RSA NETWITNESS® PLATFORM

Decoder et Log Decoder Guide de configuration

pour la version 11.2

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

Dell estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

mars 2019

Sommaire

Configuration rapide de Decoder et de Log Decoder

Un réseau de base RSA NetWitness® Platform comprend au minimum des Brokers, des Concentrators et des Decoders. Les Brokers agrègent les données à partir des Concentrators et les Concentrators utilisent les données d'au moins un Network Decoder ou Log Decoder. Le réseau de base peut inclure deux types de Decoders. Les Network Decoders sont généralement appelés Decoders et ils capturent les données réseau sous forme de paquets. Les Log Decoders capturent les données de log sous forme d'événements.

L'ajout d'un Decoder le rend visible et disponible pour une utilisation avec NetWitness Platform Administration, Live Services et Investigate. Pour ajouter un service dans NetWitness Platform, vous sélectionnez le type de service, fournissez les informations de connexion au service et confirmez que le service est accessible. Le *Guide de mise en route des hôtes et des services* fournit les informations dont vous avez besoin pour comprendre et installer tous les services NetWitness Platform.

Lorsque tous les services sont ajoutés, vous devez configurer chaque service. Voici l'ordre de préférence pour configurer votre système :

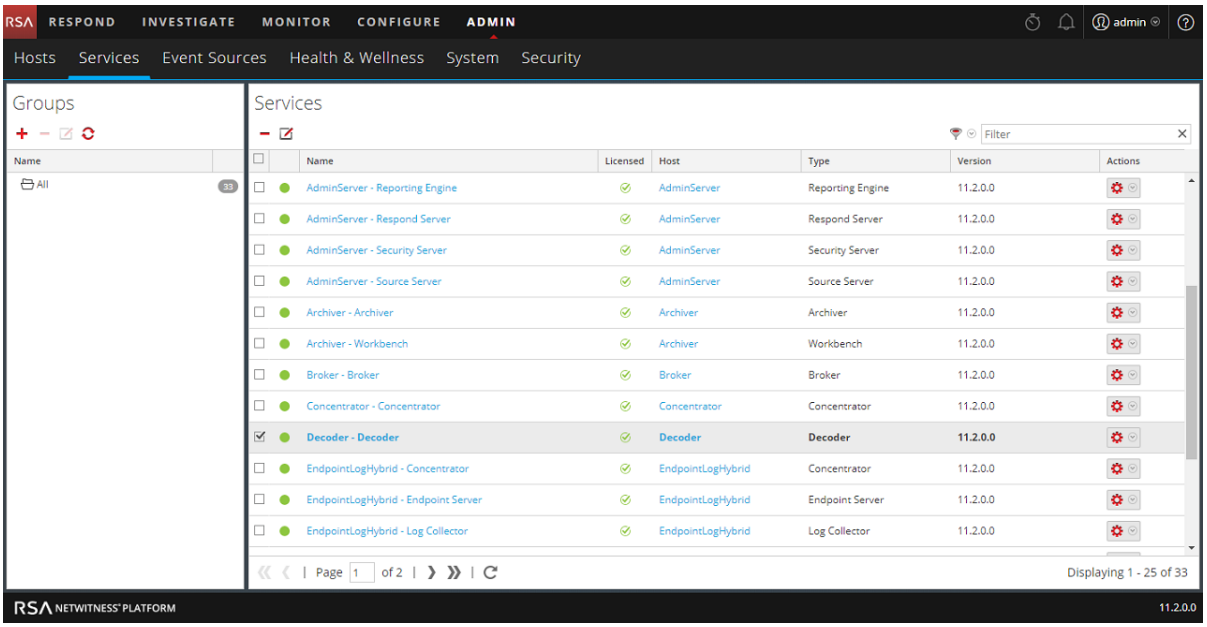
1. Decoders
2. Log Decoders
3. Concentrators (reportez-vous au *Guide de configuration de Broker et Concentrator*)
4. Brokers (reportez-vous au *Guide de configuration de Broker et Concentrator*)

Remarque : Un Log Decoder est un type particulier de Decoder qui est configuré et géré de manière équivalente. La plupart des informations de cette section se rapportent aux deux types de Decoders. « Decoder » fait référence à ces deux types de Decoders. Les informations qui s'appliquent exclusivement aux Network Decoders ou Log Decoders sont clairement identifiées.

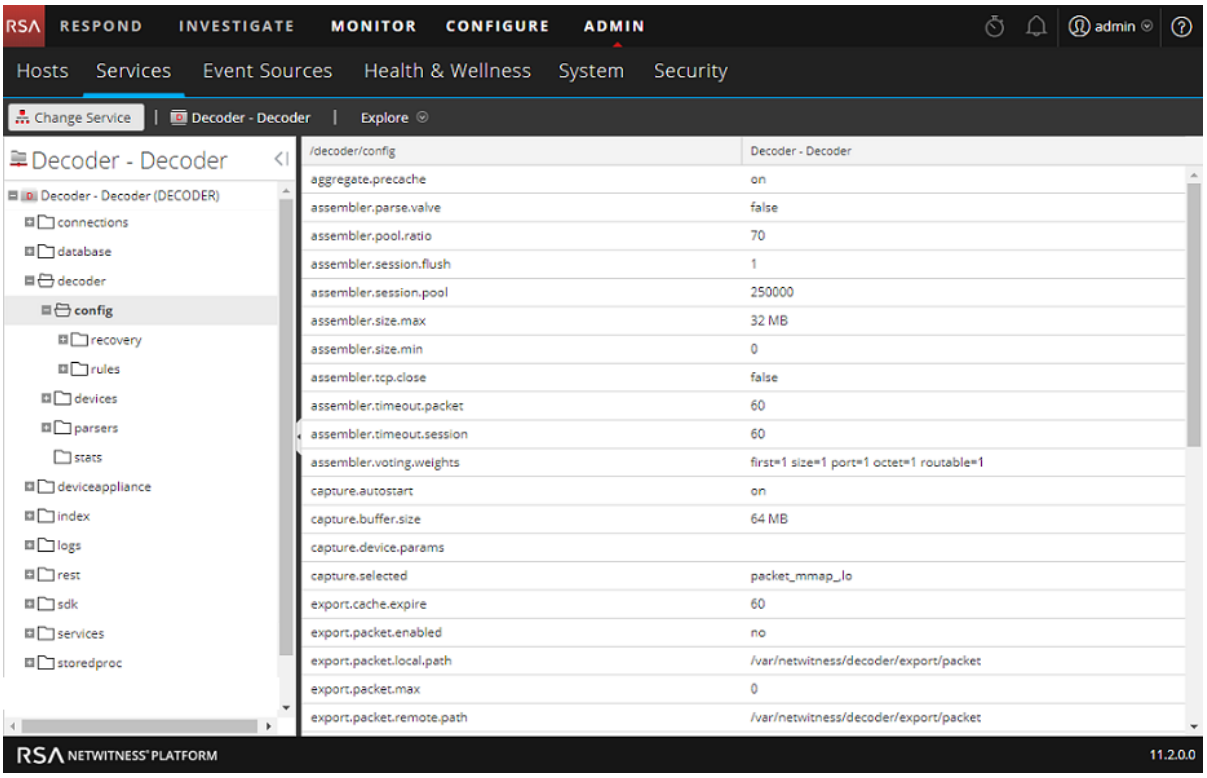
La Configuration de base du Decoder implique la sélection d'une interface de carte réseau et le démarrage de la capture des données.

En outre, vous pouvez configurer chaque Decoder pour contrôler le type de trafic capturé à l'aide de règles, feeds et analyseurs. Les tâches de configuration avancées permettent des fonctions supplémentaires qui correspondent à des applications spécifiques. Par exemple, configurer un 10G Decoder, créer des clés méta personnalisées ou déchiffrer les paquets entrants.

Le moyen le plus simple de configurer tous les paramètres requis pour le Decoder et Log Decoder est d'utiliser les options dans l'interface utilisateur NetWitness Platform. Pour l'essentiel, la configuration s'effectue dans le Vue Services d'administration (ADMIN > Services).



Les administrateurs qui préfèrent travailler en dehors de l'interface utilisateur peuvent configurer les paramètres de base ainsi que les paramètres avancés en modifiant les nœuds de la base de données dans l'arborescence des nœuds Decoder à l'aide de la Vue Explorer les services.

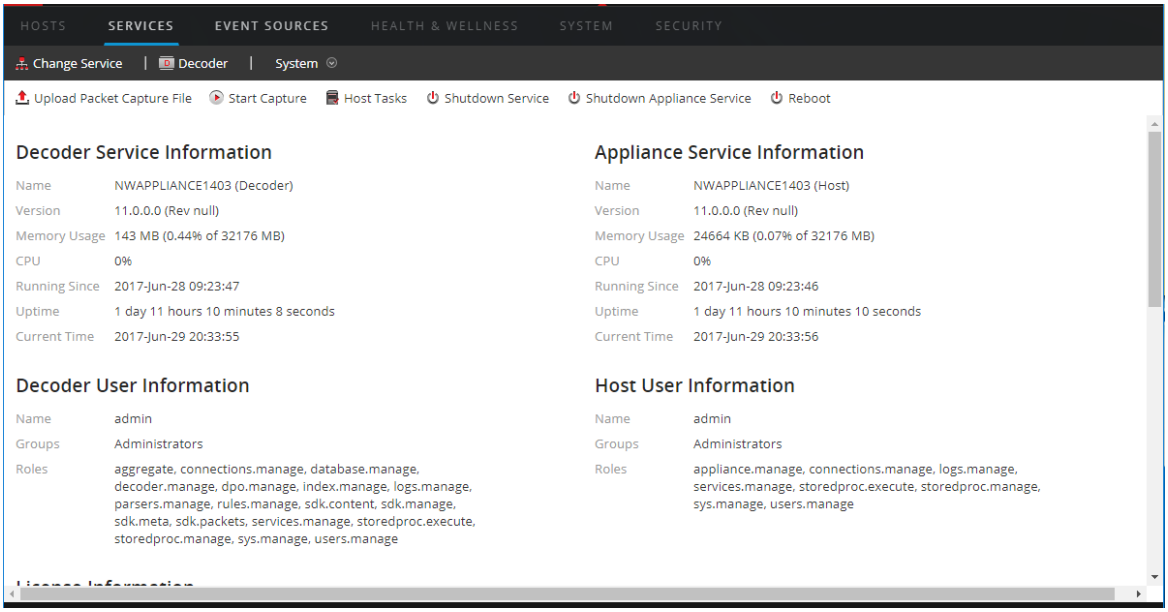


Effectuer la configuration initiale rapide

Cette procédure permet de réaliser la configuration initiale basique d'un Decoder, et lance la capture de données. Lorsque la configuration de base est terminée, le Decoder commence à capturer les données pour le Concentrator.

Pour configurer un Decoder et démarrer la capture des données :

1. Attribuer une interface réseau pour capturer des données. Pour plus d'informations, consultez la section « Sélectionner une carte réseau » dans Configurer les paramètres de capture.
2. Exécutez l'une des opérations suivantes :
   a. Pour démarrer la capture, sélectionnez le Decoder et > **Vue** > **Système**. Dans la barre d'outils, cliquez sur Start Capture .



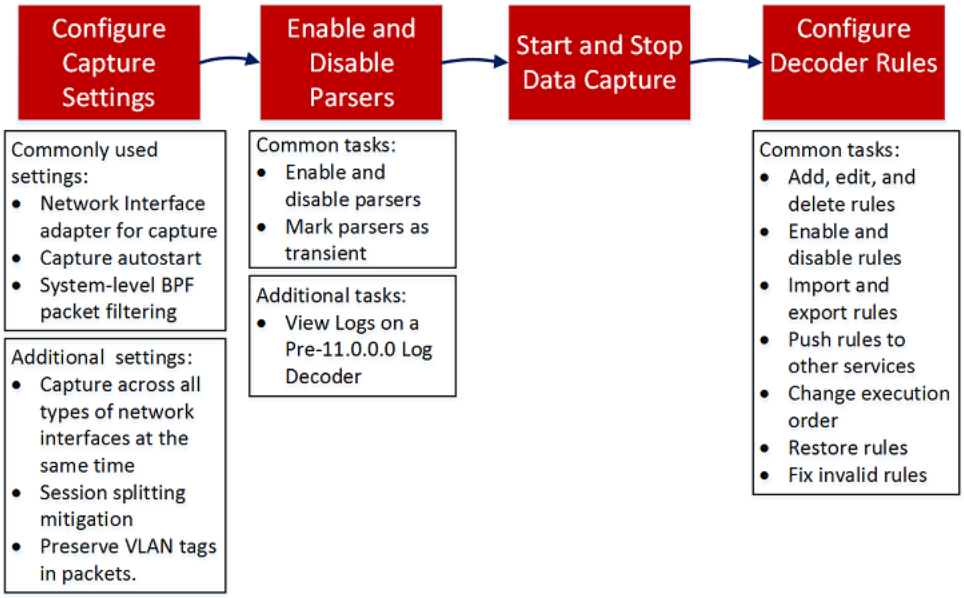
   b. Pour activer le démarrage automatique de la capture, reportez-vous à la section « Configurer un Decoder pour commencer automatiquement la capture des données » dans Configurer les paramètres de capture.
   Le Decoder commence à capturer les données pour leur utilisation par un Concentrator. Pour obtenir des options de configuration supplémentaires, reportez-vous à la section Configurer les paramètres communs sur un Decoder et Procédures supplémentaires de Decoder et Log Decoder

Configurer les paramètres communs sur un Decoder

Cette section présente les paramètres de configuration couramment utilisées sur un Decoder avec des procédures et des informations générales. Après avoir terminé la Configuration rapide de Decoder et de Log Decoder, vous pouvez affiner votre configuration à l'aide d'analyseurs, de feeds et de règles afin de limiter les données capturées.

Remarque : Un Log Decoder est un type particulier de Decoder qui est configuré et géré de manière équivalente. La plupart des informations de cette section se rapportent aux deux types de Decoders. « Decoder » fait référence à ces deux types de Decoders. Les informations qui s'appliquent exclusivement aux Network Decoders ou Log Decoders sont clairement identifiées.

Le workflow suivant illustre les paramètres les plus utilisés et décompose le processus de configuration en quatre étapes.

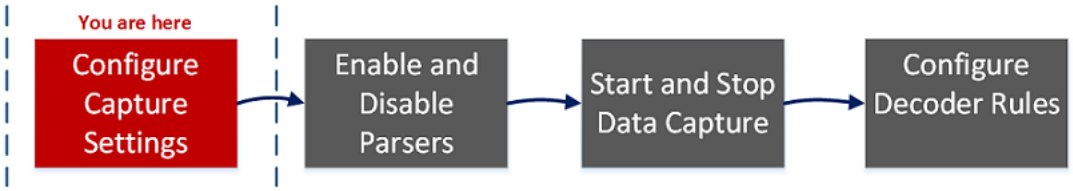


Étape de configuration	Description
Configurer les paramètres de capture	Lors de la configuration initiale du Decoder, la configuration de l'interface de carte réseau est obligatoire. Des paramètres supplémentaires de capture (facultatifs) sont disponibles. Le Démarrage automatique de la capture est l'un de ces paramètres fréquemment utilisés.
Activer et désactiver les analyseurs et les analyseurs de logs	Affichez les analyseurs qui ont été téléchargés et déployés depuis Live et gérez ceux qui sont activés ou désactivés.

