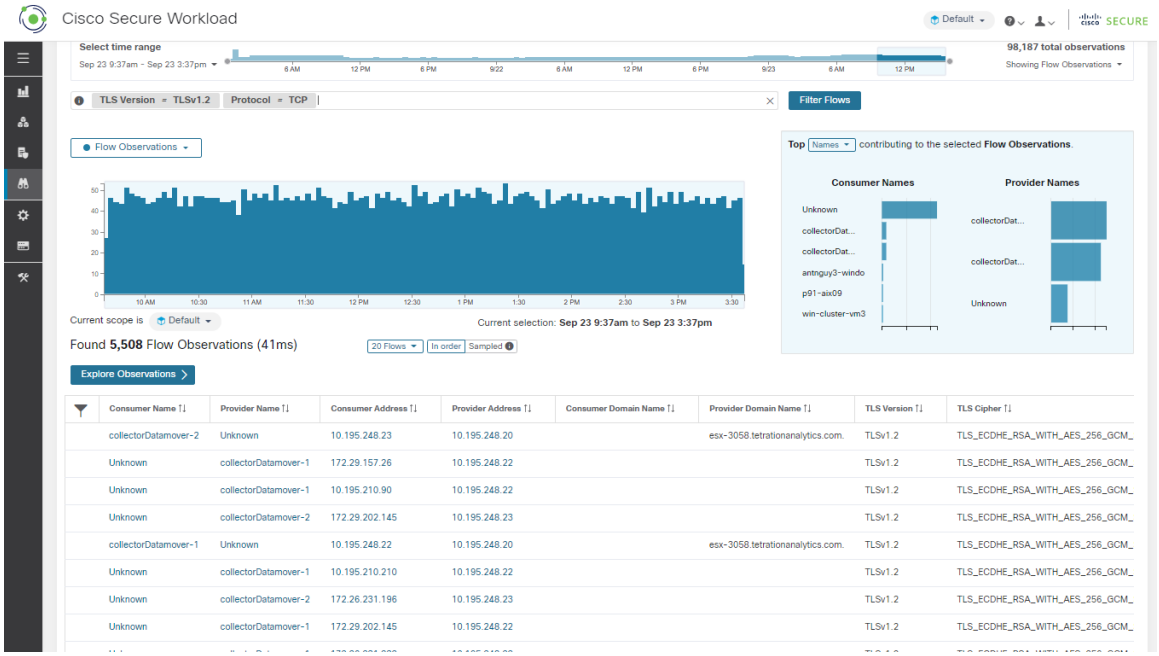
Flux de réseau – Visibilité du trafic

Sur l'interface utilisateur de Cisco Secure Workload, dans le volet de navigation, choisissez **Investigate (Enquêter)** > **Traffic (Trafic)** qui permet d'accéder à la page de recherche de flux. Cette page fournit les moyens de filtrer et d'explorer rapidement le contenu des flux. L'unité de base est **Flow Observation** (l'observation de flux), qui est une agrégation par minute de chaque flux unique. Les deux côtés du flux sont appelés **Consumer** (consommateur) et **Provider** (fournisseur), le consommateur lance le flux et le fournisseur répond au consommateur (par exemple, **client** et **serveur** respectivement). Chaque observation suit le nombre de paquets, d'octets et autres mesures dans chaque direction pour ce flux et pendant cet intervalle d'une minute. En plus de permettre un filtrage rapide, les flux peuvent être explorés visuellement à l'aide des **Explore Observations** (observations Explore). Vous pouvez cliquer sur la liste d'observations de flux qui en résulte pour afficher les détails de ce flux, y compris la latence, les paquets et les octets sur la durée de vie de ce flux.

Avertissement Pour les hôtes dotés d'agents de visibilité approfondie oud'application, Cisco Secure Workload est en mesure de corréler les données de flux avec le processus qui fournit ou consomme le flux. Par conséquent, les arguments de ligne de commande complets, qui peuvent inclure **des informations sensibles telles que les informations d'authentification de la base de données ou de l'API**, utilisés pour lancer le processus sont disponibles pour l'analyse et l'affichage.

Illustration 1 : Présentation des flux



Sélecteur de corpus

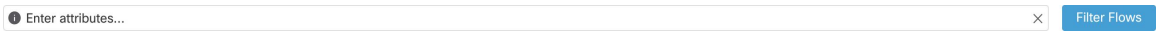
Figure 2: Sélecteur de corpus

Il s'agit des données chronologiques sommaires non filtrées pour la **portée** actuelle pour l'ensemble du corpus. Le but de ce composant est de vous permettre de savoir quelle plage de dates est affichée et de modifier facilement cette plage de dates en la faisant glisser dans le composant. Les données du tableau sont présentes pour le cas où elles seraient utiles pour décider quelle plage temporelle sélectionner. Vous pouvez sélectionner différentes mesures à afficher (par défaut, le nombre d' **observations de flux** est affiché).

Le sélecteur de corpus peut actuellement prendre en charge la sélection d'*environ* **2 milliards d'observations de flux**.

Colonnes et filtres

Figure 3: Filtrer l'entrée



C'est ici que vous définissez les filtres pour affiner les résultats de la recherche. Cliquez sur l'icône **(?)** à côté du mot **Filters** (filtres) pour afficher toutes les dimensions possibles. 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 :

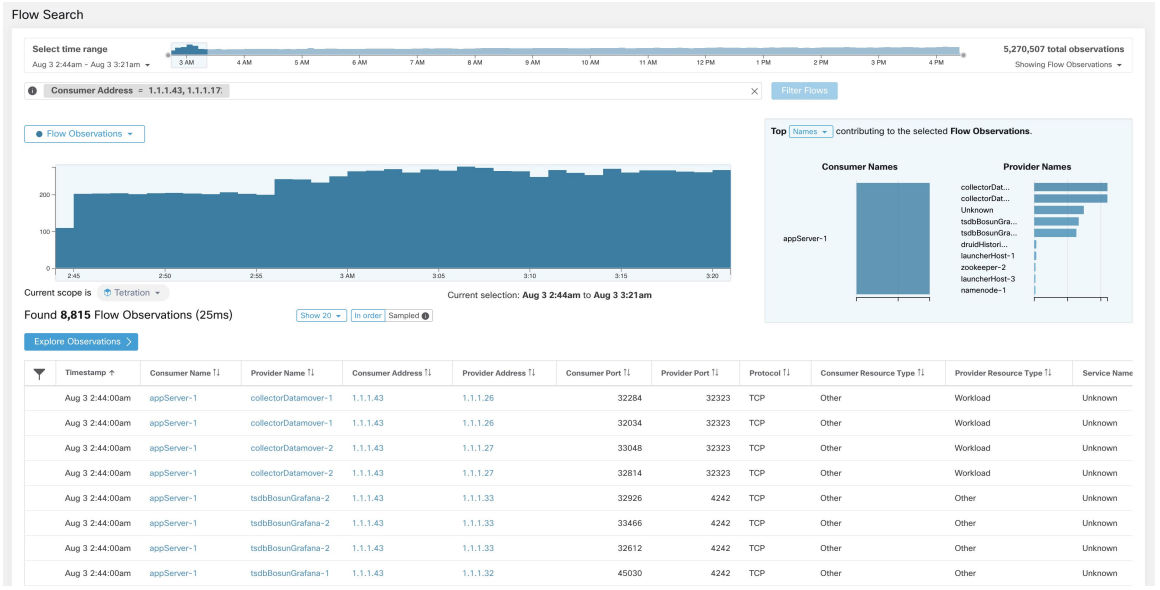
Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1

Et pour filtrer également sur Protocol = 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 4: Prise en charge de l'entrée du filtre pour l'adresse du consommateur



