Inventory

Inventory is the IP addresses of all the workloads on your network, annotated with labels and other data that describes them. Your inventory includes workloads running on bare metal or virtual machines, in containers, and in the cloud. If applicable, it may also include workloads running on partner networks.

Collecting inventory data is an iterative process. Data from different sources for a single IP address can be merged, and new and changed IP addresses can be updated. Over time, management of your inventory should become increasingly dynamic.

You will work with and group your inventory using searches, filters, and scopes, based on the labels and annotations that are associated with each inventory item. Policies are applied to groups of workloads that are defined by the filters and scopes you define for your inventory.

Options for working with inventory vary depending on your role but may include **Search**, **Filters**, and **Upload**.

Étiquettes de charge de travail

Les étiquettes (parfois appelées balises, annotations, attributs, métadonnées ou contexte, bien que ces termes ne soient pas toujours complètement synonymes) sont la clé de la puissance de Cisco Secure Workload.

Des étiquettes lisibles par un humain décrivent vos charges de travail selon leur fonction, leur emplacement et d'autres critères.

Cisco Secure Workload prend en charge les méthodes suivantes pour l'ajout d'étiquettes d'utilisateur :

- Découverte par les agents Cisco Secure Workload exécutés sur les éléments de l'inventaire
- Importation manuelle à partir de fichiers de valeurs séparées par des virgules (CSV)

- Affectation manuelle au moyen de l'interface utilisateur
- Importation automatisée à l'aide des connecteurs de points terminaux
- Importation automatisée à l'aide des connecteurs pour l'enrichissement de l'inventaire
- Importation automatisée des étiquettes générées et personnalisées par l'orchestrateur (voir Orchestrateur externes)
- Importation automatisée à partir de connecteurs infonuagiques (voir Connecteurs infonuagiques)
- Vous pouvez spécifier des étiquettes d'inventaire lors de la création du script d'installation. Tous les agents installés à l'aide du script reçoivent automatiquement ces étiquettes. Seuls les déploiements de charges de travail Linux et Windows prennent en charge cette fonctionnalité.

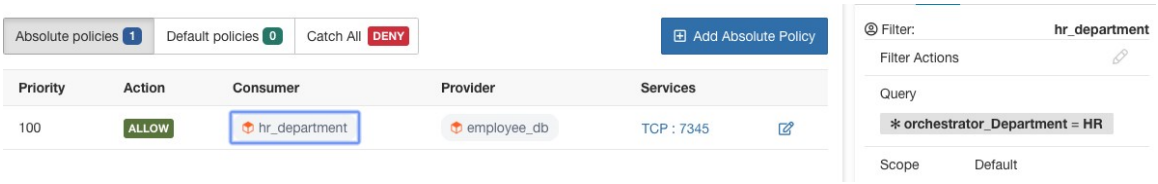
Importance des étiquettes

Les étiquettes vous permettent de définir une politique logique. Par exemple :

autoriser le trafic du consommateur hr_department au fournisseur employee_db

Plutôt que de préciser les membres des groupes de charges de travail de consommateurs et de fournisseurs, nous pouvons définir la politique logique à l'aide des étiquettes, comme le montre la figure suivante. Notez que cela permet de modifier dynamiquement les membres des groupes de consommateurs et de fournisseurs sans qu'il soit nécessaire de modifier la politique logique. Au fur et à mesure que des charges de travail sont ajoutées et retirées, Cisco Secure Workload est averti par les services que vous avez configurés, tels que les orchestrateurs externes et les connecteurs infonuagiques. Cela permet à Cisco Secure Workload d'évaluer l'appartenance au groupe de consommateurs *hr_department* et au groupe de fournisseurs *employee_db*.

Figure 1: Exemple de politique avec des étiquettes



Héritage d'étiquette basé sur le sous-réseau

L'héritage d'étiquette basé sur le sous-réseau est pris en charge. Les adresses IP et les sous-réseaux plus restreints héritent des étiquettes des sous-réseaux plus importants dont ils relèvent lorsque l'une des conditions suivantes est satisfaite :

- L'étiquette ne figure pas dans la liste des étiquettes pour le sous-réseau ou l'adresse de niveau inférieur.
- La valeur d'étiquette pour le sous-réseau/adresse de niveau inférieur est vide.

Considérez l'exemple suivant :

IP	Nom	Objectif	Environnement	Esprit-animal
10.0.0.1	Serveur 1	Trafic Web	production	
10.0.0.2				grenouille

IP	Nom	Objectif	Environnement	Esprit-animal
10.0.0.3				aigle
10.0.0.0/24	vlan Web		intégration	
10.0.0.0/16		Trafic Web		blaireau
10.0.0.0/8			test	ours

Les étiquettes pour l'adresse IP *10.0.0.3* sont *{« nom » : « Vlan Web », « objectif » : « trafic Web », « environnement » : « intégration », « esprit-animal »: « aigle »}*.

Préfixes d'étiquettes

Les étiquettes sont automatiquement affichées, avec un préfixe qui identifie la source des renseignements.

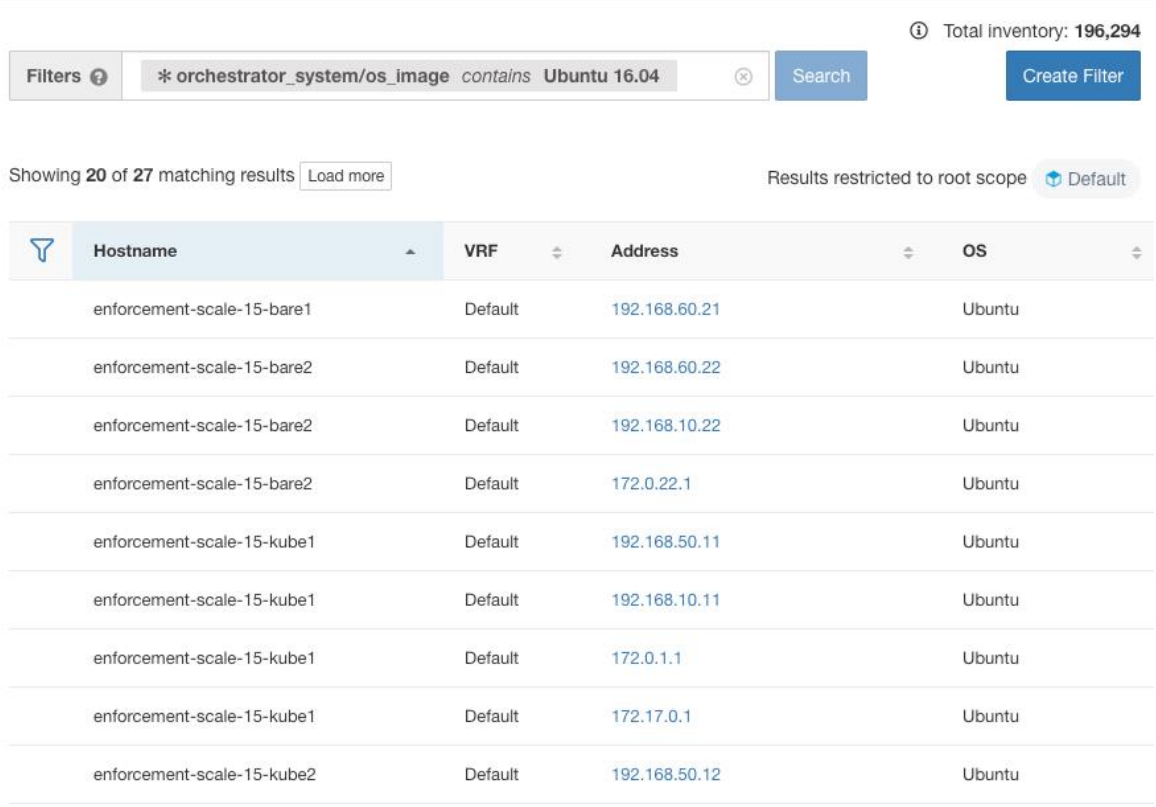
Toutes les étiquettes d'utilisateur sont précédées de * dans l'interface utilisateur (*user_* dans OpenAPI). En outre, les étiquettes importées automatiquement à partir d'orchestrateurs externes ou de connecteurs infonuagiques portent le préfixe orchestrator_. Pour les étiquettes importées à partir de connecteurs de point terminal, consultez les détails dans la section Connecteurs pour points terminaux, mais peut inclure des étiquettes précédées de *ldap_*.

Par exemple, une étiquette avec une clé de *department* (service) importée à partir de fichiers CSV téléversés par l'utilisateur apparaît dans l'interface utilisateur en tant que * *department* et dans OpenAPI en tant que *user_department*. Une étiquette avec une clé *location* (emplacement) importée d'un orchestrateur externe apparaît dans l'interface utilisateur en tant que * *orchestrator_location* et dans OpenAPI en tant que *user_orchestrator_location*.

La figure suivante montre un exemple de recherche dans l'inventaire utilisant l'étiquette générée par l'orchestrateur en utilisant le préfixe :

orchestrator_system/os_image:

Figure 2: Exemple de recherche d'inventaire avec des étiquettes générées par l'orchestrateur



Étiquettes générées par les connecteurs infonuagiques

Ces étiquettes s'appliquent aux données AWS et Azure. La source de ces étiquettes provient des charges de travail et des interfaces réseau d'un réseau virtuel AWS ou Azure. Les balises de la source sont fusionnées et affichées dans Cisco Secure Workload. Par exemple, si la balise de charge de travail est

```
env: prod
```

et la balise de l'interface réseau est

```
env: prod
```

, la valeur de l'étiquette dans Cisco Secure Workload est

```
prod,test
```

, qui s'affiche dans la colonne **orchestrator_env** sur la page du connecteur respective.

Pour connaître les étiquettes propres à AKS, EKS et GKE, consultez également les étiquettes relatives aux grappes Kubernetes.

Table 1: Étiquettes dans l'inventaire effectué à l'aide d'un connecteur infonuagique

Clé	Valeur
orchestrator_system/orch_type	AWS ou Azure

Clé	Valeur
orchestrator_system/cluster_name	*<Cluster_name est le nom donné par l'utilisateur pour la configuration de ce connecteur>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/cluster_id	*<ID du réseau virtuel>*

Étiquettes spécifiques à l'instance

Les étiquettes suivantes sont propres à chaque nœud :

Clé	Valeur
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	*<Numéro d'instance attribué par la plateforme>*
orchestrator_system/machine_name	<PublicDNS(Nom de domaine complet) attribué à ce nœud par AWS>-ou-<Nom d'instance dans Azure>
orchestrator_system/segmentation_enabled	*<Indicateur permettant de déterminer si la segmentation est activée sur l'inventaire>*
orchestrator_system/virtual_network_id	*<ID du réseau virtuel auquel l'inventaire appartient>*
orchestrator_system/virtual_network_name	*<Nom du réseau virtuel auquel appartient l'inventaire>*
orchestrator_system/interface_id	<Identifiant de l'interface réseau élastique attachée à cet inventaire>
orchestrator_system/region	<Région à laquelle appartient l'inventaire>
orchestrator_system/resource_group	(Cette balise s'applique uniquement à l'inventaire Azure)
orchestrator_'<Tag Key>'	<Valeur de l'étiquette>Paire valeur-clé pour un nombre quelconque de balises personnalisées affectées à l'inventaire dans le portail infonuagique.

Étiquettes liées aux grappes Kubernetes

Les informations suivantes s'appliquent à Kubernetes standard, OpenShift et à Kubernetes exécuté sur les plateformes infonuagique prises en charge (EKS, AKS et GKE).

Pour chaque type d'objet, Cisco Secure Workload importe l'inventaire en direct à partir d'une grappe Kubernetes, y compris les étiquettes associées à l'objet. Les clés et les valeurs d'étiquettes sont importées telles quelles.

En plus d'importer les étiquettes définies pour les objets Kubernetes, Cisco Secure Workload génère également des étiquettes qui facilitent l'utilisation de ces objets dans les filtres d'inventaire. Ces étiquettes supplémentaires sont particulièrement utiles pour définir les portées et les politiques.

Générer des étiquettes pour toutes les ressources

Cisco Secure Workload ajoute les étiquettes suivantes à tous les nœuds, pods et services récupérés du serveur d'API Kubernetes/OpenShift/EKS/AKS/GKE.

Clé	Valeur
orchestrator_system/orch_type	kubernetes
orchestrator_system/cluster_id	*<L'identifiant unique UUID de la configuration de la grappe dans Cisco Secure Workload>*
orchestrator_system/cluster_name	*<Nom de la grappe Kubernetes>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/namespace	*<L'espace de noms Kubernetes/OpenShift/EKS/AKS/GKE de cet élément>*

Étiquettes propres au nœud

Les étiquettes suivantes sont générées pour les nœuds uniquement.

Clé	Valeur
orchestrator_system/workload_type	Machine
orchestrator_system/machine_id	*<UUID attribué par Kubernetes/OpenShift>*
orchestrator_system/machine_name	*<Nom donné à ce nœud>*
orchestrator_system/kubelet_version	*<Version du kubelet fonctionnant sur ce nœud>*
orchestrator_system/container_runtime_version	*<La version du conteneur en cours d'exécution sur ce nœud>*

Étiquettes spécifiques aux pods

Les étiquettes suivantes sont générées pour les pods uniquement.

Clé	Valeur
orchestrator_system/workload_type	pod
orchestrator_system/pod_id	*<UUID attribué par Kubernetes/OpenShift>*
orchestrator_system/pod_name	*<Nom donné à ce pod>*
orchestrator_system/hostnetwork	*<vrai|faux>indiquant si le pod est en cours d'exécution dans le réseau hôte*
orchestrator_system/machine_name	*<Nom du nœud sur lequel le pod est exécuté>*
orchestrator_system/service_endpoint	*[Liste des noms de services fournis par ce pod]*

Étiquettes propres au service

Les étiquettes suivantes sont générées pour les services uniquement.

Clé	Valeur
orchestrator_system/workload_type	service
orchestrator_system/service_name	*<Nom donné à ce service>*

- (Pour Kubernetes géré infonuagique uniquement) Les services de type ServiceType : Équilibreur de charge sont pris en charge uniquement pour la collecte de métadonnées, et non pour la collecte de données de flux ou pour l'application de politiques.

Tip Le filtrage des éléments à l'aide de **orchestrator_system/service_name** n'est pas la même chose que l'utilisation de **orchestrator_system/service_endpoint**.

Par exemple, l'utilisation du filtre **orchestrator_system/service_name=web** sélectionne tous les *services* avec le nom **web** tandis que **orchestrator_system/service_endpoint=web** sélectionne tous les *pods* qui fournissent un service avec le nom **web**.

Exemple d'étiquettes pour les grappes Kubernetes

L'exemple suivant montre une représentation YAML partielle d'un nœud Kubernetes et les étiquettes correspondantes importées par Cisco Secure Workload.

```
- apiVersion: v1
kind: Node
metadata:
  annotations:
    node.alpha.kubernetes.io/ttl: "0"
    volumes.kubernetes.io/controller-managed-attach-detach: "true"
  labels:
    beta.kubernetes.io/arch: amd64
    beta.kubernetes.io/os: linux
    kubernetes.io/hostname: k8s-controller
```

Table 2: Étiquettes clés importées de Kubernetes

Clés d'étiquette importées
orchestrator_beta.kubernetes.io/arch
orchestrator_beta.kubernetes.io/os
orchestrator_kubernetes.io/hostname
orchestrator_annotation/node.alpha.kubernetes.io/ttl
orchestrator_annotation/volumes.kubernetes.io/controller-managed-attach-detach
orchestrator_system/orch_type
orchestrator_system/cluster_id

Clés d'étiquette importées
orchestrator_system/cluster_name
orchestrator_system/namespace
orchestrator_system/workload_type
orchestrator_system/machine_id
orchestrator_system/machine_name
orchestrator_system/kubelet_version
orchestrator_system/container_runtime_version

Importation d'étiquettes personnalisées

Vous pouvez téléverser ou attribuer manuellement des étiquettes personnalisées pour associer des données définies par l'utilisateur à des hôtes spécifiques. Ces données définies par l'utilisateur sont utilisées pour annoter les flux et l'inventaire associés.

Il y a des limites sur le nombre d'adresses IPv4/IPv6 et de sous-réseaux qui peuvent être étiquetés dans toutes les portées racine, quelle que soit la source de l'étiquette (saisie manuellement ou téléversée, intégrée à l'aide de connecteurs ou d'orchestrateurs externes, etc.). Pour en savoir plus, consultez Limites d'étiquettes.

Lignes directrices pour le chargement de fichiers d'étiquettes

Procedure

Étape 1 Pour afficher un exemple de fichier, dans le volet gauche, sélectionnez **Organize(Organiser)** > **Label Management (Gestion des étiquettes)** > **User Defined Label Upload**(Chargement d'étiquettes définies par l'utilisateur) , puis cliquez sur **Download a Sample** (Télécharger un exemple).

Étape 2 Les fichiers CSV utilisés pour charger les étiquettes utilisateur doivent inclure une clé d'étiquette (adresse IP).

Étape 3 Pour utiliser des caractères non latins dans les étiquettes, le fichier CSV doit être au format UTF-8.

Étape 4 Assurez-vous que les fichiers CSV respectent les directives décrites dans la section Schéma de clé d'étiquette.

Étape 5 Tous les fichiers téléversés doivent suivre le même schéma.

Schéma de clé d'étiquette

Lignes directrices régissant les noms de colonne

- Il doit y avoir une colonne avec un en-tête « IP » dans le schéma de clé d'étiquette. En outre, il doit y avoir au moins une autre colonne avec des attributs pour l'adresse IP.

- La colonne « VRF » revêt une signification particulière dans le schéma d'étiquette. Si elle figure, elle doit correspondre à la portée racine dans laquelle vous téléversez les étiquettes. Elle est obligatoire lors du chargement du fichier CSV à l'aide d'une API indépendante de la portée.
- Les noms de colonne ne peuvent contenir que les caractères suivants : des lettres, des chiffres, des espaces, des tirets, des traits de soulignement et des barres obliques.
- Les noms de colonne ne peuvent pas dépasser 200 caractères.
- Les noms de colonnes ne peuvent pas comporter le préfixe « orchestrator_ », « TA_ », « ISE_ », « SNOW_ » ou « LDAP_ », car ils peuvent entrer en conflit avec les étiquettes des applications internes.
- Le fichier CSV ne doit pas contenir de noms de colonnes en double.

Directives régissant les valeurs de colonne

- Le nombre de caractères du nom est limité à 255. Toutefois, ils doivent être aussi courts que possible tout en restant clairs, caractéristiques et significatifs pour les utilisateurs.
- Les clés et les valeurs ne sont pas sensibles à la casse. Cependant, une cohérence est recommandée.
- Les adresses figurant dans la colonne « IP » doivent être conformes au format suivant :
  - Les adresses IPv4 peuvent être au format « x.x.x.x » et « x.x.x.x/32 ».
  - Les sous-réseaux IPv4 doivent être du format « x.x.x.x/<netmask>, où netmask est un entier compris entre 0 et 31.
  - Les adresses IPv6 au format long (« x:x:x:x:x:x:x:x » ou « x:x:x:x:x:x:x:x/128 ») et au format canonique (« x:x::x » ou « x:x::x/128 ») sont pris en charge.
  - Les sous-réseaux IPv6 au format long (« x:x:x:x:x:x:x:x/<netmask> ») et le format canonique (« x:x::x/<netmask> » sont pris en charge. Le masque réseau doit être un entier compris entre 0 et 127.

L'ordre des colonnes n'a pas d'importance. Les 32 premières colonnes définies par l'utilisateur seront automatiquement activées en vue de l'étiquetage. Si plus de 32 colonnes sont téléversées, vous pouvez en activer jusqu'à 32 en utilisant les cases à cocher à droite de la page.

Charger des étiquettes personnalisées

Les étapes suivantes expliquent comment les utilisateurs ayant un rôle d' **administrateur de site**, **d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent charger des étiquettes.

Before you begin

Pour charger les étiquettes personnalisées, créez un fichier CSV selon les directives de la section sur le chargement des fichiers d'étiquettes.

Procedure

Étape 1 Dans le volet gauche, sélectionnez **Organize (Organiser)** > **User Defined Label Upload(Chargement d'étiquettes définies par l'utilisateur)** > **CSV Upload (Chargement CSV)**, puis sous **Upload New Labels**(Télécharger de nouvelles étiquettes), cliquez sur **Select File** (Sélectionner un fichier).

Étape 2 Dans le volet gauche, sélectionnez **Organize (Organiser)** > **Label Management (Gestion des étiquettes)**, puis sous **Upload New Labels** (Télécharger de nouvelles étiquettes), cliquez sur **Select File** (Sélectionner un fichier).

Étape 3 Sélectionnez l'opération Ajouter, Fusionner ou Supprimer.

- **Add (Ajouter) :** Ajoute des étiquettes aux adresses ou aux sous-réseaux nouveaux et existants. Résout les conflits en sélectionnant les nouvelles étiquettes plutôt que les existantes. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo » : « 1 », « bar » : « 2 »}* et que le fichier CSV contient *{« z » : « 1 », « bar » : « 3 »}*, Add (Ajouter) définit les étiquettes pour cette adresse sur *{« foo » : « 1 », « z » : « 1 », « bar » : « 3 »}*.
- **Merge (Fusionner) :** Fusionne les étiquettes avec les adresses ou les sous-réseaux existants. Résout les conflits en sélectionnant des valeurs non vides sur les valeurs vides. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo » : « 1 », « bar » : « 2 », « qux », « corge » : « 4 »}* et que le fichier CSV contient *{ « z » : « 1 , « bar » : « », « qux » : « 3 », « corge : « 4-updated »}*, Merge (Fusionner) définit les étiquettes pour cette adresse à *{« foo » : "1 » , « z » : « 1« 1 »», « bar » : « 2 », « qux » : « 3 », « corge » : « 4-updated »}*.

  Note La valeur de « bar » dans n'est pas réinitialisée à « » (vide), au lieu de cela, la valeur existante de « bar » = « 2 » est conservée.

- **Delete (Supprimer) :** Cette option supprime les étiquettes pour une adresse ou un sous-réseau, ce qui peut avoir une incidence considérable sur les portées, les filtres, les politiques et le comportement appliqué. Pour obtenir des renseignements importants, consultez la section *Supprimer des étiquettes*.

Important : La fonction de suppression, lors du chargement des étiquettes personnalisées, supprimera TOUTES les étiquettes associées aux adresses IP ou aux sous-réseaux précisés, et ne se limitera pas aux colonnes répertoriées dans le fichier CSV. Par conséquent, l'opération Delete (Supprimer) doit être utilisée avec prudence.

Étape 4 Cliquez sur **Upload** (Téléverser).

Rechercher des étiquettes

Les utilisateurs ayant un rôle d' **administrateur de site**, **de service d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent rechercher, afficher et modifier les étiquettes attribuées à une adresse IP ou à un sous-réseau.

Procedure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes), cliquez sur **Search and Assign** (Rechercher et attribuer).

Étape 2 Dans le champ **IP or Subnet** (adresse IP ou sous-réseau), saisissez l'adresse IP ou le sous-réseau, puis cliquez sur **Next**(suivant).

Dans la page Assign Labels (Attribuer des étiquettes), les étiquettes existantes saisies pour l'adresse IP ou le sous-réseau sont affichées.

Attribuer ou modifier manuellement des étiquettes personnalisées

Les utilisateurs ayant le rôle d' **administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent affecter manuellement des étiquettes à une adresse IP ou à un sous-réseau donné.

Procédure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes), cliquez sur **Search and Assign** (Rechercher et attribuer).

Étape 2 Dans le champ **IP or Subnet** (adresse IP ou sous-réseau), saisissez l'adresse IP ou le sous-réseau, puis cliquez sur **Next**(suivant).

La page Assign Labels (Affecter des étiquettes) s'affiche. Notez que les étiquettes existantes seront affichées et peuvent être modifiées.

Étape 3 Pour ajouter une nouvelle étiquette, dans la section **Étiquettes de <IP address/subnet>** , saisissez le nom et la valeur de l'étiquette, puis cliquez sur **Confirm** (Confirmer). Cliquez sur **Next** (suivant).

Étape 4 Passez en revue les modifications et cliquez sur **Assign** (Affecter) pour les valider.

Télécharger des étiquettes

Les utilisateurs ayant un rôle d' **administrateur de site**, **de service d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent télécharger des étiquettes précédemment définies appartenant à une portée racine.

Procedure

Étape 1 Dans la page **Label Management** (gestion des étiquettes), cliquez sur **User Defined Label Upload** (téléverser les étiquettes définies par l'utilisateur).

Étape 2 Dans la section **Download Existing Labels**(Télécharger les étiquettes existantes), cliquez sur **Download Labels** (Télécharger les étiquettes).

Les étiquettes utilisées par Cisco Secure Workload sont téléchargées dans un fichier CSV.

Modifier les étiquettes

Avertissement Si vous devez modifier une étiquette, faites-le avec prudence, car cela modifie les membres et les effets des requêtes, des filtres, des portées, des grappes, des politiques et du comportement appliqué existants qui reposent sur cette dernière.

Procédure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes), cliquez sur l'onglet **Search and Assign** (Rechercher et attribuer).

Étape 2 Dans le champ **IP or Subnet** (adresse IP ou sous-réseau), saisissez l'adresse IP ou le sous-réseau, puis cliquez sur **Next**(suivant).

Les étiquettes utilisées par Cisco Secure Workload pour l'adresse IP ou le sous-réseau saisi s'affichent.

Étape 3 Dans la colonne **Actions**, cliquez sur l'icône **Edit** (modifier) pour modifier le nom et la valeur de l'étiquette requise.

Étape 4 Cliquez sur **Confirm** (Confirmer) puis sur **Next**(suivant).

Étape 5 Passez en revue les modifications et cliquez sur **Assign** (Attribuer).

Désactiver les étiquettes

Une façon de modifier le schéma consiste à désactiver les étiquettes. *Procédez avec prudence*.

Procédure

Étape 1 Accédez à la page **Label Management** (gestion des étiquettes).

Étape 2 Pour l'étiquette requise, dans la colonne **Actions**, sélectionnez **Disable** (désactiver) et confirmez pour supprimer l'étiquette de l'inventaire en cliquant sur **Yes**(oui).

Si vous décidez ultérieurement d'activer l'étiquette, cliquez sur **Enable**(Activer) pour utiliser l'étiquette.

Supprimer des étiquettes

Avertissement Une façon de modifier le schéma consiste à désactiver les étiquettes et à les supprimer. Procédez avec prudence. Cette action supprime l'étiquette sélectionnée, ce qui a une incidence sur tous les **filtres** et toutes les **portées** qui en dépendent. Assurez-vous que ces étiquettes ne sont pas utilisées. Cette action ne peut pas être annulée.

Procédure

Étape 1 Désactivez les étiquettes. Consultez la section désactiver_étiquettes.

Étape 2 Cliquez sur l'icône de la **corbeille** et confirmez en cliquant sur **Yes** (oui) pour supprimer l'étiquette.

Afficher l'utilisation des étiquettes

L'inventaire des adresses IP ou des sous-réseaux est mis à jour avec les étiquettes personnalisées téléversées à l'aide de fichiers CSV ou attribuées manuellement par les utilisateurs. Les étiquettes sont ensuite utilisées pour définir les portées et les filtres, et les politiques d'application sont créées en fonction de ces filtres. Par conséquent, la compréhension de l'utilisation des étiquettes est essentielle, car toute modification apportée aux étiquettes a une incidence directe sur les portées, les filtres et les politiques de Cisco Secure Workload.

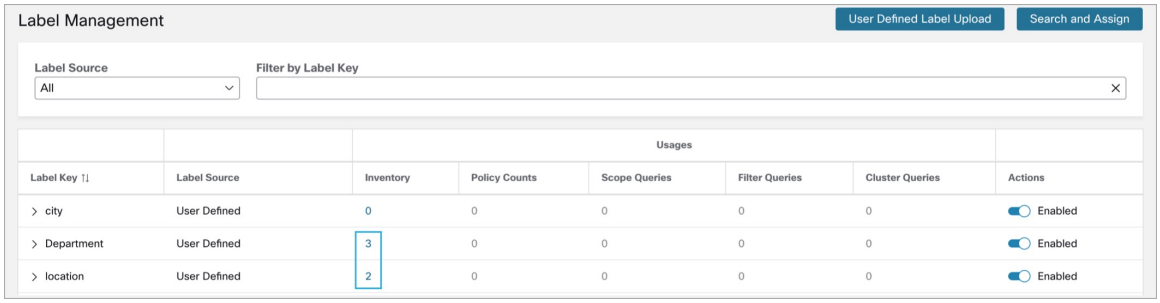
Pour afficher l'utilisation des étiquettes :

Procédure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes) , les clés d'étiquette, les cinq principales valeurs des étiquettes utilisées, l'inventaire, les portées, les filtres et les grappes utilisant les étiquettes personnalisées sont affichés.

Étape 2 Dans la colonne Usages (utilisations), cliquez sur les valeurs de décompte de l'inventaire, des portées ou des filtres. Par exemple, pour afficher les portées à l'aide de l'étiquette « Location » (Emplacements), cliquez sur le nombre de requêtes sur la portée.

Illustration 3 : Afficher les portées de l'étiquette sélectionnée



La page Scopes and Inventory (Portées et inventaire) s'affiche et la requête filtre automatiquement les portées avec l'étiquette sélectionnée.

Remarque Vous pouvez uniquement afficher l'utilisation des étiquettes téléversées à l'aide de fichiers CSV ou attribuées manuellement à l'adresse IP ou au sous-réseau.

Créer un processus pour la tenue des étiquettes

Votre réseau et votre inventaire changeront, et vous devez planifier de mettre à jour les étiquettes pour refléter ces changements.

Par exemple, si une charge de travail est supprimée et que son adresse IP est réaffectée à une charge de travail avec un objectif différent, vous devez mettre à jour les étiquettes associées à cette charge de travail. Cela est vrai pour les étiquettes téléversées manuellement et pour les étiquettes conservées dans d'autres systèmes et acquises à partir d'autres systèmes, comme une base de données de gestion de configuration (CMDB).