Étape de configuration	Description
Démarrer et arrêter la capture de données	Lorsqu'un Decoder démarre, il commence automatiquement à agréger des données si le démarrage automatique de capture est activé. Lorsque le démarrage automatique n'est pas activé, vous pouvez démarrer et arrêter la capture de données manuellement.
Configurer les règles de Decoder	Les règles de capture peuvent ajouter des alertes ou des informations contextuelles aux sessions ou aux logs. Elles peuvent également définir les données qui sont filtrées par un Decoder ou un Log Decoder. Par défaut, aucune règle de capture n'est définie lors de la première configuration de NetWitness Platform. À moins que des règles ne soient spécifiées et qu'elles soient valides, les paquets ne sont pas filtrés. Vous pouvez déployer les dernières règles à partir de Live, comme décrit dans le *Guide de gestion des Services Live*. Vous pouvez définir des règles de capture à tout moment, et vous pouvez définir des règles qui utilisent une syntaxe non valide (Corriger les règles contenant une syntaxe non valide).

Configurer les paramètres de capture

Lors de la configuration initiale du Decoder, la configuration de l'interface de carte réseau est obligatoire. Des paramètres supplémentaires de capture (facultatifs) sont disponibles. En voici deux fréquemment utilisés : le filtre BPF (Berkley Packet Filter) et le Démarrage automatique de la capture.



Outre la configuration basique de l'interface de l'adaptateur réseau, vous pouvez décider d'utiliser l'une des configurations spéciales décrites dans (Facultatif) Conserver les balises VLAN lors de l'Interface de Capture de paquet MMAP ou (Facultatif) Configurer un Decoder pour capturer les données sur tous les types d'interfaces réseau

Les autres paramètres de capture présentent des valeurs par défaut choisies pour leur efficacité dans la plupart des cas (voir la liste détaillée dans Vue Configuration des services - onglet Général). Vous pouvez les modifier dans certaines circonstances, par exemple, si le support client le conseille. Vous pouvez modifier les paramètres de capture à tout moment.

Sélectionner une carte réseau

Le tableau ci-dessous décrit les paramètres de carte réseau pour un Decoder. L'administrateur système configure les cartes réseau par défaut lorsque le Decoder est installé. Consultez votre administrateur système pour plus d'informations.

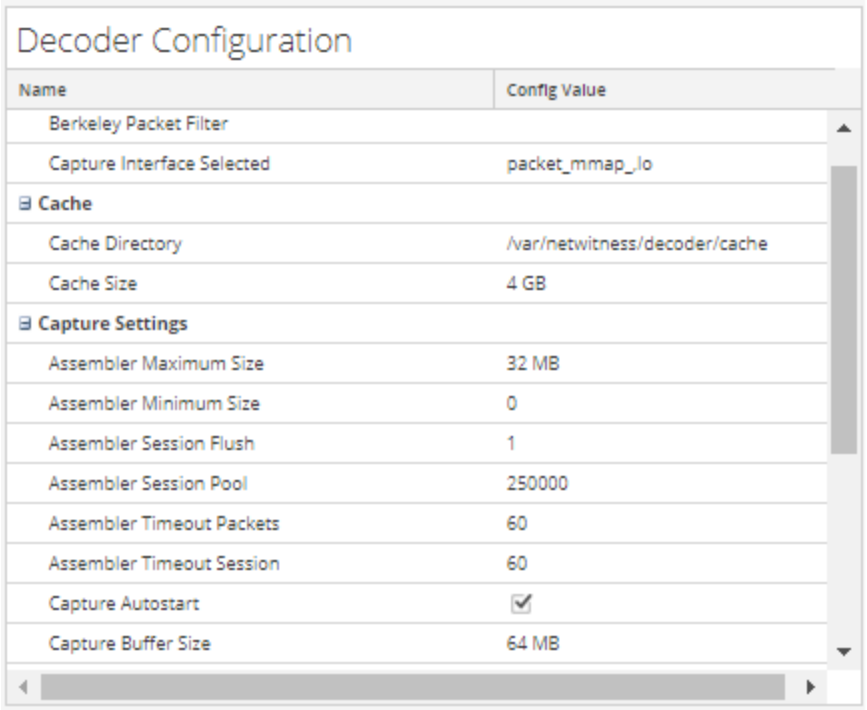
Paramètre d'adaptateur	Description
Berkley Packet Filter	Les filtres BPF (Berkeley Packet Filters) sont appliqués au flux des paquets avant que ces derniers ne soient copiés vers l'adaptateur Decoder à des fins d'analyse. Cela permet d'abandonner efficacement le trafic indésirable. Toutefois, les paquets ignorés ne sont pas comptabilisés dans les statistiques de Decoder (taux de capture, paquets abandonnés, paquets filtrés et total des paquets).

Paramètre d'adaptateur	Description
Interface de capture sélectionnée	Sélectionnez l'adaptateur utilisé par Decoder pour capturer les paquets. Pour l'interface de capture interne à vitesse réduite, utilisez l'adaptateur `packet_mmap_,7,eth1` , qui correspond au port du moniteur situé sur la carte mère. Il existe six ports de capture supplémentaires : • `packet_mmap_,1,lo (bpf)` • `packet_mmap_,2,eth2 (bpf)` • `packet_mmap_,3,eth3 (bpf)` • `packet_mmap_,4,eth4 (bpf)` • `packet_mmap_,5,eth5 (bpf)` • `packet_mmap_,8,ALL (bpf)` Trois services de capture sans fil sont disponibles : • `packet_netmon_ (Microsoft Netmon)` • `packet_mac80211_ (Linux mac80211)` • `packet_airport_ (Mac OS X AirPort)`
Interface de capture sélectionnée pour Log Decoder	Le service de capture suivant est disponible : • `log_events,Log Events`

Pour configurer la carte réseau sur un Decoder :

1. Accédez à **ADMIN > Services**.

2. Dans la **Vue Services d'administration**, sélectionnez le Decoder et > **Vue** > **Config.**
   La Vue Configuration des services s'ouvre sur l'onglet Général.

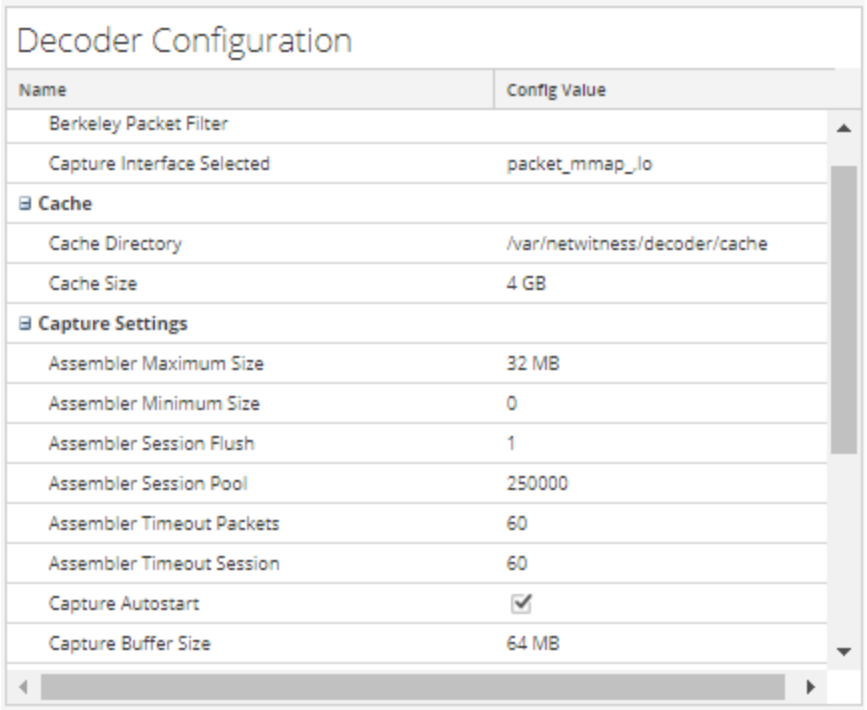


3. Dans le champ **Interface de capture sélectionnée**, sélectionnez la carte réseau qui répond le mieux au Decoder.
4. Pour enregistrer les modifications, cliquez sur **Appliquer**.
5. Si vous devez appliquer les modifications, revenez à la **Vue Services d'administration**, sélectionnez le Decoder, puis sélectionnez > **Redémarrer**.

Configurer un Decoder pour commencer automatiquement la capture des données

1. Accédez à **ADMIN** > **Services**.

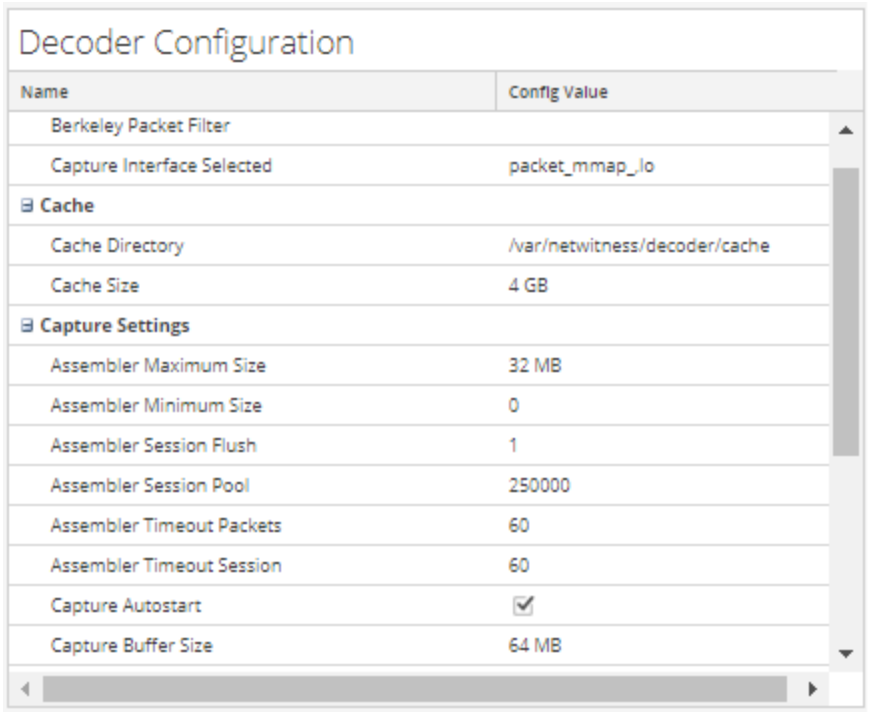
2. Dans la **Vue Services d'administration**, sélectionnez le Decoder et > **Vue** > **Config.**
La Vue Configuration des services s'ouvre sur l'onglet Général

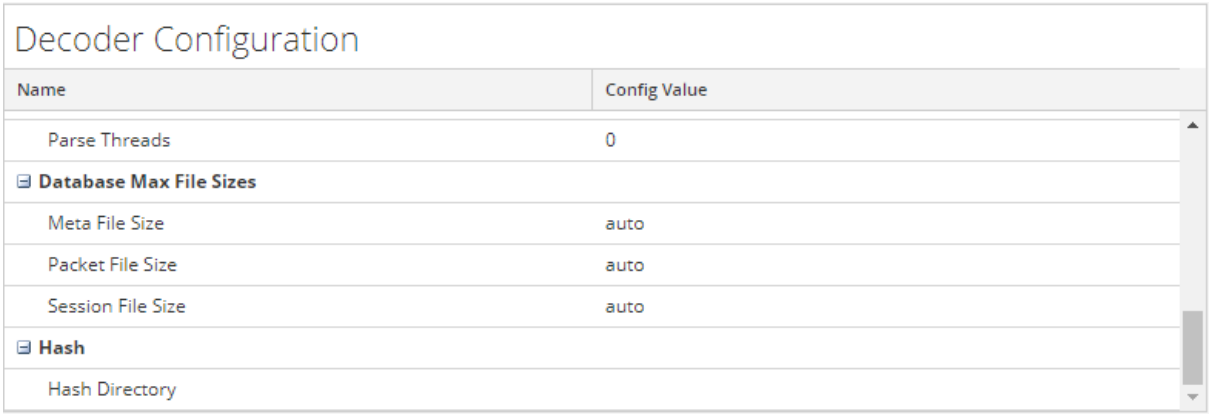


3. Sous **Paramètres de capture**, sélectionnez la case à cocher **Démarrage automatique de la capture**.
4. Pour enregistrer les modifications, cliquez sur **Appliquer**.
5. Si vous devez appliquer les modifications, revenez à la **Vue Services d'administration**, sélectionnez le Decoder, puis sélectionnez > **Redémarrer**.

Configurer les paramètres de capture factultatifs

1. Accédez à **ADMIN** > **Services**.
2. Dans la **Vue Services d'administration**, sélectionnez le Decoder et > **Vue** > **Config.**
La Vue Configuration des services s'ouvre sur l'onglet Général.





3. Si vous souhaitez appliquer un filtre au niveau du système dans le flux de paquets avant que les paquets ne soient copiés vers la carte du Decoder pour l'analyse, configurez le filtre Berkeley Packet Filter, comme décrit dans la section (Facultatif) Configurer le filtrage de paquets BPF au niveau du système.
4. Dans les sections **Paramètres de capture**, vérifiez les valeurs par défaut. Lorsque vous ajoutez un service pour la première fois, les valeurs par défaut sont en vigueur et doivent être modifiées uniquement dans des circonstances particulières, par exemple, si le support client conseille une modification. Reportez-vous à la section Vue Configuration des services - onglet Général pour une description de ces paramètres.
5. Dans la section **Tailles de fichier maximales de la base de données**, vérifiez les valeurs par défaut. Lorsque vous ajoutez un service pour la première fois, les valeurs par défaut sont en vigueur et doivent être modifiées uniquement dans des circonstances particulières, par exemple, si le support

client conseille une modification. Reportez-vous à la section Vue Configuration des services - onglet Général pour une description de ces paramètres.

6. Dans la section **Hachage**, définir un répertoire pour les fichiers de hachage si vous utilisez cette fonction. Reportez-vous à la section Vue Configuration des services - onglet Général pour une description de ces paramètres.

(Facultatif) Configurer le filtrage de paquets BPF au niveau du système

Vous pouvez utiliser les BPF (Berkeley Packet Filter) pour contrôler les paquets et les logs qui sont traités par un Decoder.

Les filtres BPF (Berkeley Packet Filters) sont appliqués au flux des paquets avant que ces derniers ne soient copiés vers l'adaptateur Decoder à des fins d'analyse. Cela permet d'abandonner efficacement le trafic indésirable. Ces paquets ignorés ne sont pas comptabilisés dans les statistiques de Decoder (taux de capture, paquets abandonnés, paquets filtrés et total des paquets).

