité de désactiver le scan. Cette action libère un jeton de licence. Le bouton “Enable scan” sera à nouveau affiché pour réactiver le scan.

→ La possibilité d’archiver l’équipement. Cette action fait disparaître l’équipement de l’interface et libère un jeton de licence.

ℹ️ **Note 1** : Les fonctions de désactivation de scan et d’archivage d’un équipement ne sont pas utilisables dans le cas d’une version gratuite.

ℹ️ **Note 2** : Lorsqu’un équipement est archivé, toutes les applications web qu’il héberge le sont aussi.

Configuration des types de données

→ La possibilité d'activer ou de désactiver un type de données sur la machine.

ℹ️ **Note** : Si un type de données est actif au niveau du groupe, ce dernier ne peut pas être désactivé sur l'équipement.

Configuration d'identifiants de scan

Il est possible de définir des identifiants afin d'effectuer des scans authentifiés sur les équipements. De la même manière que pour un groupe, chaque équipement peut posséder un identifiant WMI (de la forme identifiant/mot de passe) et/ou un identifiant SSH (au choix entre identifiant/mot de passe ou identifiant/clé privée).

Le comportement de ces vignettes est le suivant :

- Si un identifiant est défini sur l'équipement, alors ce dernier y sera affiché.
- Si aucun identifiant n'est défini sur l'équipement, mais qu'un l'a été sur un des groupes parents de l'équipement, alors ce dernier y apparaitra.
- Dans le cas où l'équipement possède plusieurs groupes parents, il est possible de choisir quel identifiant appliquer.
- En cliquant simplement sur la vignette, la liste de tous les identifiants possibles apparait.
- Dans le cas où aucun identifiant n'a été défini, ni sur les groupes parents, ni sur l'équipement, alors la vignette apparaît comme vide.

Dans le cas où un identifiant a été défini sur plusieurs groupes parents, la vignette se présente comme suit :

Il est alors possible de choisir quel identifiant appliquer. La création d'un identifiant fonctionne de la même manière que sur les groupes (voir 1.3 – Groups).

Configuration avancée

Ce bloc permet de configurer (ou surcharger) les caractéristiques de scan suivantes :

- **Excluded ports** : possibilité de définir des ports et/ou plages de ports à exclure lors de la réalisation d'un scan. Les plages de ports doivent être saisies avec le séparateur - entre le premier port à exclure et le dernier. Exemple : 22-55 (=> Exclusion des ports 22 à 55)
- **Detection quality level** : possibilité de définir le niveau de qualité de détection minimal à prendre en compte dans la remontée des vulnérabilités. Par défaut, IKare remonte toutes les vulnérabilités détectées, qu'elles aient une qualité de détection faible, moyenne ou forte. En sélectionnant un seuil dans la liste déroulante (Low [par défaut], Medium ou High), IKare ne fera remonter que les vulnérabilités ayant une qualité de détection égale ou supérieure à la valeur sélectionnée

ℹ️ **Note** : Le champ Inherited excluded ports affiche les ports / plages de ports qui ont été exclus dans les groupes d'appartenance de l'équipement courant.

2.5.5 Vue Tableau

Sur cette vue vous avez la possibilité de réaliser des actions groupées. Vous pouvez retrouver tous vos équipements listés dans un tableau avec les colonnes suivantes :

- **La colonne de sélection**
- **Asset** : icône qui représente le type d'équipement
- **Grade** : la note de votre équipement
- **Name** : le nom de votre équipement
- **IP** : son IP
- **Discover date** : date de découverte
- **Last scan date** : la date du dernier scan
- **Actions** : les actions individuelles possibles sur l'équipement

Bandeau

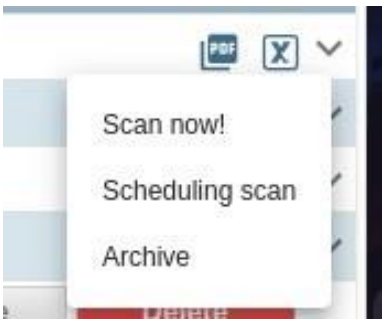
Vous pouvez retrouver en haut le même bandeau que sur les vues précédentes. Les filtres, la pagination et le tri marche de la même manière.