Créez un processus pour vous assurer que vos étiquettes sont mises à jour régulièrement et en permanence, et ajoutez ce processus à votre routine d'entretien du réseau.

Portées et inventaire

Aperçu de la portée et de l'inventaire

Cette section permet de visualiser la hiérarchie de la portée, ainsi que tout l'inventaire qu'elle contient. Les portées classent l'ensemble de l'inventaire selon une structure hiérarchique. Consultez Inventory, on page 1. Sur la gauche se trouve l'interface utilisateur du répertoire de la portée. Ici, vous pouvez parcourir votre hiérarchie de portée. Chaque portée est affichée dans une carte de portée. Elle affiche le nom de la portée, le nombre de portées enfants, le décompte de l'inventaire et, le cas échéant, l'inventaire non catégorisé. Cliquer sur une carte de portée met à jour le volet de droite pour afficher les détails de cette portée ainsi qu'une liste filtrable de tout son inventaire.

Principes de conception de la portée

1. L'inventaire est apparié à l'arborescence de la portée en fonction de la correspondance de requête dynamique.
   - Les requêtes peuvent correspondre à l'adresse IP ou au sous-réseau, ou à l'étiquette (option préférée)
   - L'arbre est formé grâce à des requêtes conjuguées à chaque couche.
2. La structure de la portée peut être propre à l'emplacement, le cas échéant.
   - Nuage combiné contre Centre de données et Nuage spécifique contre Emplacement géographique
3. Chaque couche de l'arborescence de portée doit constituer un point d'ancrage pour le :
   - Contrôle des politiques
   - Contrôle d'accès en fonction des rôles (RBAC)
4. Chaque portée enfant doit être un sous-ensemble de sa portée parente.
   - Assurez-vous que les portées ne se chevauchent pas, voir Chevauchement de portée

Note Chaque organisation est structurée différemment et, selon votre secteur d'activité, nécessite des approches différentes. choisir un objectif lors de la conception de votre hiérarchie de portée; l'emplacement, l'environnement ou l'application.

Note N'utilisez pas d'adresse IP ou de sous-réseau pour définir des portées qui impliquent l'inventaire Kubernetes. Vous devez utiliser des étiquettes pour définir la portée et la politique pour ces charges de travail. L'adresse IP seule n'est pas suffisante pour identifier les services de pods; l'utilisation de l'adresse IP pour la définition de la portée produira des résultats non fiables.

Principales caractéristiques

La fonction de filtrage pour les portées et l'inventaire vous permet de parcourir rapidement l'arborescence des portées ou de filtrer la hiérarchie des portées et les éléments d'inventaire de la portée sélectionnée.

Le décompte de l'inventaire est affiché dans la carte des portées, ce qui permet de voir rapidement le nombre de charges de travail dans la portée.

Portées

Les portées sont un élément essentiel de la configuration et des politiques dans Cisco Secure Workload. Les portées constituent un ensemble de charges de travail organisées selon une hiérarchie. Les charges de travail étiquetées pour servir d'attributs qui construisent un modèle sur leur emplacement, leur rôle et leur fonction dans votre environnement. Les portées fournissent une structure pour prendre en charge des mécanismes dynamiques comme l'identification et les attributs associés à une adresse IP qui peuvent évoluer avec le temps.

Les portées sont utilisées pour regrouper les applications de centre de données et, avec les rôles, elles permettent un contrôle précis de leur gestion. Par exemple, les portées sont utilisées sur l'ensemble du produit pour définir l'accès aux Gérer le cycle de vie des politiques dans Cisco Secure Workload, aux flux et aux Filtres.

Les portées sont définies hiérarchiquement comme des ensembles d'arborescences, la racine correspondant à un **VRF**. Par conséquent, chaque hiérarchie d'arborescence de portée représente des données disjointes qui ne se chevauchent pas avec une autre arborescence de portée, voir la section Chevauchement de portée.

Définition de la portée

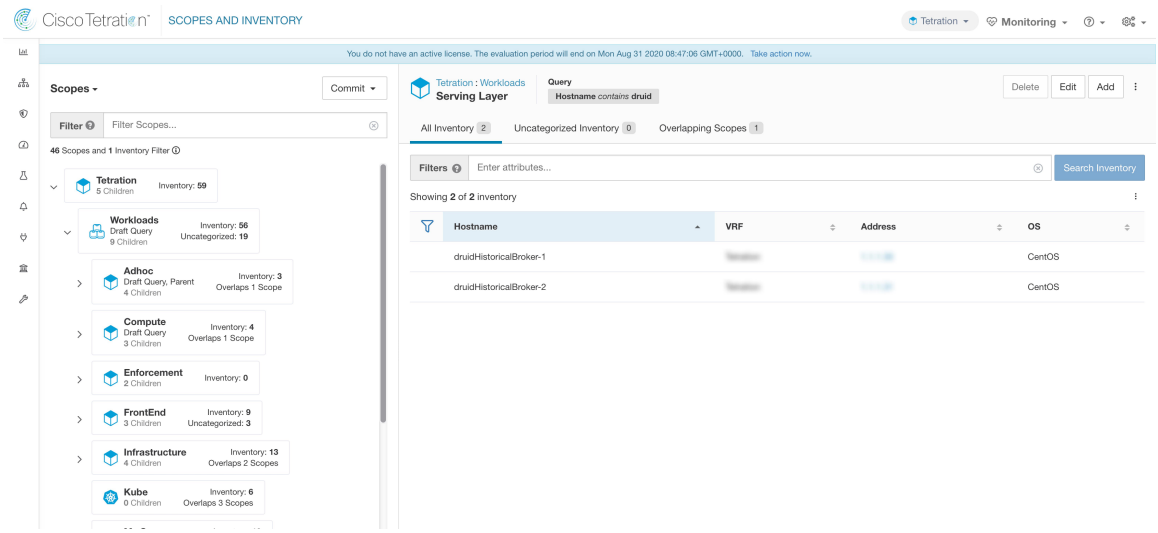
Chaque portée est définie par les attributs ci-dessous :

Attribut	Description
Portée parente	Le parent de la nouvelle portée définit la structure hiérarchique de l'arborescence.
Nom	Le nom pour identifier la portée.
Type	Utilisé pour spécifier différentes catégories d'inventaire. Si aucun n'est applicable, ou si la portée contient une combinaison, ce champ peut être laissé vide.
Requête	La requête définissant la portée individuelle.

Note Les portées doivent être définies dans une hiérarchie qui imite la hiérarchie de propriété des applications de l'organisation.

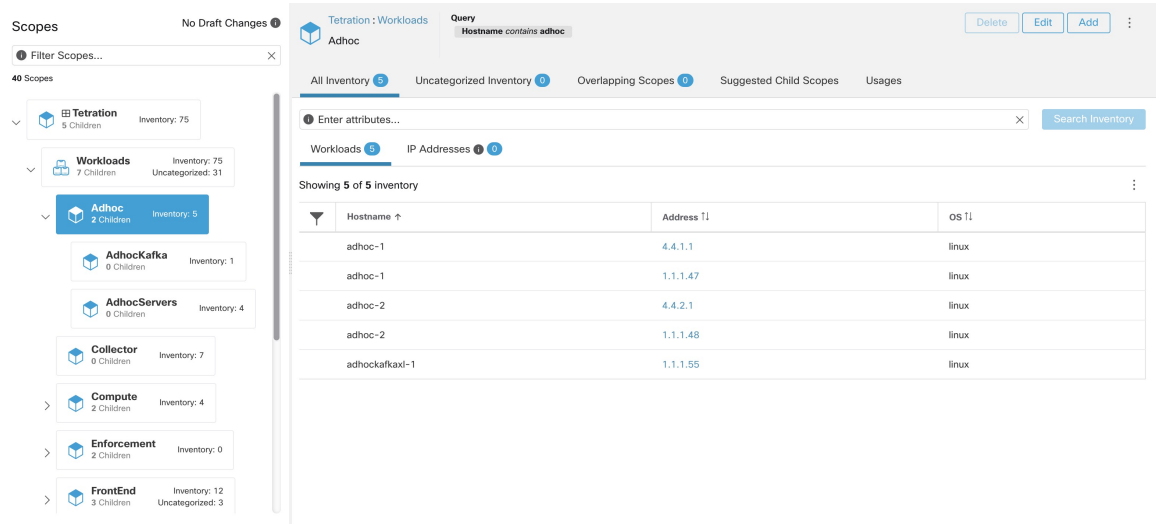
Note La requête peut correspondre à l'adresse IP du sous-réseau ou à d'autres attributs de l'inventaire.

Figure 4: Exemple de navigation dans la hiérarchie des portées



Le répertoire des portées affiche la hiérarchie des portées et certains détails de chaque portée (par exemple, le nombre d'inventaires, le nombre de portées enfants, les espaces de travail). Cliquez sur une portée pour la sélectionner, et le volet d'informations à droite se met à jour avec plus d'informations sur cette portée et l'inventaire de cette dernière.

Figure 5: Inventaire



Filtre de portée

Les utilisateurs peuvent utiliser le filtre Portée pour identifier rapidement différents détails de portée tels que les portées et les requêtes qui se chevauchent. La fonction de filtre est également utile pour identifier les modifications de requête, les modifications de parent, etc.

Champ	Description
Nom	Filtrer par le nom de la portée ou du filtre d'inventaire.

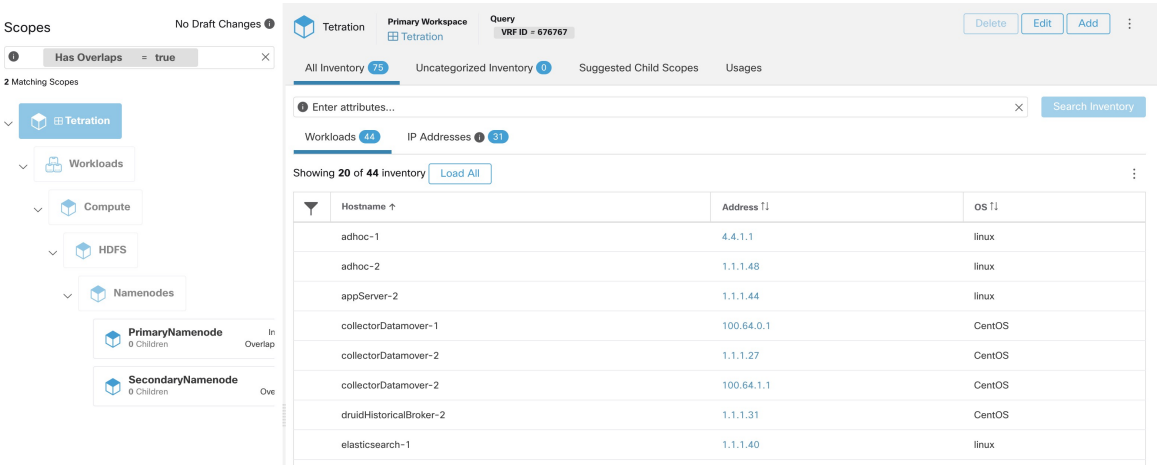
Champ	Description
Description	Filtrer en fonction du texte figurant dans la description d'une portée.
Requête	Filtrer par champs ou valeurs utilisés dans la requête.
Changement de requête	Filtrer par portées qui ont une requête non validée.
Changement de parent	Filtrer par portées qui ont été déplacées dans le brouillon mais non validées.
Est-ce un filtre d'inventaire?	Affichez les filtres d'inventaire limités à leur portée de propriété.
Possède un espace de travail	Filtrez par portées qui ont un espace de travail principal.
Possède un espace de travail appliqué	Filtrer par portées qui ont un espace de travail principal appliqué.
A des chevauchements	Filtrer par portées qui ont un inventaire en commun avec une portée connexe.
A une requête non valide	Filtrez par portées dont la requête utilise des étiquettes non valides ou inconnues.

Exemples :

A des chevauchements

Exemple de chevauchement de portée

Figure 6: A des chevauchements

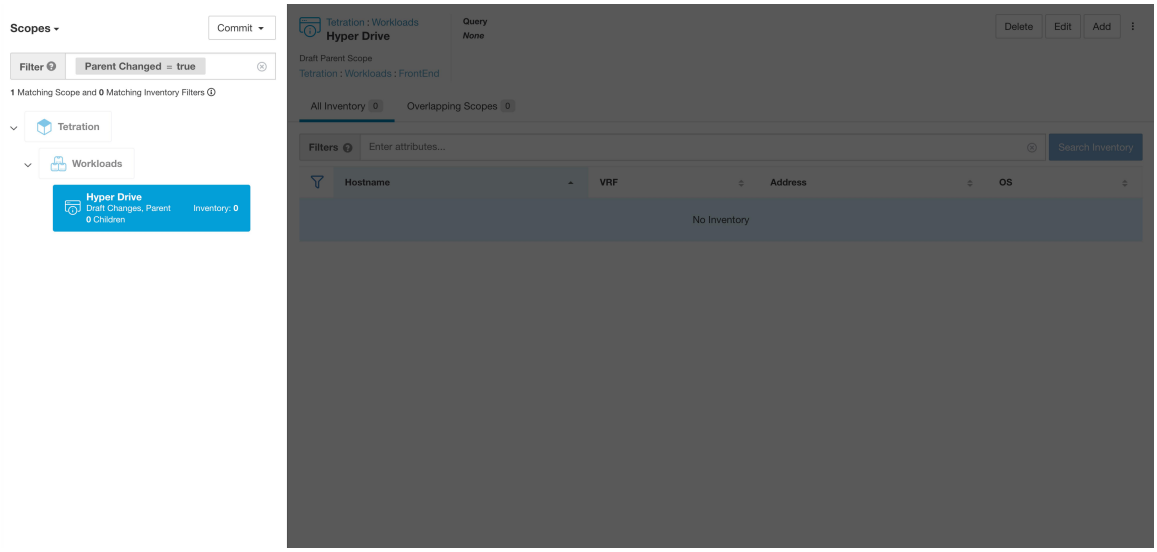


Pour en savoir plus, consultez Chevauchement de portée.

Changement de parent

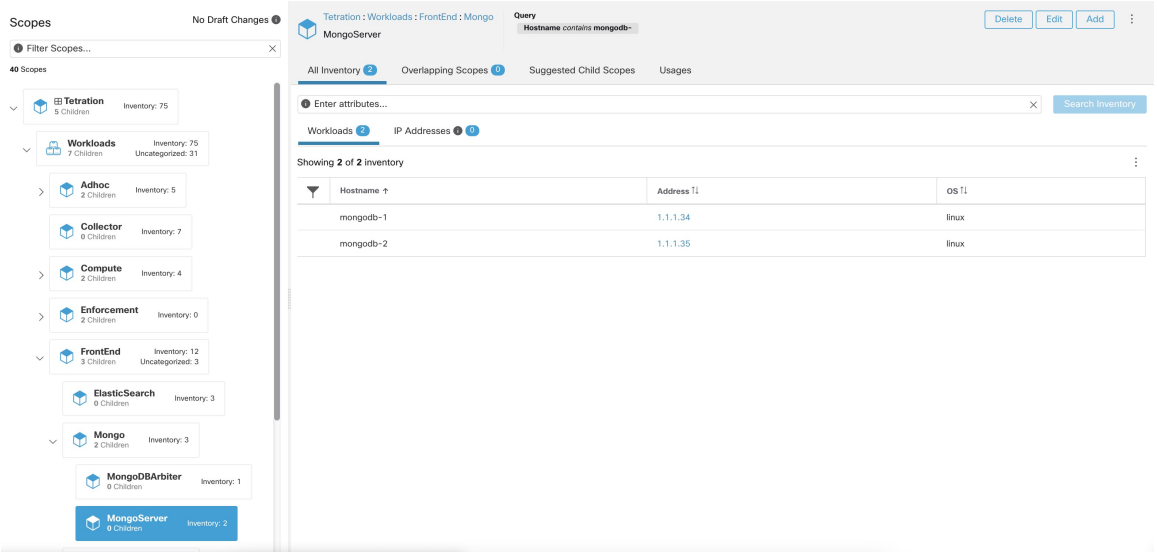
Les portées ont été déplacés dans le brouillon, mais pas encore validés.

Figure 7: Changement de parent



Requêtes de portée complète

Figure 8: Exemple de hiérarchie de portée



Les portées sont définies hiérarchiquement, la requête complète de la portée est définie comme le « et » logique de la portée avec tous ses parents. En utilisant l'exemple ci-dessus, les ressources affectées à `Workloads:FrontEnd:Mongo`

La portée correspondrait à :

```
vrf_id = 676767 and (ip in 1.1.1.0/24) and (Hostname contains mongo).
```

Où vrf_id = 676767 provient de la requête de portée racine et IP dans 1.1.1.0/24 de la requête de portée parente.

Note Il est conseillé de ne pas avoir des requêtes qui se chevauchent au même niveau. Cela supprime l'importance de l'ordre et réduit la confusion. Voir Chevauchement de portée

Fourniture de l'accès aux portées

Vous pouvez accorder les capacités de lecture, d'écriture, de mise en application et de propriétaire sur les portées. Pour en savoir plus, consultez la section sur les **rôles** dans le *Guide de l'utilisateur de Cisco Secure Workload*.

Un utilisateur a accès à une « sous-arborescence ». C'est-à-dire à une portée donnée et tous ses enfants. Dans l'exemple précédent, vous avez l'accès en lecture à la portée `Workloads:FrontEnd` et auriez, par héritage, accès en lecture à toutes les portées sous `Workloads:FrontEndl`, y compris :

- `Workloads:FrontEnd:Mongo`
- `Workloads:FrontEnd:ElasticSearch`
- `Workloads:FrontEnd:Redis`
- `etc. . .`

Il est possible de définir des rôles avec un accès à plusieurs portées. Par exemple, un rôle « Administrateur Mongo » pourrait avoir un accès Propriétaire aux portées :

- `Workloads:FrontEnd:Mongo:MongoServer`
- `Workloads:FrontEnd:Mongo:MongoDBArbiter`

Les rôles et les capacités vous permettent d'avoir un accès horizontal à la hiérarchie de la portée.

Les capacités de portée sont également héritées. Par exemple, avoir la capacité d'écriture sur une portée permet également de lire ces informations.

Affichage des portées

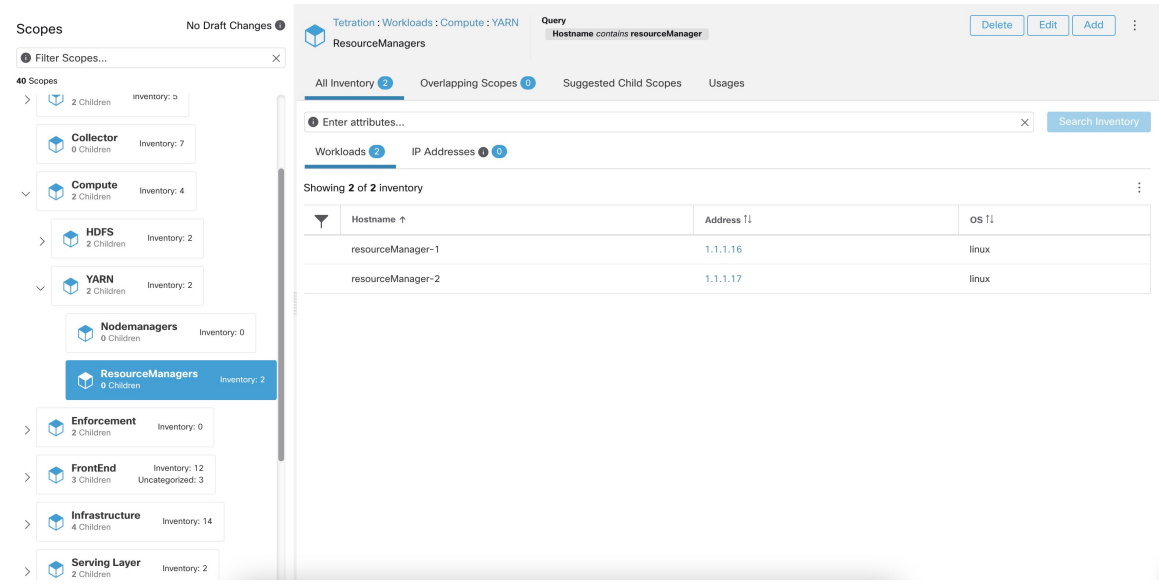
Chaque utilisateur peut afficher l'arborescence de portées à laquelle il a accès. Les utilisateurs qui ont le droit de propriétaire sur la portée racine ont la possibilité de créer, de modifier et de supprimer une portée dans cette arborescence. Pour accéder à cet affichage :

Dans la barre de navigation de gauche, cliquez sur **Organize (Organiser)** > **Scopes and Inventory (Portées et inventaire).**

Vous pouvez parcourir la hiérarchie complète des portées (jusqu'à la racine) pour toutes les portées auxquelles vous avez accès. Ce parcours complet fournit un contexte, car les utilisateurs peuvent créer des politiques pour n'importe quelle portée. Plusieurs actions peuvent être effectuées sur cette page :

- Cliquez sur le chevron dans la hiérarchie de la portée pour afficher les enfants de cette portée.
- En cliquant sur la carte de la portée, le volet de droite s'actualise et affiche les détails de cette portée ainsi qu'une liste filtrable de l'ensemble de son inventaire.

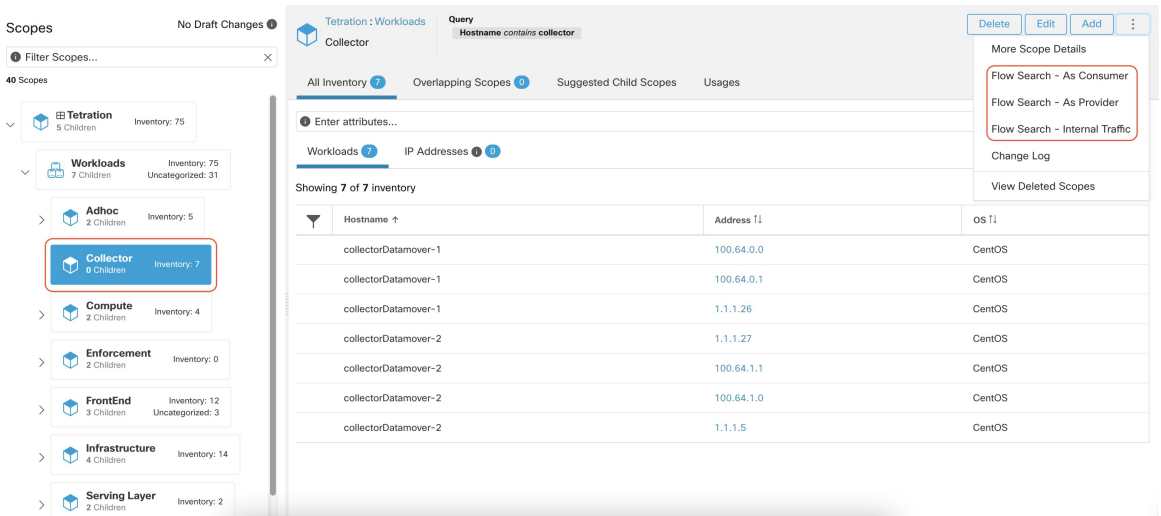
Figure 9: Exemple d'affichage non administrateur



Recherche de flux faisant référence à une portée

Des raccourcis sont proposés sur la page des portées pour aider l'utilisateur dans les scénarios où il doit rechercher des flux dont l'un ou les deux points terminaux se situent dans une portée donnée.

Figure 10: Recherche de flux pour une portée



Après avoir sélectionné la portée souhaitée dans l'arborescence (panneau de gauche), comme le montre la figure ci-dessus, l'utilisateur peut choisir entre les trois options suivantes :

1. *Recherche de flux en tant que consommateur* fournit un raccourci vers la page de recherche de flux pour aider à rechercher des flux avec la portée sélectionnée comme portée de *consommateur* pour les flux. En d'autres termes, le point terminal consommateur ou source dans les flux appartient à la portée sélectionnée.

2. *Recherche de flux en tant que fournisseur* fournit un raccourci vers la page de recherche de flux pour aider à rechercher des flux avec la portée sélectionnée comme portée du *fournisseur* pour les flux. Autrement dit, le fournisseur ou le point terminal de destination dans les flux appartient à la portée sélectionnée.
3. *Recherche de flux de trafic interne* fournit un raccourci vers la page de recherche de flux pour aider à rechercher des flux qui sont complètement limités à la portée sélectionnée. En d'autres termes, les deux points terminaux des flux (le client et le fournisseur) appartiennent à la portée sélectionnée.

Création d'une nouvelle portée

Les portées enfants sont créées sur la page d'administration **Scopes** (Portées). Cette action nécessite la capacité `SCOPE_OWNER` (PROPRIÉTAIRE_PORTÉE) sur la portée racine.Les **administrateurs de site** sont propriétaires de toutes les portées.

La création d'une portée enfant aura une incidence sur les membres à l'inventaire de l'application (charges de travail membres) de la portée parente. Par conséquent, la portée parente sera marquée comme ayant des « modifications en cours ». Les modifications devront être validées, et les structures tributaires devront être mises à jour. Reportez-vous à Valider les modifications.

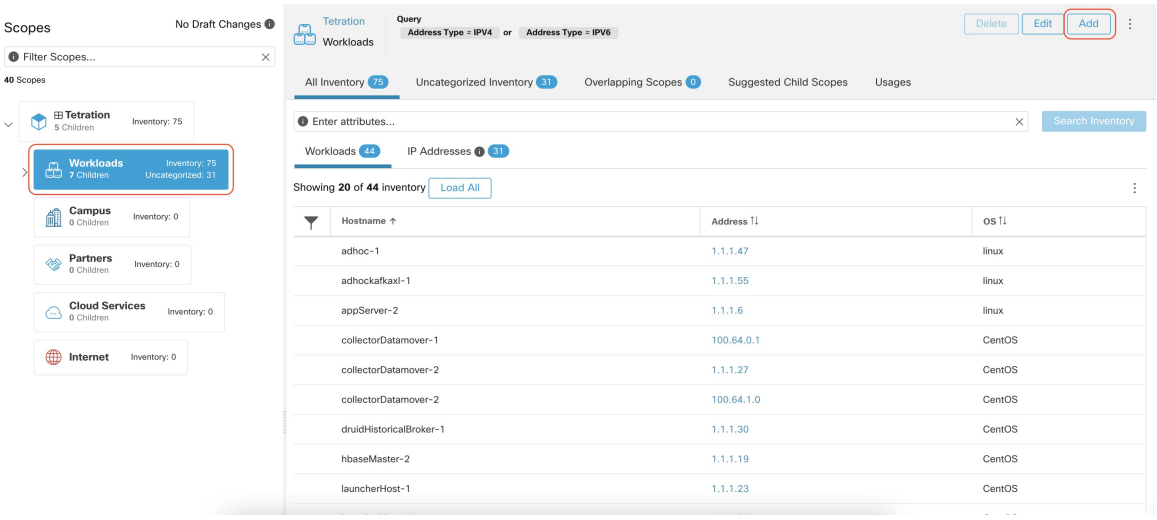
Procedure

Étape 1 Dans la barre de navigation de gauche, cliquez sur **Organize (Organiser)** > **Scopes and Inventory (Portées et inventaire).** La page affiche les portées racine correspondant aux détenteurs + VRF déjà créés sur le système.

Étape 2 Sélectionnez une portée enfant dans le répertoire des portées. Vous pouvez d'abord filtrer les portées si nécessaire.

Étape 3 Cliquez sur le bouton **Add** (ajouter).

Figure 11: Bouton Ajouter une portée

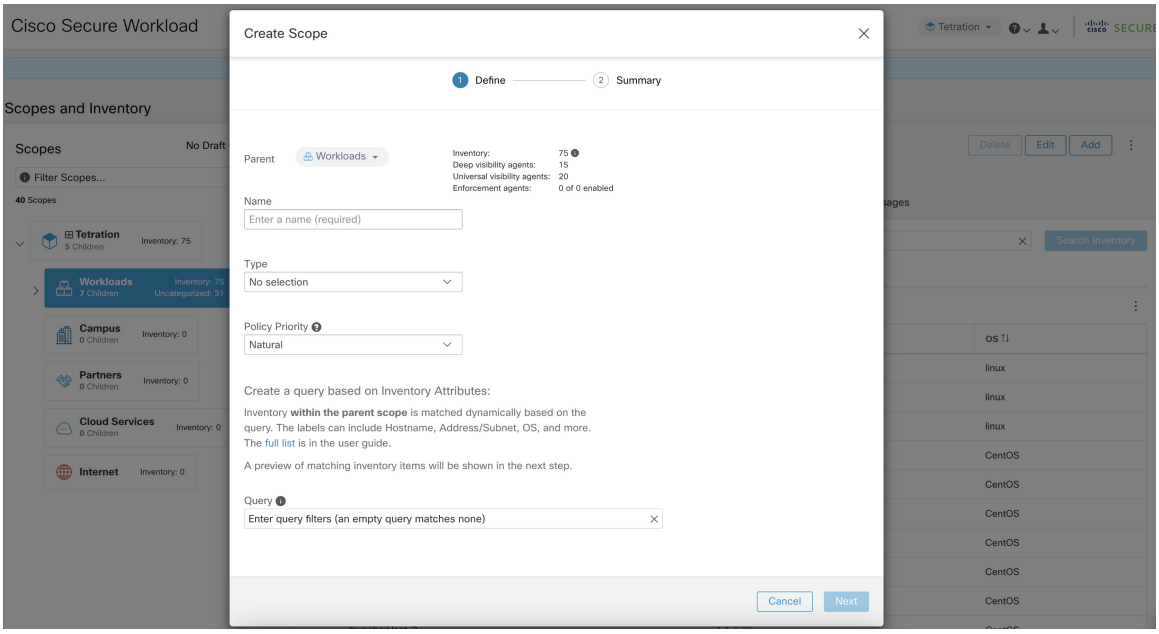


Étape 4 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Parents	Le parent de la nouvelle portée.

Champ	Description
Nom	Le nom pour identifier la portée. Doit être unique dans la portée parente
Type	Sélectionnez une catégorie pour la nouvelle portée.
Requête	La requête/le filtre à mettre en correspondance avec les ressources.