Timestamp	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Aug 3 2:44:00am	appServer-1	collectorDatamover-1	1.1.1.43	1.1.1.26	32284	32323	TCP	Other	Workload	Unknown
Aug 3 2:44:00am	appServer-1	collectorDatamover-1	1.1.1.43	1.1.1.26	32034	32323	TCP	Other	Workload	Unknown
Aug 3 2:44:00am	appServer-1	collectorDatamover-2	1.1.1.43	1.1.1.27	33048	32323	TCP	Other	Workload	Unknown
Aug 3 2:44:00am	appServer-1	collectorDatamover-2	1.1.1.43	1.1.1.27	32814	32323	TCP	Other	Workload	Unknown
Aug 3 2:44:00am	appServer-1	tsdbBosunGrafana-2	1.1.1.43	1.1.1.33	32926	4242	TCP	Other	Other	Unknown
Aug 3 2:44:00am	appServer-1	tsdbBosunGrafana-2	1.1.1.43	1.1.1.33	33466	4242	TCP	Other	Other	Unknown
Aug 3 2:44:00am	appServer-1	tsdbBosunGrafana-2	1.1.1.43	1.1.1.33	32612	4242	TCP	Other	Other	Unknown
Aug 3 2:44:00am	appServer-1	tsdbBosunGrafana-1	1.1.1.43	1.1.1.32	45030	4242	TCP	Other	Other	Unknown

Figure 5: L'entrée du filtre prend en charge la requête de plage pour l'adresse du consommateur

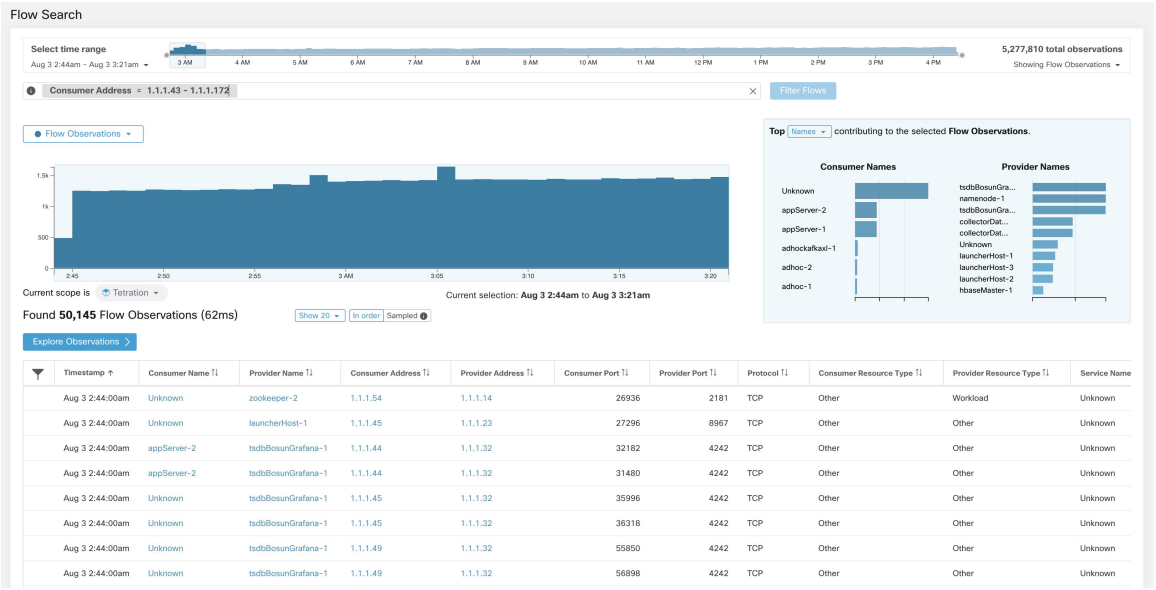


Table 1: Colonnes et filtres disponibles

Colonnes (noms affichés dans l'API)	Description	Source
Adresse du consommateur (*src_address*)	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 dont l'adresse du consommateur recouvre l'adresse IP ou le sous-réseau fourni.	Agents logiciels et dispositifs d'acquisition
Adresse du fournisseur (*dst_address*)	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 dont l'adresse du fournisseur recouvre l'adresse IP ou le sous-réseau fourni.	Agents logiciels et dispositifs d'acquisition
Consumer Name	Recherche les observations de flux dont le nom de la charge de travail du consommateur recouvre le nom de la charge de travail du consommateur saisi.	Agents logiciels et connecteur AnyConnect
Provider Name	Recherche les observations de flux dont le nom de la charge de travail du fournisseur recouvre le nom de la charge de travail du fournisseur saisi.	Agents logiciels et connecteur AnyConnect
Utilisateur consommateur	Recherche les observations de flux dont le nom du consommateur recouvre le nom du consommateur qui a généré le flux.	Agents logiciels et connecteur AnyConnect
Utilisateur fournisseur	Recherche les observations de flux dont le nom du fournisseur recouvre le nom du fournisseur saisi qui a géré le flux.	Agents logiciels et connecteur AnyConnect

Colonnes (noms affichés dans l'API)	Description	Source
Nom de domaine du consommateur	Recherche les observations de flux dont le nom de domaine client (associé à l'adresse IP du client ou au sous-réseau) recouvre le nom de domaine client saisi.	Agents logiciels et connecteur AnyConnect
Nom de domaine du fournisseur	Recherche les observations de flux dont le nom de domaine du fournisseur (associé à l'adresse IP ou au sous-réseau du fournisseur) recouvre le nom de domaine du fournisseur saisi.	Agents logiciels et connecteur AnyConnect
Nom d'hôte du consommateur (*src_hostname*)	Correspond aux flux dont le nom d'hôte du consommateur recouvre le nom d'hôte fourni.	Agents logiciels et connecteur AnyConnect
Nom d'hôte du fournisseur (*dst_hostname*)	Recherche les flux dont le nom d'hôte du fournisseur recouvre le nom d'hôte fourni.	Agents logiciels et connecteur AnyConnect
Groupe d'application du consommateur (*src_enforcement_epg_name*)	Le groupe d'application du consommateur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques appliquées qui correspond au consommateur.	Interne
Groupe d'application du fournisseur (*dst_enforcement_epg_name*)	Le groupe d'application du fournisseur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques appliquées qui correspond au fournisseur.	Interne
Groupe d'analyse du consommateur	Le groupe d'analyse du consommateur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques analysées qui correspond au consommateur.	Interne
Groupe d'analyse des fournisseurs	Le groupe d'analyse du fournisseur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques analysées qui correspond au fournisseur.	Interne
Portée du consommateur (*src_scope_name*)	Correspond aux flux dont le consommateur appartient à la portée spécifiée.	Interne
Portée du fournisseur (*dst_scope_name*)	Correspond aux flux dont le fournisseur appartient à la portée spécifiée.	Interne
Port du consommateur (*src_port*)	Correspond aux flux dont le port de consommateur recouvre le port fourni.	Agents logiciels, ERSPAN et NetFlow
Port du fournisseur (*port_dst*)	Correspond aux flux dont le port du fournisseur recouvre le port fourni.	Agents logiciels, ERSPAN et NetFlow

Colonnes (noms affichés dans l'API)	Description	Source
Pays du consommateur (*src_country*)	Correspond aux flux dont le pays du consommateur recouvre le pays fourni.	Interne
Pays du fournisseur (*dst_country*)	Correspond aux flux dont le pays du fournisseur recouvre le pays fourni.	Interne
Subdivision du consommateur (*src_subdivision*)	Correspond aux flux dont la sous-division du consommateur recouvre la sous-division fournie ((État).	Interne
Subdivision du fournisseur (*dst_Subdivision*)	Correspond aux flux dont la sous-division du fournisseur recouvre la sous-division fournie (État).	Interne
Organisation du système autonome du consommateur (*src_ autonomous_system_organization*)	Correspond aux flux dont l'organisation du système autonome du consommateur recouvre l'organisation du système autonome (ASO) fourni.	Interne
Organisation du système autonome du fournisseur (*dst_autonomous_system_organisation*)	Correspond aux flux dont l'organisation du système autonome du fournisseur recouvre l'organisation du système autonome (ASO) fourni.	Interne
Protocole (*proto*)	Filtrez les observations de flux par type de protocole (TCP, UDP, ICMP).	Agents logiciels et dispositifs d'acquisition
Type d'adresse (*key_type*)	Filtrez les observations de flux par type d'adresse (IPv4, IPv6, DHCPv4).	Agents logiciels et dispositifs d'acquisition
Indicateurs TCP Avant	Filtrez les observations de flux par indicateurs (SYN, ACK, ECHO).	Agents logiciels, ERSPAN et NetFlow
Indicateurs TCP Retour	Filtrez les observations de flux par indicateurs (SYN, ACK, ECHO).	Agents logiciels, ERSPAN et NetFlow
UID de processus Avant (*fwd_process_owner*)	Filtrez les observations de flux par UID de propriétaire de processus (root, admin, yarn, mapred).	Agents logiciels
UID du processus Rev. (*rev_process_owner*)	Filtrez les observations de flux par UID de propriétaire de processus (root, admin, yarn, mapred).	Agents logiciels
Processus Avant (*fwd_process_string*)	Filtrez les observations de flux par processus (java, Hadoop, nginx). Voir l'avertissement relatif à la visibilité de la chaîne de processus	Agents logiciels