Actions individuelles

Dans la colonne actions vous avez à votre disposition les actions de base :

- **PDF report** : Générer le rapport PDF sur l'équipement sélectionné (icône PDF)
- **CSV report** : Générer le rapport CSV sur l'équipement sélectionné (icône X)
- **Scan now!** : Relancer un scan immédiat sur un équipement pour s'assurer de la remédiation de vulnérabilités. (Icône flèche vers le bas)
- **Scheduling scan** : Programmer un scan sur un équipement pour s'assurer de la remédiation de vulnérabilités. (Icône flèche vers le bas)

- **Archive :** Archiver l'équipement et le fait disparaître de l'affichage (icône flèche vers le bas)



ℹ️ **Note 1** : L'action "Archive" libère un jeton de licence. Seuls les "managers" et les "administrateurs" peuvent réaliser cette action

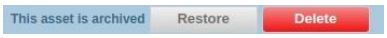
ℹ️ **Note 2** : L'action "Scan now !" relance le scan immédiatement sans prise en compte des plages horaires définies pour le groupe. Cette action n'est pas accessible pour les utilisateurs ayant le rôle "user".

ℹ️ **Note 3** : L'action "Scheduling scan" relance le scan en prenant en compte les plages horaires définies pour le groupe (le scan s'exécutera lors de la prochaine plage horaire autorisée pour son groupe d'appartenance). Cette action n'est pas accessible pour les utilisateurs ayant le rôle 'user'.

- **Enable scan** : Activer l'équipement pour le scan

ℹ️ **Note 4** : L'action "Enable scan" consomme un jeton de licence. Seuls les "managers" et les "administrateurs" peuvent réaliser cette action

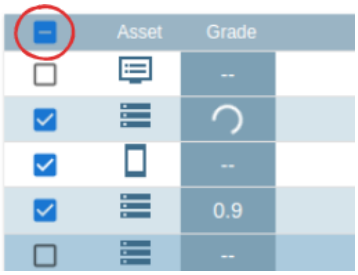
- **Restore** : Restaurer un équipement archivé
- **Delete** : Supprimer totalement un équipement



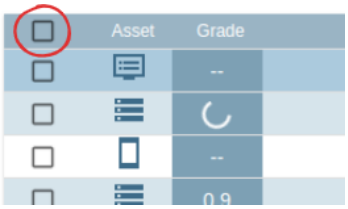
Actions de groupe

Vous pouvez sélectionner vos équipements en les cochant sur le côté :

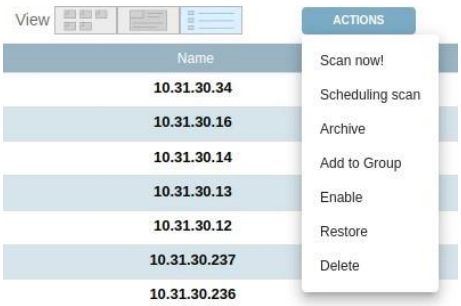
Vous pouvez utiliser le bouton suivant pour tout désélectionner :



Ou au même endroit le bouton suivant pour tout sélectionner :

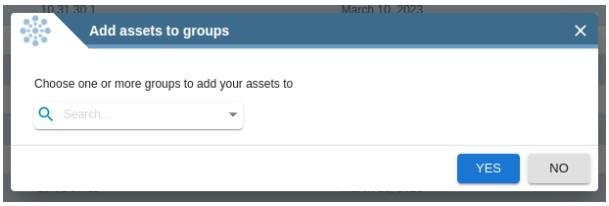


Lorsque votre sélection est faite, le bouton Actions se débloque (grisé auparavant sans sélection) :



Vous avez accès aux actions suivantes :

- **Scan now!** : Relancer un scan immédiat sur les équipements sélectionnés pour s'assurer de la remédiation de vulnérabilités.
- **Scheduling scan :** Programmer un scan sur les équipements sélectionnés pour s'assurer de la remédiation de vulnérabilités.
- **Archive :** archive les équipements sélectionnés et les fait disparaitre de la liste
- **Add to group :** Ajouter aux groupes sélectionnés les équipements sélectionnés. Une fenêtre s'ouvre vous permettant de choisir le/les groupes voulus :



- **Enable** : Activer les équipements sélectionnés
- **Restore** : Restaurer les équipements sélectionnés
- **Delete** : Supprimer les équipements sélectionnés

ℹ️ **Note** : L'action "Enable" consomme un jeton de licence pour chaque équipement. Seuls les "managers" et les "administrateurs" peuvent réaliser cette action

