Gérer le cycle de vie des politiques dans Cisco Secure Workload

Principes de base de la politique de segmentation

Le but des politiques de segmentation et de microsegmentation est de n'autoriser que le trafic dont votre entreprise a besoin pour ses activités et de bloquer tout le reste. L'objectif est de réduire la surface d'attaque de votre réseau sans perturber les tâches opérationnelles.

Les politiques de segmentation de Cisco Secure Workload autorisent ou bloquent le trafic en fonction de sa source, de sa destination, de son port, de son protocole et de quelques autres attributs qui sont généralement propres à la plateforme.

Vous pouvez créer des politiques manuellement et utiliser la puissante fonctionnalité de découverte automatique des politiques de Cisco Secure Workload pour générer d'autres politiques en fonction du trafic réseau existant.

Vous pouvez passer en revue, affiner et analyser vos politiques, puis les appliquer lorsque vous êtes sûr qu'elles n'autorisent que le trafic dont votre entreprise a besoin.

Important La microsegmentation crée essentiellement un pare-feu autour de chaque charge de travail.

Par conséquent, pour que le trafic passe entre chaque paire client-fournisseur, les deux extrémités de la conversation doivent autoriser la conversation : le client et le fournisseur doivent chacun avoir une politique autorisant le trafic.

Remarque Les termes *règle de pare-feu*, *périphérie* et *périphérie de grappe* sont parfois utilisés pour signifier « politique ».

Utiliser des espaces de travail pour gérer les politiques

Les espaces de travail (anciennement « espaces de travail d'applications » ou « applications ») sont les endroits où vous travaillez et gérez les politiques.

Vous pouvez effectuer toutes les activités liées aux politiques pour une portée particulière, telles que la création, l'analyse et l'application des politiques, dans l'espace de travail ou les espaces de travail associés à cette portée.

Chaque espace de travail constitue un environnement indépendant, permettant des expérimentations sans effet sur les autres espaces de travail.

Contrôle de l'accès des utilisateurs aux espaces de travail

Les espaces de travail sont destinés à être utilisés par plusieurs utilisateurs de la même équipe en tant que documents partagés.

Pour contrôler l'accès à un espace de travail, attribuez des rôles d'utilisateur pour la portée associée à l'espace de travail. Pour en savoir plus, consultez la section Rôles.

Utilisation des politiques : Accès à la page des espaces de travail

- **Pour utiliser les politiques, afficher les espaces de travail d'application existants ou en créer de nouveaux :**

  Choisissez **Defend (Défendre)** > **Segmentation (Segmentation)** dans la barre de navigation à gauche de la fenêtre.

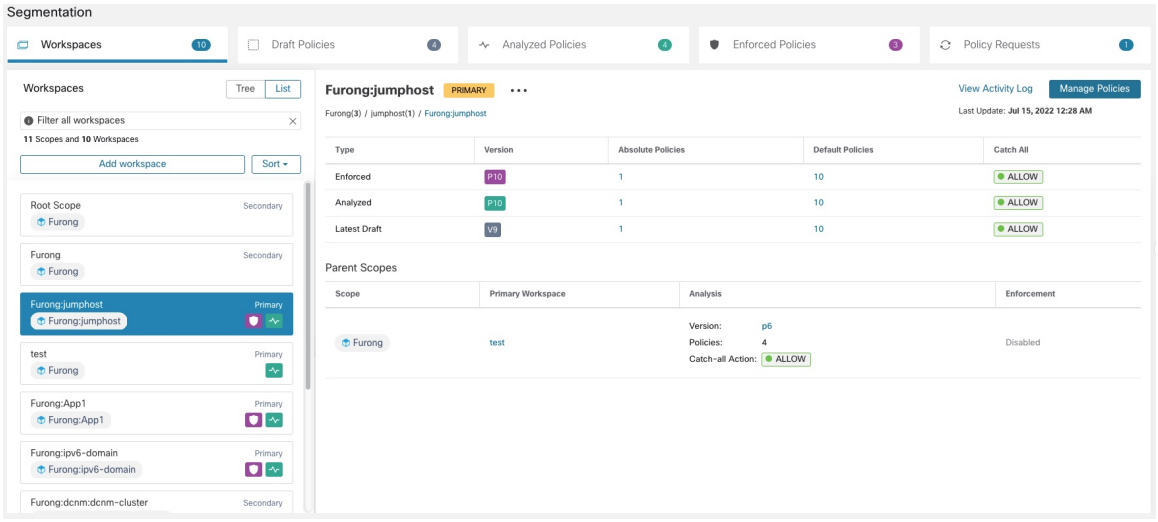
- **Pour afficher un espace de travail en particulier :**

  Dans la liste des portées sur le côté gauche de la page Workspaces (Espaces de travail), accédez à la portée associée à l'espace de travail, puis cliquez sur ce dernier. L'espace de travail actif actuel est mis en surbrillance dans la liste.

- **Si vous êtes à la recherche d'un espace de travail et que vous souhaitez revenir à la liste des espaces de travail :**

  Cliquez sur le lien **Workspaces** (Espaces de travail) près du côté gauche de la page que vous examinez.

Figure 1: Page Workspace Management (Gestion de l'espace de travail)



Créer un espace de travail

Pour créer des politiques pour une portée, créez d'abord un espace de travail pour cette dernière.

Pour créer un espace de travail :

1. Dans le menu de navigation sur le côté gauche de la fenêtre, choisissez **Defend (Défendre)** > **Segmentation (Segmentation)**.
2. Dans la liste des portées située à gauche de la page, recherchez la portée pour laquelle vous souhaitez créer des politiques ou faites défiler l'écran jusqu'à cette portée.
3. Passez le curseur sur la portée jusqu'à ce qu'un signe + bleu s'affiche, puis cliquez dessus.
4. Remplissez le formulaire et cliquez sur **Create** (Créer) lorsque vous avez terminé.

S'il existe un espace de travail pour la portée, tout espace de travail supplémentaire est créé en tant qu'espace de travail secondaire.

Espaces de travail principal et secondaire

Pour chaque portée, vous pouvez créer un espace de travail principal et plusieurs espaces de travail secondaires.

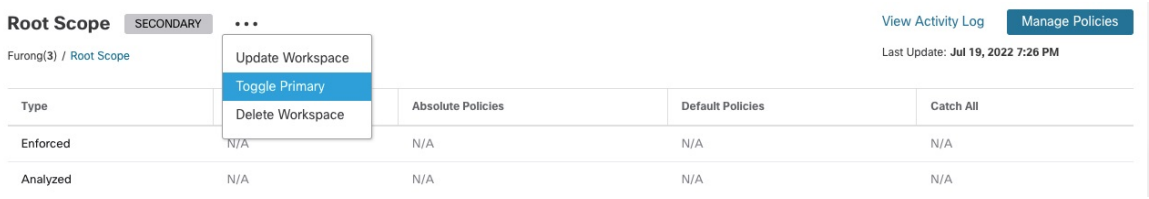
Seul un espace de travail principal peut être mis en application. Parmi les autres fonctionnalités disponibles uniquement pour les espaces de travail principaux, citons la possibilité de gérer des politiques dans lesquelles le consommateur et le fournisseur résident dans des portées différentes, l'analyse en direct des politiques, les rapports de conformité et la définition collaborative des politiques de sécurité.

Utilisez des espaces de travail secondaires pour essayer les politiques lorsque vous souhaitez conserver les politiques existantes dans l'espace de travail principal.

Pour faire d'un espace de travail un espace de travail principal ou secondaire :

Vous pouvez faire basculer un espace de travail de principal à secondaire et inversement à tout moment en cliquant sur l'icône de menu à côté du nom de l'espace de travail en haut de la page et en sélectionnant **Toggle Primary**(basculer l'espace de travail principal).

Figure 2: Commutation d'un espace de travail entre principal et secondaire



Renommer un espace de travail

Pour renommer un espace de travail :

Cliquez sur le ••• côté du type d'espace de travail (principal ou secondaire) affiché près du haut de la page et choisissez **Update Workspace** (Mettre à jour l'espace de travail).

Afficher les charges de travail d'une portée

Dans n'importe quel espace de travail, cliquez sur l'onglet **Matching Inventories** (Inventaires correspondants).

Rechercher dans un espace de travail

Pour rechercher dans un espace de travail des charges de travail, des grappes ou des politiques :

1. Sélectionnez **Defend (Défendre)** > **Segmentation (Segmentation)**.
2. Dans la liste des portées sur la gauche, cliquez sur la portée et l'espace de travail qui vous intéressent.
3. Cliquez sur **Manage Policies** (Gestion des politiques).
4. Cliquez sur la loupe.
5. Saisissez les critères de recherche

Critères de recherche

Plusieurs critères sont traités comme ET logique.

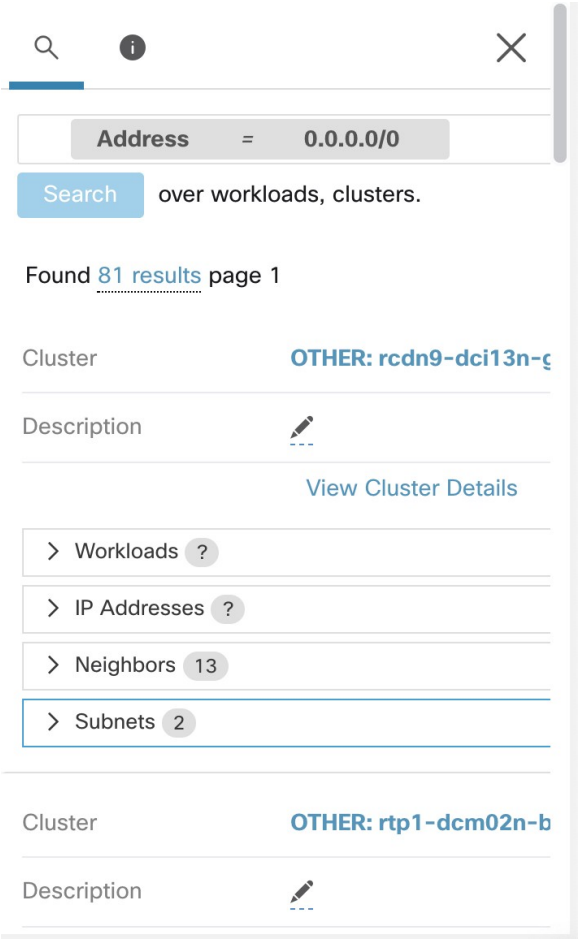
Pour les adresses IP et les valeurs numériques :

- Indiquez le OU logique à l'aide d'une virgule : « port: 80,443 ».
- Les requêtes de plage sont également prises en charge pour les valeurs numériques : « port : 3000-3999 ».

Filtres	Description
Nom	Saisissez un nom de grappe ou de charge de travail. Effectue une recherche de sous-chaîne sensible à la casse.

Filtres	Description
Description	Recherche les descriptions des grappes.
Approuvé	Correspond aux groupes approuvés en utilisant les valeurs « vrai » ou « faux ».
Address (adresse)	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux charges de travail ou aux grappes qui recoupent ce sous-réseau.
Super-réseau	Saisissez un sous-réseau en notation CIDR (par exemple, 10.11.12.0/24) pour correspondre aux grappes dont les charges de travail sont entièrement contenues dans ce sous-réseau.
Processus	Recherche les processus de charge de travail à l'aide de la recherche de sous-chaîne sensible à la casse.
UID de processus	Recherche les noms d'utilisateurs des processus de charge de travail.
Port	Recherche à la fois le port du fournisseur de charge de travail et le port de la politique.
Protocol	Recherche à la fois le protocole du fournisseur de charge de travail et le protocole de politique.
Consumer Name	Correspond au nom de la grappe de consommateurs d'une politique. Effectue une correspondance de sous-chaîne sensible à la casse.
Provider Name	Correspond au nom de la grappe de fournisseurs d'une politique. Effectue une correspondance de sous-chaîne sensible à la casse.
Adresse du client	Correspond aux politiques dont l'adresse du client recouvre l'adresse IP ou le sous-réseau fournis.
Adresse du fournisseur	Correspond aux politiques dont l'adresse de fournisseur recouvre l'adresse IP ou le sous-réseau fournis.

Exemple de recherche

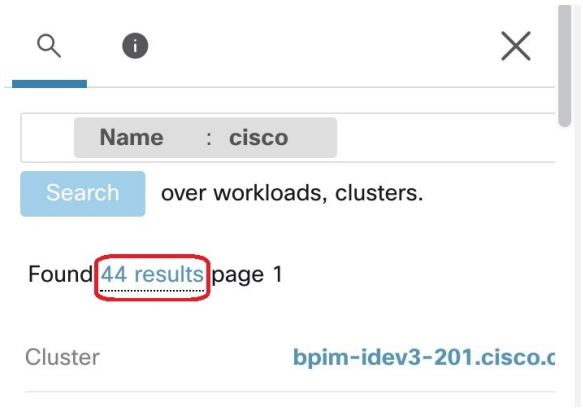


Filtrage des résultats de la recherche pour un type spécifique

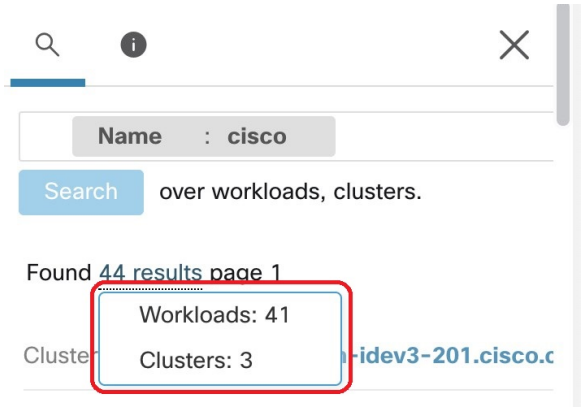
Les résultats de la recherche peuvent inclure plusieurs types d'objets, par exemple des charges de travail et des grappes.

Pour filtrer les résultats de la recherche pour un type spécifique :

1. Cliquez sur le total du résultat :



2. Sélectionnez le type dans la liste déroulante :



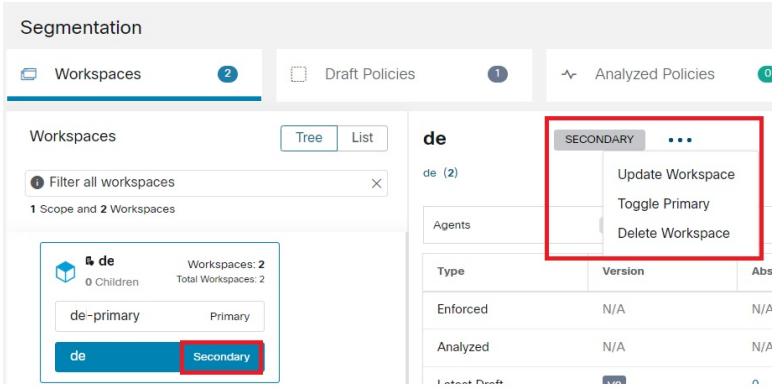
3. Un filtre de type sera ajouté et la recherche sera réexécutée.

Suppression d'espaces de travail

Seuls les espaces de travail secondaires (non principaux) peuvent être supprimés. Pour faire passer un espace de travail au niveau secondaire, consultez Espaces de travail principal et secondaire, on page 3.

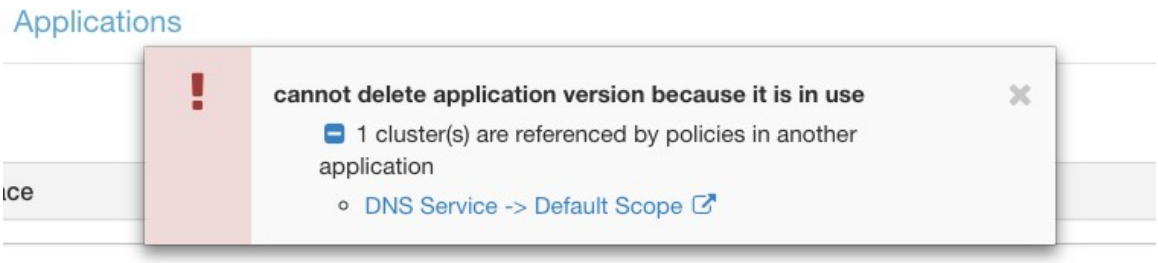
Pour supprimer un espace de travail :

1. Choisissez **Defend (défense) > Segmentation (segmentation).**
2. Dans la liste des portées sur le côté gauche de la page, accédez à la portée contenant l'espace de travail à supprimer et cliquez dessus.
3. Cliquez sur l'espace de travail à supprimer.
4. Cliquez sur le ••• à côté de **Secondary (Secondaire)** et choisissez **Delete Workspace** (Supprimer l'espace de travail).



Si une charge de travail ou une grappe dans un espace de travail est référencée par une politique dans un autre espace de travail à la suite d'un service fourni, l'espace de travail dépendant ne peut pas être supprimé et une liste des dépendances sera renvoyée. Ces informations peuvent être utilisées pour corriger la dépendance.

Figure 3: Liste des éléments empêchant la suppression de l'espace de travail



Dans de rares cas, il peut y avoir une dépendance croisée où l'espace de travail A dépend d'une grappe dans l'espace de travail B et un espace de travail B dépend d'une grappe dans l'espace de travail A. Dans ce cas, les politiques individuelles ou les versions de politiques publiées (p*) doivent être supprimées. L'erreur « delete restrictions » (restrictions de suppression) fournit des liens vers toutes les politiques permettant d'y parvenir.

Pour supprimer les versions p*, consultez Afficher, comparer et gérer les versions des politiques analysées, on page 128 ou Afficher, comparer et gérer les versions des politiques appliquées, on page 143.

À propos des politiques

Attributs de la politique

Table 1: Propriétés de la politique

Propriétés de la politique de sécurité	Description
Portée pour laquelle la politique est définie	Une politique a généralement une incidence uniquement sur les charges de travail qui sont membres de la portée associée à l'espace de travail dans lequel la politique est définie. (Cependant, consultez également les rubriques sous Aborder les complexités de la politique, on page 87). Pour en savoir plus, consultez Exemple de politique, on page 11.
Consommateur	Le client d'un service ou l'initiateur d'une connexion. N'importe quel filtre de portée, de grappe ou d'inventaire peut être utilisé en tant que consommateur dans une politique. Consultez les informations importantes dans À propos du consommateur et du fournisseur dans les politiques, on page 11.
Fournisseur	Le serveur ou le destinataire d'une connexion. N'importe quel filtre de portée, de grappe ou d'inventaire peut être utilisé comme fournisseur dans une politique. Consultez les informations importantes dans À propos du consommateur et du fournisseur dans les politiques, on page 11.
Protocoles et ports	Le port (d'écoute) du serveur et le protocole IP du service mis à disposition par le fournisseur qui doivent être autorisés ou bloqués.
Action	ALLOW ou DENY : s'il faut autoriser ou abandonner le trafic du consommateur au fournisseur sur le port de service/protocole donné.
Rang et priorité	Pour en savoir plus sur le rang et la priorité des politiques dans un espace de travail, consultez Rang de politique : Absolue, Par défaut et Collectrice, on page 9.

Rang de politique : Absolue, Par défaut et Collectrice

Le rang de la politique détermine si une politique est remplacée par une politique plus spécifique inférieure dans la liste de priorité (ou dans une portée inférieure de l'arborescence des portées). La politique de priorité la plus basse de chaque portée est toujours la règle Collectrice.

Rang de la politique	Description
Absolue	Les politiques absolues prennent effet même si elles contredisent des politiques spécifiques à l'application situées à un niveau inférieur dans la liste des politiques (et donc moins prioritaires) ou dans des portées situées à un niveau inférieur dans l'arborescence des portées. En général, utilisez les politiques absolues pour appliquer les bonnes pratiques, protéger différentes zones ou charges de travail spécifiques à la mise en quarantaine. Par exemple, utilisez des politiques absolues pour contrôler le trafic vers les serveurs DNS ou NTP, ou pour répondre aux exigences réglementaires. Les politiques absolues sont répertoriées à un niveau supérieur à celui des politiques par défaut dans la liste de priorités des politiques.
Par défaut	Les politiques par défaut peuvent être remplacées par des politiques inférieures dans la liste des politiques ou dans des portées inférieures dans l'arborescence des portées. En général, les politiques précises sont des politiques par défaut. Les politiques par défaut sont répertoriées à un niveau inférieur à celui des politiques absolues dans la liste de priorités des politiques.
Collectrice	Chaque espace de travail est doté d'une politique collectrice fourre-tout qui gère le trafic dans chaque direction qui ne correspond à aucune politique explicitement spécifiée dans l'espace de travail. L'action Collectrice peut être Allow (Autoriser) ou Deny (refuser). En général, définissez la politique Catch-All (Collectrice) comme suit : • **Allow** (Autoriser) le trafic dans les portées supérieures de l'arborescence, de sorte que les politiques des portées inférieures de l'arborescence puissent évaluer le trafic. • **Deny** (Refuser) le trafic au niveau de l'extrémité la plus précise, au bas de l'arborescence de la portée. Cela permet aux politiques de toutes les portées de l'arborescence de mettre en correspondance le trafic, tout en bloquant le trafic qui ne correspond à aucune politique d'aucune portée. La règle « collectrice » est appliquée à toutes les interfaces de chaque charge de travail dans l'espace de travail.

Héritage des politiques et arborescence de portée

Vos charges de travail étant organisées en une arborescence hiérarchique, vous pouvez créer des politiques générales une fois dans une portée située au sommet de l'arborescence ou à proximité, et les politiques peuvent éventuellement s'appliquer à toutes les charges de travail dans toutes les portées situées en dessous de cette portée dans l'arborescence.

Vous spécifiez si les politiques générales peuvent être remplacées par des politiques plus spécifiques, plus bas dans l'arborescence.

Consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 9.

À propos du consommateur et du fournisseur dans les politiques

Le consommateur et le fournisseur précisés dans une politique servent aux fins suivantes :

- Ils précisent les charges de travail ou les agents Cisco Secure Workload qui reçoivent les règles de politique ou de pare-feu.
- Ils précisent l'ensemble d'adresses IP auxquelles les règles de pare-feu installées sur les charges de travail s'appliquent.

Si un hôte possède plusieurs interfaces (adresses IP), les politiques s’appliquent à toutes les interfaces.

Important Les éléments ci-dessus représentent le comportement par défaut de la programmation des règles de pare-feu sur les charges de travail. Si les adresses IP spécifiées dans les règles de pare-feu différentes des adresses IP des charges de travail sur lesquelles la politique est installée, vous devez séparer les deux objectifs des consommateurs et des fournisseurs dans une politique. Consultez Consommateur ou fournisseur réel, à la page 107.

Exemple de politique

L’exemple de politique suivant illustre l’importance de la portée dans laquelle une politique est définie, l’incidence de l’héritabilité des politiques et de l’utilisation de filtres d’inventaire pour créer des politiques spécifiques ou des politiques qui s’appliquent aux charges de travail dans plusieurs portées.

Considérons l’exemple suivant concernant trois portées :

- **`Applis`**

  et leurs portées enfants

  - **`Apps:HR`** et
  - **`Apps:Commerce`**

En outre, les filtres d’inventaire PRODUCTION et NON-PRODUCTION précisent respectivement les hôtes de production et les hôtes hors production. (Vous pouvez définir un filtre d’inventaire à appliquer aux hôtes dans une portée ou dans plusieurs).

Supposons que la politique suivante soit définie pour la portée **`Applications`** :

```
DENY PRODUCTION -> NON-PRODUCTION on TCP port 8000 (Absolute)
```

Étant donné qu’il s’agit d’une politique absolue définie dans l’espace de travail principal sous la portée **`Applications`**, elle affecte tous les hôtes DE PRODUCTION ET HORS DE PRODUCTION membres de la portée **`Applications`**, y compris les membres de ses portées descendantes (hôtes qui appartiennent aux environnements **`Apps:RH`** et **`Apps:Commerce`**).

Considérons maintenant le cas où exactement la même politique est définie dans l’espace de travail associé à la portée **`Apps:HR`**. Dans ce scénario, la politique ne peut affecter que les hôtes PRODUCTION ET NON-PRODUCTION membres de la portée **`Apps:HR`**. Plus précisément, cette politique fait en sorte que les règles d’entrée sur les hôtes RH NON PRODUCTION (le cas échéant) refusent les connexions sur le port TCP 8000 à partir de **n’importe quel** hôte PRODUCTION, et les règles sortantes sur les hôtes de

PRODUCTION RH (le cas échéant) abandonnent les demandes de connexion vers **tout** hôte HORS-PRODUCTION.

Créer et découvrir des politiques

Bonnes pratiques pour la création de politiques

- Pour une présentation de l'ensemble du processus de segmentation, consultez Premiers pas avec la segmentation et la microsegmentation et les sous-rubriques.
- Créez manuellement des politiques qui s'appliquent globalement à votre réseau.

  Par exemple, bloquez le trafic indésirable vers vos charges de travail provenant de l'extérieur de votre réseau ou mettez les hôtes vulnérables en quarantaine.

  - Créez des politiques manuelles dans des portées au sommet de votre arborescence ou à proximité de celui-ci.

    Par exemple, pour bloquer tout le trafic provenant de l'extérieur de votre réseau vers chaque hôte de votre réseau, placez la politique dans la portée en haut de l'arborescence.
  - Si vous souhaitez pouvoir remplacer la politique générale pour certaines charges de travail (par exemple, dans l'exemple ci-dessus, vous souhaitez bloquer l'accès général depuis l'extérieur de votre réseau, mais vous voulez que certaines charges de travail soient accessibles depuis l'extérieur de ce dernier), créez les politiques globales en tant que politiques par défaut. Créez ensuite des politiques spécifiques pour les charges de travail applicables.
  - Pensez à utiliser des modèles pour accélérer la création de politiques.
  - Consultez les sections Créer manuellement des politiques, à la page 13, Politiques à des fins précises, à la page 14 et Modèles de politiques, à la page 17.

- (Facultatif) Dans un premier temps, découvrez automatiquement les politiques d'une portée proche du sommet de votre arborescence, pour toutes les portées d'une branche de l'arborescence, afin de créer des politiques générales qui autorisent tout le trafic existant et limitent le futur trafic indésirable. Vous pouvez ensuite créer des politiques plus fines qui protègent votre réseau contre le trafic inutile ou indésirable.

  Consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 25 et Découvrir automatiquement les politiques, à la page 21 pour de plus amples renseignements.
- Lorsque vous êtes prêt à découvrir des politiques plus fines, découvrez automatiquement des politiques pour les portées situées au bas ou près du bas de l'arborescence de votre portée, en particulier dans les portées des applications individuelles.

  Consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 25 et Découvrir automatiquement les politiques, à la page 21 pour de plus amples renseignements.
- Assurez-vous d'avoir des politiques qui traitent des activités et des scénarios inhabituels ou rares, tels que le basculement, la restauration à partir d'une sauvegarde, les activités annuelles, etc.
- Après avoir identifié et autorisé le trafic nécessaire à vos applications, recherchez tout trafic qui ne devrait pas se produire et bloquez ces instances.

Examinez d'abord le trafic entrant et sortant de vos applications les plus sensibles.

Par exemple, si vous constatez du trafic depuis votre application Web destinée aux clients vers la base de données de votre application de recherche et développement top secrète, vous devez enquêter.

- Collaborez avec vos collègues pour vous assurer que les bonnes politiques sont appliquées aux bonnes charges de travail.
- Pour commencer, lorsque vous appliquez des politiques, envisagez de définir la règle collectrice sur Allow (Autoriser). Ensuite, surveillez le trafic pour voir ce qui correspond à la règle collectrice. Lorsqu'aucun trafic nécessaire ne correspond à la règle « collectrice », vous pouvez définir ce paramètre sur Deny (Refuser).

Créer manuellement des politiques

En règle générale, vous pouvez créer manuellement des politiques qui s'appliquent globalement à votre réseau.

Par exemple, vous pouvez créer manuellement des politiques pour :

- Autoriser l'accès de toutes les charges de travail internes à vos serveurs NTP, DNS, Active Directory ou à l'analyse des vulnérabilités.
- Refuser l'accès de tous les hôtes extérieurs à votre organisation aux hôtes à l'intérieur de votre réseau, sauf autorisation explicite.
- Mettre les charges de travail vulnérables en quarantaine.

Vous pouvez créer des politiques absolues qui ne peuvent pas être remplacées par des politiques appliquées de manière plus granulaire, et des politiques par défaut qui peuvent être remplacées s'il existe une politique plus spécifique.

Vous pouvez créer des politiques manuelles pour les portées proches du sommet de votre arborescence.

Avant de commencer

- (Facultatif) Utilisez l'un des modèles disponibles à partir de **Defend (Défendre) > Policy Templates** (Modèles de politique).
- (Facultatif) Si vous savez que vous possédez un ensemble de charges de travail qui reçoivent les mêmes politiques, utilisez un filtre d'inventaire pour les regrouper afin de pouvoir facilement appliquer des politiques à l'ensemble. Le filtre d'inventaire ne peut s'appliquer qu'à une seule portée ou à des charges de travail de n'importe quelle portée. Consultez Créer un filtre d'inventaire.
- Assurez-vous que les charges de travail de cette portée sont celles que vous prévoyez d'y trouver. Consultez Afficher les charges de travail d'une portée, à la page 4.

Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Dans la liste de gauche, recherchez ou accédez à la portée dans laquelle vous souhaitez créer la politique.

Étape 3 Cliquez sur la portée et l'espace de travail dans lesquels vous souhaitez créer la politique.

Si vous n'avez pas encore créé l'espace de travail pour cette portée, consultez Créer un espace de travail, à la page 3.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 5 Cliquez sur l'onglet **Policies** (Politiques) s'il n'est pas déjà sélectionné.

Étape 6 Cliquez sur **Add Policy** (ajouter une politique).

Si vous ne voyez pas de bouton Add Policy (Ajouter une politique), consultez Si le bouton Add Policy (Ajouter une politique) n'est pas disponible, à la page 14.

Étape 7 Saisir des renseignements

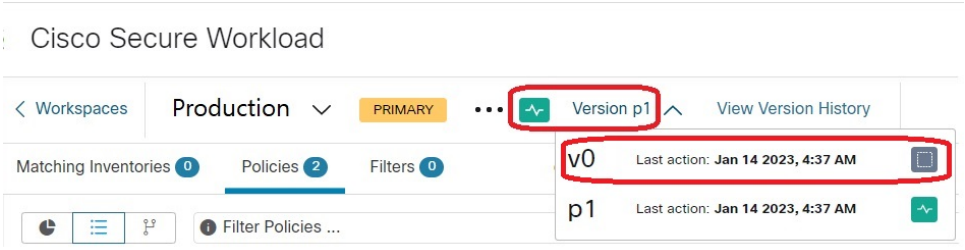
- Pour en savoir plus sur la case à cocher **Absolute** (Absolue), consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 9. En général, si vous créez des politiques pour lesquelles vous ne vous attendez pas à des exceptions, cochez cette case.
- **Priority (La priorité)** définit l'ordre de la politique dans la liste. Pour en savoir plus sur la définition de l'ordre des politiques, consultez Priorités des politiques, à la page 88 et les sous-sections. (Vous pouvez définir l'ordre des politiques ultérieurement).
- Le consommateur et le fournisseur peuvent correspondre à une portée entière ou, si vous avez créé des groupes de charges de travail à l'aide de filtres d'inventaire (ou, de manière moins optimale, des grappes dans le même espace de travail), vous pouvez les choisir.

Prochaine étape

Assurez-vous que l'action **Collectrice** est appropriée pour l'espace de travail. Consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 9.

Si le bouton Add Policy (Ajouter une politique) n'est pas disponible

Si vous essayez de créer une politique et que le bouton **Add Policy** (ajouter une politique) n'est pas disponible, cliquez sur la version affichée en haut de la page et choisissez la dernière version « v », qui est indiquée par un carré gris :



Politiques à des fins précises

Créer des politiques InfoSec pour bloquer le trafic provenant de l'extérieur de votre réseau

Utilisez cette procédure pour créer rapidement un ensemble complet de politiques pour contrôler le trafic entrant dans votre réseau en provenance de l'extérieur. L'ensemble de règles par défaut autorise uniquement

le trafic utilisant des ports et des protocoles courants et refuse tout autre trafic. Vous pouvez modifier l'ensemble de règles par défaut selon vos besoins.

Avant de commencer

Utilisez cette procédure si les critères suivants sont remplis :

- Votre arborescence de portées a une portée nommée **Internal** (Interne) juste en dessous de la portée racine.

  Les membres de cette portée comprennent, ou incluront, des sous-réseaux englobant toutes les charges de travail sur votre réseau interne.

- La portée interne n'a encore aucune politique définie.

Remarque Sinon, vous pouvez utiliser le modèle **InfoSec** disponible dans **Defend > Policy Templates** (Défendre> Modèles de politiques) pour y parvenir en quelques étapes supplémentaires.

Procédure

Étape 1 Choisissez **Defend (défense) > Segmentation (segmentation).**

Étape 2 Cliquez sur la portée **Internal** (interne), puis sur l'espace de travail principal.

Si l'espace de travail principal n'existe pas encore, cliquez sur le bouton + pour le créer.

Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 4 Cliquez sur **Add InfoSec Policies** (Ajouter des politiques InfoSec).

Étape 5 Vérifiez que toutes les politiques de la liste, y compris les protocoles et les ports, sont des politiques que vous souhaitez, puis supprimez et modifiez les politiques à votre convenance.

Étape 6 Cliquez sur **Create** (créer).

Prochaine étape

(Facultatif) Ajoutez des politiques supplémentaires à votre portée interne, telles que les politiques qui autorisent certains trafics externes vers des charges de travail spécifiques.

Placez toutes les politiques spécifiques sous des politiques plus générales dans la liste.

Créer des politiques pour traiter les menaces immédiates

Si vous devez faire face à une menace immédiate, vous pouvez ajouter manuellement une politique absolue étroitement ciblée à une portée au sommet ou à proximité de ce dernier de votre arborescence, puis appliquer l'espace de travail principal à cette portée.

Après avoir corrigé la menace, vous pouvez supprimer cette politique et renforcer l'espace de travail.

Créer une politique de mise en quarantaine des charges de travail vulnérables

Vous pouvez réaliser les actions suivantes :

- Créer des politiques à l'avance pour mettre automatiquement en quarantaine les charges de travail présentant des vulnérabilités connues ou un seuil de gravité de vulnérabilité que vous définissez.
- Créer des politiques pour mettre immédiatement en quarantaine les charges de travail pour lesquelles des vulnérabilités connues ont été détectées et que vous jugez suffisamment problématiques.

Cette rubrique décrit le processus à suivre dans les deux cas.

Avant de commencer

Examinez Afficher le tableau de bord des vulnérabilités pour voir quelles politiques sont requises.

Procédure

Étape 1 Créez un filtre d'inventaire qui définit les vulnérabilités ou le seuil de gravité de la vulnérabilité que vous souhaitez mettre en quarantaine :

a) Dans la barre de navigation à gauche de la fenêtre, choisissez **Organize > Inventory Filters** (Organiser > Filtres d'inventaires).
b) Cliquez sur **Create Inventory Filter (créer un filtre d'inventaire).**
c) Cliquez sur le bouton **(i)** à côté de **Query** (requête) et saisissez **`CVE`** pour afficher les options de filtre appropriées.
d) Saisissez les critères de filtre qui déterminent les charges de travail que vous souhaitez mettre en quarantaine.
e) Assurez-vous que l'option **Restrict query to ownership scope** (Restreindre la requête à la portée de la propriété) n'est PAS cochée.

Étape 2 Créez une politique pour mettre en quarantaine les charges de travail touchées :

Pour plus d'informations générales sur les instructions, consultez Créer manuellement des politiques, à la page 13.

les recommandations :

- Créez la politique dans votre portée **interne** ou autre près du sommet de votre arborescence.
- La politique doit être une politique absolue, sauf si vous souhaitez autoriser des exceptions. Assurez-vous de créer des politiques pour traiter d'éventuelles exceptions.
- Créez des politiques distinctes pour le consommateur et le fournisseur.
- Définissez la priorité de chaque politique sur un nombre faible afin qu'elle soit atteinte avant les autres politiques de la liste.
- Définissez l'action sur **Deny** (Refuser).

Étape 3 Examiner, analyser et appliquer la politique ou les politiques.

Prochaine étape

Créez une alerte pour être averti lorsque le trafic atteint cette politique afin de pouvoir résoudre le problème et restaurer le trafic vers la charge de travail vulnérable. Consultez Configurer les alertes.

Modèles de politiques

Les modèles de politiques sont utilisés pour appliquer des ensembles de politiques similaires à plusieurs espaces de travail.

Cisco Secure Workload comprend des modèles prédéfinis, et vous pouvez créer vos propres modèles.

Les modèles de politique nécessitent la capacité de propriétaire de la portée sur la portée racine.

Modèles de politiques définis par le système

Pour afficher les modèles de politique disponibles, accédez à **Defend > Policy Templates** (Défendre > Modèles de politique).

Pour utiliser un modèle de politique, consultez Application d'un modèle, à la page 20.

Pour modifier un modèle défini par le système, téléchargez le fichier JSON, modifiez-le, puis téléversez-le.

Créer des modèles de politiques personnalisés

Schéma JSON pour les modèles de politique

Le schéma JSON du modèle de politique est conçu pour imiter le schéma des Exporter un espace de travail. Vous pouvez créer un ensemble de politiques dans un espace de travail, l'exporter au format JSON, modifier le JSON, puis l'importer en tant que modèle de politique.

Attribut	Type	Description
name	chaîne	(Facultatif) Utilisé comme nom du modèle lors de l'importation.
description	chaîne	(Facultatif) Description du modèle qui s'affiche pendant le processus d'application.
paramètres	objet Paramètres	Paramètres du modèle, voir ci-dessous.
absolute_policies	tableau d'objets politiques	(Facultatif) Tableau de politiques absolues.
default_policies	tableau d'objets politiques	(obligatoire) Le tableau de politiques par défaut peut être vide.

Objet Paramètres

L'objet Paramètres est facultatif, mais il peut être utilisé pour définir dynamiquement des filtres en tant que paramètres du modèle. Les paramètres sont référencés à l'aide des attributs de politique `consumer_filter_ref` ou `provider_filter_ref`.

Les clés de l'objet Paramètres sont les noms de référence. Les valeurs sont un objet avec un « `type` » obligatoire. « `Filter` » et une description facultative. Un exemple d'objet Paramètres est présenté ci-dessous :

```
{
```

```
  "parameters": {
    "HTTP Consumer": {
      "type": "Filter",
      "description": "Consumer of the HTTP and HTTPS service"
    },
    "HTTP Provider": {
      "type": "Filter",
      "description": "Provider of the HTTP and HTTPS service"
    }
  }
}
```

Les paramètres peuvent être référencés dans les objets de politique, par exemple : « consumer_filter_ref » : « HTTP Consumer » ou « provider_filter_ref » : « HTTP Provider ».

Références de paramètres spéciaux

Quelques références particulières sont automatiquement mappées à un filtre et n'ont pas besoin d'être définies comme paramètres.

Référence	Description
_workspaceScope	Détermine la portée de l'espace de travail auquel le modèle est appliqué.
_rootScope	Résout la portée de niveau racine/supérieur.

Objet politique

Pour maintenir la compatibilité avec le JSON d'exportation d'espace de travail, l'objet politique contient plusieurs clés pour les consommateurs et les fournisseurs. Ces objets sont résolus comme suit :

```
if *_filter_ref is defined
  use the filter resolved by that parameter
else if *_filter_id is defined
  use the filter referenced by that id
else if *_filter_name is defined
  use the filter that has that name
else
  use the workspace scope.
```

Si un filtre ne peut pas être résolu comme défini ci-dessus, une erreur est renvoyée au moment de l'application et au moment du téléchargement.

Attribut	Type	Description
action	chaîne	(facultatif) Action de la politique, ALLOW (AUTORISER) ou DENY (REFUSER)(ALLOW par défaut).
priority	nombre entier	(Facultatif) Priorité de la politique (100 par défaut).
consumer_filter_ref	chaîne	Référence à un paramètre.
consumer_filter_name	chaîne	Référence à un filtre par nom.

Attribut	Type	Description
consumer_filter_id	chaîne	l'identifiant d'une portée ou d'un filtre d'inventaire défini.
provider_filter_ref	chaîne	Référence à un paramètre.
provider_filter_name	chaîne	Référence à un filtre par nom.
provider_filter_id	chaîne	l'identifiant d'une portée ou d'un filtre d'inventaire défini.
l4_params	tableau de l4 paramètres	Liste des ports et des protocoles autorisés.
Attribut	Type	Description
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	nombre entier	Plage de ports inclusive, par exemple, [80, 80] ou [5000, 6000] (NULL signifie tous les ports).

Objet L4param

Attribut	Type	Description
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	nombre entier	Plage de ports inclusive, par exemple, [80, 80] ou [5000, 6000] (NULL signifie tous les ports).

Échantillon de modèle

```
{
  "name": "Allow HTTP/HTTPS and SSH",
  "parameters": {
    "HTTP Consumer": {
      "type": "Filter",
      "description": "Consumer of the HTTP and HTTPS service"
    },
    "HTTP Provider": {
      "type": "Filter",
      "description": "Provider of the HTTP and HTTPS service"
    }
  },
  "default_policies": [
    {
      "action": "ALLOW",
      "priority": 100,
      "consumer_filter_ref": "__rootScope",
      "provider_filter_ref": "__workspaceScope",
      "l4_params": [
```

```
        { "proto": 6, "port": [22, 22] },
      ]
    },
    {
      "action": "ALLOW",
      "priority": 100,
      "consumer_filter_ref": "HTTP Consumer",
      "provider_filter_ref": "HTTP Provider",
      "l4_params": [
        { "proto": 6, "port": [80, 80] },
        { "proto": 6, "port": [443, 443] }
      ]
    }
  ]
}
```

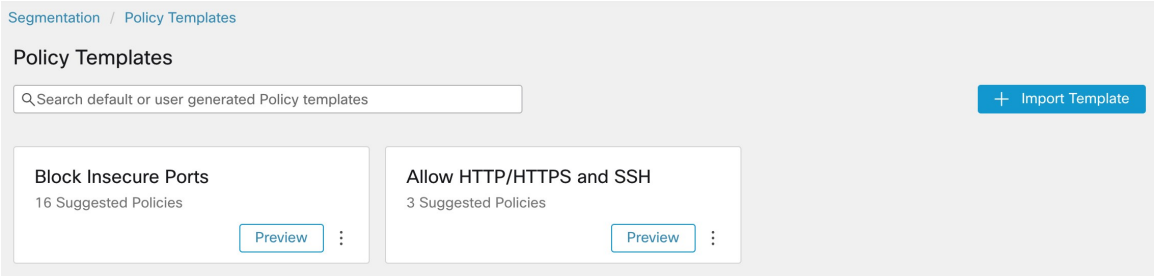
Importation de modèle

Les modèles de politiques sont affichés dans la page des modèles de politiques et accessibles à partir de la page principale de segmentation. C'est à ce niveau que les modèles peuvent être importés ou téléchargés en utilisant le bouton « Import Template) Importer un modèle ».

L'exactitude des modèles est validée lorsqu'ils sont téléversés. Une liste d'erreurs utile est fournie pour déboguer les problèmes.

Une fois qu'un modèle est téléversé, le nom et la description peuvent être appliqués, téléchargés ou mis à jour.

Figure 4: Affichage des modèles disponibles



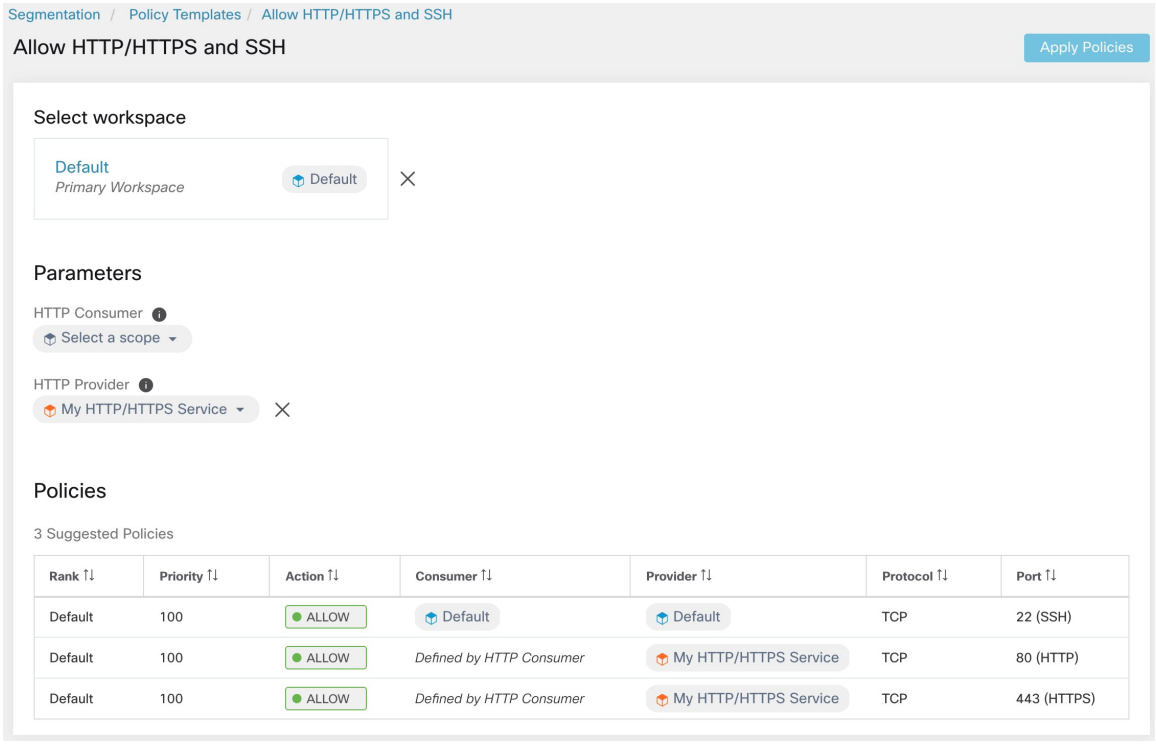
Application d'un modèle

L'application d'un modèle à un espace de travail se fait en plusieurs étapes :

1. Sélectionnez un modèle pour obtenir un aperçu.
2. Sélectionnez un espace de travail auquel appliquer le modèle.
3. Renseignez les paramètres si nécessaire.
4. Passez en revue les politiques.
5. Appliquez les politiques.

Les politiques seront ajoutées à la dernière version de l'espace de travail sélectionné. Les politiques créées à l'aide d'un modèle peuvent être filtrées à l'aide de l`From Template? (Du modèle?) = vrai` pour le filtre.

Figure 5: Application d'un modèle de politique



Découvrir automatiquement les politiques

La découverte automatique des politiques, parfois appelée détection de politiques et anciennement ADM (Application Dependency Mapping), utilise les flux de trafic existants et d'autres données pour effectuer ce qui suit :

- Suggérer un ensemble de politiques « autorisées » en fonction de l'activité réussie du réseau.

  L'objectif de ces politiques est d'identifier le trafic dont votre entreprise a besoin et de bloquer tout autre trafic.

- Regrouper les charges de travail en grappes en fonction de la ressemblance de leur comportement informatique

  Par exemple, si une application comprend plusieurs serveurs Web, ceux-ci peuvent être regroupés.

  Pour en savoir plus, consultez Grappes, on page 78.

Vous pouvez découvrir des politiques pour chaque portée. En règle générale, vous découvrez les politiques pour les portées au bas de l'arborescence ou près de celle-ci, par exemple au niveau de l'application. Cependant, pour le déploiement initial, vous pouvez souhaiter découvrir les politiques à une portée de niveau supérieur, de sorte que vous avez des politiques générales temporaires en place pendant que vous créez des politiques plus affinées.

Vous pouvez procéder à la découverte des politiques aussi souvent que vous le souhaitez pour affiner les suggestions de politiques en fonction d'informations supplémentaires.

Vous pouvez modifier manuellement les politiques et les grappes suggérées, et/ou les approuver, afin qu'elles soient reportées et non modifiées par les cycles de découverte ultérieurs.

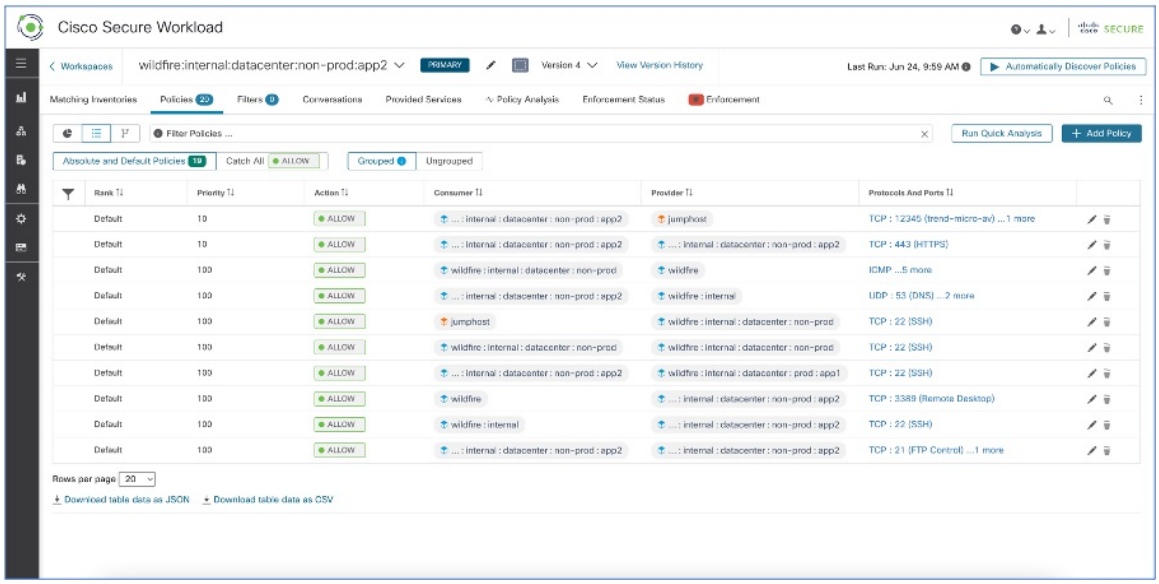
Vous pouvez inclure les politiques créées manuellement et les politiques découvertes dans un espace de travail.

Après avoir découvert les politiques, vous les passerez en revue et les analyserez avant de les appliquer.

Pour commencer à découvrir les politiques, consultez Comment découvrir automatiquement les politiques, on page 23.

Pour en savoir plus, consultez Détails de la découverte des politiques, on page 22.

Figure 6: Exemple : politiques détectées automatiquement



Détails de la découverte des politiques

Renseignements supplémentaires sur la découverte automatique des politiques :

- La découverte automatique des politiques prend en compte les conversations dans lesquelles au moins une extrémité est une charge de travail de membre de la portée dans la plage temporelle sélectionnée. L'appartenance à la portée est basée uniquement sur la définition la plus récente de la portée; l'appartenance antérieure n'est pas prise en compte.
- Par défaut, la découverte de politiques produit des politiques et des grappes en analysant les flux de communication (« conversations »), mais peut éventuellement prendre en compte d'autres renseignements tels que les processus en cours d'exécution sur les charges de travail ou les configurations d'équilibreurs de charge.

  Consultez Inclure les données des équilibreurs de charge et des routeurs lors de la découverte des politiques, à la page 39.
- Vous pouvez découvrir des politiques dans n'importe quel espace de travail de la portée. Les résultats de la découverte de chaque espace de travail sont indépendants des résultats des autres espaces de travail de la portée.

- Pour lire les des discussions détaillées sur les concepts complexes liés à la découverte automatique des politiques, consultez Fonctionnalités avancées de découverte automatique des politiques, à la page 31 et Aborder les complexités de la politique, à la page 87.

Comment découvrir automatiquement les politiques

Effectuez les étapes suivantes. À tout moment, vous pouvez décider de découvrir à nouveau les politiques.

Collaborez avec des collègues, au besoin, pour effectuer ces étapes.

Étape	Faire ceci	Autres renseignements
1	Chargez et étiquetez votre inventaire de charge de travail, et recueillez les données de flux qui informent la découverte des politiques.	Consultez Premiers pas avec la segmentation et la microsegmentation et les sous-sections.
2	Choisissez si vous souhaitez découvrir les politiques pour : • Les charges de travail dans une seule portée • Les charges de travail dans toutes les portées d'une branche de l'arborescence des portées	Consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 25. (Vous pouvez toujours redécouvrir les politiques à tout moment).
3	Choisissez la portée dans laquelle vous découvrez les politiques.	Cela dépend en partie du fait que vous découvriez des politiques pour une seule portée ou pour une branche de l'arborescence des portées.
4	Choisissez l'espace de travail dans lequel vous découvrez les politiques.	En général, vous découvrirez les politiques dans l'espace de travail principal de la portée, car vous ne pouvez analyser les politiques que dans un espace de travail principal. (Cependant, vous pouvez toujours remplacer un espace de travail par un principal ultérieurement). Si la portée que vous avez choisie ne comporte pas encore d'espace de travail, consultez Créer un espace de travail, à la page 3.
5	Confirmez l'inventaire que vous souhaitez inclure dans la découverte de politiques.	Vérifiez les charges de travail auxquelles la découverte de politiques s'appliquera, à la page 27
6	(Facultatif) Créez des filtres d'inventaire pour regrouper les charges de travail que vous souhaitez traiter comme un groupe.	Consultez Créer un filtre d'inventaire.
7	Définissez l'action **Collectrice** (c'est à dire fourre-tout) pour l'espace de travail	Voir la section Rang de politique : Absolue, Par défaut et Collectrice, à la page 9.

Étape	Faire ceci	Autres renseignements
8	Découvrir les politiques	Découvrir automatiquement les politiques, à la page 21 Assurez-vous de remplir les conditions préalables décrites dans la section « Avant de commencer ».
9	Afficher et gérer les grappes (groupes de charges de travail) créées par la découverte de politiques. (Cette étape s'applique uniquement lorsque vous découvrez des politiques pour une seule portée; les grappes ne sont pas générées lorsque vous découvrez des politiques pour une branche de l'arborescence).	Consultez Grappes, à la page 78 et les sous-sections. Évaluez les grappes suggérées, modifiez éventuellement l'appartenance aux grappes le cas échéant et approuvez (ou mieux encore, convertissez en filtres d'inventaire) toutes les grappes que vous souhaitez rendre permanentes.
10	Tenez compte des complexités telles que l'hérédité des politiques et les politiques multiportées.	Consultez Aborder les complexités de la politique, à la page 87.
11	Examiner les politiques générées.	Consultez Consulter les politiques découvertes automatiquement, à la page 110 et les sous-sections.
12	Approuvez les politiques que vous souhaitez conserver.	Approuver les politiques, à la page 51
13	Découvrez à nouveau les politiques si vous le souhaitez, pour refléter des données de flux supplémentaires, des changements dans la composition de la portée, ou d'autres changements.	Important : Avant de réexécuter la découverte automatique des politiques, à la page 54 Vous pouvez réexécuter la découverte de politiques à tout moment. Passez en revue et approuvez les politiques et les groupes chaque fois que vous découvrez des politiques.
14	Exécutez une analyse en direct pour voir comment vos politiques affectent votre trafic réel.	Lorsque vous estimez que vos politiques produisent ce que vous attendez d'elles, démarrez Analyse des politiques en temps réel, à la page 118. Si vous modifiez les politiques ou les redécouvrez, redémarrez l'analyse des politiques (pour analyser les politiques actuelles).
15	Si vous redécouvrez des politiques ou apportez d'autres modifications, redémarrez l'analyse en direct.	Consultez Après avoir modifié les politiques, analyser les politiques les plus récentes, à la page 127.
16	Lorsque vous êtes sûr que les politiques ne bloqueront pas le trafic essentiel, appliquez l'espace de travail.	Voir Appliquer des politiques et les sous-thèmes.
17	Vérifier que l'application fonctionne comme prévu.	Voir la section Vérifier que l'application fonctionne comme prévu, à la page 139.

Étape	Faire ceci	Autres renseignements
18	(Facultatif) Configurez les paramètres de découverte de politiques par défaut qui s'appliquent facultativement lors de la découverte de politiques dans n'importe quel espace de travail.	Consultez Configuration de la découverte de politiques par défaut, à la page 49 et les rubriques connexes. Puisqu'il s'agit de paramètres avancés, nous vous recommandons de les modifier uniquement si vous avez un besoin particulier de le faire. Vous pouvez les modifier à tout moment au cours de votre processus si vous prenez conscience d'un besoin.

Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée

Si l'une ou l'autre de ces options n'est possible lorsque vous découvrez les politiques pour une portée particulière, la sélection est effectuée pour vous, et vous ne verrez pas de choix d'options.

Tableau 2 : Découverte des politiques pour :

Une branche de l'arborescence de la portée	Une seule portée
Utilisez cette méthode comme point de départ, lorsque vous commencez à utiliser Cisco Secure Workload, pour générer rapidement un ensemble temporaire de politiques générales qui autorisent le trafic existant tout en vous aidant à protéger votre réseau contre les menaces futures.	Utilisez cette méthode pour affiner les politiques de segmentation et vous assurer que tous les flux autorisés sont attendus; le nombre plus restreint de politiques permet de repérer plus facilement les anomalies existantes qui nécessitent une enquête.
En règle générale, vous utilisez cette méthode pour les portées situées plus près du sommet de votre arborescence. Le sommet de la branche peut correspondre à n'importe quelle portée dans l'arborescence.	En règle générale, vous utilisez cette méthode pour les portées situées au bas de l'arborescence, par exemple pour les portées dédiées à une seule application.
Politiques de découverte uniquement dans une seule portée : la portée située en haut de la branche de votre choix.	Découvrir les politiques pour chaque portée de la branche, le cas échéant.
Toutes les charges de travail dans la portée choisie et toutes les portées enfants et descendants sont incluses dans la découverte.	Les charges de travail qui sont également membres d'une portée enfant ne sont pas incluses dans la découverte pour cette portée. Les politiques sont générées uniquement pour les charges de travail qui apparaissent dans l'onglet **Uncategorized Inventory (Inventaire non classé)** pour cette portée sur la page **Organize > Scopes and Inventory** (Organiser > Portées et inventaire). Vous pouvez découvrir des politiques pour les charges de travail dans les portées enfant et descendante séparément.