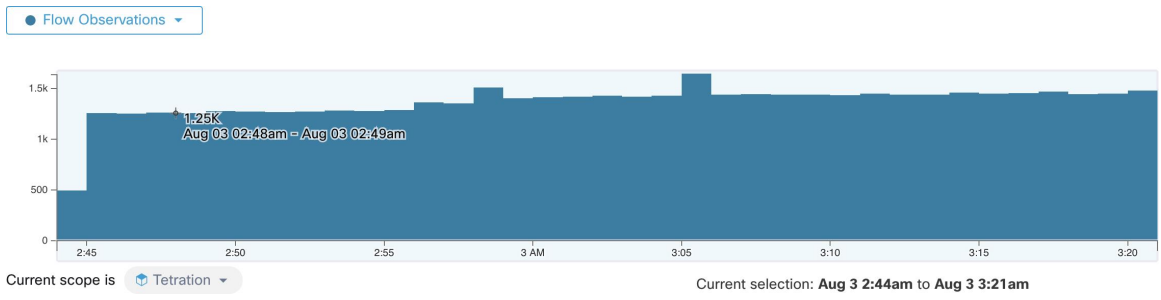
Colonnes (noms affichés dans l'API)	Description	Source
Processus Retour (*rev_process_string*)	Filtrez les observations de flux par processus (java, Hadoop, nginx). Voir l'avertissement relatif à la visibilité de la chaîne de processus	Agents logiciels
Consumer In Collection Rules?	Mettre en correspondance uniquement les consommateurs internes.	Interne
Provider In Collection Rules?	Mettre en correspondance uniquement les fournisseurs internes.	Interne
SRTT disponible	Met en correspondance les flux pour lesquels des mesures SRTT sont disponibles en utilisant les valeurs « vrai » ou « faux ». (Ceci équivaut à un SRTT > 0).	Interne
Octets	Filtrez les observations de flux par tranche de trafic d'octets. Correspond aux flux dont les valeurs de tranche de trafic d'octets sont =, <, > (regroupées par puissances de 2 (0, 2, 64, 1024)).	Agent logiciel et appareils d'acquisition
Paquets	Filtrez les observations de flux par tranche de trafic de paquets. Correspond aux flux dont les valeurs de tranches de trafic de paquets sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel et appareils d'acquisition
Durée du flux (µs)	Filtrez les observations de flux par tranche de durée de flux. Correspond aux flux dont les valeurs de tranche de durée de flux sont =, <, > (regroupées par puissances de 2 (0, 2, 64, 1024)).	Interne
Durée des données (µs)	Filtrez les observations de flux par tranche de durée des données. Correspond aux flux dont les valeurs de tranche de durée de données sont =, <, > (regroupées par puissances de 2 (0, 2, 64, 1024)).	Interne
SRTT (µs) (*srtt_dim_usec*)	Filtrez les observations de flux par tranche SRTT. Correspond aux flux dont les valeurs de tranches SRTT sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel
Retransmissions de paquets Avant (*fwd_tcp_pkts_retransmitted*)	Filtrez les observations de flux par tranches de retransmissions de paquets. Correspond aux flux dont les valeurs de tranches de retransmissions de paquets sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel
Retransmissions de paquets Retour (*rev_tcp_pkts_retransmitted*)	Filtrez les observations de flux par tranches de retransmissions de paquets. Correspond aux flux dont les valeurs de tranches de retransmissions de paquets sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel

Colonnes (noms affichés dans l'API)	Description	Source
Étiquettes d'utilisateur (* ou préfixe *user_*)	Données définies par l'utilisateur qui sont associées aux étiquettes personnalisées chargées manuellement qui commencent par * dans l'interface utilisateur et *user_* dans OpenAPI.	CMDB
TLS Version (Version TLS)	Version du protocole SSL utilisée dans le flux.	Agent logiciel
Chiffrement TLS	Type d'algorithme utilisé par le protocole SSL dans le flux.	Agent logiciel
Type d'agent du consommateur	Préciser le type d'agent de consommateur.	Interne
Type d'agent du fournisseur	Précisez le type d'agent du fournisseur.	Interne
Type de ressource consommateur	Représente le flux de ressources d'une source à un consommateur. Il peut s'agir d'une charge de travail, de pods, de services ou autres	Interne
Type de ressource de fournisseur	Représente le flux de ressources d'un fournisseur à un consommateur. . Il peut s'agir d'une charge de travail, de pods, de services ou autres.	Interne

Note Comme les données de flux sont marquées avec des étiquettes d'utilisateur uniquement au moment de l'acquisition, les étiquettes d'utilisateur ne s'affichent pas immédiatement après leur activation. Quelques minutes peuvent s'écouler avant que les étiquettes ne commencent à apparaître dans la recherche de flux. En outre, les étiquettes d'utilisateur disponibles varient en fonction de la partie du **sélecteur de corps** que vous avez sélectionnée, car les étiquettes activées peuvent avoir été modifiées à divers moments.

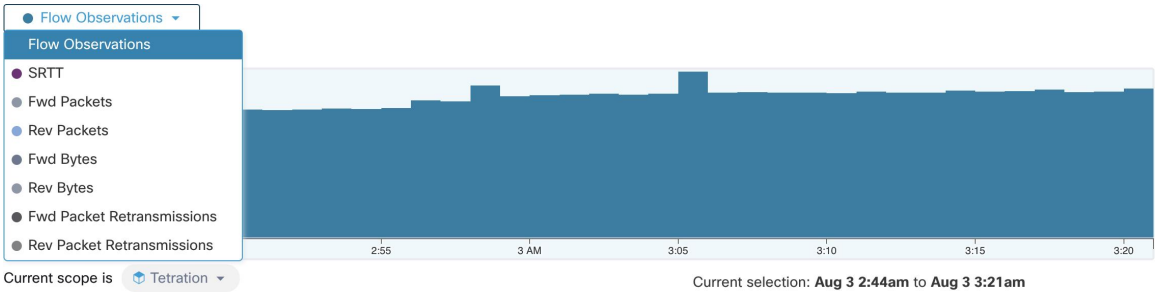
Séries temporelles filtrées

Figure 6: Séries temporelles filtrées



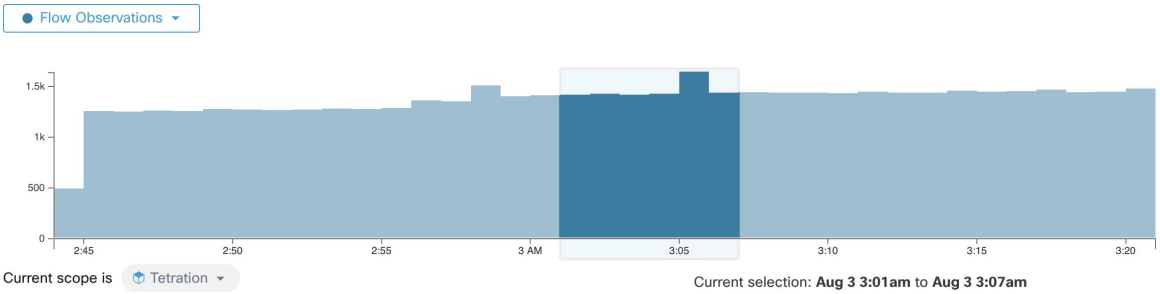
Ce composant affiche les totaux agrégés de diverses mesures pour l'intervalle sélectionné (sélection effectuée dans Sélecteur de corpus, on page 2). Utilisez la liste déroulante pour modifier la mesure à afficher.