Figure 12: Boîte de dialogue modale de création de portée

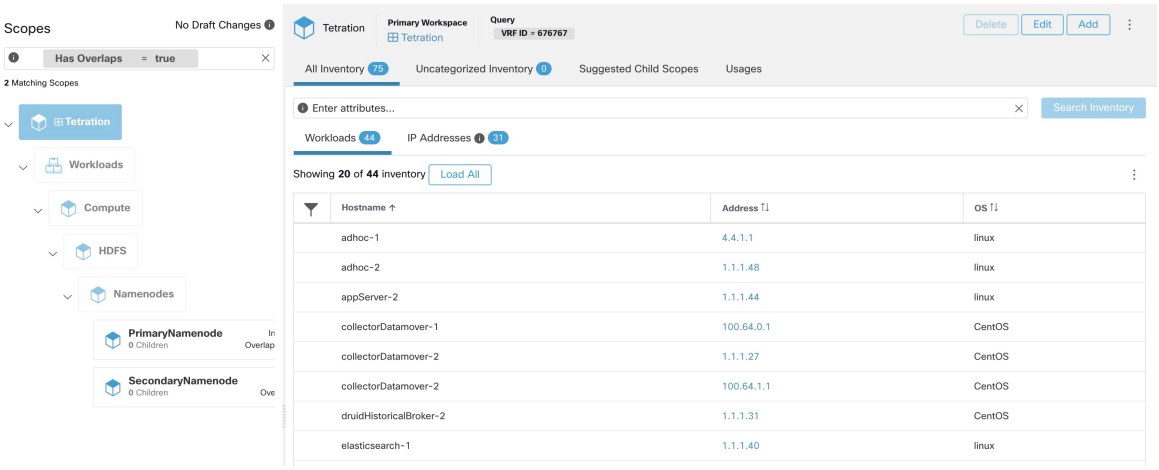


Chevauchement de portée

Lors de l'ajout de portées, il est recommandé d'éviter le chevauchement des portées. Lorsque les portées se chevauchent, les politiques générées pour les portées qui se chevauchent peuvent potentiellement créer de la confusion chez les utilisateurs finaux. Cette fonctionnalité avise l'utilisateur de manière proactive en cas de chevauchement d'appartenances à des portées, c'est-à-dire si le même inventaire appartient à plusieurs portées à la même profondeur dans l'arborescence des portées (portées jumelles). L'objectif est d'éviter que la même charge de travail se trouve dans différentes parties de l'arborescence de la portée.

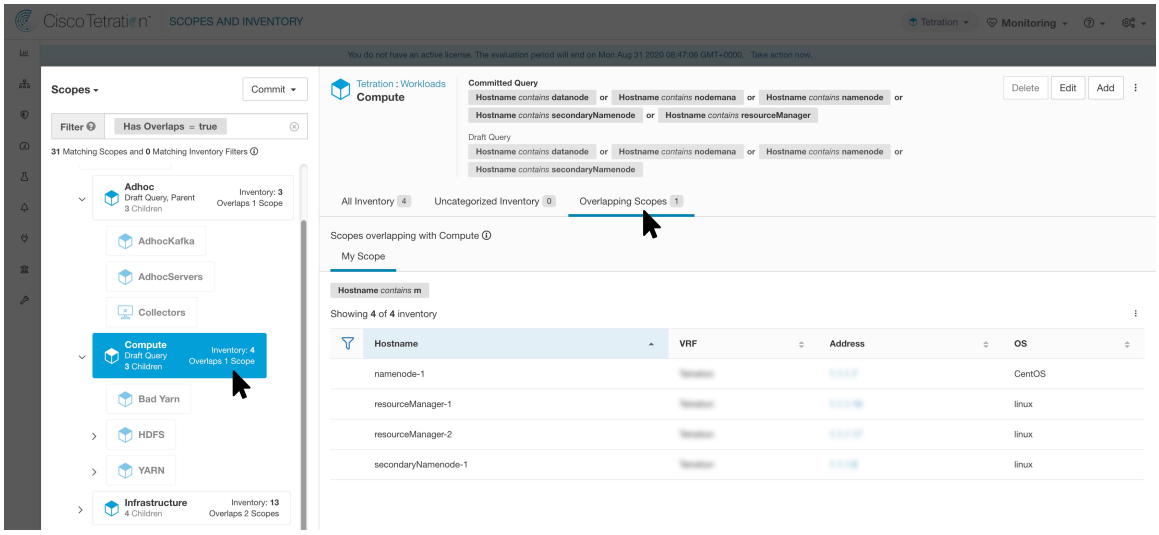
Pour afficher les éléments de l'inventaire appartenant à plusieurs portées, utilisez le filtre de portée et saisissez le critère **Has Overlaps = vrai**.

Figure 13: Critère de chevauchement dans le filtre de portée



La liste des portées qui se chevauchent et des adresses IP qui se chevauchent correspondantes peut être consultée en parcourant l'arborescence de la portée et en sélectionnant l'onglet **Overlapping Scopes** (portées en chevauchement).

Figure 14: Chevauchement des portées et des adresses IP



Modification des portées

Les portées peuvent uniquement être modifiées par les utilisateurs ayant la capacité `SCOPE_OWNER` (Propriétaire de portée) sur la portée racine. Les administrateurs de site sont propriétaires de toutes les portées.

Modification d'un nom de portée

La modification d'un nom de portée se produit immédiatement et peut prendre plusieurs minutes en fonction du nombre de portées enfants à mettre à jour.

Note Les recherches de flux par nom de portée seront affectées lors de la modification du nom de la portée.

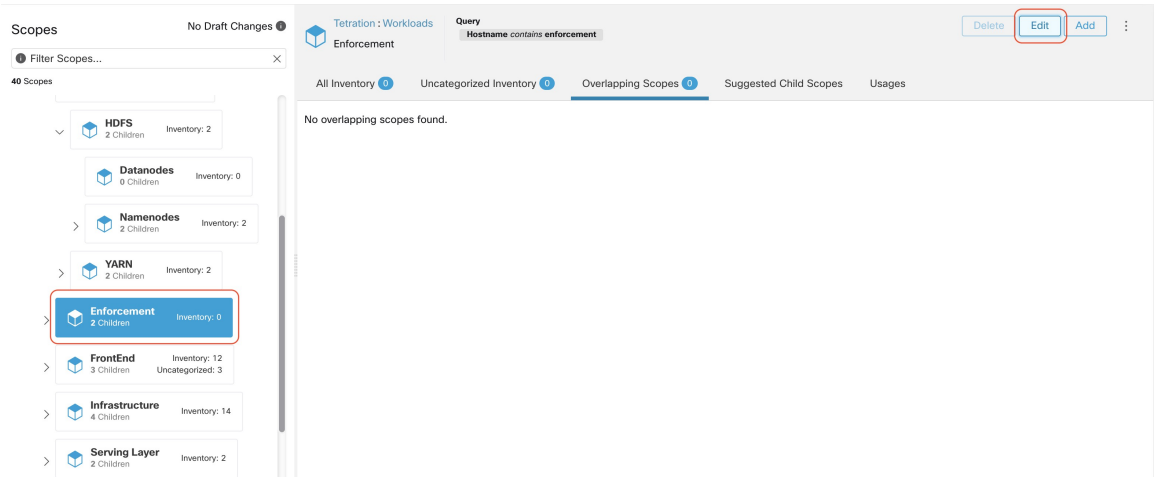
Modification d'une requête de portée

Lorsqu'une requête de portée est modifiée, les portées parentes et enfant directes sont touchées. Ces portées sont marquées comme ayant des « modifications en cours » indiquant que des modifications ont été apportées à l'arborescence qui n'ont pas été validées. Une fois que toutes les mises à jour des requêtes ont été effectuées, l'utilisateur doit cliquer sur le bouton **Commit Changes** (Valider les modifications) au-dessus du répertoire de la portée pour rendre la modification permanente. Cela déclenchera une tâche en arrière-plan pour mettre à jour toutes les requêtes de portée et les « requêtes de grappe dynamique » dans l'espace de travail.

Warning La mise à jour d'une requête de portée peut avoir une incidence sur les membres de l'inventaire des portées (les charges de travail qui sont membres de la portée). Les modifications prendront effet pendant le processus de **validation des modifications**. Pour atténuer les risques, vous pouvez comparer les changements d'affiliation pour une analyse d'impact plus approfondie à partir de la fenêtre Examiner l'incidence des modifications de la portée/du filtre (Examiner la portée/l'impact des changements de filtre).

De nouvelles règles de pare-feu d'hôte seront insérées et toutes les règles existantes seront supprimées sur les hôtes concernés.

Figure 15: Modifier une portée



Pour modifier une portée :

Procedure

Étape 1 Cliquez sur le **bouton Edit**) (Modifier) de la portée à modifier.

Étape 2 Modifiez le nom ou la requête pour la portée sélectionnée.

Étape 3 Comparez les modifications entre l'ancienne et la nouvelle requête provisoire en cliquant sur le lien **Review query change impact** (Examiner l'impact des modifications de la requête).

Étape 4 Cliquez sur **Save** (enregistrer). Le nom est mis à jour immédiatement.

Étape 5 Pour mettre à jour la requête de toutes les portées, cliquez sur le bouton **Commit Changes** (Valider les modifications).

Étape 6 Vous obtiendrez une confirmation contextuelle qui indiquera les conséquences de la modification de la portée. La mise à jour est traitée de manière asynchrone dans une tâche en arrière-plan.

Étape 7 Cliquez sur **Save** (enregistrer). Selon le nombre de modifications, l'opération peut prendre une minute ou plus.

Figure 16: Examiner l'incidence de la modification de la requête

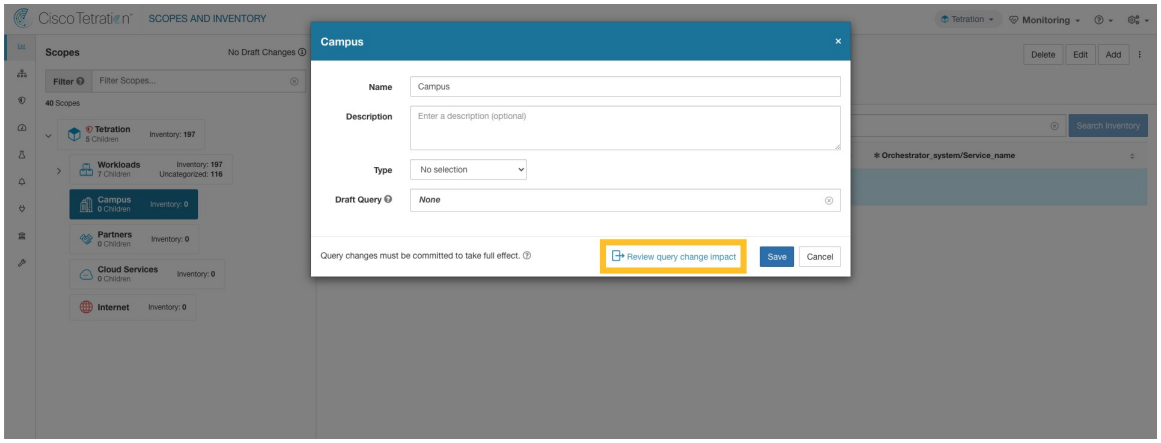
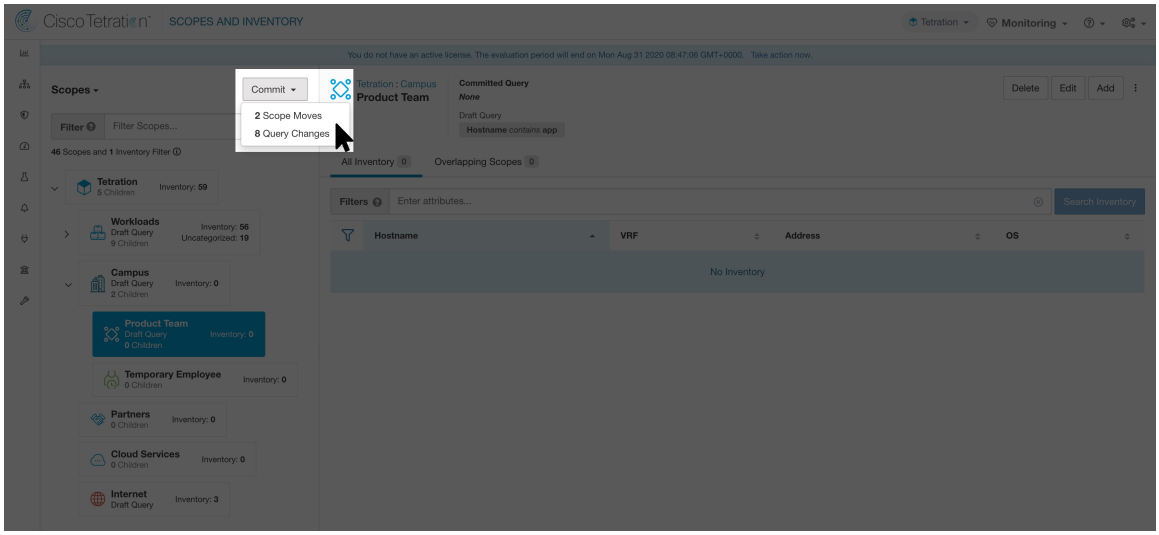


Figure 17: Valider les modifications



Modification du parent d'une portée

Lorsque le parent d'une portée est mis à jour, la requête de portée change. Cette modification affecte les membres des portées parent et enfant. Tout comme la modification de la requête de portée, ces modifications sont initialement enregistrées en tant que « brouillons de modifications » et n'entreront en vigueur que si elles sont validées. L'utilisateur peut valider l'incidence de cette modification avant de s'engager en cliquant sur « Revoir la requête de modification de l'impact » dans la boîte de dialogue modale Edit Scope (modifier la

portée). Une fois validées, les modifications peuvent être validées en cliquant sur « Commit » (Valider) et en acceptant les « déplacements de la portée » et les « modifications de requêtes ».

Pour modifier le parent d'une portée :

Procedure

Étape 1 Cliquez sur le **bouton Edit**) (Modifier) de la portée à modifier.

Étape 2 Modifiez le parent de la portée sélectionnée.

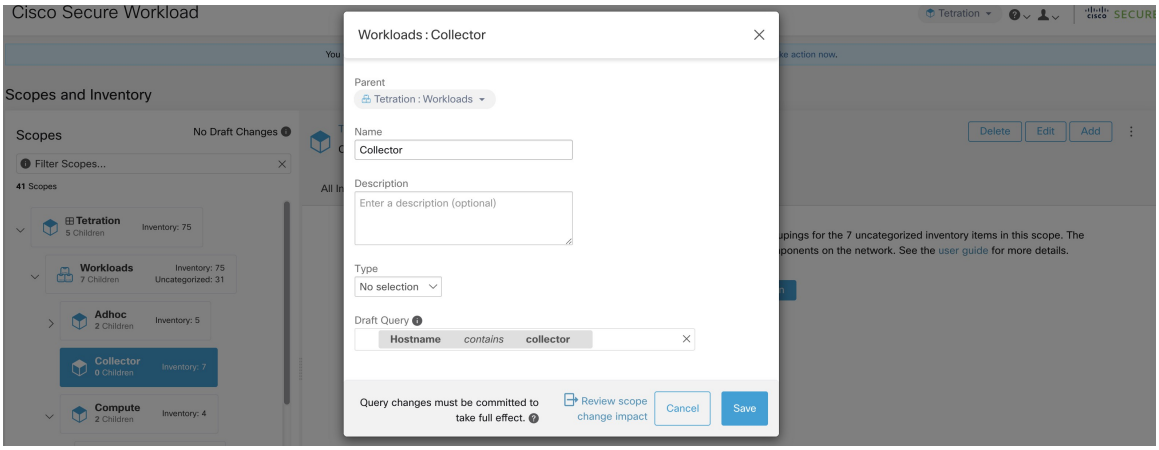
Étape 3 Comparez les modifications entre l'ancienne et la nouvelle version provisoire de la requête en cliquant sur le lien **Examiner l'incidence des modifications de la requête**.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Cliquez sur « Commit » (valider) et acceptez les « déplacements de portée » et les « modifications de requête ». La mise à jour est traitée de manière asynchrone dans une tâche en arrière-plan.

Étape 6 Cela peut prendre une minute ou plus selon le nombre de charges de travail concernées par cette modification.

Figure 18: Modification de la portée parente de la portée par défaut à Default:ProdHosts



Suppression des portées

Les portées peuvent uniquement être supprimées par les utilisateurs avec la capacité `SCOPE_OWNER` sur la portée racine. Les administrateurs de site sont propriétaires de toutes les portées.

La suppression d'une portée aura une incidence sur les membres de l'inventaire des applications de la portée parente (les charges de travail qui sont membres de la portée parente). . Par conséquent, la portée parente sera marquée comme ayant des « modifications en cours ». Les modifications devront être validées, et les structures tributaires devront être mises à jour. Reportez-vous à Valider les modifications.

Les portées avec des objets dépendants ne peuvent pas être supprimées. Une erreur est renvoyée si :

- Un espace de travail est défini pour la portée.
- Un filtre d'inventaire est affecté à la portée.
- Il existe une politique qui utilise la portée pour définir ses consommateurs ou ses fournisseurs.

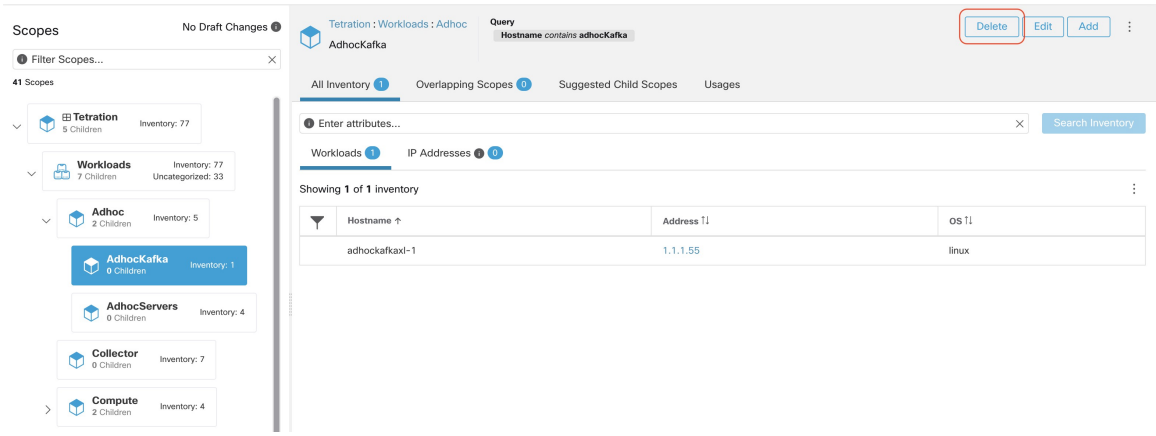
- Un intent (action associée des données) de configuration d'agent est défini sur la portée
- Un intent de configuration d'interface est définie sur la portée.
- Un intent de configuration de criminalistique est définie sur la portée.

Pour approfondir davantage les dépendances de la portée, vous pouvez consulter l'onglet **Dependencies** 'Dépendances) dans la fenêtre Examiner l'incidence des modifications de la portée/du filtre (Examiner la portée/l'impact des modifications de filtre).

Ces objets doivent être supprimés avant que la portée ne puisse être supprimée.

1. Dans le menu de navigation de gauche, choisissez **Organize (Organiser)** > **Scopes and Inventory (Portée et inventaire)**.
2. Sélectionnez une « portée », puis cliquez à nouveau pour afficher les portées enfants. Sélectionnez la portée enfant que vous souhaitez supprimer.
3. Cliquez sur le bouton **Delete** (Supprimer) à côté des boutons de modification et d'ajout.

Figure 19: Supprimer une portée



Note Seules les portées sans enfant peuvent être supprimées

Note Les portées racine doivent être supprimées en retirant le VRF (Virtual Routing and Forwarding, Instance virtuelle de routage et de transmission) de la page Tenants (Détenteurs).

Réinitialiser l'arborescence des portées

Si l'une des configurations ci-dessus existe, vous devez la supprimer avant de pouvoir réinitialiser l'arborescence de la portée. Tant que vous ne le faites pas, le bouton Reset (réinitialiser) n'est pas disponible.

Pour réinitialiser l'arborescence de la portée :

Avant de commencer

Vous pouvez supprimer l'ensemble de l'arborescence de la portée et recommencer.

La réinitialisation de l'arborescence des portées supprime toutes les portées, les étiquettes, les espaces de travail et les règles de collecte. Elle ne supprime pas les données intégrées/acquises (ingested).

Seul un utilisateur avec la capacité `SCOPE_OWNER` sur la portée racine peut réinitialiser l'arborescence de la portée.

Cependant, vous ne pouvez pas réinitialiser l'arborescence des portées si l'une des conditions suivantes est définie pour une portée de l'arborescence :

- Espaces de travail (à l'exception de l'espace de travail unique créé si vous avez créé l'arborescence de la portée à l'aide de l'assistant)
- Filtres d'inventaire
- Politiques
- Intents de configuration de l'agent
- Intents de configuration d'interface
- Intents de configuration criminalistique

Procédure

Étape 1 Dans le menu de navigation de gauche, choisissez **Organize (Organiser)** > **Scopes and Inventory (Portée et inventaire).**

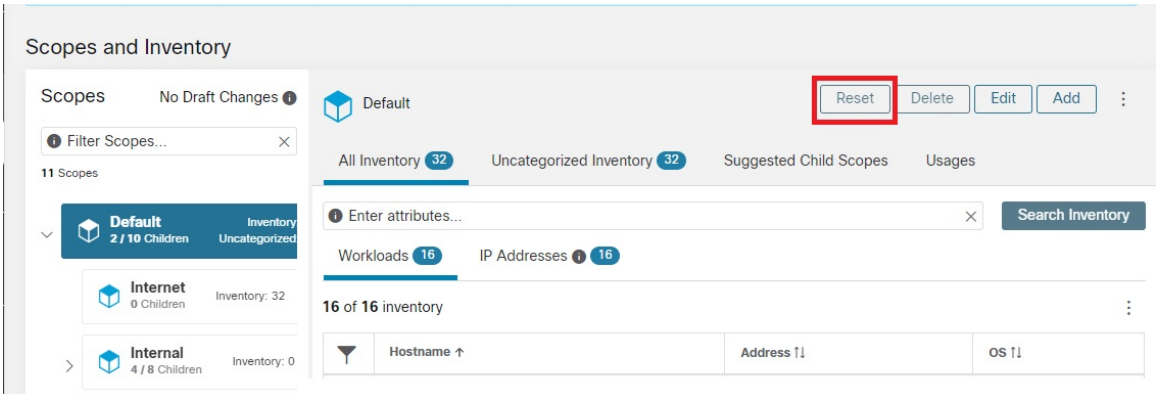
Étape 2 Cliquez sur la portée au sommet de l'arborescence.

Étape 3 Cliquez sur **Reset** (Réinitialiser).

Étape 4 Confirmez votre choix.

Étape 5 Si nécessaire, actualisez la page du navigateur pour continuer.

Illustration 20 : Réinitialiser l'arborescence de la portée



Valider les modifications

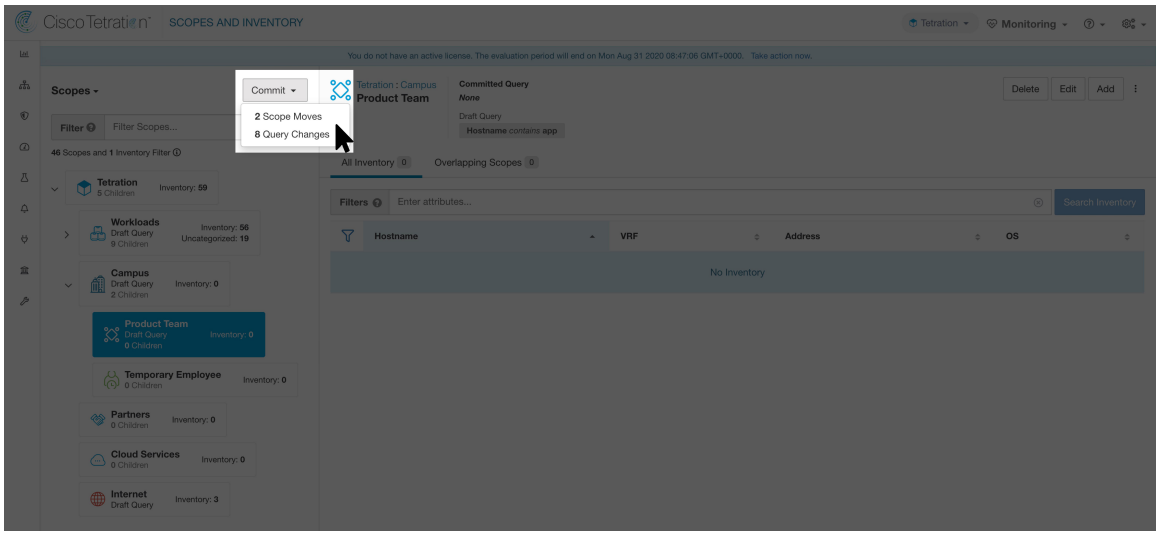
La définition de requête d'inventaire des applications d'une portée est définie par sa requête et celles de ses portées enfants directes. Lorsque cela se produit, la portée est marquée comme ayant des « modifications au stade du brouillon et non validées » et la requête, les espaces de travail et les grappes de la portée ne seront pas modifiés tant que la tâche en arrière-plan de**Commit Changes** (Valider les modifications) ne sera pas exécutée. Lorsqu'une portée est à l'état de brouillon, le symbole triangulaire d'avertissement est affiché à côté des icônes des portées concernées, et le bouton « Commit Changes » (valider les modifications) est affiché sur la page des portées (en haut à droite) et doit être pressé pour exécuter la tâche en arrière-plan **Valider les modifications**.

Événements qui peuvent marquer une portée comme au stade du brouillon :

- Mise à jour de la requête
- La requête de toute portée parent est mise à jour.
- Une portée enfant directe est ajoutée.
- Un enfant direct est supprimé.
- La requête directe de la portée enfant est mise à jour.

La modification du nom d'une portée ne modifie pas l'état de brouillon de la portée.

Figure 21: Valider les modifications



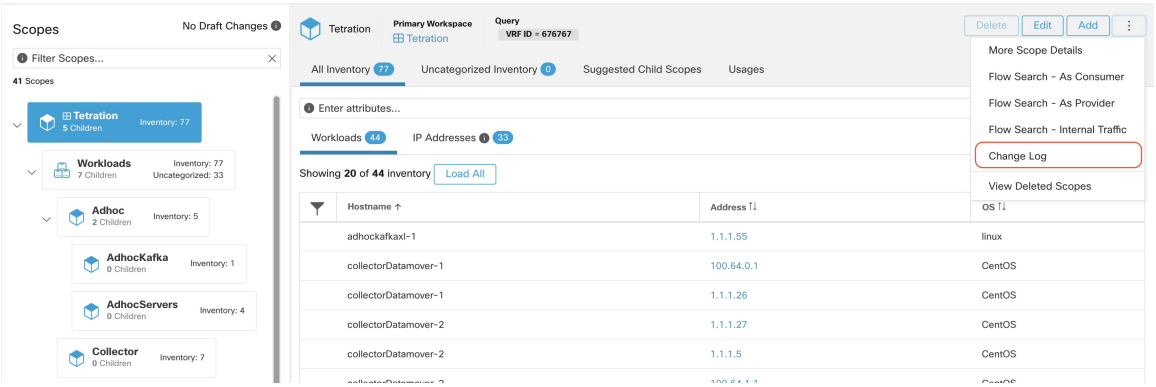
Note La tâche **Valider les modifications** est asynchrone. Elle prend généralement plusieurs secondes, mais les arborescences de portées volumineuses peuvent prendre plusieurs minutes.

Note La tâche de mise à jour de la portée sera terminée lorsque la portée racine ne sera plus à l'état de brouillon. Actualisez la page pour obtenir le dernier état.

Journal des modifications

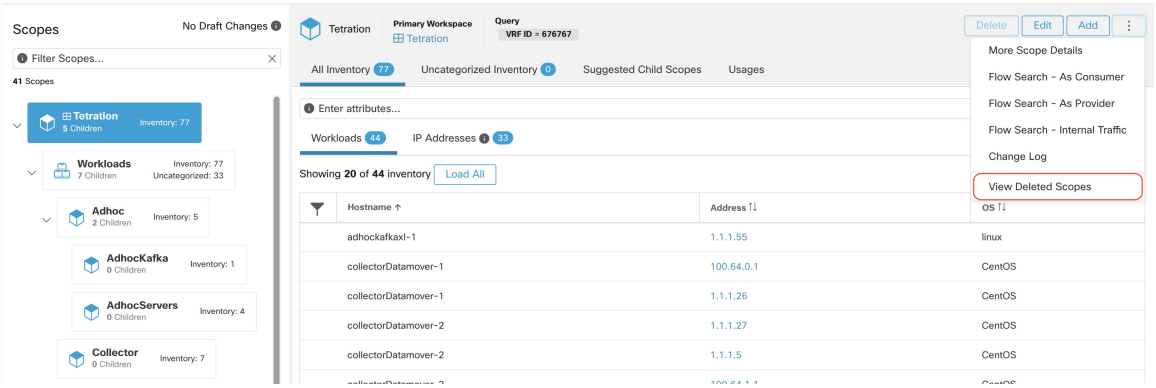
Les **administrateurs du site** et les utilisateurs avec la capacité `SCOPE_OWNER` sur la portée racine peuvent afficher les journaux des modifications pour chaque portée en cliquant sur change log (journal des modifications) dans le menu à développer en haut à droite.

Figure 22: Journal des modifications



Ces utilisateurs peuvent également afficher une liste des portées supprimées en cliquant sur le lien **View Deleted Scopes** (Afficher les portées supprimées) dans le menu à développer dans le coin supérieur droit.

Figure 23: Afficher les portées supprimées



Création d'un nouveau détenteur

Les portées au niveau racine sont mappées aux VRF qui sont créés sous les détenteurs ou par le biais de la page d'administration des **portées**. Cette action est uniquement disponible pour les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle**.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **Tenants (Détenteurs).**

Étape 2 Cliquez sur le bouton **Create New Tenant** (Créer un nouveau détenteur).