Une branche de l'arborescence de la portée	Une seule portée
Toutes les politiques relatives aux charges de travail de toutes les portées de la branche résident dans la portée située au sommet de la branche.	En supposant que vous créiez également des politiques pour les charges de travail dans les portées enfant et descendante, les politiques résident dans plusieurs portées.
Cette méthode génère généralement un grand nombre de politiques.	Cette méthode génère moins de politiques dans une portée individuelle.
Les politiques découvertes s'appliquent à des portées entières; cette option ne peut pas créer de politiques propres aux sous-ensembles de charges de travail dans les portées.	Cette option peut générer des politiques qui s'appliquent à des sous-ensembles de charges de travail dans la portée du consommateur ou du fournisseur. (Les charges de travail peuvent être regroupées par grappes générées ou par filtres d'inventaire configurés, et les politiques appliquées uniquement à ces sous-ensembles).
Toutes les politiques sont créées dans une seule portée, en haut de la branche, donc aucune étape supplémentaire n'est requise lorsque le consommateur et le fournisseur d'une politique se trouvent dans des portées différentes.	Autoriser le trafic entre les consommateurs et les fournisseurs dans différentes portées nécessite des étapes supplémentaires. Consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 94.
La découverte peut s'exécuter même si une portée n'a aucune charge de travail de membre avec des agents installés, tant que les portées descendantes comportent des agents ou des orchestrateurs ou des connecteurs externes qui recueillent les données de flux.	La portée doit avoir des charges de travail de membres avec des agents installés ou des orchestrateurs ou des connecteurs externes qui recueillent des données de flux.
Cette option est disponible uniquement pour les propriétaires de portée racine et les administrateurs de site.	Vous devez avoir des privilèges pour créer des politiques pour cette portée.
Le nombre maximal d'agents et de conversations est différent pour chaque option. Consultez Limites liées aux politiques.	
Cette option était auparavant l'option de configuration avancée Advanced Policy Generation pour la découverte automatique des politiques. Le comportement n'a pas changé.	Il s'agissait auparavant du comportement par défaut pour la découverte automatique des politiques.
Pour en savoir plus, consultez Découverte des politiques pour une branche de l'arborescence d'une portée : informations supplémentaires, à la page 26.	--

Découverte des politiques pour une branche de l'arborescence d'une portée : informations supplémentaires

- Toutes les charges de travail qui sont des points terminaux de conversation, qu'elles soient membres ou non de la portée dans laquelle la découverte de politiques est exécutée, reçoivent l'étiquette de portée correspondante la plus élevée en fonction de l'ordre ascendant donné dans la liste des dépendances externes.

- Pour les options de configuration avancée disponibles lorsque vous générez des politiques pour une branche de l'arborescence de portée, consultez :
  - Activer la suppression des politiques redondantes, à la page 46
  - Compression des politiques, à la page 42 et les sous-thèmes connexes, Compression hiérarchique des politiques, à la page 42
- Actuellement, le nombre de charges de travail affiché pour la découverte automatique des politiques n'inclut que celles qui ne sont pas également membres d'une sous-portée.

Vérifiez les charges de travail auxquelles la découverte de politiques s'appliquera

Avant de découvrir automatiquement les politiques, vérifiez que les charges de travail sur lesquelles la découverte de politiques sera basée correspondent bien à l'ensemble de charges de travail attendu. Les politiques de découvertes seront générées à partir des données de flux capturées par les agents sur ces charges de travail.

Avant de commencer

Décidez laquelle des options de Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 25 vous pouvez utiliser.

Procédure

Étape 1 Dans le menu de navigation de gauche, choisissez **Defend > Segmentation** (défense > segmentation).

Étape 2 Cliquez sur la portée pour laquelle vous souhaitez découvrir les politiques.

Étape 3 Cliquez sur l'espace de travail dans lequel vous souhaitez découvrir les politiques.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 5 Cliquez sur **Matching Inventories** (Inventaires correspondants).

Étape 6 Si vous découvrez des politiques pour une seule portée :

a) Cliquez sur **Uncategorized Inventory** (Inventaire non classé)

Cette page affiche les charges de travail qui ne sont pas également membres des portées enfants. (Dans la découverte automatique des politiques standard, les politiques et les grappes sont générées dans cette portée uniquement pour les charges de travail qui ne sont pas également membres des portées enfants).

b) Cliquez sur **IP Addresses** (Adresses IP).

Les adresses IP sur cette page ne comportent pas d'agents Cisco Secure Workload.

Puisqu'elles n'ont pas d'agents installés, ces adresses IP ne sont pas prises en compte lors de la découverte automatique des politiques pour cette portée sauf dans les cas suivants :

- La politique est gérée par un connecteur infonuagique
- Les adresses IP sont basées sur un inventaire fondé sur le conteneur, auquel cas les charges de travail individuelles apparaissent sur l'onglet « **Pods** », ou
- les charges de travail communiquent avec une charge de travail dans cette portée prise en compte lors de la découverte de politique.

Avant de découvrir les politiques, envisagez d'installer des agents sur les charges de travail qui en ont besoin et de laisser passer un certain temps pour que les données de flux s'accumulent.

c) Cliquez sur **Workloads** (Charges de travail).

Les politiques et les grappes sont générées uniquement pour les charges de travail sur cette page et pour les adresses IP dans l'onglet IP address (adresses IP) qui répondent aux critères précisés ci-dessus.

d) Si vous avez un inventaire Kubernetes ou OpenShift, vous verrez un onglet **Services** et un onglet **Pods**.

Si vous avez installé des agents sur vos charges de travail Kubernetes/OpenShift vérifiez également l'inventaire dans ces onglets.

e) Si vous avez un inventaire de l'équilibreur de charge, celui-ci s'affiche sous l'onglet **Services**.

Étape 7 Si vous découvrez des politiques pour une branche de l'arborescence :

a) Cliquez sur **All Inventory** (Tout l'inventaire).

Ce processus génère des politiques (mais pas de grappes) pour toutes les charges de travail de cette portée, qu'elles soient également membres ou non de portées enfants.

b) Cliquez sur **IP Addresses** (Adresses IP).

Les adresses IP sur cette page ne comportent pas d'agents Cisco Secure Workload.

Puisqu'aucun agent n'est installé, ces adresses IP ne seront pas prises en compte lors de la découverte automatique des politiques pour cette portée, sauf si :

- La politique est gérée par un connecteur infonuagique
- Les adresses IP sont basées sur un inventaire fondé sur le conteneur, auquel cas les charges de travail individuelles apparaissent sur l'onglet « **Pods** », ou
- les charges de travail communiquent avec une charge de travail dans cette portée prise en compte lors de la découverte de politique.

Avant de découvrir les politiques, pensez à installer des agents sur ces charges de travail et attendez que les données de flux s'accumulent.

c) Cliquez sur **Workloads** (Charges de travail).

Les politiques sont générées uniquement pour les charges de travail sur cette page et pour les adresses IP dans l'onglet IP address (adresses IP) qui répondent aux critères précisés ci-dessus.

d) Si vous avez un inventaire Kubernetes ou OpenShift, vous verrez un onglet **Services** et un onglet **Pods**.

Si vous avez installé des agents sur vos charges de travail Kubernetes/OpenShift vérifiez également l'inventaire dans ces onglets.

e) Si vous avez un inventaire de l'équilibreur de charge, celui-ci s'affiche sous l'onglet **Services**.

Étape 8 Vérifiez que les charges de travail sont bien l'ensemble attendu.

Découvrir automatiquement les politiques

Utilisez cette procédure pour générer des suggestions de politiques d'autorisation en fonction du trafic existant sur votre réseau.

Vous pouvez réexécuter la découverte de politiques à tout moment.

Avant de commencer

- Rassembler des données de flux avant de pouvoir découvrir automatiquement les politiques.

  En général, cela signifie que vous avez installé les agents sur les charges de travail de la portée, ou que vous avez configuré et recueilli des données à l'aide d'un connecteur infonuagique ou d'un orchestrateur externe.

  Les données de résumé de flux utilisées par la découverte automatique des politiques sont calculées toutes les 6 heures. Ainsi, lors du déploiement initial de Cisco Secure Workload, la découverte automatique des politiques n'est pas possible tant que ces données ne sont pas disponibles.

  Un plus grand nombre de données de flux produit généralement des résultats plus précis.

  Avant d'appliquer une politique, vous devez recueillir suffisamment de données pour inclure le trafic qui ne se produit que périodiquement (mensuel, trimestriel, annuel, etc.). Par exemple, si une application génère un rapport trimestriel qui recueille des informations provenant de sources auxquelles l'application n'accède pas à d'autres moments, assurez-vous que les données de flux incluent au moins une instance de ce processus de génération de rapports.

- Suivez les étapes décrites ci-dessus dans Comment découvrir automatiquement les politiques, à la page 23.
- Respectez le Limites liées aux politiques liée à la découverte des politiques

  Si nécessaire, scindez les portées les plus importantes en portées enfants plus petites.

- Validez toutes les modifications de portée avant de découvrir les politiques, sinon les filtres d'exclusion configurés pourraient ne pas correspondre aux flux comme prévu (ne pas les exclure). Consultez Valider les modifications.

Important Si vous réexécutez la découverte de politiques, consultez d'abord ces considérations importantes : Important : Avant de réexécuter la découverte automatique des politiques, à la page 54.

Procédure

Étape 1 Sélectionnez**Defend (Défendre)** > **Segmentation (Segmentation)**.

Étape 2 Dans l'arborescence des portées ou dans la liste des portées dans le volet de gauche, faites défiler la liste ou recherchez la portée pour laquelle vous souhaitez générer des politiques.

Étape 3 Cliquez sur un espace de travail (principal ou secondaire) dans la portée.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 5 Cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques).

Étape 6 Si vous voyez une option pour découvrir des politiques dans une branche de l'arborescence ou une portée complète, choisissez une option.

Si vous ne voyez pas d'option, une seule option est possible pour la portée pour laquelle vous découvrez des politiques.

Pour en savoir plus, consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 25.

Étape 7 Choisissez la plage temporelle des données de flux que vous souhaitez inclure.

Testez pour déterminer la bonne plage temporelle; vous pouvez générer des politiques aussi souvent que nécessaire pour obtenir des résultats optimaux.

Une plage temporelle plus courte génère des résultats plus rapidement et peut en générer moins.

En général, une plage temporelle plus longue produit des politiques plus précises. Toutefois, si la définition de la portée a été modifiée, n'incluez pas les dates précédant la modification.

Votre plage temporelle doit inclure le trafic qui ne se produit que périodiquement (mensuel, trimestriel, annuel, etc)., le cas échéant. Par exemple, si une application génère un rapport trimestriel qui recueille des renseignements provenant de sources auxquelles elle n'accède pas à d'autres moments, assurez-vous que la plage temporelle comprend au moins une instance de ce processus de génération de rapports.

Pour configurer une plage temporelle au-delà des 30 derniers jours, sélectionnez la plage **personnalisée** et remplissez les heures de début et de fin requises dans le gadget déroulant de sélection de l'heure.

Étape 8 (Facultatif) Spécifiez les paramètres avancés.

En général, nous vous suggérons de ne pas modifier les paramètres avancés des cycles de découverte initiaux, puis d'apporter les modifications nécessaires uniquement pour la résolution de problèmes spécifiques.

Pour de plus amples renseignements, consultez la section Configurations avancées pour la découverte automatique des politiques, à la page 39.

Étape 9 Cliquez sur **Discover Policies** (Découvrir les politiques). Les politiques générées s'affichent sur cette page.

Prochaine étape

- Affichez Arrêter la découverte automatique des politiques en cours, à la page 30.
- Revenez à Comment découvrir automatiquement les politiques, à la page 23 et passez à l'étape suivante dans le tableau.
- Vous pouvez réexécuter la découverte de politiques à tout moment. Pour connaître les actions à effectuer en premier, consultez Important : Avant de réexécuter la découverte automatique des politiques, à la page 54.

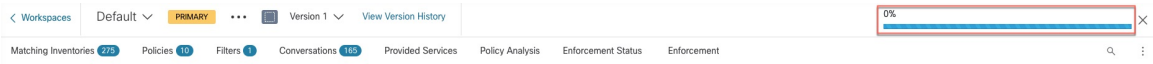
Arrêter la découverte automatique des politiques en cours

La progression de la découverte automatique des politiques est toujours visible dans l'en-tête. La navigation vers d'autres espaces de travail n'affecte pas la progression.

Pour arrêter l'analyse pendant qu'elle est en cours, cliquez sur le bouton **Abort** (abandonner).

Une fois l'analyse terminée, un message s'affiche. En cas de réussite, **Cliquez pour voir les résultats** permet d'accéder à une vue différente indiquant les modifications avant et après l'exécution. L'échec de la découverte automatique des politiques est indiqué par un message et une raison différents.

Figure 7: Progression de la découverte automatique des politiques



Fonctionnalités avancées de découverte automatique des politiques

Vous devez spécifier une plage temporelle pour l'exécution de la découverte. Au besoin, vous pouvez configurer des options avancées.

Vous pouvez configurer des options avancées pour chaque espace de travail ou définir des valeurs par défaut pour tous les espaces de travail (l'ensemble de la portée racine), puis modifier les paramètres de chaque espace de travail au besoin.

Tableau 3 : Configurer les options avancées pour la découverte automatique des politiques

Pour un espace de travail	Pour tous les espaces de travail
Les descriptions des options pour les espaces de travail individuels (dans la colonne 1) s'appliquent également à tous les espaces de travail (dans la colonne 2).	
Dépendances externes, à la page 34	Configuration de la découverte de politiques par défaut, à la page 49
Configurations avancées pour la découverte automatique des politiques, à la page 39	Configuration de la découverte de politiques par défaut, à la page 49
Filtres d'exclusion, à la page 31	Filtres d'exclusion par défaut, à la page 50

Filtres d'exclusion

Si certains flux génèrent des politiques indésirables, vous pouvez exclure ces flux de la découverte automatique des politiques à l'aide de filtres d'exclusion.

Par exemple, pour interdire certains protocoles comme ICMP dans le modèle de liste d'autorisation finale, vous pouvez créer un filtre d'exclusion avec un champ de protocole défini à ICMP.

Note

- Les conversations qui correspondent aux filtres d'exclusion sont exclues à des fins de génération de politiques et de mise en grappe, mais restent présentent dans l'affichage des conversations avec l'icône rouge « excluded » (exclue) (voir la vue du tableau dans Conversations). De même, les charges de travail de l'espace de travail impliquées dans ces conversations restent également visibles.
- Un filtre d'exclusion qui utilise une grappe ou une définition de filtre d'un espace de travail n'est efficace que dans les espaces de travail principaux (sinon, ses définitions de grappe ne sont pas visibles par le système d'étiquettes et toutes les conversations correspondantes ne sont pas exclues).
- Les filtres d'exclusion font l'objet de versions; pour suivre les modifications, consultez Journaux d'activités et historique des versions (Historique et Diff.).
- Pour connaître les limites du nombre de filtres d'exclusion, consultez Limites liées aux politiques.

Vous pouvez créer l'un des éléments suivants ou les deux, puis activer l'un ou l'autre ou les deux lors de la découverte des politiques :

- Une liste de filtres d'exclusion pour chaque espace de travail.
- Une liste de filtres d'exclusion par défaut disponibles pour tous les espaces de travail de votre détenteur.

Vous pouvez également activer ou désactiver l'une des listes ou les deux pour la configuration de découverte de politiques par défaut.

Pour plus de renseignements sur les instructions, consultez Configurer, modifier ou supprimer les filtres d'exclusion, on page 32 et Activer ou désactiver les filtres d'exclusion, on page 34.

Configurer, modifier ou supprimer les filtres d'exclusion

Vous pouvez utiliser cette procédure pour créer une liste de filtres d'exclusion pour un espace de travail unique, ou une liste de filtres d'exclusion par défaut qui sont disponibles pour tous les espaces de travail.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

Destinataire	Faire ceci
Configurer les filtres d'exclusion pour un espace de travail spécifique	Accédez à l'espace de travail, puis effectuez l'une des opérations suivantes : • Cliquez sur **Manage Policies** (gestion des politiques), puis sur le (Autre) près du coin supérieur droit de la page et sélectionnez **Exclusion Filters** (filtres d'exclusion). • Dans la page de configuration de découverte automatique des politiques, cliquez sur le lien **Exclusion Filters** (Filtres d'exclusion) dans la section Advanced Configurations (Advanced Configurations). • Supprimer une politique découverte; vous verrez une option pour créer un filtre d'exclusion qui le permette.
Configurer les filtres d'exclusion par défaut qui sont disponibles pour n'importe quel espace de travail	1. Choisissez **Defend (défense)** > **Segmentation (segmentation)**, 2. Cliquez sur le signe d'insertion sur le côté droit de la page pour développer le menu Outils, puis choisissez **Default Policy Discovery Config** (Configuration de la découverte des politiques par défaut). 3. Accédez au bas de la page 4. Cliquez sur **Default Exclusion Filters** (filtres d'exclusion par défaut).

Étape 2 Pour créer un filtre d'exclusion, cliquez sur **Add Exclusion Filter** (Ajouter un filtre d'exclusion).

Étape 3 Préciser les paramètres des flux à exclure de la prise en compte lors de la découverte des politiques :

Vous n'avez pas besoin de saisir des valeurs pour tous les champs. Tout champ vide est traité comme un caractère générique pour les flux correspondants.

Toute conversation correspondant à tous les champs d'un filtre d'exclusion est ignorée lors de la création de la politique et de la mise en grappe.

Option	Description
Consumer	Correspond aux conversations pour lesquelles l'adresse du consommateur est membre de la portée sélectionnée, du filtre d'inventaire ou de la grappe (pour les filtres d'exclusion spécifiques à l'espace de travail uniquement). Vous pouvez spécifier n'importe quel espace d'adresse en créant un nouveau filtre personnalisé.
Provider	Correspond aux conversations pour lesquelles l'adresse du fournisseur est membre de la portée sélectionnée, du filtre d'inventaire ou de la grappe (pour les filtres d'exclusion spécifiques à l'espace de travail uniquement). Vous pouvez spécifier n'importe quel espace d'adresse en créant un nouveau filtre personnalisé.
Protocol	Correspond aux conversations avec le protocole spécifié.
Port	Correspond aux conversations avec le port du fournisseur (serveur) correspondant au port ou à la plage de ports spécifié. Saisissez les plages de ports en utilisant un tiret, par exemple « 100-200 »

Étape 4 Pour modifier ou supprimer un filtre d'exclusion, survolez la ligne applicable pour voir les boutons **Modifier** et **Supprimer**.

Étape 5 Si vous configurez des filtres d'exclusion par défaut :

Lorsque les filtres configurés sont prêts à l'emploi, revenez à la page **Default Policy Discovery Config** (Configuration de la découverte des politiques par défaut) et cliquez sur **Save (Enregistrer)** pour rendre les modifications disponibles pour les espaces de travail individuels.

Prochaine étape

Important Les filtres d'exclusion sont activés par défaut dans l'espace de travail dans lequel ils sont configurés.

Les filtres d'exclusion par défaut sont activés par défaut dans tous les espaces de travail.

Les deux types de filtres d'exclusion sont activés par défaut dans la configuration de découverte des politiques par défaut.

Avant de découvrir les politiques :

- Activer ou désactiver les filtres d'exclusion et les filtres d'exclusion par défaut.
  - Dans chaque espace de travail
  - Dans la page de configuration de la découverte des politiques par défaut :

  Pour plus d'informations sur les instructions, consultez Activer ou désactiver les filtres d'exclusion, à la page 34
- Validez toute modification de portée, sinon les filtres pourraient ne pas correspondre (et donc exclure) les flux attendus. Consultez Valider les modifications.

Activer ou désactiver les filtres d'exclusion

Vous pouvez créer des filtres d'exclusion dans chaque espace de travail et/ou créer un ensemble de filtres d'exclusion par défaut que vous pouvez appliquer à tous les espaces de travail.

Par défaut, les deux types de filtres d'exclusion sont activés.

Pour apporter des modifications

- Pour activer ou désactiver les filtres d'exclusion pour un seul espace de travail :

  Dans l'espace de travail, cliquez sur **Manage Policies (Gérer les politiques)**, sur **Automatically Discover Policies (Découvrir automatiquement les politiques)**, puis sur **Advanced Configurations (Configurations avancées).** Vous pouvez activer des filtres d'exclusion ou des filtres d'exclusion par défaut pour cet espace de travail.

- Pour activer ou désactiver les filtres d'exclusion dans la configuration de découverte des politiques par défaut :

  Choisissez **Defend > Segmentation (défendre la segmentation)**, puis cliquez sur le signe d'insertion dans la partie droite de la page pour développer le menu Tools (outils). Choisissez ensuite **Default Policy Discovery Config (Configuration de la découverte des politiques par défaut).** Faites défiler la liste jusqu'à **Configurations avancées**, ou cliquez dessus. Vous pouvez activer des filtres d'exclusion et/ou des filtres d'exclusion par défaut.

Dépendances externes

Les dépendances externes ne sont pertinentes que lorsque vous utilisez le processus décrit dans (Avancé) Créer des politiques de portées croisées, on page 95.

Les paramètres de dépendances externes s'appliquent aux politiques découvertes automatiquement et impliquant des communications vers et depuis des charges de travail qui sont membres d'une portée autre que celle dans laquelle les politiques sont découvertes. (C'est-à-dire les communications impliquant des « charges de travail externes »).

Une charge de travail qui n'est pas membre de la portée dans laquelle la politique existe est une *charge de travail externe*. Ces charges de travail constituent l'autre extrémité d'une conversation avec une *charge de travail cible* (qui *est* membre de la portée dans laquelle la politique existe).

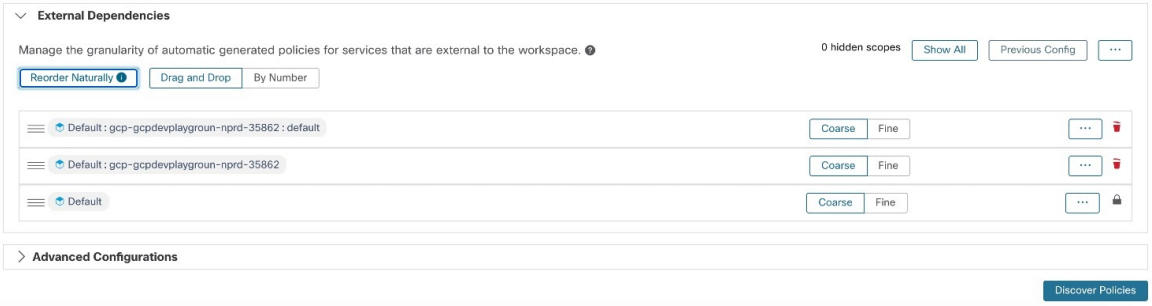
La liste des dépendances externes est une liste ordonnée de tous les portées de votre hiérarchie. Chaque portée de la liste est définie sur l'une des options suivantes :

- Générer des politiques spécifiques ou affinées (plus sécurisées), OU
- Générer des politiques plus globales dans des portées plus élevées, qui peuvent mieux se généraliser (c'est-à-dire qui sont plus susceptibles d'autoriser des flux légitimes qui n'ont pas été vus dans la plage temporelle spécifiée lors de la découverte des politiques).

Lors de la découverte de politique, la première portée (ou filtre de grappe ou d'inventaire - voir ci-dessous) qui correspond à la charge de travail sera utilisée pour générer la politique « autoriser », où l'ordre de correspondance (et le niveau de granularité qui en découle) est déterminé par le classement affiché dans la section Dépendances externes.

Un ordre des portées par défaut est configuré à votre intention, avec toutes les portées définies sur « globales » par défaut.

Figure 8: Dépendances externes par défaut



Destinataire	Faire ceci
Afficher ou affiner les dépendances externes pour un espace de travail :	Accédez à l'espace de travail et cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques), puis sur **External Dependencies** (Dépendances externes). Pour réorganiser les portées et choisir des options granulaires pour chacune, consultez Ajuster les dépendances externes d'un espace de travail, on page 36.
Configurez les dépendances externes par défaut pour la portée racine complète :	Consultez Configuration de la découverte de politiques par défaut, on page 49.

Dépendances externes : politiques granulaires impliquant des sous-ensembles de portées

Vous pouvez éventuellement découvrir des politiques à un niveau plus granulaire que le niveau de portée à portée, afin de contrôler le trafic vers un sous-ensemble spécifié de charges de travail dans une portée.

Par exemple, vous pouvez créer des politiques spécifiques à un certain type d'hôte au sein d'une application, comme les serveurs API ; vous pouvez regrouper ces charges de travail dans un sous-ensemble au sein de la portée de l'application.

Pour générer des politiques spécifiques à un sous-ensemble de charges de travail dans une portée, consultez Ajuster les dépendances externes d'un espace de travail, on page 36.

Conseils pour l'exploration des dépendances externes

Utilisez les conseils suivants pour explorer le comportement de la découverte automatique des politiques pour les politiques impliquant des espaces de travail qui ne sont pas membres de la portée associée à l'espace de travail dans lequel les politiques se trouvent.

Astuces

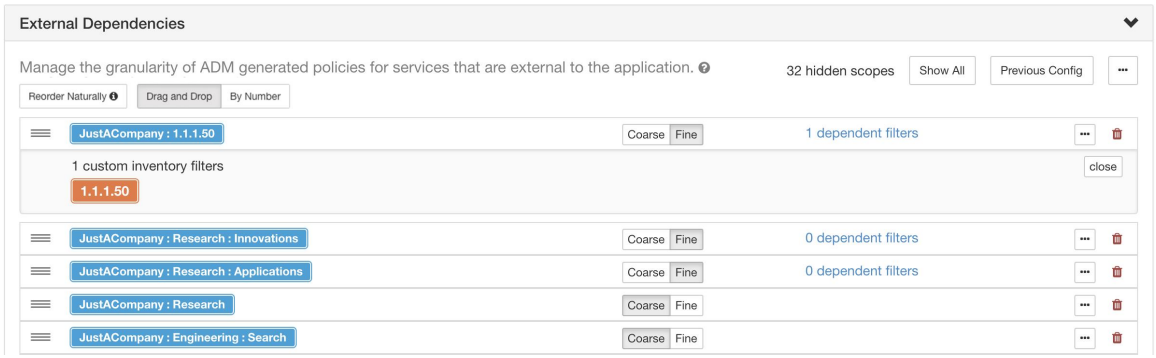
- Vous pouvez supprimer et réorganiser la liste pour générer des politiques avec la granularité souhaitée. Par exemple, la suppression de tous les sous-portées d'entreprise : RTP permettra de générer des politiques portées pour l'ensemble de la portée Entreprise : RTP, mais pas ses composants individuels, tout en maintenant une granularité plus élevée pour la portée SJC de l'entreprise. En outre, vous pouvez cliquer sur le bouton **Fine** (Fin) à côté de n'importe quelle portée et voir s'il existe des candidats à une granularité plus fine définis dans cette portée.
- Par défaut, la portée racine est configurée comme l'entrée la plus basse dans la liste des dépendances externes, de sorte que la découverte automatique des politiques génère toujours des politiques pour des portées plus spécifiques, chaque fois que cela est possible. Au départ, pour afficher relativement peu de politiques générales, vous pouvez placer temporairement la portée racine au-dessus des dépendances externes. De cette façon, après la découverte automatique des politiques, vous verrez toutes les politiques externes de l'espace de travail se connecter à une seule portée, la portée racine (car chaque charge de travail externe est mappée à la portée racine). Le nombre de politiques générées qui en résulte est réduit et plus facile à examiner et à comprendre.
- Vous pouvez également regrouper temporairement toutes les charges de travail qui sont membres de la portée associée à l'espace de travail (« charges de travail internes ») en une seule grappe, approuver la grappe, puis découvrir les politiques. Là encore, l'ensemble des politiques est réduit, car il n'y a pas de regroupement (subdivision de l'espace de travail/de la portée). Vous pouvez donc voir les politiques internes (connexion à des charges de travail internes) ou externes (connexion d'une charge de travail interne à une charge de travail externe). Ultérieurement, vous pourrez afficher des politiques de plus en plus affinées en dissociant les charges de travail internes et en disposant une ou plusieurs portées d'intérêt externes au-dessus de la racine.
- **important** Examinez toujours attentivement les politiques impliquant la portée racine, car ces politiques autorisent tout le trafic vers et à partir de l'ensemble du réseau. Cela est particulièrement important lorsque la portée racine est placée en bas de la liste des dépendances externes et que vous n'avez pas l'intention de générer des politiques générales. De telles politiques peuvent ne pas avoir résulté du trafic à l'échelle du réseau entrant ou sortant de la portée de l'espace de travail. Elles peuvent plutôt être déclenchées par quelques points terminaux externes qui n'ont pas réussi à recevoir des portées plus précises ou des affectations de filtres d'inventaire au-delà de la simple portée racine.

  Lors de l'audit de ces politiques, vous devez examiner les conversations associées (voir la section Conversations) pour identifier ces points terminaux, puis les classer en portées plus fines ou en filtres d'inventaire, pour éviter des politiques moins sécurisées au niveau de la portée racine.

Ajuster les dépendances externes d'un espace de travail

Cette procédure permet de créer des politiques entre des sous-ensembles spécifiés de charges de travail au sein de portées (plutôt qu'entre des portées entières) lors de la découverte automatique de politiques, lorsque le fournisseur d'une politique appartient à une portée différente de celle dans laquelle les politiques sont découvertes.

Illustration 9 : Réglage fin des dépendances externes



Avant de commencer

- Configurez un filtre d'inventaire pour chaque sous-ensemble de charges de travail pour lequel vous souhaitez générer des politiques spécifiques. Vous pouvez créer n'importe quel nombre de filtres d'inventaire, dans n'importe quelle portée.

  Il existe plusieurs façons de créer des filtres d'inventaire :

  - Convertir les grappes d'intérêt en filtres d'inventaire.

    (voir Convertir une grappe en filtre d'inventaire, à la page 82),

    et/ou

  - Créez de nouveaux filtres d'inventaire.

    Consultez Créer un filtre d'inventaire.

  Ces filtres doivent avoir les options suivantes activées :

  - **Restrict query to ownership scope** (Limiter la requête à la portée de la propriété)

    Provides a service external of its scope (Fournit un service hors de sa portée)

- Consultez aussi Conseils pour l'exploration des dépendances externes, à la page 35.

Procédure

Étape 1 Accédez à l'espace de travail dans lequel vous découvrirez les politiques.

Étape 2 Cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques).

Étape 3 Cliquez sur **External Dependencies** (Dépendances externes).

Étape 4 Si nécessaire, cliquez sur **Show All scopes** (Afficher toutes les portées).

Étape 5 (Facultatif) Exploitez les configurations précédentes :

- Pour réutiliser les modifications que vous avez apportées à la liste la dernière fois que vous avez détecté les politiques, cliquez sur **Previous Config** (Configuration précédente).
- Si vous avez configuré des dépendances externes dans la configuration par défaut de découverte des politiques par défaut, vous pouvez utiliser la liste globale en cliquant sur **Default Config** (Configuration

par défaut). Ou, après avoir obtenu la liste par défaut, vous pouvez la modifier comme vous le souhaitez (pour cet espace de travail uniquement), puis utiliser la version personnalisée lors des exécutions suivantes en cliquant une fois sur **Previous Config** (Configuration précédente).

Étape 6 Réorganiser les portées (et les filtres d'inventaire, le cas échéant) selon les besoins.

La politique est appliquée sur la base de la première portée ou du premier filtre d'inventaire de la liste (en commençant par le haut) qui correspond au trafic. À cette fin, vous souhaitez généralement appliquer la politique la plus spécifique qui corresponde au trafic, et vous voulez donc que les portées enfant (plus spécifiques) soient placées au-dessus de leurs parents (moins spécifiques).

- Si vous avez récemment créé de nouvelles portées enfants, qui sont par défaut ajoutées au bas de la liste, réorganisez la liste entière pour placer les portées enfants au-dessus de leurs parents :

  (Recommandé) Cliquez sur **Reorder Naturally** (Réorganiser naturellement).

  Illustration 10 : Réorganiser naturellement

- (Si vous avez une raison précise) Pour réorganiser la liste manuellement :
  - Cliquez sur **Drag and Drop** (Glisser et déposer).
  - Cliquez **By Number** (Par numéro) :

    Les dépendances externes se verront attribuer des valeurs de priorité par multiples de 10. Modifiez les valeurs pour modifier l'ordre.

    Une fois les numéros modifiés, cliquez sur **View** (afficher) pour mettre à jour l'ordre de la liste et réaffecter des multiples de 10 à chacune des priorités.

Étape 7 Précisez la granularité pour chaque ligne :

- Cliquez sur **Fine** (fine) pour chaque ligne pour laquelle vous souhaitez générer des politiques spécifiques aux filtres d'inventaire ou aux grappes configurés.

  Cliquez sur **Coarse** (grossière) pour générer des politiques qui s'appliquent à l'ensemble de la portée.

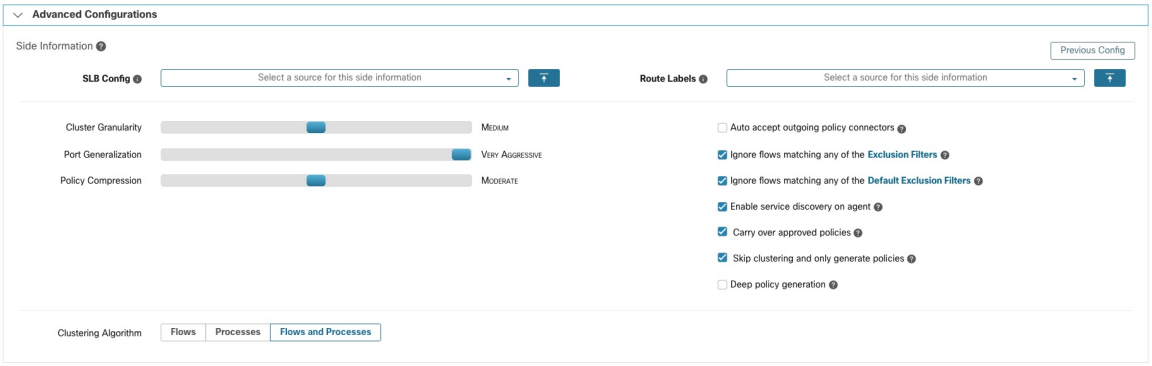
- Pour appliquer la granularité à toutes les sous-portées d'une portée : Cliquez sur le ··· situé à la fin de la ligne de la portée.

Configurations avancées pour la découverte automatique des politiques

Utilisez les paramètres avancés pour inclure des informations supplémentaires lors de la découverte de politiques ou pour vous adapter à un environnement particulier.

- Pour accéder à ces paramètres pour un espace de travail spécifique, cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques) dans l'espace de travail applicable.
- Pour modifier les valeurs par défaut de tous les espaces de travail, consultez Configuration de la découverte de politiques par défaut, on page 49.

Figure 11: Configurations avancées de découverte automatique des politiques



Inclure les données des équilibreurs de charge et des routeurs lors de la découverte des politiques

Vous pouvez charger des données à partir d'équilibreurs de charge et de routeurs pour fournir des éléments à la découverte automatique des politiques.

Pour accéder aux options suivantes, cliquez sur **Advanced Configurations** (Configurations avancées) dans les paramètres de découverte automatique des politiques et consultez la section « Side Information » ou « sideinfo » (Renseignements complémentaires).

Option	Description
Configuration SLB (Télécharger les configurations de l'équilibreur de charge)	Pour télécharger des données de votre équilibreur de charge dans le format correct, consultez Récupération des configurations de LoadBalancer pour la configuration de découverte avancée de politiques. Formats pris en charge pour le chargement des configurations de l'équilibreur de charge : • **F5 BIG-IP** • **Citrix Netscaler** • **HAProxy** • Autres : Utilisez le schéma **JSON normalisé**. Vous devez convertir toute configuration d'équilibreur de charge non prise en charge dans ce schéma. Ce schéma simple comprend des informations de base sur les adresses IP virtuelles (VIP) et les adresses IP principales. Pour télécharger un exemple de fichier JSON, cliquez sur le bouton d'informations à côté de **SLB Config** (Configuration SLB).
Charger des **étiquettes de routage**	Vous pouvez téléverser une liste de sous-réseaux/routes mis à disposition à partir des routeurs pour aider à partitionner les hôtes en fonction d'un ensemble de sous-réseaux pré-mis à disposition. Les résultats de mise en grappe générés par la découverte automatique des politiques ne dépassent jamais les limites du sous-réseau telles que définies par les données téléversées. Vous pouvez modifier les résultats une fois la découverte automatique des politiques terminée. Pour télécharger un exemple de fichier JSON, cliquez sur le bouton Renseignements à côté de **Route Labels** (étiquettes de routage).

Note Les grappes ne franchissent pas les limites des partitions, ce qui signifie qu'une grappe calculée par la découverte automatique de politiques ne contient pas de charges de travail cibles provenant de deux partitions différentes. Les partitions sont calculées à partir des données de l'équilibreur de charge ou du routeur téléversées. Cependant, vous pouvez déplacer librement les charges de travail d'une grappe à une autre, par exemple en modifiant les définitions de requête de grappe (modification manuelle de la grappe), ou désactiver le chargement de toutes les informations complémentaires.

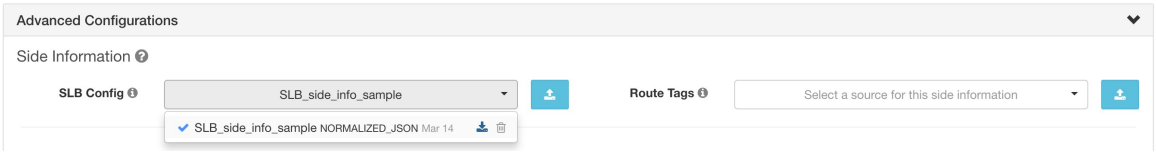
Pour afficher ou supprimer un fichier d'équilibreur de charge (configuration SLB) ou d'étiquettes de routage précédemment téléversé :

1. Cliquez dans la zone respective intitulée **Select a source for this side information** (Sélectionnez une source pour ces informations complémentaires).

   Une liste des fichiers téléversés apparaîtra.

2. Cliquez sur l'icône de téléchargement ou de corbeille à côté du fichier à afficher ou à supprimer.

Figure 12: Informations complémentaires téléversées



Granularité de la grappe

La granularité de la mise en grappe vous permet de contrôler la taille des grappes générées par la découverte automatique des politiques.

- **Fine** entraîne la formation d'un plus grand nombre de grappes, mais de taille plus réduite
- **Grossière** entraîne une diminution du nombre de grappes, mais une augmentation de leur taille

Note Vous pourriez ne pas observer de changement important dans les résultats en raison de nombreux autres signaux pris en compte par nos algorithmes. Par exemple, si le niveau de confiance des grappes générées est très élevé, la modification de ce contrôle modifiera peu les résultats.

Généralisation des ports

L'option de **Port Generalization** (généralisation de ports) dans **Advanced Configurations** (configurations avancées) pour la découverte automatique des politiques contrôle le niveau de signification statistique requis lors de la généralisation de ports, c'est-à-dire le remplacement de nombreux ports utilisés comme ports de serveur sur une seule charge de travail par un intervalle de port.

Ce paramètre peut avoir une incidence sur la précision, le nombre et la compacité des politiques ainsi que sur le temps nécessaire à leur génération.

Pour désactiver la généralisation de port, déplacez le curseur vers l'extrémité gauche. Notez que si elle est désactivée, la découverte automatique des politiques ou le temps de rendu de l'interface utilisateur de découverte automatique des politiques peut être considérablement réduit, si de nombreux ports de serveur sont utilisés par les charges de travail.

À mesure que le curseur se déplace vers la droite vers une généralisation plus audacieuse, moins de preuves sont nécessaires pour créer des intervalles de port et le critère de remplacement des politiques d'origine (impliquant des ports uniques) par des intervalles de port est assoupli.

Contexte

Certaines applications comme Hadoop utilisent et modifient de nombreux ports de serveur à un certain intervalle, par exemple entre 32000 et 61000. La découverte automatique des politiques tente de détecter ce comportement pour chaque charge de travail, en utilisant l'utilisation des ports de serveur de la charge de travail dans les flux observés : en observant seulement une fraction du total des ports possibles (mais de nombreux ports, par exemple des centaines), la découverte automatique des politiques peut « généraliser » que n'importe quel port entre, par exemple, 32000 et 61000, pourrait être utilisé comme port de serveur par la charge de travail. Les ports qui se trouvent à l'intérieur des intervalles sont remplacés par ces intervalles (lorsque certains critères relatifs aux nombres minimums observés sont remplis). Cela se traduit par moins de

politiques plus compactes. L'estimation de l'intervalle est importante pour le calcul de politiques précises : sans généralisation suffisante, de nombreux flux futurs légitimes seraient abandonnés si la politique est appliquée. En fusionnant de nombreux ports en un seul ou plusieurs intervalles, le temps de rendu de l'interface utilisateur est également considérablement réduit.

Vous pouvez contrôler le degré de généralisation des ports, y compris en le désactivant.

Compression des politiques

Lorsque la compression des politiques est activée, si les politiques de plusieurs grappes de l'espace de travail sont similaires, elles peuvent être remplacées par une ou plusieurs politiques applicables à l'ensemble de l'espace parent. Par exemple, si toutes ou presque les grappes de l'espace de travail fournissent le même port au même consommateur, toutes ces politiques spécifiques aux grappes sont remplacées par une seule politique dans la portée parente. Cela réduit considérablement le nombre de politiques, l'encombrement et peut également permettre des flux futurs légitimes qui auraient été abandonnés (généralisation précise).

Plus le paramètre de compression est élevé, plus le seuil requis pour la fréquence des politiques est bas afin de remplacer les politiques spécifiques aux grappes par une politique applicable à l'ensemble du parent.

Lors de la génération de politiques pour une branche de l'arborescence de la portée :

Ce bouton peut être utilisé pour modifier le niveau de Compression hiérarchique des politiques.

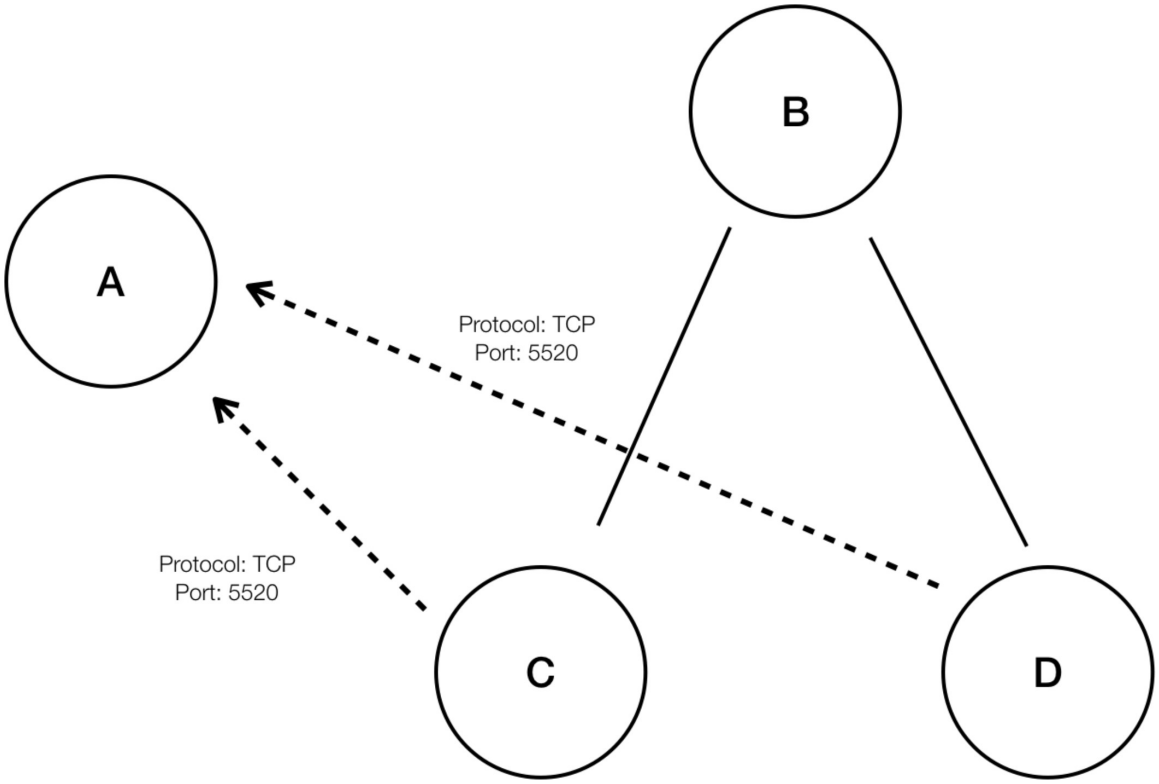
Note Actuellement, la page des conversations de découverte automatique des politiques ne permet pas d'afficher les conversations qui ont conduit à une politique compressée (vous devrez peut-être désactiver la compression ou utiliser la recherche de flux).

Compression hiérarchique des politiques

La compression des politiques peut également être effectuée lors de la génération de politiques pour une branche de l'arborescence de la portée. Le bouton Compression des politiques (Compression des politiques) peut être utilisé pour modifier le niveau de compression hiérarchique des politiques. Un exemple de compression hiérarchique des politiques est illustré ci-dessous.

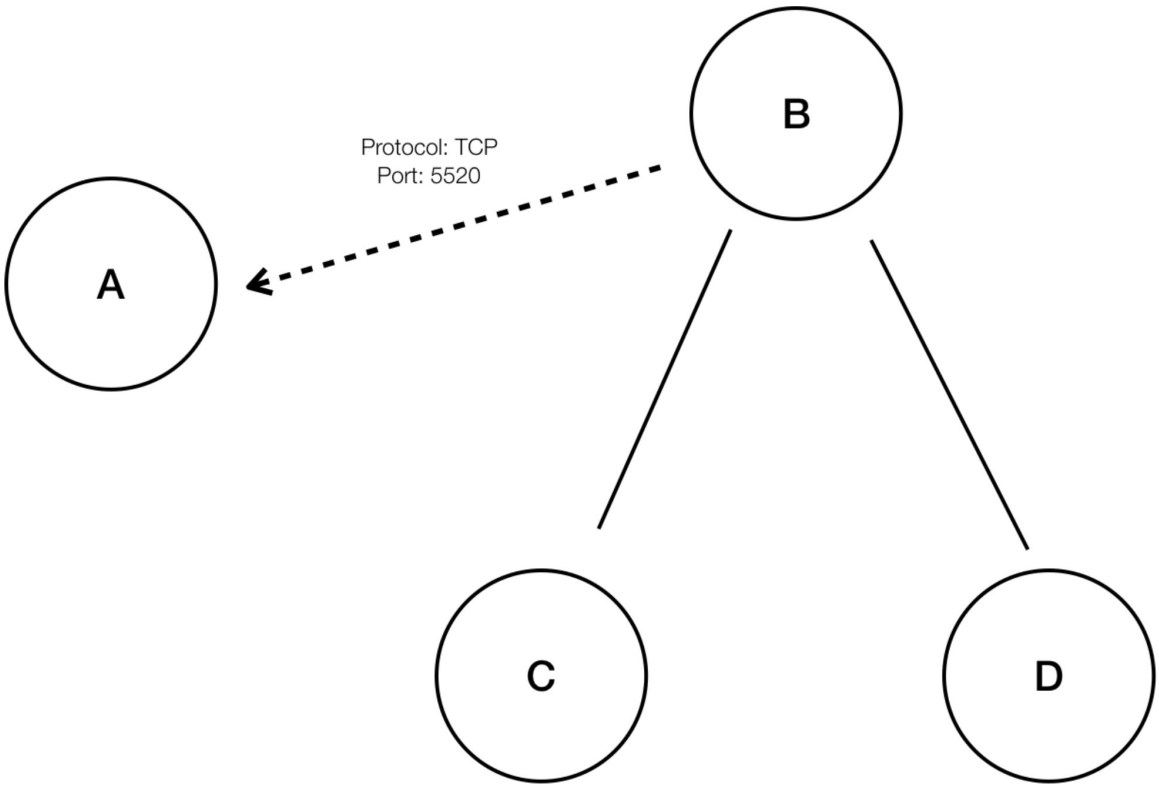
- Soit A, B, C et D, des portées faisant partie d'une arborescence de portées, où « C » et « D » sont les portées enfants de « B ». Soit « C » → » « A » soit une politique TCP « ALLOW (AUTORISER) » sur le port 5520 et « D » → » « A » soit la politique TCP « ALLOW » sur le port 5520.

Figure 13: Avant la compression hiérarchique des politiques



- Avec la compression hiérarchique des politiques, si un groupe suffisamment important de portées enfants implique des politiques partageant le même port, le même protocole et la même destination ou source, ces politiques seront remplacées par une politique généralisée qui relie la portée parente à la source ou à la destination commune. Dans le cas mentionné ci-dessus, « C » et « D » sont les portées enfants de « B » et les politiques « C » → » « A » et « D » → » « A » partagent la même destination, le même port et le même protocole. Étant donné que 100 % des portées enfants de « B » contiennent la politique similaire, la politique sera promue comme suit : « B » → » « A ». En outre, la compression hiérarchique peut être répétée afin qu'une politique généralisée puisse aller jusqu'à la racine de la sous-arborescence (branche de l'arborescence de la portée) .

Figure 14: Après la compression hiérarchique de la politique



- Le bouton Policy Compression (Compression de la politique) vous permet d'ajuster le degré de cette compression, en modifiant la proportion minimale requise des portées enfants partageant la politique (généralement mesurée en tant que fraction du nombre total de portées enfants) pour déclencher la compression. Lorsque cette option est désactivée, chaque politique est générée entre les portées de priorité la plus élevée en fonction de la liste des dépendances externes. Par la suite, si vous choisissez la liste des dépendances externes ordonnée naturellement, les politiques générées seront les politiques les plus granulaires parmi les portées.

Algorithme de mise en grappe (entrée de la mise en grappe)

Les utilisateurs avancés peuvent choisir la principale source de données pour les algorithmes de mise en grappe, c'est-à-dire les flux réseau en direct, ou l'exécution de processus, ou les deux.

Accepter automatiquement les connecteurs de politique sortants

Cette option s'applique uniquement lorsque vous utilisez la découverte automatique des politiques pour créer des politiques inter-portées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 95.

Toutes les demandes de politique sortantes créées lors de la découverte automatique des politiques sont automatiquement acceptées.

Pour obtenir des renseignements complets, consultez Connecteurs de politiques d'acceptation automatique, on page 104 et la section Demandes de politiques.

Note Cette option est uniquement disponible pour les propriétaires de portée racine et les administrateurs de site.

Approuver automatiquement les politiques générées

Cette option est applicable si vous souhaitez approuver toutes les politiques générées par la découverte de politiques.

Note Sachez que si vous choisissez cette option, et plus tard si vous devez modifier ou annuler des modifications, vous ne pourrez le faire que manuellement.

Pour en savoir plus, consultez les Connecteurs de politiques d'acceptation automatique, on page 104 et Demandes de politiques.

Note Cette option est disponible pour les propriétaires de portée racine et les administrateurs de site.

Ignorer les flux correspondants à des filtres d'exclusion

Pour ignorer les flux de conversation que vous spécifiez, activez l'option applicable. Pour afficher ou modifier l'une ou l'autre des listes de filtres, cliquez sur le lien **Exclusion Filters** (Filtres d'exclusion) applicables. Pour en savoir plus, consultez Filtres d'exclusion, Filtres d'exclusion par défaut, on page 50 et Configurer, modifier ou supprimer les filtres d'exclusion, on page 32.

Activer la découverte de service sur l'agent

Dans certaines applications, une large gamme de ports peut être désignée pour être utilisée, mais le trafic réel peut n'utiliser qu'un sous-ensemble de ces ports pendant la période de temps incluse dans la découverte de la politique. Cette option permet d'inclure l'ensemble du regroupement de ports désignés pour ces applications dans des politiques applicables à ces applications, plutôt que seulement les ports observés dans le trafic réel.

L'activation de cette option permet de recueillir des renseignements relatifs aux plages de ports éphémères concernant les services présents sur le nœud de l'agent. Des politiques sont ensuite générées en fonction de ces informations de plage de ports.

Exemple :

- Le serveur de domaine Windows Active Directory utilise la plage de ports éphémères Windows par défaut **49152 à 65535** pour traiter les demandes. Lorsque cet indicateur est défini, l'agent envoie des renseignements sur la plage de ports, et des politiques sont générées en fonction de ces informations.

Figure 15: Découverte de service activée sur l'agent

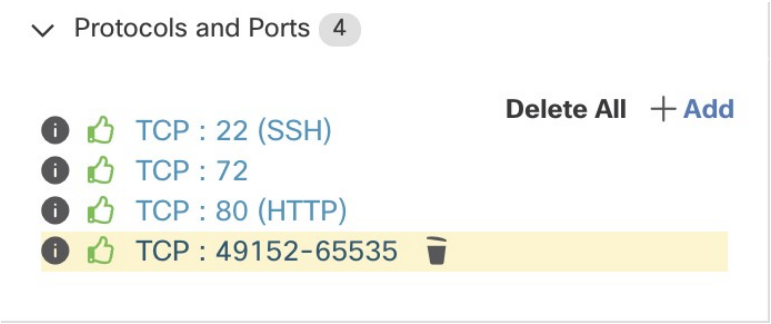
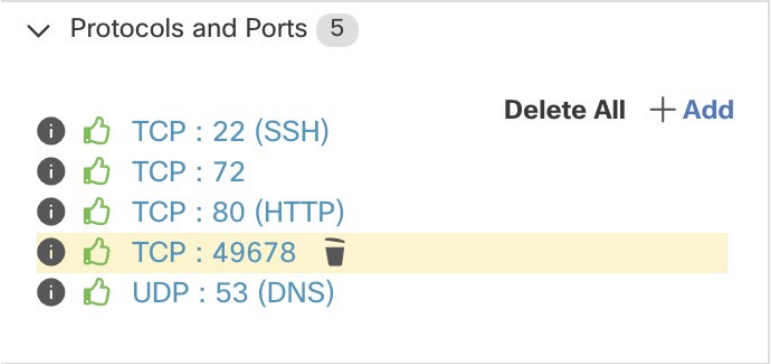


Figure 16: Découverte de service non activée sur l'agent



Reporter des politiques approuvées

Par défaut, cette option est activée.

Lorsque cet indicateur est défini, toutes les politiques que vous avez marquées comme approuvées (y compris celles approuvées à l'aide d'OpenAPI) seront conservées. Cela vous évite d'avoir à redéfinir une règle DENY de refus large particulière qui devrait prendre effet quelles que soient les politiques d'autorisation ALLOW détectées par la découverte automatique de politiques.

Pour de plus amples renseignements, consultez la section Politiques approuvées, on page 51.

Ignorer la mise en grappe et générer uniquement les politiques

Si cette option est sélectionnée, aucune nouvelle grappe n'est générée et les politiques sont générées à partir de toutes les grappes ou filtres d'inventaire approuvés existants et concernent l'ensemble de la portée associée à l'espace de travail (ce qui revient à traiter l'ensemble de la portée comme une seule grappe). Cette option permet de réduire considérablement le nombre de politiques (mais de les rendre plus approximatives).

Activer la suppression des politiques redondantes

Cette option n'est disponible que lors de la génération de politiques pour une branche de l'arborescence de la portée.

Cette option active/désactive la suppression des politiques granulaires redondantes.