Figure 7: Liste déroulante des séries chronologiques



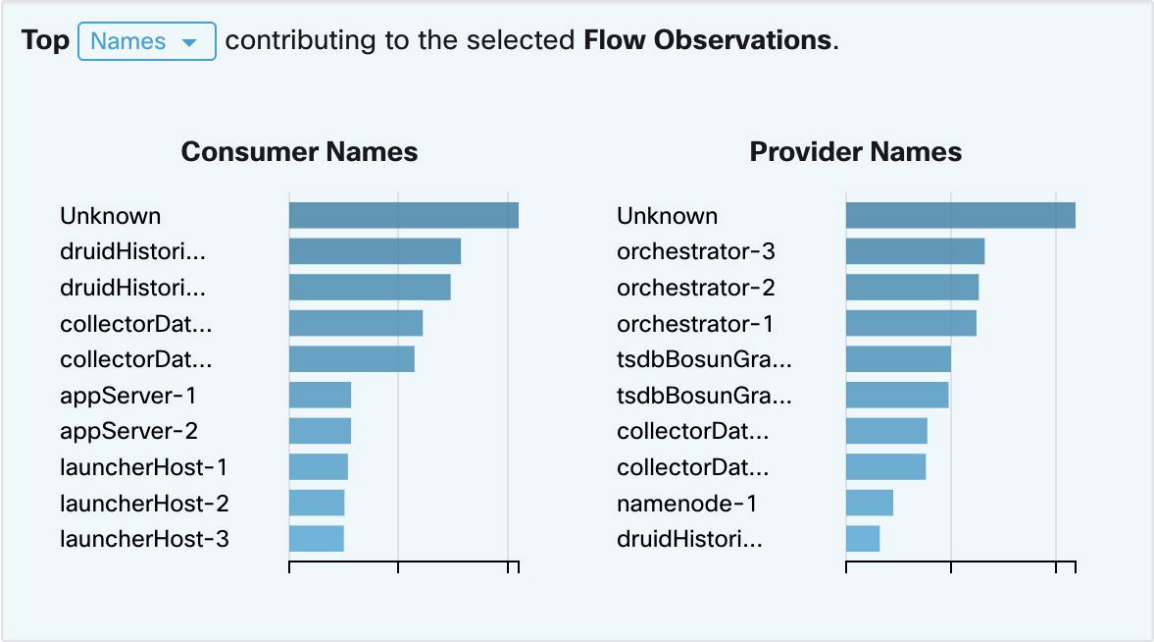
Il est également possible de réduire davantage l'intervalle sélectionné dans ce composant. Cliquez sur la zone du graphique sur laquelle vous souhaitez vous concentrer. Les N principaux graphiques et les données ci-dessous seront tous mis à jour pour inclure uniquement les données de l'intervalle sélectionné.

Figure 8: Séries chronologiques avec sélection



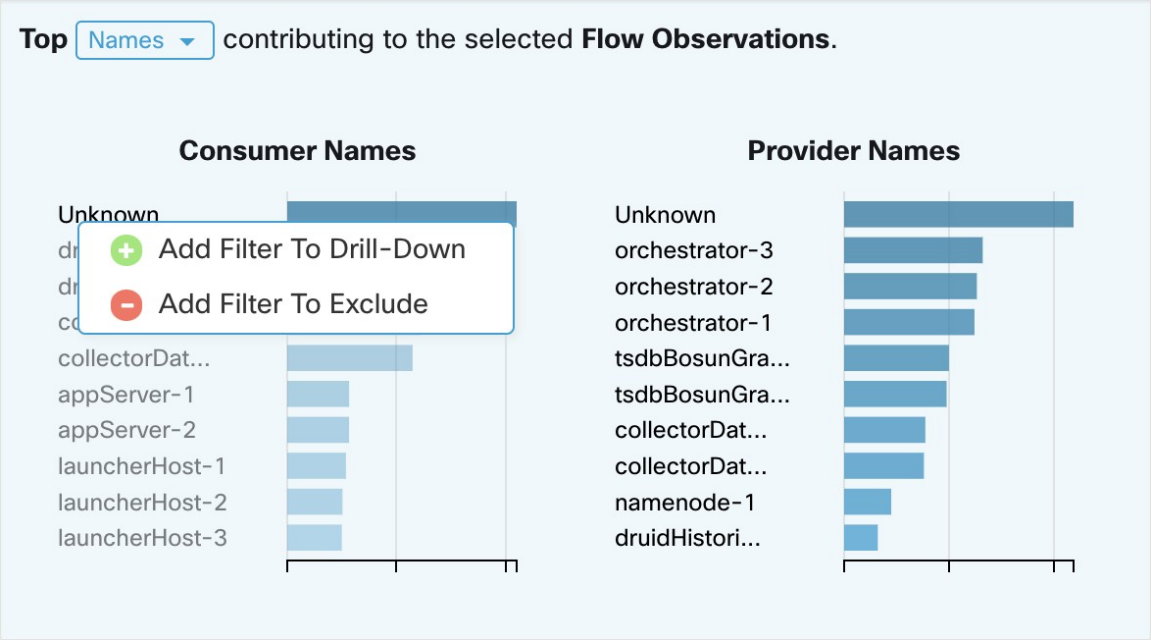
N principales valeurs

Figure 9: N principales valeurs



Les tableaux affichent les N valeurs les plus élevées qui contribuent à la sélection dans le graphique des séries chronologiques filtrées situé à gauche. La sélection d'un pic dans les observations de flux dans le tableau de séries chronologiques et de noms d'hôtes dans les tableaux des N principales valeurs, permet d'afficher la liste des noms d'hôte (consommateur et fournisseur) qui contribuent le plus à ces observations de flux. De plus, si le tableau de série chronologique est configuré pour afficher un SRTT, les principaux noms d'hôte affichent ceux qui contribuent le plus au SRTT sélectionné.

Figure 10: Approfondir/Exclure

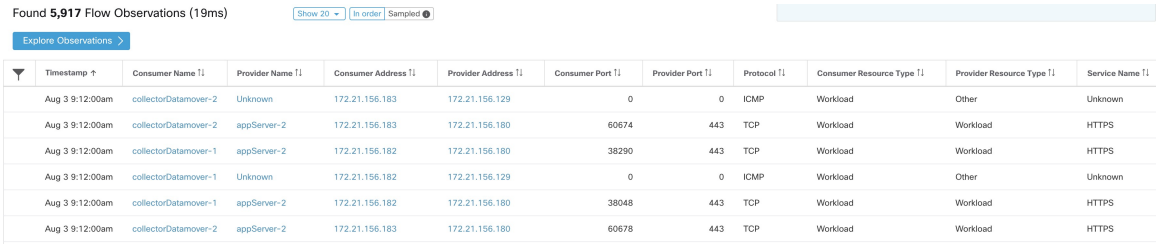


Cliquez sur l'un des éléments des tableaux des N principales valeurs pour afficher un menu qui vous permet d'**approfondir** ou d'**exclure** cette valeur.

- Cliquez sur **Drill-Down** (Approfondir) pour ajouter un filtre qui limite les résultats à cette valeur.
- Cliquez sur **Exclude** (Exclure) pour ajouter un filtre qui exclut cette valeur des résultats.

Note Après avoir cliqué sur **Approfondir** ou **Exclure**, vous devez appuyer sur l'icône **Filtrer** pour que le filtre prenne effet. Cela afin que plusieurs actions d **exclusion** puissent être effectuées rapidement sans que la page soit mise à jour à plusieurs reprises en même temps.