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Le nom pour identifier la portée. Doit être unique dans la portée parente
Description	Description facultative

Étape 4 Cliquez sur le bouton **Create** (créer).

Figure 24: Créer un détenteur

Inventaire

Pour utiliser l'inventaire, cliquez sur **Organize (Organiser)** > **Scopes and Inventory** (Portée et inventaire) dans la barre de navigation de gauche.

Recherche dans l'inventaire

Tout l'inventaire détecté sur le réseau peut faire l'objet d'une recherche. Pour rechercher dans l'inventaire, utilisez le bouton **Search Inventory** (rechercher dans l'inventaire). Chaque article de l'inventaire est identifiable de manière unique par son adresse IP et son Instance virtuelle de routage et de transmission (VRF) et peut être utilisé pour effectuer une recherche. Il n'est pas possible de rechercher un élément d'inventaire de service à l'aide de son adresse IP. Utilisez l'une des étiquettes d'utilisateur associées au service, par exemple user_orchestrator_system/service_name, pour rechercher un inventaire de service. Une fois qu'un hôte a été trouvé, vous pouvez afficher des informations détaillées le concernant sur la page de profil d'hôte.

Éléments constitutifs de l'inventaire

1. Portée racine
   - Racine de la hiérarchie de la portée sous un détenteur donné
   - Fournit une séparation logique pour les domaines d'adresse L3
2. Champ d'application
   - Conteneur d'inventaire défini par une requête dynamique
   - Foundation pour le modèle de politique hiérarchique
   - Point d'ancrage pour la configuration des politiques, RBAC et des filtres

3. Filtre
    - Conception flexible basée sur une requête d'inventaire dynamique
    - Point d'ancrage pour la définition des intents, des services fournis et la définition de la politique

Note Comprend toutes les adresses IP des partenaires et tout ce qui communique dans votre environnement. Qu'ils soient accompagnés d'un agent ou non, vous devez définir ce qu'ils sont au moyen d'une étiquette.

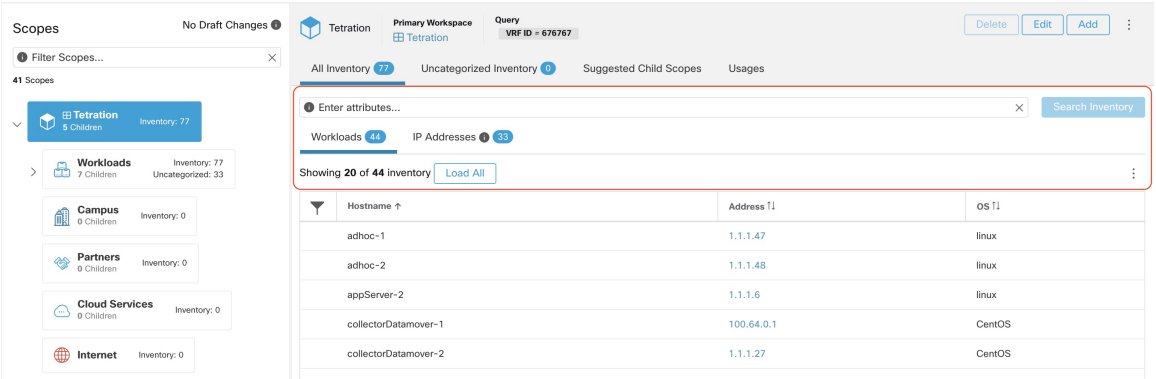
Facteurs à prendre en considération pour la planification des étiquettes

1. Source des données
    - Réseaux – IPAM? Tables de routage Feuilles de calcul?
    - Hôtes : CMDB, hyperviseur, nuage, propriétaires d'applications?
2. Exactitude des données
3. le niveau de dynamique des données et la façon dont elles seront mises à jour.
    - Chargement manuel?
    - Intégration d'API?
4. Commencez par les éléments de base et poursuivez la progression
    - Utilisez des étiquettes de réseau pour créer une structure de portée générale.
    - Utilisez des étiquettes d'hôte pour créer une structure de portée plus détaillée au niveau de l'application.

Rechercher dans l'inventaire

La recherche dans l'inventaire permet d'afficher des informations sur des éléments d'inventaire spécifiques.

Figure 25: Recherche dans l'inventaire



Procedure

Étape 1 Dans le volet de navigation, sélectionnez **Organize** > **Scopes and Inventory** (Organiser > Portées et inventaire).

Étape 2 Dans le champ **Filters** (Filtres), saisissez les attributs pour les éléments d'inventaire que vous recherchez. Les attributs sont les suivants :

Attributs	Description
Hostname (Nom d'hôte)	Saisissez un nom d'hôte complet ou partiel.
Nom VRF	Saisissez un nom de VRF
ID VRF	Saisissez un ID VRF (numérique).
Address (adresse)	Saisissez une adresse IP ou un sous-réseau valide (IPv4 ou IPv6).
Address Type (Type d'adresse)	Sélectionnez IPv4 ou IPv6.
SE	Saisissez un nom de système d'exploitation (p. ex., CentOS).
Version du système d'exploitation	Saisissez une version du système d'exploitation (p. ex., 6.5).
Interface Name (Nom d'interface)	Saisissez un nom d'interface (p. ex., eth0).
MAC	Saisissez l'adresse MAC.
Dans les règles de collecte?	Saisissez vrai ou faux.
Ligne de commande de processus	Saisissez la sous-chaîne d'une commande qui s'exécute sur l'hôte (Remarque : cet aspect ne peut pas être enregistré dans le cadre du filtre d'inventaire).
Traiter le condensé binaire	Saisissez le condensé de processus d'une commande qui s'exécute sur l'hôte (Remarque : cet aspect ne peut pas être enregistré dans le cadre du filtre d'inventaire).
Renseignements sur le paquet	Saisissez le nom du paquet, suivi facultativement d'une version du paquet (préfixée par #).
Paquet CVE	Saisissez une partie ou un ID CVE complet.
Note CVE v2	Saisissez une note CVSSv2 (Common Vulnerability Scoring System) (numérique
Note CVE v3	Saisissez une note CVSSv3 (Common Vulnerability Scoring System) (numérique).
Étiquettes d'utilisateur	Les attributs préfixés proviennent d'étiquettes d'utilisateur.

Étape 3 Cliquez sur **Search Inventory** (Rechercher dans l'inventaire). Les résultats sont affichés sous le champ **Filters** (filtres) regroupés dans quatre onglets. Chaque onglet comporte un tableau avec les colonnes pertinentes. Des colonnes supplémentaires peuvent être affichées en cliquant sur l'icône d'entonnoir dans l'en-tête du tableau. Si des étiquettes d'utilisateur sont disponibles, elles seront préfixées et peuvent être activées ici.

Figure 26: Résultats de la recherche d'inventaire

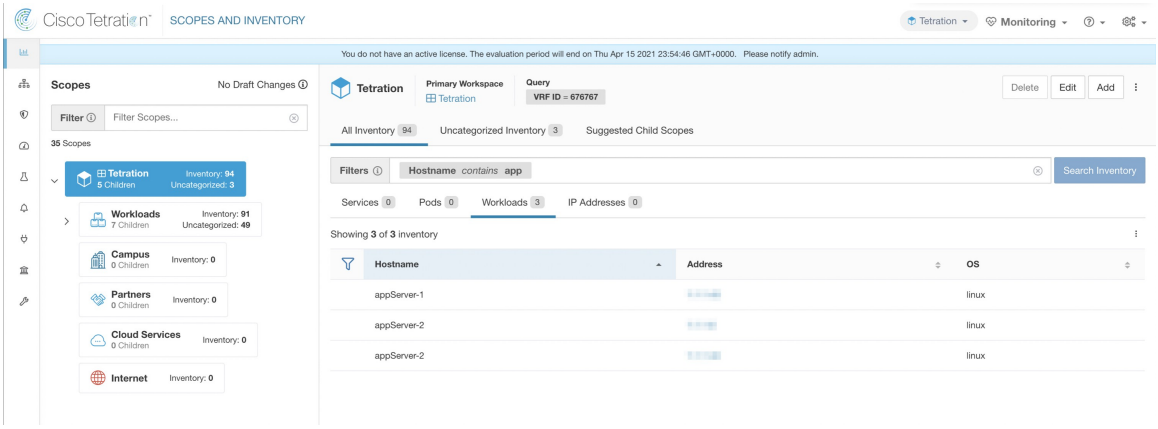
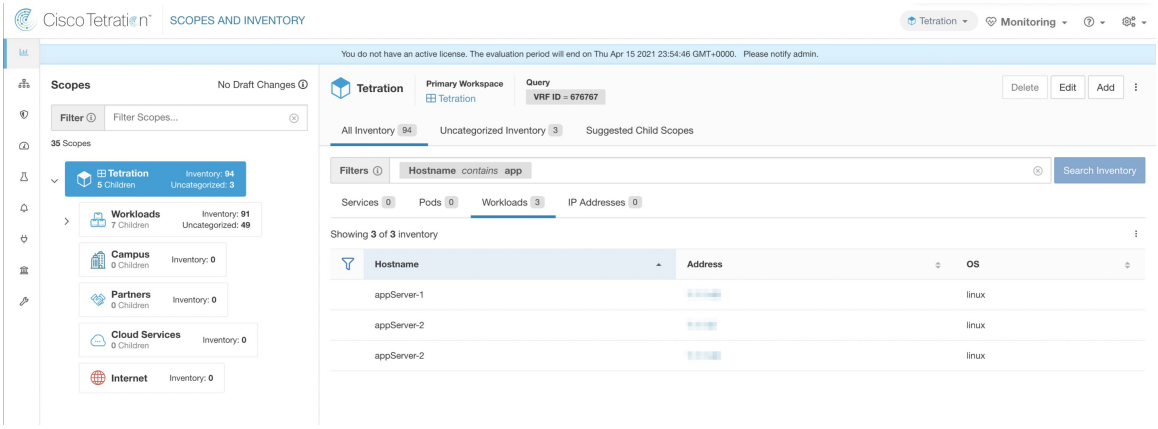


Figure 27: Résultats de la recherche d'inventaire



Les résultats de la recherche sont regroupés dans quatre onglets :

Onglet	Description
Services	Répertorie les services Kubernetes et les équilibreurs de charge détectés par les orchestrateurs externes. Cet onglet est masqué, sauf si un orchestrateur externe connexe est configuré.
Modules	Répertorie les pods Kubernetes. Cet onglet est masqué, sauf si un orchestrateur externe connexe est configuré.
Charges de travail	Répertorie les articles d'inventaire signalés par les agents Cisco Secure Workload.

Onglet	Description
Adresses IP	Répertorie les éléments de l'inventaire découverts par : • Téléversement de l'inventaire • Apprentissage des flux • Étiquettes téléversées manuellement • Étiquettes intégrées par les connecteurs et des orchestrateurs externes De plus, les listes de sous-réseaux signalés provenant des mêmes sources.

Note Par défaut, l'interception de tous les sous-réseaux pour les adresses IPv4 et IPv6 s'affiche dans chaque client hébergé.

Il y a également une mention du nombre d'inventaires à côté de chaque onglet. Les informations immédiatement disponibles lors d'hune recherche comprennent le nom d'hôte, les adresses IP avec les sous-réseaux, le système d'exploitation, la version du système d'exploitation, le nom du service et le nom du pod. La liste des colonnes affichées peut être modifiée en cliquant sur l'icône d'entonnoir dans l'en-tête du tableau. Les résultats de la recherche sont limités à la portée actuellement sélectionnée dans le répertoire des portées. Vous trouverez plus d'informations sur la page de profil respective en cliquant sur un élément dans les résultats de recherche.

Plus de détails sur chaque hôte sont affichés dans le **Profil de charge de travail**, accessible en cliquant dans le champ d'adresse IP d'une rangée de résultats de recherche. Consultez le Profil de la charge de travail pour en savoir plus.

Pour créer des filtres d'inventaire à l'aide de la barre latérale : Choisissez **Organize (Organiser)** > **Inventory filters (Filtres d'inventaire)** dans le menu supérieur. Cliquez sur le bouton **Create Filter** (créer un filtre). Une boîte de dialogue modale apparaît dans laquelle vous pouvez nommer votre filtre enregistré.

Suggérer des portées enfants

Suggest Child Scopes (Suggérer des portées enfants) est un outil qui utilise des algorithmes d'apprentissage automatique (comme la détection de communauté dans les réseaux) pour découvrir des groupes qui pourraient servir de portées . Cet outil est utile lors de la création d'une hiérarchie de portées et facilite le processus de définition de portées enfants plus granulaires pour une portée donnée. Les portées enfants candidates sont affichées sous forme de suggestions, qui peuvent ensuite être sélectionnés et ajoutés.

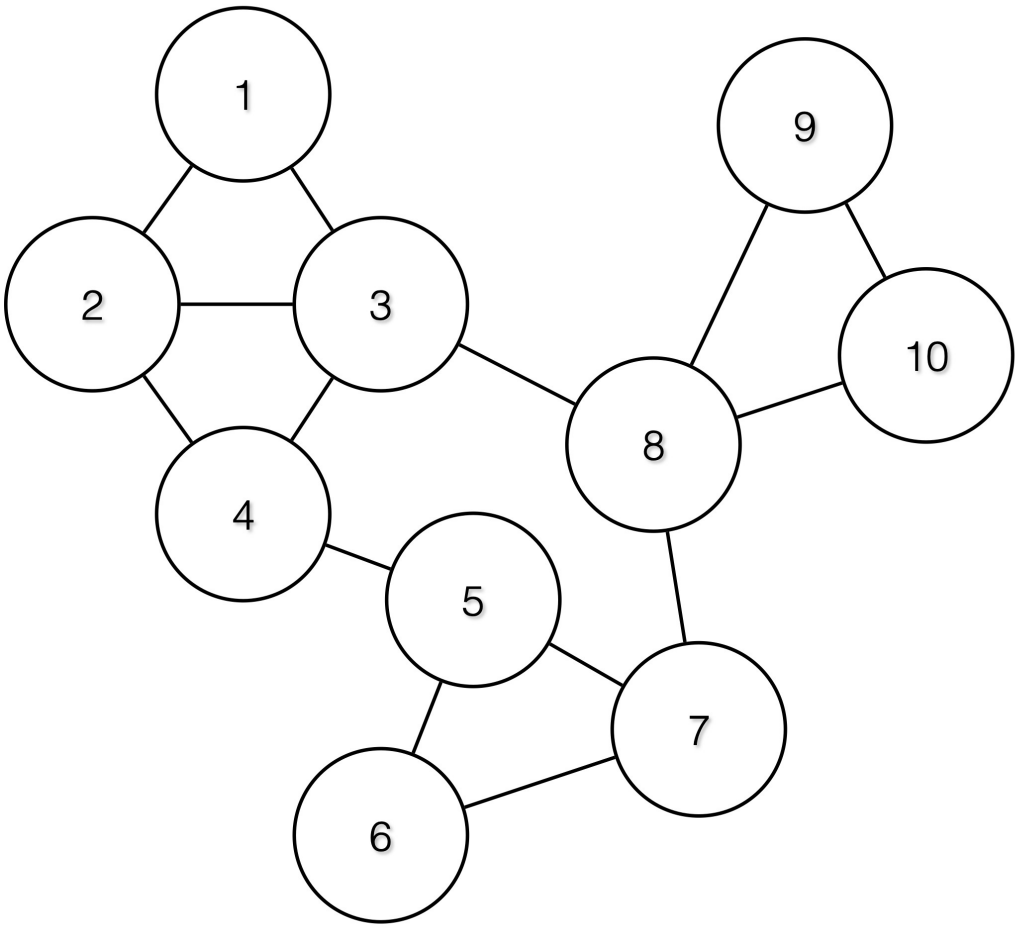
Description des algorithmes : Un graphe basé sur les communications entre les membres non réclamés de la portée parentale est d'abord créé (note : les membres non réclamés sont ceux qui n'appartiennent à aucune portée enfant de la portée parentale), et le graphe est prétraité, par exemple les algorithmes tentent d'identifier les points terminaux qui communiquent avec une proportion suffisamment élevée d'autres points terminaux dans le graphe. Un tel groupe de points terminaux, le cas échéant, est affiché pour l'utilisateur en tant que groupe candidat **de services communs**. Le reste du graphique est traité pour détecter les groupes qui se comportent comme **des communautés**, ce qui signifie en gros que les points terminaux communiquent entre eux de manière disproportionnée, plus souvent (ou sur plus de ports de fournisseur) qu'avec des points terminaux à l'extérieur du groupe. Chacun de ces regroupements peut correspondre à une application ou à un

service de l'l'entreprise. Un tel découpage peut également conduire à des politiques plus éparses entre les portées.

Exemple :

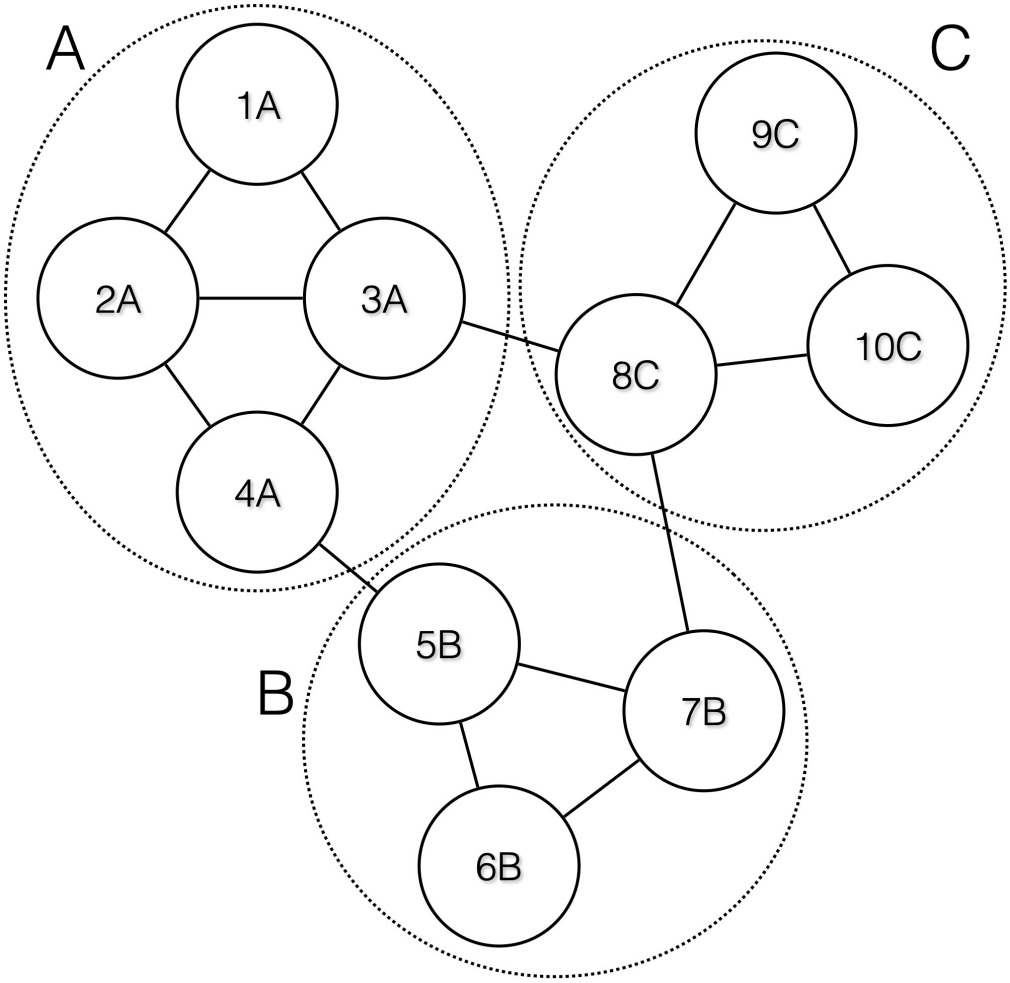
Les chiffres 1 à 10 représentent les adresses IP individuelles des points terminaux. Supposons que le graphique d'entrée (des communications) soit le suivant :

Figure 28: Graphique d'entrée



Ainsi, les points terminaux 1 à 4, 5 à 7 et 8 à 10 seront regroupés, car ils ont un degré de communication relativement élevé (nombre de périphéries) entre eux et de relativement faibles communications avec d'autres points terminaux.

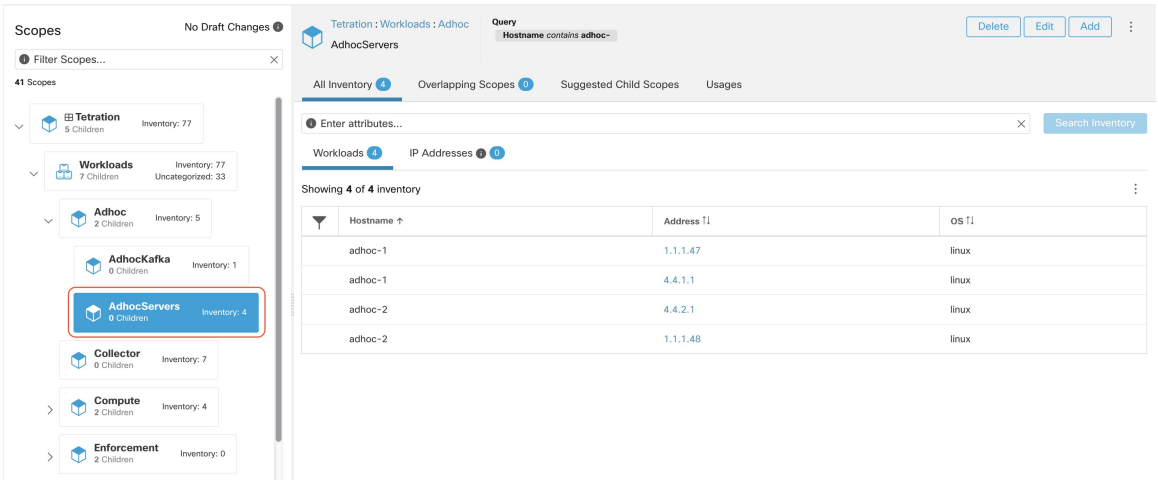
Figure 29: Groupes de sortie



Étapes de la proposition de portées

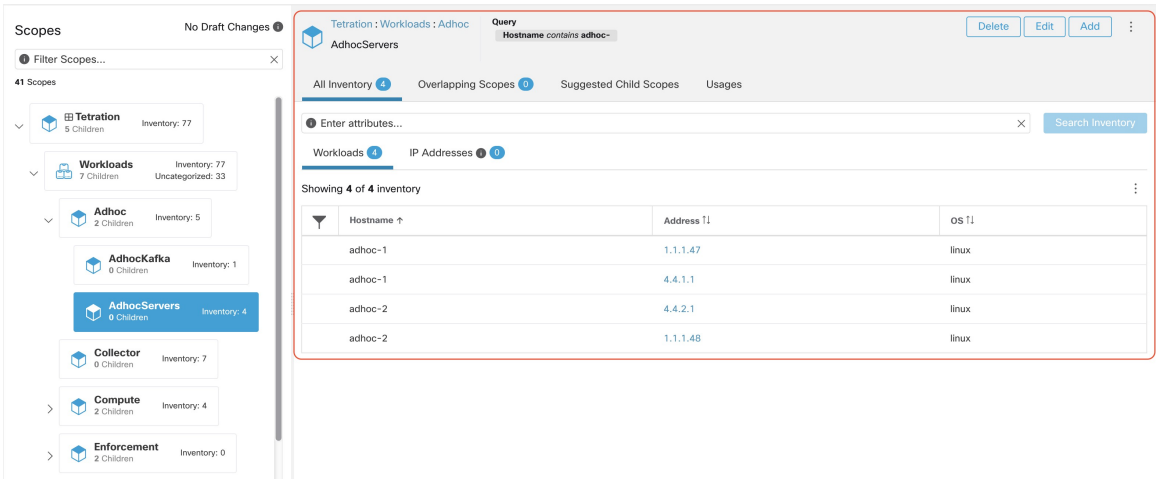
Pour invoquer la suggestion de portée pour une portée souhaitée, l'utilisateur doit se rendre sur la page des portées et la sélectionner.

Figure 30: Sélectionner une portée



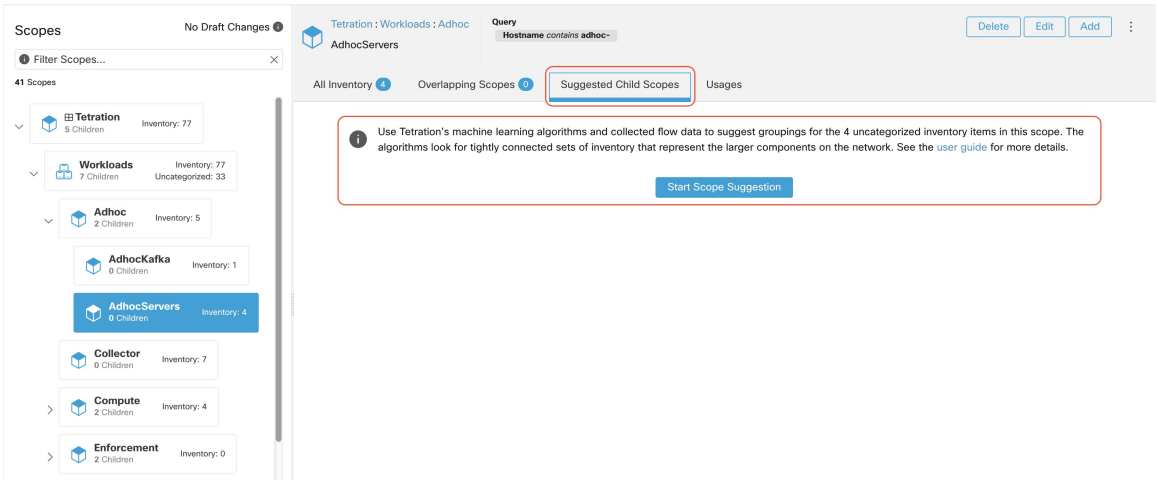
Dans la fenêtre, l'utilisateur peut parcourir l'inventaire, les *articles stockés non classés*, c'est-à-dire les articles qui appartiennent à la portée actuellement sélectionnée et qui n'appartiennent à aucune des portées enfants de la portée actuellement sélectionnée. Cliquer sur les **uncategorized inventory items (articles d'inventaire non classés)** pour afficher cette liste.

Figure 31: Fenêtre de portée



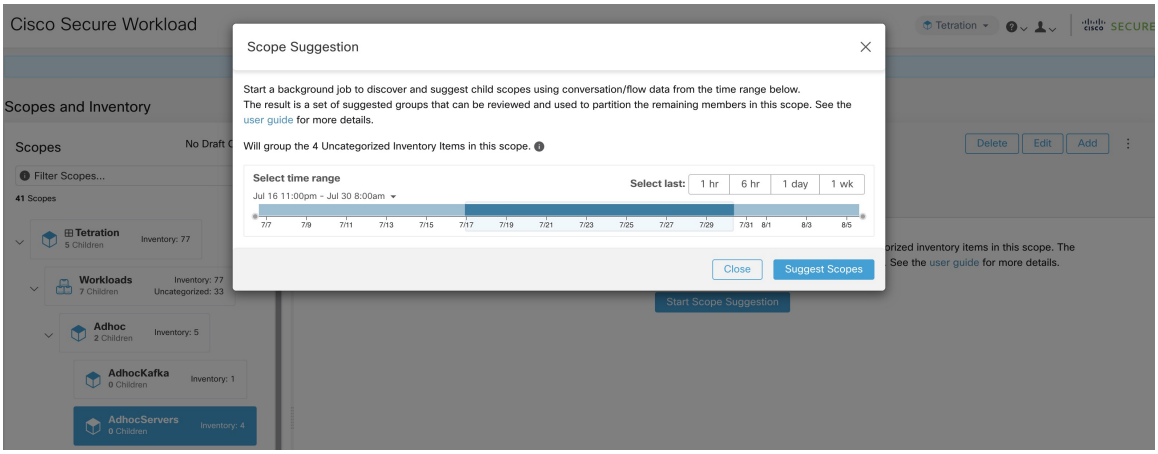
Après avoir sélectionné la portée, l'utilisateur peut cliquer sur **Suggest Children Scope** (Suggestions de portées enfants), puis sur **Start Scope Suggestion** (Démarrer la suggestion de portée) (ou cliquer sur Rerun, (Réexécution) si ce n'est pas la première fois). Notez que l'entrée d'un cycle de suggestion de portée sera les articles en inventaire non catégorisés.

Figure 32: Portées enfants



L'utilisateur peut définir la plage de dates comme entrée pour la suggestion de portée et cliquer sur **Suggest Scopes** (Suggérer des portées). L'exécution d'une suggestion de portée est souvent rapide lorsque la charge globale est moyenne, et ne prend que quelques minutes pour traiter des dizaines de milliers de points terminaux, comportant des dizaines de milliers de conversations.