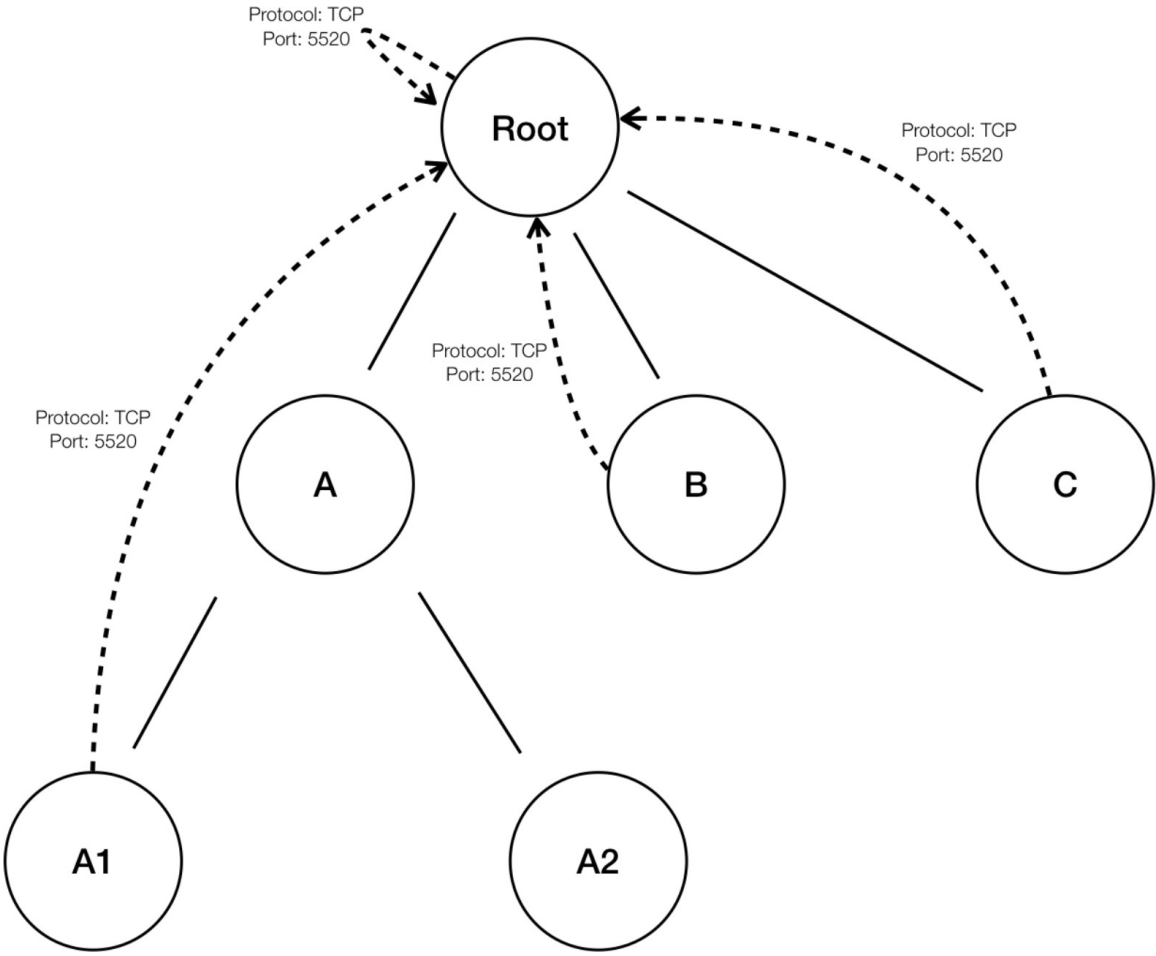
Exemple :

- Soit la racine Root, A, B, C, A1 et A2 des portées faisant partie d'une arborescence de portées. Soit les politiques suivantes :

  1. « Root » → « Root »
  2. « B » → « Root »
  3. « C » → « Root »

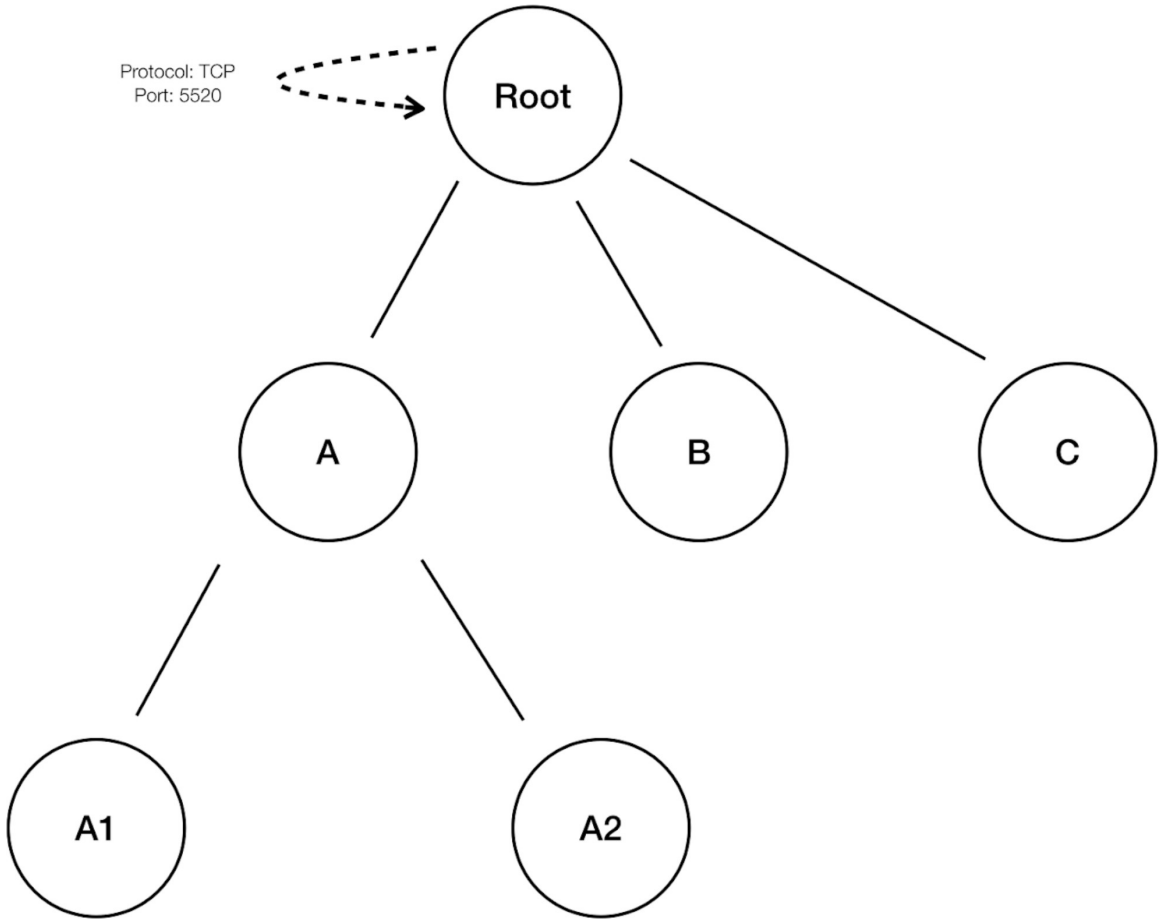
  4. « A1 » → « Root »

Figure 17: Avant la suppression des politiques redondantes



- Les politiques « B » →« Root », « C » →« Root » and « A1 »→ « Root » sont redondantes, car la politique « Root »→« Root » couvre ces politiques. La fonction de suppression des politiques redondantes vérifie et supprime ces politiques. Il n'y a donc qu'une seule politique, « Root »→ « Root », comme suit.

Figure 18: Après la suppression des politiques redondantes



La suppression des politiques redondantes peut être très utile pour conserver un ensemble succinct de politiques interprétables. L'ensemble de politiques réduit contient le nombre minimal de politiques au niveau de compression choisi pour couvrir tout le trafic de charge de travail. Cependant, vous devez toujours effectuer un audit de la politique au moyen d'une analyse des politiques et examiner les conversations correspondantes pour évaluer le caractère strict des politiques qui en résultent. Cela est particulièrement important lorsqu'il existe un trafic à destination ou en provenance des points terminaux qui ne sont pas classés dans des portées plus précises ou des filtres d'inventaire. Ces points terminaux peuvent déclencher la génération de politiques plus globales que prévu, comme des politiques impliquant la portée racine. Si la suppression des politiques redondantes est activée en même temps, les politiques plus granulaires seront supprimées et ne vous seront pas présentées. Pour diagnostiquer la source des politiques (compressées) et pour afficher les politiques de niveau plus précis, désactivez la compression des politiques et la suppression des politiques redondantes. Notez également qu'actuellement, la page des conversations de découverte automatique des politiques peut ne pas afficher les conversations qui mènent à une politique compressée/généralisée. Pour contourner ce problème, vous pouvez désactiver la compression et la suppression des politiques redondantes, afin qu'il soit plus facile de trouver les conversations qui mènent aux politiques générées.

Tip Étant donné que la - en découvrant les politiques pour une branche de l'arborescence de l'espace de travail - découvre toutes les politiques pour le sous-arborescence de l'espace de travail ayant pour racine l'espace de travail, ces politiques couvriront tout le trafic légal vu par la découverte automatique de politiques pour toutes les charges de travail sous la sous-arborescence. Lorsque vous analysez ces politiques à l'aide d'outils comme l'analyse des politiques (voir l'article sur les politiques), vous devez désactiver l'analyse des politiques dans tous les espaces de travail associés aux sous-portées. De cette façon, les politiques (le cas échéant) résidant dans les espaces de travail de sous-portée (qui reçoivent généralement une priorité élevée en raison d'une définition de portée plus spécifique) ne seront pas prioritaires et n'interféreront pas avec les résultats. Cependant, des exceptions s'appliquent lorsque les politiques des espaces de travail de sous-portée sont configurées pour couvrir différents ensembles de trafic qui impliquent généralement des filtres d'inventaire plus fins ou des grappes spécifiques aux sous-portées.

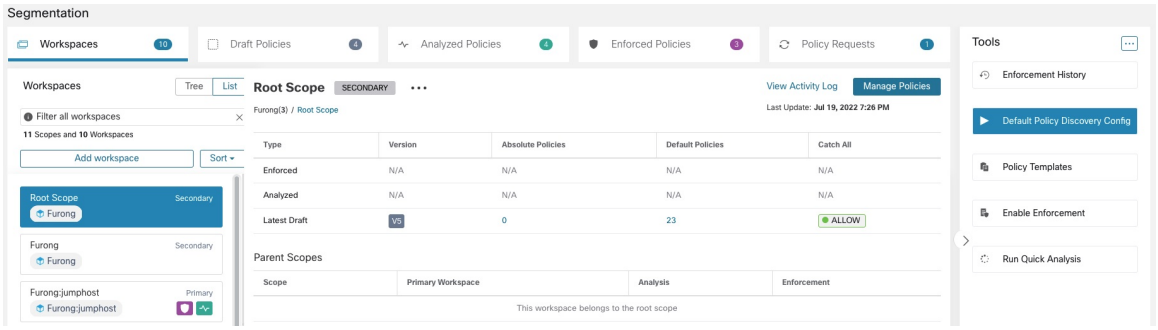
Configuration de la découverte de politiques par défaut

Vous pouvez configurer les paramètres de découverte automatique des politiques par défaut qui peuvent éventuellement être utilisés dans n'importe quel espace de travail dans l'ensemble de la portée racine.

Pour configurer les options par défaut pour la découverte de politiques :

Choisissez **Defend** > **Segmentation** (défendre la segmentation), puis cliquez sur le signe d'insertion dans la partie droite de la page pour développer le menu Tools (outils). Choisissez ensuite **Default Policy Discovery Config** (Configuration de la découverte des politiques par défaut).

Figure 19: Accès à la page de configuration de la découverte des politiques par défaut



Pour en savoir plus sur les options de la page de configuration de la découverte des politiques par défaut, consultez :

- Dépendances externes, on page 34 et les rubriques secondaires
- Configurations avancées pour la découverte automatique des politiques, on page 39 et les rubriques secondaires
- Filtres d'exclusion par défaut, on page 50

Important Lorsque vos configurations par défaut sont terminées et prêtes à l'utilisation dans des espaces de travail individuels, cliquez sur **Save** (Enregistrer).

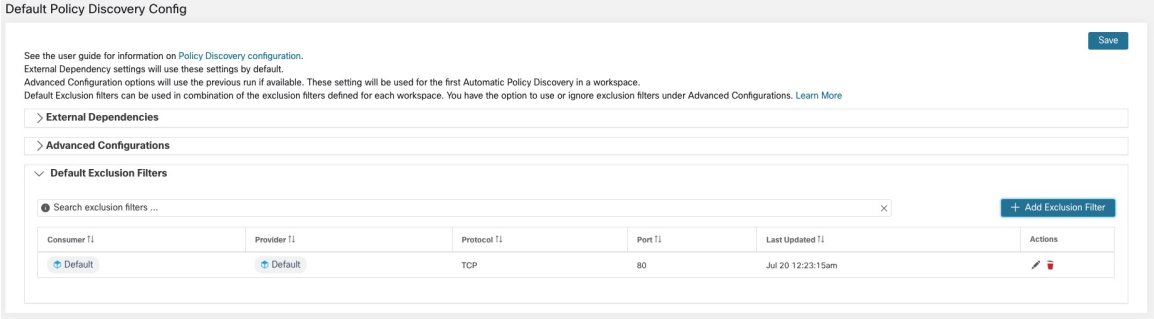
Filtres d'exclusion par défaut

Les filtres d'exclusion vous aident à affiner les politiques et les grappes suggérées par la découverte automatique des politiques en spécifiant les flux de trafic à exclure de l'entrée de la découverte.

Pour en savoir plus, consultez les Filtres d'exclusion.

Vous pouvez créer une liste globale des filtres d'exclusion par défaut qui soit disponible pour tous les espaces de travail de votre détenteur, puis préciser pour chaque espace de travail si vous souhaitez utiliser ou non cette liste par défaut lors de la découverte des politiques.

Figure 20: Filtres d'exclusion par défaut



Pour configurer les filtres d'exclusion par défaut, consultez Configurer, modifier ou supprimer les filtres d'exclusion, on page 32.

Pour activer ou désactiver les filtres d'exclusion par défaut, consultez Activer ou désactiver les filtres d'exclusion, on page 34.

Récupération des configurations de LoadBalancer pour la configuration de découverte avancée de politiques

Vous trouverez ci-dessous des instructions pour récupérer les fichiers de configuration d'équilibreur de charge pris en charge dans un format qui peut être directement téléversé dans Cisco Secure Workload pour une utilisation dans la découverte de politiques. Pour en savoir plus, consultez les sections Configurations avancées pour la découverte automatique des politiques et Inclure les données des équilibreurs de charge et des routeurs lors de la découverte des politiques, on page 39.

Notez que tous les fichiers doivent être encodés en ASCII.

Citrix Netscaler

Concaténez la sortie de `show run` dans votre console et téléchargez le fichier.

Voir un exemple de fichier de configuration

F5 BIG-IP

Chargez le fichier `bigip.conf`.

Note Si vous possédez un fichier avec une extension .UCS, décompressez le dossier d'archive et chargez uniquement le `fichier bigip.conf` dans la vidage de configuration. S'il existe plusieurs `fichiers bigip.conf`, concaténez-les, puis téléchargez-les.

Voir un exemple de fichier de configuration

HAProxy

Chargez votre fichier `haproxy.cfg`. Le chemin d'accès est généralement `/etc/haproxy/haproxy.cfg`.

Voir un exemple de fichier de configuration

JSON normalisé

Si vous trouvez que les options ci-dessus sont contraignantes, convertissez vos configurations selon le schéma JSON suivant et téléversez-les directement. L'exemple de fichier JSON peut être téléchargé directement en cliquant sur l'icône **i** à côté de Configuration SLB Config dans Configurations d'exécution avancées pour la découverte automatique des politiques.

Voir un exemple de fichier de configuration

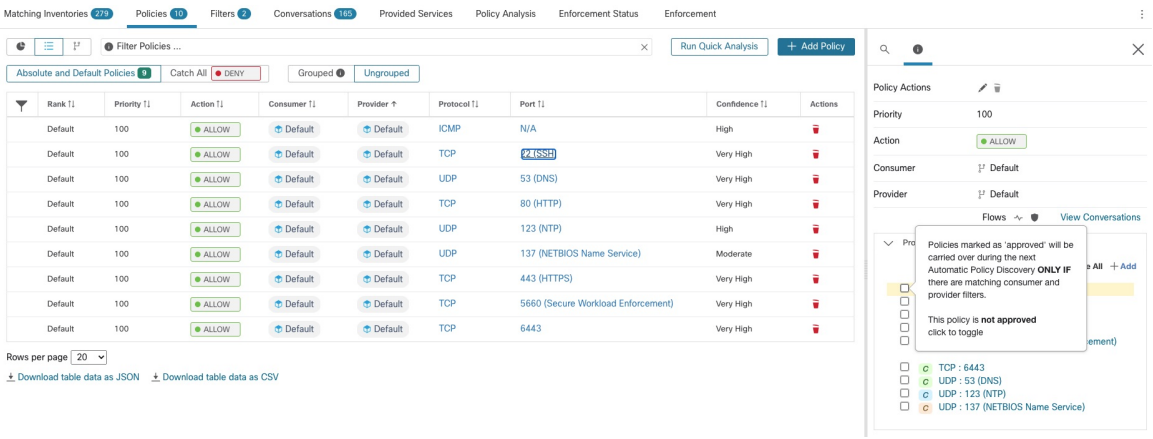
Approuver les politiques

Lorsque vous passez en revue les résultats de la découverte des politiques, approuvez les politiques découvertes que vous souhaitez conserver pour les conserver telles quelles lorsque vous découvrirez des politiques ultérieurement. Pour en savoir plus, consultez Politiques approuvées, à la page 51.

Pour approuver une politique :

1. Dans la page Policies (Politiques), pour la politique que vous souhaitez protéger, cliquez sur la valeur dans la colonne **Protocols and Ports** (Protocoles et Ports).
2. Dans le panneau qui s'ouvre sur la droite, cochez la case à gauche de chaque protocole et port pour lesquels vous souhaitez conserver la politique lors de la découverte future de politiques.

Illustration 21 : Approuver les politiques



Vous pouvez également utiliser cette procédure pour supprimer l'approbation d'une politique.

Politiques approuvées

En général, les politiques approuvées ne sont pas modifiées lors de la recherche automatique de politiques, et cette dernière ne suggère pas de politiques qui feraient double emploi ou chevaucheraient les effets des politiques approuvées.

Les politiques suivantes sont approuvées :

- Les politiques créées manuellement.

- Les politiques découvertes qui sont approuvées manuellement

  (Lorsque vous êtes convaincu qu'une politique se comporte comme prévu, vous l'approuvez pour la protéger contre les modifications lors de la future découverte automatique des politiques. Voir Approuver les politiques, on page 51).

- Politiques téléversées, à moins qu'elles ne soient explicitement marquées comme `approuvées : faux`.

- Les politiques approuvées qui sont définies dans les portées parent et ancêtre (en particulier, à partir des dernières versions de leurs espaces de travail principal) qui s'appliquent aux charges de travail de cette portée.

- Les politiques créées lorsque des demandes de politique sont acceptées à partir d'un autre espace de travail, lorsque des politiques à portée croisée sont gérées à l'aide de la méthode avancée décrite dans Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, on page 94. Par exemple, cela inclut les politiques incluses à partir de l'onglet Services fournis, on page 106.

Les politiques approuvées sont accompagnées d'une icône représentant un pouces vers le haut à côté du type de protocole lorsque vous cliquez sur les liens des ports ou des protocoles d'une politique et que vous affichez les détails dans le panneau à droite de la page.

Exceptions aux protections de politiques approuvées

Les politiques approuvées sont conservées lors de la découverte automatique future des politiques si *les deux* extrémités de la politique sont parmi les suivantes : grappe approuvée; filtre d'inventaire; demande de politique acceptée (pour les politiques couvrant plusieurs portées); ou grappe qui ne modifie pas de manière significative les membres. (Cependant, les membres de la grappe peuvent avoir changé dans le dernier cas).

Les politiques approuvées pourraient ne pas être protégées lors des futures exécutions de découverte automatique des politiques si l'une des extrémités des politiques est une grappe qui n'est pas approuvée et si, lors de la découverte automatique des politiques, aucune nouvelle grappe générée ne présente un chevauchement suffisamment élevé avec cette grappe.

Pour protéger une politique qui implique une grappe non approuvée, vous devez approuver explicitement les grappes à chaque extrémité de la politique.

Il existe également une configuration avancée pour la découverte automatique des politiques qui est activée par défaut. Si vous ne souhaitez pas protéger les politiques approuvées contre les modifications, vous pouvez désélectionner cette option pour un espace de travail ou pour la configuration de découverte de politiques par défaut globale :. Consultez Reporter des politiques approuvées, on page 46.

Dépanner les politiques approuvées

Les politiques approuvées ne sont pas reportées

Si les politiques approuvées ne sont pas reportées comme prévu, assurez-vous que l'option de report **des politiques approuvées** est sélectionnée dans les paramètres de configuration avancés ou par défaut pour la découverte automatique des politiques.

Trouver les conversations exclues de la génération de politiques

Lors de la découverte automatique des politiques, toutes les conversations correspondant aux critères d'une politique approuvée existante sont exclues de la génération de politique. Cette omission empêche la génération de politiques redondantes couvrant les mêmes conversations. (Ce processus diffère des filtres d'exclusion

(voir la section Filtres d'exclusion), dans laquelle vous définissez des filtres de correspondance au lieu de politiques. Les filtres d'exclusion empêchent les conversations correspondantes d'être visibles dans toutes les parties de la découverte automatique des politiques.)

Notez que même si des politiques redondantes ne sont pas générées à partir de ces conversations, celles-ci sont toujours prises en compte lorsque la découverte automatique des politiques analyse et génère des grappes.

Pour voir quelles conversations sont exclues de la découverte automatique des politiques par les politiques approuvées existantes :

Dans l'affichage des conversations (voir l'article Conversations), utilisez l'indicateur d'**exclusion** pour filtrer les conversations. Vous pouvez également voir quelles politiques approuvées existantes entraînent l'exclusion de ces conversations dans la vue détaillée de la politique qui s'ouvre sur le côté droit de la page lorsque vous cliquez sur le lien Ports et protocoles dans une politique, puis sur l'icône d'exclusion à côté de la conversation. (Survolez les icônes pour trouver l'icône appropriée).

Réviser les politiques de manière itérative

La définition et la précision des politiques, pour une portée unique et pour l'ensemble d'un réseau, constituent un processus itératif.

Vous pouvez vous attendre à réviser à la fois les politiques découvertes et celles créées manuellement.

Réexécution de la découverte automatique des politiques

Vous pouvez réexécuter la découverte automatique des politiques à tout moment. Les raisons principales de réexécuter la recherche automatique de politiques sont d'inclure des renseignements supplémentaires qui n'ont pas été inclus dans l'exécution précédente, ou d'exclure des renseignements qui ne sont pas utiles. Par exemple, vous pouvez :

- Installer des agents supplémentaires ou configurer des connecteurs supplémentaires et permettre à certaines données de flux de s'accumuler.
- Augmenter la durée utilisée pour la découverte, afin d'inclure davantage de données.
- Approuver les grappes (avec ou sans modification au préalable), ce qui peut améliorer la mise en grappe d'autres charges de travail lors de la réexécution. Consultez Approbation des grappes, on page 86.
- Exclure les flux dont vous savez que vous ne voulez pas influencer la politique afin de ne pas avoir à les supprimer. Consultez Filtres d'exclusion, on page 31.
- Modifier les paramètres avancés (pour en savoir plus, voir Configurations avancées pour la découverte automatique des politiques, on page 39).
- Capturer les modifications après avoir modifié Aborder les complexités de la politique, on page 87.

La redécouverte automatique des politiques sur un espace de travail existant peut générer des grappes et des politiques différentes dans cet espace.

Si un hôte ne fait plus partie de la portée de l'espace de travail, il n'apparaîtra dans aucune grappe lors d'une exécution de découverte automatique des politiques ultérieure; S'il se trouve dans une grappe approuvée, il n'y apparaîtra plus. Même avec le même ensemble de charges de travail de membres, mais avec une configuration différente dans le temps, la découverte automatique des politiques peut générer différentes grappes.

Note Pour obtenir la liste des types de politiques qui ne sont pas modifiés lors de la découverte de la politique, consultez Politiques approuvées, on page 51.

Note *Suppression des politiques redondantes* Lors de la découverte automatique ultérieure de politiques, les politiques approuvées dans les espaces de travail principaux supprimeront les conversations correspondantes pour la génération de politiques, de sorte que des politiques redondantes ne seront pas générées. Notez que, comme c'est le cas pour les filtres d'exclusion, cette fonctionnalité peut ne pas fonctionner parfaitement sur les espaces de travail non principaux si la politique utilise un filtre de grappe défini dans l'espace de travail. Les filtres de grappe des espaces de travail non principaux ne sont pas actifs et ne correspondront à aucun flux. Par conséquent, des politiques redondantes peuvent toujours être générées dans ces espaces de travail lors de la découverte automatique des politiques.

Important : Avant de réexécuter la découverte automatique des politiques

Important Répondez aux questions suivantes avant de relancer la découverte des politiques dans un espace de travail :

- Par défaut, chaque fois que vous découvrez des politiques dans un espace de travail particulier, l'ensemble précédent de politiques et de grappes découvertes est remplacé en fonction des données incluses dans la nouvelle période de découverte. Si vous souhaitez conserver certaines politiques et certaines grappes, mais pas d'autres, approuvez ces politiques et ces grappes.
- Si vous souhaitez conserver les grappes générées existantes, consultez Prévention de la modification des grappes lors des réexécutions de découverte automatique des politiques ou Approbation des grappes, on page 86.
- Si vous souhaitez conserver les politiques générées existantes, consultez Approuver les politiques, on page 51.
- Tous les paramètres de configuration **avancée** existants configurés lors de l'exécution de découverte précédente sont utilisés, sauf si vous les modifiez.

  Cependant, toutes les dépendances externes configurées *par défaut* seront utilisées à la place de celles de l'exécution précédente.
- Si la version actuellement affichée des politiques découvertes n'est pas la dernière version et que vous souhaitez conserver les versions précédemment découvertes, cliquez sur la version affichée en haut de la page et choisissez la dernière version v*.

  Si une version précédente est affichée, toutes les versions comprises entre cette version et la nouvelle version découverte seront supprimées.

  Pour de plus amples renseignements, consultez la section Afficher, comparer et gérer les versions de politiques découvertes, on page 55.

Pour réexécuter la découverte de politique, consultez Découvrir automatiquement les politiques, on page 28. Une fois que vous avez abordé les points de cette rubrique, le processus est le même chaque fois que vous découvrez des politiques.

Afficher, comparer et gérer les versions de politiques découvertes

Chaque fois que vous découvrez des politiques dans un espace de travail, le numéro de version (v*) affecté à l'ensemble de politiques est incrémenté.

Pour en savoir plus, consultez À propos des versions des politiques (v* et p*), à la page 147.

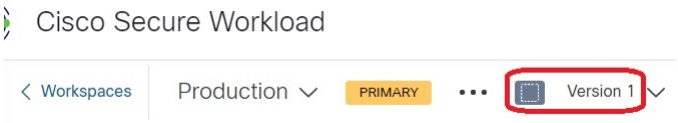
Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Accédez à l'espace de travail

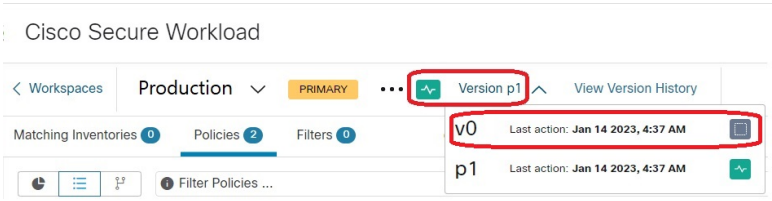
Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

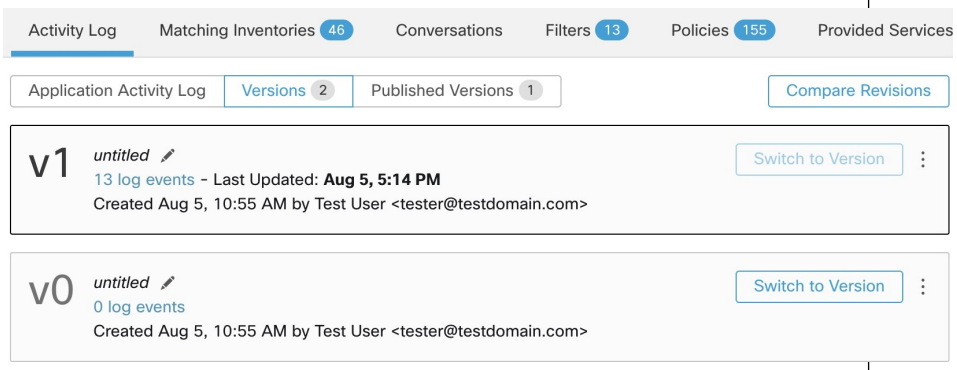
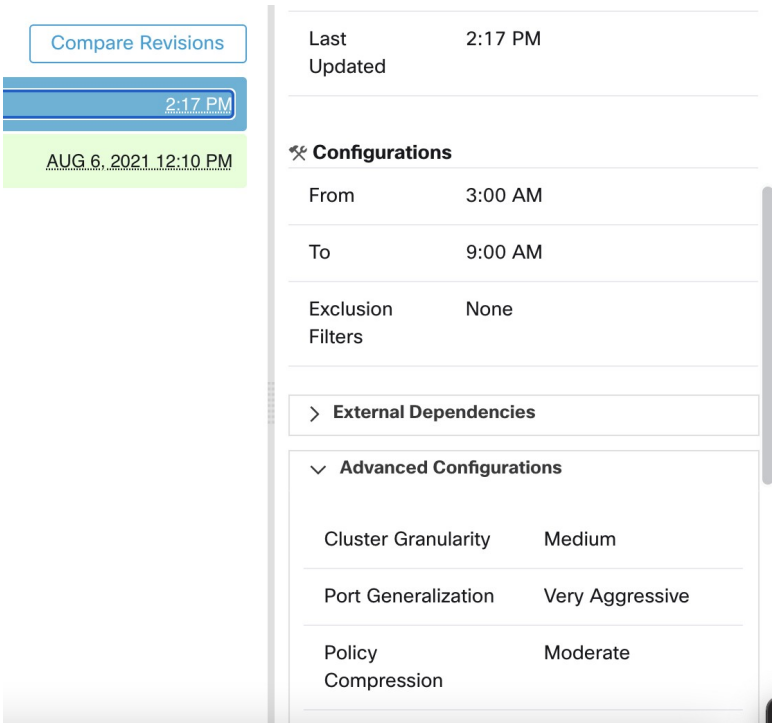
Étape 4 La version actuellement affichée des politiques générées par la découverte automatique des politiques est indiquée en haut de la page :



Si vous avez déjà analysé ou appliqué des politiques, la version affichée peut être une version de découverte de politiques, une version analysée ou une version appliquée.

Étape 5 Effectuez l'une des opérations suivantes :

Afficher une version différente des politiques générées par la découverte automatique des politiques :	Cliquez sur la version actuelle et choisissez une autre version v*. (Si des versions p* s'affichent, il s'agit de versions analysées et/ou appliquées, et non de versions des politiques découvertes).  **Important!** Consultez la mise en garde dans la section Que faire ensuite à la fin de cette procédure?

Afficher les détails d'une version	**1.** Cliquez sur **View Version History** (Afficher l'historique des versions) en haut de la page à côté dans la version actuelle. **2.** Cliquez sur l'onglet **Versions** pour voir les versions des politiques détectées. (Il ne s'agit pas de l'onglet Published Versions (Versions publiées).) La liste des versions s'affiche : ***Illustration 22 : Liste des versions de politique générées avec des renseignements résumés***  **3.** Cliquez sur le lien **log events** (journal des événements) dans la version. **4.** Cliquez sur un lien dans une ligne d'événement. Les renseignements détaillés disponibles comprennent les statistiques, les filtres d'exclusion, les dépendances externes et les configurations pour l'exécution. ***Illustration 23 : Configurations utilisées pour des exécutions particulières de découverte automatique de politiques*** 

Comparez deux versions pour voir ce qui a changé :	1. Cliquez sur **Compare Revisions** (Comparer les révisions). 2. Choisissez les versions à comparer. 3. Pour en savoir plus sur les résultats, consultez Comparaison des versions des politiques : différence de politique, à la page 149.
Supprimez une version indésirable :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Delete** (Supprimer). Vous ne pouvez pas supprimer la dernière version générée par la découverte automatique des politiques (version v*).
Exporter une version :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Export...** (Exporter...).

Prochaine étape

Important Si vous souhaitez conserver les versions précédentes des politiques découvertes, affichez toujours la version actuelle des politiques découvertes lorsque vous avez fini d'utiliser des versions plus anciennes.

Si la version la plus récente des politiques détectées ne s'affiche pas lors de la prochaine découverte des politiques pour cet espace de travail, les versions plus anciennes peuvent être supprimées.

Par exemple, si la version la plus récente des politiques découvertes est la v4 et que la version v2 s'affiche lorsque vous découvrez à nouveau des politiques, les versions v3 et v4 existantes seront supprimées, et la nouvelle version découverte sera la v3.

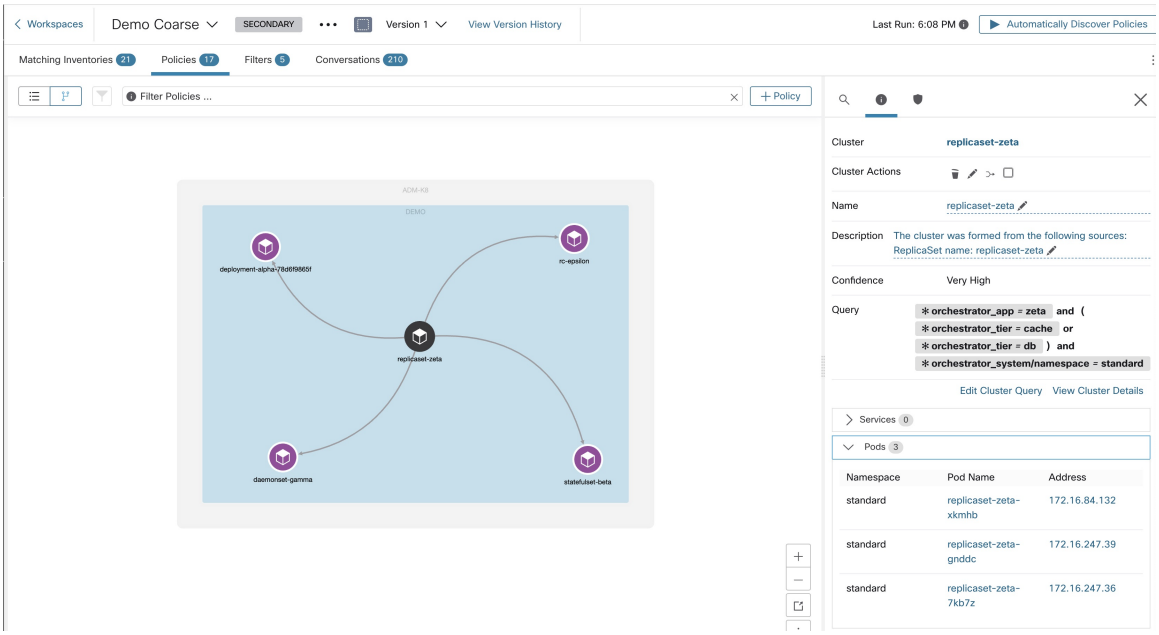
Ce comportement garantit un historique de version linéaire, ce qui simplifie le retour à une version précédente si vous le souhaitez.

En outre, vous ne pouvez créer manuellement des politiques que si la dernière version v* est affichée.

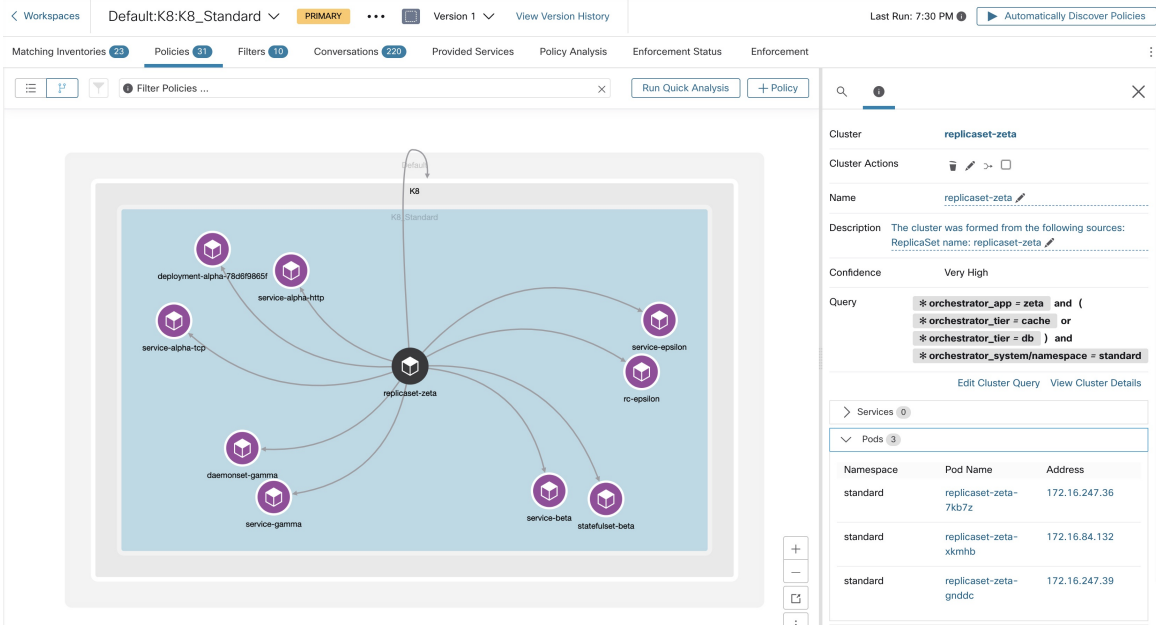
Soutien Kubernetes de la découverte des politiques

La découverte des politiques utilise les informations sur les pods et les services de la configuration Kubernetes pour créer des grappes à la fois pour les pods et les services et les politiques respectives sont générées.

Si la granularité de la grappe est COARSE (GROSSIÈRE) ou VERY COARSE (TRÈS GROSSIÈRE), les services et les pods qui les soutiennent sont mis en grappe ensemble.



Si la granularité de la grappe est définie sur moyenne, fine ou très fine, les services et les pods qui les soutiennent sont mis en grappe séparément.



Pour les grappes de pods, les informations sur la source sont ajoutées dans le cadre de la description de la grappe et chaque grappe de la description contient les informations sur l'entité à l'origine de la formation de la grappe.

Par exemple, **description** : « *La grappe a été formée à partir des sources suivantes : Nom de l'ensemble de réplications : ReplicaSet-zeta* ».

Importer/Exporter

Exporter un espace de travail

Tout le contenu pertinent des groupes et des politiques de chaque espace de travail peut être téléchargé en un fichier unique dans plusieurs formats de documents structurés couramment utilisés comme JSON, XML et YAML. Ces fichiers peuvent être utilisés pour un traitement ultérieur en interne ou pour être incorporés dans d'autres outils d'analyse ou d'application de la politique.

Accédez à l'élément du menu **. .** dans l'en-tête de l'espace de travail et cliquez sur l'élément **export** (exporter). Cela affichera la boîte de dialogue d'exportation. Vous pouvez choisir si le fichier exporté doit inclure uniquement le contenu de la grappe ou de la grappe et des politiques de sécurité parmi les grappes générées par la découverte automatique des politiques en fonction des flux de réseau réels. Choisissez le format souhaité et cliquez sur download (télécharger) pour télécharger le fichier dans le système de fichiers local.

Figure 24: Éléments de menu Import/Export (Importer/Exporter)

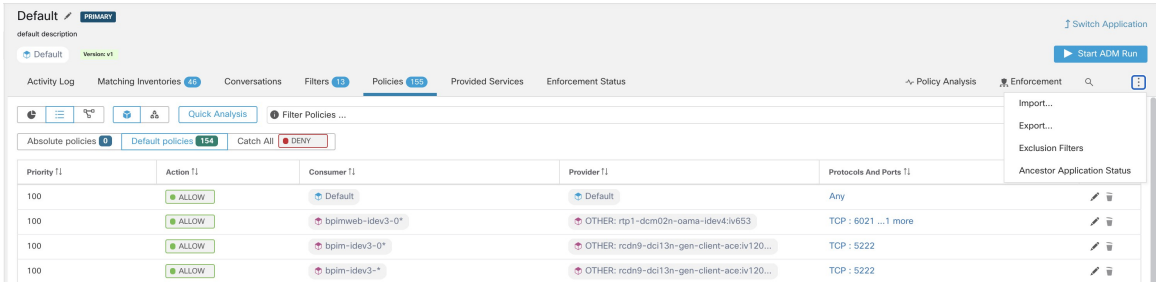
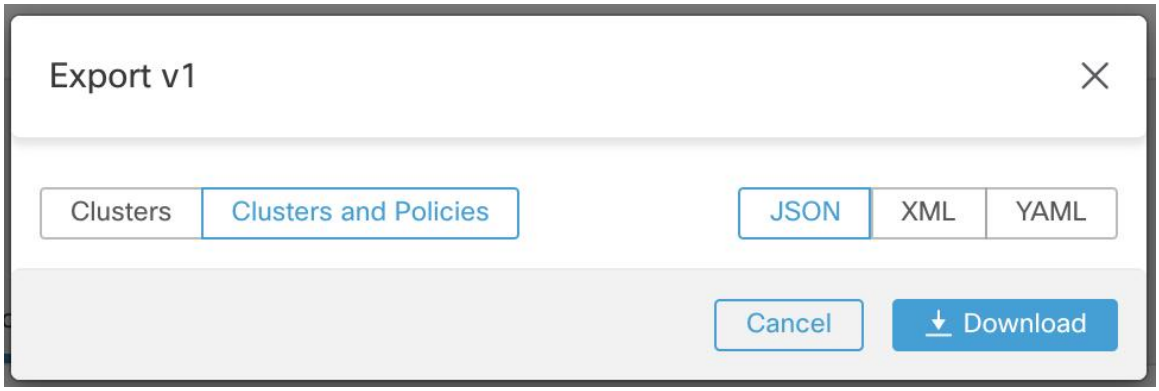


Figure 25: Exportation des politiques d'un espace de travail



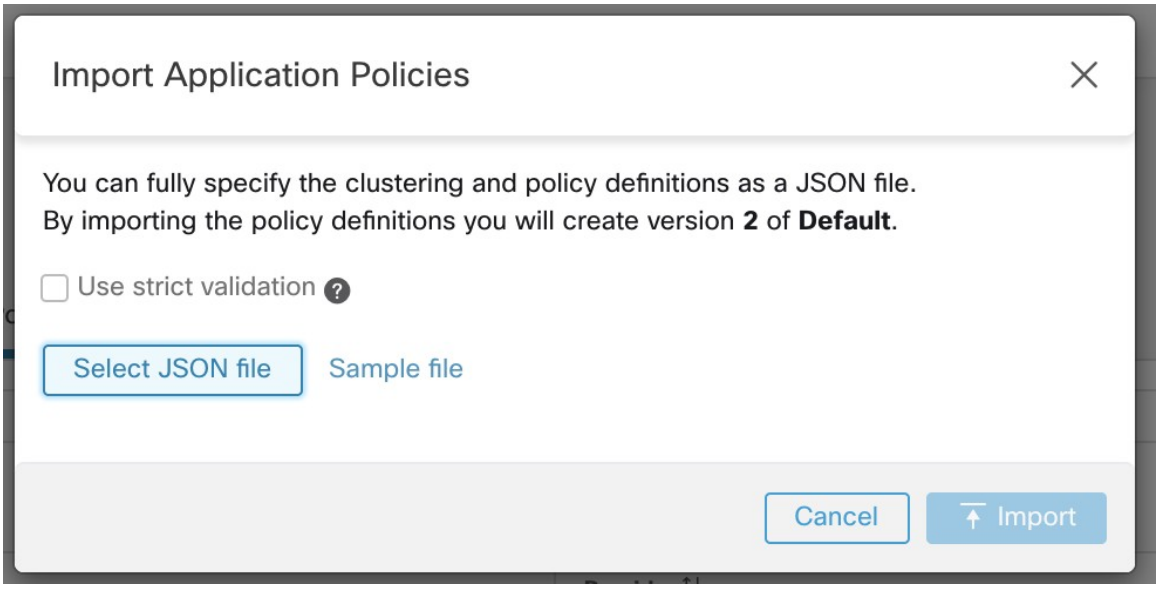
Lorsque vous exportez un espace de travail, le paramètre Auto accept outgoing policy connectors (« Accepter automatiquement les connecteurs de politique sortants ») dans la configuration de découverte automatique des politiques est inclus et sera actif dans l'espace de travail importé.

Importer

Vous pouvez importer des définitions connues de grappes et de politiques dans un espace de travail en chargeant directement un fichier JSON. Tout comme la découverte automatique des politiques, le chargement de politiques dans un espace de travail existant crée une nouvelle version et place la grappe et les définitions de politiques sous la nouvelle version. Les filtres manquants et les valeurs de propriété incorrectes renverront une erreur.

Cliquez sur l'élément de menu **Import** (Importer) dans **. Menu** dans l'en-tête de l'espace de travail. Dans la boîte de dialogue d'importation, vous pouvez sélectionner un fichier JSON avec un format valide. Vous pouvez obtenir un petit exemple de fichier JSON illustrant le schéma pour les politiques et les grappes en cliquant sur le bouton **Example** (Exemple).

Figure 26: Importation des grappes et politiques



La validation stricte, si elle est activée, renverra une erreur si le JSON contient des attributs non reconnus. Ceci est utile pour localiser les fautes de frappe ou les champs facultatifs mal identifiés.

Note Toutes les politiques importées sont marquées comme approuvées par défaut, sauf si elles sont explicitement marquées comme `approved: false` (approuvées : faux). Vous avez la possibilité de maintenir ces politiques approuvées pendant la découverte automatique des politiques afin de générer un nouvel ensemble de politiques. Consultez Politiques approuvées, on page 51 pour en savoir plus.

Conseil de pro : Le schéma du fichier JSON récupéré lors de l'exportation d'un espace de travail d'application est compatible avec le schéma du format attendu pour l'importation de politiques dans un espace de travail. Par conséquent, vous pouvez copier les politiques d'un espace de travail d'application vers un autre en utilisant une exportation suivie d'une importation. Notez que de nombreuses fonctionnalités peuvent ne pas fonctionner de la même manière lors de l'exportation puis de l'importation de politiques. Par exemple, les conversations à l'appui des politiques ne sont pas incluses dans l'exportation et ne seront pas présentes lors de l'importation des politiques non plus.

Politiques spécifiques à la plateforme

Pour des renseignements importants sur la façon dont les agents appliquent les politiques sur chaque plateforme, consultez Application des politiques par le biais d'agents. Pour Kubernetes/OpenShift, consultez Application des conteneurs, à la page 138.

Windows

Configuration de politique basée sur le système d'exploitation Windows recommandée

Toujours spécifier les ports et les protocoles dans les politiques, lorsque cela est possible; nous vous recommandons de ne permettre AUCUN port, AUCUN protocole.

Par exemple, une politique générée avec des restrictions de port et de protocole pourrait ressembler à ceci :

```
dst_ports {
 start_port: 22
 end_port: 22
 consumer_filters {
   application_name: "c:\\test\\putty.exe"
 }
}}
ip_protocol: TCP
```

En revanche, si vous autorisez les connexions réseau lancées par iperf.exe avec TOUS les protocoles et TOUS les ports, la politique générée ressemblera à ceci :

```
match_set {
  dst_ports {
    end_port: 65535
    consumer_filters {
      application_name: "c:\\test\\iperf.exe"
    }
  }
  address_family: IPv4
  inspection_point: EGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

Pour le filtre ci-dessus, Cisco Secure Workload crée une règle de politique pour autoriser le trafic réseau sur le fournisseur comme suit :

```
match_set {
    dst_ports {
    end_port: 65535
  }
  address_family: IPv4
  inspection_point: INGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

Cette règle de réseau ouvre tous les ports sur le fournisseur. Nous vous déconseillons de créer des filtres basés sur le système d'exploitation avec le protocole *Any* (Tous).

Configurer les politiques pour les attributs Windows

Pour plus de granularité lors de l'application d'une politique sur les charges de travail basées sur Windows, vous pouvez filtrer le trafic réseau par :

- Nom de l'application
- Nom du service
- Noms d'utilisateur avec ou sans groupes d'utilisateurs

Cette option est prise en charge dans les modes WAF et WFP. Les filtres basés sur le système d'exploitation Windows sont classés en tant que *filtres de consommateur* et de *filtres de fournisseur* dans la politique de réseau générée. Les filtres des consommateurs filtrent le trafic réseau qui est initié par la charge de travail des consommateurs et les filtres des fournisseurs filtrent le trafic réseau qui est destiné au travail du fournisseur.

Avant de commencer

Cette procédure suppose que vous modifiez une politique existante. Si vous n'avez pas encore créé la politique à laquelle ajouter un filtre basé sur le système d'exploitation Windows, créez d'abord cette politique.

Important Consultez Mises en garde et Limites connues pour des renseignements sur les politiques impliquant les attributs Windows.

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Defend (Défendre)** > **Segmentation** .

Étape 2 Cliquez sur la portée qui contient la politique pour laquelle vous souhaitez configurer des filtres basés sur le système d'exploitation Windows.

Étape 3 Cliquez sur l'espace de travail dans lequel vous souhaitez modifier la politique.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

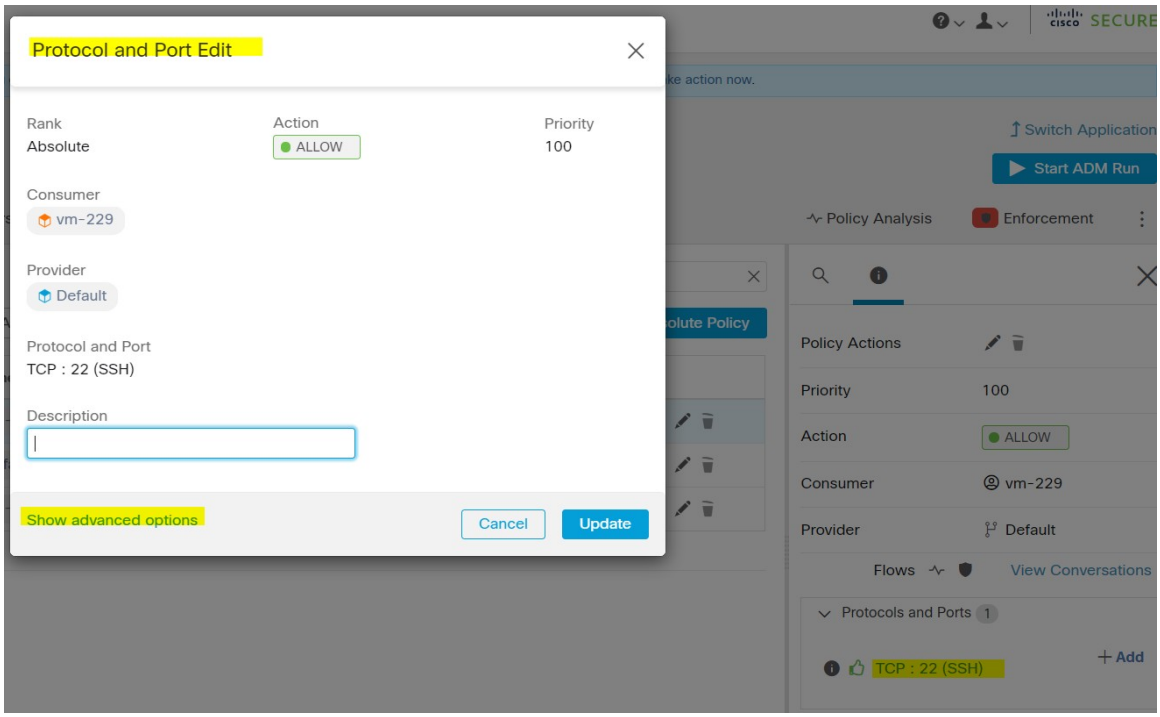
Étape 5 Choisissez la politique à modifier.

Important Le client et le fournisseur doivent inclure uniquement les charges de travail Windows.

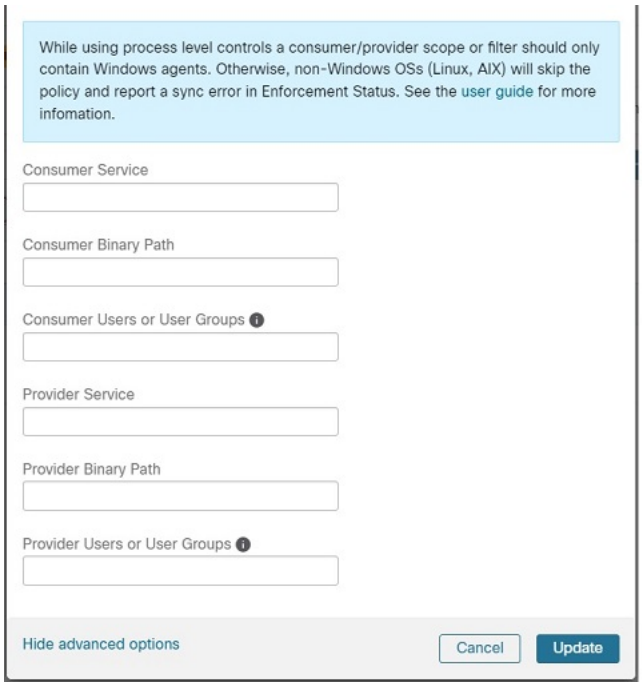
Étape 6 Dans la ligne du tableau permettant de modifier la politique, cliquez sur la valeur existante dans la colonne **Protocols and Ports** (protocoles et ports).

Étape 7 Dans le volet de droite, cliquez sur la valeur existante sous **Protocols and Ports**.

Dans l'exemple, cliquez sur **`TCP : 22 (SSH).`**



Étape 8 Cliquez sur **Show Advanced Options** (Afficher les options avancées).



Étape 9 Configurez les filtres de consommateur en fonction du nom de l'application, du nom du service ou du nom d'utilisateur.

- Le nom de l'application doit être un chemin d'accès complet.

- Le nom du service doit être un nom de service court.
- Le nom d'utilisateur peut être un nom d'utilisateur local (par exemple, tetter) ou un nom d'utilisateur de domaine (par exemple, capteur-dev@capteur-dev.com ou capteur-dev\capteur-dev)
- Le groupe d'utilisateurs peut être un groupe d'utilisateurs local (par exemple, Administrateurs) ou un groupe d'utilisateurs de domaine (par exemple, domaine utilisateurs\\capteur-dev)
- Plusieurs noms d'utilisateurs et/ou de groupes d'utilisateurs peuvent être spécifiés, séparés par « , » (par exemple, capteur-dev\@capteur-dev.com,utilisateurs du domaine\\capteur-dev)
- Le nom du service et le nom d’utilisateur ne peuvent pas être configurés ensemble.

Étape 10 Configurez les filtres de fournisseur en fonction du nom de l’application, du nom de service ou du nom d’utilisateur.

Suivez les mêmes directives que celles données à l’étape précédente pour les filtres du consommateur.

Étape 11 Saisissez les chemins d’accès au fichier binaire, le cas échéant.

Par exemple, saisissez **`c:\test\putty.exe`**

Étape 12 Cliquez sur **Update** (mettre à jour).

Limites connues

- Windows 2008 R2 ne prend pas en charge les politiques de filtrage basées sur le système d’exploitation Windows.
- La politique de réseau peut être configurée avec un nom d’utilisateur unique, tandis que l’interface utilisateur du pare-feu Microsoft prend en charge plusieurs utilisateurs.

Mises en garde

- Lors de l’utilisation de politiques basées sur le système d’exploitation Windows, une portée ou un filtre consommateur ou fournisseur ne doit contenir que des agents Windows. Sinon, les systèmes d’exploitation autres que Windows (Linux, AIX) ignorent la politique et signalent une erreur de synchronisation dans l’état d’application.
- Évitez de créer des filtres de système d’exploitation Windows avec des critères de filtrage *peu rigoureux*. De tels critères peuvent ouvrir des ports réseau indésirables.
- Si les filtres de système d’exploitation sont configurés pour le client, les politiques ne s’appliquent qu’au client. De même, s’ils sont configurés pour le fournisseur, ils ne s’appliquent qu’au fournisseur.
- Étant donné que les connaissances relatives au contexte du processus, de l’utilisateur ou de service sont limitées ou inexistantes, il y aura des écarts dans l’analyse des politiques si elles comportent des filtres basés sur le système d’exploitation Windows.

Vérification et dépannage des politiques avec les attributs de filtrage basés sur le système d’exploitation Windows

Si vous utilisez des attributs de filtrage basés sur le système d’exploitation Windows, les rubriques suivantes vous fourniront des informations de vérification et de dépannage.

Le service d'assistance Cisco TAC peut utiliser ces informations au besoin pour effectuer le dépannage de ces politiques.

Politiques basées sur le nom de l'application

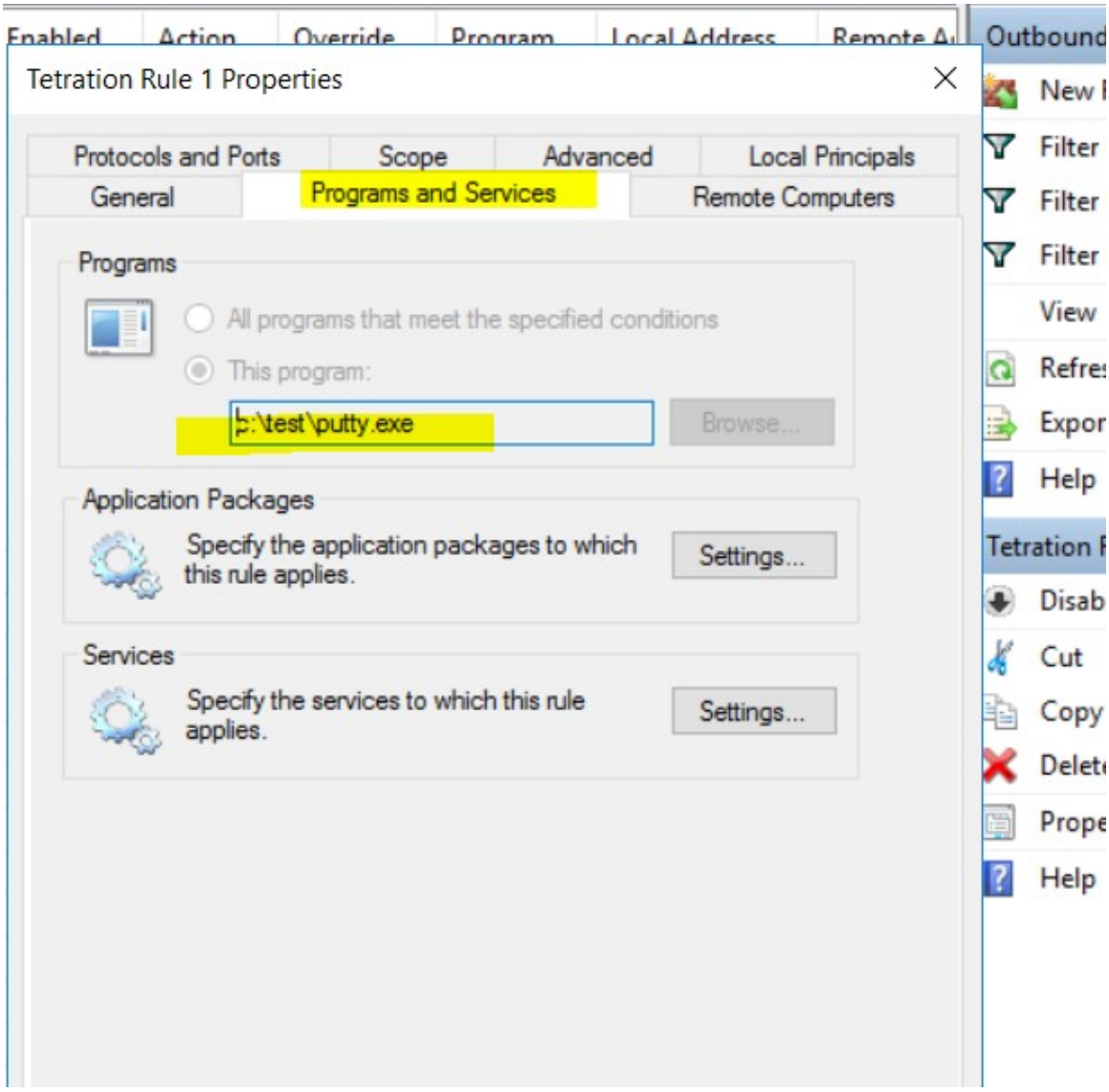
Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom de l'application sur les charges de travail avec système d'exploitation Windows.