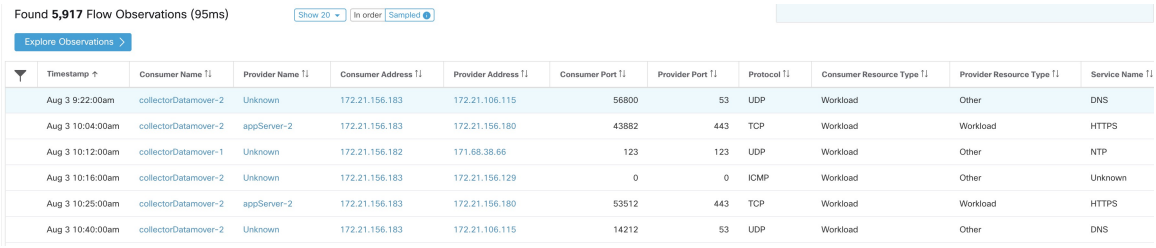
Liste d'observations



Ceci est la liste des **observations de flux** réelles qui correspondent aux filtres et aux sélections de la page ci-dessus. Par défaut, 20 fichiers seront chargés en commençant par le début de l'intervalle. Il est possible d'augmenter le nombre de fichiers chargés en utilisant la liste déroulante. Il est également possible de charger un ensemble aléatoire d'observations de flux à partir de l'intervalle sélectionné en utilisant la commande

Sampled (Échantillonné) plutôt que **In order** (Dans l'ordre). Le paramètre **Échantillonné** est utile pour obtenir un ensemble plus représentant d'observations de débit à partir de l'intervalle sélectionné plutôt que de les charger successivement à partir du début de l'intervalle.

Figure 11: Échantillonné



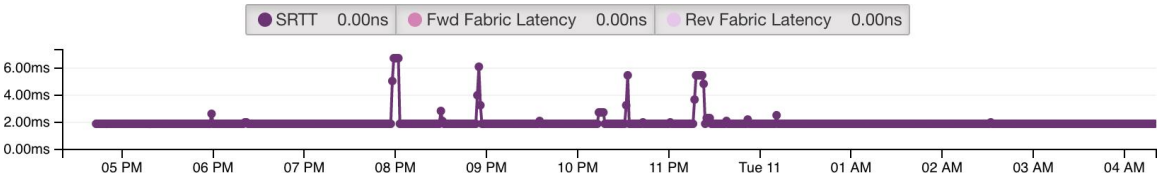
Détails des flux

Cliquez sur l'une des lignes pour développer la section **Flow Details** (détails d flux).es Cette fonction permet d'afficher un résumé du flux et des tableaux de diverses mesures pour la durée de vie de ce flux. Pour les flux de longue durée, un tableau récapitulatif s'affiche au bas de la page. Il vous permet de choisir différents intervalles pour lesquels afficher les données de séries chronologiques.

Figure 12: Détails des flux

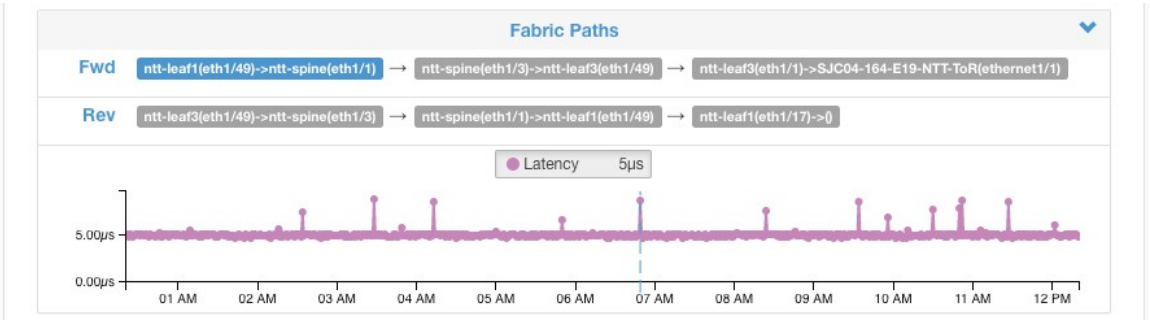
Pour les flux étiquetés avec des informations sur le chemin de la structure, **la latence de trame avant/retour** et **SRTT** sont disponibles. Les tableaux de séries chronologiques pour d'autres mesures, comme les **indicateurs de rafale avant/retour et les indicateurs de rafale avant/retour + Abandon,** peuvent être affichés s'ils sont disponibles. Reportez-vous à Avertissement relatif à la visibilité.

Figure 13: Latence



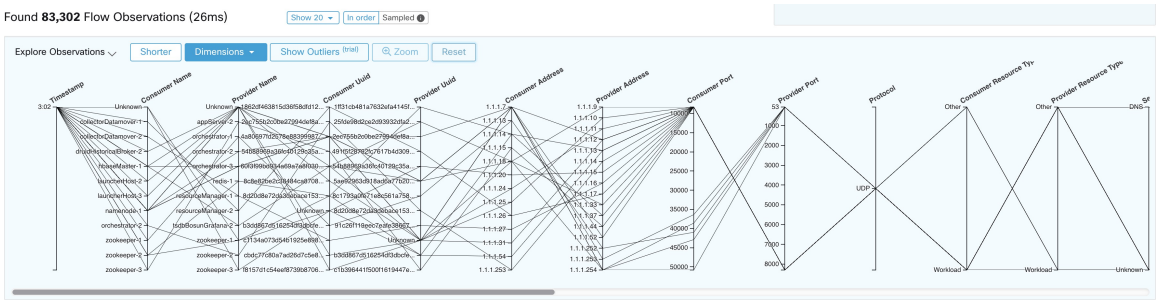
Des détails sur le **chemin de structure Avant/Retour** sont également disponibles. Chaque lien est cliquable, ce qui active les tableaux de série chronologique de **latence** et d'**abandon** (lorsqu'ils sont non nuls). Cliquez sur **Fwd** (Avant) ou **Rev** (Retour) pour accéder au détail de la page Fabric Path Overlay (Superposition de chemins de la structure) pour le flux.

Figure 14: Chemins de la structure



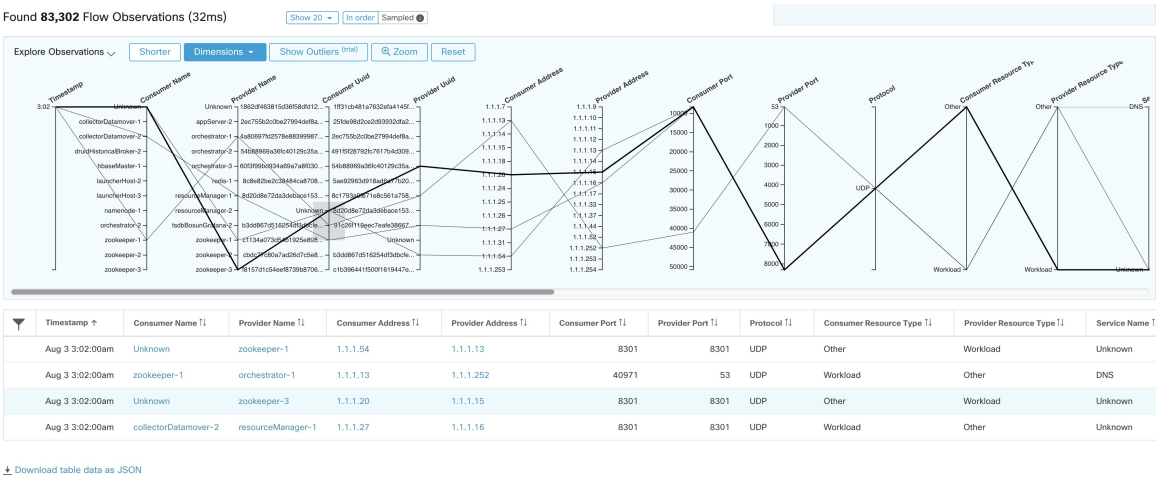
Explorer les observations

Figure 15: Explorer les observations



Cliquez sur **Explore Observations** (explorer les observations) pour activer un affichage graphique permettant d'explorer rapidement les données dont les dimensions sont élevées **(graphique à coordonnées parallèles**). Un peu impressionnant au premier abord, ce tableau est 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 16: Observation de flux survolée par le curseur



Timestamp ↑	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Aug 3 3:02:00am	Unknown	zookeeper-1	1.1.1.54	1.1.1.13	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	zookeeper-1	orchestrator-1	1.1.1.13	1.1.1.252	40971	53	UDP	Workload	Other	DNS
Aug 3 3:02:00am	Unknown	zookeeper-3	1.1.1.20	1.1.1.15	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	collectorDatamover-2	resourceManager-1	1.1.1.27	1.1.1.16	8301	8301	UDP	Workload	Other	Unknown

Download table data as JSON

En raison de la nature complexe des données de flux, ce graphique est large par défaut et nécessite de le faire défiler vers la droite pour le voir en entier. C'est pourquoi il est utile de désactiver toutes les dimensions sauf celles qui vous intéressent.