Figure 33: Sélecteur de plages de données de suggestions de portée

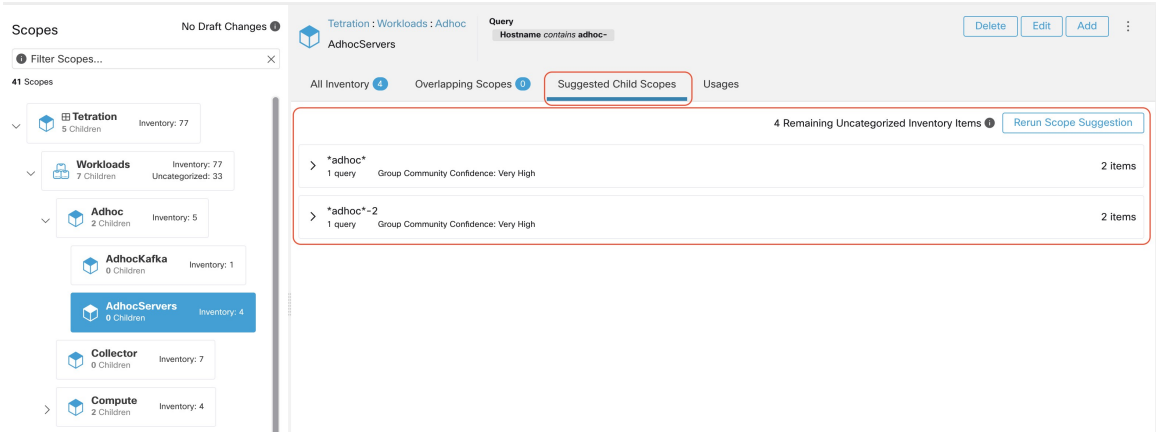


Le résultat est présenté à l'utilisateur sous la forme d'une liste de candidats, actuellement jusqu'à 20 groupes (illustrés), chacun accompagné d'informations telles que la confiance dans le groupe (qualité), le nom de la portée du candidat et les requêtes. Chaque groupe découvert est associé à un **niveau de confiance de la communauté de groupe**. Les valeurs possibles sont les suivantes : **très élevée**, **élevée**, **moyenne** et **faible**. Il s'agit d'une mesure de la propriété **communauté** du groupe : plus la confiance est élevée, plus la propriété communautaire du groupe donné de points terminaux est élevée (beaucoup de périphéries à l'intérieur du groupe, relativement peu de périphéries vers l'extérieur). Actuellement, le sous-ensemble de groupes à afficher sont sélectionnés en fonction de la confiance de la communauté du groupe. Les groupes découverts peuvent actuellement appartenir à l'un de ces quatre types de groupes :

- **Groupe générique** : tout groupe découvert par apprentissage automatique en fonction de la propriété de la communauté. Notez que tout groupe qui n'est pas explicitement désigné avec les types spéciaux ci-dessous est un groupe générique.

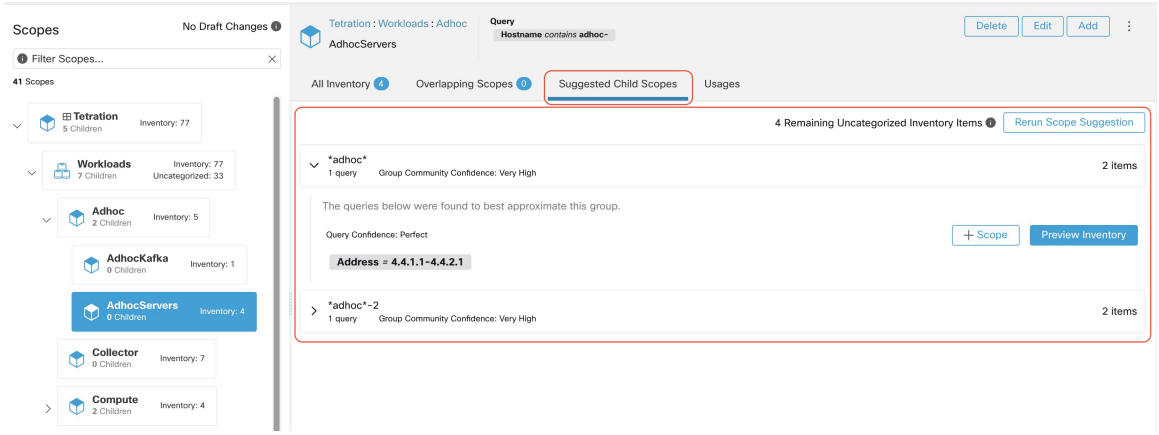
- **Services communs** : ce groupe se compose de terminaux qui communiquent avec une grande partie de l'inventaire d'entrée. Ces points terminaux exécutent peut-être des services partagés.
- **Clients des services communs** : ce groupe se compose de points terminaux qui communiquent uniquement avec le groupe **de services communs**.
- **Non groupé** : ce groupe se compose de points terminaux qui ne peuvent pas être regroupés, car leurs communications ne sont pas suffisantes.

Figure 34: Sortie des suggestions de portée



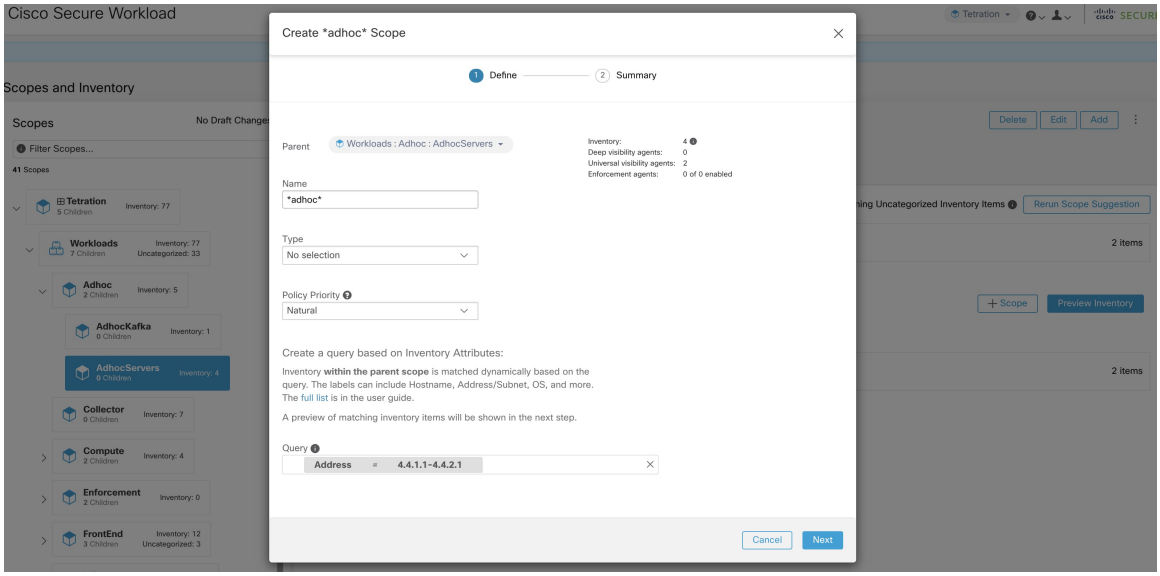
L'utilisateur peut cliquer sur un groupe découvert pour afficher la liste des requêtes générées pour le groupe sélectionné. L'utilisateur peut avoir un aperçu de l'inventaire couvert par la requête, qui définira avec précision le groupe découvert. Les requêtes consistent en des plages d'adresses IP, des sous-réseaux, des noms d'hôte et des étiquettes téléversées par l'utilisateur. Une mesure de confiance est associée à chaque groupe appelé **Query confidence** (confiance de la requête) qui peut avoir l'une des plages de valeurs suivantes : **Idéale**, **très élevée**, **élevée**, **moyenne** et **faible**. Pour la génération de requêtes, les groupes sont d'abord détectés par traitement de graphique et apprentissage automatique, puis les requêtes sont générées pour chaque groupe. Le niveau de **confiance de la requête** est une mesure de la capacité de la requête à couvrir les points terminaux. Un niveau de confiance de requête **Perfect** (idéal) indique que la requête couvre exactement le groupe suggéré (découvert). À l'autre extrême, un niveau de confiance de requête **Low** (faible) indique que la requête manque de manière significative la capture exacte du groupe suggéré, ce qui signifie que la requête couvre de nombreuses **adresses IP supplémentaires** (ne faisant pas partie du groupe découvert) et/ou a de nombreuses **adresses IP manquantes** (non couvertes par la requête).

Figure 35: Requêtes de sortie des suggestions de portée



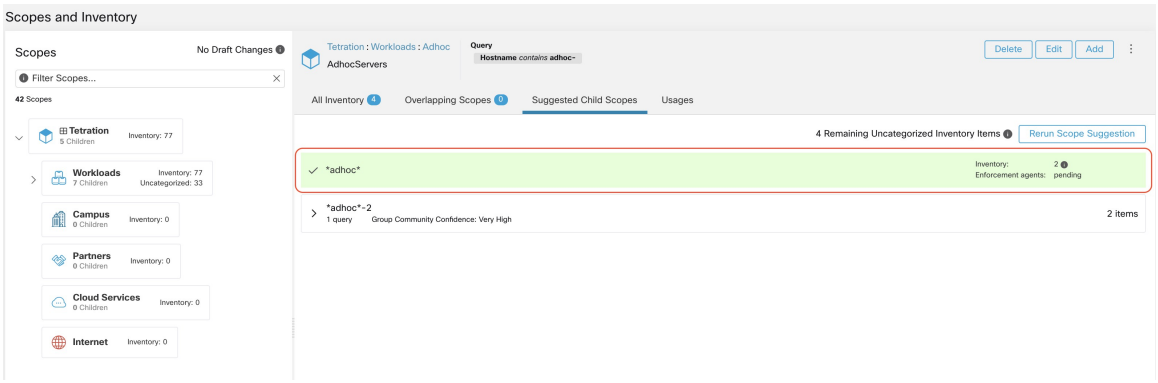
L'utilisateur peut cliquer sur le bouton **+ Scope** (+ Portée), ce qui le mènera à une fenêtre de modification dans laquelle il pourra modifier le nom du groupe et la requête de groupe. L'utilisateur peut examiner une requête, les adresses IP auxquelles elle correspond et décider si certaines adresses IP doivent être ajoutées ou supprimées en ajustant la requête. Une fois satisfait, l'utilisateur peut cliquer sur **Next**(suivant) pour examiner et convertir le groupe en une portée sur le sur le canevas de la vue préliminaire.

Figure 36: Fenêtre de modification des suggestions de portée



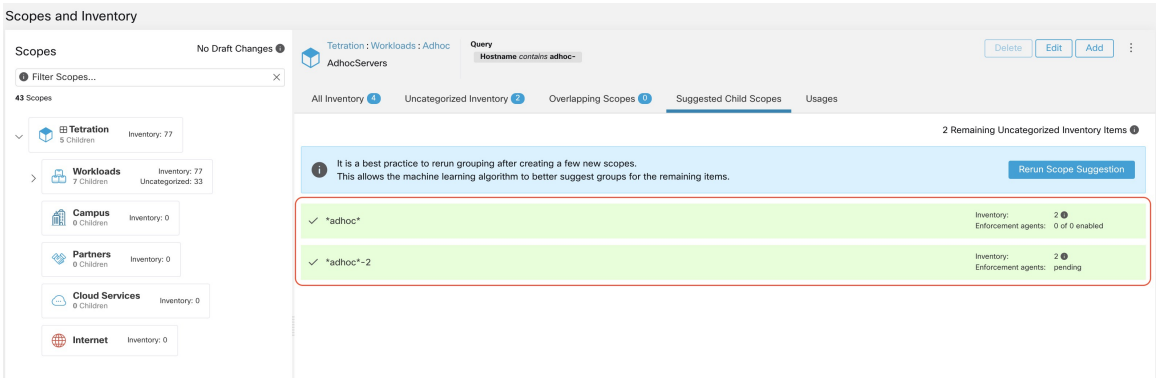
Une fois que l'utilisateur a converti un groupe suggéré en portée, l'emplacement de groupe devient vert et le **nombre Uncategorized Inventory Items (d'éléments en stock non catégorisés)** diminue.

Figure 37: Exemple de résultat de suggestion de portée après conversion d'un groupe suggéré en portée



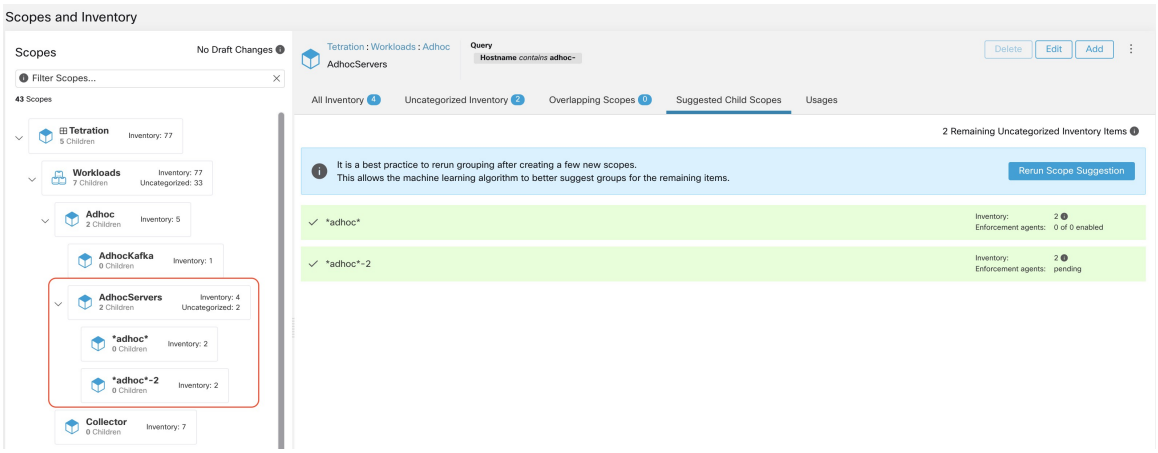
L'utilisateur peut répéter le processus de création de portée à partir de la liste de groupes restante. Le flux de travail recommandé est de créer une ou plusieurs portées, puis de réexécuter la **Suggestion de portée**. Un nombre nul **Uncategorized Inventory Items** (d'éléments d'inventaire non catégorisés) indique qu'il n'y a plus d'inventaire à délimiter (pour la portée parentale actuellement sélectionnée).

Figure 38: Résultat de suggestion de portée à partir de plusieurs créations de portée



Une fois le processus de création de portée terminé (le nombre non catégorisé est 0), l'utilisateur peut répéter ce processus sur les portées enfants nouvellement créées afin de générer une arborescence de portées plus approfondie, s'il le souhaite.

Figure 39: Liste des portées après la suggestion et la création de la portée initiale



Note Il est également possible que les éléments non catégorisés dans une portée ne se partitionnent pas bien (par exemple, qu'ils ne forment pas de communautés). Dans ce cas, l'algorithme peut ne renvoyer aucun regroupement (un résultat vide).

Filtres

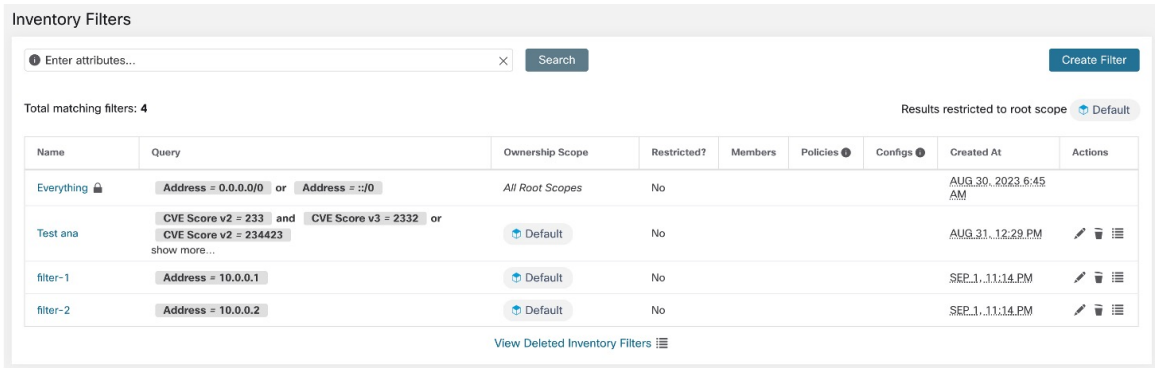
Les filtres sont des recherches d'inventaire enregistrées utilisées pour définir les politiques, les intents de configuration, etc. Évitez tout filtre associé à une portée, qui définit la portée de la propriété du filtre.

Pour afficher les filtres existants, cliquez sur **Organize (Organiser)** > **Inventory filters (Filtres d'inventaire)** dans la barre de navigation. Vous pouvez également afficher les filtres d'inventaire spécifiques à n'importe quel espace de travail pour n'importe quelle portée.

La liste des filtres est limitée en fonction de la racine de la portée actuellement sélectionnée.

Les filtres affichent également le nombre de membres, le nombre de politiques dans lesquelles il est impliqué, la somme des projets de politiques analysés et appliqués.

Figure 40: Filtres d'inventaire



Vous pouvez examiner les modifications apportées à l'appartenance à l'inventaire par rapport à la portée parente sélectionnée en consultant la fenêtre Examiner l'incidence des modifications de la portée/du filtre.

Créer un filtre d'inventaire

Créez des filtres d'inventaire pour :

- Créer ou découvrir des politiques spécifiques à des sous-ensembles de charges de travail dans une portée.

  Par exemple, créez un groupe de serveurs d'API dans la portée, les serveurs doivent être accessibles via l'interface d'API. Créez des politiques pour autoriser uniquement le trafic autorisé, mais bloquez l'accès à toutes les autres charges de travail pour cette application.

- Créez des politiques pour les charges de travail qui existent dans de nombreuses portées.

  Par exemple, pour créer une politique qui s'applique à toutes les charges de travail sur le réseau exécutant un système d'exploitation particulier, créez un filtre d'inventaire qui s'étend sur plusieurs ou sur toutes les portées.

Astuces Pour convertir une grappe existante en filtre d'inventaire, consultez Convertir une grappe en filtre d'inventaire.

Procédure

Étape 1 Accédez à l'un des emplacements suivants :

- Choisissez **Organize (Organiser) > Inventory filters (Filtres d'inventaire).**
- Accédez à n'importe quel espace de travail dans une portée pour lequel vous souhaitez créer un filtre d'inventaire et cliquez sur **Manage Policies** (Gérer des politiques) **> Filters** (Filtres).

Étape 2 Cliquez sur **Create Filter** (créer un filtre) ou **Add Inventory Filter**(ajouter un filtre d'inventaire).

Étape 3 Ajoutez un nom, une description et une requête qui inclut toutes les charges de travail, et seulement celles à inclure dans le filtre.

Étape 4 Cliquez sur **Show Advanced Options** (Afficher les options avancées).

Étape 5 Précisez la portée du filtre.

- Pour modifier le filtre, vous devez avoir un accès en écriture à la portée spécifiée ou à l'un de ses ascendants.
- (Selon les autres paramètres de cette procédure) Charges de travail incluses dans le filtre.

Étape 6 Configurer les options :

Destinataire	Faire ceci
Incluez les charges de travail qui répondent aux critères de requête du filtre, qu'elles soient ou non membres de la portée spécifiée dans ce filtre.	Désélectionnez **Restrict Query to Ownership Scope** (Restreindre la portée de la requête à la propriété)

Destinataire	Faire ceci
incluez uniquement les charges de travail qui sont membres de la portée spécifiée dans ce filtre.	Choisissez **Restrict Query to Ownership Scope** (Restreindre la requête à la portée de la propriété).
Autorisez la découverte automatique des politiques à suggérer des politiques spécifiques à l'ensemble de charges de travail défini par ce filtre. Ces charges de travail doivent constituer un sous-ensemble de la portée spécifiée dans le filtre.	Sélectionnez **Restrict Query to Ownership Scope (Restreindre la requête à la portée de la propriété)** et **Provides a Service External of its Scope (fournit un service externe à sa portée).** Pour utiliser ce filtre, vous devez configurer des dépendances externes. Pour en savoir plus, consultez Ajuster les dépendances externes d'un espace de travail.

Étape 7 Cliquez sur **Next** (suivant).

Étape 8 Passez en revue les renseignements détaillés et cliquez sur **Create** (Créer).

Créer un filtre de domaine

Utilisez un filtre de domaine pour regrouper les domaines et identifier les flux pour lesquels un nom de domaine de consommateur ou de fournisseur correspond au filtre défini dans votre environnement.

En mode conversation, seuls certains types de serveurs mandataires sont pris en charge pour l'application du domaine, comme les mandataires HTTP et TCP. Dans le cas de TCP, lorsqu'un domaine est bloqué par un intent, le premier paquet peut le traverser; cependant, la connexion est bloquée avant même la fin de l'établissement de liaison.

Règles pour les filtres de domaine

- Vous ne pouvez saisir que deux noms de domaine dans le champ de **requête**, par exemple mail.cisco.com ou domain name=*cisco.com. Les noms de domaine tels que .com, .org ou .net ne sont pas pris en charge.
- Chaque étiquette du nom de domaine ne peut contenir que des lettres, des chiffres ou un tiret.
- Utilisez le caractère générique * dans le nom de domaine et uniquement pour la première étiquette, par exemple .Amazon.com, mais n'utilisez pas aws.com. De plus, ne combinez pas les caractères génériques avec d'autres caractères à l'aide de l'expression régulière, par exemple, n'utilisez pas aws*.com.
- Un caractère générique correspond à n'importe quel nombre d'étiquettes (sous-domaines), par exemple, .yahoo.com correspond à finance.yahoo.com, web.finance.yahoo.com et à tous ses sous-domaines. Cependant, il ne correspond pas à yahoo.com.
- Le préfixe www est traité comme un sous-domaine et n'est donc pas traité comme le domaine lui-même; par exemple, google.com et www.google.com sont des domaines distincts.
- Ne limitez pas la portée des filtres d'inventaire. Si un objet correspond au filtre, appliquez-le à l'ensemble du détenteur en saisissant DOMAIN.

Procédure

Étape 1 Accédez à l'un de ces emplacements :

- Choisissez **Organize (Organiser) > Inventory filters (Filtres d'inventaire).**
- Accédez à un espace de travail dans la portée pour créer un filtre d'inventaire, cliquez sur **Manage Policies (Gérer les politiques)** > **Filters(Filtres)** > **Inventory Filters (Filtres d'inventaire).**

Étape 2 Cliquez sur **Create Filter** ou **Add Inventory Filter** (Ajouter un filtre d'inventaire) pour afficher la page Inventory Filter (filtre d'inventaire).

Étape 3 Cochez la case. **Domain Filter** (Filtre de domaine).

Étape 4 Saisissez un nom et une requête pour le filtre de domaine, puis cliquez sur **Next**(suivant).

Étape 5 Passez en revue les détails et cliquez sur **Create** (créer) pour créer un filtre de domaine.

Pour chaque nouveau filtre d'inventaire, créez un nouveau type d'objet correspondant qui définit le type d'objets pour les correspondances de filtre. Les valeurs possibles sont les suivantes :

- **INVENTORY (INVENTAIRE)** comprend les charges de travail, les services, les pods et les adresses IP.
- **DOMAIN (DOMAINE)** fait référence aux domaines. Le nom de domaine est la seule option disponible pour la mise en correspondance des domaines; toutes les autres options correspondent uniquement au type **INVENTORY**.

Vous pouvez créer un filtre hétérogène en utilisant le nom de domaine et une autre option avec un opérateur **OU** , par exemple domain name= `*.google.com` OR hostname that contains `mach`. Cependant, il n'est pas possible d'utiliser **AND** pour combiner ces aspects à l'aide de l'opérateur **AND**, par exemple domain name=`*.Google.com` **AND** hostname that contains `mach`.

Limiter à la portée de la propriété

Cochez la case **Restrict to Ownership Scope?** (Restriction à la portée de la propriété?) pour déterminer si la portée a une incidence sur l'inventaire qui correspond au filtre. Par exemple, dans la structure suivante :

1. Détenteur avec requête

   ```
   VRF ID = 3
   ```

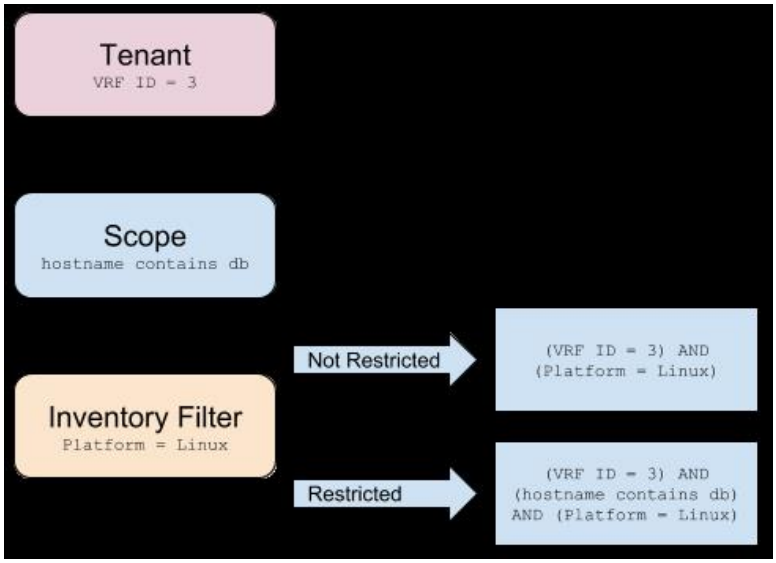
2. Portée au sein du détenteur avec la requête

   ```
   hostname contains db
   ```

3. Filtre d'inventaire avec la requête suivante associée à une portée.

   ```
   Platform = Linux
   ```

Figure 41: Structure de filtre des détenteurs, de la portée et de l'inventaire



- Si vous ne choisissez pas **Restrict to Ownership Scope**(Restreindre à la portée de la propriété), le filtre correspond à tous les hôtes du détenteur qui correspondent également au filtre. Saisissez la requête suivante :

  ```
  (VRF ID = 3) AND (Platform = Linux)
  ```

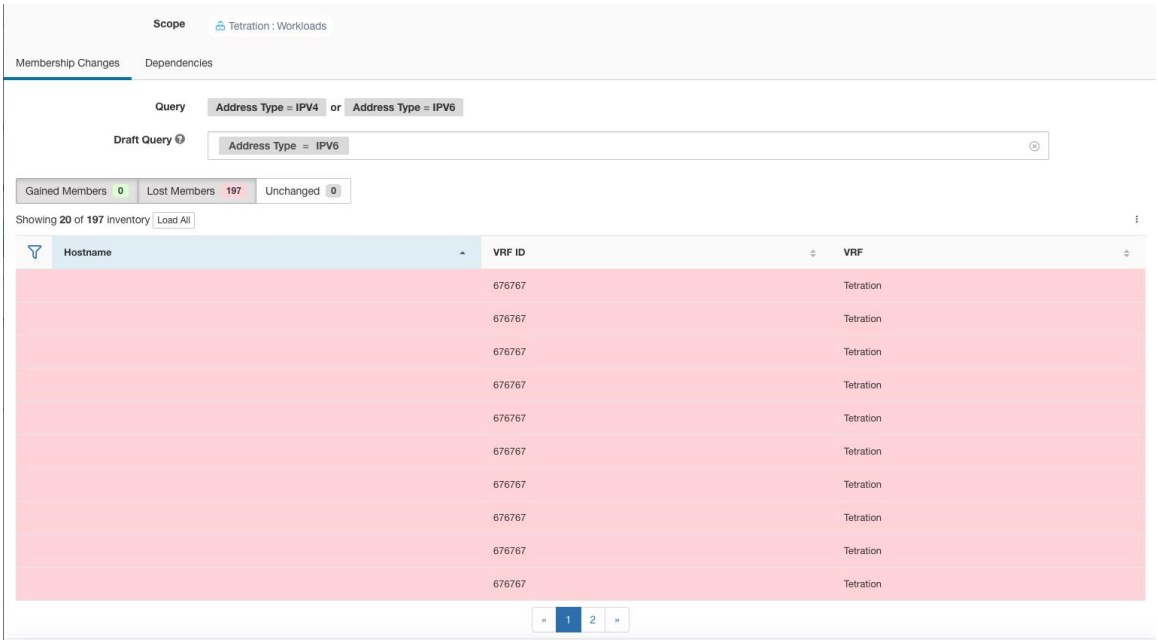
- Si vous choisissez **Restreindre à la portée de la propriété**, le filtre ne correspondra qu'aux hôtes du détenteur et de la portée qui correspondent également au filtre. Saisissez la requête suivante :

  ```
  (VRF ID = 3) AND (hostname contains db) AND (Platform = Linux)
  ```

Examiner l'incidence des modifications de la portée/du filtre

La mise à jour d'une requête de portée peut avoir une incidence sur les membres de l'inventaire de la portée après sa validation. De même, la modification de la requête de filtre, qui est enregistrée directement, peut également avoir une incidence sur les membres de l'inventaire de la portée. Vous pouvez identifier les changements de membres entre les nouvelles et les anciennes requêtes en suivant le lien **Review query change impact** (Examiner l'impact des modifications de requêtes) dans les boîtes de dialogue Scopes (Portée) ou Filter Edit (Modifier les filtres). En outre, connaître la portée ou les dépendances des filtres peut être utile pour l'analyse d'impact et la suppression de tous les objets nécessaires à la suppression de la portée. Visitez également l'onglet **Dépendances** pour parcourir l'arborescence des dépendances de la portée et obtenir de plus amples renseignements.

Figure 42: Télécharger le tableau des membres



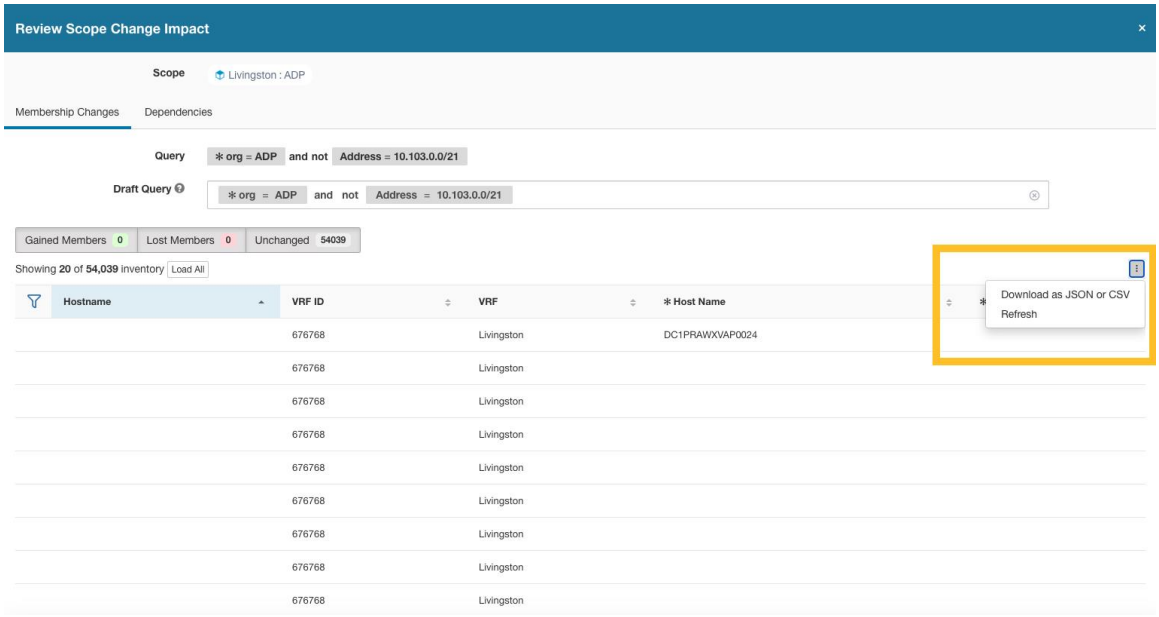
Boîte de dialogue de l'incidence de la modification de la requête de portée

Vous pouvez accéder à l'onglet **Membership Changes** (Modifications de l'adhésion) **Dependencies** (Dépendances) en cliquant sur le lien **Review query change impact** (Examiner l'impact des modifications de la requête) sur la fenêtre Scope Edit (Modification de la portée).