Les sections suivantes décrivent la façon dont les politiques doivent s'afficher sur la charge de travail pour un fichier binaire d'application saisi sous la forme **`c:\test\putty.exe`**.

Exemple de politique basée sur le nom de l'application

```
dst_ports {
start_port: 22
end_port: 22
consumer_filters {
application_name: "c:\test\putty.exe"
}
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

Règle de pare-feu générée



Filtre généré à l'aide de netsh

Pour vérifier, à l'aide des outils Windows natifs, qu'un filtre a été ajouté à une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_APP_ID pour le nom de l'application dans le fichier de sortie : filter.xml.

```
<fieldKey>FWPM_CONDITION_ALE_APP_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
```

```
                              <type>FWP_BYTE_BLOB_TYPE</type>
                              <byteBlob>
                                     <data>
‹→5c006400650076006900630065005c006800610072006400640069007300 6b0076006f006
‹→</data>
                                  <asString>\device\harddiskvolume2\temp\putty.exe</
‹→asString>
                 </byteBlob>
        </conditionValue>
```

Filtre WFP généré à l'aide de tetenf.exe -l -f

```
Filter Name:                    Cisco Secure Workload Rule 1
----------------------------------------------------
EffectiveWeight:                18446744073709551592
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    22
Protocol:                       6
AppID:                          \device\harddiskvolume2\test\putty.exe
```

Nom d'application non valide

- En mode WAF, une règle de pare-feu est créée pour un nom d’application non valide.
- En mode WFP, le filtre WFP n’est pas créé pour un nom d’application non valide, mais le NPC n’est pas rejeté. L'agent consigne un message d'avertissement et configure le reste des règles de politique.

Politiques basées sur le nom du service

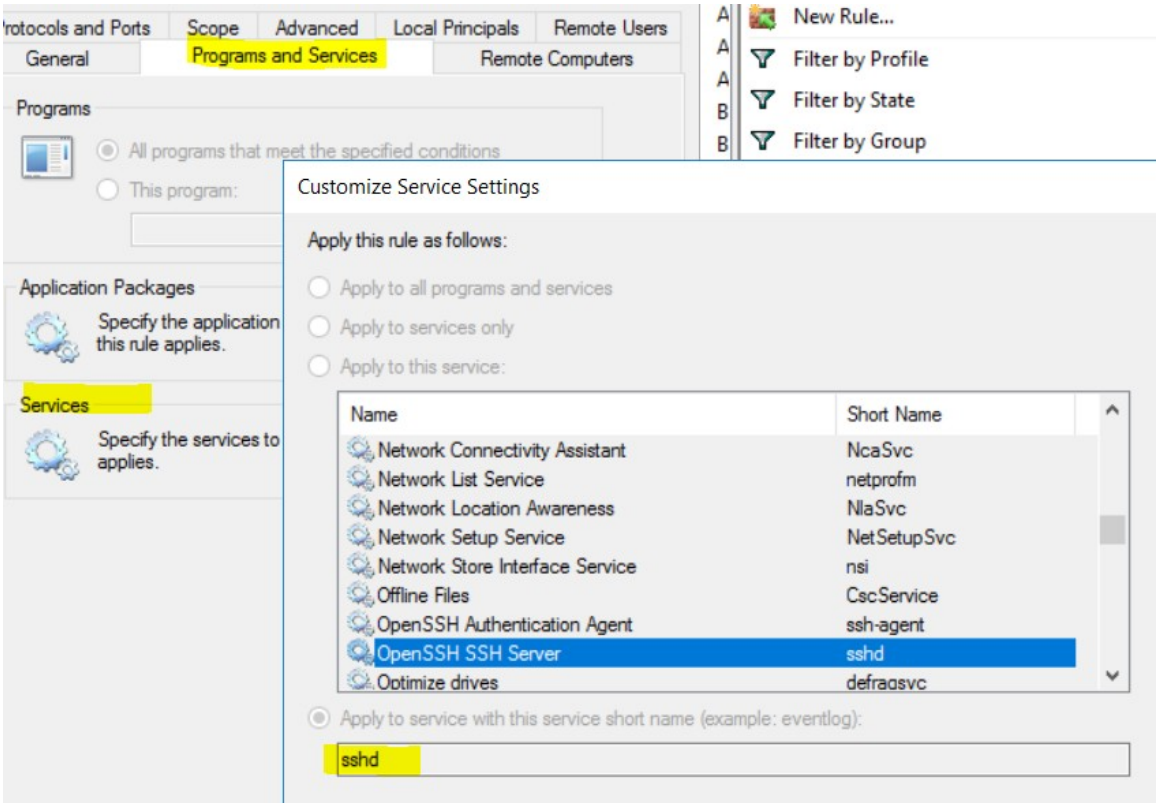
Utilisez les informations suivantes pour vérifier et dépanner les politiques basées sur le nom du service sur les charges de travail fonctionnant sous le système d’exploitation Windows.

Les sections suivantes décrivent la façon dont les politiques doivent s’afficher sur la charge de travail.

Exemple de politique basée sur le nom de service

```
    dst_ports {
             start_port: 22
             end_port: 22
             provider_filters {
                    service_name: “sshd”
             }
         }}
         ip_protocol: TCP
         address_family: IPv4
         inspection_point: INGRESS
```

Règle de pare-feu générée



Filtre généré à l'aide de netsh

Pour vérifier à l'aide des outils Windows natifs qu'un filtre a été ajouté pour une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_USER_ID pour déterminer le nom d'utilisateur dans le fichier de sortie : filter.xml.

```
<item>
                    <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
                              <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>

<sd>O:SYG:SYD:(A;;CCRC;;;S-1-5-80-3847866527-469524349-687026318-
→516638107)</sd>
                    </conditionValue>
</item>
```

Filtre WFP généré à l'aide de tetenf.exe -l -f

```
Filter Name:       Cisco Secure Workload Rule 3
----------------------------------------------------
```

```
EffectiveWeight:            18446744073709551590
LayerKey:                   FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
Action:                     Permit
Local Port:                 22
Protocol:                   6
User or Service:            NT SERVICE\sshd
```

Nom non valide

- En mode WAF, la règle de pare-feu est créée pour un nom de service inexistant.
- En mode WFP, le filtre WFP n'est pas créé pour un nom de service inexistant.
- Le type de SID du service doit être *Unrestricted* (non restreint) ou *Restricted* (Restreint). Si le type de service est *None* (Aucun), la règle de pare-feu et le filtre WFP peuvent être ajoutés, mais n'ont aucun effet.

  Pour vérifier le type de SID, exécutez la commande suivante :

  ```
  sc qsidtype <service name>
  ```

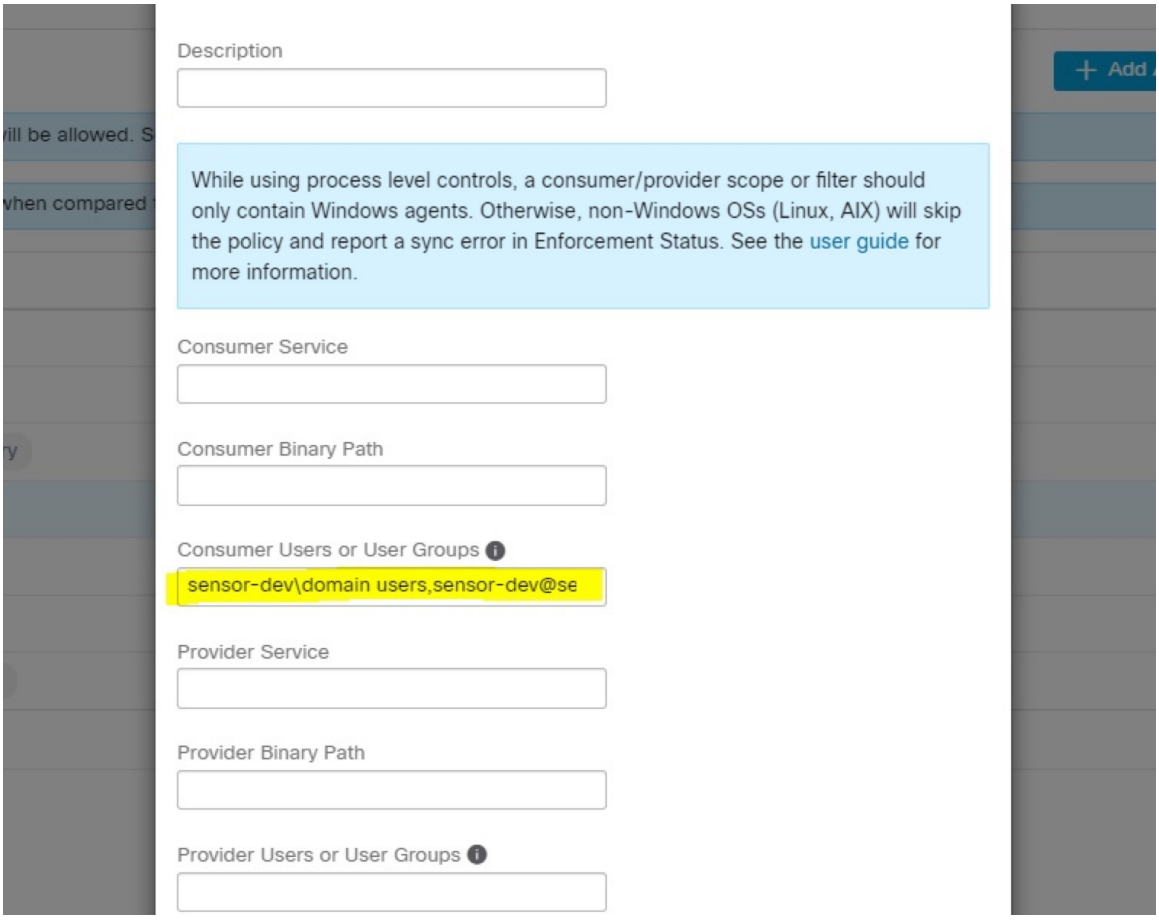
Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur

Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom d'utilisateur (avec et sans nom de groupe d'utilisateurs) sur les charges de travail avec système d'exploitation Windows.

Les sections de cette rubrique décrivent la manière dont les politiques doivent apparaître sur la charge de travail.

Les exemples présentés dans cette rubrique sont basés sur des politiques configurées avec les informations suivantes :

Figure 27: Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur



Exemple de politique basée sur le nom d'utilisateur

```
dst_ports {
          start_port: 30000
          end_port: 30000
          provider_filters {
               user_name: "sensor-dev\sensor-dev"
           }
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

Exemple de politique basée sur le groupe d'utilisateurs et le nom d'utilisateur

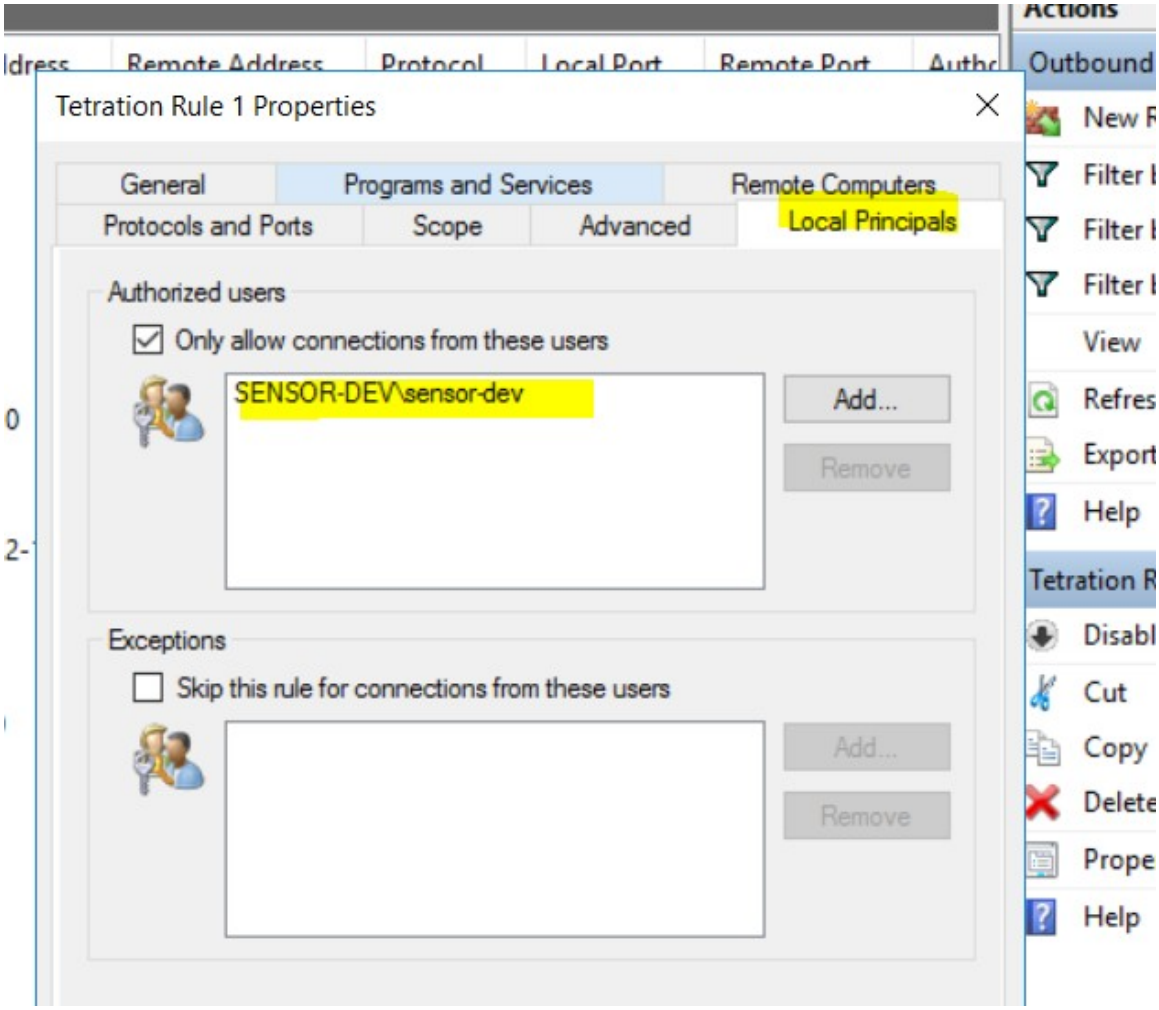
```
dst_ports {
start_port: 30000
end_port: 30000
provider_filters {
user_name: "sensor-dev\domain users,sensor-dev\sensor-dev"
}
}}
ip_protocol: TCP
```

```
address_family: IPv4
inspection_point: EGRESS
```

Règle de pare-feu générée

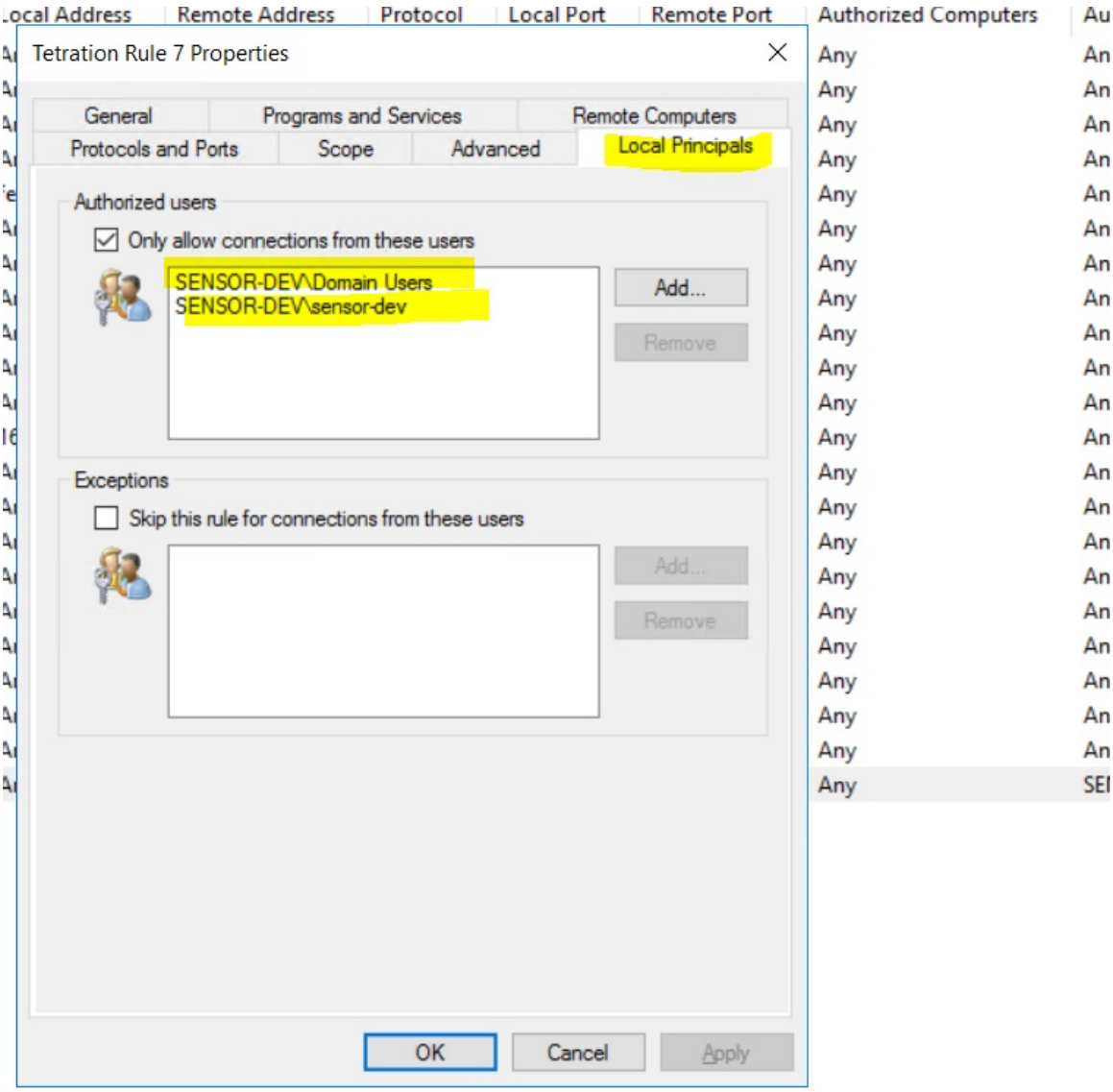
Règle de pare-feu basée sur le nom d'utilisateur

Exemple : règle de pare-feu basée sur le nom d'utilisateur, sensor-dev\\sensor-dev



Règle de pare-feu basée sur le groupe d'utilisateurs et le nom d'utilisateur

Exemple : règle de pare-feu basée sur le nom d'utilisateur, sensor-dev\sensor-dev et le groupe d'utilisateurs, domain users\sensor-dev



Filtre généré à l'aide de netsh

Pour vérifier à l'aide des outils Windows natifs qu'un filtre a été ajouté pour une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_USER_ID pour déterminer le nom d'utilisateur dans le fichier de sortie : filter.xml.

```
<item>
            <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
            <matchType>FWP_MATCH_EQUAL</matchType>
            <conditionValue>
```

```
                    <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>
                    <sd>O:LSD:(A;;CC;;;S-1-5-21-4172447896-825920244-2358685150)</sd>
                </conditionValue>
    </item>
```

Filtres WFP générés à l'aide de tetenf.exe -l -f

Filtrer en fonction du nom d'utilisateur

Exemple : règle WFP basée sur le nom d'utilisateur, SENSOR-DEV\capteur-dev

```
Filter Name:                    Cisco Secure Workload Rule 1
---------------------------------------------------------
EffectiveWeight:                18446744073709551590
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    30000
Protocol:                       6
User or Service:                SENSOR-DEV\sensor-dev
```

Filtrer en fonction du groupe d'utilisateurs et du nom d'utilisateur

Exemple : règle WFP basée sur le nom d'utilisateur, SENSOR-DEV\\sensor-dev et le nom du groupe d'utilisateurs, SENSOR-DEV\\Domain Users

```
Filter Name:         Cisco Secure Workload Rule 1
---------------------------------------------------------
EffectiveWeight:              18446744073709551590
LayerKey:                     FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                       Permit
RemoteIP:                     10.195.210.15-10.195.210.15
Remote Port:                  30000
Protocol:                     6
User or Service:              SENSOR-DEV\Domain Users, SENSOR-DEV\sensor-dev
```

Le nom du service et le nom d'utilisateur ne peuvent pas être configurés dans le cadre d'une règle de politiques réseau.

Note La politique réseau est rejetée par l'agent Windows si le nom d'utilisateur ou le groupe d'utilisateurs n'est pas valide.

Kubernetes et OpenShift

(Facultatif) Politiques supplémentaires pour les charges de travail Kubernetes

Les procédures suivantes sont facultatives, selon votre environnement Kubernetes.

Politiques pour le contrôleur d'entrée Nginx de Kubernetes fonctionnant en mode hôte-réseau

Cisco Secure Workload applique les politiques au niveau du contrôleur d'entrée nginx et au niveau des pods de arrière-plan lorsque ces derniers sont accessibles aux clients externes à l'aide de l'objet d'entrée de Kubernetes.

Note Si le contrôleur d'entrée ne fonctionne pas en mode réseau hôte, consultez IngressControllerAPI

Note IBM-ICP utilise le contrôleur d'entrée Nginx de Kubernetes par défaut et s'exécute sur les nœuds du plan de commande en mode réseau hôte.

Voici les étapes pour appliquer la politique à l'aide du contrôleur d'entrée Nginx Kubernetes.

Procedure

Étape 1 Créez un orchestrateur externe pour Kubernetes/OpenShift comme décrit ici.

```
→  ~
→  ~ k8s get ingress
NAME           HOSTS   ADDRESS          PORTS   AGE
test-ingress   *       192.168.60.100   80      7s
→  ~
```

Étape 2 Créez un objet d'entrée dans la grappe Kubernetes. Un instantané du fichier yaml utilisé pour créer l'objet d'entrée est fourni dans l'image suivante.

```
▶ k8s get ingress
NAME                      HOSTS   ADDRESS          PORTS   AGE
svc-ce2e-teeksitlbiwlc    *       192.168.10.13    80      74s
```

```
~
▶ k8s get ingress -o yaml
apiVersion: v1
items:
- apiVersion: extensions/v1beta1
  kind: Ingress
  metadata:
    annotations:
      virtual-server.f5.com/ip: 192.168.10.13
      virtual-server.f5.com/partition: k8scluster
    creationTimestamp: "2020-06-26T21:31:01Z"
    generation: 1
    labels:
      e2e-test: "yes"
    name: svc-ce2e-teeksitlbiwlc
    namespace: default
    resourceVersion: "1074475"
    selfLink: /apis/extensions/v1beta1/namespaces/default/ingresses/svc-ce2e-teeksitlbiwlc
    uid: 5526b4a3-b7f4-11ea-aa09-525400d58002
  spec:
    backend:
      serviceName: svc-ce2e-teeksitlbiwlc
      servicePort: 80
  status:
    loadBalancer:
      ingress:
      - ip: 192.168.10.13
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
```

Étape 3 Déployez le contrôleur d'entrée Nginx de Kubernetes dans la grappe Kubernetes. Les pods du contrôleur d'entrée IBM-ICP s'exécutent sur les nœuds du plan de commande par défaut.

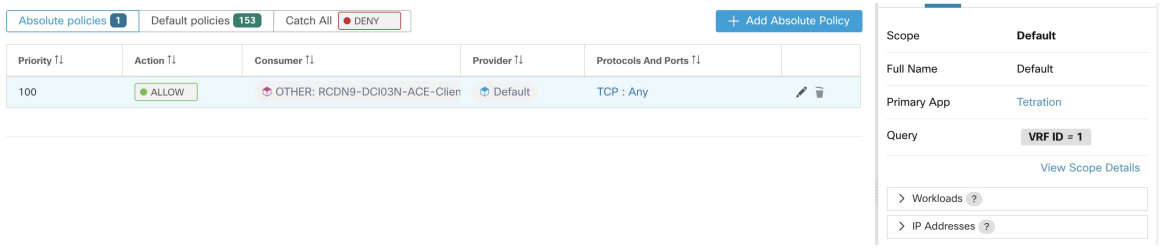
```
~
▶ k8s get pods -o wide -n ingress-nginx
NAME                                 READY   STATUS    RESTARTS   AGE     IP             NODE                         NOMINATED NODE
nginx-ingress-controller-6bc9c6745c-scfzs   1/1     Running   0          2m11s   192.168.10.13   enforcement-scale-16-kube3   <none>

~
▶ k8s get node enforcement-scale-16-kube3 -o wide
NAME                         STATUS   ROLES    AGE    VERSION   INTERNAL-IP     EXTERNAL-IP   OS-IMAGE            KERNEL-VERSION      CONTAINER-RUNTIME
enforcement-scale-16-kube3   Ready    <none>   7d5h   v1.12.3   192.168.10.13   <none>        Ubuntu 16.04.5 LTS   4.4.0-139-generic   docker://18.6.1
```

Étape 4 Créez un service de serveur backend (principal) auquel les consommateurs externes à la grappe accéderont. Dans l'exemple ci-dessous, nous avons créé un service simple *svc-ce2e-teeksitlbiwlc* (http-echo).

```
~
▶ k8s get svc svc-ce2e-teeksitlbiwlc
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
svc-ce2e-teeksitlbiwlc   ClusterIP   10.102.30.231   <none>        80/TCP    6m11s
```

Étape 5 Créez une politique entre le consommateur externe et le service backend.



Étape 6 Lorsque vous êtes prêt, appliquez la politique.

Étape 7 Dans le cas d'un contrôleur d'entrée Nginx, le logiciel Cisco Secure Workload applique la règle d'autorisation/abandon appropriée selon laquelle la source sera le consommateur spécifié à l'étape ci-dessus et la destination sera l'adresse IP du pod du contrôleur d'entrée correspondante. Dans le cas de pods backend, le logiciel Cisco Secure Workload appliquera la règle d'autorisation/abandon appropriée où la source sera le pod d'entrée et la destination sera l'adresse IP du pod backend (principal).

Politiques pour le contrôleur d'entrée de Kubernetes Nginx/Haproxy fonctionnant en tant que Déploiement/Daemonset

Cisco Secure Workload appliquera les politiques au contrôleur d'entrée et aux pods de l'arrière-plan (backend) lorsque les pods sont accessibles aux clients externes à l'aide de l'objet d'entrée de Kubernetes.

Voici les étapes à suivre pour appliquer les politiques sur le contrôleur d'entrée.

Procedure

Étape 1 Créer ou mettre à jour un orchestrateur externe pour Kubernetes/OpenShift à l'aide d'OpenAPI. Consultez la section Orchestrateurs pour en savoir plus sur la création de l'orchestrateur externe à l'aide d'OpenAPI. Ajoutez des informations sur les contrôleurs d'entrée pour la configuration de l'orchestrateur externe.

Étape 2 Créez un objet d'entrée dans la grappe Kubernetes.

Étape 3 Déployez le contrôleur d'entrée dans la grappe Kubernetes.

Étape 4 Créez un service de serveur backend (principal) auquel les consommateurs externes à la grappe accéderont.

Étape 5 Créez une politique entre le consommateur externe et le service backend.

Étape 6 Lorsque vous êtes prêt, appliquez la politique.

Étape 7 Dans le cas de contrôleurs d'entrée, Cisco Secure Workload le logiciel appliquera la règle d'autorisation/abandon appropriée selon laquelle la source sera le consommateur spécifié à l'étape ci-dessus et la destination sera l'adresse IP de pod du contrôleur d'entrée correspondante. Dans le cas de pods backend, le logiciel Cisco Secure Workload appliquera la règle d'autorisation/abandon appropriée où la source sera le pod d'entrée et la destination sera l'adresse IP du pod backend (principal).

Regroupement des charges de travail : grappes et filtres d'inventaire

Les grappes et les filtres d'inventaire ont des objectifs similaires, mais présentent des différences importantes :

Tableau 4 : Comparaison des grappes et des filtres d'inventaire

Grappes	Filtres d'inventaire
Sont utilisés pour appliquer une politique à un sous-ensemble des charges de travail dans une portée.	Peut être utilisé pour appliquer une politique à un sous-ensemble des charges de travail dans une portée. Peut également être utilisé pour appliquer une politique aux charges de travail, quelle que soit la portée (par exemple, pour appliquer une politique à toutes les charges de travail exécutant un système d'exploitation particulier).
Sont définis par une requête	Sont définis par une requête.
Peut inclure uniquement les charges de travail dans une seule portée.	L'adhésion peut être restreinte à une seule portée ou inclure des charges de travail de n'importe quelle portée (par exemple, si le filtre est basé sur le système d'exploitation).
Ne peut être utilisé que par les politiques du même espace de travail et de la même version de l'espace de travail.	Peut être utilisé par les politiques dans n'importe quelle portée et dans n'importe quel espace de travail.
Peut être créé automatiquement lors de la découverte automatique des politiques.	Doit être créé ou converti manuellement à partir d'une grappe existante.
Peut être remplacé lors de la découverte automatique des politiques s'il n'est pas approuvé. L'approbation de grappes connues intègres peut améliorer la précision d'autres grappes dans les futurs exécutions de découverte.	Ne sont jamais modifiés par la découverte automatique des politiques.
Profitez des fonctionnalités importantes de la découverte automatique des politiques. Il : • Disposer d'un indice de confiance qui vous aide à évaluer si les charges de travail du groupe doivent être regroupées. • Peuvent être comparées aux grappes générées lors d'autres exécutions de découverte de politiques sur le même espace de travail.	--
Ne peut pas être utilisée lors de la configuration de Dépendances externes, à la page 34 et des autres fonctionnalités liées aux politiques à portée croisée et à la découverte de politiques.	Peut être utilisé pour configurer des politiques granulaires impliquant des dépendances externes et d'autres fonctionnalités liées aux politiques à portée croisée, telles que les règles de pilote automatique.
Consultez Grappes, à la page 78 et les sous-sections.	Consultez les sections Créer un filtre d'inventaire et Convertir une grappe en filtre d'inventaire, à la page 82.

Grappes

Une grappe est un ensemble de charges de travail qui sont regroupées dans un espace de travail. (Un déploiement Cisco Secure Workload peut également être appelé une grappe, mais les deux utilisations ne sont pas liées).

Par exemple, si la portée de votre application comprend plusieurs serveurs web parmi les nombreux autres types de serveurs et d'hôtes qui composent votre application, vous pourriez vouloir une grappe de serveurs web dans cette portée d'application, de sorte que vous puissiez attribuer des politiques spécifiques uniquement à ces serveurs web.

La découverte automatique des politiques regroupe les charges de travail en grappes en fonction des signaux observés pendant la période spécifiée lors de la configuration de l'exécution.

Chaque grappe est définie par une requête

Les requêtes de grappe sont dynamiques, sauf si vous les définissez avec des adresses IP spécifiques. Avec les requêtes dynamiques, les membres de la grappe peuvent changer au fil du temps pour refléter les modifications de votre inventaire : des charges de travail plus nombreuses, moins nombreuses ou différentes peuvent correspondre à la requête.

Par exemple, si une requête de grappe est basée sur un nom d'hôte contenant la sous-chaîne « RH ».

La découverte automatique des politiques examine les noms d'hôte et les étiquettes associés aux charges de travail. Pour chaque grappe, la découverte automatique des politiques génère une courte liste de requêtes candidates en fonction des noms d'hôte et de ces étiquettes. Parmi ces requêtes, vous pouvez en sélectionner une, éventuellement la modifier et l'associer à la grappe. Notez que, dans certains cas, lorsque la découverte automatique des politiques ne peut pas formuler de requêtes suffisamment simples en fonction des noms d'hôte et des étiquettes, aucune (autre) requête n'est suggérée.

Les charges de travail dans les grappes approuvées ne sont pas affectées par la découverte de politiques futures

Seules les charges de travail qui ne sont pas encore membres d'une grappe approuvée dans l'espace de travail approprié sont affectées par la découverte de politiques. Une **grappe approuvée** est une grappe que vous avez approuvée manuellement. Pour de plus amples renseignements, consultez la section Approbation des grappes, on page 86.

Modifier les grappes pour améliorer le regroupement

Dans les sections suivantes, nous décrivons quelques flux de travail pour modifier, améliorer et approuver les résultats de la mise en grappe. Notez que l'on ne peut modifier/approuver les grappes que dans la dernière version d'un espace de travail (voir Journaux d'activités et historique des versions).

Consultez Modification des grappes, on page 80.

Grappes concernant l'inventaire Kubernetes

Note Si votre espace de travail comprend l'inventaire de plusieurs espaces de noms Kubernetes, chaque requête de grappe doit être filtrée par espace de noms. Ajoutez le filtre d'espace de nom à chaque requête s'il n'est pas déjà présent. Si vous modifiez une requête, redécouvre automatiquement les politiques.

Une grappe peut comprendre une seule charge de travail.

Vous pouvez créer des politiques concernant une seule charge de travail.

Les grappes peuvent être converties en filtres d'inventaire

À l'instar des grappes approuvées, les grappes promues en filtres d'inventaire ne sont pas modifiées lors de la découverte ultérieure des politiques .

Contrairement aux grappes, les filtres d'inventaire ne sont pas liés à un espace de travail, mais sont disponibles globalement dans votre déploiement de Cisco Secure Workload.

Pour une comparaison des grappes et des filtres d'inventaire, consultez Regroupement des charges de travail : grappes et filtres d'inventaire, on page 76.

Consultez Convertir une grappe en filtre d'inventaire, on page 82.

Niveau de confiance de la grappe

Utiliser le niveau de confiance ou le niveau de qualité d'une grappe pour déterminer les grappes à améliorer.

Le niveau de confiance pour une grappe correspond à la moyenne des niveaux de confiance des charges de travail des membres. En général, plus une charge de travail est similaire aux autres membres de la grappe qui lui a été attribuée et plus elle est différente des charges de travail de la grappe alternative la plus proche (la plus similaire), plus la confiance en cette charge de travail est élevée.

Lorsque les flux sont utilisés pour le regroupement, deux charges de travail sont similaires lorsqu'elles ont un modèle de conversation similaire (comme des ensembles similaires de voisins dans le graphe de conversation, c'est-à-dire des ensembles similaires de charges de travail et de ports de consommateurs et de fournisseurs).

Note

- Le niveau de confiance des grappes n'est pas calculé (est indéfini) pour :
  - les grappes contenant une seule charge de travail
  - les grappes approuvées
  - les charges de travail de la portée pour lesquelles aucune communication n'a été observée (ou aucune information sur les processus n'est disponible, si le regroupement basé sur les processus a été choisi)
- Les grappes ne dépassent pas les limites de la partition (comme les limites de sous-réseau, reportez-vous aux étiquettes de routage des configurations de découverte automatique de politiques avancées). Cependant, dans le calcul de la confiance et de la grappe de secours, ces limites sont ignorées. Cela indique l'existence potentielle de charges de travail ou de grappes qui se comportent de manière très similaire, même si elles se trouvent dans des sous-réseaux différents.
- Après la modification des grappes, les niveaux de confiance peuvent devenir inexacts, car ils ne sont PAS recalculés avant que vous ne détectiez à nouveau les politiques.

Pour afficher le niveau de confiance de la grappe, voir Afficher les grappes, on page 79.

Afficher les grappes

La vue des grappes prend en charge l'association requête à grappe et la modification des requêtes.

Dans la vue des grappes, vous pouvez cliquer sur un en-tête de colonne du tableau pour trier les grappes en fonction de cette colonne (comme le nom, le nombre de charges de travail ou le niveau de confiance).

Pour chaque grappe, en cliquant sur la ligne, vous pouvez afficher d'autres informations sur la grappe, telles que la description, les requêtes suggérées ou approuvées, et les charges de travail des membres dans le panneau de droite. Plusieurs de ces champs sont modifiables.

Pour afficher les grappes et leurs détails :

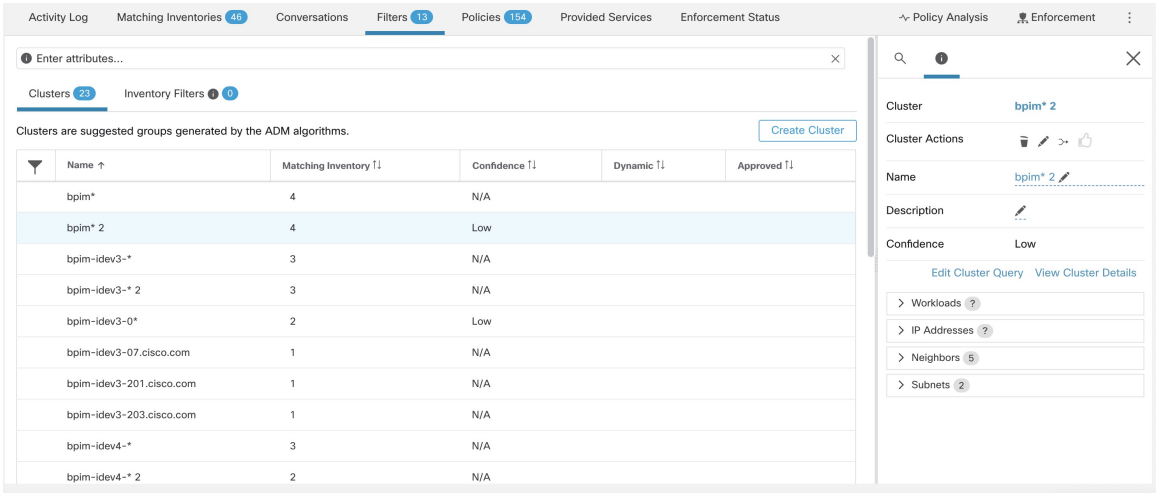
1. Accédez à la portée et à l'espace de travail qui vous intéressent.

   Les grappes sont spécifiques à un espace de travail; chaque espace de travail d'une portée peut avoir des grappes différentes. Pour rendre les grappes disponibles en dehors de leur espace de travail actuel, consultez Convertir une grappe en filtre d'inventaire, on page 82.

2. Cliquez sur **Manage Policies** (Gestion des politiques).
3. Cliquez sur **Filters** (Filtres).
4. Cliquez sur **Clusters** (Grappes).
5. Pour afficher des informations sur une grappe, cliquez sur cette dernière.
   a. Regardez dans le panneau qui s'ouvre sur la droite.
   b. Pour en savoir plus, cliquez sur **View cluster Details**(Afficher les détails de la grappe) .

      La page Cluster Details (détails de la grappe) s'ouvre dans un onglet de navigateur distinct.

Figure 28: Affichage des grappes



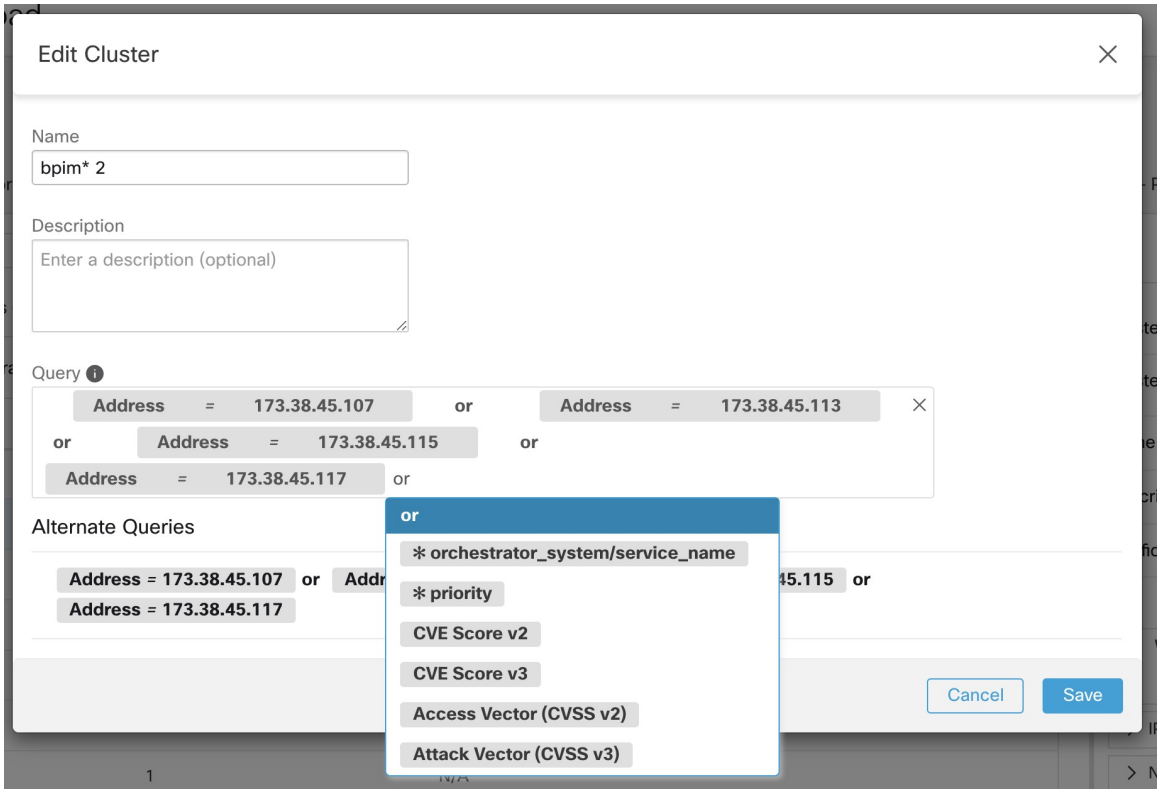
Modification des grappes

La découverte automatique des politiques crée une ou plusieurs requêtes candidate pour chaque grappe.

Si les résultats de la mise en grappe ne correspondent pas complètement à vos attentes, vous pouvez améliorer cette dernière en modifiant la requête.

Pour parcourir et modifier des grappes : Cliquez sur la zone **clusters** (grappes) en haut de la page. Pour modifier une grappe (par ex., modifier les membres d'une grappe ou sélectionner/modifier sa requête), sélectionnez/modifiez la requête de la grappe, comme indiqué ci-dessous.

Figure 29: Modifier la grappe



Vous pouvez ajouter ou supprimer des adresses IP explicites, ou choisir une autre requête dans la liste d'alternatives fournie et modifier cette requête. La requête d'une grappe peut correspondre à n'importe quel filtre de requête exprimé en termes d'adresses, de noms d'hôte et d'étiquettes. Si vous définissez une requête basée sur des étiquettes plutôt que sur des adresses IP explicites, la grappe sera dynamique et un inventaire nouveau, modifié ou supprimé qui est correctement étiqueté sera automatiquement inclus ou exclu de la grappe.

Une fois la sélection de la requête et les modifications possibles terminées, cliquez sur Save (Enregistrer). Notez qu'une fois que vous avez cliqué sur le bouton SAVE, la grappe est automatiquement marquée comme approuvée et l'icône représentant un pouce levé devient bleu (qu'une modification ait été apportée ou non). L'icône d'approbation peut être alternée pour modifier le statut d'approbation comme vous le souhaitez. Pour en savoir plus, reportez-vous à Approbation des grappes, on page 86

Important Lorsque l'appartenance à une grappe est modifiée, il peut être nécessaire de découvrir à nouveau les politiques pour obtenir une politique mise à jour reflétant avec précision les modifications des flux entre les grappes modifiées. En effet, les appartenances aux grappes peuvent avoir changé (par exemple, de nouveaux nœuds ont été ajoutés à une grappe). Une situation similaire peut se produire si la portée correspondant à l'espace de travail est modifiée ou, de manière générale, lorsque l'appartenance à l'espace de travail change. De même, les niveaux de confiance des grappes peuvent ne plus être précis selon les modifications apportées aux adhésions aux grappes. Dans tous ces cas, la nouvelle découverte automatique des politiques est utile pour obtenir des politiques et des niveaux de confiance des grappes à jour (niveau de confiance mis à jour sur les grappes non approuvées).

Si vous modifiez des requêtes de grappe, il est possible que les grappes associées aux requêtes se chevauchent.

Convertir une grappe en filtre d'inventaire

Convertir une grappe en filtre d'inventaire si :

- Vous ne souhaitez pas que la grappe soit modifiée par les futures exécutions de découverte automatique de la politique, ce qui constitue une alternative plus souple à l'approbation de la grappe.
- Vous souhaitez que la grappe soit indépendante de l'espace de travail et dans la version de l'espace de travail.
- Vous créez ou découvrez des politiques dans lesquelles le consommateur et le fournisseur appartiennent à des portées différentes, et vous souhaitez créer des politiques spécifiques à un sous-ensemble de charges de travail dans une portée, pas seulement des politiques impliquant la portée entière.

  Vous devez utiliser des filtres d'inventaire plutôt que des grappes à cette fin si vous créez des politiques concernant plusieurs portées à l'aide de la méthode avancée décrite en Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 94 et que vous souhaitez que les politiques soient plus appliquées plus finement que de portée à portée.

Procédure

Étape 1 Accédez à l'espace de travail qui contient la grappe à promouvoir.

Étape 2 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 3 Cliquez sur **Filters** (Filtres).

Étape 4 Cliquez sur **Clusters** (Grappes).

Étape 5 Cliquez sur la grappe que vous souhaitez utiliser dans la politique multiportée.

Étape 6 Dans le panneau de droite, dans la section **Cluster Actions** (Actions de niveau grappe), cliquez sur (Promote to Inventory Filter)(Promouvoir en tant que filtre d'inventaire).

Étape 7 Vérifiez que le nom, la description et la requête sont conformes aux attentes.

Étape 8 Sélectionnez **Restrict Query to Ownership Scope** Restreindre la requête au propriétaire de la portée)..

(Les filtres d'inventaire peuvent dépasser les limites de la portée, mais ce n'est pas ce que vous recherchez; vous souhaitez que ce filtre n'inclue que les charges de travail de cette portée).

Étape 9 Si vous souhaitez que l'application définie par ce filtre d'inventaire soit le fournisseur dans les politiques générées lors de la découverte automatique des politiques, sélectionnez **Provides a service external of its scope** (Fournit un service externe à sa portée).

Si cette application est un consommateur plutôt qu'un fournisseur, ou si vous utilisez ce filtre d'inventaire uniquement pour les politiques créées manuellement, vous n'avez pas besoin d'activer cette option.

Étape 10 Cliquez sur **Promote Cluster** (Promouvoir la grappe).

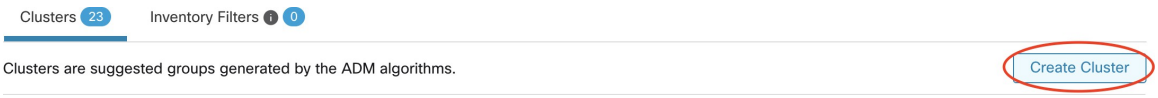
Étape 11 Vérifiez que la grappe a été déplacée vers l'onglet **Inventory Filters** (filtres d'inventaire).

Vous devrez peut-être actualiser la page pour constater ce changement.

Création ou suppression des grappes

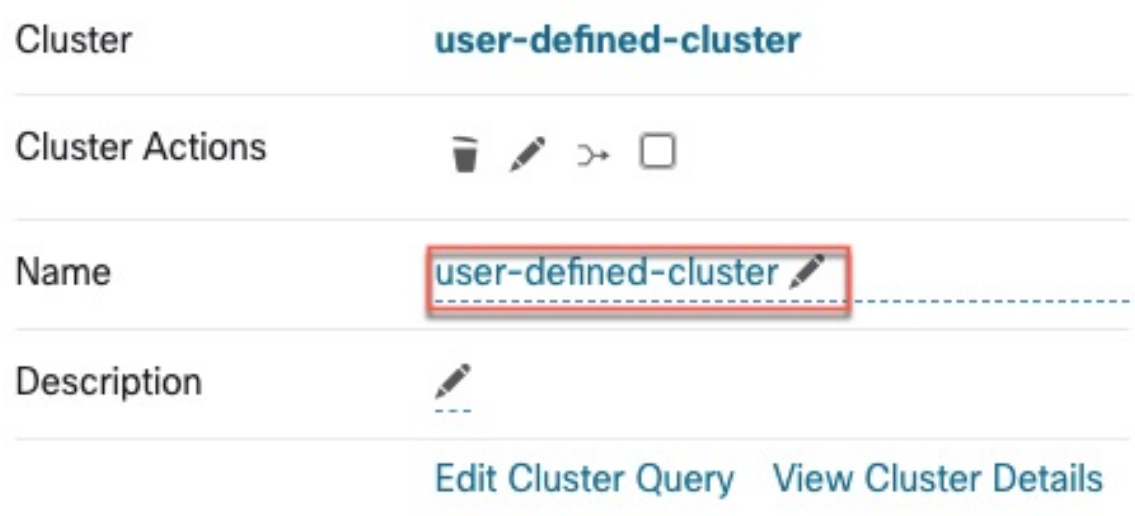
Cliquez sur le bouton **Create Cluster** (créer une grappe) dans la page des grappes pour créer une nouvelle grappe vide. Vous pouvez également créer une grappe à partir de la page de découverte automatique des politiques en cliquant sur le bouton **Create Filter** (Créer un filtre) dans la barre latérale de démarrage et en sélectionnant Grappes dans la boîte de dialogue modale.

Figure 30: Création d'une nouvelle grappe



La nouvelle grappe définie par l'utilisateur s'affichera dans le panneau latéral pour être renommée, si nécessaire.

Figure 31: Changement de nom d'une grappe



Une grappe vide peut être supprimée en la sélectionnant dans l'une des vues afin que les détails s'affichent dans le panneau latéral, puis en cliquant sur la corbeille dans l'en-tête de la vue détaillée de la grappe. Voir la figure ci-dessus.

Comparaison des versions des grappes générées : vues des différences

Après avoir détecté automatiquement au moins deux fois les politiques pour un espace de travail, vous pouvez comparer les grappes générées dans différents cycles de découverte.

Procedure

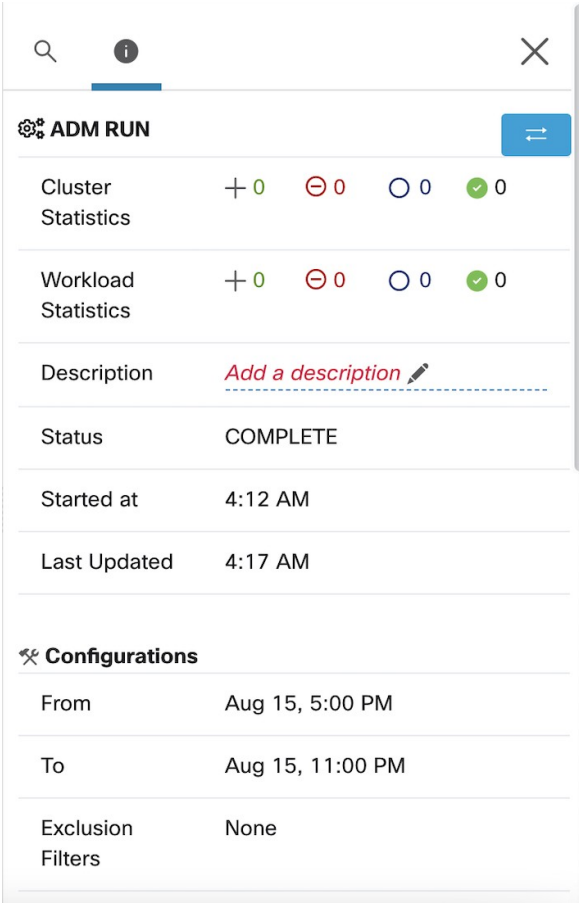
Étape 1 Accédez à la vue diff des grappes en utilisant l'un des chemins suivants :

- Après la découverte des politiques avec succès, un message s'affichera pour indiquer la réussite avec un lien qui mène à la vue du diff affichant les résultats de la découverte. Cliquez sur le lien des résultats.

Figure 32: Exécution réussie de la découverte automatique des politiques

- Comparer les révisions à partir de la vue des versions :
  a. Suivez les étapes dans Afficher, comparer et gérer les versions de politiques découvertes, on page 55.
  b. Après avoir cliqué sur **Compare Revisions** (Comparer les révisions), cliquez sur **Clusters** (Grappes).
- Dans le panneau latéral des détails dans la version :
  a. Suivez les étapes pour afficher les détails dans la version dans Afficher, comparer et gérer les versions de politiques découvertes, on page 55.
  b. Lorsque le panneau latéral affiche les informations contextuelles d'un cycle de découverte automatique des politiques, cliquez sur le bouton à double flèche situé dans le coin supérieur droit de ce panneau :

Figure 33: Affichage des informations de contexte



Étape 2 Choisissez les versions à comparer.

Étape 3 Passez en revue les résultats de la comparaison :

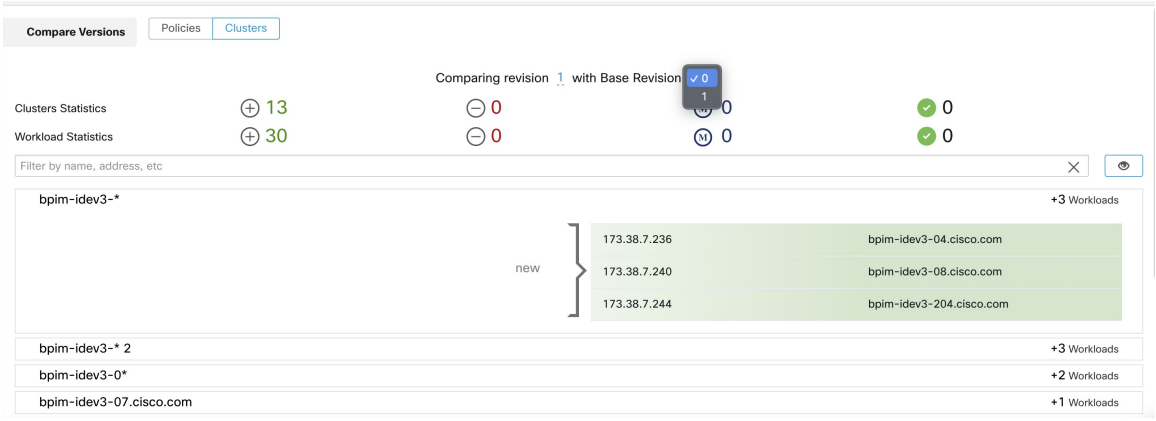
Au niveau supérieur, la vue Diff pour les politiques détectées automatiquement présente des statistiques générales sur les modifications apportées aux grappes et aux charges de travail en indiquant le nombre de grappes et de charges de travail ajoutées, supprimées, modifiées et inchangées.

Le reste de la vue est organisé sous forme de liste de groupes dans l'ordre d'ajout, de suppression, de modification et de changement, chaque couleur étant codée pour refléter l'état ainsi que le nombre de charges de travail ajoutées ou supprimées de la grappe.

Vous pouvez rechercher un groupe ou une charge de travail en particulier par son nom ou son adresse IP. Pour voir comment le contenu d'une grappe a changé, cliquez sur l'une des lignes représentant une grappe pour développer cette ligne.

Note Par défaut, les grappes inchangées sont masquées. Pour afficher les grappes inchangées, cliquez sur le bouton avec l'icône en forme d'œil.

Figure 34: Vue des différences de la grappe



What to do next

Pour afficher une comparaison similaire pour les politiques, consultez Comparaison des versions des politiques : différence de politique.

Prévention de la modification des grappes lors des réexécutions de découverte automatique des politiques

Si vous ne souhaitez pas que la découverte automatique des politiques (anciennement ADM) modifie une grappe lorsque vous découvrirez automatiquement les politiques de l'espace de travail à l'avenir, approuvez la grappe.

Par exemple, approuvez la grappe si vous avez modifié la requête de grappe et que vous devez maintenant ajouter de nouvelles charges de travail à la portée et les regrouper sans affecter les politiques existantes. L'approbation de la grappe fige le contenu et les attributs de la grappe dans l'état actuel. La découverte automatique des politiques ne modifie pas les grappes approuvées.

Consultez Approbation des grappes, à la page 86.

Sinon, vous pouvez promouvoir la grappe en tant que filtre d'inventaire, qui ne sera jamais modifié par la découverte de politiques. Consultez Convertir une grappe en filtre d'inventaire, à la page 82.

Approbation des grappes

Note Consultez également Convertir une grappe en filtre d'inventaire, on page 82, qui peut être une option plus appropriée pour vos besoins.

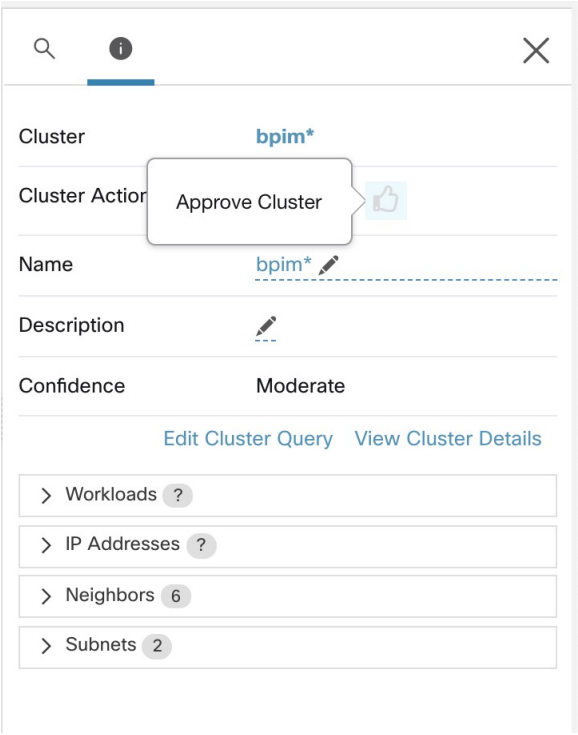
Après avoir approuvé une grappe, la découverte automatique ultérieure des politiques ne modifie pas la requête de cette grappe. Les adhésions aux grappes approuvées ne peuvent changer que si les membres de l'espace de travail changent.

Les charges de travail qui sont membres d'une grappe approuvée peuvent être appelées « charges de travail approuvées ».