Decoder prend également en charge le filtrage des paquets au niveau système, défini à l'aide de la syntaxe `tcpdump/libpcap`. En spécifiant un filtre `Libpcap`, vous pouvez réduire efficacement le volume des paquets en fonction des attributs de la couche 2 à la couche 4. Un filtre `Libpcap` s'avère approprié lorsqu'un Decoder reçoit un volume de trafic qui augmente la charge des ressources physiques de la plateforme. Dans ce scénario, le Decoder peut abandonner les paquets de manière régulière et disposer d'un grand nombre de pages de capture (`/decoder/stats/capture.pagefree` est élevé). Ce qui suit est un exemple de filtre `libpcap` qui garde uniquement les paquets n'ayant pas à la fois une adresse source et une adresse de destination dans le sous-réseau 10.21.0.0/16.

```
not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)
```

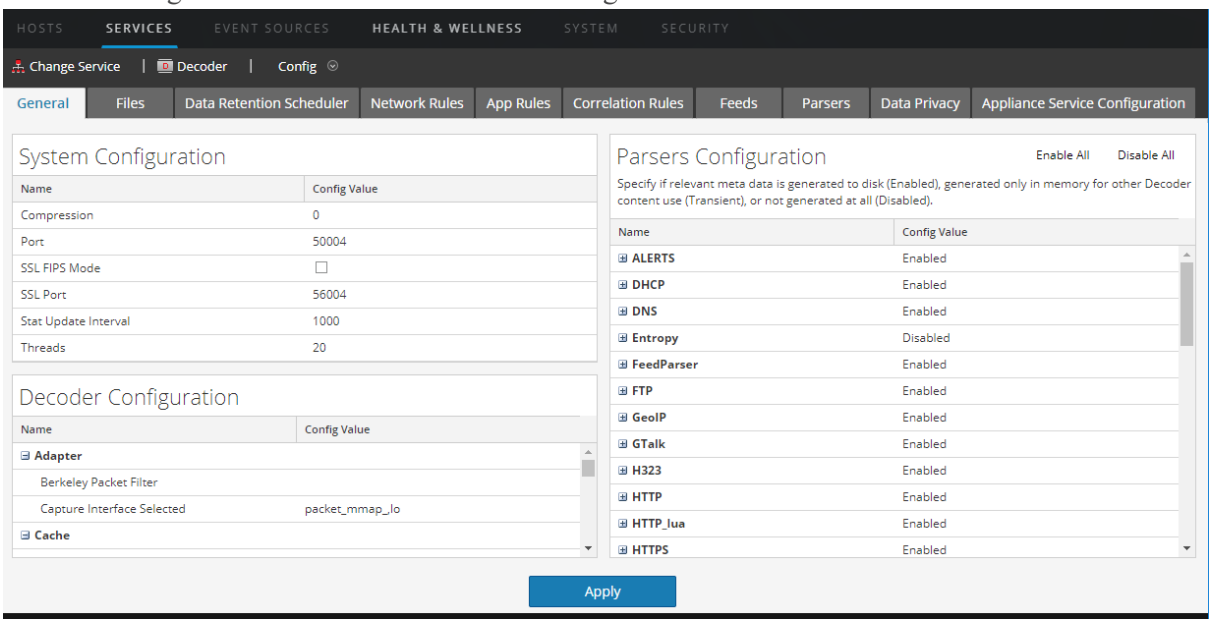
Pour une référence complète de la syntaxe du filtre `Libpcap`, consultez les pages principales :

- tcpdump (http://www.tcpdump.org/tcpdump_man.html).
- pcap-filter (http://www.unix.com/manpage/FreeBSD/7/pcap-filter/).

Pour ajouter un filtre de paquets Berkeley niveau système :

1. Accédez à **ADMIN > Services.**
2. Dans la Vue Services d'administration, sélectionnez un service Decoder et **> Vue > Configuration.**

La Vue Configuration des services s'ouvre sur l'onglet Général.



3. Dans la **Section Configuration de Decoder**, sous **Adaptateur**, cliquez dans le champ en regard de **Filtre de paquets Berkeley**.
4. Saisissez un seul filtre dans le champ. Si vous voulez filtrer plusieurs éléments, associez plusieurs expressions en utilisant `and`. Plusieurs exemples sont fournis ci-dessous.
   L'interface utilisateur valide l'entrée au moment où vous saisissez votre chaîne de filtre.
5. Pour enregistrer le filtre, cliquez sur **Appliquer**.
   Si la syntaxe est correcte, un message de confirmation s'affiche.
   Si la syntaxe est incorrecte, un message **Filtre de paquets non valide** s'affiche et un message de log correspondant suivra dans les messages de log sur le Decoder :
   ```
   164474800 2015-May-01 19:03:08 warning Decoder Failed to parse filter 'example_badrule': syntax error
   ```
6. Pour activer le filtre, vous devez arrêter et démarrer la capture sur le Decoder :
   a. Remplacer la vue **Config** par la vue **Système**.
   b. Cliquez sur **Arrêter la capture**.
   c. Cliquez sur **Démarrer la capture**.
      Le filtre actif s'affichera dans les logs Decoder.

Exemples

Voici plusieurs exemples de filtres :

- Abandonner des paquets vers ou depuis toute adresse dans le sous-réseau 10.21.0.0/16 :
  ```
  not (net 10.21.0.0/16)
  ```

- Abandonner des paquets associés à la fois à des adresses source et destination dans le sous-réseau 10.21.0.0/16 :
  `not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`
- Abandonner des paquets venant de 10.21.1.2 ou se dirigeant vers 10.21.1.3.
  `not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Associer IP et HOST :
  `not (host 192.168.1.10) and not (host api.wxbug.net)`
- Abandonner tout le trafic port 53, TCP et UDP :
  `not (port 53)`
- Abandonner uniquement le trafic port 53 UDP :
  `not (udp port 53)`
- Abandonner tout trafic de protocole IP 50 (IPSEC) :
  `not (ip proto 50)`
- Abandonner tout trafic sur les ports TCP 133 à 135.
  `not (tcp portrange 133-135`

Les filtres suivants associent certains des susmentionnés pour démontrer comment placer plusieurs directives dans un filtre :

- Abandonner n'importe quel trafic de port 53(DNS) provenant de 10.21.1.2 ou à destination de 10.21.1.3.
  `not (port 53) and not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Abandonner n'importe quel trafic utilisant IP proto 50 ou le port 53 ou tout trafic depuis le net 10.21.0.0/16 destiné au net 10.21.0.0/16
  `not (ip proto 50 or port 53) or not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`

Attention : L'utilisation des parenthèses peut avoir un impact important et potentiellement perturbateur sur l'utilisation des filtres de paquets. Au titre des bonnes pratiques, conservez les opérations « not » en dehors des parenthèses et testez toujours vos règles avant de les déployer. Si vous ne parvenez pas à mettre en forme correctement vos règles (en dépit d'une validation de saisie), un filtre de paquets peut en conséquence abandonner TOUT trafic ou se comporter d'autres manières inattendues. Cela est dû à la manière dont les filtres de paquets `Libpcap` fonctionnent et cela n'est pas le résultat d'une logique au sein du logiciel NetWitness Platform.

Tests

Avant de les mettre en œuvre, et afin de s'assurer qu'ils auront pour résultat le comportement attendu, les filtres BPF peuvent et doivent être testés en utilisant `tcpdump` ou `windump`. Cet exemple illustre un d'un filtre en utilisant windump :

```
windump -nni 2 not (port 53 or port 443) or not (ip proto 50)
```

Conversions

Si à des fins de performance, vous avez décidé qu'un filtre Règle réseau existant s'exécuterait mieux en tant que Filtre de paquets au niveau du système, vous pouvez le convertir. Il y a peu d'éléments à mémoriser lors de la réalisation de conversions.

- `&&` devient `and`
- `ip.addr` devient `host` dans le cas d'un hôte unique ou **net** dans le cas d'un réseau.
- `ip.src` devient `src host` dans le cas d'un hôte unique ou `src net` dans le cas d'un réseau.
- `ip.dst` devient `dst host` dans le cas d'un hôte unique ou `dst net` dans le cas d'un réseau.
- Utilisez la notation CIDR lorsque vous répertoriez un réseau (à savoir, 10.10.10.0/24).
- `||` devient `or`
- `!` devient `not`
- Plusieurs règles doivent être associées à `and`.

Le manuel pour TCPDump donne également des exemples de filtres et de chaînes qui peuvent être utilisés :
http://www.tcpdump.org/tcpdump_man.html

En outre, le site suivant fournit une excellente référence pour les filtres de paquets type BPF :
http://biot.com/capstats/bpf.html

Attention : Si vous capturez des paquets à marquage `vlan`, le filtre BPF standard ci-dessus pourra ne pas fonctionner. Par exemple, si vous utilisez `not (udp port 123)` pour filtrer le trafic NTP à marquage `vlan` sur un port UDP 123, cela ne fonctionnera pas. Cela est dû au fait que le dispositif du filtre BPF est simple et ne prend pas en compte les protocoles non référencés dans la règle. Ainsi, le système d'exploitation exécutant le filtre BPF recherchera les valeurs `udp port` au décalage d'octet auquel elles se produiraient dans un paquet Ethernet/UDP standard ; mais les champs de balise `vlan` en option dans l'en-tête Ethernet pousse ces valeurs de 4 octets, ce qui fait que la règle de filtre BPF va échouer. Pour résoudre ce problème, vous devez remplacer le filtre BPF comme suit : `not (vlan and udp port 123)`.

(Facultatif) Configurer un Decoder pour capturer les données sur tous les types d'interfaces réseau

L'adaptateur `packet_mmap_,ALL` est capable de capturer des données sur tous les types d'interfaces réseau en même temps. Par exemple, cela peut inclure des éléments tels que des interfaces réseau physiques sur différents types de média et des interfaces de tunnel.

Le comportement par défaut de l'adaptateur `ALL` est de capturer les données à partir de toutes les interfaces du système, à l'exception des valeurs par défaut codées en dur de `lo`, `eth0` et `em1`.

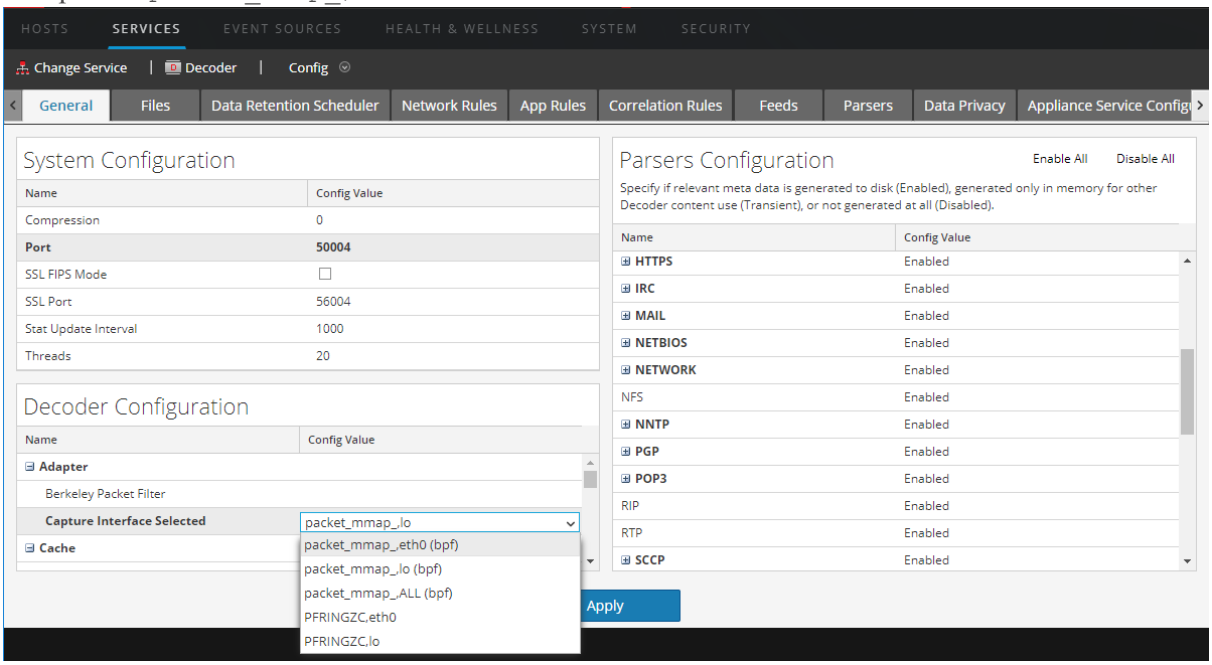
Vous pouvez sélectionner un sous-ensemble d'interfaces de capture en modifiant le nœud de configuration Decoder `/decoder/config/capture.device.params` pour inclure un paramètre `interfaces=`. Le paramètre `interfaces` contient une liste d'interfaces séparées par des virgules qui sont utilisées pour la capture. Au lieu d'utiliser toutes les interfaces pour la capture, seules les interfaces spécifiées sont utilisées.

Par exemple, si vous souhaitez forcer la capture sur les interfaces `em1`, `em2` et `em4`, et ignorer `em3`, vous pouvez sélectionner l'adaptateur `packet_mmap_,ALL`, puis ajouter cette ligne à `capture.device.params` : `interfaces=em1,em2,em4`

Remarque : L'utilisation du paramètre `interfaces` pour sélectionner `eth0`, `lo` ou `em1` permet de remplacer le comportement par défaut qui consiste à interrompre le trafic sur ces ports.

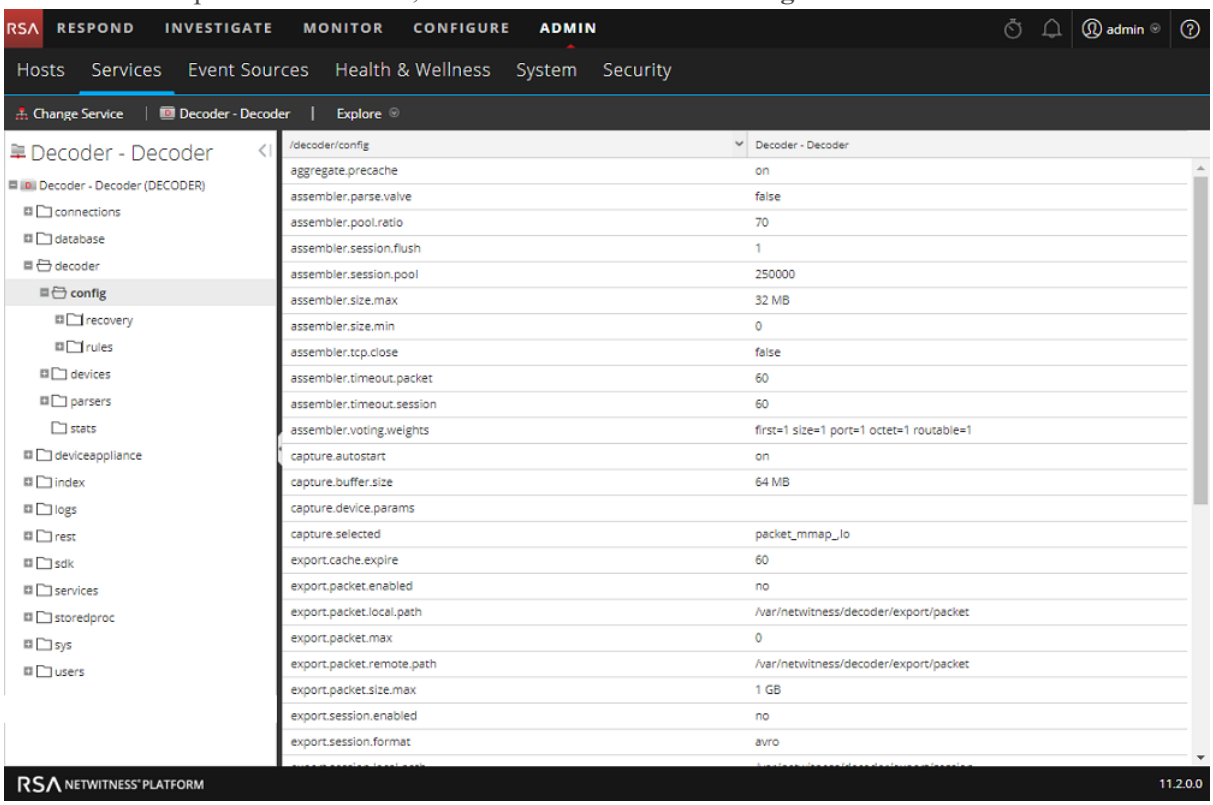
Pour configurer l'adaptateur `packet_mmap_,ALL` pour capturer à partir d'interfaces spécifiques au lieu de toutes les interfaces :

1. Accédez à **ADMIN** > **Services**, sélectionnez le service Decoder, puis > **Vue > Config.**
2. Dans la **Vue Configuration des services**, définissez **Interface de capture sélectionnée** sur l'adaptateur `packet_mmap_,ALL`.