Modifications apportées aux membres

Le tableau d'inventaire sous la vue Membres affiche toutes les colonnes par défaut. Vous pouvez choisir les colonnes à afficher. En outre, vous pouvez télécharger le fichier csv ou json des colonnes et des lignes d'adhésion choisies avec une colonne Diff supplémentaire indiquant si l'inventaire est **gagné**, **perdu** ou **inchangé**. Assurez-vous que toute la sélection de tableaux que vous souhaitez télécharger est visible dans la vue du tableau.

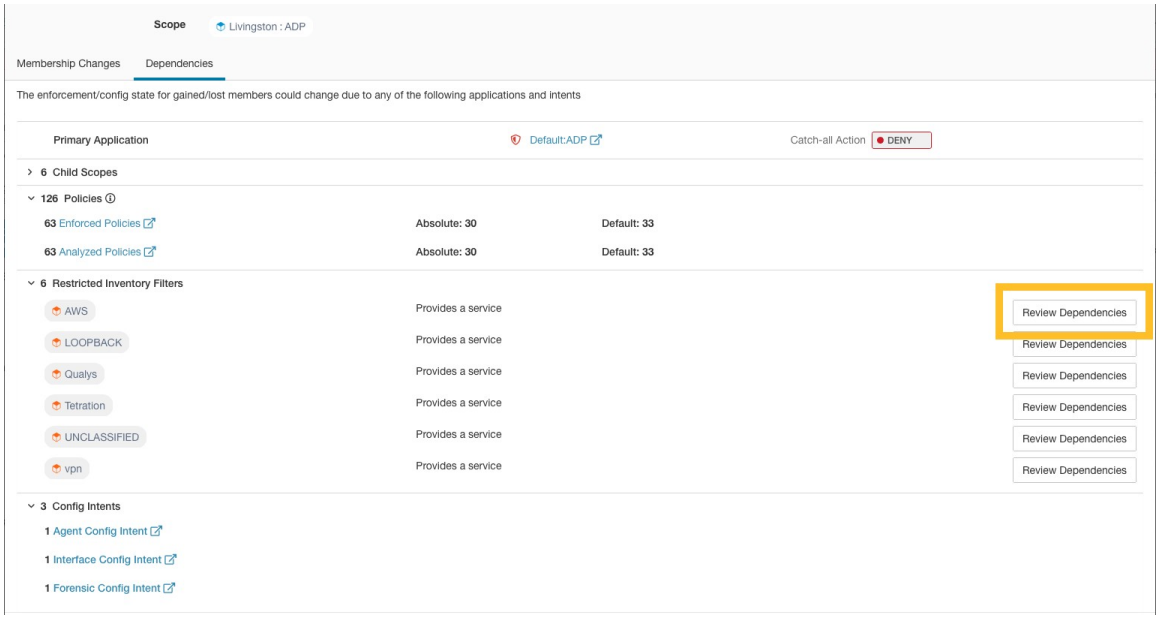
Figure 43: Modifications apportées aux membres de la portée



Dépendances

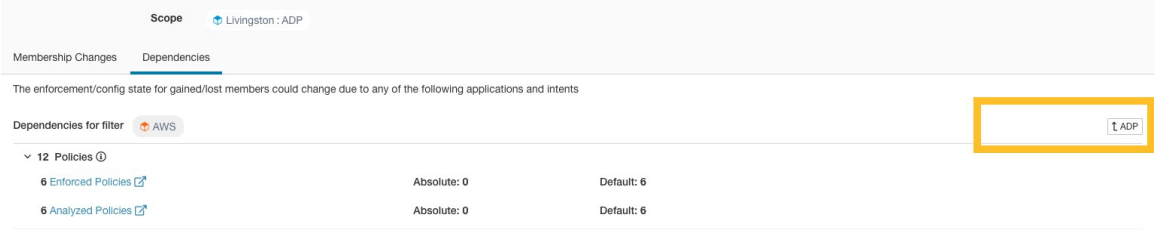
Vous pouvez parcourir les dépendances imbriquées en cliquant sur **Review Dependencies** (Examiner les dépendances).

Figure 44: Examiner les dépendances



Vous pouvez parcourir la sauvegarde de l'arborescence des dépendances en sélectionnant le lien parent sélectionné :

Figure 45: Lien parent



Les dépendances de portée qui peuvent exister sont les suivantes :

Table 3: Les dépendances de portée qui peuvent exister sont les suivantes

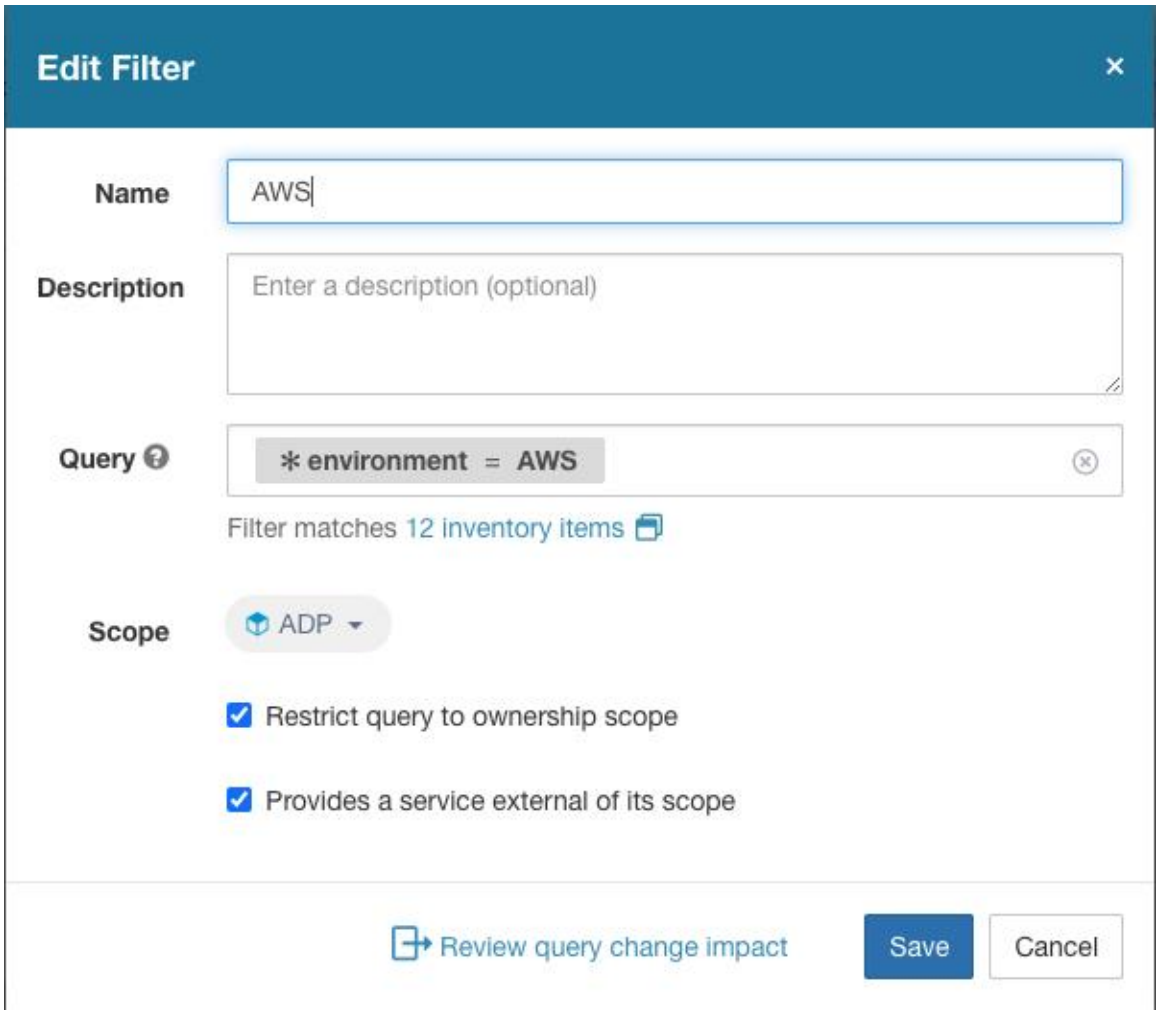
Type	Description
Application	Comporte des noms d'applications principales et secondaires et des liens vers des espaces de travail spécifiques dans la section Segmentation.
Portées enfants	Comporte des noms et des liens vers les vues détaillées de la portée enfant. Permet d'accéder aux dépendances de niveau inférieur.
Policies	A analysé et appliqué le nombre de politiques et les liens vers les vues de politiques globales respectives, filtrées par la portée sélectionnée.
Filtres d'inventaire restreint	Comporte des noms et des liens vers les vues détaillées des filtres enfants. Permet d'accéder aux dépendances de niveau inférieur.
Config Intents	Dispose de noms et de liens vers les affichages des intents de configuration d'agent, d'interface et criminalistiques.

Boîte de dialogue de l'incidence de la modification de la requête de filtre

Vous pouvez accéder à l'onglet **Membership Changes** (Modifications de l'adhésion) et à l'onglet **Dependencies** (Dépendances) en cliquant sur le lien **Review query change impact** (Examiner l'impact des modifications de la requête) dans la fenêtre de modification du filtre d'inventaire.

Modifications apportées aux membres

Figure 46: Modifications apportées aux membres pour le filtre d'inventaire



Dépendances

Voici les dépendances de filtres qui peuvent exister :

Type	Description
Policies	A analysé et appliqué le nombre de politiques et les liens vers les vues de politiques globales respectives, filtrées par la portée sélectionnée.
Config Intents	Dispose de noms et de liens vers les affichages des intents de configuration d'agent, d'interface et criminalistiques.

Profil d'inventaire

Note Il existe des liens vers une page de profil d'inventaire à partir de divers emplacements. L'une des façons d'afficher un profil d'inventaire consiste à effectuer une recherche d'inventaire, puis à cliquer sur une adresse IP pour accéder à son profil. Si vous travaillez dans la page Scopes and Inventory (Portées et inventaire), cliquez sur une adresse IP de l'onglet IP address (adresses IP), et non sur une adresse IP dans l'onglet Workloads (Charges de travail). (Cliquer sur une adresse IP dans l'onglet Workloads (Charges de travail) pour afficher le profil de charge de travail et non le profil d'inventaire).

Les renseignements suivants sont disponibles pour l'inventaire :

Champ	Description
Portées	Liste des portées à laquelle appartient l'inventaire.
Type d'inventaire	• L'inventaire **Flow learnt** (flux appris) a été enregistré en fonction des flux observés. • L'inventaire**Labeled** (étiqueté) a été téléversé manuellement à l'aide de l'utilitaire de téléchargement d'inventaire. • L'inventaire de l'**Agent** a été signalé par l'agent logiciel installé sur un hôte. • L'inventaire **Tagged** (marqué) a été signalé par les connecteurs ou par des orchestrateurs externes.
Étiquettes d'utilisateur	La liste des attributs téléversés par l'utilisateur pour cet inventaire. Consultez la section Étiquettes de charge de travail (Étiquettes d'utilisateur) pour en savoir plus.

Des renseignements supplémentaires ne sont disponibles que si les deux conditions suivantes sont remplies :

1. L'inventaire a été intégré par un connecteur infonuagique.
2. La segmentation est activée pour le réseau virtuel dans lequel se trouve l'inventaire.

Champ	Description
Intégrité de l'application	Les renseignements sur l'état de l'agent logiciel hôte. Consultez Onglet Agent Health (Intégrité de l'agent) (intégrité de l'agent) pour en savoir plus.

Champ	Description
Politiques concrètes	Cet onglet affiche politiques application concrètes de Cisco Secure Workload appliquées à l'hôte. Consultez Onglet Concrete Policies (Politiques concrètes) (Politiques concrètes) pour en savoir plus.
Groupes de sécurité	La liste des groupes de sécurité et leurs politiques appliquées à cet inventaire.

Renseignements sur le profil de l'inventaire

Champ	Description
Groupes **expérimentaux**	Une liste de filtres d'inventaire définis par la grappe ou par l'utilisateur qui sont utilisés pour l'analyse en temps réel des politiques.
Groupes d'**application**	Une liste des filtres d'inventaire définis par la grappe ou par l'utilisateur qui sont utilisés pour l'application des politiques. Ils peuvent être différents des groupes expérimentaux selon les versions des politiques analysées ou appliquées dans le système.

Note Les détails du profil d'inventaire peuvent ne pas être disponibles pour une adresse IP donnée dans les cas suivants :

- L'inventaire est exclu des règles de collecte.
- Dans un flux unidirectionnel, l'inventaire n'est disponible que pendant deux minutes, puis il est supprimé.
- Dans un flux bidirectionnel, l'inventaire est disponible pendant 30 jours. Si plus aucun flux n'est observé pendant ces 30 jours, les renseignements détaillés de l'inventaire sont supprimés.

Profil de la charge de travail

Le profil de charge de travail affiche des informations détaillées sur un hôte sur lequel un agent logiciel Cisco Secure Workload est installé. Cette section explique comment afficher un profil de charge de travail et les renseignements qu'il contient.

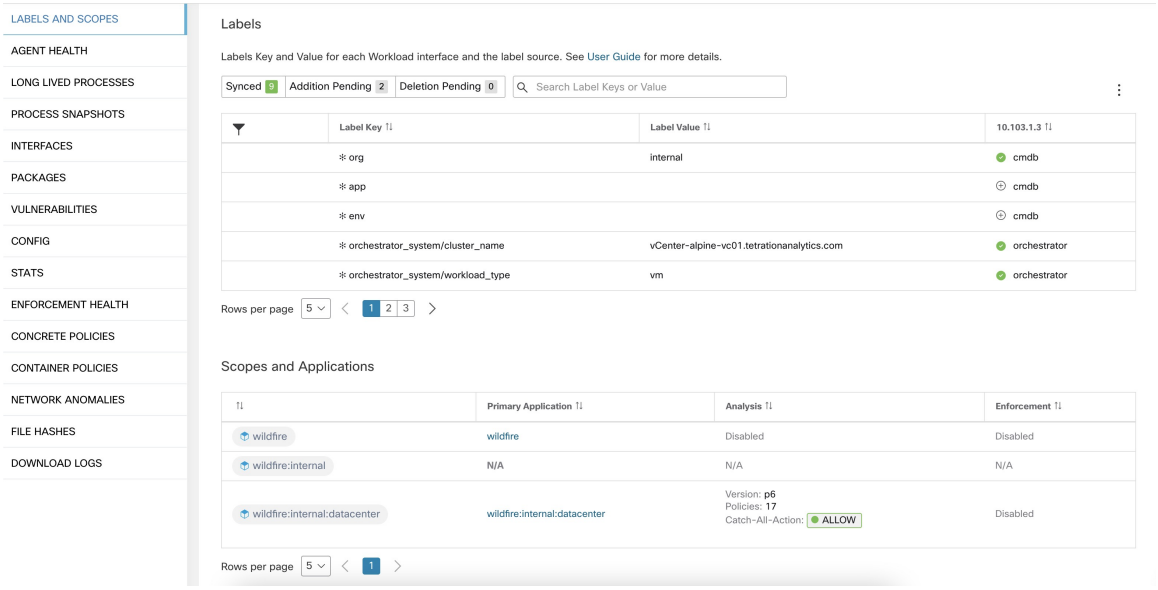
Note Il existe des liens vers une page de profil de charge de travail à partir de divers emplacements. L'une des façons d'afficher un profil de charge de travail consiste à rechercher un hôte comme décrit dans la section de recherche

Dans les résultats de la recherche d'inventaire, cliquez sur l'adresse IP de l'hôte pour accéder à son profil. En fonction du type d'agent installé sur l'hôte, les onglets suivants sont disponibles sur la page. Notez que vous pourriez vous aboutir à la page de profil d'inventaire si l'agent logiciel Cisco Secure Workload n'est pas installé sur l'hôte auquel cet inventaire appartient.

Onglet Labels and Scopes (Étiquettes et portées)

Cet onglet comprend les groupes d'applications et expérimentaux, auxquels l'hôte appartient. Les groupes expérimentaux sont des filtres d'inventaire utilisés pour l'analyse en direct des politiques, tandis que les groupes d'application sont des filtres utilisés pour l'application de celles-ci. Ils peuvent être différents selon les versions des politiques analysées ou appliquées dans le système.

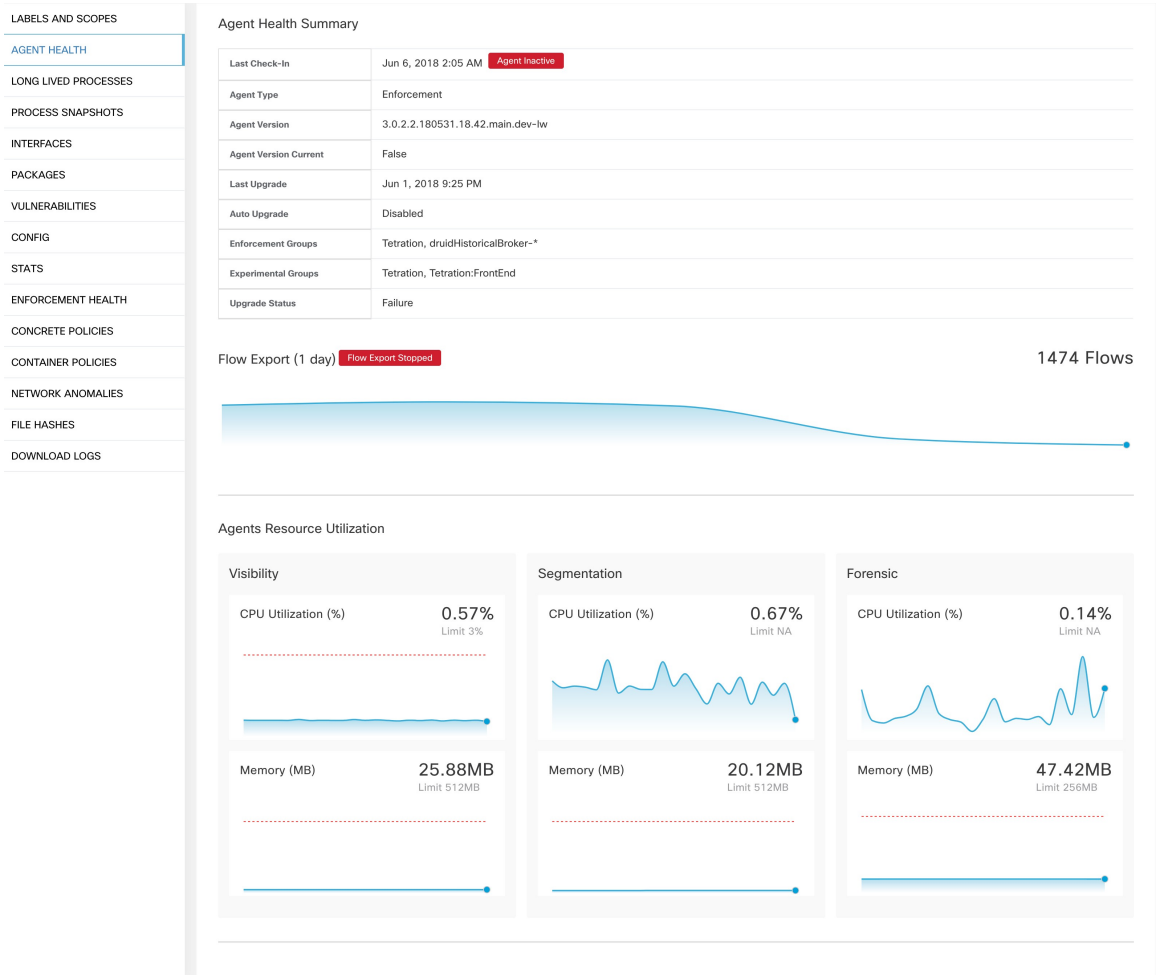
Figure 47: Étiquettes et portées de charge de travail



Onglet Agent Health (Intégrité de l'agent)

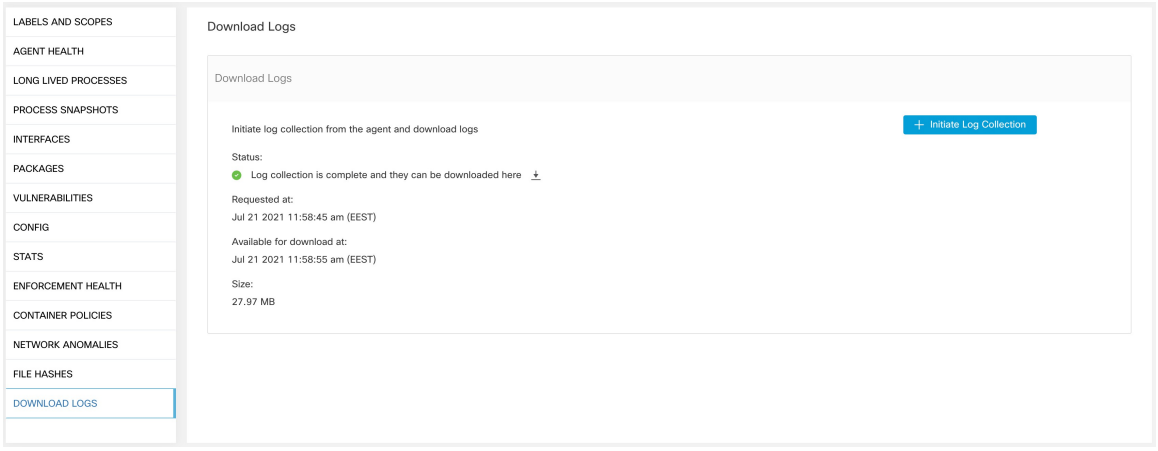
Les renseignements sur l'état de l'agent logiciel hôte, comme son type, la plateforme de système d'exploitation, la version de l'agent et l'heure de la dernière connexion, sont également affichés dans l'onglet **Agent Health (** intégrité de l'agent). Reportez-vous à la section Configuration de l'agent logiciel pour en savoir plus. Cet onglet affiche également les données de série chronologiques détaillées pour les octets de trafic et les paquets générés pour une journée.

Figure 48: Détails de l'intégrité des agents de charge de travail



Pour les utilisateurs disposant de privilèges de propriétaire de portée racine, la page de résumé comprend également une section pour recueillir et télécharger les journaux des agents pour les agents de visibilité approfondie et d'application (versions 3.3 ou ultérieures) de cette portée racine. Notez également que cette fonction n'est pas disponible pour les agents exécutés sur les plateformes AIX et SUSE Linux Enterprise Server (s390x-Linux sur architectures IBM Z). Utilisez le bouton « Lancer la collecte des journaux » pour collecter les journaux de l'agent. Ces journaux sont disponibles pour téléchargement quelques minutes plus tard. Si le téléchargement échoue, réessayez de collecter les journaux, puis tentez à nouveau le téléchargement.

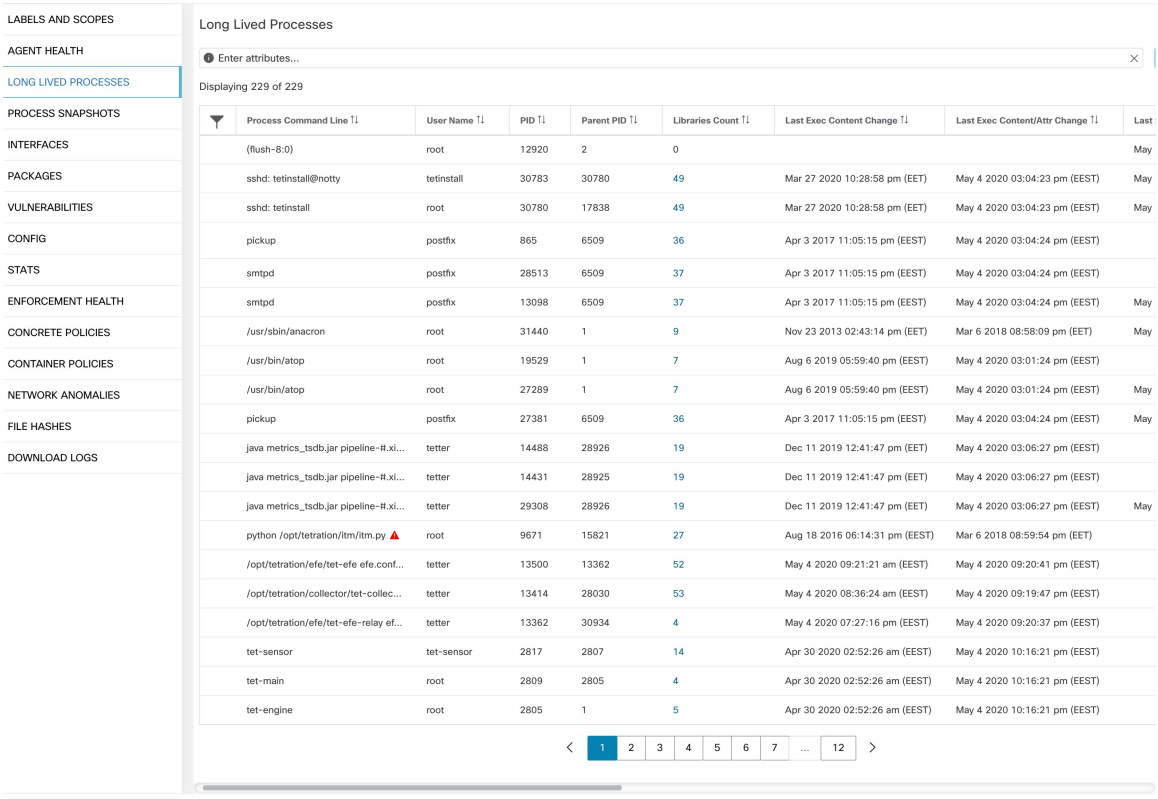
Figure 49: Journaux des agents



Onglet Liste de processus

Cet onglet affiche la liste des processus en cours d'exécution sur l'hôte. Un filtre est également disponible pour affiner la liste des processus en fonction des attributs d'un processus affichés dans l'en-tête du tableau ci-dessous.

Figure 50: Liste des processus de charge de travail



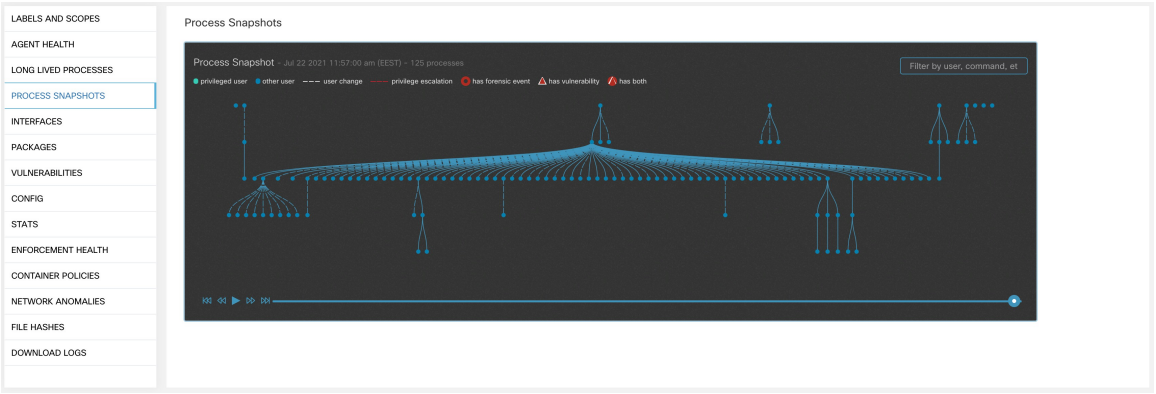
Descriptions des attributs :

Attribut	Description
Last Exec Content Change	Similaire à mtime dans Linux. Il s'agit de l'horodatage lorsque seul le contenu du fichier change.
Last Exec Content Change	Similaire à ctime dans Linux. Il s'agit de l'horodatage auquel le contenu ou l'attribut du fichier change.
Last Seen	Dernière fois que le processus est observé. Disponible lorsque le processus est arrêté.
Utilisation du processeur	Tendance d'utilisation du processeur par le processus au cours de la dernière heure.
Memory Usage	Tendance d'utilisation de la mémoire par le processus au cours de la dernière heure.
Traiter le condensé binaire	Condensé SHA256 du fichier binaire de processus dans la chaîne hexadécimale, également appelé condensé de processus. Non disponible pour les processus du noyau.
Note d'anomalie	Note de condensé de processus (anomalie). Consultez la section Détection des anomalies de condensé de processus pour plus d'informations.
Verdict	Verdict du condensé du processus (soit malveillant, soit bénin). Le verdict est déterminé en fonction de l'appartenance du condensé du processus à une liste de condensés définie par l'utilisateur ou à une base de données de condensés connue de renseignements sur les menaces. Consultez la section Détection des anomalies de condensé de processus pour plus d'informations.
Verdict Source	Source du verdict. La source de verdict peut être définie par l'utilisateur, Nuage Cisco Secure Workload ou NIST. Cet attribut est connu sous le nom de source de base de données de condensé dans les versions précédentes. Consultez la section Détection des anomalies de condensé de processus pour plus d'informations.

Onglet Process Snapshot (Instantané du processus)

Cet onglet affiche l'arborescence des processus interrogeable observé pour la charge de travail.