Pour approuver une grappe :

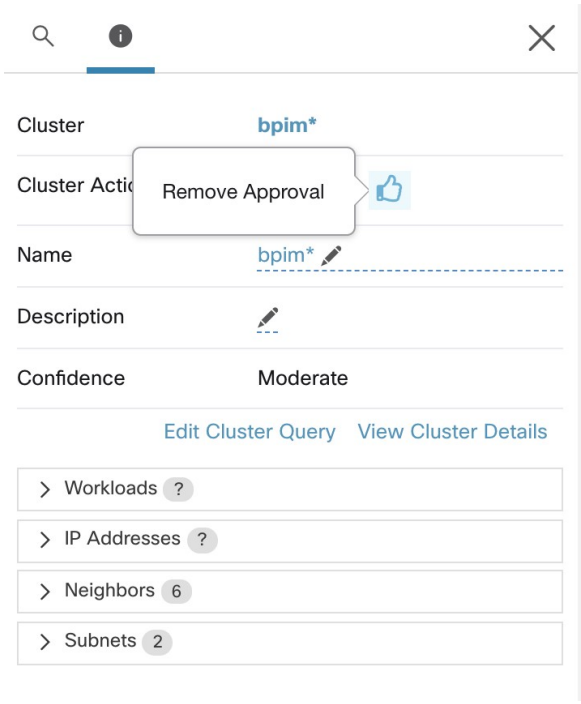
Vérifiez que la grappe qui vous intéresse est affichée sur le panneau latéral. Pour ce faire, vous devez rechercher la grappe ou cliquer sur la grappe souhaitée sur le tableau dans l'un des affichages. Ensuite, cochez la case dans le coin supérieur droit des informations de grappe sur le panneau latéral, comme illustré ci-dessous. Une fois qu'une grappe est approuvée, elle indique qu'elle restera inchangée par la future découverte automatique de politiques.

Figure 35: Approbation des grappes



Pour supprimer l'approbation d'une grappe, cliquez sur l'icône d'approbation .

Figure 36: Suppression de l'approbation d'une grappe



Aborder les complexités de la politique

Les résultats de l'application sont concernés par des facteurs tels que les éléments suivants :

- Type et rang de règle :
  - Politiques absolues et politiques par défaut
  - Le paramètre collecteur 'catch-all) pour l'espace de travail

  Consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 9.
- Ordre des politiques dans l'espace de travail

  Consultez Priorités des politiques, à la page 88.
- Politiques héritées des portées parents ou ancêtres, y compris la règle « collectrice »

  Vous devez vous assurer qu'une politique de priorité plus élevée n'atteint pas de trafic avant la politique qui est censée atteindre ce trafic.

  Pour connaître les incidences des politiques dans les portées ascendantes, exécutez une analyse en direct des politiques sur toutes les portées concernées. Consultez Analyse des politiques en temps réel, à la page 118.

  Lorsque vous êtes prêt à appliquer les politiques d'un espace de travail, un assistant vous indique quelles politiques héritées ont une incidence sur les charges de travail dans l'espace de travail. Pour en savoir plus, consultez Assistant d'application des politiques, à la page 136.
- Interactions avec les politiques entre portées

(Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes ou qu'une extrémité de la conversation se trouve dans une portée différente de celle de la politique)

Consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 94.

- Situations dans lesquelles le consommateur ou le fournisseur réel dans une politique peut différer des consommateurs et fournisseur configurés par défaut, par exemple dans des scénarios de basculement.

  Consultez Consommateur ou fournisseur réel, à la page 107.

Priorités des politiques

Le traitement du trafic est affecté par :

- La priorité des politiques dans la portée; et
- Ordre global des politiques et résolution des conflits, on page 88

les priorités des politiques dans une portée

Dans un espace de travail, l'ordre des politiques dans la liste reflète la priorité relative de chaque politique, la politique de priorité la plus élevée en haut de la liste et la politique de priorité la plus faible en bas de la liste.

Dans chaque espace de travail, les politiques absolues ont priorité sur les politiques par défaut, et la politique Collectrice est la politique de priorité la plus basse de l'espace de travail.

Pour de plus amples renseignements, consultez la section Rang de politique : Absolue, Par défaut et Collectrice, on page 9.

Ordre global des politiques et résolution des conflits

Des conflits peuvent survenir entre différentes politiques définies dans différentes portées. Plus précisément, des conflits surviennent pour les charges de travail (éléments de l'inventaire) qui appartiennent à plusieurs portées, comme parent/enfant, lorsque ces portées ont des politiques contradictoires.

Il n'est pas possible de résoudre ces conflits manuellement en raison de la nature dynamique de l'appartenance à la portée; les charges de travail peuvent entrer et sortir de la portée à mesure que leurs propriétés changent. Par conséquent, le système applique un ordre global à toutes les politiques, comme décrit ci-dessous, en fonction de la portée dans laquelle elles sont définies. Pour chaque charge de travail, la liste des politiques pertinentes (selon le consommateur/fournisseur/portée) est identifiée et triée par ordre global. La décision d'autoriser ou d'abandonner un flux est prise en fonction de la *première* politique correspondante de la liste triée.

En comprenant le schéma d'ordre général des politiques de sécurité, les administrateurs réseau peuvent définir les portées correctes et leurs priorités pour appliquer l'ensemble des politiques souhaitées sur les charges de travail. Dans chaque portée, les propriétaires d'applications conservent la capacité d'appliquer des politiques précises sur leurs charges de travail respectives.

Une politique de réseau global présente les caractéristiques suivantes :

- Un ensemble de portées classées par priorité (priorité la plus élevée en premier).
- L'espace de travail principal de chaque portée comporte des politiques absolues, des politiques par défaut et une action collectrice (catch-all) globale.

- Chaque groupe de politiques absolues ou par défaut de chaque espace de travail est trié en fonction de ses priorités locales (la plus élevée en premier).

L'ordre global des politiques est défini comme suit :

- Groupes de politiques absolues des espaces de travail principaux de toutes les portées (classés de la priorité la plus élevée à la plus faible).
- Groupes de politiques par défaut de l'espace de travail principal, toutes les portées (classés de la priorité la plus basse à la plus élevée).
- Politiques collectrices globales de toutes les portées (classées de la priorité la plus basse à la plus élevée).

Notez que l'ordre de portée s'applique aux groupes de politiques des catégories 1 et 2 plutôt qu'aux politiques individuelles. Dans chaque groupe, les politiques individuelles ayant des numéros de priorité de politiques inférieurs prévalent.

Pour une charge de travail spécifique, le sous-ensemble de portées auquel elle appartient est déterminé, puis l'ordre ci-dessus est appliqué. La politique globale de l'espace de travail de priorité la plus basse (appliquée) auquel cette charge de travail appartient est la règle collectrice applicable (mais une politique absolue ou par défaut peut la remplacer). Pour un flux donné sur cette charge de travail, l'action de la politique de correspondance la plus élevée est appliquée.

Note

- Si un espace de travail n'a ni politique absolue ni politique par défaut définies, il est ignoré. La politique collectrice globale de l'espace de travail ne sera pas incluse dans l'ordre global.
- L'ordre des politiques par défaut dans l'ordre global est inversé par rapport aux priorités de la portée. Cela vous permet de définir des politiques générales pour toutes les portées afin de sécuriser le périmètre de tous les espaces de travail, y compris ceux pour lesquels l'application des politiques n'est pas activée. Dans le même temps, les propriétaires d'applications qui ont activé la mise en application sur leur portée ont la possibilité de remplacer ces politiques par défaut.
- Le chevauchement des portées n'est pas recommandé. Consultez Chevauchement de portée pour en savoir plus. Toutefois, si une charge de travail comporte au moins deux interfaces, dans des portées qui se chevauchent ou disjointes, la politique collectrice catch-all de l'espace de travail de priorité le plus bas pour laquelle la mise en application est activée s'appliquera (parmi toutes les politiques collectrices applicables).

Nous développons notre exemple précédent à trois portées pour illustrer ce schéma de commande. Supposons que les priorités suivantes sont attribuées aux trois portées Utiliser des espaces de travail pour gérer les politiques pour obtenir des instructions sur la façon de modifier les priorités de portées) :

1. Applis
2. Applis RH
3. Applis Commerce

L'espace de travail principal de chacune de ces portées comporte des politiques absolues, des politiques par défaut et une action collectrice. Chaque groupe de politiques absolues ou par défaut de chaque espace de travail est trié en fonction de ses priorités locales.

L'ordre global des politiques est le suivant :

1. Politiques absolues Applis
2. Politiques absolues Applis RH
3. Politiques absolues Applis Commerce
4. Politiques par défaut Applis Commerce
5. Politiques par défaut Applis RH
6. Politiques par défaut Applis
7. Politique collectrice Applis Commerce
8. Politique collectrice Applis RH
9. Politique collectrice Applis

Une charge de travail qui appartient à la portée *Applis* ne recevra que les politiques suivantes dans l'ordre donné :

1. Politiques absolues Applis qui correspondent à la charge de travail
2. Politiques par défaut Applis
3. Politique collectrice Applis

Une charge de travail qui appartient aux portées *Applis* et *Applis Commerce* ne reçoit que les politiques suivantes dans l'ordre donné :

1. Politiques absolues Applis
2. Politiques absolues Applis Commerce
3. Politiques par défaut Applis Commerce
4. Politiques par défaut Applis
5. Politique collectrice Applis Commerce

Une charge de travail qui appartient aux portées *Applis* et *Applis RH* ne recevra que les politiques suivantes dans l'ordre donné :

1. Politiques absolues Applis
2. Politiques absolues Applis RH
3. Politiques par défaut Applis RH
4. Politiques par défaut Applis
5. Politique collectrice Applis RH

Ordre des politiques et chevauchement des portées

Important Le scénario suivant comporte des portées qui se chevauchent. Vous devez éviter que des portées connexes ne se chevauchent : les charges de travail ne doivent pas être membres de plusieurs branches de l'arborescence de la portée. Pour en savoir plus, consultez Chevauchement de portée.

Une charge de travail qui appartient aux trois portées *Applis*, *Applis RH* et *Applis Commerce* recevra les politiques suivantes dans l'ordre donné :

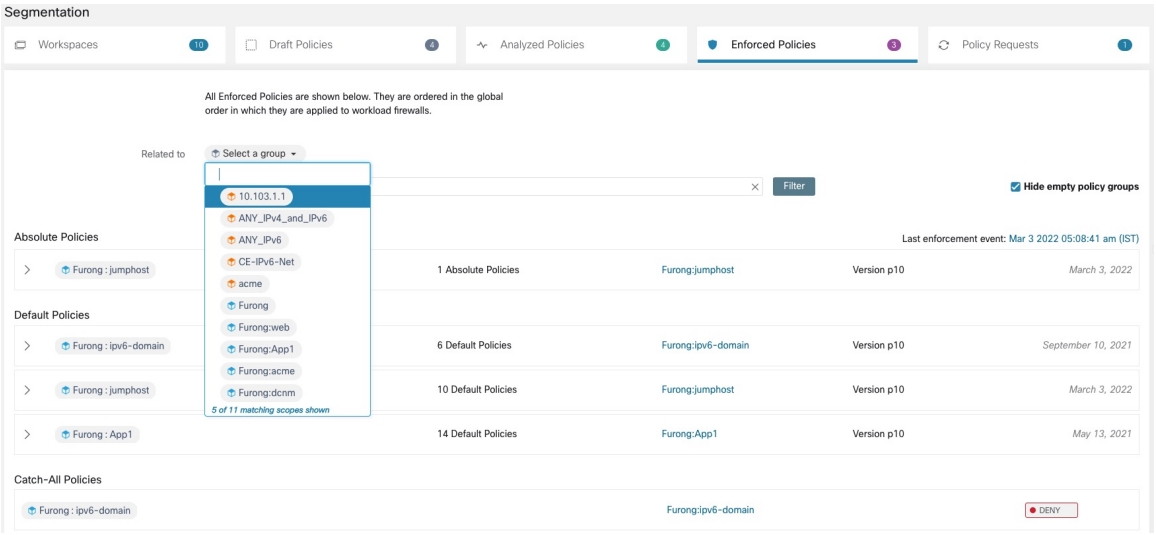
1. Politiques absolues Applis
2. Politiques absolues Applis RH
3. Politiques absolues Applis Commerce
4. Politiques par défaut Applis Commerce
5. Politiques par défaut Applis RH
6. Politiques par défaut Applis
7. Politique collectrice Applis Commerce

Notez que l'ordre relatif des portées *Applis RH* et *Applis Commerce* n'a d'importance que si les deux portées se chevauchent (c'est-à-dire si certaines charges de travail appartiennent aux deux portées connexes). En effet, les politiques sont toujours définies dans une portée. Une charge de travail appartenant à une seule portée ne sera pas affectée par les politiques de l'autre portée, donc l'ordre n'a pas d'importance.

Valider l'ordre et la priorité des politiques

Pour valider l'ordre et la priorité des politiques dans les espaces de travail parents/ancêtres, cliquez sur l'onglet **Analyzed Policies** (Politiques analysées) ou **Enforced Policies** (Politiques appliquées) en haut de la page Defend (Défendre) > Segmentation (Segmentation). Ces affichages fournissent une vue globale des politiques analysées et appliquées respectivement.

Figure 37: Exemple : liste des politiques appliquées par ordre de priorité



- Pour limiter la liste de politiques à celles qui incluent une portée ou un filtre particulier en tant que consommateur ou fournisseur, sélectionnez une portée ou saisissez un filtre.
- Filtres disponibles :

Nom du filtre	Définition
Port	Port de politique à mettre en correspondance, par exemple 80.
Protocol	Protocole de politique à mettre en correspondance, p. ex., TCP.
Approuvé	Correspond aux politiques qui ont été marquées comme Politiques approuvées
External? (Externe?)	Politiques dans lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes.
Action	Action de la politique : Allow (Autoriser) ou Deny (Refuser)

(Avancé) Modifier les priorités de la politique

⚠

Mise en garde Il est rarement nécessaire de modifier l'ordre de priorité des politiques de portée. Étant donné que la modification des priorités des politiques peut affecter les résultats de la mise en application sur tous les espaces de travail, procédez avec prudence.

L'accès à cette fonctionnalité est limité aux utilisateurs ayant des rôles à privilèges très élevés, tels qu'un administrateur du site.

Avant de commencer

Avant de modifier l'ordre de priorité de la portée :

- Comprendre la logique de tri des politiques et comment les priorités des politiques sur les portées se reflètent dans l'ordre des intents de politique individuelles. Consultez Priorités des politiques, à la page 88.
- Effectuez les modifications dans un espace de travail secondaire jusqu'à ce que vous soyez sûr que le nouvel ordre sera conforme aux attentes.
- Planifiez vos modifications en tenant compte des directives suivantes :

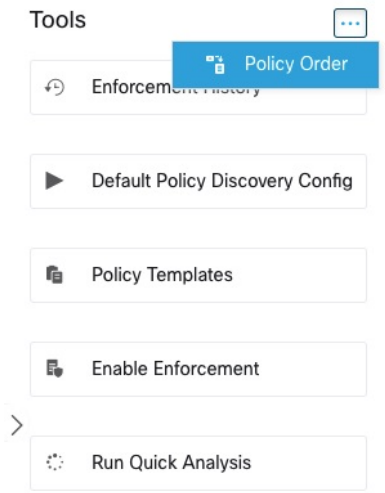
  Lors de la réorganisation, conservez l'ordre des parents en premier (les portées parents au-dessus des portées enfants) afin de tirer parti de la structure hiérarchique de votre arborescence de portées.

  (Si vous avez des portées jumelles qui se chevauchent, il peut être nécessaire de réorganiser ces dernières et leurs enfants. Le chevauchement des portées n'est pas recommandé. Corrigez ces problèmes en mettant à jour les requêtes de portée. Voir Chevauchement de portée).

Procédure

Étape 1 Pour réorganiser la priorité des politiques, cliquez sur l'icône de menu à côté de **Tools** (Outils) et sélectionnez **Policies Order** (Ordre des politiques) :

Illustration 38 : Accès à la page des priorités de politique

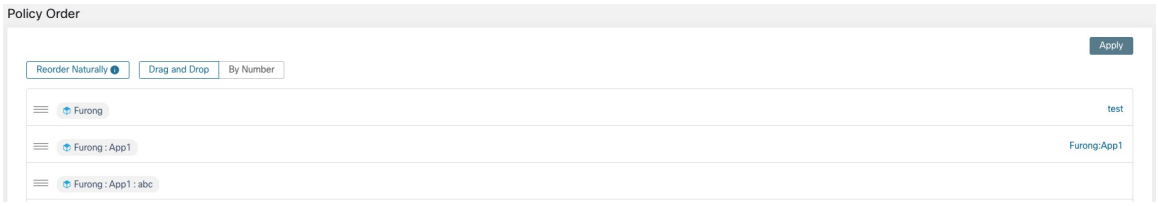


Une fois sur la page de l'ordre des politiques, vous pouvez voir la liste de toutes les portées et de leurs espaces de travail principaux correspondants en fonction de la priorité actuelle des politiques.

Étape 2 Il existe plusieurs façons de réorganiser les portées :

- Pour réorganiser la liste complète afin de placer les portées parentes au-dessus des portées enfants (« ordre préalable ») : Cliquez sur **Réorganiser naturellement**. Il s'agit de l'ordre recommandé et tout écart par rapport à cet ordre doit être effectué avec prudence.
- Pour réorganiser la liste manuellement :
  - Faites glisser les lignes vers le haut ou vers le bas.
  - Cliquez sur **By Number** (par numéro) pour définir un numéro pour chaque portée à utiliser pour le tri. Cela peut être plus facile pour les listes volumineuses.

Illustration 39 : Définition des priorités de politique pour les portées



Prochaine étape

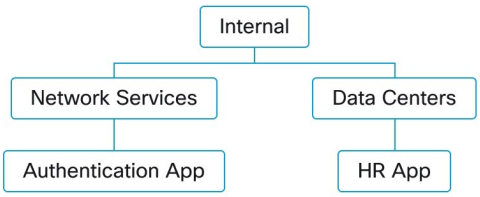
Exécutez l'analyse rapide pour afficher les résultats de vos modifications.

Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques

Exemple de scénario

La situation suivante est un exemple illustrant le trafic entre portées :

Votre hiérarchie de portée comprend une portée de services réseau qui comprend une application d'authentification (le fournisseur). Une application RH, membre d'une portée située sur une autre branche de la hiérarchie des portées, est un consommateur du service fourni par l'application d'authentification.



Options de politiques

Cisco Secure Workload offre plusieurs façons de résoudre cette situation :

Option	Instructions	Avantages et inconvénients
Créez ces politiques dans une portée parente ou ancestrale qui inclut à la fois le consommateur et le fournisseur en tant qu'enfants ou descendants.	• Créez manuellement une ou plusieurs politiques dans la portée ancestrale commun. (Facultatif) Pour des politiques plus précises, regroupez les charges de travail à l'aide de filtres d'inventaire. Pour obtenir des exemples et des instructions, consultez Créer un filtre d'inventaire. • Détectez automatiquement les politiques dans la portée ancestrale commune, pour la branche entière de l'arborescence de la portée.	Ces méthodes constituent le moyen le plus simple d'aborder les politiques à portée multiple. Ces méthodes ne nécessitent qu'une seule politique par paire consommateur-fournisseur. Si vous envisagez d'utiliser la découverte automatique des politiques, consultez les considérations importantes dans Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, on page 25.
Utiliser la méthode avancée pour créer des politiques à portées croisées	Détectez automatiquement les politiques pour chaque portée. Consultez (Avancé) Créer des politiques de portées croisées, on page 95. (Cette procédure s'applique aux politiques créées manuellement et aux politiques découvertes).	Cette méthode nécessite deux politiques pour chaque paire client-fournisseur : une politique pour le client et une pour le fournisseur. Cette méthode permet la création de politiques lorsque les politiques d consommateur et du fournisseur appartiennent à des personnes différentes. Reportez-vous aux autres considérations en Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, on page 25.

(Avancé) Créer des politiques de portées croisées

Cette procédure décrit la méthode avancée de création de politiques à portée croisée (politiques dans lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes). Elle s'applique aux politiques créées manuellement et aux politiques détectées automatiquement.

Cette méthode nécessite deux politiques pour chaque paire consommateur-fournisseur, car les deux extrémités de la conversation doivent autoriser la conversation :

- Une politique dans la portée consommateur doit autoriser les conversations avec le fournisseur,

  et

- Une politique dans la portée du fournisseur doit autoriser les conversations avec le consommateur.

Cette procédure comprend les étapes qui doivent être suivies par le propriétaire de chaque portée afin de créer des politiques inter-portées. Si vos privilèges d'accès vous permettent de modifier les deux portées, vous pouvez effectuer toutes les étapes.

Avant de commencer

- Envisagez des options plus simples pour gérer le trafic entre les portées. Consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 94.
- Les politiques qui utilisent cette méthode doivent être créées dans l'espace de travail principal du consommateur et du fournisseur.

  Si la portée du fournisseur à spécifier dans la politique n'a pas encore d'espace de travail principal, créez-le avant de créer des politiques de portée croisée à l'aide de cette méthode.
- Les politiques doivent comporter l'action ALLOW (AUTORISER) pour que des demandes de politiques soient créées.
- Pour plus de détails sur ces exigences, consultez Demandes de politiques, à la page 97.
- (Facultatif) Envisagez des options de traitement automatique des demandes de politiques à portée croisée. Consultez Automatiser le traitement des demandes de politique globales, à la page 101.
- (Facultatif) Si vous souhaitez que les politiques multiportées ne s'appliquent qu'aux charges de travail d'une grappe dans la portée du consommateur ou du fournisseur, et non à la portée entière, consultez Convertir une grappe en filtre d'inventaire, à la page 82. Les grappes ne peuvent pas être utilisées dans les politiques à portée croisée créées à l'aide de cette procédure.

  Si vous détectez les politiques automatiquement, consultez aussi Dépendances externes, à la page 34 et Ajuster les dépendances externes d'un espace de travail, à la page 36.

Procédure

Étape 1 Dans l'espace de travail principal du consommateur, créez la politique souhaitée, manuellement ou à l'aide de la découverte automatique des politiques.

Pour chaque politique inter-portée créée, une demande de politique est automatiquement créée pour le fournisseur.

Pour afficher les demandes de politique, consultez Affichage, acceptation et refus des demandes de politique, à la page 97.

Remarque : Si une politique existante dans l'espace de travail de l'application du fournisseur correspond à ce trafic, une nouvelle politique n'est pas nécessaire et la demande n'est pas créée. Cette situation est signalée comme décrit dans Demandes de politiques résolues, à la page 105.

Étape 2 Vous (ou le propriétaire de l'application du fournisseur) devez répondre à chaque demande de politique :

Consultez Affichage, acceptation et refus des demandes de politique, à la page 97.

L'acceptation d'une demande de politique crée automatiquement la politique requise dans l'espace de travail principal du fournisseur, permettant le trafic entre les deux applications.

Si vous ne souhaitez pas autoriser le trafic de l'application requérante, rejetez la demande.

Étape 3 (Facultatif) Si vous découvrez automatiquement les politiques, vous pouvez Ajuster les dépendances externes d'un espace de travail, à la page 36.

Étape 4 Passez en revue et analysez les deux espaces de travail principaux.

Prochaine étape

Lorsque vous êtes prêt à appliquer ces politiques, vous devez les appliquer sur les deux espaces de travail principal.

Demandes de politiques

Les demandes de politique sont générées lorsque vous créez des politiques inter-portées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 95. Chaque fois qu'une politique est créée dans l'espace de travail principal d'une portée de consommateur lorsque le fournisseur est membre d'une portée différente, si la politique n'existe pas encore dans l'espace de travail principal associé à la portée du fournisseur, une demande de politique est générée.

Cette demande de politique alerte le propriétaire de l'application du fournisseur pour permettre aux applications tributaires d'accéder aux services nécessaires.

Consultez les options d'affichage et de réponse aux demandes de politique aux adresses Affichage, acceptation et refus des demandes de politique, on page 97 et Automatiser le traitement des demandes de politique globales, on page 101.

Renseignements supplémentaires sur les demandes de politique

- La page des services fournis (sur laquelle les demandes de politique apparaissent) n'est disponible que pour les espaces de travail principaux. Ainsi, des expériences isolées sur des espaces de travail secondaires ne créent pas de notifications dans d'autres espaces de travail principaux.
- Si une portée externe (lorsque le fournisseur spécifié dans la politique appartient à une autre portée que le consommateur) n'a pas d'espace de travail principal, aucune demande n'est envoyée (par exemple, cela peut être le cas pour la portée racine ou toute autre portée définie pour les charges de travail à l'extérieur de l'organisation). Si une portée externe n'a publié aucune politique, l'analyse et l'application de la politique sont effectuées du côté consommateur uniquement.
- Les grappes ne sont pas prises en charge lorsque le fournisseur se trouve dans une portée différente de celle du consommateur. Si le consommateur de la politique est une grappe, la demande de politique sera effectuée comme si la demande de politique provenait de la portée de l'application consommateur. Plusieurs politiques utilisant le même service d'un fournisseur pourraient être regroupées.
- Les demandes de politiques sont générées uniquement pour les fournisseurs, et non pour les consommateurs. Si un espace de travail consommateur analyse ou applique des politiques, il doit inclure explicitement des politiques qui autorisent tous ses flux de consommation légitimes, soit par le biais de la découverte automatique des politiques, soit en élaborant explicitement des politiques (aucune demande de politiques des espaces de travail de fournisseurs externes n'est générée).

Affichage, acceptation et refus des demandes de politique

Lors de la création de politiques multiportées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 95, une politique est requise dans l'espace de travail principal de la portée du fournisseur en plus de la politique dans la portée du consommateur. Lorsqu'une politique multiportée est créée dans l'espace de travail principal de la portée du consommateur, une demande de politique est automatiquement créée dans l'espace de travail principal de la portée du fournisseur.

Utilisez les informations de cette rubrique pour accepter la demande (pour créer la politique requise dans la portée du fournisseur) ou rejeter la demande (auquel cas la politique multiportée ne prendra pas effet).

Pour afficher, accepter ou refuser des demandes de politique :

Destinataire	Faire ceci
Afficher toutes les demandes de politique	**1.** Choisissez **Defend (défense) > Segmentation (segmentation).** **2.** Cliquez sur **Policy Requests** (Demandes de politiques) en haut de la page. **3.** Cliquez sur une portée de consommateur pour afficher les demandes de politique de cette portée.
Afficher les demandes de politique pour une portée particulière	Pour afficher les demandes de politique en attente pour la portée d'un fournisseur : **1.** Choisissez **Defend (défense) > Segmentation (segmentation).** **2.** Cliquez sur l'espace de travail principal de la portée applicable. **3.** Cliquez sur **Manage Policies** (Gestion des politiques). **4.** Cliquez sur **Provided Services** (Services fournis). Si l'onglet n'affiche pas un numéro, il n'y a aucune demande de politique en attente pour cet espace de travail. **5.** Cliquez sur **Policy Requests**(demandes de politiques). **6.** Cliquez sur une portée de consommateur pour afficher les demandes de politique de cette portée. Ou Pour afficher une demande de politique à partir de la portée consommateur : Dans l'onglet Policies (Polices) de l'espace de travail principal de la portée consommateur, cliquez sur la valeur de la colonne **Protocols and Ports** (protocoles et ports), puis examinez le panneau qui s'ouvre sur le côté droit de la page. Dans la section **Protocols and Ports** (protocoles et ports), cliquez sur un point jaune pour voir les demandes de politique en attente.
Accepter manuellement une demande et créer automatiquement la politique requise dans la portée du fournisseur	À partir de l'un des emplacements ci-dessus, cliquez sur **Accept** (accepter) à côté de la demande de politique.
Rejeter manuellement une demande	À partir de l'un des emplacements ci-dessus, cliquez sur **Reject** (Rejeter) à côté de la demande de politique.

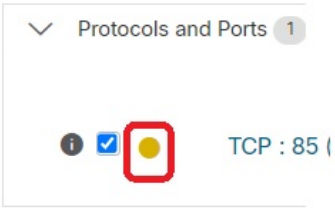
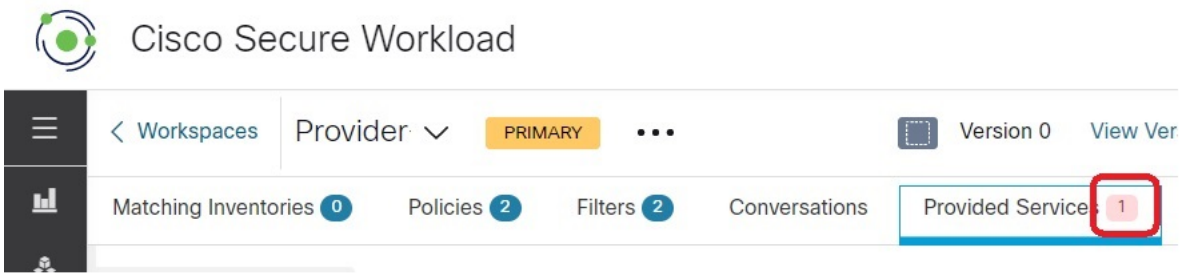
Destinataire	Faire ceci
Afficher l'état de la demande de politique à partir de l'espace de travail du consommateur	Dans la page Policies (Politiques) de l'espace de travail du consommateur principal, cliquez sur la politique, puis sur la valeur du port/du protocole. L'état est affiché dans le panneau qui s'ouvre sur la droite. Les demandes en attente sont accompagnées d'un point jaune :  Lorsque la demande est acceptée, le point se transforme en coche verte :  Cliquez sur l'indicateur pour en savoir plus.
Afficher l'état de la demande de politique à partir de l'espace de travail du fournisseur	Affichez l'état de la demande sous l'onglet **Provided Services** (Services fournis) décrit ci-dessus.
Autoriser la découverte de politiques à créer la politique requise pour le fournisseur	Détectez automatiquement les politiques dans l'espace de travail principal de la portée du fournisseur en utilisant une plage temporelle qui garantit que les flux correspondants sont visibles, puis publiez la politique.
Consultez aussi les options d'automatisation du traitement des demandes de politique	Automatiser le traitement des demandes de politique globales, on page 101

Figure 40: Demandes de politique en attente dans l'espace de travail du fournisseur



Acceptation des demandes de politique : détails

Accepter une demande de politique sur un service équivaut à créer une politique à partir du filtre demandé, en tant que consommateur, vers le service, en tant que fournisseur. De plus, lors de l'acceptation d'une demande de politique, la politique d'origine de l'espace de travail de l'application consommateur (dans l'exemple, l'application frontale et la couche de service) sera marquée comme acceptée (voir les figures i-dessous).

Figure 41: Acceptation/rejet des demandes de politique

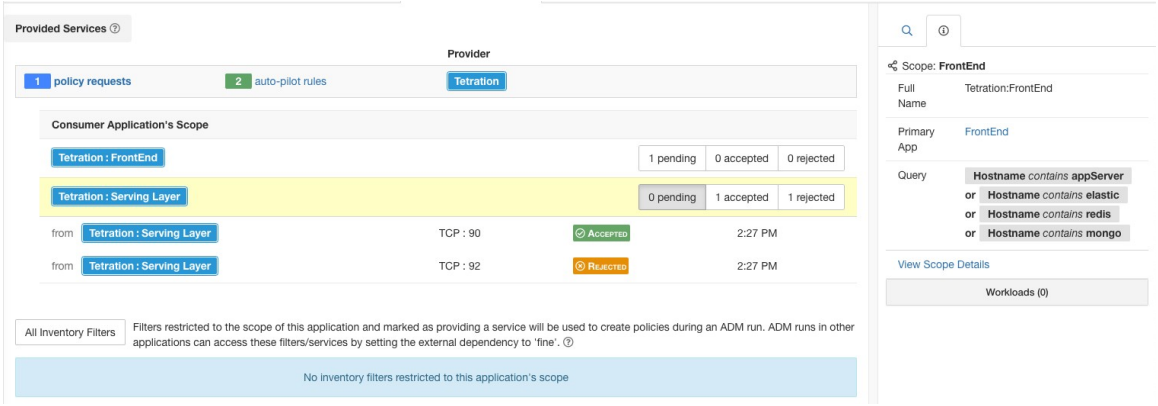
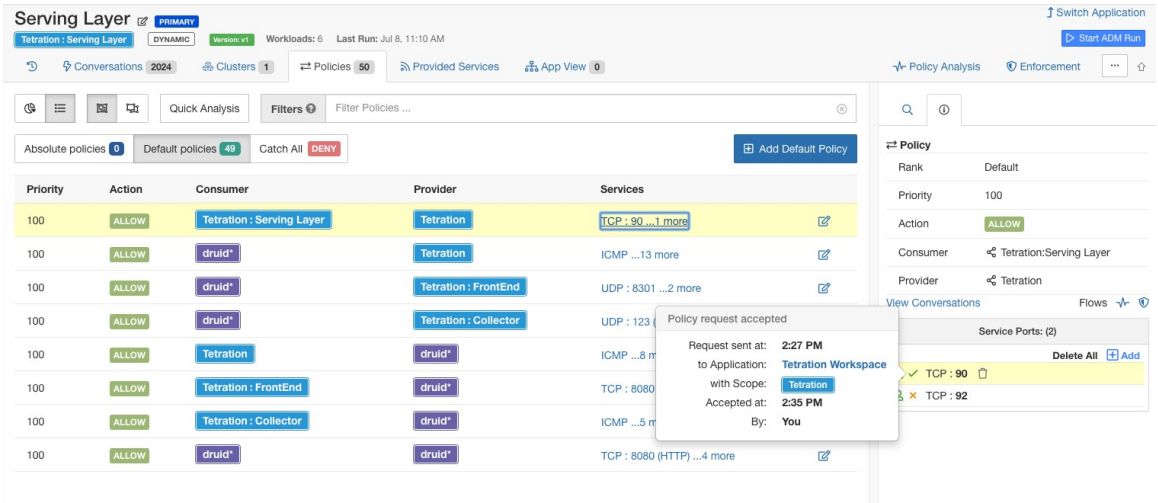


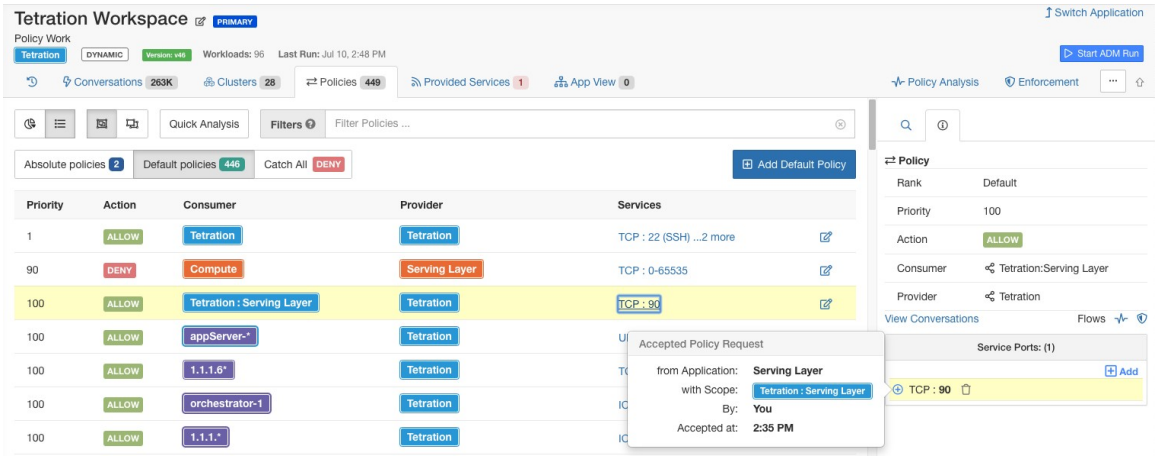
Figure 42: État de la politique affiché comme accepté



La nouvelle politique créée sur l'espace de travail de l'application du fournisseur (dans cet exemple, l'espace de travail est nommé Tetration) est marquée d'un icône **plus** indiquant que cette politique a été créée en raison d'une demande de politique externe.

Note Si la politique d'origine du côté du consommateur est supprimée après l'acceptation de la demande de politique, la politique du côté du fournisseur ne sera pas supprimée. Cependant, l'info-bulle à côté de la politique indique que la politique d'origine a été supprimée avec l'horodatage de l'événement :

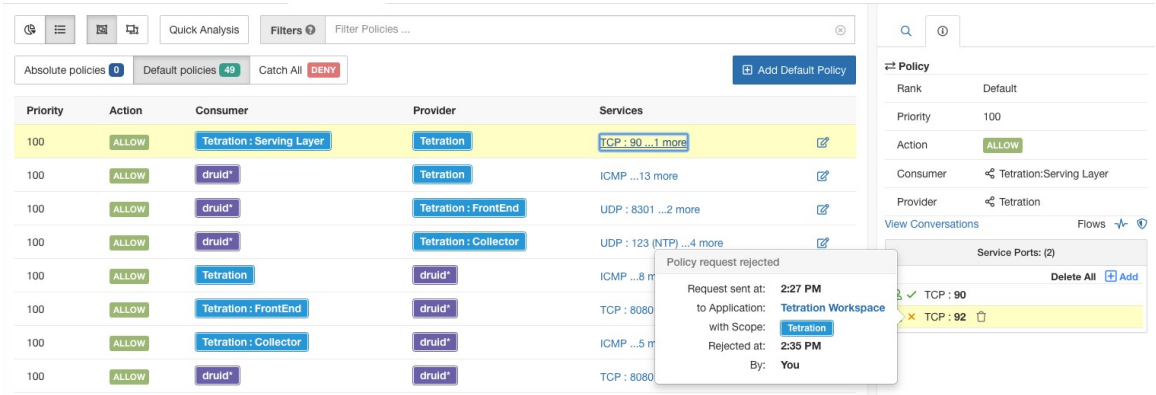
Figure 43: Politique du côté du fournisseur, créée en acceptant une demande de politique



Rejet des demandes de politique : Détails

Le rejet d'une demande de politique n'entraîne ni la création ni la mise à jour de politiques. La politique d'origine de l'espace de travail de l'application consommateur (dans l'exemple, application de la couche de service) sera marquée comme rejetée, mais la politique reste en vigueur, c'est-à-dire que le trafic sortant sera toujours autorisé. L'info-bulle à côté de la politique de rejet contient des informations sur l'application du fournisseur, l'utilisateur qui a rejeté la demande de politique ainsi que l'heure du rejet.

Figure 44: État de la politique affiché comme Rejeté



Automatiser le traitement des demandes de politique globales

Les demandes de politique sont générées lorsque vous créez des politiques inter-portées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, à la page 95.

Il existe plusieurs options pour réduire le nombre de demandes de politiques générées lors de la création de politiques inter-portées :

Tableau 5 : Options de traitement automatique des demandes de politique

Destinataire	Faire ceci
Préciser le traitement des demandes de politique entre des paires consommateur-fournisseur données	Consultez Règles de pilote automatique, à la page 102. Vous devez avoir les privilèges requis.
Créer automatiquement toutes les politiques requises pour les fournisseurs pour toutes les politiques de portées croisées créées lors de la découverte de politiques dans un espace de travail en particulier	Lorsque vous démarrez une exécution de découverte automatique de politique, activez l'option d' **Auto accept outgoing policy connectors** (Acceptation automatique des connecteurs de politique sortants) dans la section Advanced Configurations (Configurations avancées). Cette option est disponible uniquement pour les propriétaires de portée racine et les administrateurs de site. Pour de plus amples renseignements, consultez la section : Configurations avancées pour la découverte automatique des politiques, à la page 39 et Connecteurs de politiques d'acceptation automatique, à la page 104
Préciser le traitement par défaut pour toutes les demandes de politique de tous les espaces de travail	Dans la page de configuration de la découverte des politiques par défaut, activez l'option **Auto accept outgoing policy connectors** (Acceptation automatique des connecteurs de politiques sortants) dans la section Advanced Configurations (configurations avancées). Cette option est disponible uniquement pour les propriétaires de portée racine et les administrateurs de site. Pour de plus amples renseignements, consultez la section : Configuration de la découverte de politiques par défaut, à la page 49 et Configurations avancées pour la découverte automatique des politiques, à la page 39 et Connecteurs de politiques d'acceptation automatique, à la page 104

Règles de pilote automatique

Cette fonctionnalité est applicable uniquement si vous créez des politiques à portée croisée en utilisant la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 95.

Les applications d'infrastructure qui fournissent des services à de nombreuses autres applications dans un centre de données peuvent recevoir un grand nombre de demandes de politique d'autres applications.

Vous pouvez réduire le volume des demandes de politiques en créant des règles de pilote automatique pour accepter ou rejeter automatiquement les futures demandes de politiques correspondantes.

Note Les règles du pilote automatique ne s'appliquent pas aux demandes de politiques existantes. Elles affectent uniquement les demandes de politiques futures.

Accepter ou rejeter automatiquement les demandes de politique à l'aide des règles de pilote automatique

Configurez les règles de pilote automatique pour accepter ou rejeter automatiquement les demandes de politique entre une paire consommateur-fournisseur donnée, sur des ports précisés. Les règles du pilote automatique peuvent être larges (portée à portée) ou s'appliquer uniquement à un sous-ensemble de charges de travail dans chaque portée (comme configuré par les filtres d'inventaire. Vous pouvez utiliser un filtre d'inventaire pour le consommateur, pour le fournisseur ou pour chacun d'entre eux).

1. Si vous souhaitez que votre règle de pilote automatique s'applique à un sous-ensemble de charges de travail au sein d'une portée plutôt qu'à l'ensemble de la portée :

   Créez un filtre d'inventaire dans la ou les portées pertinentes pour regrouper les charges de travail. Assurez-vous que l'option **Restrict Query to Ownership Scope** (Restreindre la requête à la portée de propriété) est sélectionnée dans chaque filtre d'inventaire, pour vous assurer que le filtre n'inclut que les charges de travail qui sont membres de la portée.

2. Choisissez **Defend (défense) > Segmentation (segmentation).**

3. Cliquez sur l'espace de travail principal de la portée du consommateur pour laquelle vous souhaitez accepter ou rejeter automatiquement les demandes de politique liées à un fournisseur spécifique.

4. Cliquez sur **Manage Policies** (Gestion des politiques).

5. Cliquez sur **Provided Services** (Services fournis).

6. Si vous créez cette règle pour un filtre d'inventaire, effectuez les étapes suivantes pour le filtre d'inventaire souhaité (les filtres d'inventaire sont identifiés par une icône orange).

   Sinon, effectuez ces étapes pour la portée (les portées sont identifiées par une icône bleue).

   Assurez-vous de cliquer au bon endroit.

7. Cliquez sur **No Auto-Pilote Rules** (aucune règle de pilote automatique) ou sur **auto-pilot Rules** (règles de pilote automatique), selon ce qui est affiché.

8. Cliquez sur **New Auto-Pilote Rule** (nouvelle règle de pilote automatique).

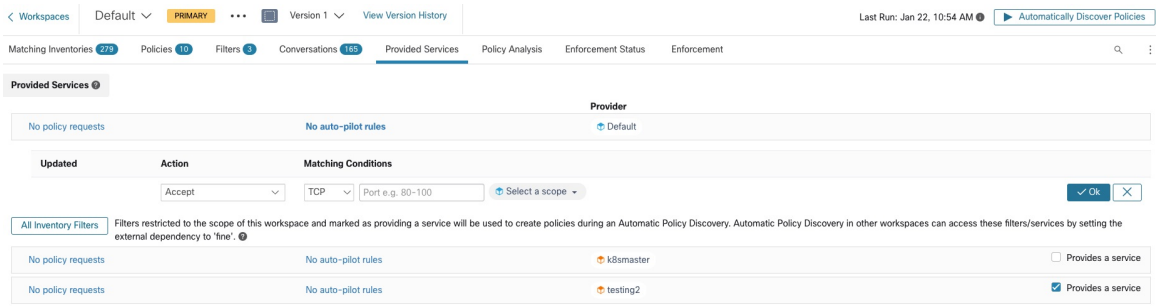
9. Configurez la règle de pilote automatique. Sélectionnez la portée ou le filtre d'inventaire qui représente le fournisseur.

10. Cliquez sur **OK**.

Exemple de règle de pilote automatique

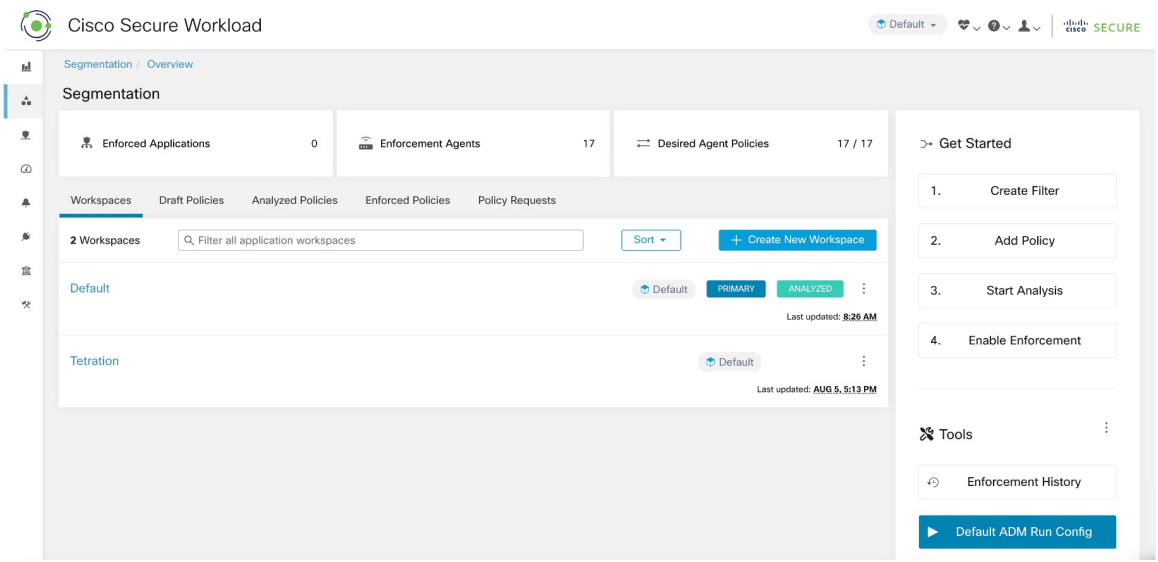
Dans l'exemple ci-dessous, nous créons une nouvelle règle de pilote automatique pour rejeter les demandes de politique TCP dans la plage de ports 1 à 200 de tout consommateur contenu dans Tetration:Adhoc du service du fournisseur Tetration

Figure 45: Création/mise à jour des règles du pilote automatique



Ensuite, nous créons une nouvelle politique dans l'espace de travail pour l'*application frontale* sur le port TCP 23. Comme la politique correspond à la règle de pilote automatique, elle sera automatiquement rejetée. L'état et le motif du refus de la politique sont indiqués dans l'info- bulle à côté de la politique rejetée.

Figure 46: Politique automatiquement rejetée par la règle de pilote automatique



Afficher le nombre des politiques récemment créées par les règles de pilote automatique

Pour afficher le nombre de politiques créées dans un espace de travail par les règles de pilote automatique depuis le dernier lancement (ou redémarrage) de l'analyse des politiques pour l'espace de travail :

Accédez à la page des services fournis pour l'espace de travail principal concerné et recherchez le nombre de politiques « créées automatiquement ».

Connecteurs de politiques d'acceptation automatique

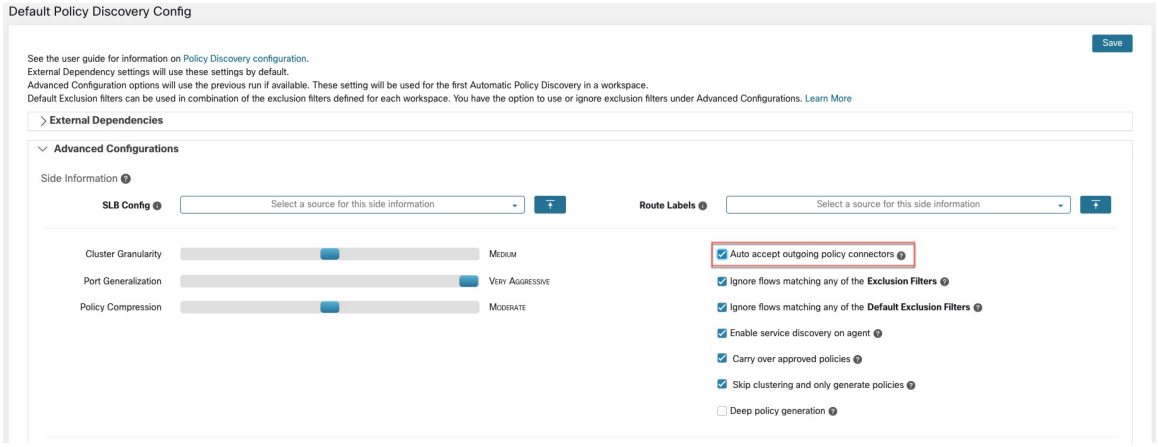
Vous pouvez définir cette option comme configuration de découverte de politiques par défaut, ou la définir dans les options avancées de découverte automatique des politiques pour chaque espace de travail.

L'option **Auto accept outgoing policy connectors** (Acceptation automatique des connecteurs de politique sortants) de la page de configuration de la découverte automatique des politiques vous permet d'accepter automatiquement toutes les demandes de politique créées dans le cadre de la découverte automatique des politiques.

Si cette option est activée dans la configuration de découverte automatique des politiques par défaut, les demandes de politiques créées manuellement ou en important un espace de travail seront également automatiquement acceptées.

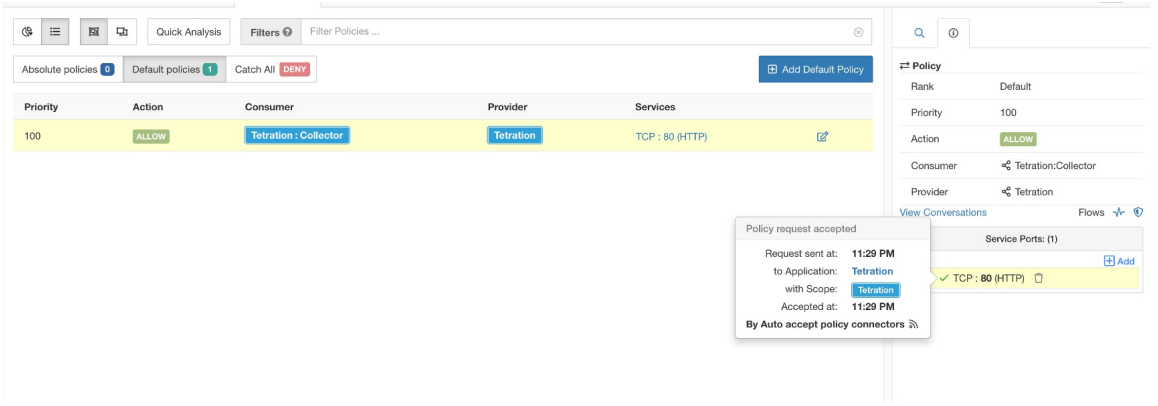
Note Cette option est uniquement disponible pour les propriétaires de portée racine ou les administrateurs de site .

Figure 47: L'option d'acceptation automatique des connecteurs de politique sortants



Une fois cette option définie, toute demande de politique créée dans un espace de travail, la portée racine ou dans l'espace de travail concerné sera automatiquement acceptée.

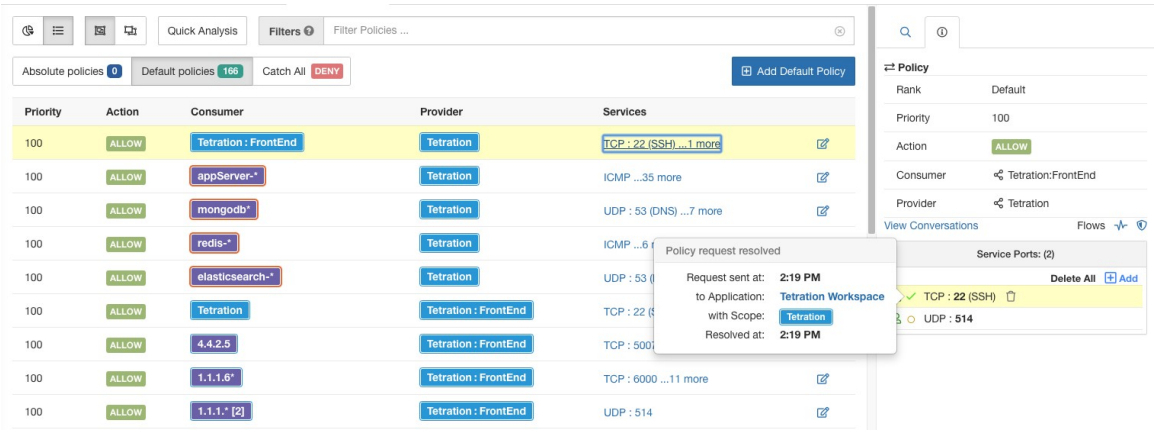
Figure 48: La politique est automatiquement acceptée par les connecteurs d'acceptation automatique de politiques



Demandes de politiques résolues

Si toutes les conditions pour la création d'une demande de politique sont réunies, mais qu'il existe déjà une politique correspondante sur l'espace de travail du fournisseur, la politique créée sur l'espace de travail de l'application client sera marquée comme résolue, ce qui indique que l'espace de travail de l'application du fournisseur autorise déjà le trafic via le port demandé.

Figure 49: État de la politique affiché comme Résolu



Services fournis

Cette page est utilisée uniquement pour la création de politiques dans lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes, et uniquement si vous utilisez la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 95.

Pour plus d'informations sur cette option, consultez :

- Demandes de politiques, on page 97
- Règles de pilote automatique, on page 102
- Créer un filtre d'inventaire et Dépendances externes, on page 34 (pour en savoir plus sur l'option **fournit un service**)

Pour accéder à cette page, accédez à un espace de travail principal, cliquez sur **Manage Policies** (Gérer des politiques), puis sur **Provided Services** (Services fournis).

Dépannage des politiques de portées croisées

Si des politiques de portée croisée ont été créées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, à la page 95, les espaces de travail principaux pour les charges de travail des consommateurs et des fournisseurs doivent chacun avoir une politique qui autorise le trafic. Assurez-vous que les politiques requises existent dans les deux espaces de travail.

Aucune notification n'est envoyée si l'une des politiques est supprimée ou modifiée.

Si la paire de politiques a été générée lors de la recherche de celles-ci, consultez les informations relatives à l'approbation des politiques afin de les protéger contre les recherches ultérieures. Consultez Approuver les politiques, à la page 51.

Vérifiez que les autres exigences sont toujours respectées, comme indiqué dans (Avancé) Créer des politiques de portées croisées, à la page 95.

Des espaces de travail pour les consommateurs et les fournisseurs ayant les politiques requises doivent être mis en application.

Outils utiles pour les politiques multi-portées

- Utiliser le filtre **External?** (Externe?) pour trouver les politiques dans lesquelles le fournisseur se trouve dans une portée différente de celle dans laquelle vous avez découvert les politiques.
- La vue des politiques comporte une option permettant d'afficher les politiques externes. Consultez Représentation visuelle des politiques, à la page 114.

Si vous utilisez la configuration de découverte de politiques par défaut

Assurez-vous d'avoir cliqué sur **Save (Enregistrer)** dans la page **Default Policy Discovery Config** (configuration de la découverte des politiques par défaut) après avoir apporté des modifications pour rendre les configurations de dépendances externes par défaut disponibles pour les espaces de travail individuels.

Consommateur ou fournisseur réel

Le consommateur et le fournisseur spécifiés dans une politique déterminent :

- L'ensemble des charges de travail dotées de d'agents Cisco Secure Workloadqui reçoivent la politique.
- L'ensemble des adresses IP qui sont affectées par les règles de pare-feu installées.

Par défaut, ce sont les mêmes.

Cependant, vous devrez peut-être spécifier un groupe d'adresses IP dans les règles de pare-feu différent des adresses IP des charges de travail qui reçoivent la politique. (Voir un exemple ci-dessous).

Pour répondre à ce besoin, vous pouvez configurer le consommateur et le fournisseur effectifs.

Comportement par défaut pour le consommateur et le fournisseur

Par défaut, lorsqu'un agent Cisco Secure Workload reçoit une politique, les règles de pare-feu sont spécifiques à cette charge de travail. C'est ce que l'exemple suivant illustre le mieux :

Considérons une politique ALLOW avec un filtre de fournisseur spécifiant le sous-réseau 1.1.1.0/24. Lorsque cette politique est programmée sur une charge de travail avec l'adresse IP 1.1.1.2, les règles de pare-feu se présentent comme suit :

- Pour le trafic entrant, les règles de pare-feu autorisent le trafic destiné à la version 1.1.1.2 en particulier et non à l'ensemble du sous-réseau 1.1.1.0/24.
- 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 (pour éviter l'usurpation d'identité).

En corollaire, les charges de travail d'agent appartenant à l'espace de travail qui n'ont pas d'adresse IP dans le sous-réseau 1.1.1.0/24 ne recevront pas les règles de pare-feu ci-dessus.

Exemple : consommateur réel ou fournisseur réel

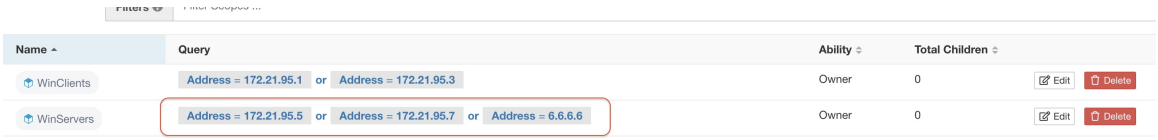
Dans cet exemple, supposons que vous configurez des politiques pour un parc de charges de travail derrière une adresse IP virtuelle (VIP), similaires aux solutions de mise en grappe Keepalive ou Windows avec basculement. Vous ferez appel à un consommateur ou à un fournisseur effectifs pour veiller à ce que le trafic ne soit pas interrompu lors d'un basculement.