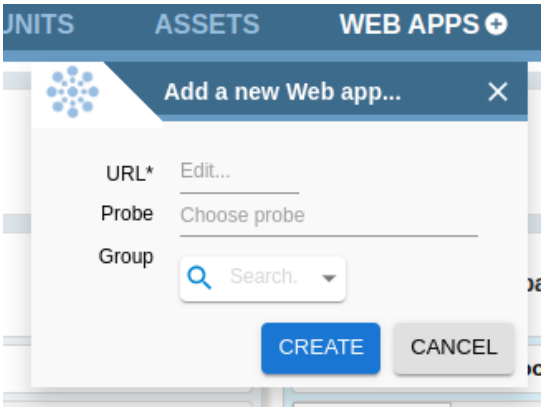
2.6 Web apps

Cette section décrit la vue Web Apps qui récapitule le niveau de sécurité globale et détaillé de chaque application web supervisée.

2.6.1 Ajout

Afin d'ajouter une application web, il suffit de cliquer sur le bouton "+" situé à côté de l'entête "WEB APPS". Une fenêtre de saisie apparait alors, dans laquelle il sera nécessaire de renseigner les éléments suivants :

- L'adresse url de l'application web à scanner
- La sonde IKare qui sera chargée de découvrir et scanner l'url (dans le cas où l'IKare n'est composé que d'un IKare Master, seule l'IKare Engine sera disponible)
- Le groupe dans lequel l'application web et l'IP de son serveur web devront être rattachés



Note : Lors de l'ajout d'une application web, IKare va détecter l'équipement sur lequel elle est hébergée. Il est donc nécessaire que l'équipement soit dans le périmètre des équipements supervisés par IKare.

Dès qu'une application web est ajoutée, elle est affichée dans l'onglet Web apps. Si plusieurs applications web sont hébergées sur un même équipement (serveur web), chaque application web va consommer un jeton de licence.

Pour activer la supervision et donc les scans sur cette application web, il suffit de cliquer sur le bouton **Enable scan**. Cette activation consomme un jeton de licence.

ℹ️ **Note** : La gestion des jetons de licence concernant les applications web contient une légère subtilité. Chaque équipement découvert offre un jeton de licence “gratuit” pour une application web qu’il héberge. Ainsi un équipement hébergeant 3 applications web ne consommera que 3 jetons au lieu de 4 (1 pour un équipement + application web et 2 pour les autres applications web)

La découverte d’une application web est effectuée de manière asynchrone par la sonde de scan IKare (soit la sonde Master soit par la sonde IKare sélectionnée).

La sonde de scan peut rencontrer une erreur lors de l’enregistrement de l’application web :

- Impossibilité d’effectuer la résolution de l’url de l’application web avec son adresse IP
- Impossibilité d’enregistrer l’IP du serveur web (IP hébergeant l’application web) dans le groupe sélectionné

Dans un de ces cas-là, une instance de l’application web est tout de même créée dans IKare mais avec un statut en cours de découverte. Pour visualiser les applications web dans cet état, il est nécessaire d’utiliser le filtre “**discovering**” avec la valeur ‘Yes’.

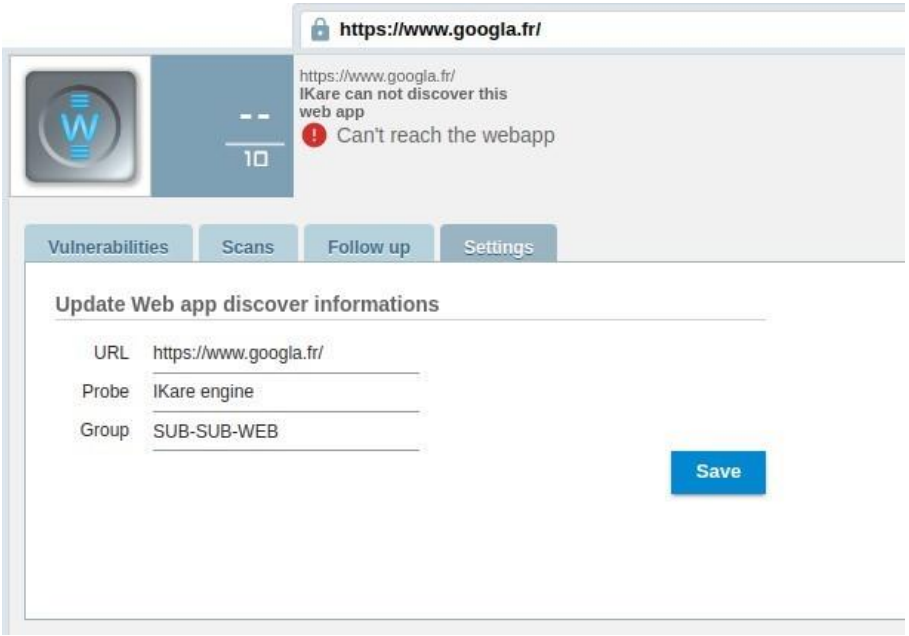
Ce filtre permet d’afficher toutes les applications web qui ne sont pas encore découvertes :