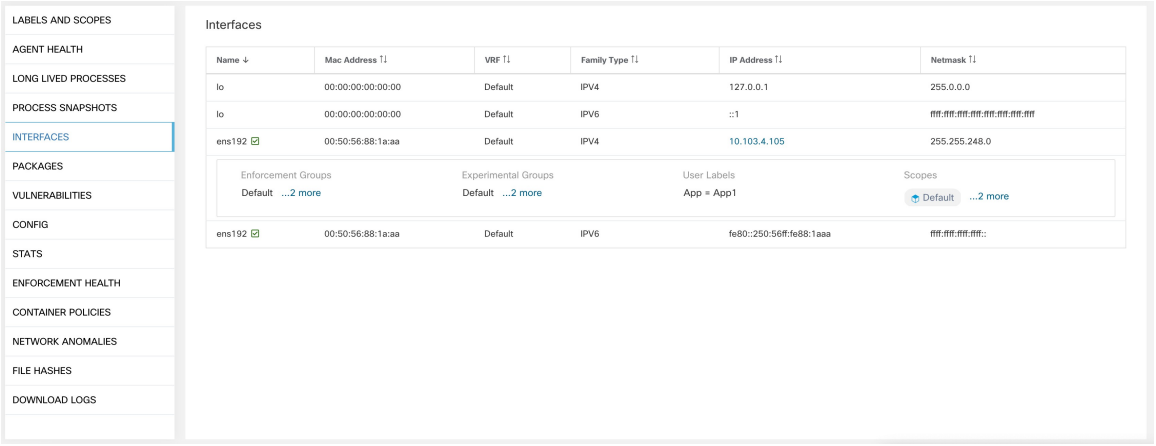
Figure 51: Instantané du processus de charge de travail



Onglet Interfaces

Cet onglet affiche des détails sur les interfaces réseau installées sur l'hôte. Il est disponible pour tous les types d'agents logiciels.

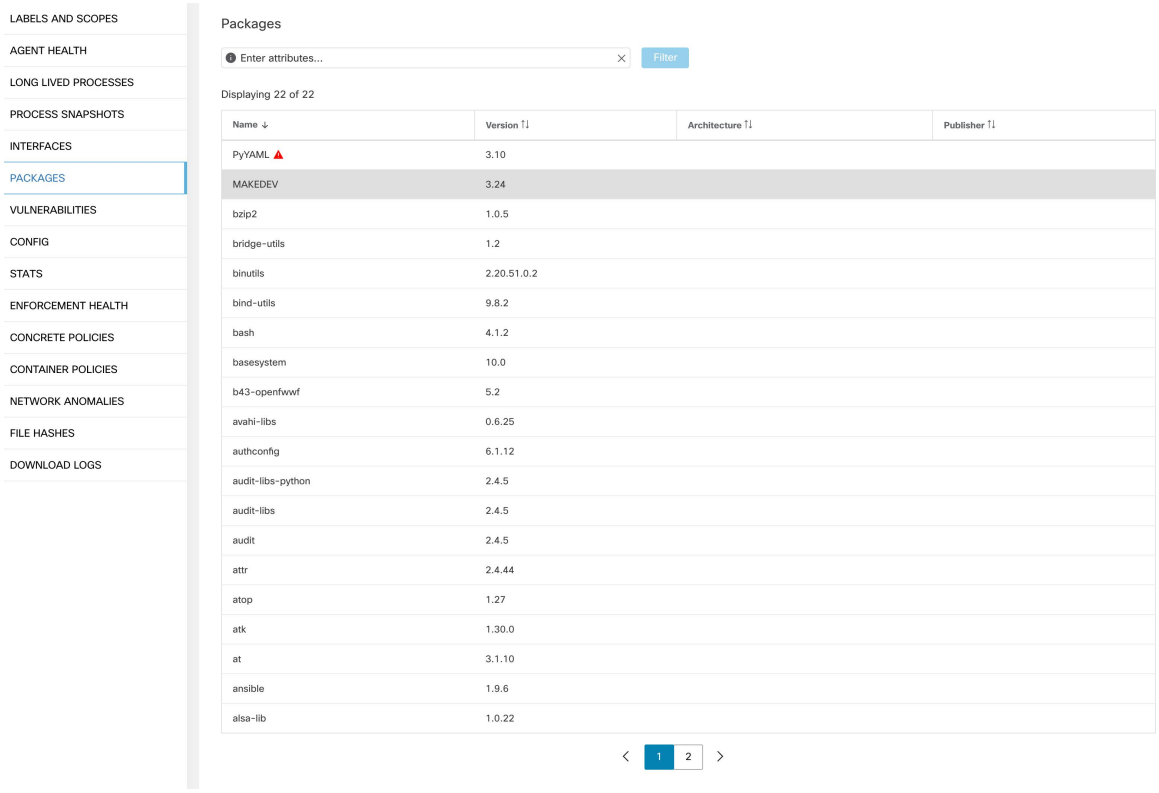
Figure 52: Liste des interfaces de charge de travail



Onglet Software Packages (Paquets logiciels)

Cet onglet affiche la liste des paquets logiciels installés sur l'hôte. Vous pouvez afficher de manière sélective les paquets logiciels en fonction des attributs du paquet dans l'en-tête du tableau.

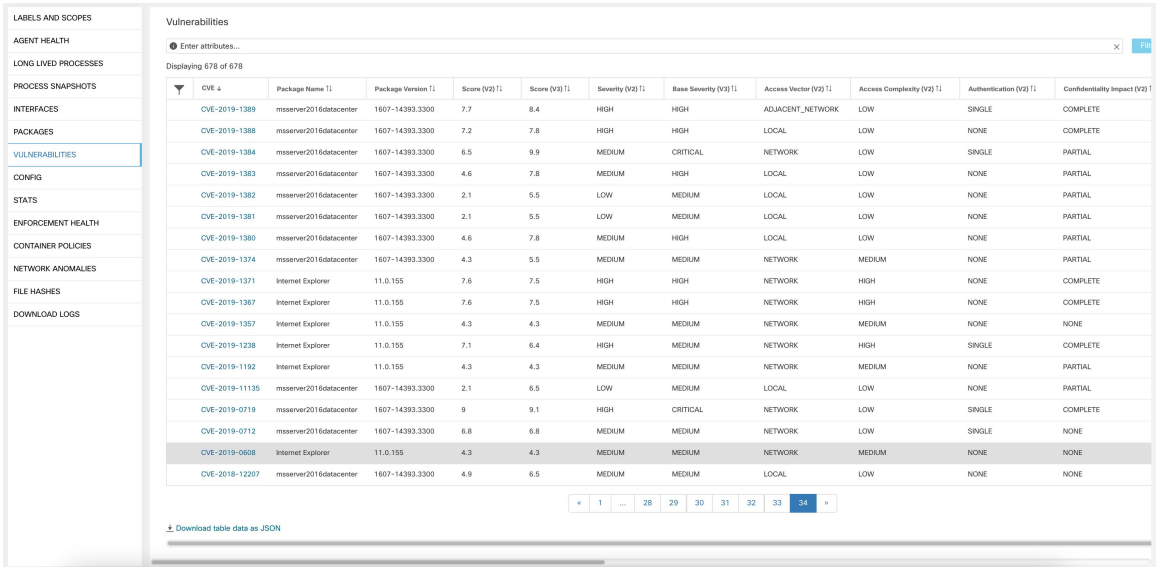
Figure 53: Liste des paquets logiciels



Onglet Vulnerabilities (Vulnérabilités)

Cet onglet affiche les vulnérabilités consultables observées sur la charge de travail en fonction des vulnérabilités et expositions courantes (CVE). Consultez la section Visibilité des données de vulnérabilité

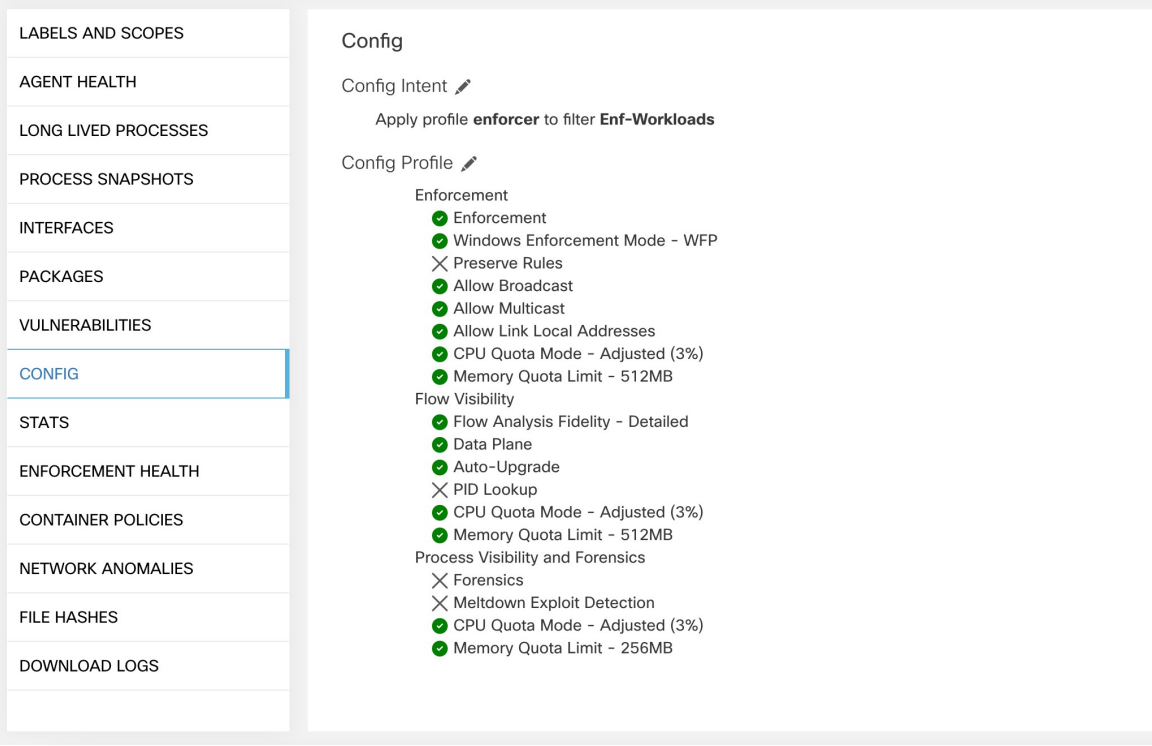
Figure 54: Onglet Vulnerabilities (Vulnérabilités)



Onglet Configuration de l'agent

Cet onglet affiche les paramètres de l’agent logiciel. Il est uniquement disponible pour les agents de visibilité approfondie et d’application. Ces paramètres peuvent être modifiés à l’aide des intents de configuration de l’agent via la page de configuration de l’agent. Voir configuration de l’agent logiciel

Figure 55: Configuration de charge de travail appliquée



Onglet Statistiques de l'agent

Cet onglet affiche les statistiques sur l'agent Cisco Secure Workload installé sur l'hôte. Il est uniquement disponible pour les agents de visibilité approfondie et d'application.

Figure 56: Statistiques des agents

Onglet Concrete Policies (Politiques concrètes)

Lorsqu'un espace de travail est mis en œuvre, chaque charge de travail reçoit uniquement les politiques de cet espace de travail qui sont spécifiques à cette charge de travail. Ces politiques qui sont effectivement programmées sur chaque charge de travail sont appelées *politiques concrètes*.

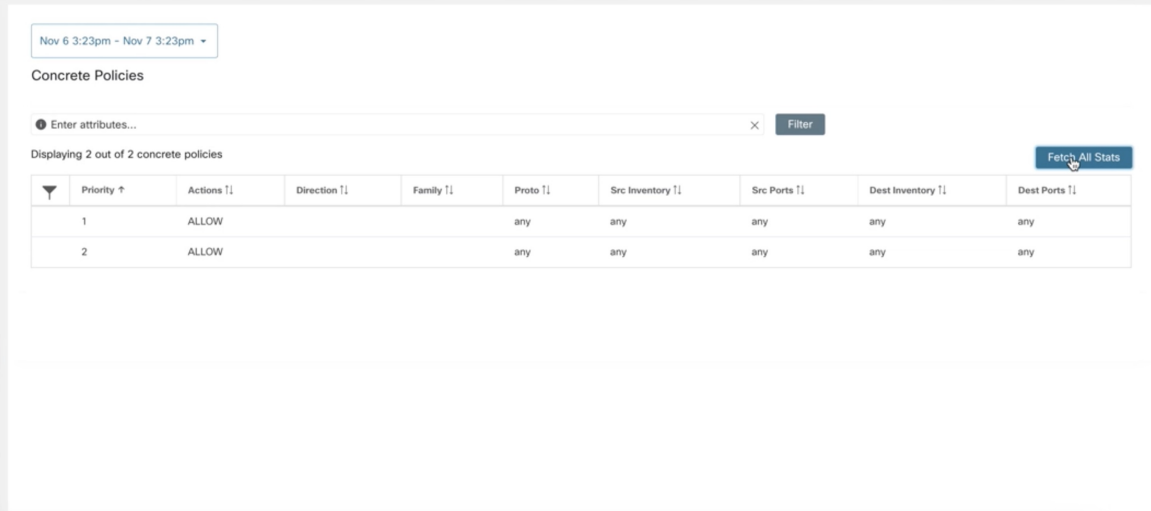
Par exemple, supposons que le fournisseur spécifié dans une politique avec l'action ALLOW (AUTORISER) inclue tout l'inventaire du sous-réseau 1.1.1.0/24. Lorsque cette politique est installée sur une charge de travail avec un agent Cisco Secure Workload et ayant l'adresse IP 1.1.1.2, les règles du pare-feu se présentent comme suit :

1. En ce qui concerne le trafic entrant, les règles du pare-feu autorisent le trafic destiné à l'adresse IP 1.1.1.2 en particulier, et non à l'ensemble du sous-réseau 1.1.1.0/24.
2. Pour le trafic sortant, les règles de pare-feu autorisent le trafic provenant dans la version 1.1.1.2 en particulier, et non de l'ensemble du sous-réseau 1.1.1.0/24.

L'onglet CONCRETE POLICIES (POLITIQUES CONCRÈTES) du profil de charge de travail affiche les politiques d'application concrètes de Cisco Secure Workload appliquées sur l'hôte. Chaque ligne de ce tableau correspond à une règle de pare-feu mise en œuvre sur l'hôte. Chaque ligne de politique peut être développée pour afficher l'intent logique dont cette politique concrète est dérivée. L'affichage de la série chronologique du nombre de paquets et d'octets est également disponible pour chaque règle. Cliquez sur le bouton **Fetch All Stats** (Récupérer toutes les statistiques) pour afficher le nombre de paquets et d'octets pour chaque règle. Un filtre est également disponible dans cet onglet pour réduire la liste des politiques appliquées en fonction

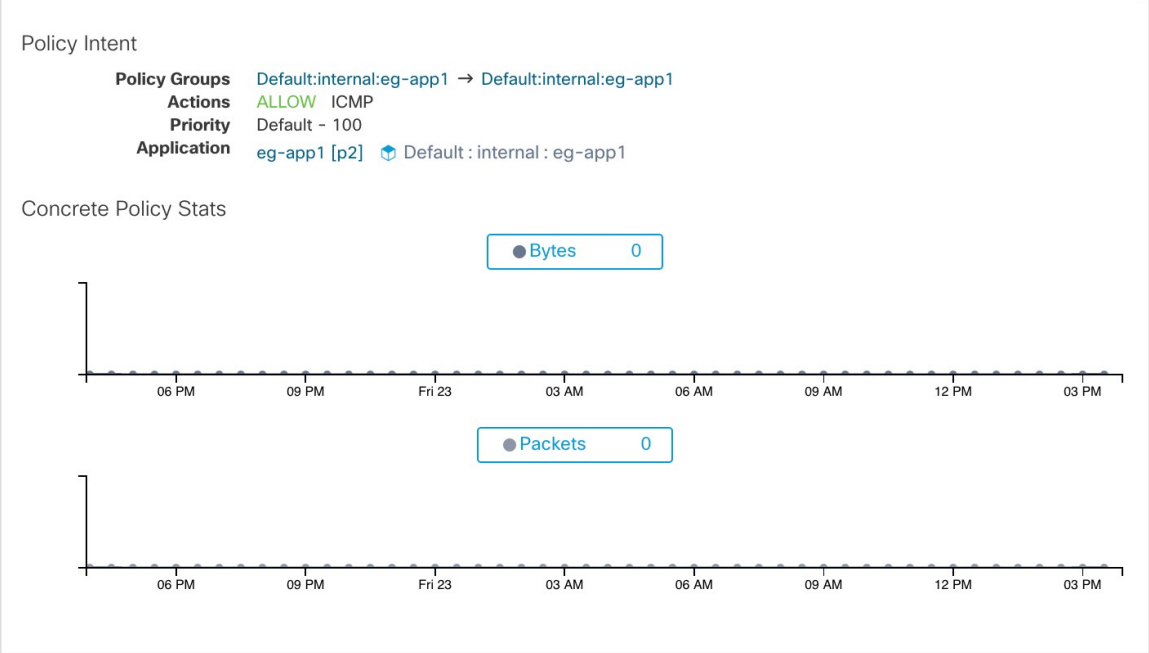
des attributs d'une politique indiqués dans l'en-tête du tableau ci-dessous. Cet onglet est disponible uniquement lorsque l'agent installé est activé pour la mise en application.

Figure 57: Liste de politiques concrètes



Dans l'image ci-dessous, les **groupes de politiques** affichent le consommateur et le fournisseur :

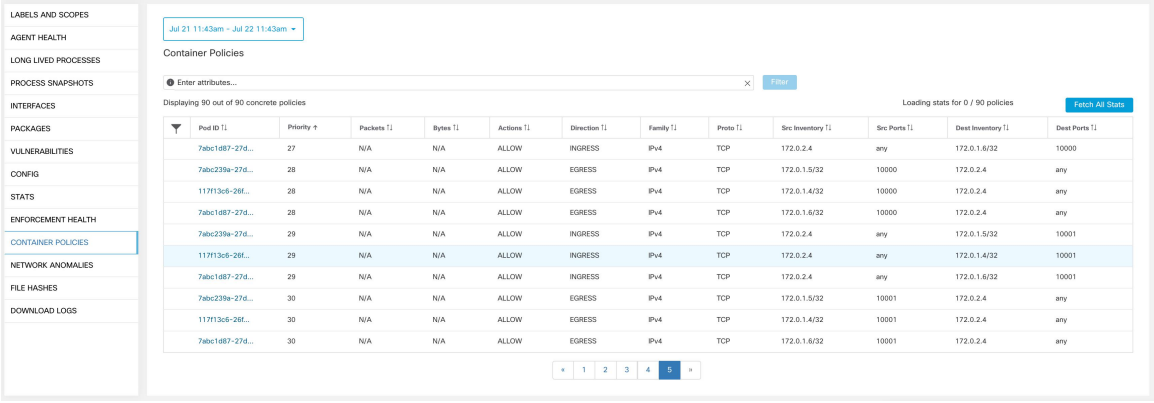
Figure 58: Ligne de politique concrète



Onglet Politiques de conteneur

Cet onglet affiche les politiques d'application concrètes Cisco Secure Workload appliquées aux conteneurs. Chaque ligne de ce tableau correspond à une règle de pare-feu mise en œuvre sur le pod de conteneur.

Figure 59: Liste des politiques concrètes de conteneur



Onglet Network Anomalies (Anomalie de réseau)

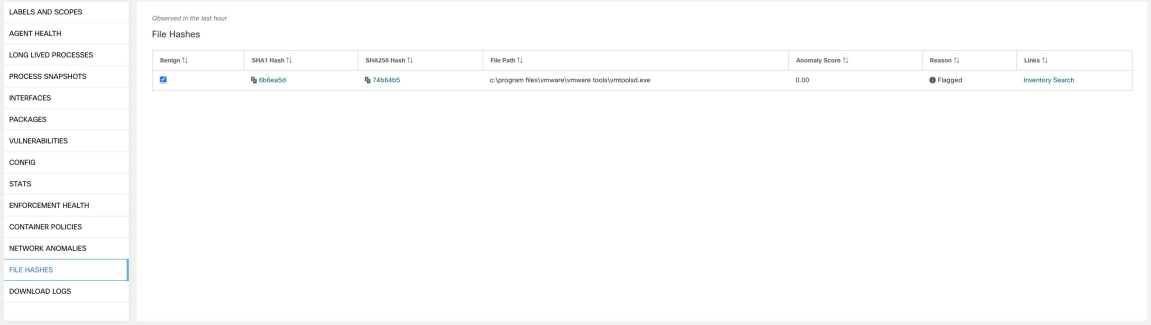
Cet onglet permet d'identifier les événements comportant des mouvements de données volumineux vers ou hors de cette charge de travail. Consultez Détection d'anomalies de réseau par PCR pour obtenir plus de renseignements.

Figure 60: Anomalie de réseau de la charge de travail

Onglet Condensés de fichiers

Cet onglet détecte les anomalies de condensé de processus en évaluant la cohérence des condensés binaires de processus dans le système. Consultez la section Détection des anomalies de condensé de processus pour en savoir plus.

Figure 61: Condensés de fichiers de charge de travail



Paquets logiciels

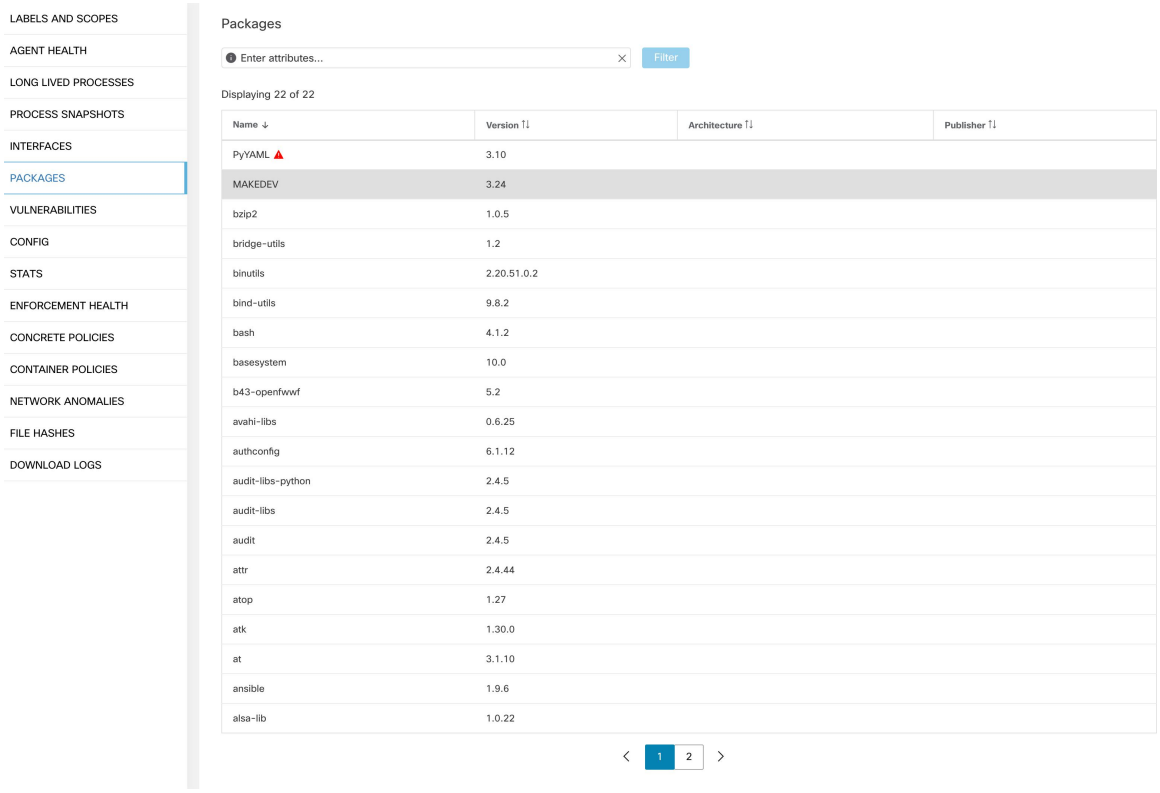
La fonctionnalité **Paquets logiciels** permet de visualiser les paquets installés sur les hôtes et les vulnérabilités qui les affectent. Plus précisément, elle permet de :

- Afficher les paquets enregistrés avec les gestionnaires de paquets suivants :
  - Linux : Gestionnaire de paquet RedHat (RPM) et gestionnaire de paquet Debian (dpkg)
  - Windows : Service de registre de Windows
- Afficher les vulnérabilités et expositions courantes (CVE) affectant les paquets installés sur un hôte.
- Définir des filtres d'inventaire en utilisant le nom et la version du paquet.

Onglet Packages (Logiciels)

Pour afficher les paquets installés sur un hôte, accédez à l'onglet Paquets sur la page Profil de la charge de travail du profil de charge de travail.

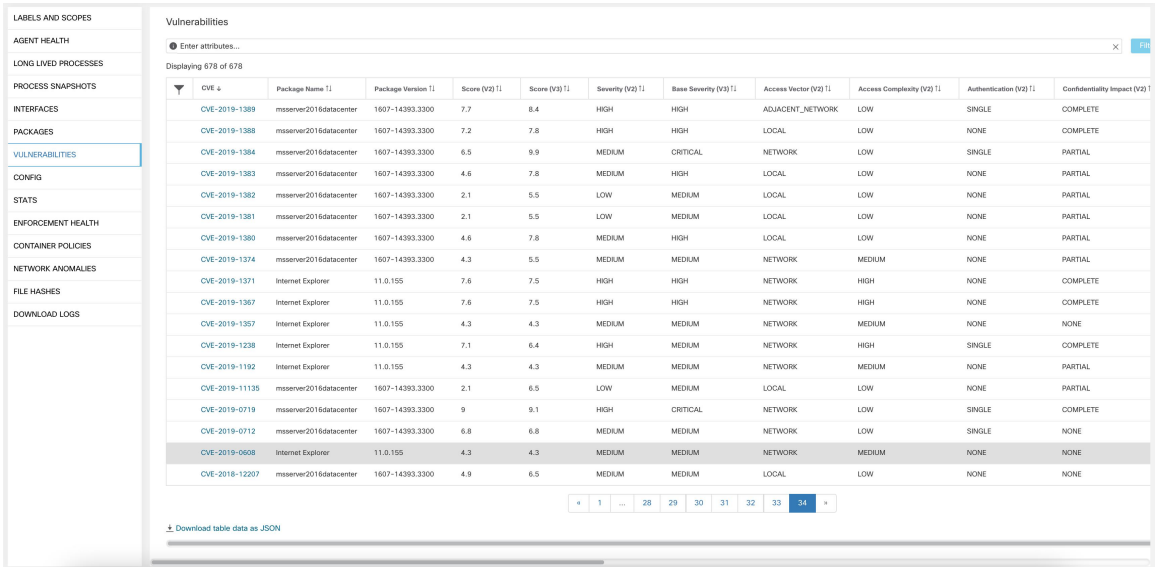
Figure 62: Paquets de profils de la charge de travail



Vulnérabilités et risques courants (CVE)

En plus d'afficher les paquets sous l'onglet Packages (paquets logiciels), nous affichons les vulnérabilités courantes qui les affectent ainsi que leur gravité. Chaque vulnérabilité contient un lien vers la base de données sur les vulnérabilités du pays (NVD) qui fournit des informations supplémentaires sur la vulnérabilité en question. En plus d'afficher l'ID CVE, nous affichons également la note d'impact (sur une échelle de 10), ce qui indique la gravité de la vulnérabilité.

Figure 63: CVE de paquets de profils de la charge de travail



Paquets Windows et CVE

La section suivante répertorie le comportement de l'agent Windows en ce qui concerne la transmission d'informations sur le paquet à Cisco Secure Workload.

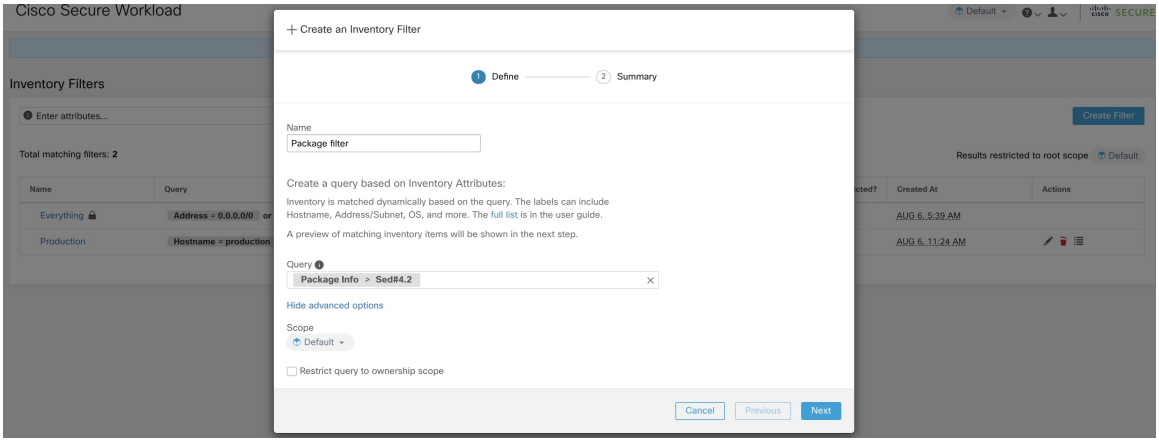
- Les applications Windows, PowerShell et IE sont présentées comme des paquets. .net Framework est également signalé en tant que paquet.
- Les autres applications Windows comme notepad.exe, cmd.exe, mstsc.exe, etc. ne sont pas signalées.
- Les rôles et les fonctionnalités configurés par un serveur Windows sont signalés en tant que paquets, mais la version peut être incorrecte. Par exemple : si le serveur DNS est configuré, la version signalée sera 0 ou 8.
- L'agent Windows signale les produits tiers installés à l'aide du programme d'installation de MSI ou du programme d'installation exe :
  - Pour les programmes d'installation MSI, les API MSI sont utilisées pour récupérer des informations sur le paquet. Par exemple, la version, le serveur de publication ou le nom du paquet.
  - Si le programme d'installation exe est utilisé pour installer le paquet, les informations sur le paquet sont extraites du registre.
  - Les champs du programme d'installation du paquet comme la version et le serveur de publication sont facultatifs. Si la version est manquante, le paquet ne sera pas signalé.
  - Si un produit est extrait du fichier compressé ou installé en tant qu'application, il ne sera pas signalé dans la liste des paquets.