Par échantillonnage ou par ordre

Il est recommandé d'effectuer les observations Explore avec **l'échantillonnage** activé et avec un plus grand nombre de flux. Cela vous permet de mieux voir la variété des flux qui composent l'intervalle sélectionné. Ainsi, si vous avez sélectionné 2 millions d'observations de flux dans le tableau de séries chronologiques ci-dessus, le chargement d'un échantillon de 1000 flux les choisira uniformément tout au long de l'intervalle, tandis que le chargement des flux **dans l'ordre** chargera les 1000 premières observations de flux depuis le tout début de intervalle :

Figure 17: 1000 par ordre

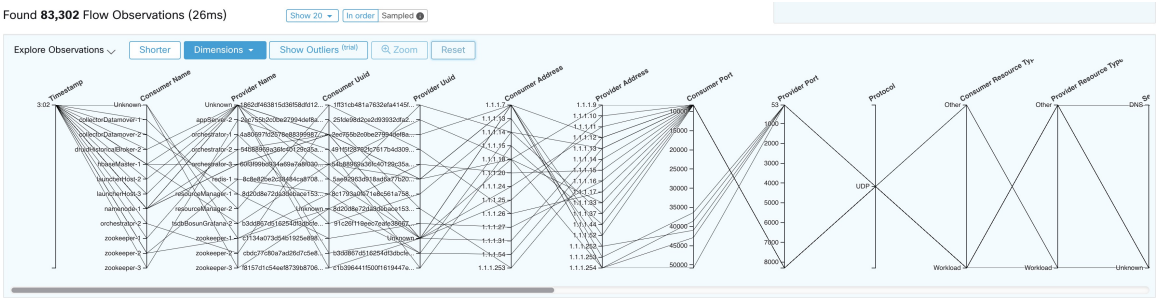
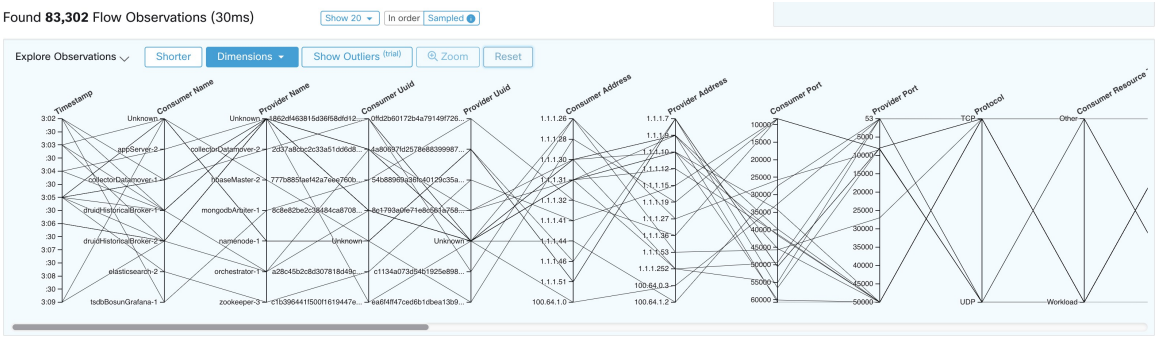


Figure 18: par rapport à 1000 échantillons

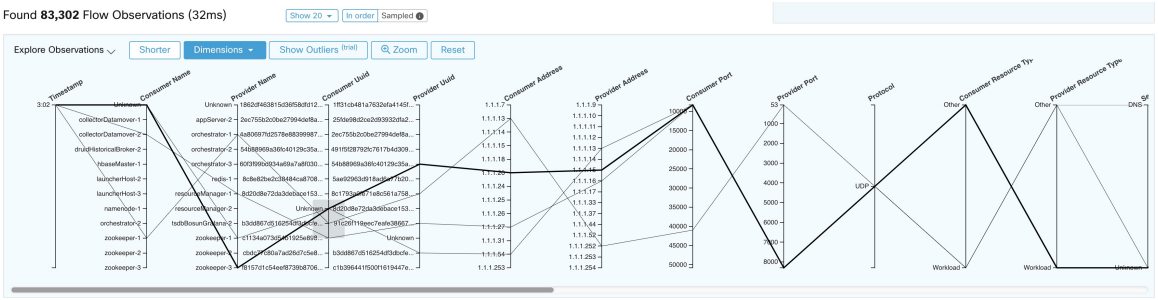


Remarquez que l' **horodatage** de toutes les observations dans l'ordre est 9:09 et que les observations sont réparties uniformément dans l'intervalle sélectionné dans la version échantillonnée.

Filtrage

Faites glisser le curseur le long de l'un des axes pour créer une sélection qui affiche 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 est mise à jour pour afficher uniquement les observations sélectionnées :

Figure 19: Explorer avec sélection



Timestamp	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Aug 3 3:02:00am	Unknown	zookeeper-1	1.1.1.54	1.1.1.13	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	zookeeper-1	orchestrator-1	1.1.1.13	1.1.1.252	40971	53	UDP	Workload	Other	DNS
Aug 3 3:02:00am	Unknown	zookeeper-3	1.1.1.20	1.1.1.15	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	collectorDatamover-2	resourceManager-1	1.1.1.27	1.1.1.16	8301	8301	UDP	Workload	Other	Unknown

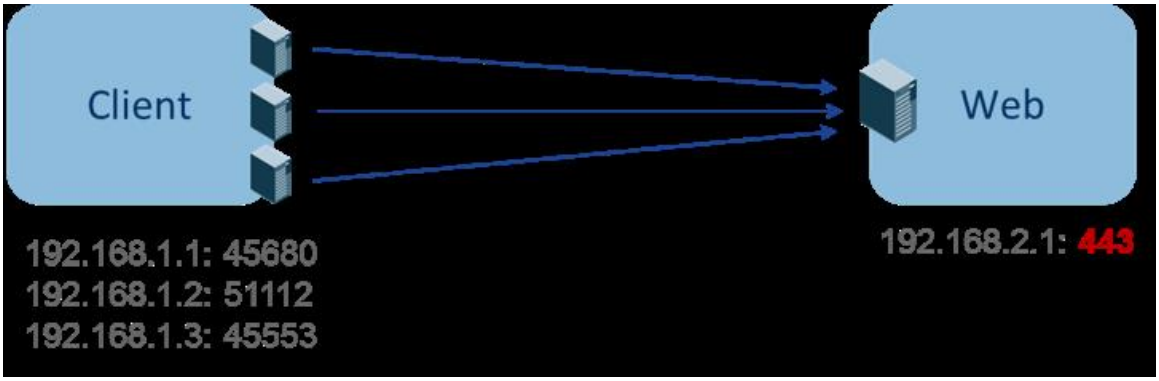
Download table data as JSON

Classification client-serveur

Le sens du flux (classification client/serveur ou fournisseur/consommateur) est important pour la visibilité, la découverte automatique et l'application des politiques. Chaque flux de monodiffusion comporte une classification client et une classification serveur.

Par exemple, si des clients (192.168.1.1-192.168.1.3) accèdent à un serveur Web (192.168.2.1) à l'aide de https, le port source est généralement un port éphémère dans la plage 1025-65535 et le port de destination est 443.