- Les applications web qui ne sont pas encore découvertes mais enregistrées par la sonde sélectionnée

- Les applications web ayant une erreur dans leur enregistrement

Pour les applications web ayant eu une erreur d'enregistrement, le dernier message d'erreur remonté lors de l'enregistrement de l'application web est affiché pour guider l'utilisateur. Celui-ci peut ensuite modifier un des éléments suivants pour relancer la découverte/enregistrement de l'application web :

- L'url de l'application web si elle est erronée
- La sonde IKare chargée de découvrir et scanner l'url
- Le groupe dans lequel l'application web doit être rattachée



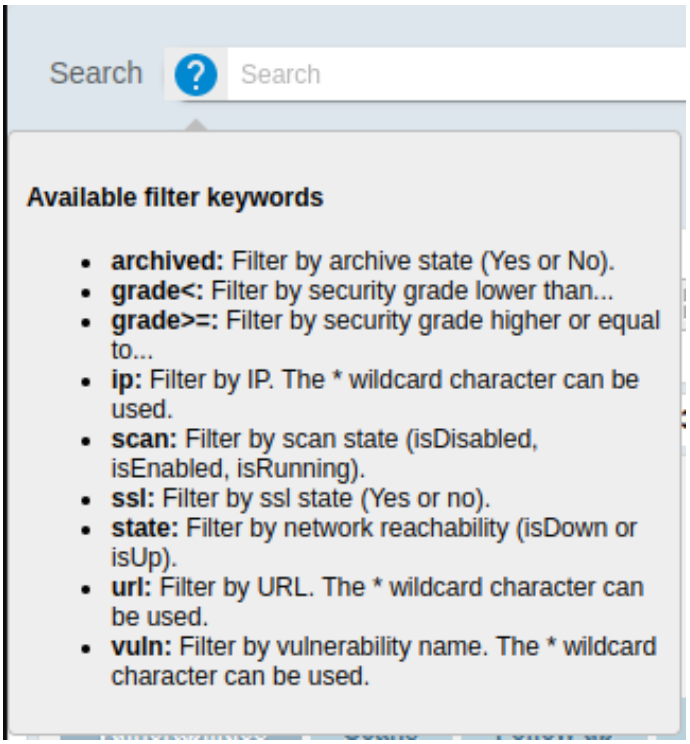
Vous avez également la possibilité de supprimer cette instance de l'application web en cliquant sur le bouton "Delete".

2.6.2 Présentation liste

La présentation liste fournissant le même but que celle des équipements, nous ne détaillerons ici que les différences.

Recherche

Tout comme dans la partie “ASSETS”, ce champ permet de filtrer les applications web en fonction de mots clés prédéfinis et de sauvegarder des vues.

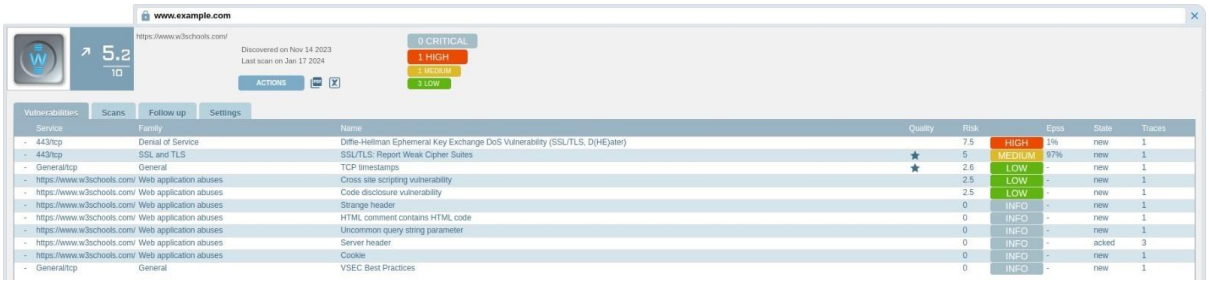


Les nouveaux mots clés possibles sont :