Filtres d'inventaire

Il est possible de rechercher des informations relatives au paquet en définissant un filtre d'inventaire avec le nom et la version du paquet (facultatif).

La syntaxe de ce filtre est la suivante : PackageName#PackageVersion

Figure 64: Ensemble d'inventaire



Les opérations suivantes sont prises en charge :

- Equality (Égalité) : renvoie les hôtes avec les paquets correspondant à PackageName et à PackageVersion (si fourni).
- Inequality (Inégalité) : renvoie les hôtes avec les paquets correspondant à PackageName mais pas à PackageVersion (si fourni).
- Greater Than (Supérieur à) : renvoie les hôtes avec des paquets correspondant à PackageName et avec une version supérieure à PackageVersion.
- Greater Than or Equal To (Supérieur ou égal à) : renvoie des hôtes avec des paquets correspondant à PackageName et avec une version supérieure ou égale à PackageVersion.
- Less Than (inférieur à) – renvoie les hôtes avec les paquets correspondant à PackageName et avec une version antérieure à PackageVersion.
- Less Than or Equal To (Inférieur ou égal à) : renvoie les hôtes avec des paquets correspondant à PackageName et avec une version inférieure ou égale à PackageVersion.

Visibilité des données de vulnérabilité

La fonctionnalité de **visibilité des données de vulnérabilités** permet de détecter et d'afficher les vulnérabilités qui affectent les paquets et les processus sur un hôte. Les filtres d'inventaire peuvent être définis à l'aide :

des ID des CVE `des notes CVSS v2 et v3.- du vecteur d'accès et complexité d'accès CVSS v2.- du vecteur d'attaque CVSS v3, complexité de l'attaque et privilège requis.`

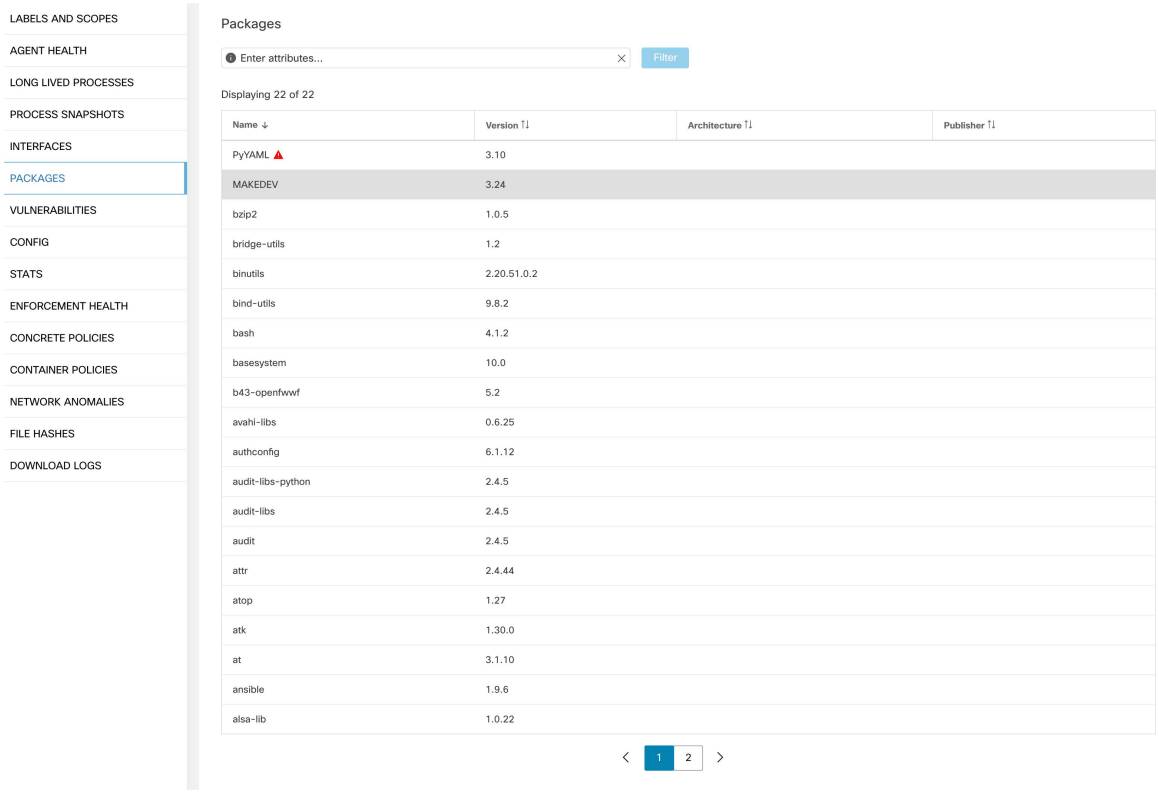
Profil de la charge de travail

Les renseignements sur les vulnérabilités qui affectent les paquets et les processus sur un système sont affichés sur la page Profil de la charge de travail (Profil de charge de travail).

Onglet Packages (Logiciels)

L'onglet des paquets répertorie les paquets installés sur un hôte et les vulnérabilités qui les affectent.

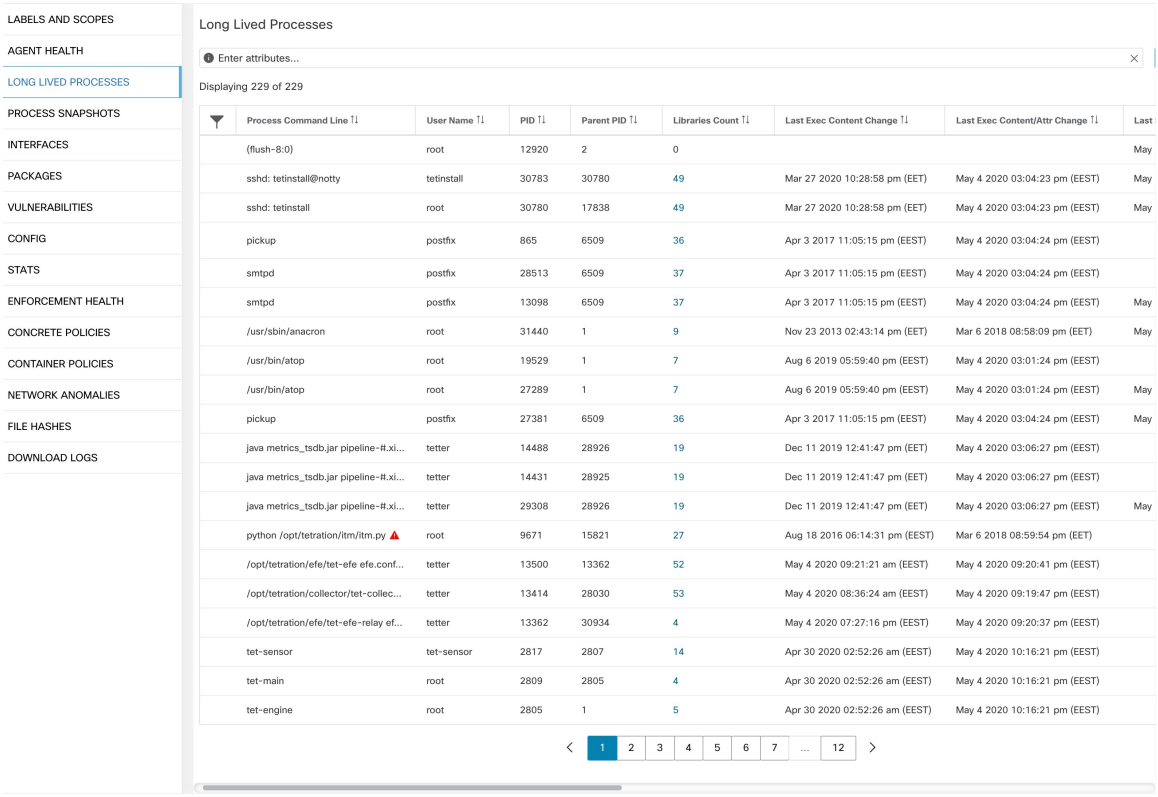
Figure 65: Paquets de profils de la charge de travail



Onglet Liste de processus

Les processus de longue durée sont affichés sous l'onglet de liste des processus.

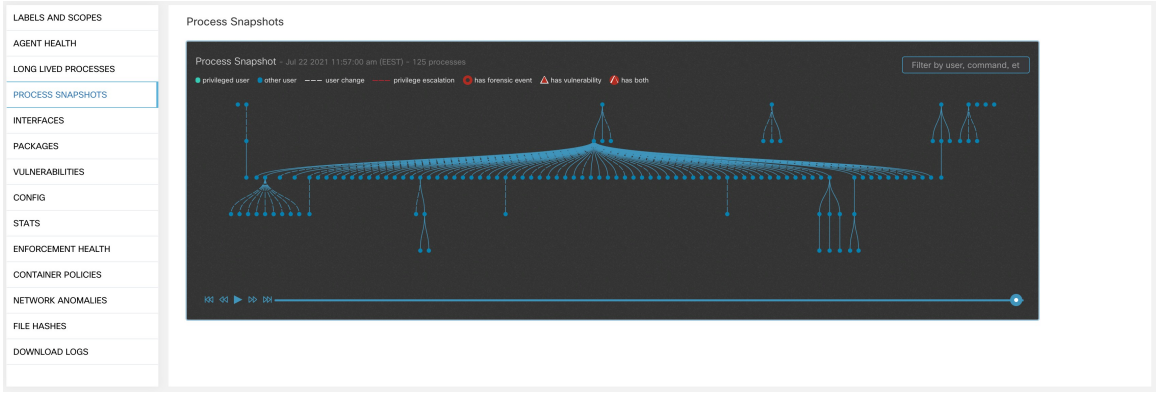
Figure 66: Liste des processus de profil de charge de travail



Onglet Process Snapshot (Instantané du processus)

Des informations sur les vulnérabilités sont affichées pour tous les processus de l'arborescence des processus sous l'onglet d'instantanés de processus.

Figure 67: Onglet d'instantané du processus de profil de charge de travail



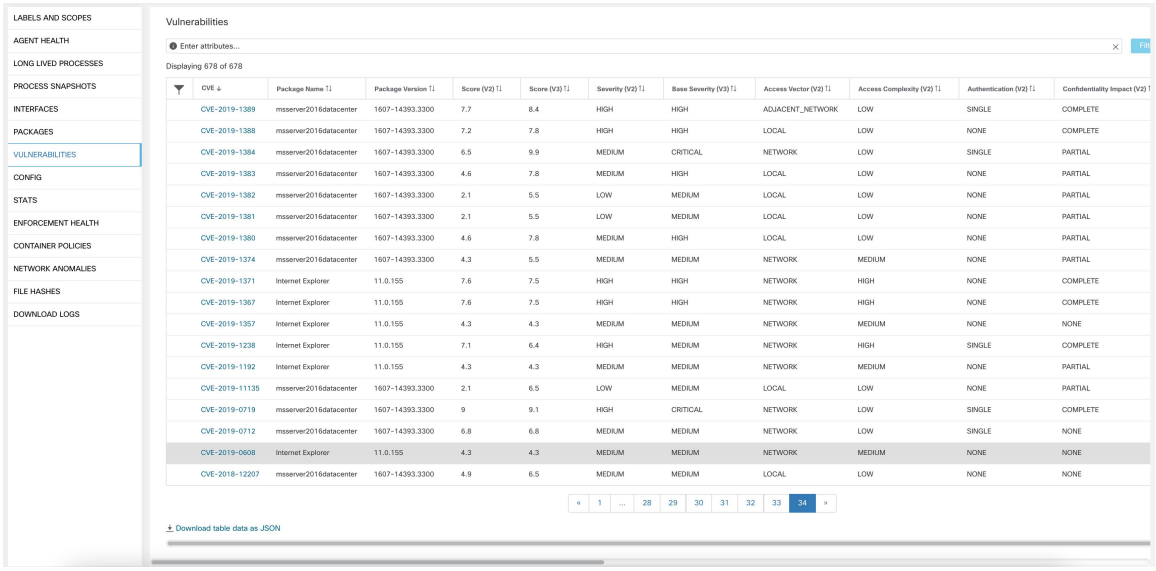
Onglet Vulnerabilities (Vulnérabilités)

L'onglet Vulnérabilités affiche la liste des vulnérabilités observées dans la charge de travail.

Pour chaque CVE, en plus des mesures d'impact de base, des informations sur les exploits basées sur nos informations sur les menaces sont affichées :

- Nombre d'exploits : nombre de fois où la CVE a été constatée exploitée de manière incontrôlée au cours de l'année écoulée
- Dernier exploit : la dernière fois que l'exploitation de la CVE de manière incontrôlée a été constatée par nos services de renseignement sur les menaces.

Figure 68: Onglet Vulnérabilités du profil de charge de travail



Filtres d'inventaire

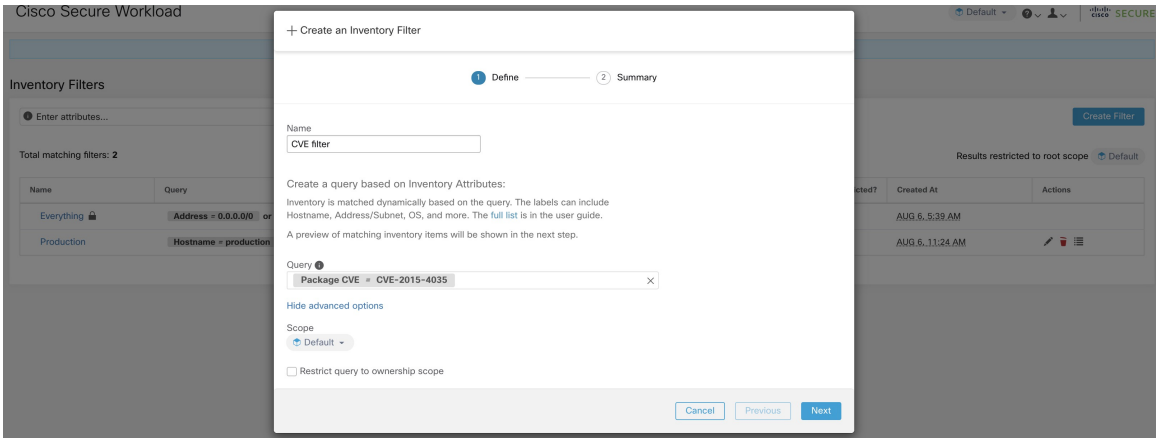
Les types de filtres d'inventaire suivants peuvent être définis pour identifier les hôtes comportant des paquets vulnérables :

Filtre basé sur l'ID CVE

Ce filtre permet de rechercher les hôtes concernés par un CVE spécifique ou n'importe quel CVE.

Pour rechercher un hôte affecté par un CVE spécifique, fournissez l'ID CVE au format : CVE-XXXX-XXXX

Figure 69: CVE de Filtre d'inventaire



Les opérations suivantes sont prises en charge :

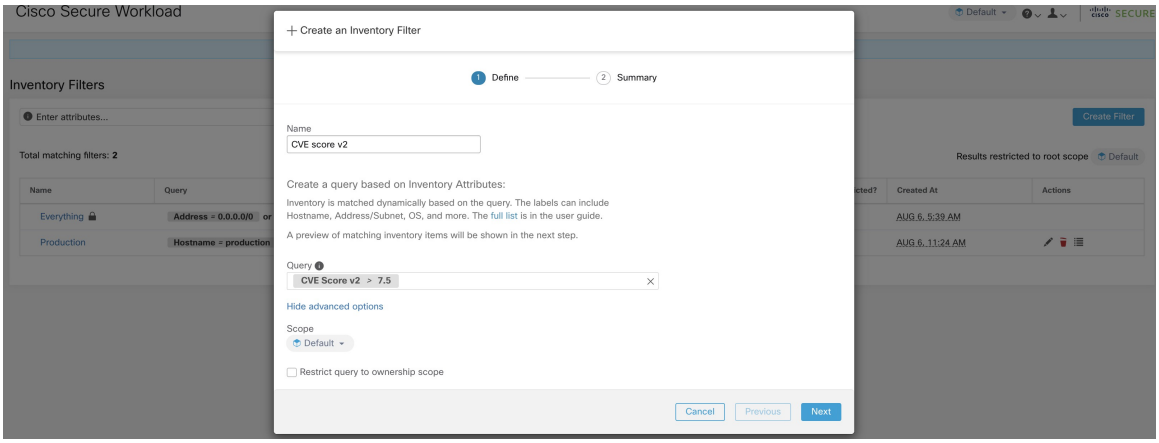
- Equality (Égalité) : renvoie les hôtes avec les paquets affectés par un ID CVE.
- Inequality (Inégalité) : renvoie les hôtes avec des paquets non affectés par un ID CVE.
- Contient (contains) renvoie les hôtes avec des paquets affectés par un CVE dans la chaîne d'entrée (la saisie de « cve » renverra les hôtes affectés par un CVE).
- Doesn't contain (Ne contient pas) : renvoie les hôtes avec des paquets non affectés par un CVE présent dans la chaîne d'entrée (la saisie de « cve » renverra les hôtes non affectés par un CVE).

Filtre basé sur la note d'impact CVSS (Common Vulnerabilities Scoring System, Système commun de notation des vulnérabilités)

Ce filtre permet de rechercher des hôtes qui ont un CVE avec le score d'impact CVSSv2 ou CVSSv3 spécifiée. Pour rechercher des hôtes qui ont des CVE avec une note d'impact (v2 ou v3), l'utilisateur peut fournir la note en format numérique.

Pour rechercher des hôtes qui ont un score d'impact CVE avec CVSSv2 supérieur à 7,5.

Figure 70: Filtre d'inventaire CVSS



Les opérations suivantes sont prises en charge :

- Égalité : renvoie les hôtes qui ont un CVE avec des notes d'impact CVSSv2 ou CVSSv3 spécifiées.
- Inégalité : renvoie des hôtes qui n'ont pas de CVE avec des notes d'impact CVSSv2 ou CVSSv3 spécifiées.
- Supérieur à : renvoie les hôtes dont les notes d'impact CVE avec CVSSv2 ou CVSSv3 sont supérieures aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.
- Supérieur ou égal à : renvoie les hôtes dont les notes d'impact CVE avec CVSSv2 ou CVSSv3 sont supérieures ou égales aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.
- Inférieur à : renvoie les hôtes dont les notes d'impact CVE avec CVSSv2 ou CVSSv3 sont inférieures aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.
- Inférieur ou égal à : renvoie les hôtes dont les scores d'impact CVE avec CVSSv2 ou CVSSv3 sont inférieures ou égales aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.

Filtres basés sur CVSSv2

Des filtres d'inventaire peuvent être créés en utilisant les vecteurs d'accès et les complexités d'accès pour identifier les hôtes vulnérables. Ces filtres prennent en charge les types d'opérations suivants :

- Equality (Égalité) : renvoie des hôtes avec des paquets affectés par des vulnérabilités correspondant au filtre.
- Inequality (Inégalité) : renvoie des hôtes avec des paquets non affectés par des vulnérabilités correspondant au filtre.

Vecteur d'accès

Le vecteur d'accès reflète la façon dont la vulnérabilité est exploitée. Plus l'agresseur peut s'éloigner du système vulnérable, plus la note de base est élevée. Le tableau ci-dessous répertorie les différents vecteurs d'accès avec leurs exigences d'accès :

Valeur	Type d'accès
LOCAL	Physique ou local (shell).
RÉSEAU_ADJACENT	Diffusion ou collision.
RÉSEAU	Exploitable à distance.

Complexité de l'accès

Cette mesure mesure la complexité de l'exploitation d'une vulnérabilité une fois que l'agresseur est en mesure d'accéder au système cible. La note de base est inversement proportionnelle à la complexité de l'accès. Les différents types de complexité d'accès sont les suivants :

Valeur	Description
ÉLEVÉE	Il existe des conditions d'accès spécialisées.
MOYENNE	Les conditions d'accès sont quelque peu spécialisées.

Valeur	Description
FAIBLE	Il n'existe pas de conditions d'accès spécifiques.

Filtres basés sur CVSSv3

Les vecteurs d'attaque, la complexité des attaques et les privilèges requis pour influencer la note CVSSv3 et qui peuvent être utilisés dans les filtres d'inventaire. Ces filtres prennent en charge les opérations suivantes :

- Equality (Égalité) : renvoie des hôtes avec des paquets affectés par des vulnérabilités correspondant au filtre.
- Inequality (Inégalité) : renvoie des hôtes avec des paquets non affectés par des vulnérabilités correspondant au filtre.

vecteur d'attaque

Cette mesure reflète le contexte dans lequel l'exploitation des vulnérabilités est possible. Plus un attaquant peut être éloigné du composant vulnérable, plus la note de base est élevée. Le tableau ci-dessous répertorie les différents vecteurs d'attaque avec leurs exigences d'accès :

Valeur	Type d'accès
LOCAL	Local (clavier, console) ou distant (SSH).
PHYSIQUE	Un accès physique est nécessaire.
RÉSEAU_ADJACENT	Diffusion ou collision.
RÉSEAU	Exploitable à distance.

Complexité de l'attaque

Cette mesure décrit les conditions qui doivent être réunies pour exploiter la vulnérabilité. La note de base est la plus élevée pour les attaques les moins complexes. Les différents types de complexité d'accès sont les suivants :

Valeur	Description
ÉLEVÉE	Des efforts importants ont été nécessaires pour la configuration et l'exécution de l'attaque.
FAIBLE	Il n'existe pas de conditions d'accès spécifiques.

Privilèges requis

Cette mesure décrit le niveau de privilèges qu'un attaquant doit posséder avant d'exploiter avec succès la vulnérabilité. La note de base est la plus élevée lorsque des privilèges ne sont pas nécessaires pour mener une attaque. Les différentes valeurs de privilège nécessaires sont les suivantes :

Valeur	Privilèges requis
ÉLEVÉE	Privilèges fournissant un contrôle important sur le composant vulnérable.
FAIBLE	Des privilèges faible qui accordent l'accès à des ressources non sensibles.
AUCUN	Aucun privilège n'est nécessaire pour effectuer une attaque.

Profil de service

Cisco Secure Workload offre une visibilité sur tous les services Kubernetes et autres équilibreurs de charge intégrés par un orchestrateur externe. La page de profil de service affiche les détails d'un service donné.

Note La page du profil de service est accessible à partir de différents endroits. L'une des façons d'afficher un profil de service consiste à rechercher un service comme décrit dans la section de recherche

Dans les résultats de la recherche, cliquez sur le nom d'un service sous l'onglet Services pour accéder à son profil. Les informations suivantes sont disponibles pour le service :

En-tête

L'en-tête comprend :

- **Nom de l'orchestrateur :** nom de l'orchestrateur externe qui a signalé ce service.
- **Type d'orchestrateur :** type de l'orchestrateur externe.
- **Espace de nom :** espace de nom du service.
- **Type de service :** type de service. Les valeurs possibles comprennent ClusterIP, Node, Port et LoadBalancer.

Adresses IP et ports

Ce tableau répertorie toutes les combinaisons possibles d'adresses IP et de ports grâce auxquelles ce service est accessible. Pour les services de type NodePort, ce tableau affiche les associations ClusterIP:Port et NodeIp:NodePort.

Étiquettes d'utilisateur

La liste des étiquettes téléversées par les utilisateurs et générées par le système par l'orchestrateur pour ce service.

Portées

Liste des portées auxquelles l'ensemble appartient.

Profil de Pod

Cisco Secure Workload offre une visibilité de tous les pods Kubernetes acquis par un orchestrateur externe Kubernetes. La page de profil de pod affiche les détails d'un pod donné.

Note La page de profil du pod est liée à plusieurs emplacements. L'une des façons d'afficher un profil de pod consiste à rechercher un pod comme décrit dans la section de recherche

Dans les résultats de la recherche, cliquez sur le nom d'un pod sous l'onglet Pods pour accéder à son profil. Les informations suivantes sont disponibles pour le pod :

En-tête

L'en-tête comprend :

- **Orchestrator Name :** nom de l'orchestrateur externe qui a signalé ce pod.
- **Type d'orchestrateur :** type de l'orchestrateur externe.
- **Espace de nom :** espace de nom du pod.
- **IP Address : adresse** IP du pod.

Étiquettes d'utilisateur

La liste des étiquettes téléversées par les utilisateurs et générées par le système par l'orchestrateur pour ce pod.

Portées

Liste des portées à laquelle le service appartient.

Container Vulnerability Scanning

It is recommended to regularly scan Kubernetes pods for vulnerabilities to maintain the health and identify potential security weaknesses.

Prerequisites

- Ensure that a Kubernetes cluster is on board.
- Ensure that the CSW Kubernetes daemonset agent is installed as part of the Kubernetes cluster.

Procedure

Étape 1 Navigate to **Manage** > **Workloads** > **Kubernetes**.

Note All onboarded clusters are displayed under **Clusters** along with the associated inventory, such as services and pods.

Étape 2 Click **Pod Vulnerability Scanning**.

Étape 3 Enable the toggle under **Actions** to start the scan. By default, the toggle is disabled.

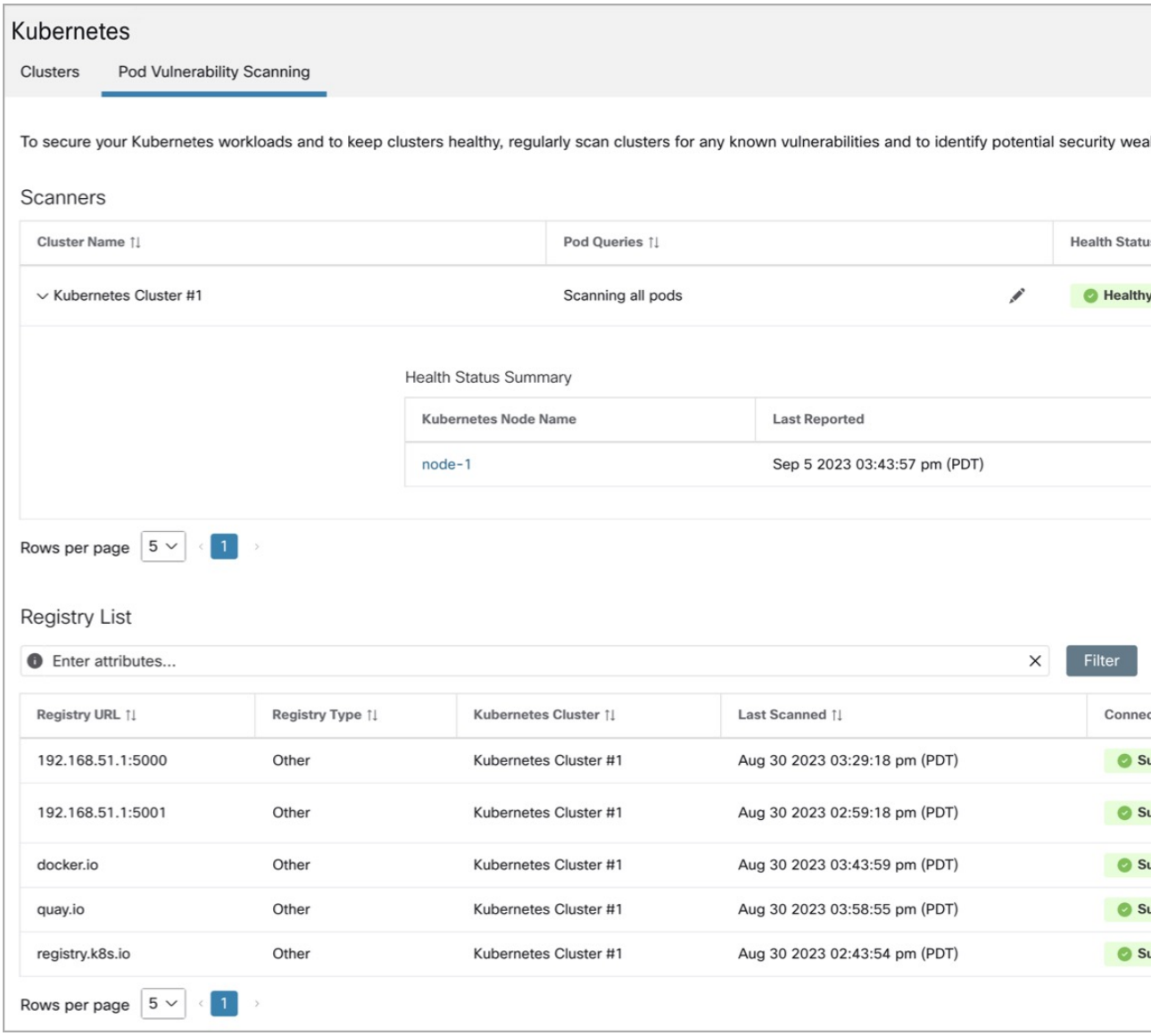
Étape 4 Click the edit icon to modify the query and select a subset of pods running on the cluster.

Note
- By default, a pod query is populated to scan all pod inventories running in the cluster. However, you can edit pod queries to select the pods to scan.
- Currently, scanning of Windows container images is not supported.

Étape 5 Expand a cluster to view the **Health Status Summary**.

- Clicking on a Kubernetes Node Name navigates you to Workload Profile.
- Enabling the toggle automatically downloads addititional information to the host so that the scanner can execute.

Figure 71: Pod Vulnerability Scanning



Étape 6 Verify the connection status and enter credentials, if required. All registries that are detected are displayed in **Registry List**.

Note Credentials may vary based on the registry enter.

Registry Type	Credentials
Azure	Tenant ID, Client ID, Secret Key
AWS	Access Key, Secret Key
GCP	Service account key in JSON format
Other	Username, Password

Troubleshooting

For the connection to be successful, ensure that the following conditions are met:

a. The scanner pod is able to connect to the registry.

b. The required network policies are in place.

c. Credentials are entered, if required.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.