Imaginez un parc de charges de travail avec des adresses IP (*172.21,95.5* et *172.21,95.7*) qui fournissent un service derrière une adresse VIP – *6.6.6.6*. Cette VIP est flottante et une seule charge de travail possède la

VIP à tout moment. L'objectif est de programmer des règles de pare-feu sur toutes les charges de travail du parc afin de permettre le trafic vers l'adresse *6.6.6.6*.

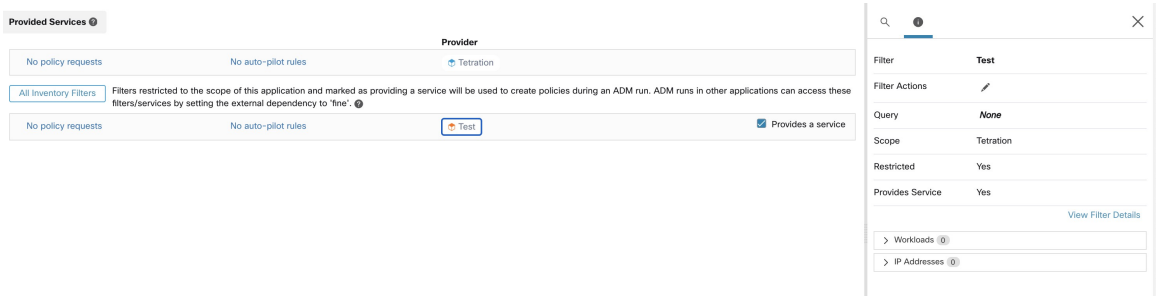
Dans cette configuration, nous avons une portée et un espace de travail correspondant qui contiennent un groupe de charges de travail qui représente le parc (*172.21,95.5* et *172.21,95.7*) ainsi que l'adresse VIP (*6.6.6.6*).

Figure 50: Portée incluant les VIP et les grappes de charges de travail



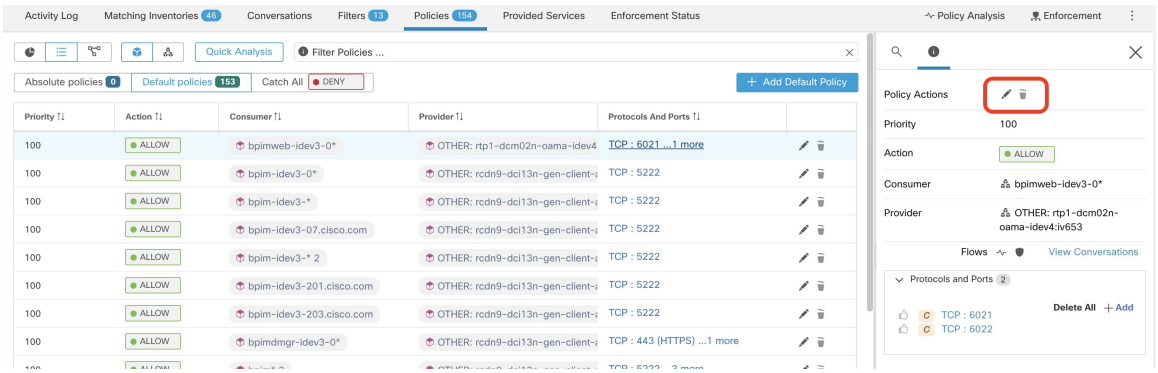
L'adresse VIP est accessible dans cet espace de travail en tant que service fourni, comme indiqué ci-dessous :

Figure 51: VIP accessible comme un service fourni



Si nous ajoutons une politique des clients de ce service à l'adresse VIP de service, les règles de pare-feu (par défaut) autorisant le trafic vers l'adresse VIP ne seront programmées que sur la charge de travail qui possède l'adresse VIP. Toutefois, en cas de basculement, il peut s'écouler un certain temps avant que la nouvelle charge de travail à laquelle appartient le service VIP ne reçoive les règles de pare-feu adéquates et le trafic peut être perturbé pendant un court laps de temps.

Figure 52: Politique autorisant le trafic des clients vers l'adresse VIP de service

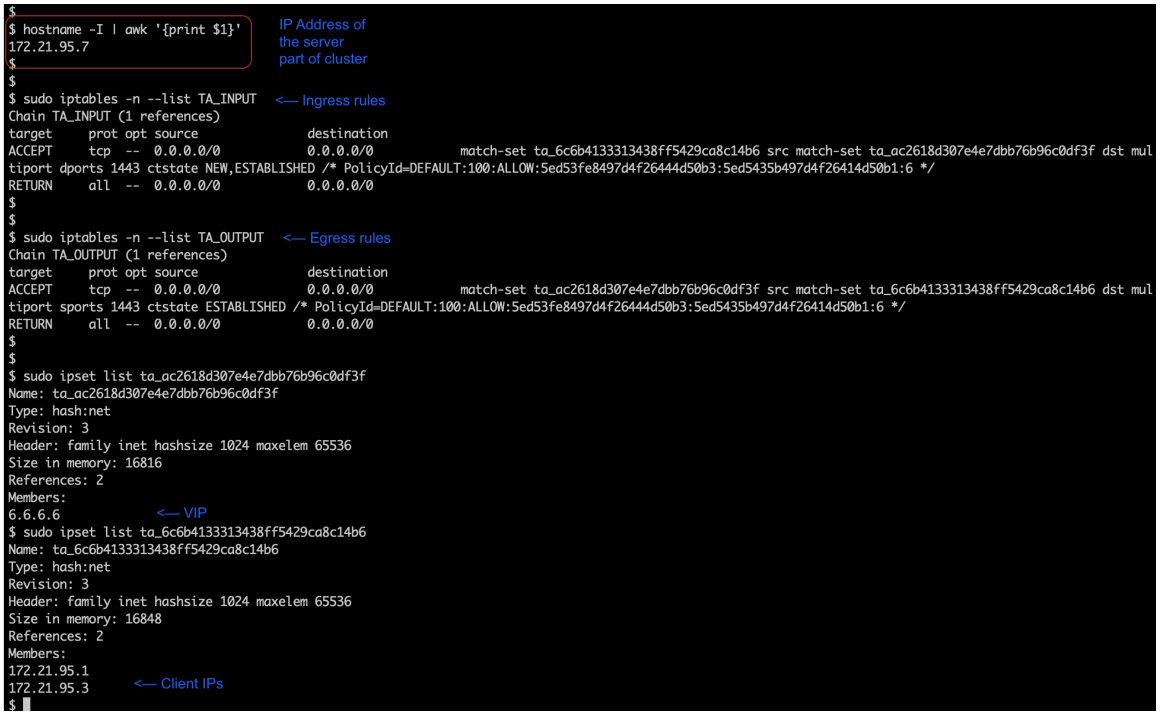


Pour résoudre ce problème, nous configurons le fournisseur effectif (en utilisant la procédure ci-dessous) Plus précisément, nous avons défini le fournisseur effectif de manière à inclure le groupe de charges de travail pour lesquelles des règles de pare-feu autorisant le trafic vers le service VIP doivent être programmées - peu importe que l'une de ces charges de travail possède ou non l'adresse VIP.

Lorsque le fournisseur effectif est défini, nous pouvons voir sur les charges de travail que les règles de pare-feu autorisant le trafic vers 6.6.6.6 sont programmées même lorsqu'une charge de travail ne possède pas l'adresse

VIP. Lorsque toutes les charges de travail qui soutiennent le service sont programmées avec ces règles, le trafic ne sera pas interrompu lors d'un événement de basculement, car les règles de pare-feu nécessaires seront programmées sur la nouvelle charge de travail principale (qui possède l'adresse VIP).

Figure 53: Règles de pare-feu sur l'hôte autorisant le trafic vers le service VIP



Comment configurer le consommateur réel ou le fournisseur réel

1. Cliquez sur la politique à modifier.
2. Cliquez sur le bouton Edit (modifier) dans le coin supérieur droit de la politique pour accéder aux options de politique avancées.
3. Cliquez sur **Effective Consumer** (Consommateur réel) ou **Effective Provider**(fournisseur réel).
4. Précisez les adresses souhaitées.
5. Vous devrez peut-être préciser des adresses à la fois pour le consommateur réel et pour le fournisseur réel.

À propos de la suppression de politiques

Important Avant de supprimer une politique, vérifiez qu'elle ne fait pas partie d'une paire de politiques requises lorsque le consommateur et le fournisseur se trouvent dans des portées différentes.

Pour le déterminer : Cliquez sur le lien de la politique dans la colonne Protocols and Ports (Protocoles et ports). Dans le panneau qui s'ouvre sur le côté droit de la page, examinez la section Protocols and Ports (protocoles et ports). Les politiques créées par l'acceptation d'une demande de politiques couvrant plusieurs portées sont indiquées par un signe + à côté du port et du protocole :

Cliquez sur le signe + pour afficher le créateur de la politique transversale et un lien vers la politique consommateur correspondante.

Remarque Les politiques suggérées par la recherche automatique de politiques qui n'ont pas été approuvées peuvent ne pas être présentes après une exécution ultérieure de la recherche de politiques, si les flux de trafic qui les ont produites ne sont pas observés au cours de l'exécution ultérieure. Pour conserver les politiques suggérées, consultez Approuver les politiques, à la page 51.

Examiner et analyser les politiques

Il est essentiel de vous assurer que vos politiques produisent les effets escomptés (et n'ont pas d'effets imprévus) avant de les appliquer.

Consulter les politiques découvertes automatiquement

Passez en revue les résultats de la découverte des politiques sur la page Policies (politiques) de l'espace de travail dans lequel vous avez découvert les politiques.

Commencez votre examen ici

Nous vous recommandons de commencer par vérifier si les politiques traitent de chacun des domaines suivants, dans l'ordre suggéré :

- Ports communs et essentiels
- Trafic Internet

- Trafic entre différentes applications (ces flux peuvent impliquer des charges de travail de différentes portées)
- Trafic au sein de la même application (ces flux sont susceptibles d'impliquer des charges de travail dans la même portée)

Outils utiles pour l'examen des politiques

- Pour faciliter la gestion de cet effort, filtrez et triez les politiques afin de pouvoir examiner les politiques associées en tant que groupe.
  - Cliquez sur les en-têtes du tableau pour trier les colonnes, par exemple par consommateur, fournisseur ou port/protocole.
  - Utilisez le filtre en haut de la liste des politiques pour afficher des sous-ensembles spécifiques.

    Pour afficher la liste des propriétés que vous pouvez filtrer, cliquez sur le bouton (i) dans la zone Filter Policies (Filtrer les politiques).

- Examinez la représentation graphique des politiques générées :

  Cliquez sur le bouton  (bouton d'affichage visuel de la politique).

  Pour en savoir plus, consultez Représentation visuelle des politiques, on page 114.
- Pour rechercher ou filtrer les lignes en fonction des ports, cliquez sur le bouton **Ungrouped** (Dégroupées).
- Par défaut, les politiques sont regroupées par consommateur/fournisseur/action. Pour revenir à cet affichage, cliquez sur le bouton **Grouped** (Groupées).
- Utiliser le filtre **External?** (Externe?) pour trouver les politiques dans lesquelles le fournisseur se trouve dans une portée différente de celle dans laquelle vous avez découvert les politiques.

  Créez des politiques pour ce trafic en utilisant l'une des méthodes décrites dans Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, on page 94.
- Examinez le niveau de confiance des politiques générées. Consultez Traiter les politiques de niveau de confiance faible, on page 112.
- Consultez le profil de charge de travail pour obtenir des renseignements détaillés sur une charge de travail. Cliquez sur l'adresse IP, puis sur **View Workload Profile** (afficher le profil de charge de travail) dans le volet de droite.
- Pour afficher les flux de trafic qui ont été utilisés pour produire une politique spécifique, cliquez sur la valeur dans la colonne **Protocols and Ports** (protocoles et ports) de cette politique, puis cliquez sur **View Conversations** (afficher les conversations) dans le panneau latéral qui s'ouvre.

  Consultez Conversations, on page 153 pour obtenir de plus amples renseignements.

  Si nécessaire, vous pouvez accéder au détail en cliquant sur **Flow Search** (recherche de flux) pour afficher les flux d'une conversation.

Autres choses à faire et à vérifier

- Repérez les adresses IP inconnues (comme les adresses IP de basculement ou autres adresses IP flottantes) et ajoutez-leur des étiquettes pour savoir de quoi il s'agit.

Vous pouvez trouver des détails utiles sur la page Inventory Profile (Profil d'inventaire). Cliquez sur l'adresse IP, puis sur **View Inventory Profile** (afficher le profil d'inventaire) dans le volet de droite.

- Recherchez tout ce qui n'est manifestement pas souhaitable ou qui n'a pas de sens.
- Regroupez les charges de travail à l'aide de filtres d'inventaire pour qu'une seule politique puisse gérer plusieurs d'entre elles. Consultez Créer un filtre d'inventaire.
- Enquêtez et contactez d'autres administrateurs réseau, au besoin, pour comprendre la nécessité des politiques que vous voyez.
- Consultez les rubriques sous Aborder les complexités de la politique, on page 87, qui peuvent impliquer des politiques manuelles et approuvées ainsi que des politiques détectées automatiquement.
- En général, il est recommandé que le nombre maximal de politiques d'une portée ne dépasse pas 500 environ. Si vous en avez beaucoup plus, essayez de regrouper des politiques similaires ou de diviser la portée.
- Lors de l'examen, approuvez toutes les politiques dont vous savez qu'elles sont correctes en l'état, afin de les conserver lors de futurs cycles de découverte.

Traiter les politiques de niveau de confiance faible

Après la découverte automatique d'une politique, les indices de confiance indiquent la précision et la pertinence de chaque politique découverte pour chaque service (port et protocole) spécifié dans cette dernière.

Pour identifier les politiques de niveau de confiance faible découvertes :

1. Accédez à la portée et à l'espace de travail applicables, puis cliquez sur **Manage Policies** (Gérer les politiques).
2. Cliquez sur l'onglet **Policies** (Politiques).
3. Cliquez sur le bouton **Ungrouped Policy List View** (Affichage de la liste des politiques non groupées).
4. Cliquez sur l'en-tête de colonne **Confidence** (Confiance) pour trier la liste des politiques par niveau de confiance.
5. Cliquez sur la valeur dans la colonne **Protocols and Ports** (Protocoles et ports) pour ouvrir un volet dans la partie droite de la fenêtre.
6. Dans la section **Protocols and ports** (Protocoles et ports), la couleur de chaque **C** indique le niveau de confiance pour chaque service (port et protocole) spécifié dans la politique.

   Pour interpréter le niveau de confiance, survolez le **C**.
7. Recherchez les indicateurs de niveau de confiance faible pour tous les services de la liste.
8. Le cas échéant, supprimez ou modifiez les politiques indésirables ou ajoutez des politiques supplémentaires.

Pour afficher les niveaux de confiance d'une politique particulière :

1. Dans l'onglet Policies (politiques), cliquez sur la valeur de la colonne **Protocols and Ports** (protocoles et ports) pour cette politique.

   Le panneau d'affichage latéral des politiques s'ouvre dans la partie droite de la fenêtre.

2. Dans la section **Protocols and ports** (Protocoles et ports), la couleur de chaque **C** indique le niveau de confiance pour chaque service (port et protocole) spécifié dans la politique.

   Pour interpréter le niveau de confiance, survolez le **C**.

Direction du flux et niveau de confiance de la politique

La précision des politiques détectées dépend de l'identification correcte de la direction du flux. Si la direction du flux est mal identifiée, le degré de confiance des résultats de la recherche automatique de politiques peut être diminué. Pour en savoir plus sur la détermination de la direction du flux pour la ou les conversations analysées pour la création de la politique, consultez Classification client-serveur.

Dépanner les résultats de la découverte automatique des politiques

Si les résultats de la découverte automatique des politiques ne sont pas conformes à vos attentes, vérifiez les points suivants :

Étendre la plage temporelle sélectionnée pour inclure plus de données

Prolonger la fenêtre temporelle pour inclure davantage de données et pour incorporer les événements qui se produisent rarement. Par exemple, si une application génère un rapport trimestriel complexe à partir de données provenant de plusieurs applications de fournisseurs, veillez à inclure une plage temporelle qui inclut ce trafic.

Éviter les données recueillies avant certaines modifications

Si la définition de la portée a été modifiée ou si des données recueillies avant un certain moment sont devenues non valides pour une autre raison, assurez-vous que votre plage temporelle n'inclut PAS de données antérieures.

Exclure les flux de trafic trompeurs

Les filtres d'exclusion doivent peut-être être configurés ou modifiés.

Les filtres d'exclusion peuvent être configurés à plusieurs endroits, ils peuvent être activés ou désactivés. Vérifiez chaque emplacement :

- Vérifiez les filtres d'exclusion configurés pour l'espace de travail.
- Vérifiez les filtres d'exclusion par défaut configurés au bas de la page de configuration de la découverte de la politique par défaut.
- Vérifiez quels filtres d'exclusion sont activés dans la section Advanced Configurations (configurations avancées) des paramètres de l'espace de travail pour la découverte automatique des politiques.
- Vérifiez quels filtres d'exclusion sont activés dans la section Advanced Configurations (configurations avancées) de la page de configuration de la découverte des politiques par défaut.
- Si vous utilisez des filtres d'exclusion par défaut, assurez-vous d'avoir cliqué sur **Save** (Enregistrer) dans la page **Default Policy Discovery Config** (configuration de la découverte de politiques par défaut) pour rendre ces configurations disponibles pour les espaces de travail individuels.

Pour en savoir plus, consultez Filtres d'exclusion, à la page 31 et les sous-sections.

Dépannage des politiques selon lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes

Consultez Dépannage des politiques de portées croisées, à la page 106.

Vérifier l'état des politiques approuvées

Consultez Dépanner les politiques approuvées, à la page 52.

Représentation visuelle des politiques

La représentation visuelle des politiques fournit une représentation graphique de ces dernières.

Pour accéder à la page de représentation visuelle des politiques : Dans la page Policies (Politiques), cliquez sur l'icône de graphique () à droite de l'icône de liste.

Éléments d'affichage de la politique

Les éléments visuels de la vue des politiques sont les suivants :

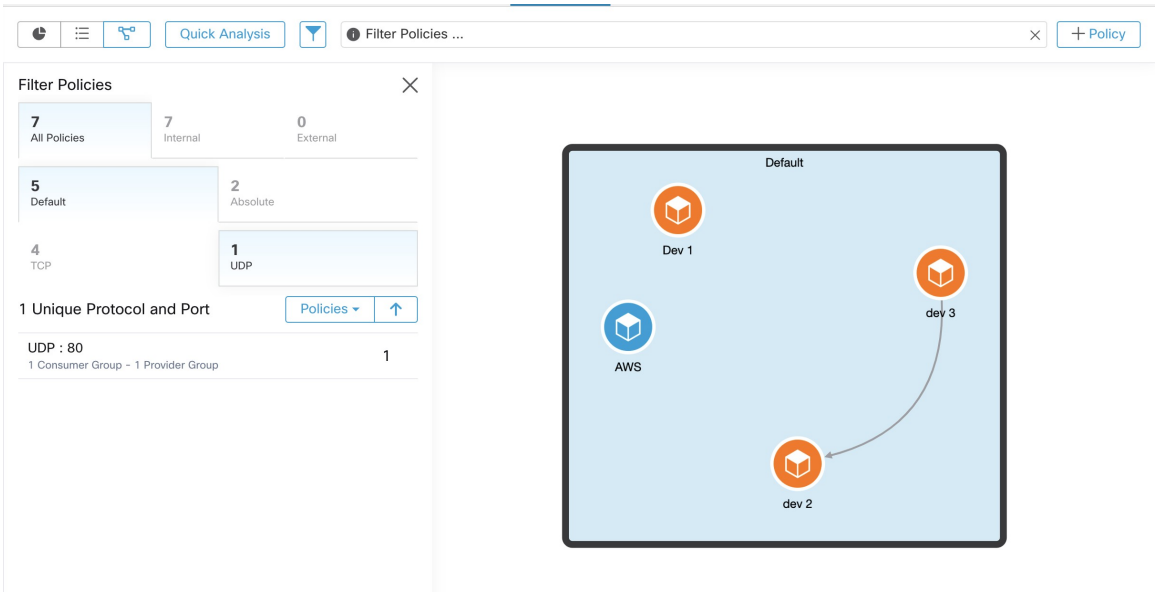
Cet élément	Représente
Une icône bleue, orangée ou mauve	Un nœud (le consommateur ou le fournisseur d'une politique)
Icône bleue	Une portée
Icône jaune	Un filtre d'inventaire
Icône mauve	Une grappe
Ligne reliant deux icônes	Une ou plusieurs politiques

Options d'affichage des politiques

Destinataire	Faire ceci
Afficher la liste des charges de travail incluses dans un nœud de consommateur ou de fournisseur	Double-cliquez sur l'icône du nœud.
Afficher les détails d'une politique telles que les services (ports), les actions (autoriser/refuser) et le protocole entre un consommateur et un fournisseur	Double-cliquez sur la ligne qui les relie. Les détails s'affichent dans le volet de droite.
Afficher les politiques entrant et sortant d'un nœud	Cliquez sur l'icône .
Afficher uniquement les politiques entre les charges de travail de la portée	Cliquez sur le bouton **interne**.
Afficher uniquement les politiques dans lesquelles le fournisseur se trouve dans une portée différente de celle du consommateur	Cliquez sur le bouton **externe**.

Destinataire	Faire ceci
Utiliser les options avancées	Cliquez sur le bouton (i) à gauche de la zone de saisie de texte du filtre pour voir les options, puis saisissez les critères de filtre.

Figure 54: Filtrage des politiques dans la vue graphique



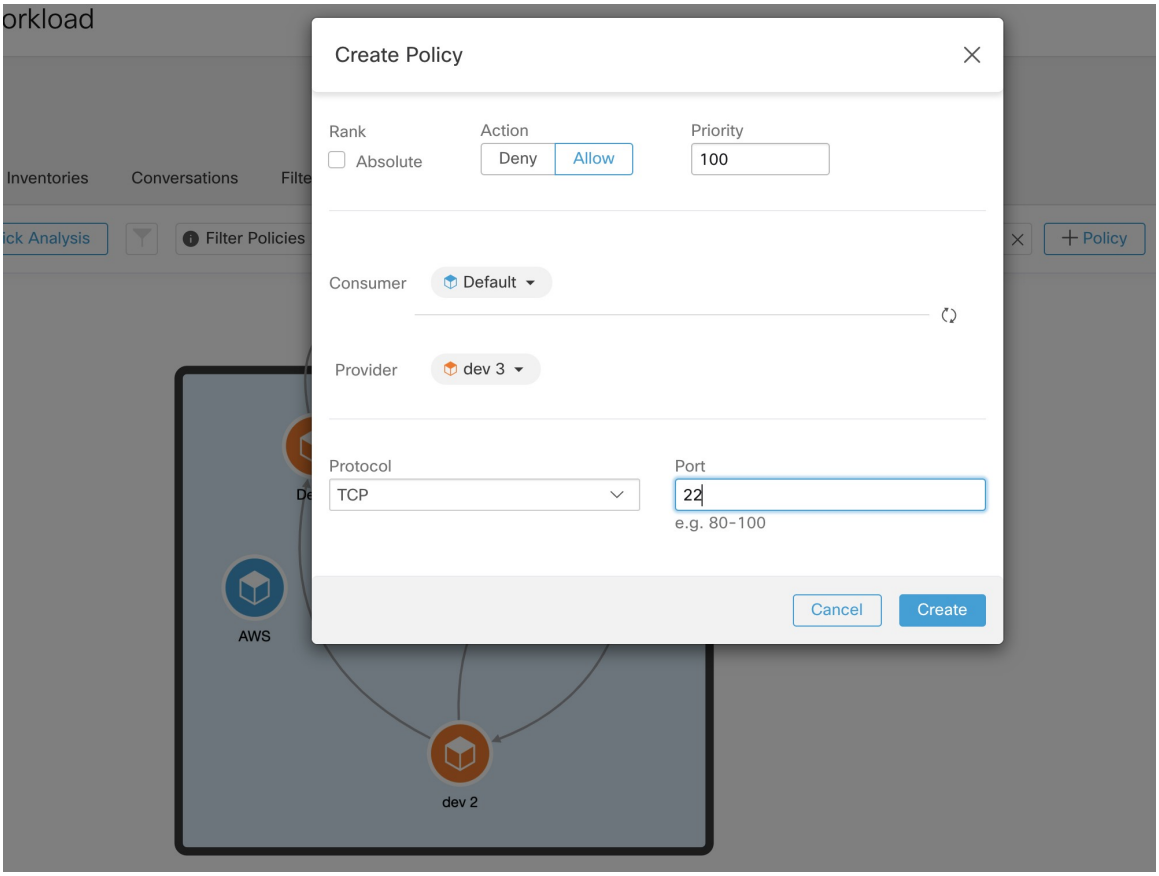
Pour télécharger une image haute résolution de la vue graphique des politiques :

1. Dans le coin inférieur droit du graphique, cliquez sur l'icône de points de suspension , puis cliquez sur **Export Image** (Exporter l'image).
2. Sélectionnez la résolution et le type d'image requis.
3. Cliquez sur **Télécharger**.

Ajouter une politique (page d'affichage des politiques)

Pour créer une politique, survolez le consommateur jusqu'à ce que vous voyiez un signe « + », puis maintenez la politique enfoncée et faites glisser la politique sur le fournisseur. Pour créer une politique Absolue, cochez la case Absolue dans la boîte de dialogue modale. Sinon, la politique est créée en tant que politique par défaut. Les politiques peuvent également être gérées en cliquant sur une ligne et en sélectionnant une politique dans la liste contextuelle. Les politiques seront affichées dans la barre latérale.

Figure 55: Création de politiques dans la vue graphique



Analyse rapide

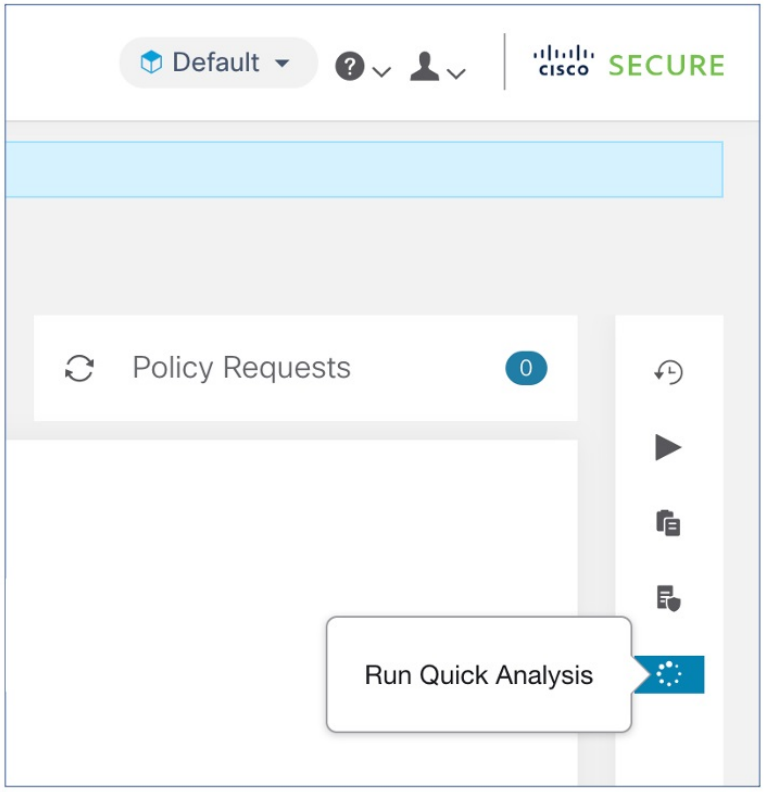
L'analyse rapide permet de tester un flux au sujet duquel on a des doutes par rapport à toutes les politiques de l'espace de travail actuel et à toutes les autres politiques pertinentes d'autres espaces de travail. L'analyse rapide facilite le débogage et l'expérience de différentes politiques de sécurité, sans qu'il soit nécessaire d'exécuter une analyse des politiques en direct pour l'espace de travail.

Restriction

- Vous ne pouvez exécuter l'analyse rapide que sur les espaces de travail principaux.
- L'analyse rapide n'est actuellement pas prise en charge sur les flux des services Kubernetes.

Cliquez sur l'onglet **Run Quick Analysis** (Exécuter l'analyse rapide) dans le volet de navigation de droite pour afficher la boîte de dialogue.

Figure 56: Onglet Analyse rapide



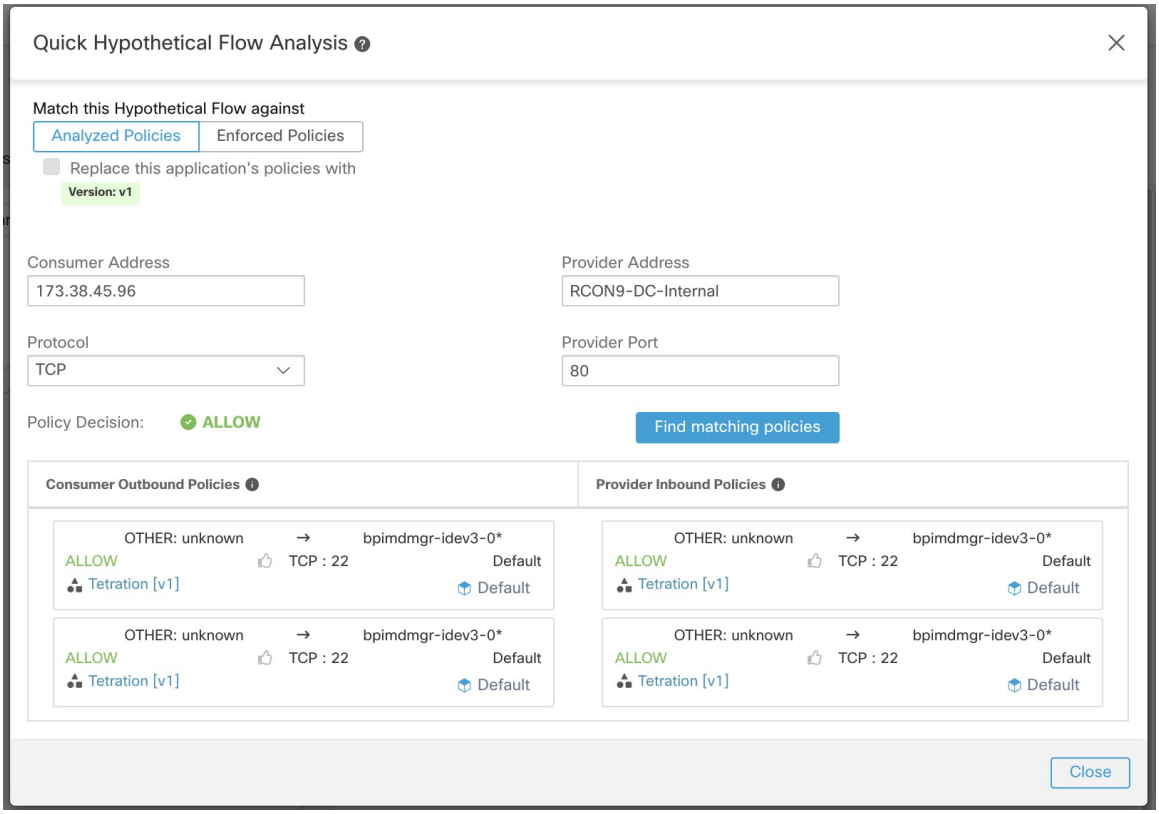
Saisissez l'adresse IP du consommateur (client), l'adresse IP du fournisseur (serveur), le port et le protocole du flux hypothétique, puis cliquez sur le bouton **Find Matching Policies** (trouver les politiques correspondantes).

Une décision de politique sera affichée, indiquant si le flux hypothétique serait autorisé ou refusé compte tenu des définitions de politique de la dernière version de l'espace de travail et de toutes les autres politiques pertinentes des espaces de travail qui sont déjà transmises pour l'analyse de politique en direct.

Au bas de la boîte de dialogue, nous affichons les politiques sortantes et entrantes correspondantes séparément, et dans leur ordre de tri global. Seule la première rangée de chaque côté a un effet. Pour qu'une connexion soit établie avec succès, nous avons besoin que la règle de trafic sortant sur le consommateur et la règle entrante supérieure du côté du fournisseur soient des règles ALLOW.

L'affichage de toutes les autres politiques correspondantes dans l'ordre fournit un outil de débogage précieux pour aider à résoudre les problèmes dans les définitions de politiques lorsqu'une certaine politique semble ne pas avoir d'effet. Vous pouvez ajouter, mettre à jour ou supprimer des politiques de l'espace de travail et répéter immédiatement l'analyse sans avoir à exécuter une analyse des politiques en direct sur l'espace de travail.

Figure 57: Analyse rapide de la politique



Analyse des politiques en temps réel

Après avoir examiné et approuvé l'ensemble de politiques de sécurité de réseau généré par la découverte automatique des politiques et avant d'appliquer les politiques, vous devez utiliser l'analyse des politiques en direct pour observer comment les politiques pourraient affecter le trafic réel sur votre réseau.

Voici des questions auxquelles l'analyse des politiques en temps réel peut vous aider à répondre :

- Quelle serait l'incidence sur les applications de cette portée si les politiques de cet espace de travail étaient appliquées maintenant?
- Aurait-on pu éviter une attaque ou un risque de sécurité connu précédemment en appliquant le nouvel ensemble de politiques?

  Consultez Exécuter des expériences de politiques pour comparer les politiques actuelles au trafic passé, on page 126.

- Nos politiques fonctionnent-elles comme nous l'attendons?

Vous devez exécuter l'analyse des politiques sur tout espace de travail qui comporte des politiques. Étant donné que les charges de travail d'une portée spécifique peuvent être affectées par des politiques d'autres portées, vous ne devez pas exécuter l'analyse des politiques uniquement pour une portée unique avant d'appliquer la politique pour cette portée. Pensez à analyser les politiques de toutes les portées qui peuvent avoir une incidence sur le trafic d'une portée particulière.

Par exemple :

- Les politiques définies dans les portées supérieures à cette portée dans l'arborescence peuvent s'appliquer aux charges de travail de cette portée.
- Si les charges de travail de cette portée communiquent avec des charges de travail d'une autre, les politiques de cette portée peuvent affecter ces communications. Lorsque l'analyse des politiques est lancée dans cette portée (ou que les dernières politiques sont analysées après un changement de politique dans cette portée), cela peut affecter les résultats de l'analyse des politiques de cette portée.

Vous devez effectuer une analyse des politiques chaque fois que vous les mettez à jour pour vous assurer que les modifications n'endommagent pas les applications.

L'exécution d'une analyse des politiques en temps réel sur un espace de travail est parfois appelée « publication » d'un espace de travail.

Commencer l'analyse des politiques en temps réel

Une fois que vous avez examiné les politiques générées dans un espace de travail par la découverte automatique des politiques et que vous pensez qu'elles sont telles que vous le souhaitez, vous pouvez commencer leur analyse.

Before you begin

Important L'analyse en temps réel comprend les effets des politiques dans d'autres espaces de travail qui exécutent également l'analyse en direct. Si vous avez activé la mise en application sur un espace de travail, mais que l'analyse n'est pas en cours sur cet espace de travail ou que la version appliquée des politiques n'est pas la même que la version analysée des politiques, les résultats de l'analyse en temps réel pour cet espace de travail risquent de ne pas être exacts.

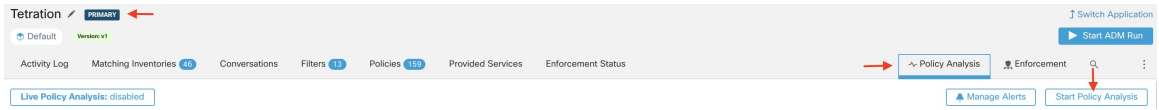
Procedure

Étape 1 Basculez l'espace de travail sur **Primary** (Principal) en cliquant sur le bouton ••• (bouton Plus) à droite de « Secondary » (Secondaire) à côté du nom de l'espace de travail dans l'en-tête.

Étape 2 Accédez à l'onglet **Policy Analysis** (analyse des politiques).

Étape 3 Cliquez sur **Start Policy Analysis** (Démarrer l'analyse des politiques) sur la droite.

Figure 58: Activer l'analyse des politiques



What to do next

- Étant donné que les politiques d'autres portées peuvent s'appliquer aux charges de travail de cette portée, envisagez d'analyser simultanément les politiques d'autres portées qui pourraient affecter les résultats de

l'analyse de cette dernière.. Consultez Exemple : Incidence des politiques analysées sur d'autres portées, on page 121.

- Si vous souhaitez être averti lorsque des flux échappés sont détectés, cliquez sur **Manage Alerts** Gérer les alertes).
- Utilisez les outils de la page pour filtrer les données. Pour afficher les critères de filtre disponibles, cliquez sur le bouton (i) dans la zone de filtre.
- Si vous ajoutez ou modifiez des politiques après avoir lancé l'analyse, vous devez redémarrer l'analyse pour inclure les modifications dans cette dernière. Consultez Après avoir modifié les politiques, analyser les politiques les plus récentes, on page 127.

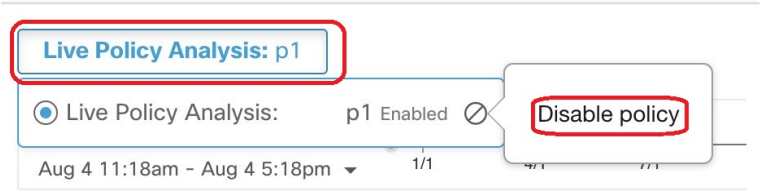
Arrêter l'analyse des politiques en direct

En général, vous devez laisser l'analyse des politiques continuer de s'exécuter, même après l'application des politiques, car les politiques de cet espace de travail peuvent avoir une incidence sur les résultats de l'analyse des politiques dans d'autres espaces de travail que vous analysez.

Pour arrêter l'analyse des politiques en direct :

Cliquez sur **Live Policy Analysis : P<number>**(Analyse de la politique en direct), puis cliquez sur **Disable Policy** (désactiver la politique) :

Figure 59: Désactiver l'analyse en temps réel des politiques

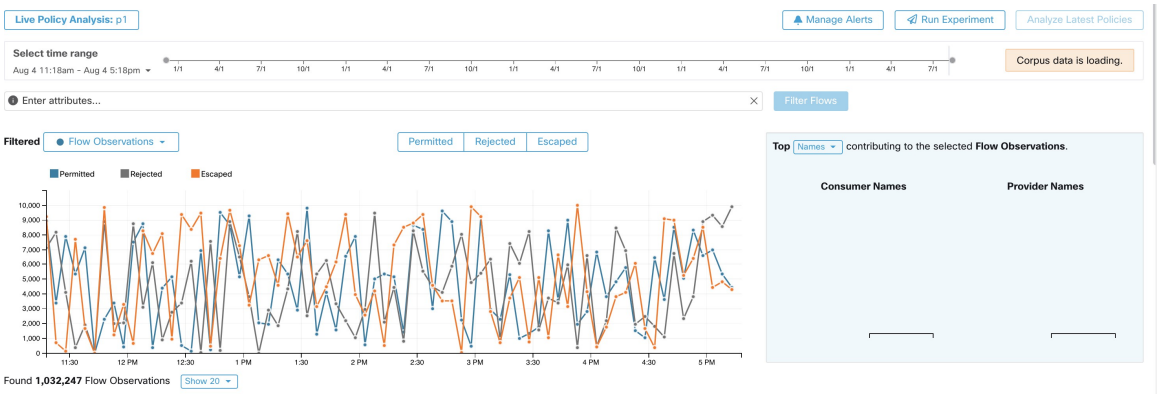


Résultats de l'analyse des politiques : comprendre les bases

Lors de l'analyse de la politique, tous les flux entrant, sortant et se trouvant dans la portée associée à l'espace de travail se voient attribuer l'un des résultats suivants :

- **Autorisé** : le flux a été autorisé par le réseau ainsi que par les politiques analysées.
- **Échappé** : le flux a été autorisé par le réseau, mais aurait dû être abandonné selon les politiques analysées.
- **Rejeté** : le flux a été abandonné par le réseau, ainsi que par les politiques analysées.

Figure 60: Page Policy Analysis (Analyse de la politique)



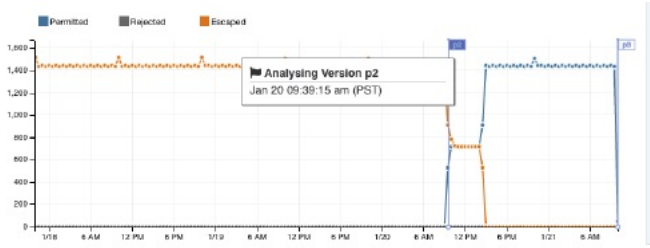
Quelques éléments à prendre en considération pour s'orienter :

- Vous pouvez filtrer les renseignements sur les flux présentés dans cette page à l'aide d'une barre de filtre à aspects multiples. Cliquez sur le bouton **Filter Flows** (Filtrer les flux) pour mettre à jour tous les graphiques en conséquence.
- Passez le curseur sur le graphique pour afficher le pourcentage des flux agrégés observés lors de cet horodatage.
- Cliquez sur un horodatage pour afficher une liste de tous les flux filtrés dans un tableau ci-dessous pour une analyse plus approfondie.
- Vous pouvez limiter les interactions à l'un des trois types de résultats en cochant ou en décochant les types en haut des graphiques de séries temporelles.
- Le tableau intitulé Top N (à droite) montre les principaux noms d'hôte, adresses, ports, etc. qui contribuent aux données présentées dans la série temporelle à gauche.

  Vous pouvez limiter le tableau des séries temporelles aux flux échappés et sélectionner « Ports » dans le tableau des N principaux pour voir les principaux ports qui contribuent aux flux échappés.

Exemple : Incidence des politiques analysées sur d'autres portées

Dans l'exemple suivant, les flux sont autorisés jusqu'à environ 12 h. À ce moment-là, l'analyse des politiques a été lancée dans un espace de travail associé à une portée différente, affectant le trafic avec des charges de travail dans cette portée et entraînant le marquage des flux comme échappés. (Vous savez que cette modification ne résultait pas de modifications de politique nouvellement analysées dans cet espace de travail, car cela aurait créé un indicateur d'étiquette).



Analyse sans politiques

Les flux entrants, sortants et à l'intérieur de la portée associée à l'espace de travail peuvent être affectés par les politiques d'autres espaces de travail en cours d'analyse. Si l'analyse des politiques en direct n'est pas activée dans cet espace de travail, les flux seront marqués avec ceux des autres espaces de travail du système dans lesquels l'analyse des politiques en direct est activée.

Note Si aucun espace de travail n'exécute d'analyse de politique en direct, le graphique de la série chronologique est vide.

Détails de l'analyse de la politique

Disposition des flux

Dans l'analyse en direct des politiques, pour décider si un flux est **autorisé**, **échappé** ou **rejeté**, nous devons d'abord déterminer la **disposition** du flux du point de vue du réseau. Chaque flux recevra la disposition **ALLOWED (AUTORISÉ)**, **DROPPED (ABANDONNÉ)** ou **PENDING (EN ATTENTE)**, en fonction des signaux et des observations donnés par les agents Cisco Secure Workload. Il existe un certain nombre de scénarios basés sur les configurations des agents le long du chemin du flux et des types de flux.

Tout d'abord, quels que soient les types de flux, si un agent sur le chemin d'un flux signale que le flux est ABANDONNÉ, ce flux recevra le statut ABANDONNÉ.

Lorsqu'aucun agent ne signale d'ABANDON le long du chemin du flux, nous considérons le cas des flux bidirectionnels et unidirectionnels séparément. Lorsque des flux bidirectionnels sont observés, nous examinons les flux par paires (aller et retour) en fonction de leur source, de leurs ports et protocoles de destination et de leur synchronisation. On ne peut pas faire de même pour les flux unidirectionnels.

Pour les flux bidirectionnels, si des agents sont installés et le plan de données activé aux deux extrémités, un flux aller recevra une disposition AUTORISÉE si l'agent de source et l'agent de destination indiquent que le flux est observé. Sinon, le flux aller aura la disposition PENDING (EN ATTENTE). Si un agent est installé sur la charge de travail source ou de destination, mais pas sur les deux, le flux aller recevra une disposition AUTORISÉE si et seulement si l'agent observe le flux inverse ultérieur durant une fenêtre de **60** secondes Sinon, l'état PENDING (EN ATTENTE) sera attribué au flux aller. La disposition de la partie inverse du flux bidirectionnel suit la même logique, sauf que maintenant la source et la destination sont inversées. Par exemple, si un seul côté comporte un agent, le fait qu'une disposition de flux inverse soit EN ATTENTE ou AUTORISÉ dépend de l'observation et du moment de son flux aller suivant selon la même logique.

Notez que nous supposons que les pare-feu mettent en œuvre la suppression silencieuse. Si un message de rejet est envoyé sur le *même* flux (par exemple, le rejet d'un SYN TCP avec RST + ACK), un flux inverse sera détecté et le flux aller précédent sera marqué comme AUTORISÉ. Cependant, si le message de rejet est envoyé sur un flux *différent* (par exemple, rejet d'un message SYN TCP avec un message ICMP), le flux aller restera PENDING (EN ATTENTE).

Pour un flux unidirectionnel, le flux sera considéré comme ABANDONNÉ s'il est signalé comme ABANDONNÉ par un agent, comme dans le cas des flux bidirectionnels. Cependant, comme il n'y a pas de flux inverse correspondant, le flux aura l'état de disposition PENDING (EN ATTENTE) si les deux agents l'observent.

Types de violations

Les dispositions de flux sont vérifiées par rapport aux politiques analysées pour déterminer les types de violation finaux.

Le type de violation d'un flux sera

- **Permitted (Autorisé)**, si sa disposition est ALLOWED ou PENDING et que son action politique décisionnelle est ALLOWED,
- **Escaped (Échappé)**, si sa disposition est ALLOWED et que son action politique décisionnelle est DENY,
- **Rejected (Rejeté)**, si sa disposition est DROPPED ou PENDING et que son action politique décisionnelle est DENY,

Un état DROPPED est attribué uniquement aux flux dont les agents concernés signalent explicitement leur état ABANDONNÉ. En l'absence de rapport explicite d'abandon pour les agents, le flux reçoit l'état PENDING (EN ATTENTE).

Lorsque la disposition est PENDING (EN ATTENTE) :

- et que l'action de la politique est DENY (REJETER), le type de violation est défini sur Rejeté.
- et que l'action de la politique est ALLOWED (AUTORISÉ), le type de violation est réglé sur Autorisé.

Dans un flux bidirectionnel, si les types de violation de politique aller et retour du flux concordent, un seul type s'affiche dans l'analyse des politiques ou dans la page d'analyse de l'application. Sinon, le trajet avant et arrière sont affichés séparément, par exemple ALLOWED:REJECTED.

Exemples de scénarios :

- Des paquets sont abandonnés au niveau de l'application côté source.
  - Dans ce cas, l'agent de sortie Cisco Secure Workload du côté source signalera que le flux est ABANDONNÉ.
- Des paquets quittent la source.
  - S'il n'y a qu'un agent du côté source, le flux sera signalé comme AUTORISÉ par l'agent de sortie si un retour de paquet est également observé par l'agent dans les 60 secondes.
  - S'il y a un agent de visibilité seulement du côté de la source et du côté de la destination, le flux recevra l'état de disposition ABANDONNÉ si et seulement si l'agent d'entrée signale que le flux est ABANDONNÉ. Sinon, le flux sera signalé comme AUTORISÉ.
  - Des paquets de flux sont reçus à destination, mais pas de trafic inverse.

    S'il n'y a pas d'agent du côté destination, le flux recevra l'état PENDING (EN ATTENTE). Sinon, le statut AUTORISÉ lui sera attribué.

Étapes suggérées pour l'analyse des flux

Lors de l'analyse de flux spécifiques lors de l'examen des résultats des politiques, les suggestions et les filtres suivants peuvent être utiles :

1. Concentrez-vous d'abord sur les *FLUX ÉCHAPPÉS* :

   Les flux **échappés** nécessitent une attention particulière, car leurs dispositions réelles de flux diffèrent des actions prévues en fonction des politiques actuellement analysées. Vérifiez que l'application de ces politiques ne bloque pas les flux nécessaires et ne nuit pas à vos applications.

   Cliquez sur le type de violation, par exemple **Échappé**.

(Vous pourrez ultérieurement consulter les flux rejetés et autorisés, si nécessaire).

Les flux échappés peuvent se produire pour de nombreuses raisons, notamment :

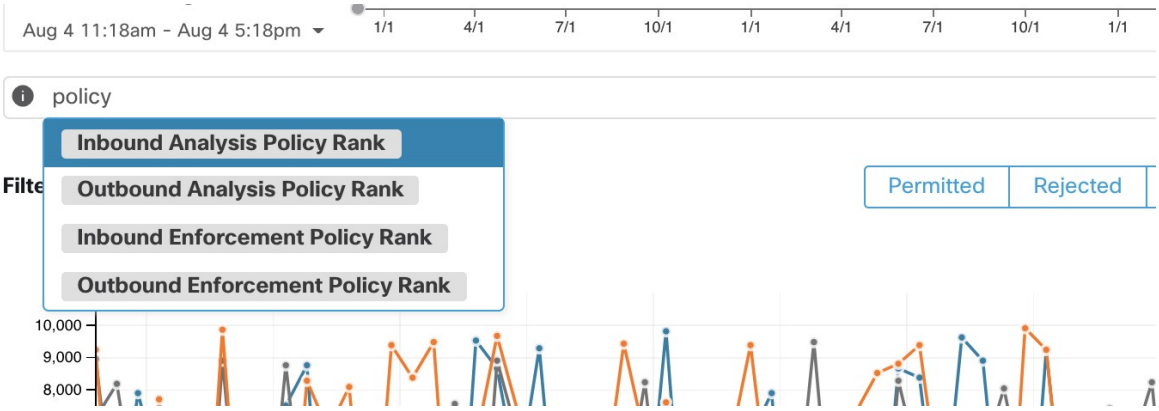
- Une autre politique plus élevée dans l'ordre de priorité est en train de prendre effet
- le trafic emprunte un chemin différent du chemin de routage indiqué par vos politiques, ou
- Par exemple, la politique que vous attendez du trafic se trouve dans un espace de travail qui n'est pas analysé (si vous regardez les flux échappés sur la page Analyse de la politique) ou mis en application (si vous regardez les flux échappés sur la page Application), par exemple dans une portée ancêtre ou même dans un espace de travail secondaire dans la même portée.

2. Identifier les flux qui correspondaient à la politique collectrice globale (entrants et sortants) :

   Il est important de comprendre quels flux sont associés aux politiques collectrices globales, en particulier dans un modèle de politique de liste d'autorisation. Si ces flux sont légitimes, mais qu'aucune politique d'autorisation explicite n'est configurée pour eux, vous pouvez ajouter des politiques explicites appropriées dans les portées entrantes ou sortantes correspondantes. S'il s'agit de flux suspects, vous devez les identifier rapidement et étudier plus avant leurs détails.

   Pour vous concentrer sur ces flux, appliquez des filtres en fonction de la valeur *catch-all* (collectrice globale) de **inbound_policy_rank** ou **out- bound_policy_rank**, selon que vous examinez le flux entrant, sortant ou les deux, comme indiqué ci-dessous.

   Illustration 61 : Options de filtrage de l'analyse des politiques pour le classement



3. Filtrer les flux TCP avec RST : *les indicateurs Fwd (Avant) ne contiennent pas RST, les indicateurs Rev (Retour) ne contiennent pas RST*

   Certains flux TCP échappés ont des indicateurs RST activés. Ces flux sont réinitialisés par leurs consommateurs ou leurs fournisseurs. Il s'agit de connexions non établies sans échange de données, mais qui peuvent être signalées comme AUTORISÉES, car les agents peuvent voir leurs paquets d'établissement de liaison. Puisque ces flux n'ont pas de connexions établies pour commencer, ils ne seront pas affectés lors de l'application des politiques actuellement analysées. Le filtrage des flux TCP qui ont l'indicateur RST de chaque côté vous permet de vous concentrer sur les flux échappés plus significatifs et plus importants, dont la connexion établie sera bloquée par les politiques actuellement analysées.

4. Si la majeure partie du trafic utilise IPv4, concentrez-vous uniquement sur les flux IPv4 :

   Filtre utilisant *address type = IPv4, address type != IPv6*. Il est également utile de filtrer les adresses *link-local* (liées locales).

5. Hiérarchisez les flux sur lesquels se concentrer lors de la prochaine étape de diagnostic en identifiant les noms d'hôte, les ports, les adresses, les portées, etc. les plus fréquemment concernées par le trafic échappé :

   Sélectionnez le *nom d' hôte, les ports ou* les *adresses* dans le volet de fonctionnalité TopN. Vous pouvez généralement les combiner avec d'autres filtres pour accéder à un type de trafic particulier lors du diagnostic des politiques.

6. Rechercher les données de flux pour les noms d'hôte, les ports, les protocoles, etc., identifiés à l'étape précédente

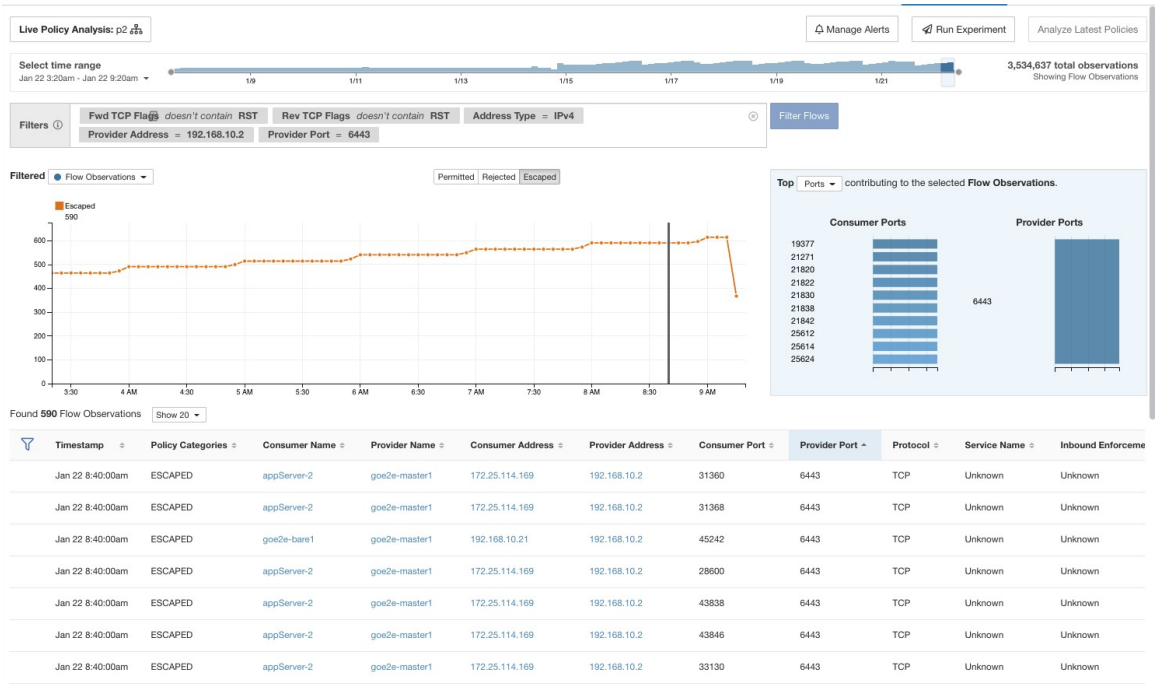
   Une fois que vous avez une idée des principaux candidats en fonction des noms d'hôte, de port, etc. des flux ciblés, vous pouvez choisir d'approfondir les flux en appliquant des filtres d'exploration directement à partir des N premières valeurs données dans la fenêtre de requête N supérieure, ou en saisissant manuellement les filtres pertinents dans la barre des filtres de recherche de flux. Par exemple, *Consumer Hostname contains {something}, Provider Hostname contains {something}, Provider Port = {some port number}, Protocol = TCP Protocol != ICMP*

7. Consultez les flux individuels et effectuez une analyse rapide :

   Enfin, vous pouvez vous concentrer sur un flux en particulier pour examiner le résultat de ses politiques en cliquant sur la ligne du tableau correspondant au flux. Soyez attentif aux politiques correspondant au flux et aux portées des adresses du consommateur et du fournisseur. Si l'action de politique ne correspond pas à l'action prévue, vous devez créer des politiques appropriées dans les espaces de travail associés aux portées du fournisseur et/ou du consommateur pour modifier l'action de la politique.

   La figure ci-dessous montre un exemple de flux de travail de réduction des flux échappés à l'aide du filtrage décrit ci-dessus. L'entrée de recherche prend également en charge les « , » et « - » pour le port, l'adresse du consommateur et l'adresse du fournisseur, en transformant les « - » en requêtes de plages.

Illustration 62 : Exemple de diagnostic d'analyse de politiques



Exécuter des expériences de politiques pour comparer les politiques actuelles au trafic passé

Si une attaque connue ou un autre modèle de trafic important à court terme s'est produit par le passé, et vous souhaitez voir comment vos politiques actuelles (ou un autre ensemble de versions de politiques) auraient géré ce trafic, vous pouvez utiliser la fonctionnalité Run Experiments « exécuter des tests ».

Before you begin

Tip Au lieu de cette procédure, vous pouvez exécuter à nouveau la découverte automatique des politiques, y compris la plage temporelle pertinente, et voir quelles politiques différentes sont suggérées.

Procedure

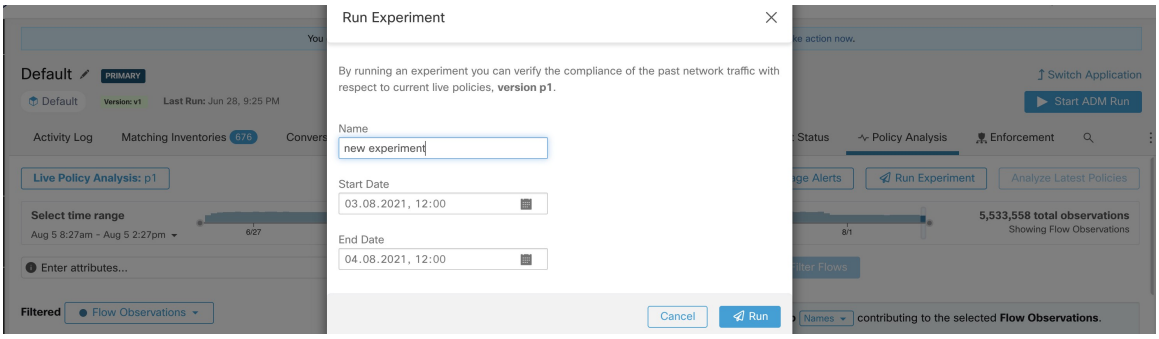
Étape 1 Accédez à la page d'analyse des politiques de votre espace de travail sélectionné.