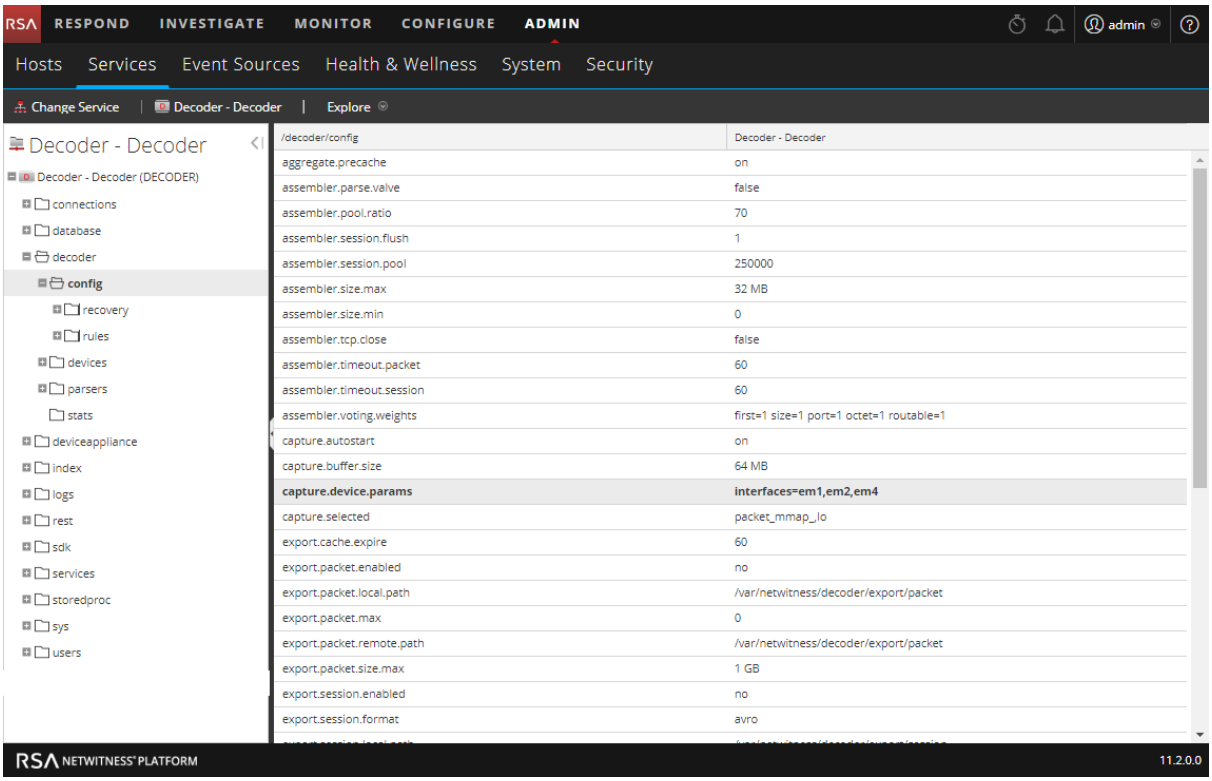


3. Pour accéder à la Vue Explorer les services, cliquez sur **Config** dans la barre d'outils et sélectionnez **Explorer** dans la liste déroulante.

4. Dans la Vue Explorer les services, sélectionnez **decoder** > **config**.



5. Cliquez sur la colonne Valeurs en regard de `capture.device.params`, saisissez **`interfaces=em1,em2,em4`** et appuyez sur **Entrée**.



La modification prend effet immédiatement. Seul le trafic sur les interfaces `em1`, `em2` et `em4` est capturé.

(Facultatif) Configurer un Decoder pour écrire des fichiers au format pcap standard

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.2 ou ultérieure.

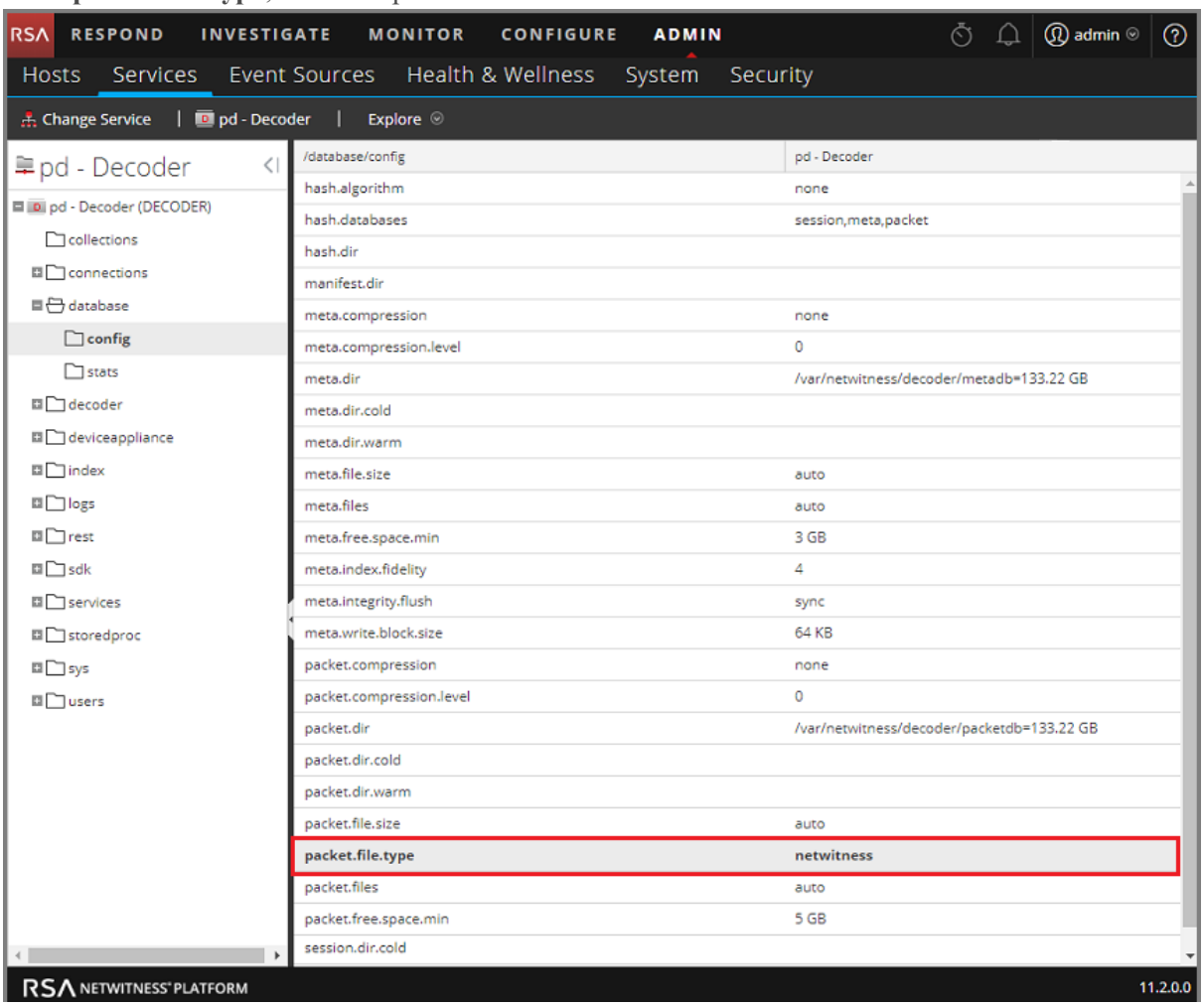
Pour fournir un format de base de données plus ouvert, le Network Decoder peut maintenant écrire des fichiers au format pcap standard. Vous pouvez activer des fichiers de base de données au format pcapng avec le nouveau nœud de configuration :
`/database/config/packet.file.type = 'netwitness' or 'pcapng'`

Remarque : Cette fonctionnalité est activée par défaut si vous installez directement la version 11.2. Si vous effectuez une mise à niveau d'une version précédente vers la version 11.2, vous devez activer manuellement les fichiers de base de données au format pcapng, ce qui peut entraîner une diminution approximative de 4 % de l'espace disque (car les fichiers pcapng requièrent plus d'espace que les fichiers nwdb). Vous pouvez également utiliser le format pcapng avec une capture de 10 Gbps, ce qui ne diminue pas significativement les performances (< 1 %).

Pour activer l'écriture de fichiers au format pcap standard :

1. Accédez à **ADMIN** > **Services**, sélectionnez un service Network Decoder, puis  > **Vue** > **Explorer**.
2. Accédez à **Base de données** > **config**.

3. Dans **packet.file.type**, la valeur par défaut est **netwitness**.



4. Pour modifier le type de fichier de paquet au format standard pcap, saisissez **pcapng**. Cette modification prendra effet immédiatement sur le prochain fichier de paquet créé.

Remarque : Dans le format de fichier de base de données pcapng, les données sont en texte clair et ne sont pas brouillées par notre format propriétaire, ce qui peut améliorer la sécurité.

Attention : Ne modifiez pas les fichiers dans les répertoires de base de données de paquets ! Vous ne devez pas lire ou modifier `pcapng` un fichier dans les répertoires de la base de données de paquets, car ils sont toujours utilisés pendant que Decoder est en cours d'exécution. Decoder attend toujours un accès complet et exclusif à ces fichiers, et d'autres processus lisant ces fichiers empêchent le fonctionnement normal de Decoder. La bonne façon d'accéder aux `pcapng` fichiers est de configurer un répertoire de stockage à froid. Cela permet à Decoder de copier des `pcapng` fichiers dans le répertoire de stockage à froid avant la suppression. À ce stade, vous êtes responsable de la gestion `pcapng` des fichiers, y compris en vous assurant que le volume de stockage à froid ne soit jamais saturé. Gardez à l'esprit que la copie des `pcapng` fichiers dans le stockage à froid nécessite une quantité non négligeable d'I/O et pourrait interférer avec la capture de paquets. Le stockage à froid de `pcapng` n'est pas supporté à des vitesses de 10G.

(Facultatif) Conserver les balises VLAN lors de l'Interface de Capture de paquet MMAP

Lors de la capture de trafic contenant des balises VLAN, vous pouvez configurer l'interface de capture Packet MMAP de sorte que les balises VLAN soient conservées dans les paquets (correction VLAN). Par défaut, le matériel de capture réseau supprime les balises. L'exécution de cette procédure conserve les balises dans les paquets, et les valeurs de celles-ci sont décryptées dans les métadonnées VLAN à des fins d'analyse supplémentaire.

Il existe deux mécanismes permettant la correction VLAN.

- Option 1 : Définissez `vlan-fix=true` dans `capture.device.params`. Cette option exécute la correction des VLAN sur tout le trafic entrant du Decoder. Cette option est appropriée dans la plupart des cas, dans la mesure où l'on suppose que tout le trafic sera balisé VLAN. Ce mécanisme fonctionne soit en mode d'interface unique, soit en mode d'interfaces multiples. Cette option remplace les paramètres de correction VLAN sur toutes les interfaces ; même les interfaces qui ne sont pas configurées pour la correction VLAN auront cette fonction activée.
- Option 2 : Utilisez le paramètre `interfaces` dans `capture.device.params` sur chaque périphérique. Le paramètre `interfaces` accepte une liste séparée par des virgules des noms d'interface sur lesquels vous souhaitez capturer des paquets. En ajoutant `:vlan` à un nom d'interface, vous pouvez activer la correction VLAN sur toutes les interfaces. Si l'interface ne dispose pas du suffixe `:vlan` ajouté, elle n'effectuera pas la correction VLAN.

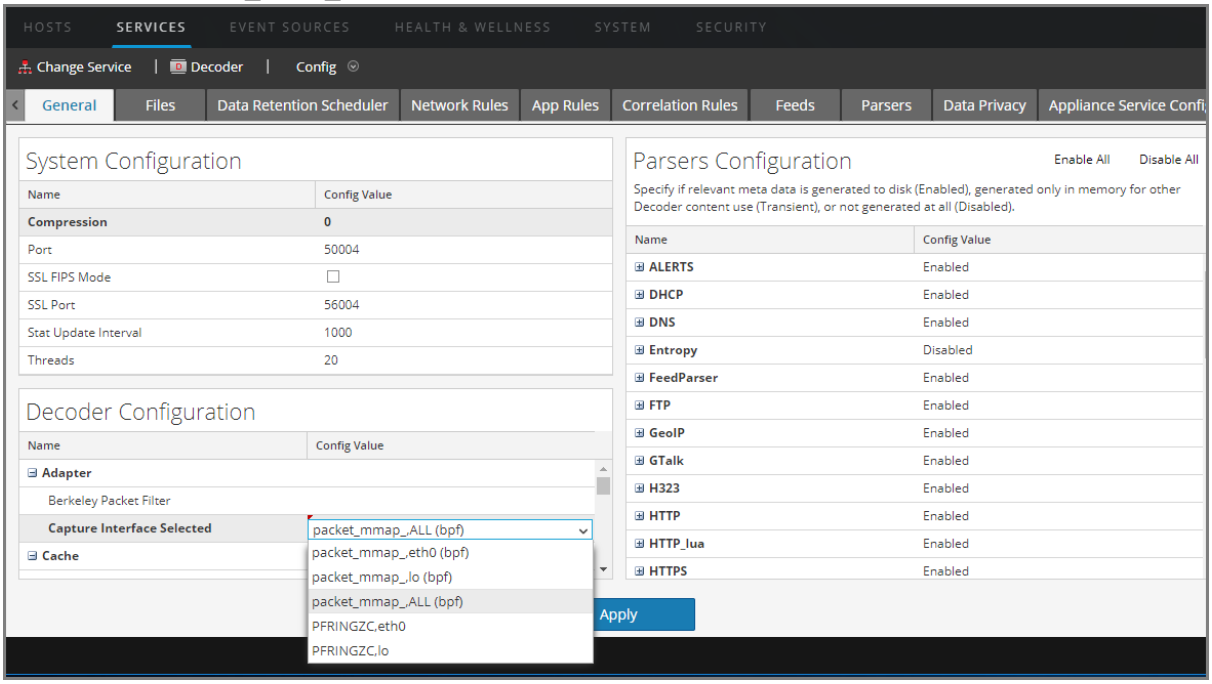
Après avoir modifié ce paramètre, vous devez redémarrer la capture sur le Decoder afin que les modifications apportées à `capture.device.params` prennent effet.

Exemples `vlan` de ces deux options. Si vous devez passer plusieurs paramètres pour `capture.device.params`, utilisez la syntaxe suivante. Notez que les guillemets sont nécessaires pour les valeurs contenant des espaces. Reportez-vous à la section *Guide d'optimisation de la base de données Core*.
`name1="value1" name2="value2"`.

Paramètre	Valeur	Effet
`capture.device.params`	`vlan-fix=true`	Correction VLAN toujours effectuée sur toutes les interfaces. La valeur par défaut est `vlan-fix=false`.
`capture.device.params`	`interfaces=eth0:vlan,eth1`	Correction VLAN effectuée sur la capture du trafic sur l'interface `eth0` uniquement
`capture.device.params`	`interfaces=eth0:vlan,eth1 vlan-fix=true`	Correction VLAN toujours effectuée, car le paramètre `vlan-fix` remplace le paramètre des interfaces.