Figure 20: Classification client-serveur



La direction précise client-serveur est :

- Client : 192.168.1.1-3
- Serveur : 192.168.2.1
- Services : Port TCP 443

Les politiques générées par la découverte automatique des politiques sont indiquées dans la figure (avec les points terminaux de gauche regroupés) :

Figure 21: Politiques générées

Maintenant, si la décision dans le sens client-serveur est inversée (une classification inexacte), l'on trouve :

- Client : 192.168.2.1
- Serveur : 192.168.1.1-3
- Services : la liste des ports éphémères (45680, 51112, 45553)

Ensuite, dans la classification inexacte ci-dessus, les politiques générées peuvent être celles indiquées dans la figure :

Figure 22: Classification inexacte

Cela consomme plus de ressources en termes d'application des politiques. En outre, selon la façon dont vous appliquez la politique, même si 192.168.1.1-3 utilise ces ports éphémères, ils ne peuvent pas accéder à 192.168.2.1. Par exemple, si vous utilisez Cisco Secure Workload, la mise en application des capteurs logiciels, la politique d'application pour la condition Client vers le Web ci-dessus (ESTAB) ne correspond pas au trafic généré par le client destiné au Web (NEW, ESTAB).

Les horodatages et les indicateurs TCP sont utilisés dans Cisco Secure Workload pour déterminer le sens client-serveur. S'il n'y a aucune information d'indicateurs TCP (SYN, SYN/ACK) parce que, par exemple, les paquets peuvent être UDP/ICMP ou parce qu'un capteur matériel ne prend pas en charge les signaux de direction, les règles de remplacement définies par l'utilisateur, les horodatages et autres méthodes empiriques sont utilisés pour déduire la direction du flux. Par définition, les méthodes empiriques ne garantissent pas une précision à 100 %. La précision client-serveur est fonction du type de capteur utilisé et des conditions dans lesquelles les capteurs sont utilisés. Vous pouvez utiliser l'API REST (OpenAPI) de Cisco Secure Workload pour insérer des règles de remplacement client-serveur afin d'identifier les ports de serveur pour les types de flux qui font que Cisco Secure Workload se trompe de direction. Autorisez ensuite Cisco Secure Workload à traiter les nouveaux flux de données captés avec ces règles en place, puis générez les politiques sur la durée lorsque la direction du flux a été déterminée. Pour plus de détails sur l'API pour spécifier les règles de remplacement, consultez : Configuration client-serveur. Vous pouvez également définir manuellement les politiques et examiner/supprimer les politiques indésirables. Consultez Politiques.

Recommandation de type de capteur

Une visibilité approfondie ou les agents logiciels d'application fournissent les meilleurs signaux aux algorithmes de classification client-serveur Cisco Secure Workload. Nous sommes invités à envisager de déployer des agents d'application ou de visibilité approfondie. Ces agents reçoivent tous les signaux nécessaires pour établir une classification client-serveur correcte. Si le déploiement d'agents d'application ou de visibilité approfondie n'est pas possible pour certaines charges de travail, il est recommandé d'utiliser les capteurs ERSPAN et de s'arrêter là pour la découverte automatique des politiques. Cisco Secure Workload nous aide du mieux possible et nous améliorons continuellement nos algorithmes heuristiques en fonction des commentaires.

Lorsque les informations correctes sur la direction client-serveur ne sont pas disponibles, Cisco Secure Workload utilise des dérogations définies par l'utilisateur ou une heuristique pour déduire la direction. Par définition, les méthodes empiriques ne garantissent pas une précision à 100 %. La précision diminue avec le type de capteur utilisé et les conditions dans lesquelles il a été utilisé.

Le tableau suivant est l'ordre recommandé pour la décision client-serveur dans les scénarios de génération de politiques :

- **Agents de visibilité approfondie ou d'application** : pour de meilleurs résultats, utilisez des capteurs logiciels (agents de visibilité approfondie ou d'application). Les flux de trafic ayant commencé avant le démarrage du capteur seront traités par une méthode heuristique qui est abordée ci-dessous.

- Les capteurs ADC de **comme F5/Citrix/. . . agents** : ces agents recueillent l'état client-serveur des périphériques ADC et diffusent cette source fiable dans Cisco Secure Workload.
- **Capteurs ERSPAN** : avec un capteur ERSPAN, l'utilisateur doit veiller à fournir une visibilité complète du trafic à destination et en provenance de la charge de travail concernée et s'assurer que le capteur ERSPAN voit tout le trafic réparti. Le capteur ERSPAN ne doit pas non plus être trop sollicité, de sorte que sa visibilité ne soit pas affectée par la communication réseau de la charge de travail. En outre, l'utilisateur doit s'assurer que les pertes de paquets des capteurs ERSPAN sont réduites au minimum. L'opérateur ne verra pas les informations de processus avec les informations de flux de réseau pour la découverte automatique des politiques.

En utilisant le capteur Netflow énuméré ci-dessous, l'utilisateur doit s'engager dans un travail manuel beaucoup plus important pour l'analyse de la politique et la génération de règles d'exception. Cisco Secure Workload utilise largement la méthode heuristique, qui, par définition, n'est pas précise à 100 %.

- **Capteur** NetFlow : NetFlow fournit des données de flux échantillonnées et agrégées. Les processus d'agrégation et d'échantillonnage provoquent la perte d'informations sur la direction client-serveur. Cela a une incidence sur les résultats de la découverte automatique des politiques et de la génération de ces dernières et rend le problème plus ardu. Les données NetFlow sont excellentes pour une visibilité globale. Cisco Secure Workloaddoit se rabattre sur l'heuristique qui, si elle est incorrecte, exige parfois davantage de travail manuel de la part de l'opérateur - comme la définition de règles d'exception pour la charge de travail sécurisée. Les données NetFlow omettent également certains des flux courts et la qualité du signal dépend du périphérique qui produit les données NetFlow. Nous vous recommandons d'utiliser NetFlow avec Cisco Secure Workload pour les cas d'utilisation spécialisés comme l'assemblage des flux à travers des périphériques NAT L3/L4 comme dans le cas des contrôleurs de livraison d'application (ou des équilibreurs de charge de serveur) pour fournir à Cisco Secure Workload la visibilité de quel flux est lié à quel autre flux.

L'analyse de la direction client-serveur est décrite plus en détail ci-après.

Identification des producteurs (serveurs) et des consommateurs (clients) d'un flux

Il existe plusieurs façons (souvent pragmatiques) de détecter les serveurs :

- Si un capteur constate l'établissement de liaison SYN, il peut déterminer qui est le serveur.
- Basée sur le temps : l'initiateur d'une connexion est considéré comme un client.
- Modèle du degré : généralement, de nombreux clients communiquent avec un serveur. En revanche, le degré du port client devrait être largement inférieur.

L'ordre de priorité est SYN_ANALYSIS/NETSTAT > USER_CONFIG > DEGREE_MODEL.

Le raisonnement qui consiste à donner à SYN_ANALYSIS une priorité plus élevée que la configuration de l'utilisateur est que la configuration peut être périmée et que le capteur a le meilleur point d'observation pour établir la réalité du terrain. DEGREE_MODEL est l'endroit où l'apprentissage et les méthodes heuristiques entrent en jeu, et la précision ne peut pas être garantie à 100 %.

Il est possible que notre approche heuristique de la détection client-serveur soit erronée, malgré nos meilleures intentions et les améliorations algorithmiques constantes que nous apportons dans ce domaine. Dans ces scénarios, l'interface OpenAPI peut être utilisée pour marquer les ports de serveur bien connus. Ces configurations ne sont pas appliquées aux flux passés et n'affectent que les marquages des flux à partir du

moment présent (c'est-à-dire les flux suivants). Il s'agit d'une solution de repli de dernier recours, plutôt que le mode de fonctionnement normal.

Nous recommandons également de ne pas continuer à intervertir le marquage client-serveur pendant toute la durée d'un flux donné (même si nous nous trompons et si nos modèles internes ont changé - ce qu'ils font au fil du temps, à mesure que de nouveaux modèles de flux sont observés ou analysés). Les mises à jour de priorité supérieure ou égale sont autorisées à remplacer celles de priorité inférieure (nous inverserons également le serveur client pour les flux existants). En d'autres termes, la régularité de la correction « pour la durée de vie d'un flux » ne s'applique qu'à la correction basée sur un modèle de degré.