Étape 2 En haut de la page, sélectionnez la version de la politique à tester.

Étape 3 Cliquez sur **Run Experiment** (Exécuter l'expérience).

Étape 4 Saisissez un nom et une durée pour le test de la politique.

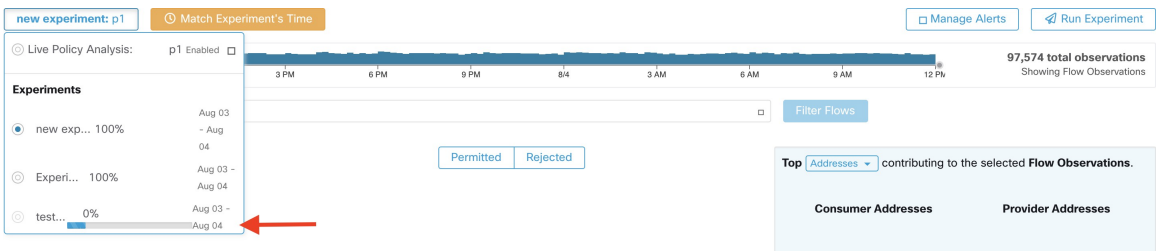
Figure 63: Exécuter le formulaire de test



Cette opération lance un nouveau travail d'analyse de la politique qui remonte dans le temps et réanalyse tous les flux de la durée sélectionnée en fonction dans la version de la politique sélectionnée.

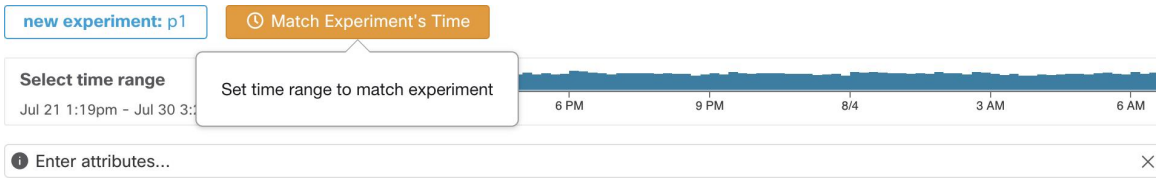
Cette tâche peut prendre quelques minutes, selon la durée sélectionnée. La progression est affichée dans le menu du sélecteur de politiques. Lorsque les résultats sont prêts à être présentés, vous devriez pouvoir sélectionner l'expérience comme n'importe quelle autre version de la politique et les graphiques de séries temporelles montrant les différentes catégories de flux seront mis à jour en conséquence.

Figure 64: Afficher l'état du test



Note Si vous ne voyez aucun flux lors de la sélection d'une expérience de politique, cela peut être dû à une inadéquation de l'intervalle de temps. Par exemple, l'intervalle de temps actuel des graphiques est d'une heure, mais la durée de l'expérience est de 6 heures dans le passé. Pour réinitialiser la plage temporelle à la durée de l'expérience, cliquez sur l'icône d'horloge à côté du sélecteur de politique.

Figure 65: Plage temporelle de la correspondance



Après avoir modifié les politiques, analyser les politiques les plus récentes

L'analyse des politiques ne reflète pas automatiquement les modifications de politique dans l'espace de travail. Lorsque vous êtes prêt à analyser l'ensemble actuel de politiques après avoir apporté vos modifications, cliquez sur **Analyze Latest Policies** (Analyser les politiques les plus récentes) pour que l'analyse des politiques reflète les modifications.

Si les politiques de l'espace de travail n'ont pas changé depuis le dernier lancement de l'analyse de politiques ou si l'analyse de politiques n'est pas actuellement activée, le bouton Analyze Last Policies (Analyser les politiques les plus récentes) n'est pas disponible. Si le bouton est cliquable, certaines modifications de politique n'ont pas encore été incluses dans l'analyse.

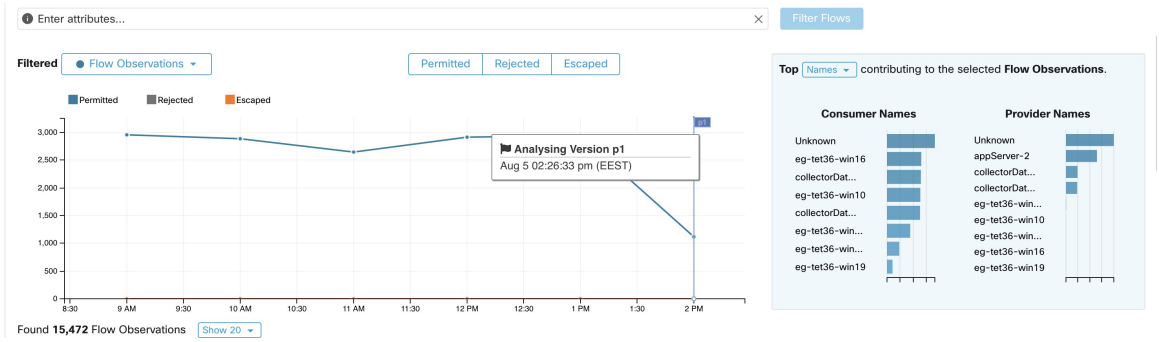
Consultez aussi Afficher, comparer et gérer les versions des politiques analysées, on page 128.

Indicateurs d'étiquette de politique

Sur le graphique de la série chronologique d'analyse des politiques, les indicateurs d'étiquettes de politique marquent le moment où l'analyse a été lancée et à chaque moment l'analyse a été redémarrée pour refléter les dernières modifications de politique et de grappe.

Cliquez sur un indicateur pour afficher la version des politiques associées à cet indicateur :

Figure 66: Indicateur d'étiquette de politique dans le graphique de série chronologique



Cliquer sur un indicateur d'étiquette de politique pour ouvrir la version correspondante de la page Policies (Politiques) et afficher les politiques analysées par cette version d'analyse de politiques.

Afficher, comparer et gérer les versions des politiques analysées

Chaque fois que vous analysez ou réanalysez les politiques dans un espace de travail après avoir apporté des modifications, une nouvelle version d'analyse (p*) est créée.

Pour en savoir plus sur la gestion des versions, consultez À propos des versions des politiques (v* et p*), à la page 147.

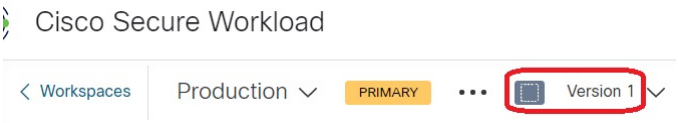
Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Accédez au portée et à l'espace de travail principal appropriés.

Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 4 La version actuellement affichée des politiques est indiquée en haut de la page :



La version affichée peut être une version de découverte de politique, une version de politique analysée ou une version de politique appliquée.

Étape 5 Vous pouvez réaliser les actions suivantes :

Pour afficher une version différente des politiques :	Cliquez sur la version actuelle et choisissez une version différente. Pour obtenir une description des versions, consultez À propos des versions des politiques (v* et p*), à la page 147. **Important!** Si vous choisissez la version av*, consultez Afficher, comparer et gérer les versions de politiques découvertes, à la page 55 au lieu de cette rubrique, sans oublier la mise en garde importante à la fin de celle-ci.
Pour afficher les détails des versions analysées :	**1.** Cliquez sur **View Version History** (Afficher l'historique des versions) en haut de la page à côté dans la version actuelle. **2.** Cliquez sur l'onglet **Published Versions** (Versions publiées) pour voir les versions des politiques analysées et appliquées. **3.** Pour afficher les entrées de journal pour une version, cliquez sur le lien dans la version. Les lignes vert clair représentent l'activité d'analyse. Les lignes vert clair représentent l'activité d'application de la politique.

Pour comparer deux versions et voir ce qui a changé :	**1.** Cliquez sur **Compare Revisions** (Comparer les révisions). **2.** Choisissez les versions à comparer. Vous pouvez comparer la dernière version provisoire, les versions analysées et appliquées. **3.** Pour en savoir plus sur les résultats, consultez Comparaison des versions des politiques : différence de politique, à la page 149.
Pour supprimer une version indésirable :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Delete** (Supprimer). Les versions de politique publiées (versions p*) peuvent être supprimées tant que la version n'est pas analysée ou appliquée activement.
Pour exporter une version :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Export...** (Exporter...). Consultez aussi Exporter un espace de travail, à la page 59.

Prochaine étape

Lorsque vous avez terminé de travailler avec les versions, remplacez la version en haut de la page de l'espace de travail par la dernière version de politique découverte (v*).

Cela évite la suppression involontaire des versions de politiques découvertes et vous permet de créer manuellement des politiques dans l'espace de travail.

Journaux d'activité de l'analyse des politiques

Tous les utilisateurs d'espace de travail peuvent afficher les journaux d'activités associés aux modifications apportées dans la page d'analyse des politiques dans l'historique de l'espace de travail (voir Journaux d'activités et historique des versions).

- Activer l'analyse des politiques

Figure 67: Activer l'analyse des politiques

- Désactiver l'analyse des politiques

Figure 68: Désactiver l'analyse des politiques

- Mettre à jour l'analyse des politiques

Figure 69: Mettre à jour l'analyse des politiques

Appliquer des politiques

Cisco Secure Workload peut appliquer des politiques en utilisant :

- Déployer des agents logiciels sur les charges de travail installés sur les charges de travail individuelles :
  - Linux
  - Windows
  - Kubernetes/OpenShift

  Pour les détails techniques sur le fonctionnement des agents sur chaque plateforme, consultez les Application des politiques par le biais d'agents et Application des conteneurs, on page 138.
- Connecteurs infonuagiques
  - AWS par l'intermédiaire de Connecteur AWS
  - Azure par l'intermédiaire de Connecteur Azure
- Intégrer les équilibreurs de charge par l'intermédiaire d'un orchestrateur externe :
  - F5 BIG-IP
  - Citrix Netscaler
- Intégration avec Cisco Secure Firewall Management Center
- Diffusion en flux continu vers des orchestrateurs tiers pour mise en application dans une infrastructure tierce

Caution Lorsque vous appliquez des politiques, le système insère de nouvelles règles de pare-feu sur les hôtes concernés et supprime toutes les règles existantes sur ces derniers.

Vérifier l'intégrité de l'agent et la préparation à la mise en application

Certaines de ces vérifications peuvent être effectuées avant ou après l'application de la politique.

Des autorisations peuvent être nécessaires pour modifier les capacités de l'agent ou du connecteur; Consultez les exigences et les prérequis dans les chapitres pertinents.

Vous n'avez pas besoin d'effectuer ces vérifications pour les charges de travail pour lesquelles vous n'avez pas l'intention d'appliquer des politiques.

Vérifiez que :	Autres renseignements
Les agents sont installés sur toutes les charges de travail de la portée qui sont associées à l'espace de travail objet de la mise en application	Cliquez sur **Defend (défense) » Segmentation (défense)** et accédez à la portée et à l'espace de travail appropriés. Cliquez sur **Matching Inventories** (Correspondance des inventaires), puis sur **IP Addresses** (Adresses IP). Les adresses IP sous cet onglet ne comportent généralement pas d'agents installés, et les agents doivent généralement être installés pour appliquer la politique. Exceptions : l'application a lieu pour les types d'inventaire suivants qui s'affichent dans l'onglet IP Addresses (adresses IP) : • Inventaire infonuagique sur lequel la politique est appliquée à l'aide d'un connecteur infonuagique. (L'installation des agents sur les charges de travail individuelles est facultative). • Les adresses Kubernetes apparaissent dans la liste des adresses IP si les agents sont installés sur des pods de charge de travail individuels; L'inventaire de Kubernetes avec les agents installés s'affiche sous l'onglet « Pods ».
La version de l'agent installé est à jour et prise en charge	Pour obtenir un aperçu des versions des agents installées, cliquez sur **Manage (Gérer) > Agents (agents)**, puis cliquez sur **Distribution** (diffusion) et consultez le tableau **Distribution Version Software Agent** (distribution des versions des logiciels de l'agent). Pour en savoir plus, cliquez sur **Manage (Gestion) > Agents (Agents)** , puis sur **Agents List (Liste des agents)** .
Les agents installés ont une capacité d'application.	Cliquez sur **Manage (Gestion) > Agents (Agents)**, puis sur **Convert to Enforcement Agent(Conversion en agent d'application)**. Dans la zone **Filter** (filtre), saisissez **`Agent Type = Advanced Visibility (visibilité approfondie).`** Convertir tous les agents qui doivent appliquer la politique.
L'application est activée pour tous les agents.	(Cette exigence est distincte de l'assurance que les agents ont des capacités d'application et de l'activation de l'application dans l'espace de travail). **Important!** Selon votre déploiement, cela peut être fait avant ou après avoir mis en application l'espace de travail. Vérifiez que Vérifier l'application est activée pour les agents.
L'application est activée pour les mécanismes d'application autres que d'agent	**Important!** N'activez pas la mise en application sur les connecteurs infonuagiques sans agents TANT QUE VOUS N'AVEZ PAS mis en application la politique sur l'espace de travail. Les orchestrateurs externes qui prennent en charge l'application doivent également être activés avant de pouvoir être appliqués.

Vérifiez que :	Autres renseignements
Le paramètre **Preserve Rules** (Conserver les règles) du profil de configuration de l'agent est approprié pour la plateforme de charge de travail	• Pour Kubernetes/OpenShft, consultez la section relative à l'application sur les conteneurs. • Pour les autres plateformes, consultez les informations pour chaque plateforme dans la section Agents logiciels. Conseil : Recherchez « Conserver les règles » dans ce document pour trouver des informations utiles.
(Une fois l'espace de travail appliqué). Tous les agents ont reçu les politiques applicables à la charge de travail	Consultez la section Vérifier si les politiques appliquées sont envoyées aux agents.
Les agents sont intègres	En plus des sources ci-dessus, les emplacements suivants contiennent des informations sur l'intégrité des agents : • Cliquez sur **Manage > Agents (Gestion > Agents)**, puis sur **Monitor**(surveillance). Regardez les informations sous **Enforcement Agents** Agents d'application). • Cliquez sur **Manage > Agents (Gestion > Agents)**, puis sur **Distribution**. Choisissez le type d'agent dans le haut de la page. • Cliquez sur le filtre **Organize > Scopes and Inventory (Organiser> Portées et inventaire)**, pour trouver une charge de travail spécifique d'intérêt, puis cliquez sur l'adresse IP. La page **Workload Profile** (Profil de la charge de travail) s'ouvre dans une fenêtre de navigateur distincte comprenant un panneau Intégrité de l'agent. Pour en savoir plus, consultez la section Profil de charge de travail.

Activer l'application des politiques

Caution L'application des politiques supprime les règles de pare-feu existantes et écrit de nouvelles règles de pare-feu pour chaque charge de travail de la portée qui est affectée par cet espace de travail.

Si vous n'avez pas totalement vérifié que vos politiques fonctionnent correctement, leur mise en application peut modifier le fonctionnement de vos applications et perturber les tâches opérationnelles.

Before you begin

- Pour commencer, lorsque vous appliquez des politiques, envisagez de définir la règle collectrice sur Allow (Autoriser). Ensuite, surveillez le trafic pour voir ce qui correspond à la règle collectrice.

Lorsqu'aucun trafic nécessaire ne correspond à la règle « collectrice », vous pouvez définir ce paramètre sur Deny (Refuser).

- Si vous appliquez des espaces de travail dans plusieurs portées à la fois, vous ne pouvez appliquer que les espaces de travail analysés. Si vous appliquez un espace de travail unique en utilisant la deuxième méthode décrite dans la procédure ci-dessous, l'analyse des politiques de l'espace de travail avant de l'appliquer est recommandée, mais est non obligatoire.

  Consultez la section Analyse des politiques en temps réel et sous-sections.

- L'assistant pour l'application d'une seule portée est plus détaillé que celui qui offre la possibilité d'appliquer plusieurs portées simultanément. Si vous avez besoin des fonctionnalités de Assistant d'application des politiques, on page 136, utilisez la deuxième méthode décrite dans la procédure ci-dessous.

- **IMPORTANT!** Vérifiez que les politiques sont correctes.

  Les résultats des politiques dans n'importe quel espace de travail peuvent être affectés par les politiques appliquées dans d'autres portées. Avant que l'application des politiques ne soit activée sur un espace de travail, la page Policy Enforcement (Application des politiques) montre comment les flux sont touchés par les politiques appliquées dans les espaces de travail associés à d'autres portées. Par exemple, une politique générale « Les hôtes de production ne doivent pas communiquer avec les hôtes hors production » de l'espace de travail appliqué d'une portée parente peut avoir une incidence sur le trafic sur les charges de travail appartenant à une application dans une portée enfant.

  Si aucun nouveau renseignement ne s'affiche dans les tableaux Enforcement (d'application), assurez-vous que la bonne plage temporelle est sélectionnée.

  Pour en savoir plus sur les informations que vous voyez sur la page Enforcement (Application), consultez Analyse des politiques en temps réel et sous-sections. (Les mêmes renseignements concernant l'analyse en direct s'appliquent également à la page Application de la politique).

  Si les résultats de l'analyse en direct diffèrent des résultats sur la page Enforcement (d'application), assurez-vous que les portées, les versions de politiques et la plage temporelle analysées sont les mêmes que les portées, les versions de politiques et la plage temporelle utilisés pour générer des résultats sur la page d'application.

- Découvrez comment les agents appliquent les politiques sur chaque plateforme. Consultez :
  - Pour les charges de travail Windows et Linux, consultez les Application des politiques par le biais d'agents et les rubriques secondaires.
  - Pour Kubernetes et OpenShift, consultez

    Application des conteneurs, on page 138.
  - Pour les équilibreurs de charge, consultez

    Application de la politique pour Citrix Netscaler et

    Application de la politique pour F5 BIG-IP.
  - Pour les charges de travail infonuagique configurées à l'aide de connecteurs infonuagiques, consultez :
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS et les rubriques connexes.
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure et les rubriques connexes.

- Vous devez avoir les autorisations requises pour appliquer des politiques :

  Vous devez avoir la capacité Appliquer ou supérieure sur la portée. Les utilisateurs disposant d'autres capacités sur la portée peuvent toujours afficher cette page, mais ne pourront pas appliquer (ou désactiver) les nouvelles politiques.

- Vérifiez que tous les agents installés pertinents et les autres points terminaux d'application, tels que les connecteurs infonuagiques, sont prêts à appliquer la politique. Pour obtenir la liste des vérifications de l'intégrité et de la préparation des agents, consultez Vérifier l'intégrité de l'agent et la préparation à la mise en application, on page 130.

Note Certaines de ces vérifications doivent être effectuées après la mise en application; par exemple, vous ne devez activer l'application sur les connecteurs infonuagiques qu'après avoir activé l'application dans l'espace de travail. Pour les agents installés, vous activez généralement l'application dans la configuration de l'agent avant d'appliquer l'espace de travail.

Procedure

Étape 1 Dans le volet de navigation, choisissez **Defend** > **Segmentation**(défendre la segmentation).

Étape 2 Vous pouvez appliquer des politiques pour une ou plusieurs portées à la fois :

Pour appliquer la politique à plusieurs portées à la fois :

(Seuls les espaces de travail qui ont été analysés peuvent être appliqués à l'aide de ce processus).

a) Cliquez sur le signe d'insertion sur le côté droit de la page pour afficher le volet Tools (outils) :
b) Cliquez sur **Enable Enforcement** (Activer l'application).
c) Cliquez sur **Next** (suivant) pour démarrer l'assistant.
d) Sélectionnez un espace de travail à mettre en application.

   (L'option permettant l'application d'espaces de travail pour des portées supplémentaires se trouve sur la dernière page de l'assistant).

e) Cliquez sur **Next** (suivant).
f) Choisissez la version de cet espace de travail à appliquer, puis cliquez sur **Next** (Suivant).
g) Pour appliquer simultanément les politiques à une autre portée, cliquez sur **+ Add Another Workspace** (+ Ajouter un autre espace de travail) et procédez comme suit.

   Répétez l'opération si nécessaire pour les autres portées.

h) Cliquez sur **Accept and Enforce** (Accepter et appliquer).

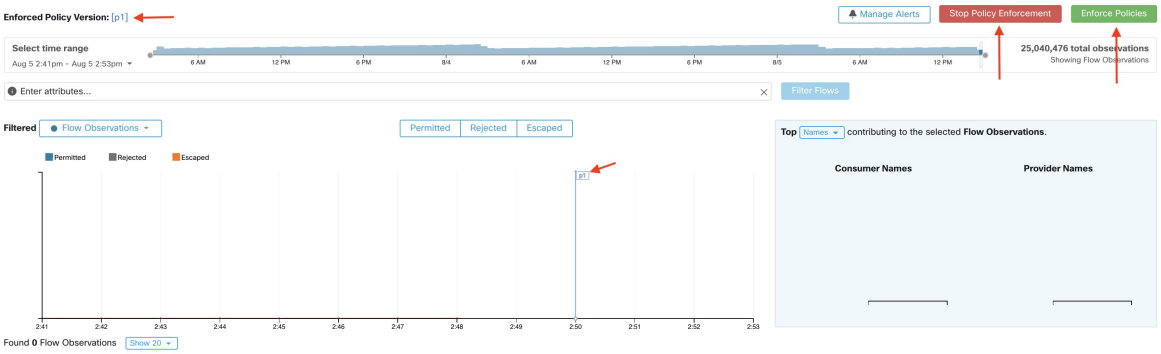
Pour appliquer des politiques à une seule portée :

a) Accédez à l'espace de travail principal de la portée pour laquelle vous souhaitez appliquer la politique.
b) Cliquez sur **Manage Policies** (Gestion des politiques).
c) Cliquez sur **Enforcement** (Mise en application).
d) Cliquez sur **Enforce Policies** (Appliquer les politiques).
e) Suivez les étapes de l'assistant.

   Pour en savoir plus sur l'assistant, consultez Assistant d'application des politiques, on page 136.

Étape 3 Cliquez sur **Accept and Enforce** (Accepter et appliquer) sur la dernière page de l'assistant pour envoyer les nouvelles règles de pare-feu vers les ressources concernées par les politiques dans cet espace de travail. Un indicateur d'étiquette est créé au moment de l'application :

Figure 70: Page Policy Enforcement (Application de la politique) avec Mise en application activée



Vous devrez peut-être actualiser la page pour voir l'indicateur.

What to do next

- Si vous avez appliqué une politique pour un seul espace de travail, demandez-vous si l'application de la politique doit également concerner d'autres espaces de travail d'autres portées afin d'obtenir les résultats escomptés en matière d'application.

  Par exemple, il peut être nécessaire d'appliquer la politique aux espaces de travail pour les portées ascendantes ou les portées qui incluent des charges de travail impliquées dans des politiques inter-portées.

- L'application n'aura pas lieu tant que la mise en application n'est pas activée pour les agents, les connecteurs infonuagiques ou les orchestrateurs externes qui assurent l'application des politiques :
  - Pour les charges de travail sur lesquelles des agents sont installés, appliquez la politique dans la configuration de l'agent pour les portées et les filtres d'inventaire pertinents. Consultez Configuration de l'agent logiciel et les sous-sections.
  - Pour les charges de travail infonuagique configurées à l'aide de connecteurs infonuagiques, consultez :
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS et les rubriques connexes.
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure et les rubriques connexes.
  - Pour Kubernetes et OpenShift consultez :
    - Application des conteneurs, on page 138
    - Configuration de l'agent logiciel
  - Pour les équilibreurs de charge, consultez :
    - Application de la politique pour F5 BIG-IP

      Application des politiques au contrôleur d'entrée F5

- Application de la politique pour Citrix Netscaler

- Vérifiez que la mise en application fonctionne comme prévu. Consultez Vérifier que l'application fonctionne comme prévu, on page 139.
- Configurez les alertes pour être informé de tout problème, par exemple si les flux sont rejetés après l'activation de la mise en application.

Assistant d'application des politiques

Lorsque vous appliquez des politiques pour un seul espace de travail à partir de la page d'application de l'espace de travail, l'assistant d'application de politiques vous permet de :

- Passer en revue les politiques avant de les mettre en œuvre sur les charges de travail.

  Cela inclut les politiques héritées des portées ascendantes.
- Télécharger les modifications à la politique pour examen.
- Comparer les versions des politiques.
- Choisissez la version analysée de l'espace de travail à appliquer.
- Restaurer les politiques à une version précédente.

Étapes de l'assistant d'application des politiques :

1. Sélectionnez les mises à jour des politiques

   Vous pouvez sélectionner la version des politiques à appliquer aux charges de travail.

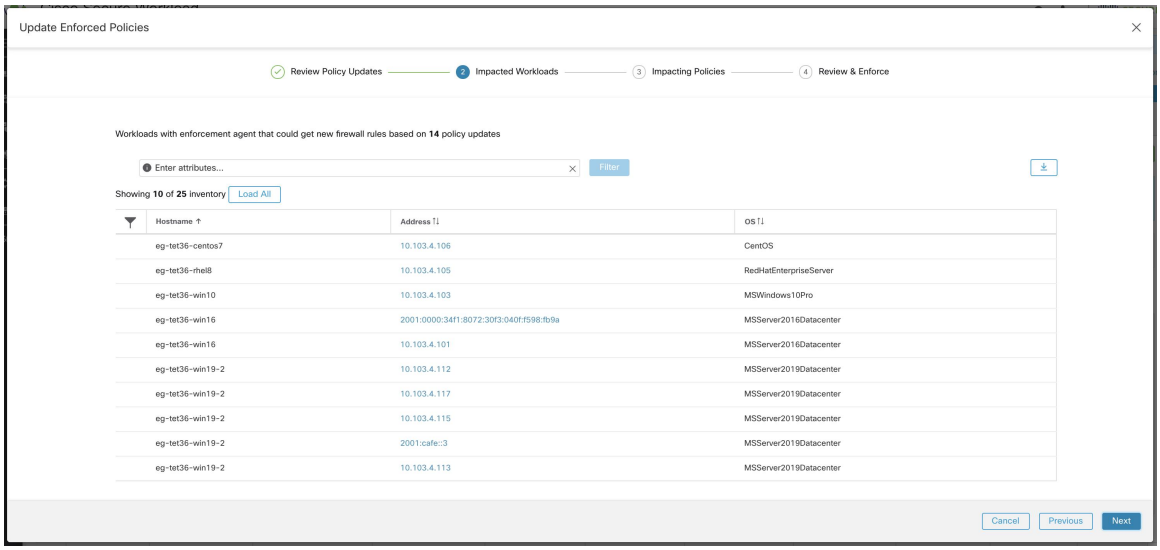
   La différence entre les politiques actuellement appliquées et les politiques dans la version sélectionnée s'affiche.

   De même pour Comparaison des versions des politiques : différence de politique ((Différences des politiques), vous pouvez filtrer et examiner les modifications de politique et les télécharger au format CSV.
2. Charges de travail affectées

   Cette étape affiche les charges de travail qui seront affectées par les nouvelles règles de pare-feu générées à partir des modifications de politique sélectionnées. Le résultat provient de la recherche de toutes les charges de travail qui ont des agents d'application dans le groupe des consommateurs/fournisseurs des changements de politique sélectionnés.

   Le nombre de charges de travail potentiellement touchées ne peut pas dépasser le nombre total de charges de travail de la portée. Cependant, le nombre réel de charges de travail concernées peut être plus faible en raison d'autres facteurs tels que les intents de configuration de l'agent.

Figure 71: Liste des charges de travail affectées

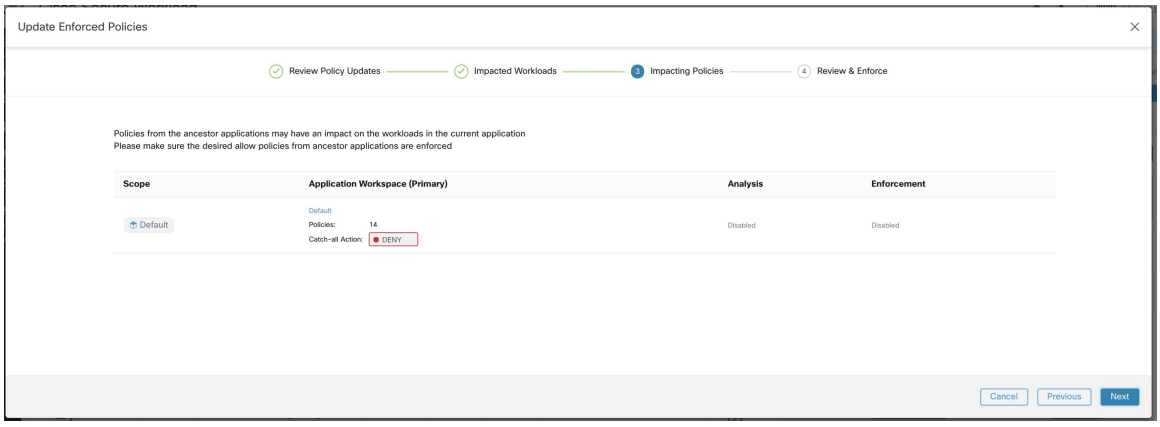


Pour plus de détails sur l'affichage, le filtrage et le téléchargement des éléments de l'inventaire, consultez Gérer l'inventaire pour Cisco Secure Workload.

3. Politiques ayant une incidence

   Les politiques des espaces de travail ascendants peuvent avoir une incidence sur les charges de travail de l'espace de travail actuel. Par conséquent, vous devez vous assurer que les politiques d'autorisation souhaitées des espaces de travail ascendants sont appliquées.

   Figure 72: Liste des espaces de travail ascendants et des versions appliquées

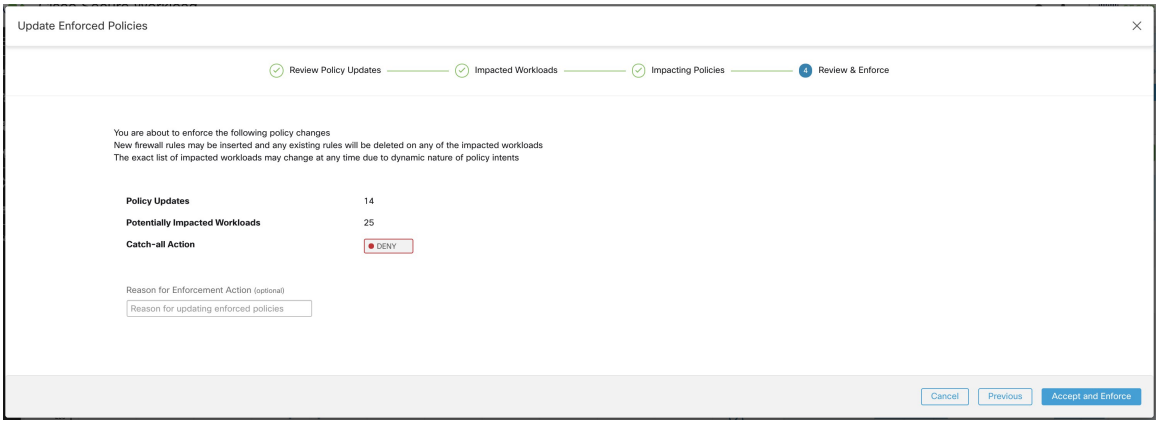


4. Lire attentivement et accepter.

   Cette dernière étape résume les modifications de politique à appliquer, le nombre de charges de travail potentiellement touchées et l'action globale qui sera appliquée. Lorsque vous cliquez sur **Accepter et appliquer**, les politiques de l'espace de travail sont utilisées pour calculer les nouvelles règles de pare-feu qui seront configurées sur les charges de travail pertinentes.

   Vous avez la possibilité de fournir un nom, une description et un motif d'action pour les politiques nouvellement appliquées pour référence future. En cas de restauration, vous pouvez fournir uniquement la raison, car le nom et la description d'une version antérieure ne peuvent pas être modifiés.

Figure 73: Examiner le résumé et appliquer les modifications à la politique



Application des conteneurs

Pour obtenir une présentation des étapes requises pour configurer la segmentation sur les charges de travail basées sur des conteneurs qui sont gérées par Kubernetes et OpenShift, consultez Configurer la microsegmentation pour les charges de travail basées sur Kubernetes.

Attention **Les agents s'exécutant sur des hôtes Kubernetes/OpenShift doivent être configurés pour conserver les règles existantes.**

Afin d'éviter que l'application n'interfère avec les règles iptables ajoutées par Kubernetes, l'agent doit être configuré avec un profil pour lequel l'option **Preserve Rules** (Conserver les règles) est activée. Voir Créer un profil de configuration d'agent.

Lors de l'application des politiques sur les conteneurs, Cisco Secure Workload permet d'utiliser les abstractions de service Kubernetes/OpenShift en tant que fournisseurs. En interne, les politiques relatives aux abstractions de services sont transformées en règles pour les pods fournisseurs et les nœuds sur lesquels ils s'exécutent. Cette transformation dépend du type du service Kubernetes/OpenShift, et elle est mise à jour de manière dynamique chaque fois que des modifications sont reçues du serveur d'API.

L'exemple suivant illustre la souplesse rendue possible par cette fonctionnalité. Tenez compte de la politique suivante, qui autorise le trafic de tous les hôtes et des pods avec l'étiquette *environment = production* vers un service Kubernetes de type *NodePort* avec le nom *db* qui expose le port TCP 27017 sur un ensemble de pods.

Consommateur	Fournisseur	Protocole/Port	Action
environment = production OU orchestrator_environment = production	orchestrator_system/service_name = db	TCP 27017	Autoriser

Cette politique produira les règles de pare-feu suivantes :

- Sur les hôtes et les pods étiquetés avec *environment = production*, autorisez les connexions sortantes vers tous les nœuds Kubernetes de la grappe à laquelle le service appartient. Cette règle utilise le port de nœud affecté à ce service par Kubernetes.
- Sur les pods avec l'étiquette *environment = production*, autorisez les connexions sortantes vers la ClusterIP attribuée à ce service par Kubernetes. Cette règle utilise le port accessible par le service (TCP 27017).
- Sur les nœuds Kubernetes de la grappe à laquelle le service appartient, autorisez les connexions sortantes vers les pods du fournisseur. Cette règle utilise le port cible accessible par le service (TCP 27017).
- Sur les pods fournissant la base de données de service, autorisez toutes les connexions entrantes de tous les nœuds Kubernetes et des hôtes et pods des consommateurs. Cette règle utilise le port cible accessible par le service (TCP 27017).

Les modifications apportées au type de service, aux ports et à l'ensemble de pods des fournisseurs sont immédiatement détectées par le générateur de règles Cisco Secure Workload et utilisées pour mettre à jour les règles de pare-feu générées.

Caution **Les politiques comprenant l'inventaire Kubernetes/OpenShift doivent être conçues avec soin pour éviter tout conflit avec le fonctionnement interne de la grappe Kubernetes.**

Les éléments Kubernetes/OpenShift importés par Cisco Secure Workload comprennent les pods et les services constituant la grappe Kubernetes (par exemple, les pods dans l'espace de noms du système Kubernetes). Cela permet de définir des politiques précises pour sécuriser la grappe Kubernetes elle-même, mais cela signifie également que des politiques mal conçues peuvent affecter le fonctionnement de la grappe.

Vérifier que l'application fonctionne comme prévu

Vérifier les agents

Consultez Vérifier l'intégrité de l'agent et la préparation à la mise en application, à la page 130.

Vérifier les flux échappés et rejetés

Dans le menu sur le côté gauche de l'écran, cliquez sur **Overview** (Aperçu).

Sur la page **Security Dashboard** (Tableau de bord de sécurité), examinez la **note de conformité de la segmentation**.

Si elle est inférieure à 100, il se peut que vous ayez des flux échappés ou rejetés, ce qui indique un problème de configuration de la politique.

Pour de plus amples renseignements, consultez la section Note de conformité de la segmentation.

Pour plus d'informations sur l'examen de ces situations, consultez Résultats de l'analyse des politiques : comprendre les bases, à la page 120 et les rubriques secondaires. (Les informations dans ces rubriques s'appliquent aux politiques appliquées affichées sous l'onglet Enforcement (Application) et aux politiques analysées affichées sous l'onglet Policy Analysis (Analyse des politiques).)

Ajoutez toutes les politiques manquantes ou modifiez les politiques existantes, par exemple en ajoutant des protocoles ou des ports supplémentaires, pour autoriser le trafic légitime requis.

Effectuez ensuite une nouvelle analyse avant de recommencer l'application de la politique.

Afficher les politiques appliquées pour une charge de travail spécifique (politiques concrètes)

Cette procédure permet d'afficher toutes les politiques appliquées pour une charge de travail spécifique (c'est-à-dire les *politiques concrètes* pour cette charge de travail). Cet affichage est utile, car toutes les politiques d'un espace de travail peuvent ne pas s'appliquer à toutes les charges de travail de ce dernier, et les politiques de plusieurs espaces de travail peuvent s'appliquer à une charge de travail particulière (par exemple, les politiques héritées dans les portées parentes ou encore précédentes).

Les politiques concrètes sont répertoriées par ordre de priorité. Pour en savoir plus sur les effets de la priorité, consultez la section sur les priorités de politique.

Avant de commencer

Remarque Les politiques concrètes ne comprennent que les politiques des espaces de travail ayant fait l'objet de mise en application. Si un espace de travail n'a pas été mis en application, les politiques qui s'appliqueraient à la charge de travail si l'espace de travail était mis en application ne s'affichent pas dans la liste.

Procédure

Étape 1 Vous pouvez accéder à la page des politiques concrètes pour une charge de travail à partir de la page Inventory (Inventaire) ou de l'espace de travail :

Pour accéder à partir de la page Scope and Inventory (Portée et inventaire) :

a) Choisissez **Organize > Scopes and Inventory** (Organiser > Portée et inventaire).
b) Recherchez l'adresse IP de la charge de travail qui vous intéresse et cliquez dessus.

Le profil de charge de travail s'ouvre dans un onglet distinct.

En général, sauf pour les charges de travail infonuagique qui sont gérées sans agents, Kubernetes et les charges de travail OpenShift, si l'adresse IP apparaît dans l'onglet **IP Addresses** (adresses IP) et non dans l'onglet **Workloads** (Charges de travail), cela signifie qu'un agent n'est pas installé sur la charge de travail, Les politiques ne peuvent donc pas être appliquées et il n'y a pas de liste de politiques concrètes.

Pour accéder à partir de la page de segmentation :

a) Choisissez **Defend (défense) > Segmentation (segmentation).**
b) Cliquez sur la portée.
c) Cliquez sur l'espace de travail principal.
d) Cliquez sur **Manage Policies** (Gestion des politiques).
e) Cliquez sur l'onglet **Matching Inventories** (Inventaires correspondants).
f) Recherchez l'adresse IP de la charge de travail qui vous intéresse et cliquez dessus.
g) Dans le panneau qui s'ouvre sur la droite, cliquez sur **View Workload Profile**(afficher le profil de charge de travail).

Le profil de charge de travail s'ouvre dans un onglet distinct.

Étape 2 Dans le menu de gauche de la page du profil de charge de travail, cliquez sur **CONCRETE POLICIES (POLITIQUES CONCRÈTES).**

Étape 3 Cliquez sur une ligne pour afficher les détails.

Pour en savoir plus, consultez l'onglet Politiques concrètes.

Étape 4 Pour voir le volume de trafic qui a atteint chaque politique :

a) Cliquez sur **Get All Stats** (récupérer toutes les statistiques).

b) Cliquez sur chaque politique qui vous intéresse.

Étape 5 Pour afficher des informations sur les charges de travail de Kubernetes ou d'OpenShift cliquez sur **CONTAINER POLICIES** (POLITIQUES DE CONTENEUR).

Prochaine étape

Choisissez **Monitor > Enforcement Status** (Surveiller > État de l'application) pour connaître l'état de politiques concrètes, par exemple pour voir si des politiques ont été ignorées. Pour en savoir plus, consultez la section État de l'application.

Vérifier que la mise en application est activée pour les agents

Procédure

Étape 1 Cliquez sur **Defend > Enforcement Status** (Défendre > État d'application).

Étape 2 Pour afficher uniquement l'état d'application pour une portée spécifique, activez le contrôle **Filter by Scope** (Filtrer par portée) et sélectionnez une portée.

Étape 3 Consultez le tableau **Agent Enforcement Enabled** (Mise en application des agents activée).

Si le tableau indique que des agents sont **Not Enforced** (ne sont pas mis en application), poursuivez cette procédure.

Sinon, ignorez le reste de la procédure, car tous les agents sont activés pour application.

Étape 4 Cliquez sur la section orangée **Not Enforced** (Non appliqué) du tableau pour afficher les charges de travail concernées au sein de la table sous le tableau.

Étape 5 Activez l'application sur ces charges de travail en modifiant le profil de configuration de l'agent.

Consultez Créer un profil de configuration d'agent.

Vérifier que les politiques appliquées sont transmises aux agents

Pour que l'application ait lieu, les politiques spécifiques à chaque charge de travail doivent être transmises avec succès vers l'agent installé sur cette charge de travail. L'état est également affiché pour l'application des politiques gérée par les connecteurs infonuagiques, même si des agents ne sont pas installés.

Avant de commencer

Appliquer des politiques pour au moins une portée.

Procédure

Étape 1 Cliquez sur **Defend > Enforcement Status** (Défendre > État d'application).

Étape 2 Pour afficher uniquement l'état d'application pour une portée spécifique, activez le contrôle **Filter by Scope** (Filtrer par portée) et sélectionnez une portée.

Étape 3 Consultez le tableau des **politiques concrètes des agents**.

Si le tableau indique que des fichiers sont **ignorés**, poursuivez cette procédure.

Sinon, ignorez le reste de cette procédure.

Étape 4 Pour afficher la liste des charges de travail touchées par ce problème, cliquez sur la partie rouge **Skipped** (Ignoré) du tableau.

Les charges de travail concernées sont répertoriées dans le tableau sous les graphiques.

Étape 5 Pour voir les raisons de ce problème :

Pour chaque charge de travail dans les résultats de la recherche, cliquez sur le bouton **(i)** à côté de **Skipped** (Ignoré) dans la colonne **Concrete Policies** (Politiques concrètes).

Message d'erreur	Autres renseignements
L'agent n'a pas de système d'exploitation Windows	Au moins une politique applicable uniquement aux charges de travail Windows comprend les consommateurs ou les fournisseurs qui n'exécutent pas le système d'exploitation Windows. Supprimez ces charges de travail de ces politiques.
Le nombre maximal de politiques a été atteint	Consultez Si l'agent dispose d'un trop grand nombre de politiques, à la page 142.

Prochaine étape

(Facultatif) Configurez une alerte pour être averti si cette situation se reproduit. Consultez Configurer les alertes.

Si l'agent dispose d'un trop grand nombre de politiques

Si l'ensemble complet des politiques concrètes applicables ne peut pas être transmis à un agent en particulier, la dernière version des politiques n'est pas transmise.

Arrière-plan : Il y a une limite au nombre de politiques prises en charge sur chaque agent. Les limites s'appliquent également aux politiques appliquées à l'aide de connecteurs infonuagiques. Vous trouverez peut-être les renseignements de Limites de configuration dans Cisco Secure Workload utiles.

Avant de commencer

Utilisez cette procédure pour résoudre ce problème si Vérifier que les politiques appliquées sont transmises aux agents, à la page 141 indique que l'agent ne peut pas prendre en charge l'ensemble complet des politiques appliquées.

Procédure

Étape 1 Accédez à l'espace de travail principal pour une portée concerné.

Étape 2 Modifiez les politiques dans l'espace de travail principal :

Essayez de réduire le nombre de politiques et de réduire les longues listes d'adresses IP du consommateur ou du fournisseur.

Par exemple, regrouper les politiques existantes et/ou baser les politiques sur les sous-réseaux plutôt que sur de longues listes d'adresses IP.

Pour les politiques appliquées à l'aide d'un connecteur infonuagique, vous pouvez également augmenter les limites imposées par la plateforme. Consultez la documentation de votre plateforme infonuagique.

Étape 3 Après avoir apporté les modifications, utilisez la dernière version de l'espace de travail et vérifiez à nouveau les politiques ignorées.

Étape 4 Répétez cette procédure pour toutes les autres portées rencontrant ce problème.

Modifier les politiques appliquées

Appliquer les politiques nouvelles et révisées

Si vous devez réviser des politiques après leur application, vous effectuez généralement les modifications dans le même espace de travail principal. Ensuite, examinez attentivement vos modifications et analysez à nouveau l'espace de travail pour vous assurer qu'elles produisent l'effet escompté. Lorsque vous êtes certain que les modifications auront l'effet souhaité, cliquez sur le bouton **Enforce Latest Policies**(Appliquer les dernières politiques) dans le coin supérieur droit de la page.

Afficher, comparer et gérer les versions des politiques appliquées

Chaque fois que vous appliquez ou renforcerez des politiques dans un espace de travail après avoir apporté des modifications, une nouvelle version (p*) est créée.

Pour en savoir plus sur la gestion des versions, consultez À propos des versions des politiques (v* et p*), à la page 147.

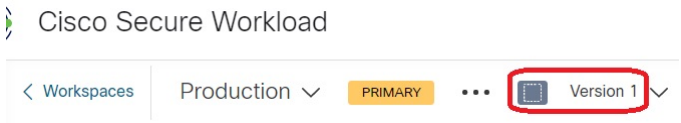
Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Accédez au portée et à l'espace de travail principal appropriés.

Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 4 La version actuellement affichée des politiques est indiquée en haut de la page :



La version affichée peut être une version de découverte de politique, une version de politique analysée ou une version de politique appliquée.

Étape 5 Effectuez l'une des opérations suivantes :

Pour afficher une version différente des politiques :	Cliquez sur la version actuelle et choisissez une version différente. Pour obtenir une description des versions, consultez À propos des versions des politiques (v* et p*), à la page 147. **Important!** Si vous choisissez la version av*, consultez Afficher, comparer et gérer les versions de politiques découvertes, à la page 55 au lieu de cette rubrique, sans oublier la mise en garde importante à la fin de celle-ci.
Pour afficher les détails des versions analysées :	1. Cliquez sur **View Version History** (Afficher l'historique des versions) en haut de la page à côté dans la version actuelle. 2. Cliquez sur l'onglet **Published Versions** (Versions publiées) pour voir les versions des politiques analysées et appliquées. 3. Pour afficher les entrées de journal pour une version, cliquez sur le lien dans la version. Les lignes vert clair représentent l'activité d'analyse. Les lignes vert clair représentent l'activité d'application de la politique.
Pour comparer deux versions et voir ce qui a changé :	1. Cliquez sur **Compare Revisions** (Comparer les révisions). 2. Choisissez les versions à comparer. Vous pouvez comparer la dernière version provisoire, les versions analysées et appliquées. 3. Pour en savoir plus sur les résultats, consultez Comparaison des versions des politiques : différence de politique, à la page 149.
Pour supprimer une version indésirable :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Delete** (Supprimer). Les versions de politique publiées (versions p*) peuvent être supprimées tant que la version n'est pas analysée ou appliquée activement.
Pour exporter une version :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Export...** (Exporter...). Consultez aussi Exporter un espace de travail, à la page 59.

Prochaine étape

Lorsque vous avez terminé de travailler avec les versions, remplacez la version en haut de la page de l'espace de travail par la dernière version de politique découverte (v*).

Cela évite la suppression involontaire des versions de politiques découvertes et vous permet de créer manuellement des politiques dans l'espace de travail.

Revenir à une version antérieure des politiques appliquées

Pour restaurer les politiques appliquées vers une version précédente, suivez l'un des processus décrits dans Activer l'application des politiques, à la page 132 et choisissez une version antérieure à appliquer.

Désactiver l'application de la politique

- **Pour désactiver l'application des politiques pour plusieurs portées simultanément** :

  Suivez la procédure pour appliquer la politique dans plusieurs portées simultanément, comme décrit dans Activer l'application des politiques, on page 132. Dans la page Select Version (sélectionner une version) de l'assistant, cliquez sur **Select a version** (sélectionner une version) et choisissez **Disable enforcement**) ((désactiver la mise en application).

- **Pour désactiver l'application des politiques pour une seule portée** :

  Accédez à la page Policy Enforcement (application des politiques) de l'espace de travail principal de la portée et cliquez sur le bouton rouge **Stop Policy Enforcement** (Arrêter l'application des politiques). Cela écrit de nouvelles règles de pare-feu dans les ressources de la portée en fonction des politiques appliquées dans les espaces de travail ascendants. Un indicateur d'étiquette avec un « x » sera créé sur le tableau des séries chronologiques.

Suspendre les mises à jour des politiques

Caution Cette option met en pause les mises à jour de politiques pour TOUTES les charges de travail dans TOUTES les portées.

Cette fonctionnalité nécessite des privilèges d'administrateur de site ou de service d'assistance à la clientèle.

Pour suspendre les mises à jour des règles pour tous les points terminaux d'application dans toutes les portées :

1. Dans le volet de navigation, choisissez **Defend (Défendre)** > **Enforcement (Mise en application)** .
2. Cliquez sur l'état à côté de **Policy Updates** (Mises à jour des politiques) .
3. Lisez et acceptez la mise en garde.

Figure 74: Les règles de pare-feu sont mises à jour en permanence

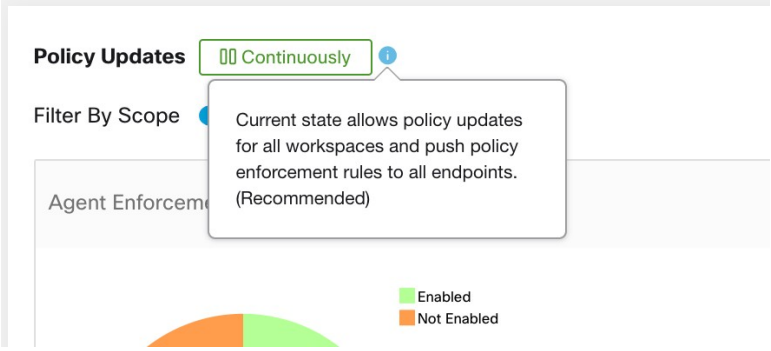


Figure 75: Les mises à jour des règles de pare-feu sont suspendues

Historique de la mise en application

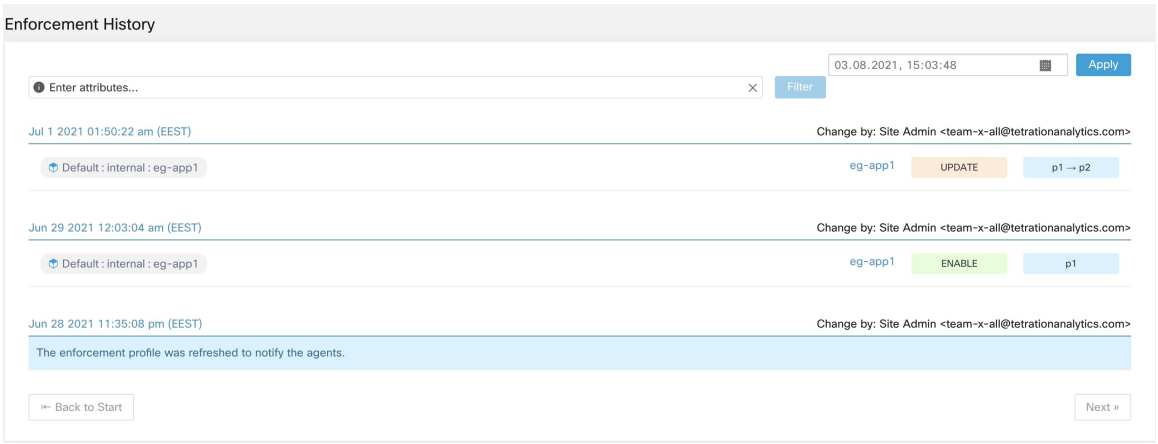
L'historique de mise en application fournit une liste des modifications apportées à la liste des espaces de travail qui ont fait l'objet de l'application de politiques et à leur version.

Pour afficher l'historique de mis en application :

1. Cliquez sur le signe d'insertion sur le côté droit de la page de segmentation pour développer le menu Tools (Outils).
2. Cliquez sur **Enforcement History** (Historique de mise en application).

   Chaque section décrit un événement et affiche un résumé de ce qui a changé.
3. Cliquez sur un événement pour obtenir des renseignements détaillés sur toutes les politiques qui ont été appliquées à ce moment-là.

Figure 76: Affichage de l'historique de mise en application

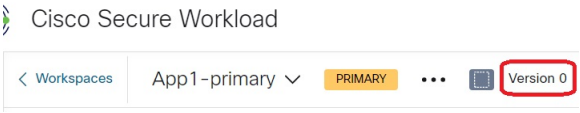


À propos des versions des politiques (v* et p*)

Les versions de politiques sont parfois appelées versions d'espace de travail.

Version affichée

La version des politiques (et des grappes) avec lesquelles vous travaillez actuellement est affichée en haut de la page de l'espace de travail :



- Les versions V* sont générées par la découverte automatique des politiques

  Pour de plus amples renseignements, voir ci-dessous
- Les versions P* sont des versions analysées et/ou appliquées.

  Pour de plus amples renseignements, voir ci-dessous

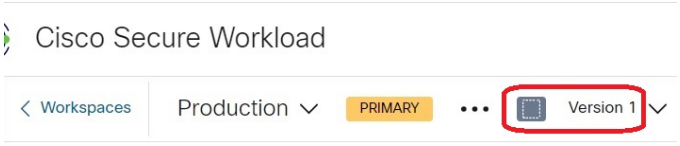
Les icônes suivantes peuvent s'afficher à côté du numéro de version :

Tableau 6 : Icônes de version

	Indique la version des politiques qui est actuellement en cours d'analyse
	Indique la version des politiques actuellement appliquées
	Indique la dernière version des politiques découvertes automatiquement
(sans icône)	Indique que la version n'est pas la dernière version de son type

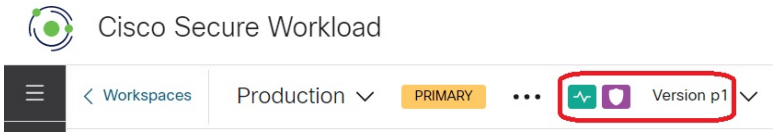
Exemples :

- La version affichée est la dernière version découverte des politiques :



- La version affichée est la version des politiques qui est actuellement en cours d'analyse :

- La version affichée est la version des politiques actuellement en cours d'analyse et d'application :



Version de découverte des politiques (v*)

Chaque fois que vous découvrez automatiquement les politiques pour un espace de travail, la version (v*) est incrémentée.

La première fois que vous découvrez automatiquement les politiques, la version 1 est générée, et toutes les modifications ultérieures à cette exécution, telles que la modification ou l'approbation des grappes (à l'exception d'une réexécution), sont également regroupées sous la version 1. Lorsque vous découvrez ensuite automatiquement les politiques, une nouvelle version est générée (sauf si la découverte échoue).

La version v* est également incrémentée si vous importez des politiques.

Pour utiliser les versions v*, consultez Afficher, comparer et gérer les versions de politiques découvertes, à la page 55.

Version publiée de la politique (p*)

Le terme version de politique « publiée » (p*) pour un espace de travail peut faire référence à :

- La version des politiques qui a été analysée, ou
- La version des politiques qui a été appliquée

Il s'agit de deux versions distinctes mais parallèles qui dépendent du contexte :

- Version de la politique pour l'analyse :

  Chaque fois que vous analysez des politiques dans un espace de travail ou que vous cliquez sur **Analyser les dernières politiques** après avoir apporté une modification, le système prend un instantané de toutes les grappes et toutes les politiques définies dans cet espace de travail, et du numéro de version de politique « publiée » (p*) pour les incréments d'analyse. La dernière version **de l'analyse des politiques en direct** est affichée dans le coin supérieur gauche de la page sur l'onglet Policy Analysis (analyse des politiques) de l'espace de travail principal.

- Version de la politique pour application :

  Chaque fois que vous activez l'application des politiques dans un espace de travail, ou réactivez l'application après avoir apporté des modifications, la version « publiée » des politiques (p*) pour l'application devient le numéro dans la version analysée que vous choisissez dans l'assistant d'application. Ainsi, si vous appliquez la version analysée 5, la version appliquée est également la version 5, même s'il s'agit, par exemple, de la première application de la politique pour l'espace de travail. La **version actuelle de la politique appliquée** est affichée dans le coin supérieur gauche de la page sous l'onglet Enforcement (Application) de l'espace de travail principal.

Gestion des versions publiées (p*)

Les versions de politique publiées ne peuvent pas être modifiées, seulement entièrement supprimées.

Remarque Les versions de politique publiées (p*) sont limitées à 100 au total. Une fois cette limite atteinte, vous devez supprimer des anciennes versions.

Pour gérer et supprimer les versions p*, consultez Afficher, comparer et gérer les versions des politiques analysées, à la page 128ou Afficher, comparer et gérer les versions des politiques appliquées, à la page 143.

Vous pouvez également utiliser l'API pour supprimer des versions publiées.