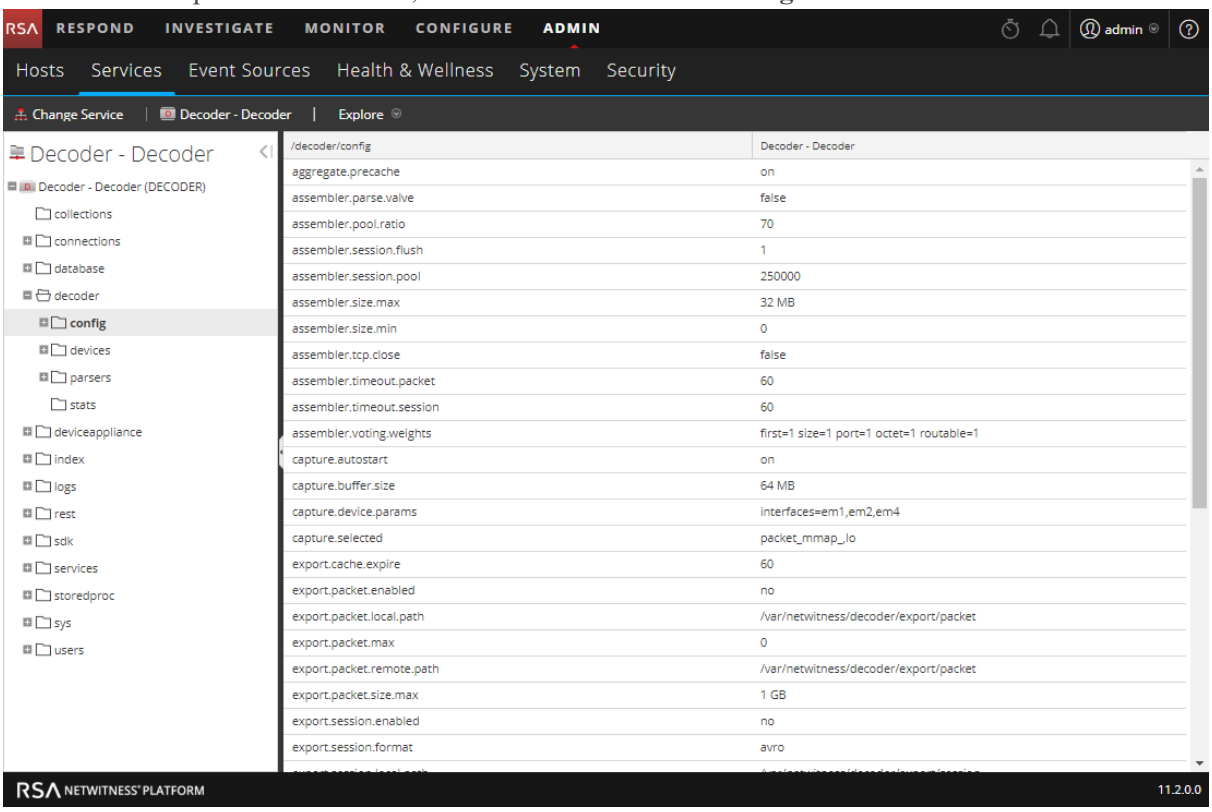
Pour configurer l'adaptateur `packet_mmap_` pour conserver les balises VLAN des paquets :

1. Dans la **Vue Services d'administration**, sélectionnez le service Decoder et **> Vue > Config.**
2. Dans la **Vue Configuration des services**, définissez **Interface de capture sélectionnée** sur l'adaptateur `packet_mmap_,ALL`.



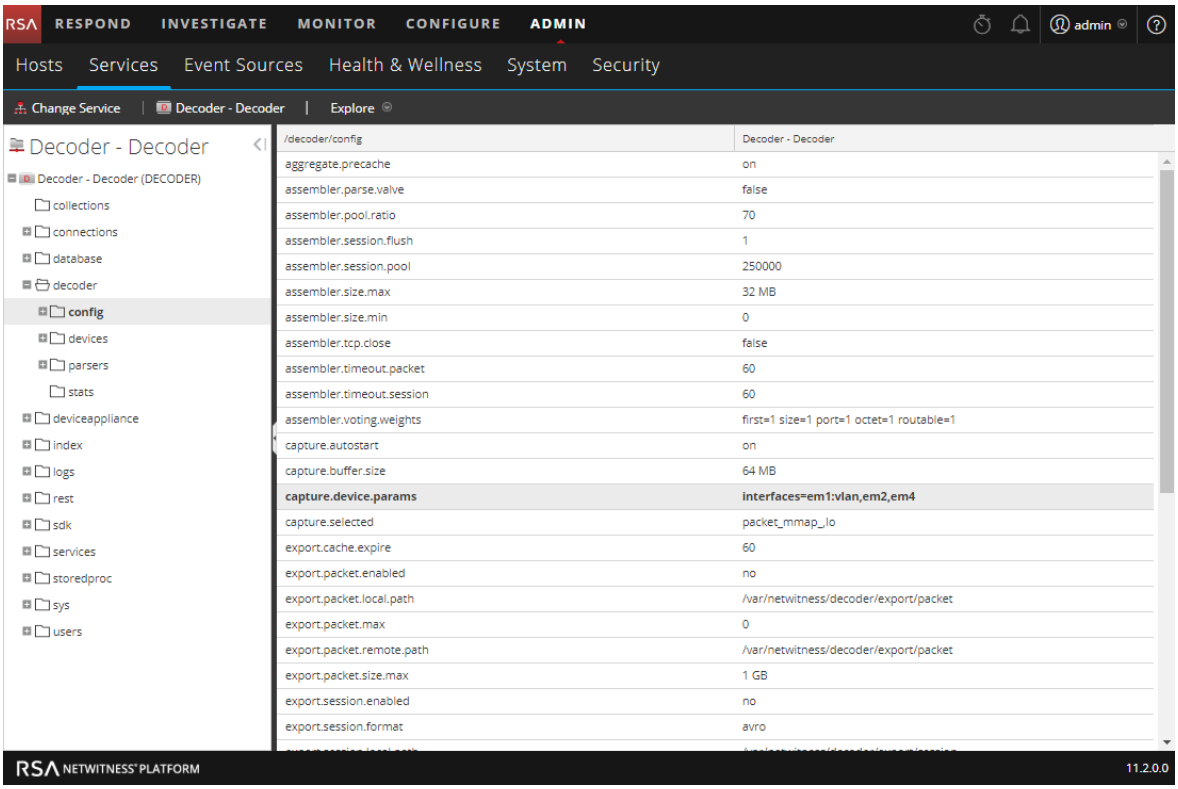
3. Pour accéder à la Vue Explorer les services, cliquez sur **Config** dans la barre d'outils et sélectionnez **Explorer** dans la liste déroulante.

4. Dans la Vue Explorer les services, sélectionnez **decoder** > **config**.



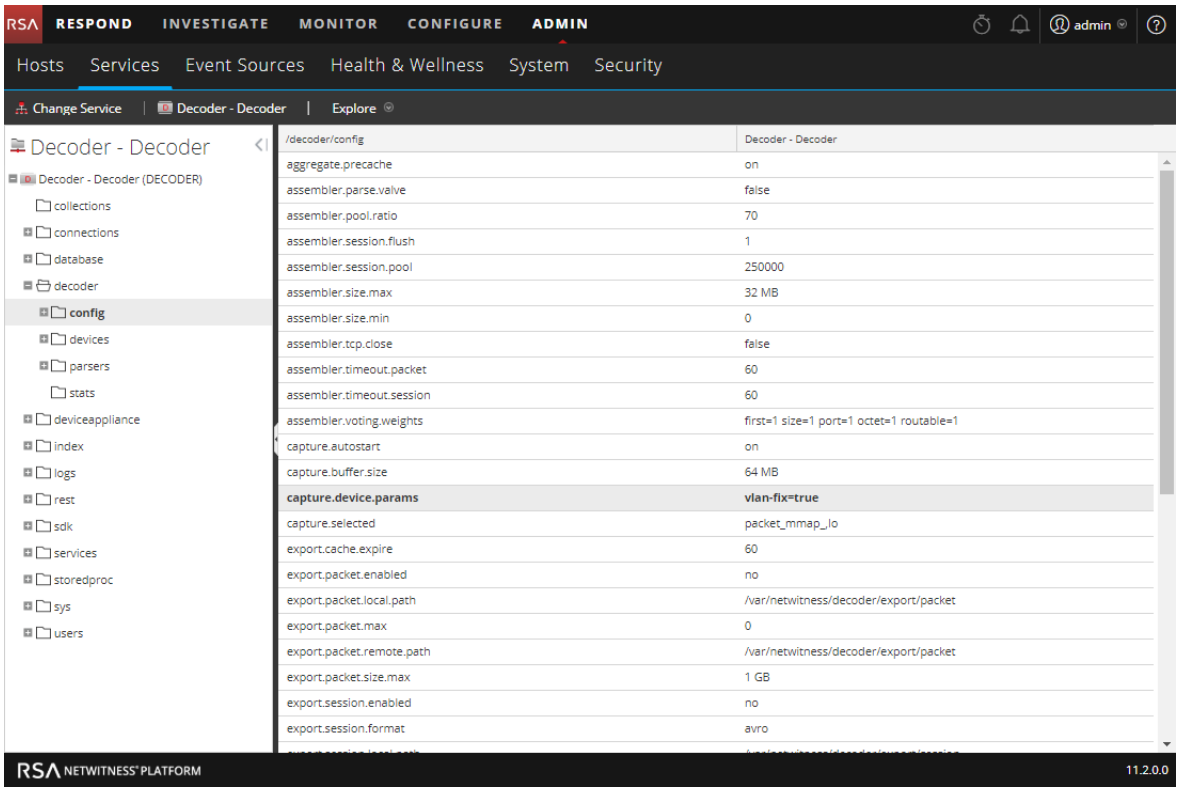
5. Cliquez sur la colonne des valeurs en regard de `capture.device.params`, puis effectuez l'une des options suivantes :

   - Pour préserver les balises VLAN d'une interface dans la liste d'interfaces, ajoutez **`:vlan`** après le nom de l'interface et appuyez sur **Entrée**. Par exemple, cela indique que les balises VLAN sont conservées sur `em1`, mais pas sur `em2` et `em4` :
     `interfaces=em1:vlan,em2,em4`



La modification prend effet immédiatement. Seul le trafic sur `em1` voit les balises VLAN conservées.

- Pour conserver les balises VLAN sur toutes les interfaces, saisissez les valeurs suivantes et appuyez sur **Entrée** :
  `vlan-fix=true`

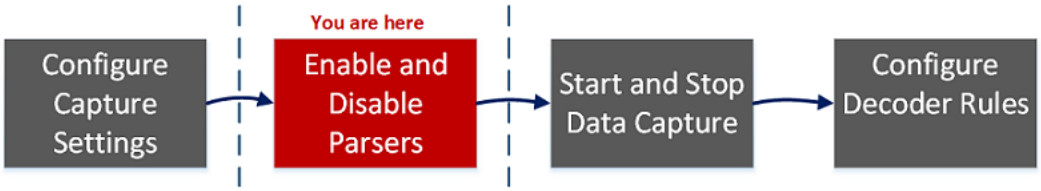


La modification prend effet immédiatement ; les balises VLAN sont conservées sur toutes les interfaces de capture.

Activer et désactiver les analyseurs et les analyseurs de logs

Les administrateurs peuvent voir les analyseurs qui ont été téléchargés à partir de Live et déployés sur un Decoder ou Log Decoder, voir parmi ces analyseurs ceux qui ont été activés, et activer ou désactiver des analyseurs et analyseurs de logs.

La figure suivante illustre les paramètres les plus utilisés sur un Decoder. Pour une configuration de base rapide avec uniquement les étapes à suivre, reportez-vous à la section Configuration rapide de Decoder et de Log Decoder.



Vous devez télécharger et déployer uniquement les analyseurs dont vous avez besoin pour les raisons suivantes :

- Il y a un impact sur les performances car vous augmentez le nombre d'analyseurs déployés.
- Plus vous déployez d'analyseurs, plus vous créez de métadonnées, ce qui influe sur la conservation des données.
- Le fait de ne pas avoir déployé d'analyseurs de logs supplémentaires (inutiles) réduit le risque de mauvaise interprétation des messages.

Le panneau Configuration des analyseurs vous permet de sélectionner les parsers à utiliser dans Decoder. Dans certains parsers, vous pouvez également configurer les métadonnées créées par le parser. Voici les options du panneau Configuration des analyseurs.

Option	Description
Activer tout Désactiver tout	Ces options donnent la possibilité de sélectionner rapidement la totalité des parsers ou aucun d'entre eux.
Nom	Noms des parsers disponibles pour Decoder. Le signe plus indique que les métadonnées générées par l'analyseur sont configurables. Lorsque vous cliquez sur le signe plus, les métadonnées que l'analyseur peut créer s'affichent.

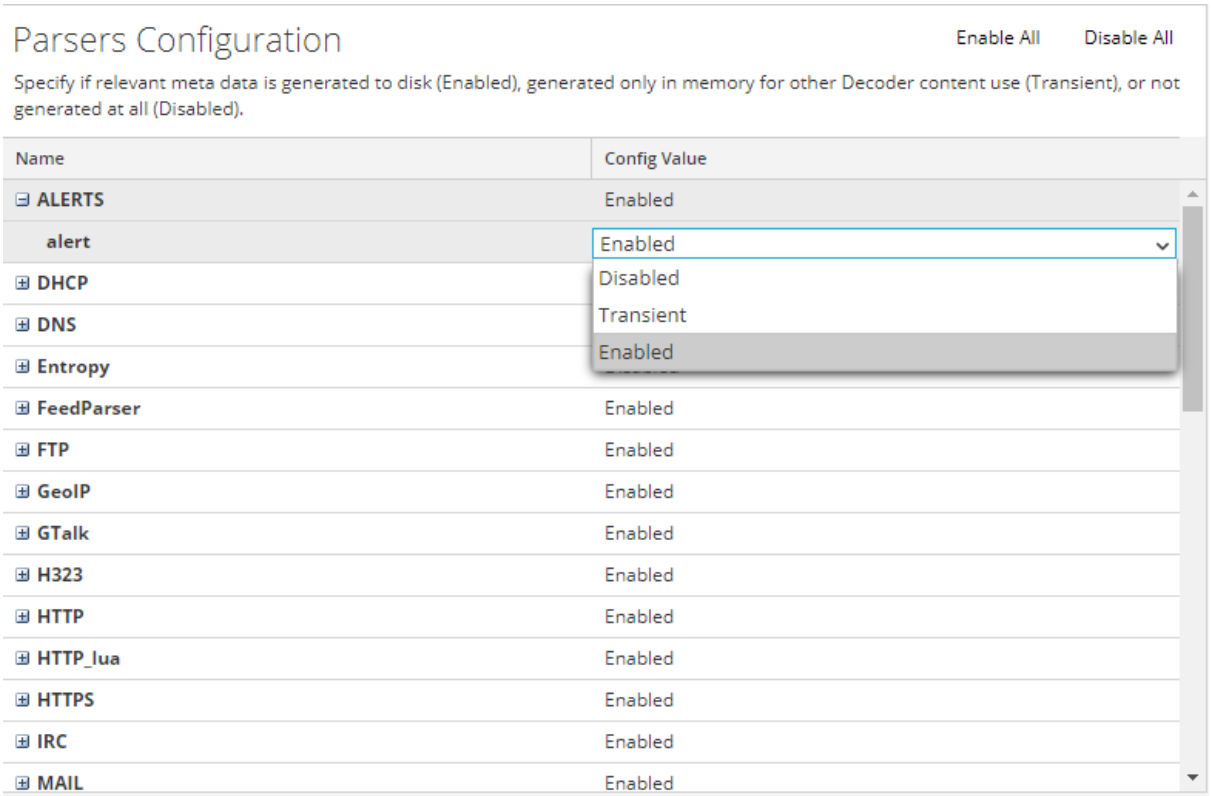
Option	Description
Valeur de configuration	Une liste déroulante vous permet de modifier la configuration du parser ou des métadonnées via les options **Activé**, **Désactivé** ou **Transitoire**. • Lorsque l'option est **Activé**, le Decoder utilise le parser pour filtrer le trafic. • Lorsque l'option est **Transitoire**, le Decoder utilise le parser pour filtrer le trafic. Les métadonnées générées ne sont pas stockées sur disque. Les métadonnées transitoires sont disponibles en mémoire pour le contenu supplémentaire (parsers, flux et règles d'application) sur ce Decoder. Cela permet aux administrateurs de protéger certaines données. Elles sont généralement mises en œuvre dans le cadre d'un plan de confidentialité des données (reportez-vous au *Guide de gestion de la confidentialité des données*). • Lorsque l'option est **Désactivée**, le Decoder n'utilise pas le parser. Si les métadonnées générées pour le parser sont configurables, le fait de cliquer sur le signe plus pour développer les parsers entraîne l'affichage des clés méta configurables. La même liste déroulante sélectionne la clé méta que le parser va créer.