- **Ssl** : Rechercher par le type de connexion HTTP (HTTPS ou HTTP)
- **Url** : Rechercher par adresse url (le caractère joker * peut être utilisé)

2.6.3 Présentation détaillée

Pour obtenir la présentation détaillée d'une application web, il suffit de cliquer sur la vignette correspondante. Onglet "vulnerabilities" :



Cet onglet fournit la liste des vulnérabilités détectées sur l'application web avec des informations similaires à la partie "**ASSETS**".

ℹ️ **Note** : Chaque application web va également lister toutes les vulnérabilités de l'équipement sur lequel elle est hébergée, en plus des vulnérabilités qui lui sont propres.

Onglet 'Settings'

Cet onglet permet de configurer plusieurs éléments de l'application web :

Configuration d'identification

→ Le nom affiché de l'application web (si l'url de l'application web n'est pas représentative)

Configuration de l'état de l'application web

→ La possibilité de désactiver le scan. Cette action libère un jeton de licence. Le bouton "Enable scan" sera à nouveau affiché pour réactiver le scan.

→ La possibilité d'archiver l'application web. Cette action fait disparaître l'application web de l'interface et libère un jeton de licence.

ℹ️ **Note 1** : Les fonctions de désactivation de scan et d'archivage d'une application web ne sont pas utilisables dans le cas d'une version gratuite.

L’onglet “Scans” est similaire à l’onglet du même nom situé dans la vue détaillée d’un équipement. Pour plus de précisions à ce sujet, veuillez-vous reporter à la partie correspondante.

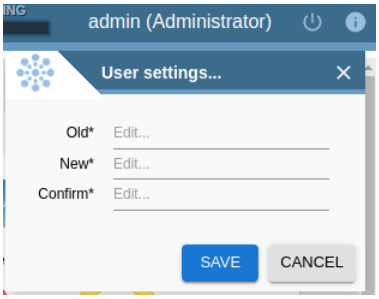
2.7 Autres fonctionnalités

2.7.1 Changement du mot de passe

Vous pouvez à tout moment modifier votre mot de passe, une fois connecté à l’application. Pour cela, il suffit de cliquer sur votre identifiant situé dans le bandeau supérieur. Une fenêtre apparaît alors vous demandant de saisir les informations suivantes :

- Votre mot de passe actuel
- Votre nouveau mot de passe
- La confirmation de votre nouveau mot de passe

Une fois ces informations renseignées, il vous suffit de valider, et la modification prend effet immédiatement.



2. Dépannage

→ **Des erreurs d'affichage surviennent ou des éléments de l'interface n'apparaissent pas**

Cette situation peut survenir si l'affichage du navigateur est "zoomé". Il suffit de rétablir l'affichage "normal" pour le voir réapparaitre.

→ **Il est impossible de télécharger le rapport avec Internet Explorer sous Windows Server**

La marche à suivre est la suivante : Dans le menu Outils de votre navigateur, sélectionnez les Options Internet, puis l'onglet Avancé. Faites descendre la barre de défilement sur le dernier chapitre Sécurité et décochez la ligne "Ne pas enregistrer les pages cryptées sur le disque".

→ **La découverte des équipements est lente**

Si la découverte est lente, la plage réseau est peut-être trop grande (/16 par exemple). Pour des résultats plus immédiats, vous pouvez réduire la plage dans un premier temps.

→ **Un équipement n'est pas découvert**

La découverte d'équipement réalise un "ping" et un scan de ports sur les 25 ports TCP les plus utilisés. Si l'équipement ne répond pas à au moins un de ces ports, l'équipement n'est pas découvert.

3. Glossaire

- **Scan** : Fait de balayer un ensemble de paramètres et de données.
- **Asset** : équipement ou ressource informatique.
- **Probe** : Sonde
- **Grades** : Notes ou évaluations
- **CVSS** : Common Vulnerability Scoring System, est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.
- **EPSS** : Exploit Prediction Scoring System, indique la probabilité qu'une vulnérabilité soit exploitée.