Comparaison des versions des politiques : différence de politique

Pour comparer les politiques, consultez l'une des rubriques suivantes : Afficher, comparer et gérer les versions de politiques découvertes, on page 55, Afficher, comparer et gérer les versions des politiques analysées, on page 128ou Afficher, comparer et gérer les versions des politiques appliquées, on page 143

Les modifications de politique seront affichées dans trois catégories : Absolute (Absolu), Default (Par défaut) and Catch All (Collectrice). Dans le tableau de comparaison :

- Les différents services appartenant à la même politique sont regroupés
- Filtrer les modifications de politique par facette ou par type de différence
- Les modifications de politique et les services sont paginés

- Télécharger les modifications de politique filtrées au format CSV

Table 7: Propriétés du filtre à facette

Propriété	Description
Priority	Par ex.100
Action	Par ex., ALLOW (AUTORISER), DENY (REFUSER)
Consumer	P. ex. Grappe de consommateurs
Provider	P. ex. Grappe de fournisseurs
Port	Par ex. 80
Protocol	Par ex. TCP

Table 8: Colonnes de sortie CSV

Colonne	Description
Rank	La catégorie de la politique. p. ex., ABSOLUTE (ABSOLUE), DEFAULT (PAR DÉFAUT), CATCH_ALL (COLLECTRICE)
Diff	Le type de différence de la modification. P. ex., ADDED (AJOUTÉ), REMOVED (RETIRÉ), UNCHANGED (NON MODIFIÉ)
Priority	Par ex.100
Action	Par ex., ALLOW (AUTORISER), DENY (REFUSER)
Consumer Name	Le nom de la grappe de consommateurs.
Consumer ID	ID de la grappe de consommateurs.
Provider Name	Nom de la grappe de fournisseurs.
Provider ID	ID de la grappe de fournisseurs.
Protocol	Par ex. TCP
Port	Par ex. 80

Dans la figure ci-dessous, les versions de politique p1 et v1 sont comparées.

Figure 77: Vue des différences des politiques

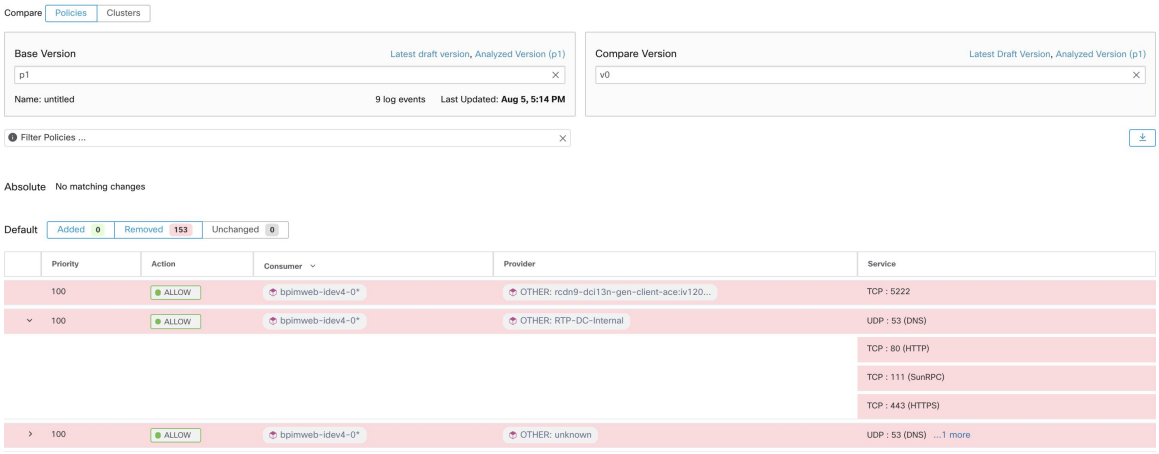


Figure 78: Bouton de téléchargement de l'affichage des différences des politiques

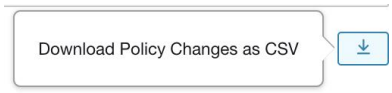


Figure 79: Filtrage de la vue des différences entre les politiques

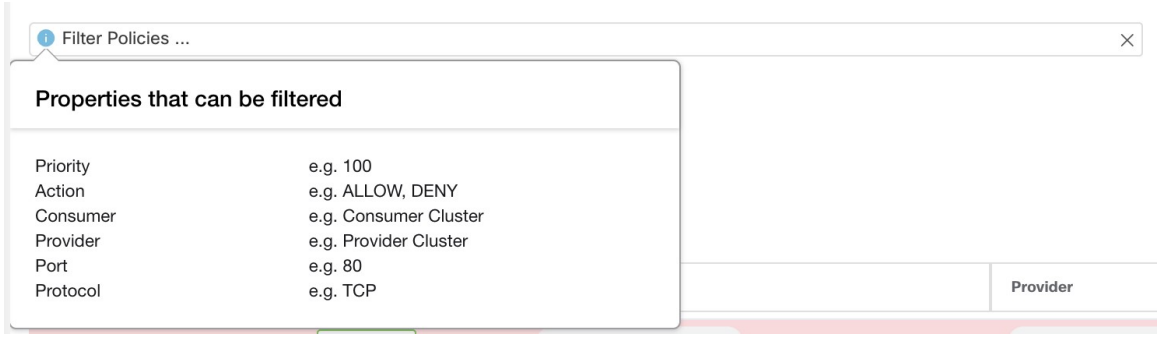


Figure 80: Filtre de type de différence de l'affichage des différences entre les politiques

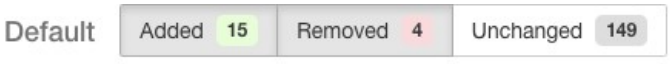


Figure 81: Regroupement des vues des différence entre les politiques

Figure 82: Sortie CSV de l'affichage de la différence entre les politiques

Rank	Diff	Priority	Action	Consumer Name	Consumer ID	Provider Name	Provider ID	Protocol	Port
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: rcdn9-dci13n-gen-client-ace:iv120	610bcda7a51e713db909d9f1	TCP	5222
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	UDP	53
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	80
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	111
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	443
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: unknown	610bcda7a51e713db909da45	UDP	53
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: unknown	610bcda7a51e713db909da45	TCP	443
DEFAULT	ADDED	100	ALLOW	bpimweb-idev3-0*	610bcda7a51e713db909da26	OTHER: rcdn9-dci13n-gen-client-ace:iv120	610bcda7a51e713db909d9f1	TCP	5222

Tip Consultez aussi Comparaison des versions des grappes générées : vues des différences, on page 83.

Journaux d'activités et historique des versions

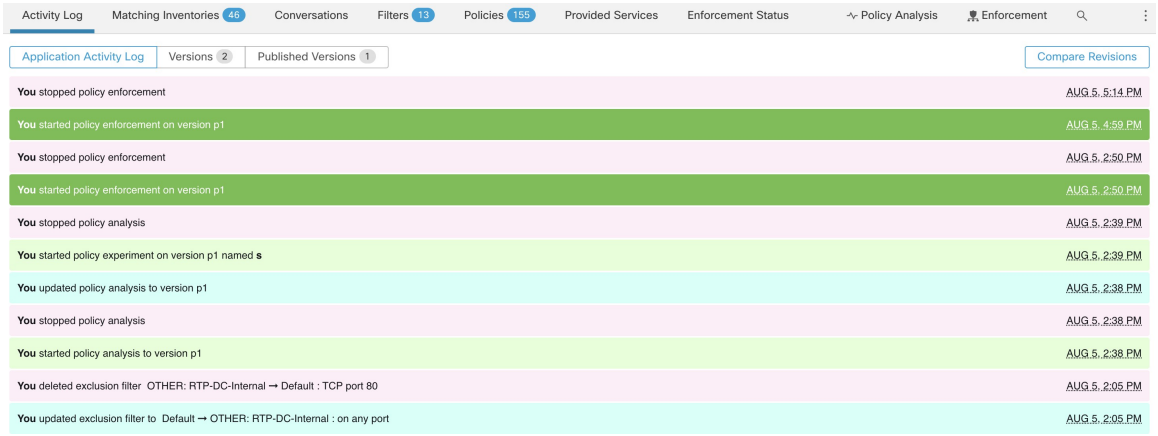
Les journaux d'activités enregistrent l'historique des modifications que vous avez appliquées à un espace de travail. Les événements affichés comprennent l'ajout, la suppression et le changement de nom de charges de travail et de grappes, le déplacement de charges de travail entre les grappes, le chargement de renseignements secondaires, la soumission et l'abandon de la découverte automatique des politiques, etc. La vue montre quel utilisateur a effectué chaque modification.

Pour afficher l'historique des modifications pour un espace de travail, cliquez sur n'importe quel lien du **journal des activités** dans l'espace de travail.

Par exemple :

1. Cliquez sur **Defend (défendre) > Segmentation (segmentation).**
2. Cliquez sur la portée et l'espace de travail appropriés.
3. Cliquez sur le lien **View Activity Log** (Afficher les journaux d'activité).
4. Cliquez sur l'onglet **Workspace Activity Log** (Journal d'activité de l'espace de travail).

Figure 83: Journal des événements applicables à la version v1 de cet espace de travail



Pour en savoir plus sur les onglets et les options de la page relatifs à la version, consultez :

- À propos des versions des politiques (v* et p*), on page 147
- Afficher, comparer et gérer les versions de politiques découvertes, on page 55
- Afficher, comparer et gérer les versions des politiques analysées, on page 128
- Afficher, comparer et gérer les versions des politiques appliquées, on page 143

Suppression automatique des anciennes versions des politiques

Chaque semaine, les éléments suivants sont automatiquement supprimés : les versions d'espace de travail qui n'ont pas été consultées depuis six mois et les politiques de test auxquelles il n'a pas été accédé au cours des 30 derniers jours.

Conversations

Une conversation est définie comme un service fourni par un hôte sur un port particulier et utilisé par un autre hôte. Une telle conversation se matérialise à partir de nombreux flux sur des instants différents. La découverte automatique de politiques prend tous ces flux, ignore les ports éphémères/clients et les dédouble pour générer le graphe de conversation. Pour toute conversation donnée entre l'hôte A et l'hôte B sur le port N du serveur (fournisseur), il y a eu au moins une observation de flux de A à B sur le port N au cours de la période pour laquelle la découverte automatique des politiques a été effectuée.

Utilisez les données de flux pour mieux comprendre quels flux sont associés à quel processus tout en évaluant les grappes générées lors de la découverte automatique des politiques.

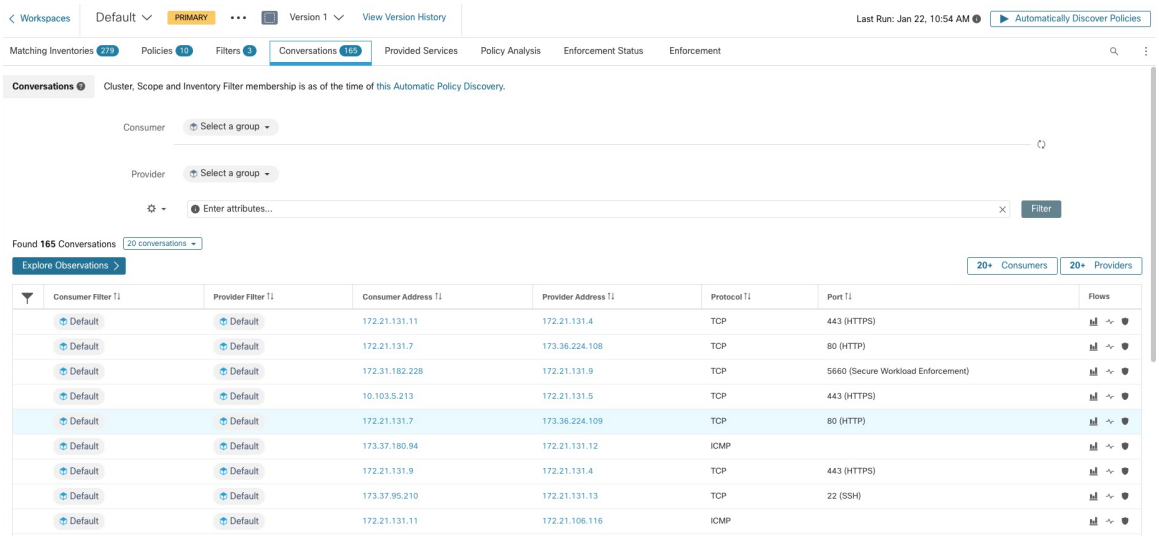
En outre, les informations collectées par les agents offrent une visibilité sur les ports L4 inutilisés. Les ports inutilisés sont ceux pour lesquels aucune communication n'a été constatée pendant l'intervalle sélectionné pour la découverte automatique des politiques. Ces informations peuvent être utilisées pour ouvrir des politiques de communication sur ces ports OU pour fermer les applications se rapportant aux ports inutilisés, réduisant ainsi la surface d'attaque de la charge de travail.

Notez que la classification client-serveur affecte la vue de la conversation de découverte automatique des politiques – elle détermine quel port doit être abandonné (jugé éphémère) dans l'agrégation : consultez Classification client-serveur.

Vue du tableau Conversations

La vue du tableau Conversations offre un moyen simple de visualiser les flux agrégés à partir de la durée de la découverte automatique des politiques, lorsque le port consommateur est supprimé et qu'il n'y a qu'un seul enregistrement pour toute la durée de la recherche. Alors que les politiques vont d'un filtre à l'autre, les conversations vont d'une adresse IP à l'autre.

Figure 84: Vue du tableau Conversations

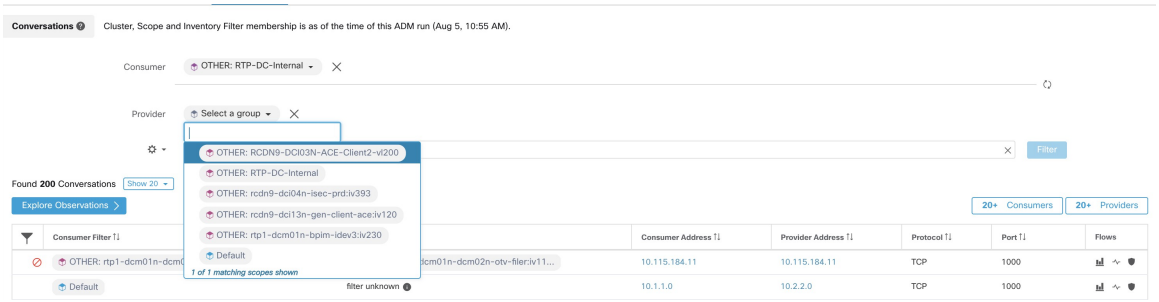


Choix du consommateur ou du fournisseur

Les consommateurs et les fournisseurs peuvent être sélectionnés à l'aide d'un sélecteur déroulant à présélection qui permet de choisir les filtres d'inventaire, les portées et les grappes, comme le montre l'exemple ci-dessous. Toutes les conversations entre le consommateur et le fournisseur choisis sont affichées. Remarque : pour supprimer un filtre existant, cliquez sur l'icône « x » (l'effacement du filtre peut ne pas fonctionner).

Par défaut, le consommateur et le fournisseur correspondent à tous les filtres d'inventaire dont une adresse IP est membre lors de la découverte automatique des politiques. Par exemple, la recherche de la « portée racine » correspondra à toutes les conversations, même si certaines adresses IP pourraient mieux correspondre à des portées plus spécifiques. Pour effectuer une correspondance plus précise, sélectionnez « Restrict scope filtering to an IP's best match (Restreindre le filtrage à l'utilisation d'une adresse IP) » dans la liste déroulante des paramètres à gauche de l'entrée du filtre à aspects.

Figure 85: Choix du consommateur ou du fournisseur



Filtres de conversations

Figure 86: Filtres de conversations

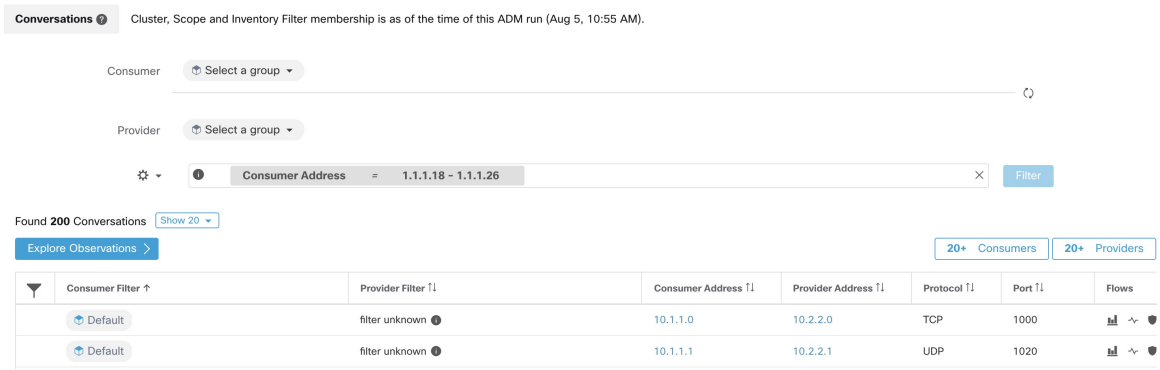
C’est ici que vous définissez les filtres pour affiner les résultats de la recherche. On peut consulter toutes les dimensions possibles en cliquant sur l’icône (?) à côté du mot Filters (Filtres). Pour toutes les données d’étiquettes d’utilisateur, ces colonnes sont également disponibles pour les intervalles appropriés. Cette entrée prend également en charge les mots-clés and, or, not et parenthesis, utilisez-les pour concevoir des filtres plus complexes. Par exemple, un filtre indépendant de la direction entre IP 1.1.1.1 et 2.2.2.2 peut s’écrire :

Adresse du consommateur = 1.1.1.1 et adresse du fournisseur = 2.2.2.2 ou Adresse du consommateur = 2.2.2.2 et adresse du fournisseur = 1.1.1.1. Pour filtrer également sur Protocole = TCP :

(Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1) and Protocol = TCP

L’entrée du filtre prend également en charge les « , » et « - » pour le port, l’adresse du client et l’adresse du fournisseur, en transformant « - » en requêtes de plages. Voici des exemples de filtres valables :

Figure 87: L’entrée du filtre prend en charge la requête de plage pour l’adresse du consommateur



Filtres disponibles :

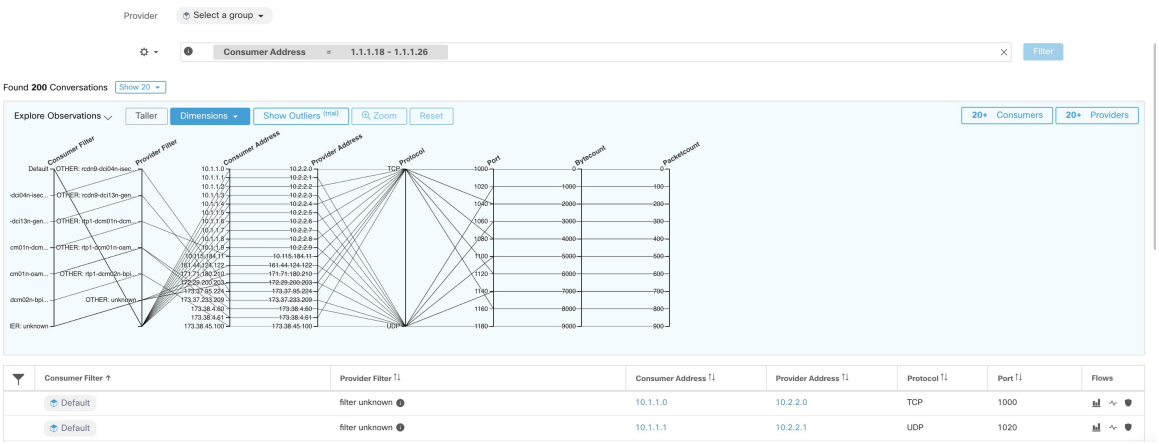
Filtres	Description
Adresse du client	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux observations de flux de conversation dont l’adresse du consommateur chevauche l’adresse IP ou le sous-réseau fourni.
Adresse du fournisseur	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux observations de flux de conversation dont l’adresse du fournisseur chevauche l’adresse IP ou le sous-réseau fourni.
Port	Correspond aux observations de flux de conversation dont le port chevauche le port fourni.
Protocol	Filtrez les observations de flux de conversation par type de protocole (TCP, UDP, ICMP).
Address Type (Type d'adresse)	Filtrez les observations de flux de conversation par type d’adresse (IPv4, IPv6, DHCPv4).

Filtres	Description
Confiance	A indiqué la confiance dans le sens du flux. Valeurs possibles : élevée, très élevée, modérée.
Exclu?	Mettre en correspondance les conversations qui sont exclues par un filtre d'exclusion ou une politique approuvée.
Exclu par	Mettre en correspondance les conversations exclues par un filtre spécifique. Les valeurs possibles : filtre d'exclusion, politique.

Explorer les observations

Cliquer sur le bouton « Explorer les observations » pour activer un affichage graphique qui permet une exploration rapide des données comportant de nombreuses dimensions à l'aide d'un graphique en « coordonnées parallèles ». Un peu impressionnant au premier abord, ce tableau peut être utile pour activer uniquement les dimensions qui vous intéressent (en décochant les éléments du menu déroulant Dimensions) et pour réorganiser l'ordre des dimensions. Une seule ligne dans ce graphique représente une seule observation et l'intersection de cette ligne avec les différents axes indique la valeur de cette observation pour cette dimension. Cela devient plus clair lorsque l'on passe le curseur sur la liste des observations sous le graphique pour voir la ligne en surbrillance représentant l'observation dans le graphique :

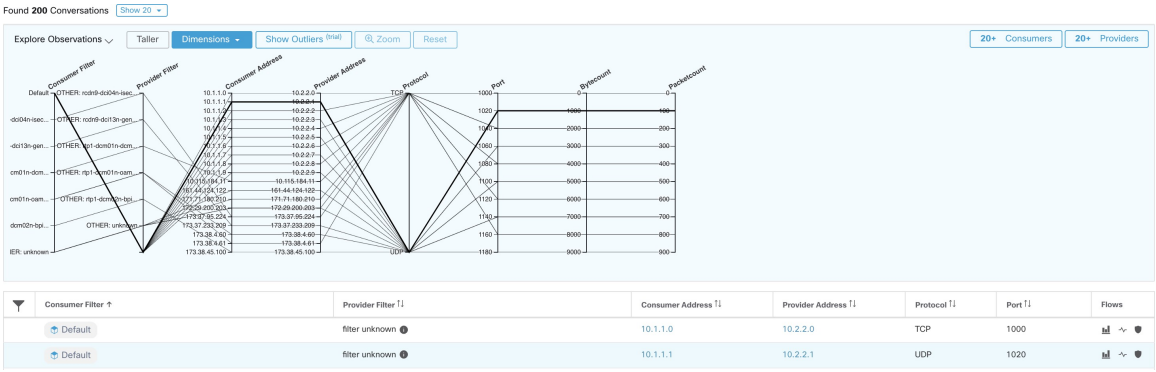
Figure 88: Explorer les observations



Observation de conversation survolée

En raison de la nature pluridimensionnelle des données des conversations, ce graphique est large par défaut et nécessite un défilement vers la droite pour le visualiser dans son intégralité. C'est pourquoi il est utile de désactiver toutes les dimensions sauf celles qui vous intéressent. La fonction de survol dans Explorer les conversations permet de mettre en correspondance (au survol) chaque conversation avec la vue de liste du tableau.

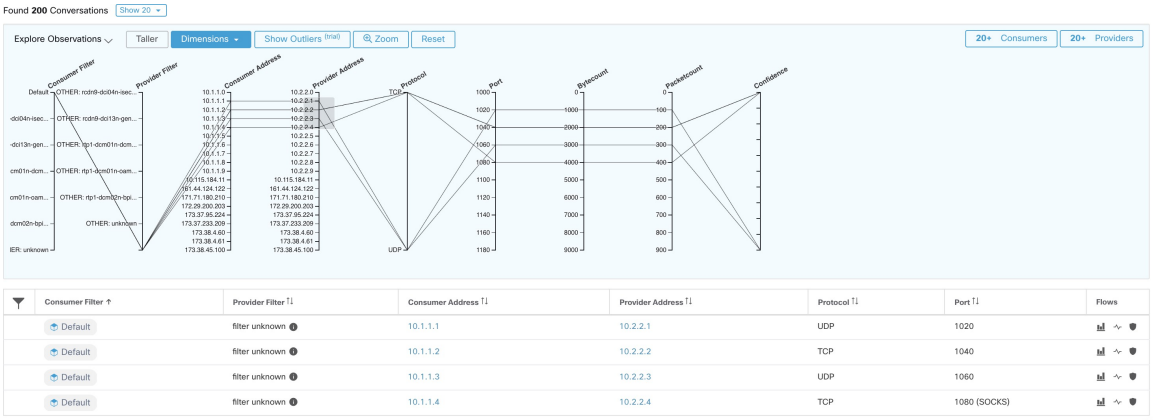
Figure 89: Observation de conversation survolée



Filtrage

Faire glisser le curseur le long de l'un des axes crée une sélection qui affichera uniquement les observations correspondant à cette sélection. Cliquez à nouveau sur l'axe pour supprimer la sélection à tout moment. Des sélections peuvent être effectuées sur n'importe quel nombre d'axes à la fois. La liste des observations sera mise à jour pour afficher uniquement les conversations sélectionnées.

Figure 90: Filtrage

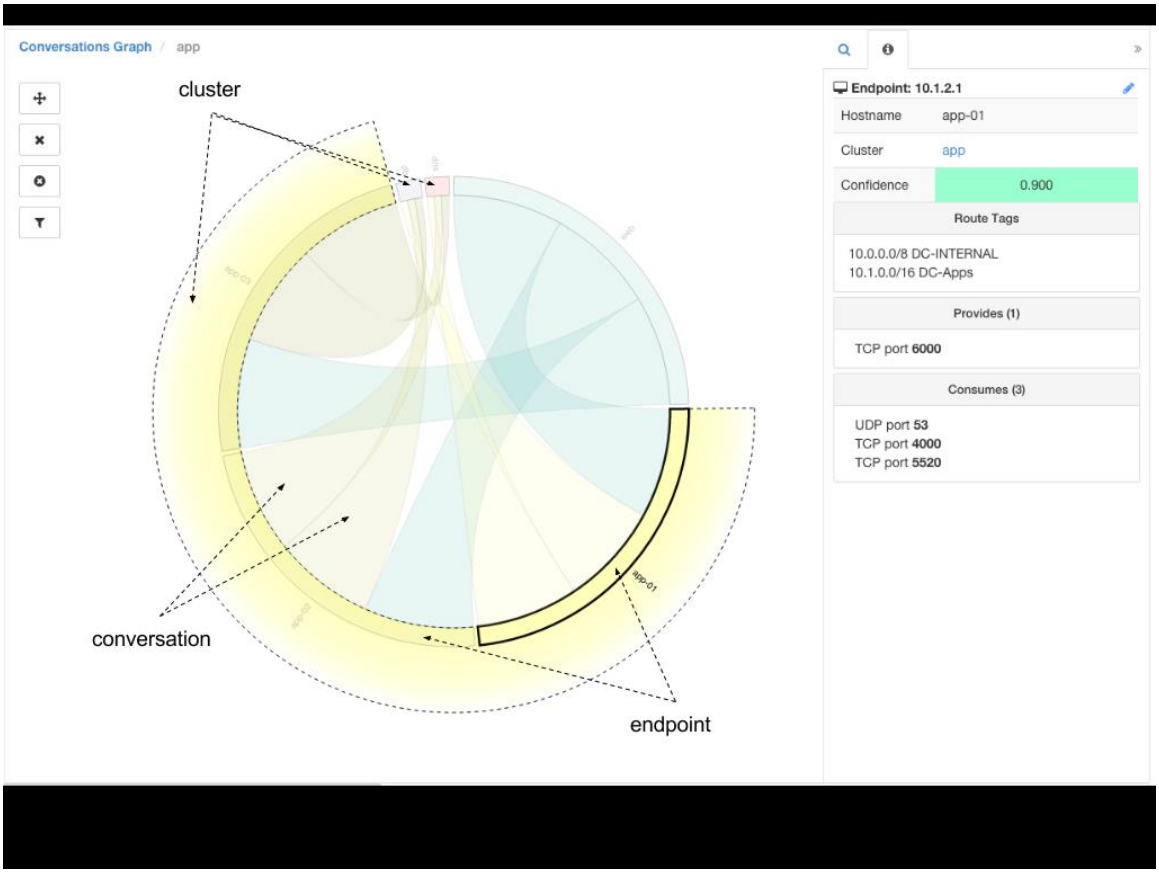


Vue graphique des conversations

La présentation du tableau des conversations est similaire à la page d'affichage des politiques, sauf qu'au lieu de se concentrer sur les partitions, grappes et politiques, elle se concentre sur les grappes/charges de travail/conversations. Comme l'illustre la figure ci-dessous, les arcs externes au niveau supérieur représentent des grappes et peuvent être développés pour afficher les hôtes membres/charges de travail comme des arcs internes. Les accords représentent les conversations ou les connexions.

Les commandes et le panneau latéral de la vue de conversation se comportent de la même manière que la vue de la politique, à l'exception du fait que les informations du panneau latéral affichent également des informations détaillées sur les charges de travail sélectionnées, telles que les services consommés/fournis, ainsi qu'un lien vers la grappe parente et des informations sur le processus, le cas échéant.

Figure 91: Vue graphique des conversations



Principaux consommateurs et fournisseurs de conversations

Le nombre de principaux consommateurs ou fournisseurs en fonction du nombre total de conversations reflétant les filtres choisis peut être consulté à partir de deux boutons en haut du tableau Conversations. Cliquez sur chacun d'eux pour voir une boîte de dialogue contenant un tableau avec la colonne Nombre de conversations ainsi que l'adresse, le nom d'hôte et d'autres colonnes annotées par l'utilisateur de chaque client ou fournisseur.

Figure 92: Au-dessus du tableau Conversations

Figure 93: Boîte de dialogue modale des principaux consommateurs

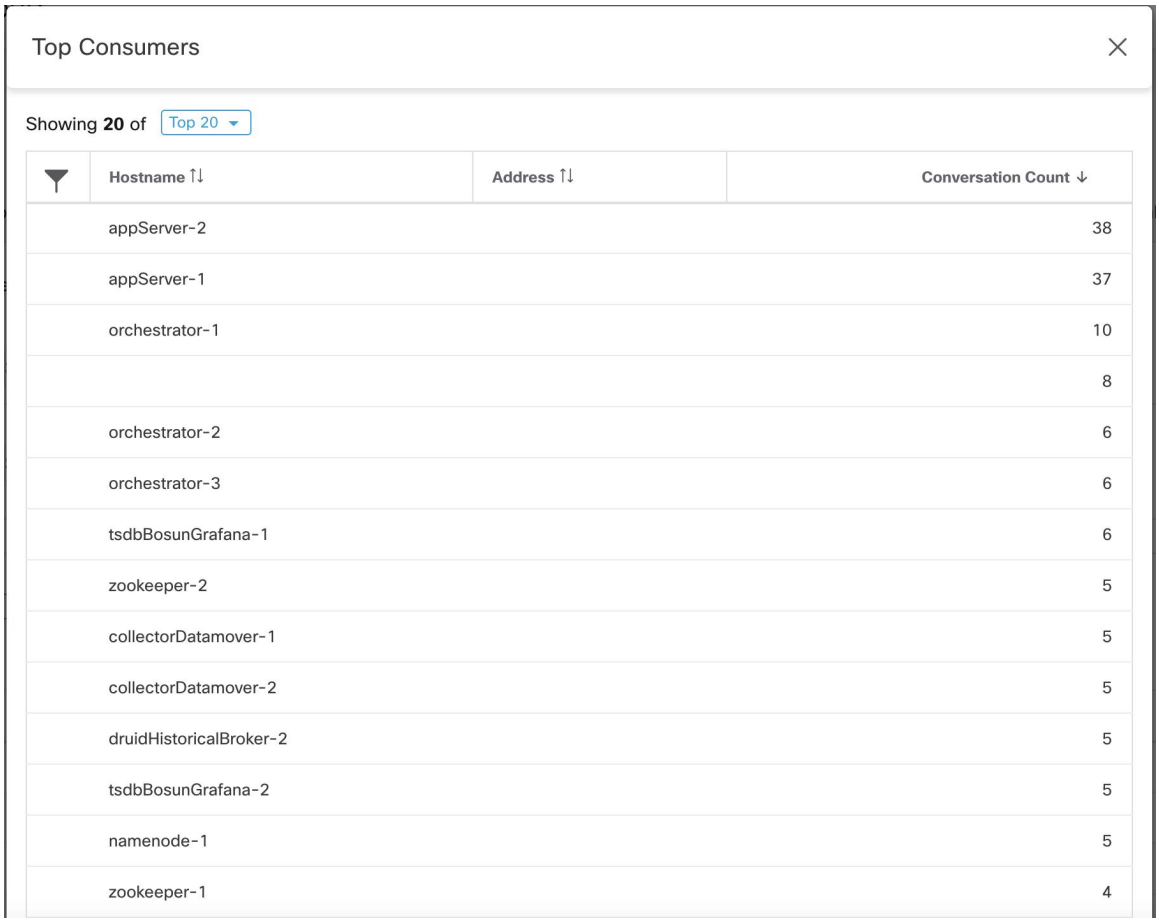
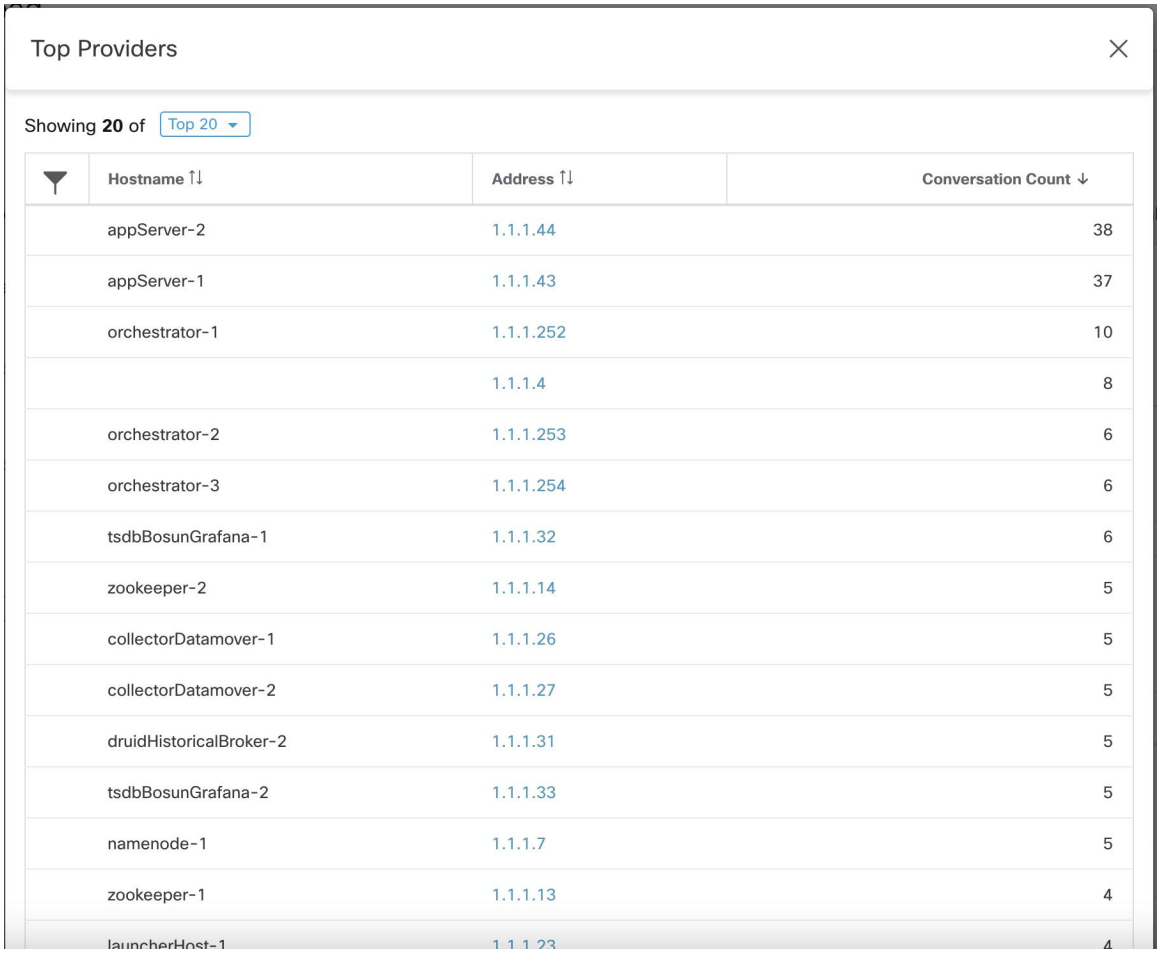


Figure 94: Boîte de dialogue modale des principaux fournisseurs



Configuration automatisée de l'équilibreur de charge pour la découverte automatique des politiques (F5 uniquement)

Important **Il s'agit d'une fonctionnalité expérimentale.**

Cette fonctionnalité et ses API sont dans la **configuration ALPHA** et sont susceptibles de changer et d'être améliorées dans les versions futures.

La découverte automatique des politiques génère ces dernières à partir de la configuration des équilibreurs de charge connectés à un orchestrateur externe. La génération de politiques à partir de la configuration réduit la dépendance à l'égard des données de flux et améliore la précision des grappes découvertes et des politiques.

Elle compte sur les clients pour transmettre les flux à l'équilibreur de charge pour générer des politiques autorisant ce trafic.

Terminologie

VIP (Adresse IP virtuelle) : adresse IP à laquelle le client envoie le trafic destiné à un service.

SNIP SNAT IP : adresse IP utilisée par l'équilibreur de charge pour envoyer le trafic aux hôtes principaux (Backend).

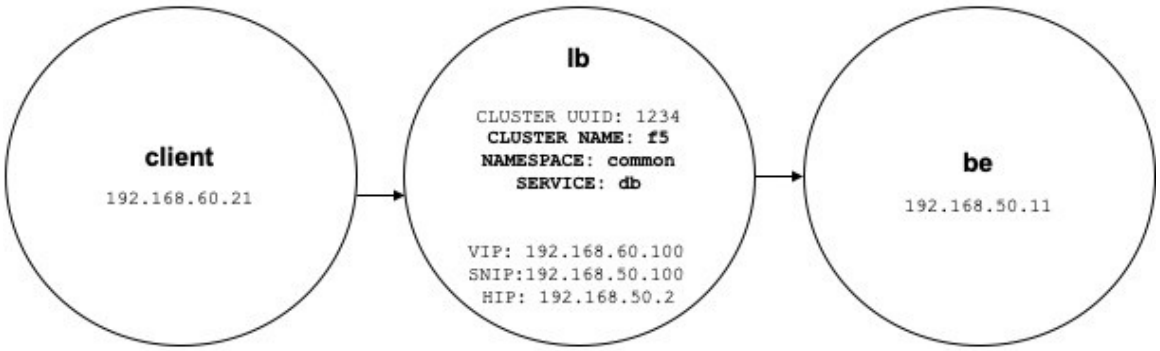
Point de terminaison Backend (principal) **BE** : adresse IP de l'hôte principal.

HIP IP de vérification de l'intégrité : adresse IP source utilisée par l'équilibreur de charge pour envoyer le trafic de vérification de l'intégrité aux hôtes principaux.

Note Les HIP sont les mêmes que les SNIP en mode automap. Cependant, les HIP et les SNIP peuvent différer lorsqu'un regroupement SNAT est configuré.

Déploiement

Figure 95: Déploiement



Envisagez le déploiement suivant dans lequel les VIP, les SNIP et les HIP de l'équilibreur de charge font partie de la portée *lb* et les BE font partie de la portée *be* . Les portées sont créées comme suit.

- Client

  La portée du client comprend les clients communiquant avec l'équilibreur de charge. Pour l'exemple ci-dessus, la requête de portée *client* est la suivante :

  ```
  address eq 192.168.60.21 or address eq 192.168.60.22
  ```

- lb

  L'orchestrateur externe F5 étiquette les VIP, les SNIP, les HIP et les BE utilisés par l'équilibreur de charge. Ces étiquettes peuvent être utilisées pour créer des requêtes de portée, où *orchestrator_system/service_name* est utilisé pour sélectionner les VIP, *orchestrator_system/service_startpoint* les SNIP, et *orchestrator_system/service_healthcheck_startpoint* des HIP pour le service. Pour l'exemple ci-dessus, une requête de portée qui inclut les VIP, les SNIP et les HIP pour la *base de données* de service est la suivante :

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  (user_orchestrator_system/service_name eq db or
  ```

```
user_orchestrator_system/service_startpoint eq db or
user_orchestrator_system/service_healthcheck_startpoint eq db)
```

Note Les SNIP et les VIP doivent se trouver dans la même portée.

- Être

  user_orchestrator_system/service_endpoint sélectionne les environnements de base (BE) pour un service. Pour l'exemple ci-dessus, une requête de portée qui inclut des éléments BE pour la *base de données de service* est la suivante :

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_endpoint eq db
  ```

Grappes

Chaque service génère jusqu'à quatre grappes découvertes, dont seule la grappe de service est visible pour l'utilisateur. Les grappes SNIP, HIP et BE apparaissent comme des grappes connexes pour la grappe de service. Les grappes HIP et BE sont générées uniquement lorsque des HIP et des BE sont présents dans la portée *lb*.

Pour l'exemple ci-dessus, la découverte automatique des politiques génère une grappe SNIP et une grappe HIP dans la portée *lb* qui incluent les SNIP et les HIP pour le service. Étant donné que les environnements BE se trouvent en dehors de la portée *lb* , la découverte automatique des politiques ne génère pas de grappe principale, mais ajoute la portée *be* à la liste des grappes associées à *db*.

Les grappes sont générées comme suit :

- Service

  La grappe de service comprend des VIP pour le service. La requête pour la grappe de services est la suivante :

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/namespace eq common and
  user_orchestrator_system/service_name eq db
  ```

- SNIP

  Les SNIP pour un service sont inclus dans la grappe SNIP. La requête pour la grappe SNIP est la suivante :

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_startpoint eq db
  ```

- HIP

  Les HIP d'un service sont inclus dans la grappe HIP. La requête pour la grappe HIP est la suivante :

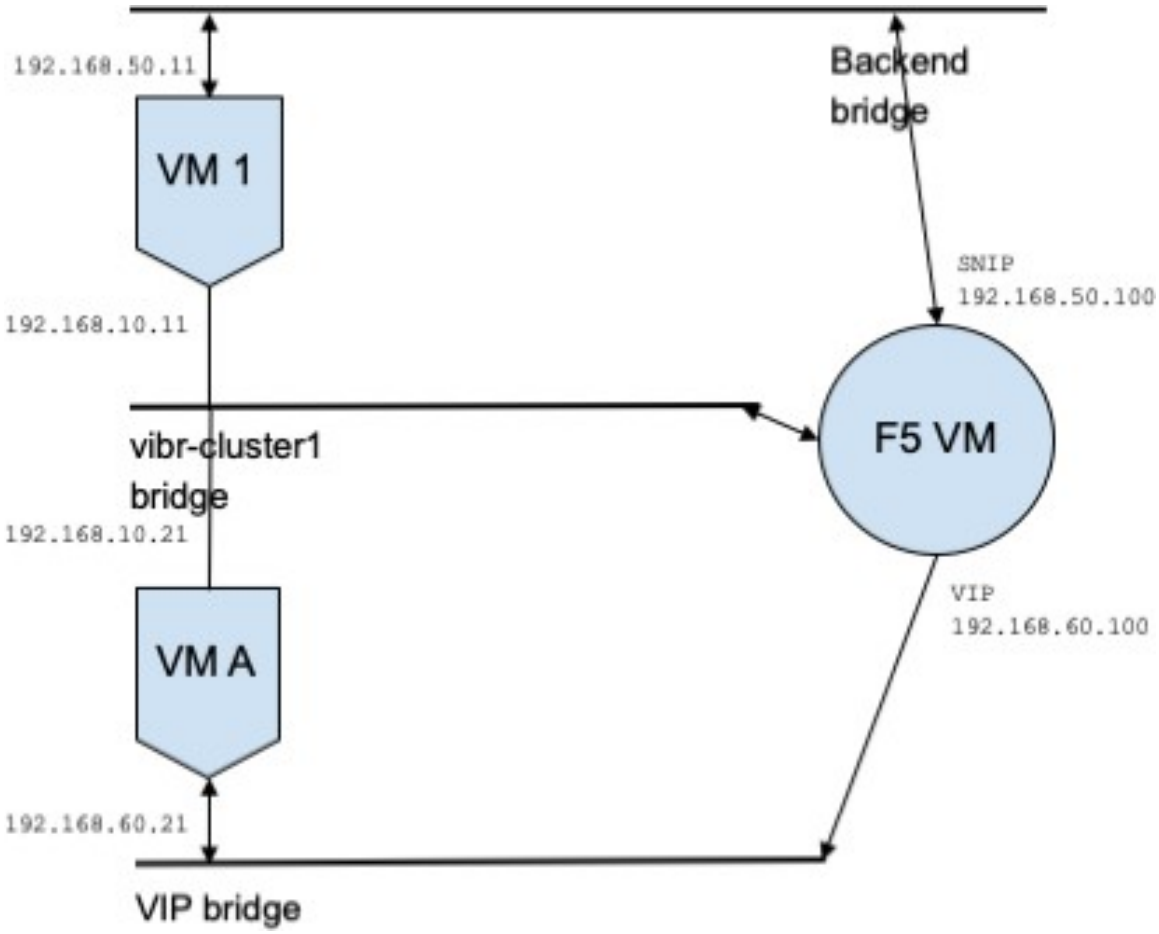
  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_healthcheck_startpoint eq db
  ```

- Backend (Système principal)

  Une grappe principale du service est générée lorsqu'un ou plusieurs BE font partie de la portée *lb*. Cela ne s'applique pas à l'exemple ci-dessus, ce qui signifie qu'aucune grappe principale n'est générée dans la portée *lb*.

Politiques

Figure 96: Génération de politiques



Supposons que nous ayons une *base de données* de service avec VIP *192.168.60.100*, SNIP *192.168.50.100* et une machine virtuelle principale avec l'adresse IP *192.168.50.11* à l'écoute sur le port 10000. Le trafic de la VM cliente *192.168.60.21* vers la *base de données* entraîne les politiques suivantes :

- Politique du client à la VIP.

  La politique suivante permet à la machine virtuelle cliente d'accéder au service *db*.

```
{
"src": "<uuid of client scope>",
"dst": "<uuid of service cluster>",
"l4_params": [
{
"port": [
10000,
10000
],
"proto": 6,
}
]
}
```

- Politique de SNIP à BE.

  Une politique autorisant le trafic de SNIP vers BE est générée automatiquement à partir de la configuration et apparaît comme politique associée pour *db*.

```
{
"src": "<uuid of SNIP cluster>",
"dst": "<uuid of be scope>",
"l4_params": [
{
"port": [
10000,
10000
],
"proto": 6,
}
]
```

  Un connecteur de politique de la portée *lb* vers la portée *be* transmet la politique suivante vers celle-ci.

Consommateur	Fournisseur	Port	Protocole	Action
SNIP	à	10 000	TCP	Autoriser

  Cela génère des règles de pare-feu sur l'hôte BE 192.168.50.11, autorisant le trafic entrant de LB SNIP 192.168.50.100 sur le port 10000.

- Politiques de HIP à BE.

  Une politique autorisant le trafic du HIP vers BE est générée automatiquement à partir de la configuration et apparaît comme politique associée pour *db*.

```
{
"src": "<uuid of HIP cluster>",
"dst": "<uuid of be scope>",
"l4_params": [
{
"port": [
0,
0
],
"proto": ICMP,
}
]
}
```

  Un connecteur de politique de la portée *lb* vers la portée *be* transmet la politique suivante vers celle-ci.

Consommateur	Fournisseur	Port	Protocole	Action
HIP	à	0	ICMP	Autoriser

  Cela génère des règles de pare-feu sur l'hôte BE *192.168.50.11* , autorisant le trafic ICMP entrant de LB HIP *192.168.50.2*.

Mises en garde

- Lorsque plusieurs services de la même instance d'équilibreur de charge portent le même nom, les règles principales générées pour ces services comprendront les pools de serveurs principaux, c.-à-d. les règles seront plus permissives que nécessaire.

Serveur de publication des politiques

Le serveur de publication des politiques est une fonctionnalité Cisco Cisco Secure Workload avancée qui permet à un fournisseur tiers de mettre en œuvre ses propres algorithmes de mise en application, qui sont optimisés pour les appareils réseau tels que les équilibreurs de charge ou les pare-feu. Cette fonctionnalité est réalisée en publiant les politiques définies sur une instance Kafka résidant dans la grappe Cisco Secure Workload et en fournissant aux clients des certificats client Kafka, ce qui permet au code du fournisseur tiers de récupérer les politiques Kafka et de les traduire correctement dans la configuration de leurs appareils réseau.

Cette section vise à décrire la procédure que les fournisseurs tiers, en abrégé les utilisateurs dans ce qui suit, doivent suivre pour exploiter la fonctionnalité de *serveur de publication des politiques* avec Java sur Linux.

Prérequis

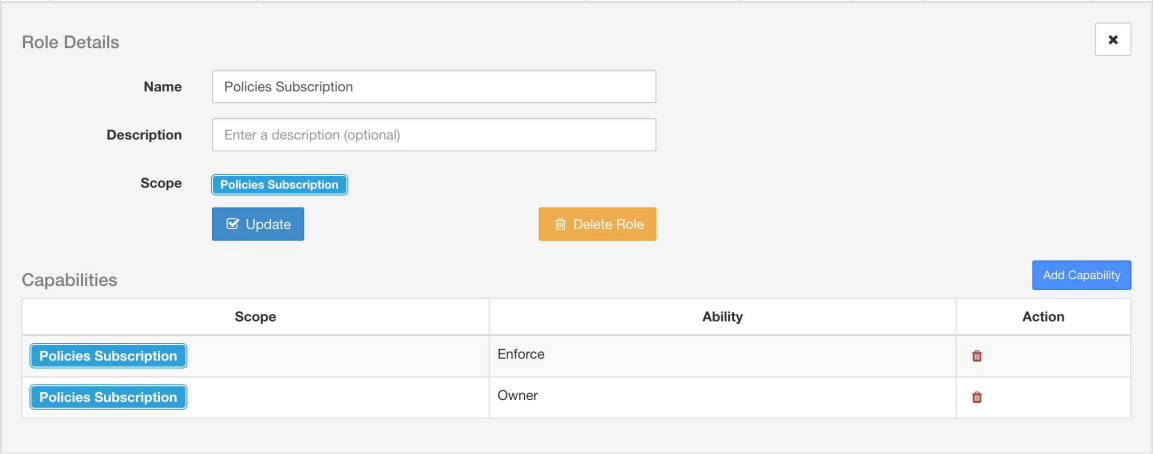
Les progiciels suivants sont installés sur un système Linux, tel qu'Ubuntu 16.04.

- JDK Java 8
- Clients Apache Kafka : kafka-clients-1.0.0.jar
- Tampons du protocole, base : protobuf-java-3.4.1.jar
- Apache Log4j : log4j-1.2.17.jar
- Façade de journalisation simple pour Java : sLF4j-api-1.7.25.jar, sLF4j-log4j12-1.7.25.jar
- Compresseur/décompresseur Snappy pour Java : Snappy-java-1.1.4.jar

Obtention des certificats client Kafka

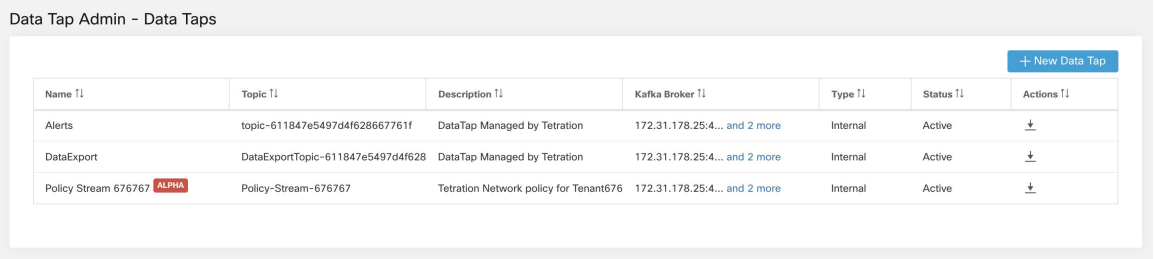
- Créez un rôle d'utilisateur avec la capacité « *Propriétaire* » et attribuez-le au compte d'utilisateur de votre choix :

Figure 97: Configuration des rôles d'utilisateurs pour recevoir les politiques Kafka



- Effectuez l'application des politiques comme décrit dans la section Appliquer des politiques. Cette première étape est nécessaire, car elle crée une rubrique Kafka associée à une portée active.
- Accédez à **Manage(Gestion) > Data Tap Admin (Administration des surveilleurs de données)**
- Sélectionnez l'onglet *« Data Taps »* (Dérivations de données) et téléchargez les certificats clients Kafka en cliquant sur le bouton de téléchargement sous la colonne *« Actions »*. Assurez-vous de sélectionner le format *Java Keystore* dans la boîte de dialogue de téléchargement.

Figure 98: Affichage des dérivations de données



- Le fichier de certificats clients téléchargé porte généralement un nom comme *Policy-Stream-10-Policies-Subscription.jks.tar.gz*. Créez un répertoire et décompressez-le sous ce dernier, comme indiqué ci-dessous :

```
    mkdir Policy-Stream-10-Policies-Subscription
    tar -C Policy-Stream-10-Policies-Subscription -zxf
Policy-Stream-10-Policies-Subscription.jks.tar.gz
```

Fichier de définition Protobuf

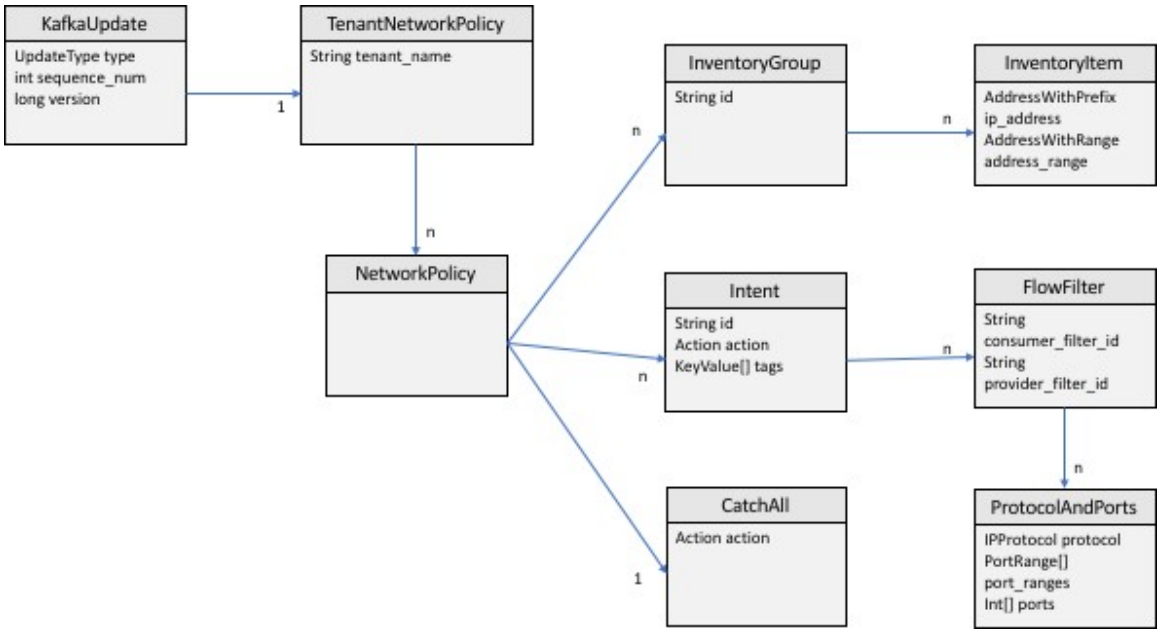
Les politiques de réseau exposées par le serveur principal Cisco Secure Workload à Kafka sont codées au format Tampons de protocole de Google. Consultez ce guide pour obtenir des instructions sur la façon de le télécharger et de l'installer sur votre système Linux.

Le fichier protocole de la politique de réseau Cisco Secure Workload peut être téléchargé ici.

Modèle de données de la politique réseau Cisco Secure Workload

L'image ci-dessous montre un diagramme UML simplifié des entités Cisco Secure Workload accessibles à Kafka :

Figure 99: Modèle de données de la politique réseau Cisco Secure Workload



Une *Cisco Secure Workload politique réseau* telle que modélisée dans protobuf se compose d'une liste de *groupes d'inventaire*, d'une liste d'*intents* et d'une politique *CatchAll* (Collectrice). Chaque politique contient tous les éléments appartenant à une portée racine. Un *InventoryGroup* contient une liste d'*InventoryItems*, qui représentent des entités Cisco Secure Workload telles que des serveurs ou des appareils en spécifiant leur adresse réseau, qu'il s'agisse d'une adresse réseau unique, d'un sous-réseau ou d'une plage d'adresses. Un *intent* décrit une action (autoriser ou refuser) à entreprendre lorsqu'un flux réseau correspond au groupe d'inventaire du consommateur *InventoryGroup*, *du fournisseur*, ainsi que les protocoles et ports réseau. *CatchAll* représente l'action globale définie pour la portée racine dans Cisco Secure Workload. Si aucun espace de travail avec application activée n'existe pour la portée racine, la politique par défaut *ALLOW* est inscrite dans la politique produite.

Lorsqu'une application est déclenchée par les utilisateurs ou par un changement de groupes d'inventaire, le serveur principal Cisco Secure Workload envoie un instantané complet des politiques de réseau définies à Kafka sous la forme d'une séquence de messages représentés par *KafkaUpdates*. Reportez-vous aux commentaires *KafkaUpdate* dans le fichier *tetration_network_politique.proto* pour savoir comment reconstituer ces messages en un instantané complet et comment gérer les conditions d'erreur.

Si la taille du message *KafkaUpdate* est supérieure à 10 Mo, le serveur principal Cisco Secure Workload divise ce message en plusieurs fragments, chacun de 10 Mo. S'il y a plusieurs fragments, seul le premier fragment comporte le champ *ScopeInfo* de *TenantNetworkPolicy*. *ScopeInfo* sera mis à zéro dans les fragments restants du message *KafkaUpdate*.

Mise en œuvre de référence d'un client de politiques de réseau Cisco Secure Workload.

Pour obtenir des instructions sur la mise en œuvre et des instructions sur la façon de compiler et d'exécuter un client de démonstration, consultez tnp-enforcement-client dans Java.

Cette implémentation fournit un code commun pour lire les politiques réseau du flux de politique Cisco Secure Workload via Kafka uniquement. Le code propre au fournisseur pour programmer les politiques réelles sur un périphérique réseau peut être intégré en mettant en œuvre l'interface requise PolicyEnforcementClient.

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.