Remarque : Pour un Log Decoder, vous devez avoir déjà déployé des analyseurs de log depuis Live. Consultez la rubrique **Trouver et déployer des ressources Live** dans *Gestion des services Live* pour obtenir plus d'informations. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Pour activer ou désactiver un analyseur, ou pour afficher l'état de chaque analyseur :

1. Accédez à**ADMIN** > **Services**.
2. Dans la **Vue Services d'administration**, sélectionnez un Log Decoder ou un Decoder, puis  **>Vue** > **Config**.

3. Dans le panneau **Configuration des analyseurs**, recherchez l'analyseur du Decoder ou l'analyseur de source d'événement du Log Decoder.



4. Dans la colonne **Valeur de configuration**, notez l'état actuel de votre analyseur.

   Vous pouvez mettre à jour l'état de tout analyseur individuel en sélectionnant sa **Valeur de configuration** et en sélectionnant **Désactivé**, **Transitoire** ou **Activé** dans le menu contextuel. Vous pouvez également sélectionner **Activer tout** ou **Désactiver tout** pour mettre à jour l'état de tous vos analyseurs de logs à la fois.

5. Cliquez sur **Appliquer**.

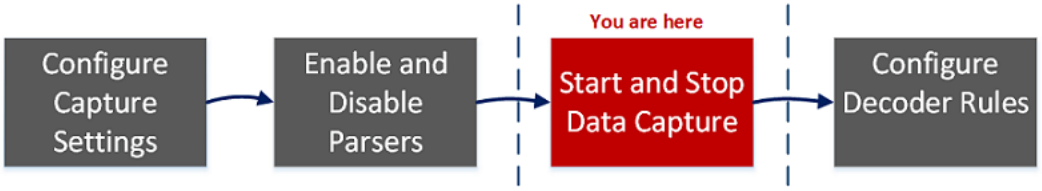
Lorsque vous cliquez sur **Appliquer**, notez que tous les analyseurs sont rechargés dans NetWitness Platform. L'état de chaque analyseur de log est mis à jour, en fonction de vos sélections.

Démarrer et arrêter la capture de données

Lorsqu'un Decoder démarre, il commence automatiquement à agréger des données si le **démarrage automatique de capture** est activé. Lorsque le démarrage automatique n'est pas activé, vous pouvez démarrer et arrêter la capture de données manuellement.

Remarque : Les paramètres de configuration de la capture dans la vue Configuration des services pour un Decoder déterminent si la fonction Démarrage automatique de la capture est activée.

La figure suivante illustre les paramètres les plus utilisés sur un Decoder. Pour une configuration de base rapide avec uniquement les étapes à suivre, reportez-vous à la section Configuration rapide de Decoder et de Log Decoder. Vous souhaiterez peut-être arrêter et démarrer la capture à d'autres moments, par exemple, avant d'arrêter le service.



Pour démarrer et arrêter la capture :

1. Accédez à **ADMIN > Services.**
2. Dans la vue **Services d'administration**, sélectionnez un service Decoder ou Log Decoder et cliquez sur  **> Vue > Système**.
3. Dans la barre d'outils, cliquez sur **Démarrer la capture**.

   Si le service est un Decoder, il commence à capturer les paquets. Si le service est un Log Decoder, il commence à capturer les logs.

   Lorsque la capture de paquets ou de logs est en cours, l'option de la barre d'outils devient **Arrêter la capture**, et l'option de téléchargement d'un fichier est disponible.
4. Pour interrompre la capture du trafic sur un Decoder, cliquez sur **Arrêter la capture**.

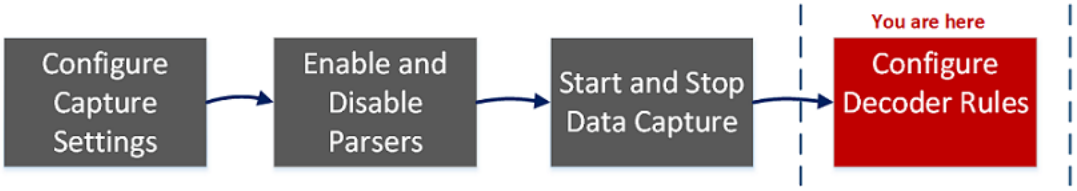
   La capture des paquets ou des logs cesse et l'option de téléchargement d'un fichier sur le service est à nouveau disponible.

Remarque : Lorsque vous arrêtez le service Log Decoder pendant l'exécution de la capture, tous les événements actuellement dans la mémoire du Log Decoder seront traités et rendus persistants. Si un problème se présente lorsqu'il est nécessaire d'arrêter rapidement le service, utilisez la vue Explorer les services pour arrêter la capture (`/decoder stop`), en passant les paramètres `flush=false` avant d'arrêter le service Log Decoder. Pour plus d'informations, reportez-vous à la section « Vue Explorer les services » du *Guide de mise en route de l'hôte et des services*.

Configurer les règles de Decoder

Cette rubrique présente des procédures permettant de créer et de gérer les règles pour la capture de trafic de Decoder ou Log Decoder dans Configuration des services > onglet Règles. La section Vue Configuration des services - onglets Règles fournit des détails sur les options de l'onglet Règles.

La figure suivante illustre les paramètres les plus utilisés sur un Decoder. Pour une configuration de base rapide avec uniquement les étapes à suivre, reportez-vous à la section Configuration rapide de Decoder et de Log Decoder.



Les règles de capture peuvent ajouter des alertes ou des informations contextuelles aux sessions ou aux logs. Elles peuvent également définir les données qui sont filtrées par un Decoder ou un Log Decoder. Les règles sont créées pour des modèles de métadonnées spécifiques. Elles se traduisent par des actions prédéfinies lorsque des correspondances sont trouvées. Par exemple, pour garder exclusivement l'ensemble du trafic qui correspond à certains critères, vous pouvez créer une règle qui effectue les actions nécessaires. Une fois appliquées, les règles affectent à la fois l'importation des fichiers de capture de paquets et la capture réseau instantanée.

La rubrique Instructions relatives aux règles et requêtes contient les directives que toutes les requêtes et conditions de règles doivent suivre dans les services NetWitness Platform Core.

Par défaut, aucune règle n'est définie lors de la première installation de NetWitness Platform. Avant que les règles soient spécifiées, les paquets ne sont pas filtrés. Vous pouvez déployer les dernières règles à partir de Live. Vous pouvez définir trois types de règles : règles réseau, règles d'application et règles de corrélation.

- Les règles réseau sont appliquées au niveau des paquets. Elles sont constituées des groupes de règles de la couche 2, de la couche 3 et de la couche 4. Plusieurs règles peuvent s'appliquer à Decoder. Les règles peuvent être appliquées à plusieurs couches (par exemple, lorsqu'une règle réseau filtre des ports spécifiques pour une adresse IP spécifique). Les règles de réseau ne sont disponibles que sur les Network Decoders.
- Les règles d'application sont appliquées au niveau de la session. Si la première règle répertoriée ne correspond pas, Decoder tente alors d'établir une correspondance avec la règle répertoriée suivante, jusqu'à ce qu'une correspondance soit trouvée.
- Les règles de corrélation sont appliquées sur une période de temps glissante configurable. Lorsqu'une correspondance est trouvée, le service crée une super session qui identifie les autres sessions correspondant à la règle, puis crée une liste de sessions à analyser.

Les deux utilisations les plus courantes des règles sont les suivantes :

- alerter et ainsi créer une métavaleur d'alerte personnalisée, lorsque certaines conditions sont réunies ;
- filtrer certains types de trafics qui n'ajoutent aucune valeur à l'analyse des données.

Les groupes de règles de capture forment les groupes de règles, que vous pouvez importer et exporter. Grâce à cette fonctionnalité, vous pouvez utiliser plusieurs groupes de règles pour différents scénarios. Vous pouvez importer le groupe de règles exporté, sous la forme d'un fichier .nwr, dans d'autres services NetWitness Platform, ce qui simplifie le déploiement et la configuration de plusieurs services.

Traitement des règles

Voici les principes qui régissent le traitement des règles de capture :

- Plusieurs règles peuvent s'appliquer à Decoder.
- Les règles de capture sont exécutées les unes après les autres, de manière séquentielle.
- Le traitement des règles s'arrête lorsque toutes les règles sont traitées, ou après la détection d'une règle configurée pour arrêter le traitement des règles.
- Une règle par défaut peut être utilisée pour inclure ou exclure le trafic qui n'a pas été sélectionné par une règle. Si une règle par défaut est utilisée, elle doit toujours être placée au bas de la liste des règles. Sinon, le traitement des règles s'arrête dès que la règle par défaut est évaluée. En effet, par définition, tout le trafic est sélectionné par la règle par défaut.
- Lorsque le traitement des règles s'arrête, la session est enregistrée à l'aide des options de session et des options de débogage configurées.

Instructions relatives aux règles et requêtes

Toutes les conditions de requêtes et de règles des services RSA NetWitness Core doivent appliquer les instructions suivantes :

Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les nombres ou les adresses MAC et IP entre guillemets.

- `extension = 'torrent'`
- `time='2015-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

Remarque : L'espace à droite et à gauche d'un opérateur est facultatif. Par exemple, vous pouvez saisir une règle sous la forme `service=80` ou `service = 80`.

Exemples de règle

Le tableau suivant présente des exemples de conditions de règle. Vous pouvez utiliser des conditions de règle pour les collections de rétention de logs dans un service Archiver et pour les règles d'application, réseau et de corrélation sur un service Decoder, Log Decoder ou Concentrator. Les conditions de règle sont également utilisées dans toutes les clauses `WHERE` de toutes les requêtes de base de données Core.

Pour obtenir des informations détaillées sur la syntaxe des règles dans NetWitness Platform, reportez-vous à « Clauses `WHERE` » dans la section « Requêtes » du *Guide de réglage de la base de données Core*.

Nom de la règle	Condition
ComplianceDevices	`device.group='PCI Devices' || device.group='HIPPA Devices'`
HighValueWindows	`device.group='Windows Compliance'`
MediumValueWindows	`device.type='winevent_nic' && msg.id='security_4624_security'`
LowValueWinLogs	`device.type='winevent_nic' && msg.id='security_4648_security'`
LowValueProxyLogs	`device.class='proxy' && msg.id='antivirus_license_expired'`
GeneralWindows	`device.type='winevent_nic'`

Règles non valides

NetWitness Platform utilise un analyseur de règles qui définit strictement la syntaxe valide pour les règles et les requêtes. Lorsqu'un service Core rencontre une syntaxe non valide, il écrit un avertissement dans les logs NetWitness Platform indiquant l'erreur.

Remarque : NetWitness Platform 11.x ne prend pas en charge l'analyse des règles de syntaxe héritées (comme le faisait la version 10.6). Après la mise à jour vers NetWitness Platform 11.x, les règles contenant une syntaxe non valide sont mises en surbrillance dans l'interface utilisateur, et aucune règle ne sera appliquée tant que les règles non valides ne seront pas corrigées. L'éditeur de règles fournit des infobulles supplémentaires. Une fois les règles corrigées, les mises en surbrillance disparaissent. Reportez-vous à la section Corriger les règles contenant une syntaxe non valide.

Les statistiques `/decoder/config/rules/rule.errors` et `/concentrator/config/rules/rule.errors` indiquent le nombre de règles contenant des erreurs. Si les statistiques `rule.errors` ne sont pas égales à zéro, NetWitness Platform génère une alerte d'intégrité pour indiquer que vous devez corriger les règles.

Consignes générales sur la syntaxe

- Toutes les valeurs de texte doivent utiliser des valeurs littérales entre guillemets. Exemple : `username = 'user1'`
- Les guillemets peuvent être des guillemets simples ou doubles ; mais ils doivent être cohérents. (Vous ne pouvez pas démarrer avec un guillemet simple et terminer avec un guillemet double.)

- Si la valeur littérale comporte des guillemets, vous pouvez insérer un caractère d'échappement (une barre oblique inversée) ou utiliser des guillemets ouvrants différents. Les deux exemples suivants sont valides : `username = "User's"`, `username = 'User\'s'`

Les règles de syntaxe suivantes sont valides :

- Pour utiliser une barre oblique inversée dans une chaîne littérale, insérez une autre barre oblique inversée en guise de caractère d'échappement : `\`
- Toutes les valeurs temporelles doivent utiliser des guillemets pour les dates au format suivant : `time = 'YYYY-MM-DD HH:MM:SS'`
- Toutes les valeurs temporelles exprimées en nombres de secondes depuis l'outil EPOCH (01/01/1970), ne doivent pas être mis entre guillemets.
  Exemple : `time = 1448034064`
- **Tout le reste** ne doit pas être mis entre guillemets : Adresses IP, adresses Mac, chiffres, etc.
  Exemple : `service = 80 && ip.src = 192.168.1.1/16`

Syntaxe des règles de capture

Les règles de capture comparent les champs aux valeurs ou à d'autres champs. Voici l'exemple d'une expression simple avec une clé méta sur le côté gauche de l'opérateur et une valeur sur le côté droit.

```
ip.dst=192.168.1.1
```

La syntaxe autorise une clé méta sur le côté droit de l'opérateur dans les Decoders et Log Decoders pour les règles d'application et réseau. La comparaison des clés méta ne s'applique pas à la clause `where` dans les requêtes. Voici l'exemple d'une expression simple avec une clé méta sur le côté gauche de l'opérateur et une clé méta sur le côté droit.

```
ip.src=ip.dst
```

Les règles qui incluent la prise en charge de la comparaison de clés méta renommées : si une règle interroge une clé méta qui a été renommée, la règle est analysée pour la clé méta renommée. Par exemple, si la clé méta `ip_dst` est utilisée dans une règle, elle est mappée en toute transparence sur la clé méta renommée : `ip.dst`. Les règles existantes qui incluent des clés d'origine déclenchent des alertes comprenant des données pour la clé méta renommée.

Voici un exemple d'une règle qui trouve des paquets ayant la même adresse `ip.src` et adresse `ip.dst` sur un Decoder, et génère une alerte sur le Concentrator.

```
alert=alert.id name=testRule8 rule="ip.src=ip.dst" order=38
```

Cette règle peut générer une erreur car `eth.src` et `ip.src` sont des formats incompatibles.

```
rule="eth.src=ip.src" name="testRule99" alert=alert.id
```

Les valeurs peuvent être exprimées sous forme de valeurs discrètes, de plages de valeurs, de limites inférieure ou supérieure, ou d'une combinaison de ces trois possibilités. Vous pouvez créer une comparaison de supériorité ou d'infériorité, et tester l'égalité ou l'inégalité par rapport à une plage de valeurs ou une limite supérieure/inférieure.

`key 0-5` (plage de valeurs)

`key = 0-u` est identique à `key >= 0` (limite supérieure, supérieur ou égal à)

Le tableau suivant résume les opérateurs sur les clés méta.