Conversation Mode

By default, the flow analysis fidelity mode in agents is "detailed". Historically, this was the only mode available, where, every observed flow was reported by the agent along with detailed stats about the observed flow. Stats like: packet and byte counts, TCP flags, connection stats, network latency, srtt, etc.

While this kind of reporting is desirable in a lot of cases, it is computationally intensive to report and process, also, it may not be strictly required when the primary use case is segmentation only.

The **Conversation Mode** offers a more lightweight alternative to the traditional detailed mode. Agents in conversation mode aim to report conversations as opposed to flows whenever possible (i.e, whenever they are able to make the client-server classification accurately). This is applicable to TCP, UDP and ICMP flows.

In detailed mode, for TCP/UDP flows, we report 5-tuple flows {source and destination IP, source and destination port, and protocol}.

While for conversation mode, agent omits the source port as they are ephemeral ports {changes on every new connection}, making it a 4-tuple flow.

Note Detecting a flow as 4-tuple also depends on client server detection algorithms, which relies on server/destination port being a well-known port (0 through 1023) .

Thus, if you are using a custom application which does not use well-known server/destination ports, the OpenAPI interface can be used to punch well known server ports. These configs are not applied to past flows, and only affect markings on flows from that point on (i.e., going forward). To optimize server ports, see Client Server Configuration.

Agent reports in conversation mode contain trimmed down information, full list of omitted fields includes: TCP/UDP source port (ephemeral ports), Fwd/Rev TCP bottleneck, TCP handshake bucket, SRTT(µs), Fwd/Rev Packet retransmissions, SRTT Available, Fwd/Rev Congestion Window Reduced, Fwd/Rev MSS Changed, Fwd/Rev TCP Rcv Window Zero?, Fwd/Rev Burst Indicator, Fwd/Rev Max Burst Size (KB).

To enable conversation mode, please refer to the Flow Visibility config section in: Software Agent Config

Note The exact benefit gained by changing agents to report in conversation mode may vary due to multiple factors, including, but not limited to percentage of TCP flows, number of services listening on well known service ports, and memory limitations at the agent.

Note After turning on “conversation” mode for some agents, there may be a mixture of conversations and flows in the observations on the flow search page.

Visibilité dans les flux mandatés

Un serveur mandataire agit comme un serveur placé entre les ordinateurs clients et Internet, contrôlant et restreignant l’accès direct du client à Internet. Lorsqu’un client souhaite accéder aux services Internet, il ordonne au serveur mandataire d’établir une connexion TCP avec les serveurs Web en son nom. Après avoir établi la connexion avec succès, le serveur mandataire envoie une réponse HTTP avec un état au client. Ultérieurement, le client interagit sur la connexion TCP établie, semblant communiquer directement avec le service Web. Le serveur mandataire sert de pont, ce qui facilite la transmission des données entre les deux connexions TCP.

La charge de travail, qui héberge une application sur laquelle l’agent CSW est installé, lance une demande de services Internet. Au départ, il demande au serveur mandataire de créer un canal de communication en son nom. L’interaction avec le service Internet a lieu via la connexion établie avec le serveur mandataire. L’agent CSW capture uniquement le flux entre la charge de travail et le serveur mandataire. La destination réelle de ce flux reste inconnue avec la configuration actuelle de l’agent CSW.

L’agent utilise le filtre pcap actuel pour analyser tous les paquets TCP sortants, à la recherche du Verbe HTTP « CONNECT » dans la charge utile. Ce processus permet à l’agent de capter la demande de serveur mandataire dans le flux. Lors de l’exportation des flux vers les collecteurs, l’agent génère un **flux effectif** pour chaque flux de serveur mandataire identifié. Il établit une connexion entre le serveur mandataire et les flux soumis à un mandataire à l’aide du champ **related_key** (clé liée) en incorporant les informations sur les quintuples.

Note Cette fonction est activée par défaut. Pour la désactiver, ajoutez *Enable_serveur mandataire_flows_visibility: 0* au fichier de configuration du capteur.

Préalables

Régler la fidélité de l’analyse de flux sur Mode détaillé.

Note

- Fonctionne uniquement avec un serveur mandataire HTTP/HTTPS.
- Capture uniquement les demandes CONNECT. Actuellement, les demandes GET ne sont pas prises en charge.
- Par défaut, le mode de fidélité pour l’analyse de flux des agents est **Conversations**.

Procédure

1. Dans le menu de navigation choisissez **Investigate** > **Traffic** (Enquêter sur le trafic).

   Cette page facilite le filtrage rapide et l’exploration en profondeur du corps de flux.

2. Développez-la pour afficher les détails du flux.

Les agents dans la version 3.9 ou ultérieure peuvent capturer la destination des flux par serveur mandataire. À la page **Investigate** > **Traffic**, vous pouvez observer les deux flux distincts :

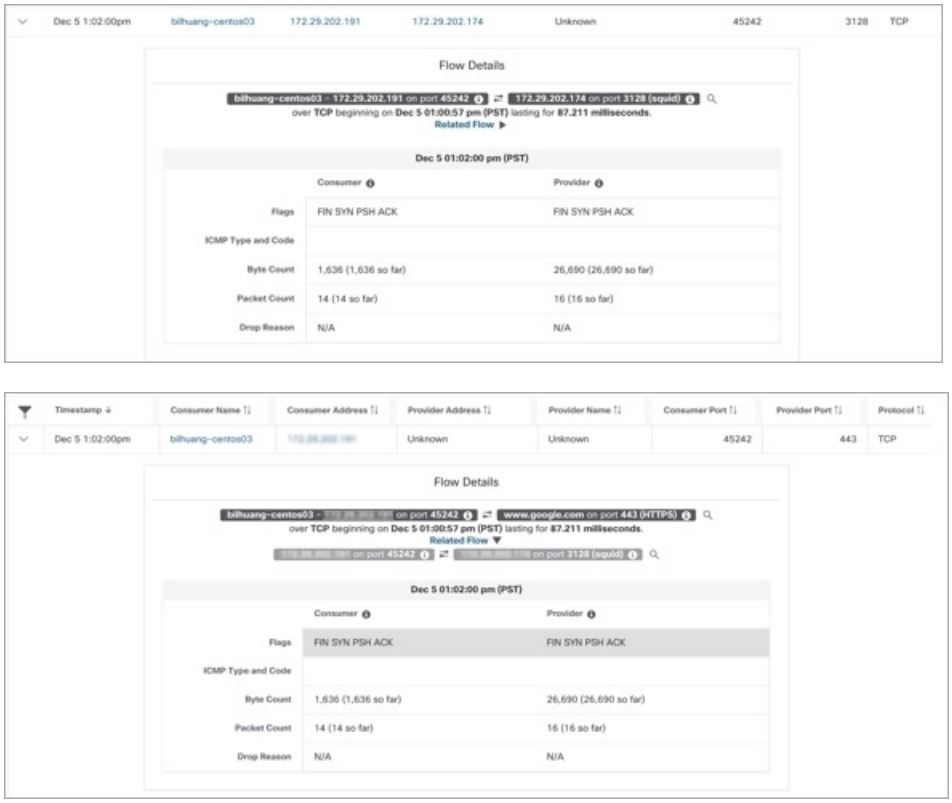
a. **Flux de serveur mandataire** : provenant de la charge de travail vers le serveur mandataire.

b. **Flux mandataire** : représentant un flux effectif et canalisé depuis la charge de travail jusqu'au nom de domaine complet (FQDN) ou l'adresse distante.

Ces flux sont interconnectés et désignés comme **Associés**. Les considérations spécifiques sont les suivantes :

- Si la demande au serveur mandataire est dirigée vers un nom de domaine complet distant, l'**adresse du fournisseur** du flux effectif est marquée comme **Unknown** (Inconnue), mais le **nom de domaine du fournisseur** est défini sur le nom de domaine complet.
- Si la demande au serveur mandataire est dirigée vers une adresse IP distante, l'adresse du **fournisseur** est cette adresse spécifique, tandis que le **nom de domaine du fournisseur** est laissé vide.

Figure 23: Détails des flux



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.