Format de l'opérande de gauche	Opérateur	Format de l'opérande de droite	Description
N'importe lequel	=	Compatible avec l'opérande de gauche	Opérateur égalité. Vous pouvez utiliser des valeurs ou des clés méta sur le côté droit de l'opérateur d'égalité.
N'importe lequel	!=	Compatible avec l'opérande de gauche	Opérateur d'inégalité. Vous pouvez utiliser des valeurs ou des clés méta sur le côté droit de l'opérateur d'inégalité.
N'importe lequel	<	Compatible avec l'opérande de gauche	Opérateur Inférieur à. Vous pouvez utiliser des valeurs ou des clés méta sur le côté droit de cet opérateur.
N'importe lequel	<=	Compatible avec l'opérande de gauche	Opérateur Inférieur ou égal à. Vous pouvez utiliser des valeurs ou des clés méta sur le côté droit de cet opérateur.
N'importe lequel	>	Compatible avec l'opérande de gauche	Opérateur Supérieur à. Vous pouvez utiliser des valeurs ou des clés méta sur le côté droit de cet opérateur.
N'importe lequel	>=	Compatible avec l'opérande de gauche	Opérateur Supérieur à ou égal. Vous pouvez utiliser des valeurs ou des clés méta sur le côté droit de cet opérateur.
Texte	contains	Texte	Recherchez des valeurs qui contiennent l'opérande de droite. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.
Texte	begins	Texte	Recherchez des valeurs qui commencent par l'opérande de droite. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.
Texte	ends	Texte	Recherchez des valeurs qui terminent par l'opérande de droite. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.
Texte	length	Entier	Recherchez des chaînes d'une certaine longueur. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.

Format de l'opérande de gauche	Opérateur	Format de l'opérande de droite	Description
N'importe lequel	`count`	Entier	Trouvez des valeurs avec un certain nombre d'occurrences dans la session. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.
N'importe lequel	`ucount` et `unique`	Entier	Recherche des valeurs se produisant de manière unique. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur. Par exemple, si les résultats incluent les instances d'une clé méta avec cinq valeurs uniques et trois de la même valeur, `ucount` est égal à six.
s.o.	`exists`	N'importe lequel	Recherche toutes les valeurs de la clé méta. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.
s.o.	`!exists`	N'importe lequel	Recherche toutes les sessions dans lesquelles la clé méta ne se produit pas. Vous pouvez utiliser des clés méta ou des valeurs sur le côté droit de cet opérateur.
Texte	`regex`	Texte	Recherche les valeurs correspondant à une expression régulière. Vous pouvez utiliser des valeurs sur le côté droit de cet opérateur.

Le tableau suivant récapitule les autres éléments de la syntaxe utilisée dans les règles.

Élément de la syntaxe	Description
*	Règle par défaut. Si vous utilisez un astérisque (*) en tant que caractère unique dans une règle, celleei sélectionne la totalité du trafic.
`u`	Limite supérieure d'une plage de temps, d'adresses IP ou de formats numériques. Par exemple, pour sélectionner tous les ports TCP au-dessus du port 40000, la syntaxe est la suivante : `tcp.port = 40000-u`
`l`	Limite inférieure d'une plage de temps, d'adresses IP ou de valeurs numériques. Par exemple, pour sélectionner tous les ports TCP en dessous du port 40000, la syntaxe est la suivante : `tcp.port = l-40000`

Élément de la syntaxe	Description
- (tiret)	Désigne une plage. Cela s'applique uniquement aux valeurs temporelles, adresses IP ou MAC, ou valeurs numériques. Séparez les limites inférieure et supérieure de la plage par un trait (-). Par exemple, pour sélectionner les ports TCP situés entre 25 et 443, la syntaxe est la suivante : `tcp.port = 25-443`
, (virgule)	Désigne une liste de plages, de valeurs ou de clés méta. Vous pouvez combiner l'utilisation de valeurs individuelles, de plages et de limites supérieure ou inférieure. Les clés méta uniques peuvent être utilisées dans une liste. Les clés méta et valeurs littérales ne peuvent pas apparaître sur le côté droit d'un opérateur. Par exemple, ce qui suit est une syntaxe valide : `tcp.port = 1-10,25,110,143-225,40000-u`
( )	Opérateur de regroupement. Vous pouvez mettre une expression entre parenthèses pour créer une expression logique. Par exemple, voici comment sélectionner le trafic sur le port 80 vers/depuis l'adresse 192.168.1.1 OU le trafic sur le port 443 vers/depuis l'adresse 10.10.10.1 : `(ip.addr=192.168.1.1 && tcp.port=80) || (ip.addr=10.10.10.1 && tcp.port=443)`
~	Opérateur logique NOT, négation d'une expression.
&&	Opérateur logique AND, combinaison de deux expressions.
||	Opérateur logique OR, disjonction de deux expressions.

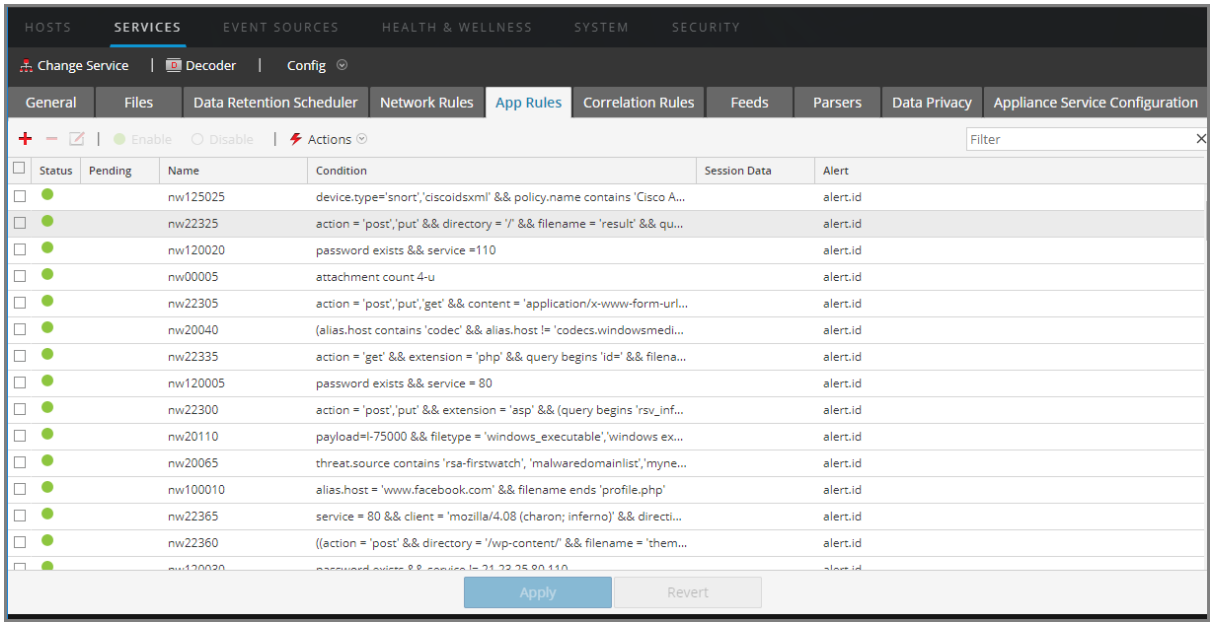
Configurer les règles de capture

Les règles de Decoder et de Log Decoder sont modifiables dans la vue Configuration des services. Bien que chaque type de règle (réseau, application et corrélation) ait son propre onglet, ses fonctions sont similaires. Vous pouvez :

- ajouter, modifier et supprimer des règles ;
- activer et désactiver des règles ;
- changer la séquence d'exécution des règles ;
- importer des règles à partir d'un fichier ;
- exporter des règles dans un fichier ;
- transmettre (push) les règles à un autre service ;
- annuler ou appliquer les modifications apportées aux règles ;
- restaurer l'une des dix dernières configurations de règle à partir d'un snapshot

Pour configurer des règles dans les onglets Règles

1. Accédez à **ADMIN > Services**.
2. Dans la vue **Services**, sélectionnez un service Decoder, puis > **Vue > Configuration**.
3. Dans la vue **Configuration des services**, sélectionnez l'un des onglets Règles : règles réseau, règles d'application ou règles de corrélation.
   La liste des règles correspondant au type de règles sélectionné s'affiche.



Chaque type de règles possède une liste avec des colonnes et des paramètres légèrement différents. Plusieurs principes de base s'appliquent à l'ensemble des activités de gestion des règles :

- Les règles sont exécutées dans l'ordre où elles apparaissent dans la liste. Pour changer la séquence d'exécution des règles, effectuez un glisser-déplacer de ces dernières vers l'emplacement approprié dans la liste, ou utilisez les options de menu contextuel pour les réorganiser au sein de la liste.
- Pour sélectionner une seule ligne, cliquez sur celleei.
- Pour sélectionner un groupe de lignes adjacentes, cliquez sur la première d'entre elles, puis appuyez sur la touche Maj et cliquez sur la ligne située à la fin du groupe.
- Pour sélectionner plusieurs lignes non adjacentes, cliquez sur la première d'entre elles, puis appuyez sur la touche Ctrl et cliquez sur les autres.
- Lorsque vous modifiez des règles sous l'onglet Règles, vous devez appliquer les modifications de configuration pour les rendre effectives.
- Tant que ces changements ne sont pas appliqués, vous pouvez ignorer les modifications apportées à la liste et revenir aux règles non modifiées.
- Une fois les règles appliquées, vous pouvez restaurer les dix dernières configurations de règle à l'aide de l'option **Historique** du menu **Actions**.

Pour ajouter une règle à un onglet Règles, procédez de l'une des façons suivantes :

- Cliquez sur + .
- Cliquez avec le bouton droit de la souris sur une règle, puis sélectionnez **Insérer au-dessus** ou **Insérer en dessous** dans le menu contextuel.
  La boîte de dialogue Éditeur de règles s'affiche pour ce type de règle.

Pour supprimer une règle :

1. Sous l'un des onglets Règles, sélectionnez les règles à supprimer de la liste de règles.
2. Cliquez sur − .
   Les règles sélectionnées sont supprimées de la grille, mais elles existent encore dans le service.

Pour modifier une règle

1. Sous l'onglet Règles, sélectionnez la règle à modifier.
2. Cliquez sur , ou double-cliquez sur la ligne de la règle.
   La boîte de dialogue Éditeur de règles s'affiche pour ce type de règle.

Pour désactiver une règle :

1. Sous l'onglet Règles, sélectionnez les règles à désactiver.
2. Cliquez sur Disable .
   La règle passe à l'état désactivé dans la liste de règles, mais elle est toujours activée dans le service.

Pour activer une règle :

1. Sous l'onglet Règles, sélectionnez les règles à activer.
2. Cliquez sur Enable .
   La règle passe à l'état activé dans la liste de règles, mais elle est toujours désactivée dans le service.

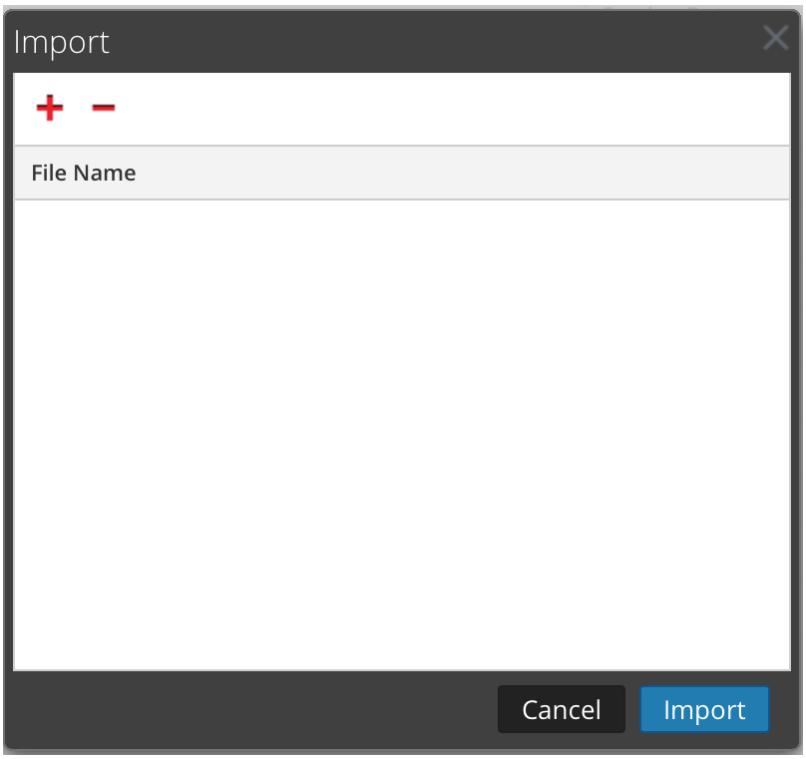
Importer des règles à partir d'un fichier et exporter des règles

Vous pouvez importer des règles réseau, d'application et de corrélation dans Decoder à partir d'un fichier qui contient des règles du même type. Une fois ces règles importées, vous pouvez les modifier et les gérer comme les autres règles.

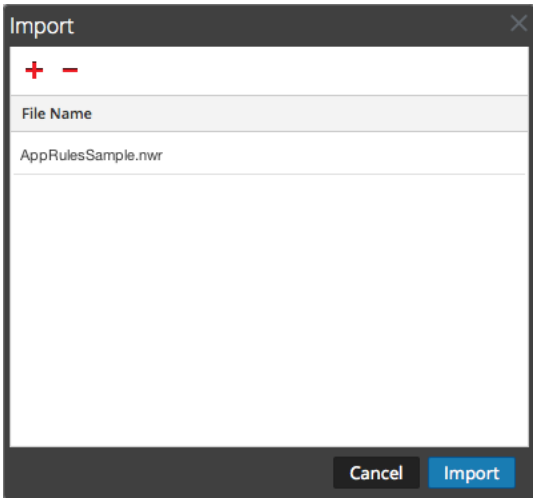
Lorsque vous essayez d'importer un groupe de règles, NetWitness Platform Administration vérifie le type de règles importées. En cas de succès, un message affiche le nombre de règles importées. Si le type de règles diffère du type d'onglets actif, les règles ne sont pas importées. Vous devez réimporter les règles sous l'onglet approprié, ou sélectionner un autre fichier à importer.

Pour importer des règles dans un service :

1. Sous l'onglet Règles, sélectionnez Actions > Import .
   La boîte de dialogue Importer s'affiche.

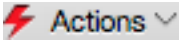


2. Cliquez sur + .
   Une vue de la structure du répertoire s'affiche.
3. Choisissez un ou plusieurs fichiers de règles NetWitness (.nwr) à importer, puis cliquez sur **Ouvrir**.
   Le fichier est ajouté à la liste de la boîte de dialogue Importer.



4. Cliquez sur **Importer**.
   Les règles sont importées dans l'interface utilisateur. Les règles importées présentent un angle rouge dans chaque colonne modifiée.
5. Modifiez ou réorganisez les règles, si nécessaire.
6. Pour enregistrer les règles dans le service, cliquez sur **Appliquer**.
   Les règles du service sont mises à jour avec les changements apportés.

Pour exporter une règle dans un fichier :

1. Pour exporter un sousensemble de règles, sélectionnez les règles à exporter.
2. Exécutez l'une des opérations suivantes :
   - Dans la barre d'outils, sélectionnez 

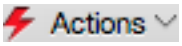
 > Exporter > Sélection. (**Exporter > Tout** exporte toutes les règles de la liste, même si vous avez sélectionné un sous-ensemble à exporter.)
   - Cliquez avec le bouton droit de la souris sur les règles sélectionnées et sélectionnez **Sélections pour l'exportation**.

     Une invite s'affiche pour le nom du fichier.
3. Saisissez le nom du fichier, puis cliquez sur **Exporter**.
   Le fichier .**nwr** est téléchargé.

Transmettre (push) les règles à d'autres services

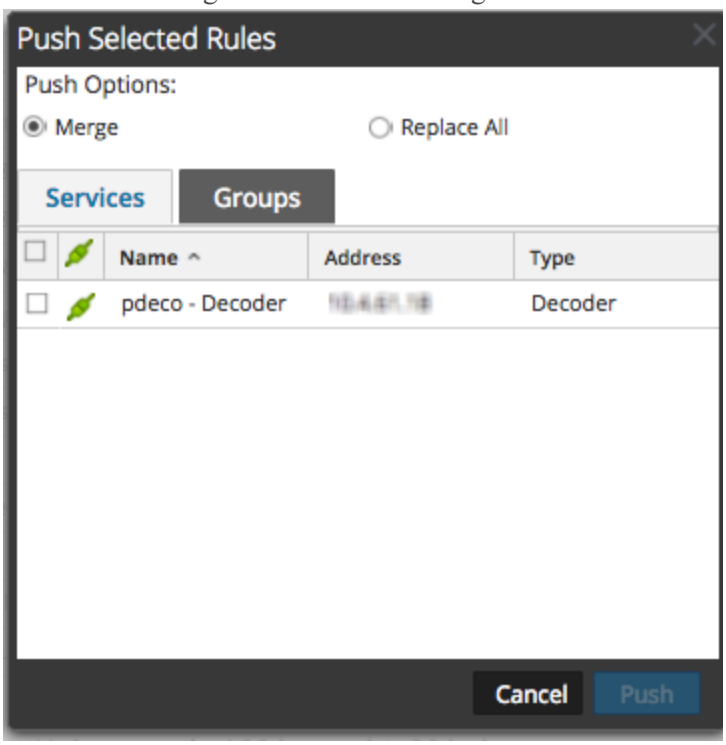
Vous pouvez transmettre (push) des règles ou les règles sélectionnées à d'autres services (Decoder ou Log Decoder) ou groupes de services. Lorsque vous transmettez toutes les règles aux autres services, toutes les règles des services de destination sont supprimées et remplacées par toutes les règles du service source.

Pour transmettre les règles sélectionnées de ce Decoder à d'autres instances de Decoder :

1. Dans un onglet Règles, sélectionnez les règles à transmettre à un autre Decoder.
2. Exécutez l'une des opérations suivantes :
   - Sélectionnez 

 > Transmettre > Sélection.
   - Cliquez avec le bouton droit de la souris sur les règles sélectionnées et sélectionnez **Transmettre les règles sélectionnées**.

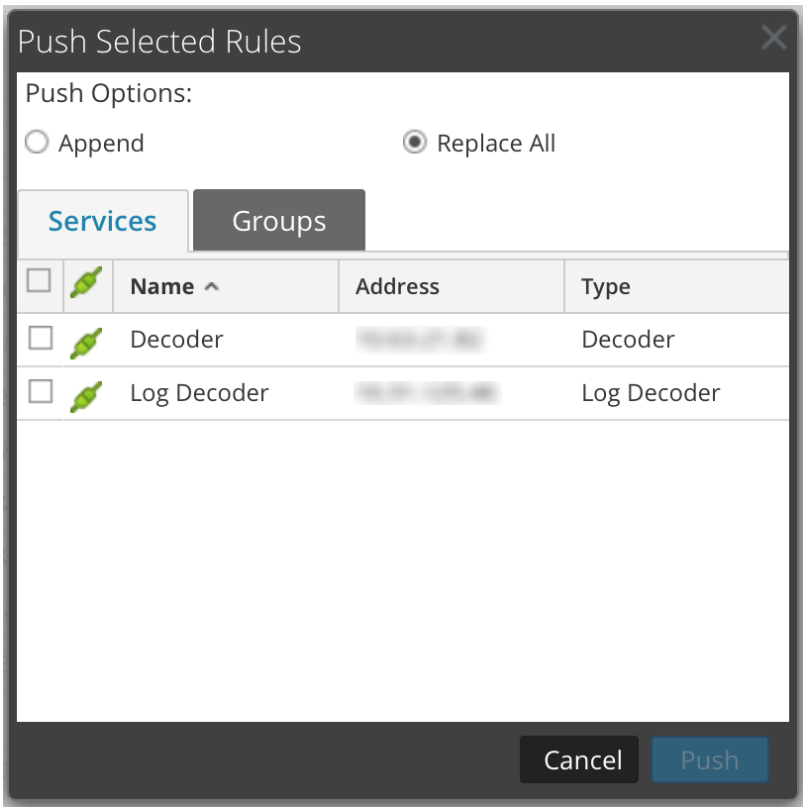
La boîte de dialogue Transmettre les règles sélectionnées s'affiche.



3. Sélectionnez une Option de transmission :
   - Sélectionnez **Tout remplacer** pour supprimer toutes les règles sur les services de destination et les remplacer par les règles sélectionnées. Voici la sélection par défaut.
   - Sélectionnez **Fusionner** pour fusionner les règles sélectionnées avec les règles existantes sur les services de destination.
4. Sous l'onglet **Services**, sélectionnez les services destinés à recevoir les règles transmises, ou sélectionnez les groupes de services sous l'onglet **Groupes**.
5. Cliquez sur **Transmettre**.
   Les règles sont transmises aux services sélectionnés, puis entrent en vigueur immédiatement.

Pour transmettre toutes les règles de ce Decoder à d'autres instances de Decoder :

1. Dans l'onglet Règles, sélectionnez Actions > **Transmettre** > **Tout**.
   (**Transmettre** > **Tout** transmet toutes les règles de la grille même si vous avez sélectionné un sous-ensemble à exporter.) La boîte de dialogue Transmettre les règles sélectionnées s'affiche.



2. Sous l'onglet **Services**, sélectionnez les services destinés à recevoir les règles transmises, ou sélectionnez les groupes de services sous l'onglet **Groupes**.
3. Cliquez sur **Transmettre**.
   Toutes les règles des services de destination sont supprimées et remplacées par toutes les règles des services source. Les règles prennent effet immédiatement.

Changer la séquence d'exécution des règles

Les règles de capture sont appliquées dans l'ordre où elles apparaissent dans la liste Règles. Pour réorganiser les règles, utilisez l'une des méthodes suivantes :

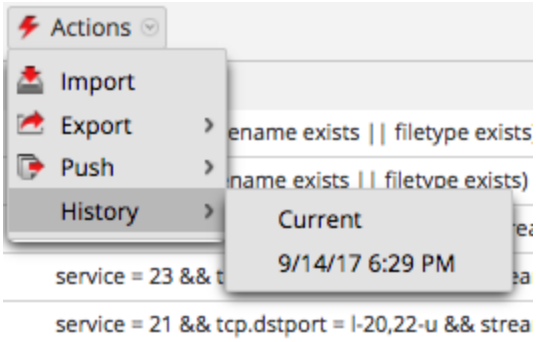
- Effectuez un glisser-déplacer des règles vers l'emplacement approprié dans la liste de règles.
- Cliquez avec le bouton droit de la souris sur une règle pour afficher le menu contextuel, puis utilisez les options **Couper** et **Coller**.

Restaurer un snapshot de règles à partir de l'historique

NetWitness Platform conserve les dix derniers snapshots de règle appliqués à un service.

Pour restaurer un snapshot de règles à partir de l'historique :

1. Sélectionnez Actions > **Historique**.
   Un sous-menu de snapshots s'affiche.



2. Sélectionnez l'heure du snapshot dans le sous-menu.
   Les règles du snapshot sont chargées dans la liste de règles, en remplacement du groupe actuel. Toutefois, le groupe actuel est toujours utilisé dans le service.
3. Pour appliquer les règles au service, cliquez sur **Appliquer**.
   Les règles sont appliquées au service.

Configurer des règles d'application

Les règles de la couche application sont appliquées au niveau de la session. Voici des exemples de règles d'application.

Pour tronquer des paquets transportés via le protocole SMB (Server Message Block), créez une règle comme suit :

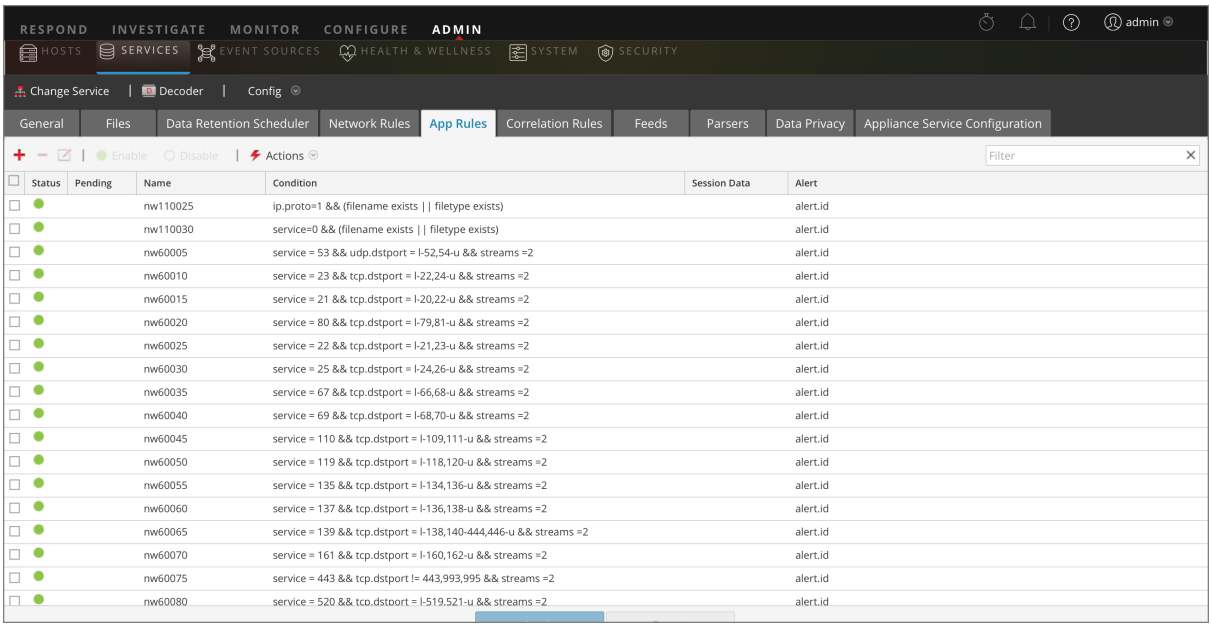
- Nom de la règle : Tronquer SMB
- Condition : `service=139`
- Action de règle : Tout tronquer

Pour conserver l'e-mail spécifique d'un expéditeur et d'un destinataire, créez une règle comme suit :

- Nom de la règle : Filtrage e-mails Tom Jones
- Condition : `email='Tom.Jones@TheShop.com'`
- Action de règle : Filtrer

Ajouter ou modifier une règle d'application :

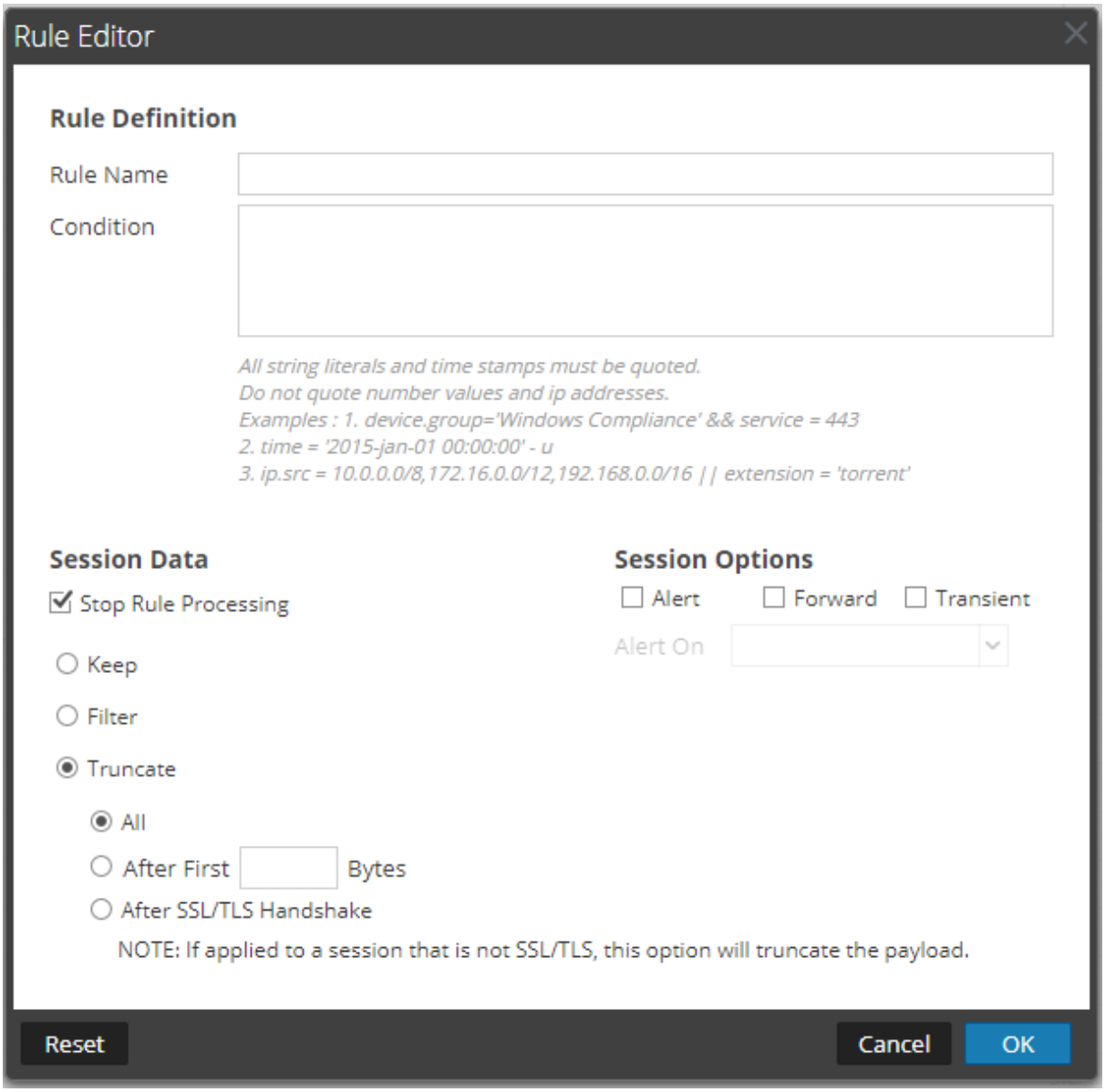
1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service Decoder ou Log Decoder, puis > **Vue > Config**.
   La vue Configuration des systèmes pour le service sélectionné s'affiche.
3. Sélectionnez l'onglet **Règles d'application**.



4. Exécutez l'une des opérations suivantes :

- Pour ajouter une nouvelle règle, cliquez sur +
- Si vous modifiez une règle, sélectionnez la règle dans la grille des règles et cliquez sur .

5. La boîte de dialogue Éditeur de règles s'affiche avec les paramètres de la règle d'application.



a. Dans le champ **Nom de la règle**, saisissez le nom de la règle. Par exemple, pour une règle qui tronque tous les SMB, saisissez **Tronquer SMB**.

b. Dans le champ **Condition**, élaborez la condition de règle qui déclenche une action lorsqu'elle est remplie. Vous pouvez effectuer votre saisie directement dans le champ ou élaborer la condition dans ce champ à l'aide des métadonnées de la fenêtre Actions. Lors de l'élaboration de la définition de règle, NetWitness Platform affiche des erreurs et avertissements de syntaxe. Par exemple, pour tronquer tous les SMB, saisissez **service=139**.

Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre et adresses IP entre guillemets. Configurer les règles de Decoder fournit des détails supplémentaires.

c. Si vous souhaitez mettre fin à l'évaluation de cette règle, activez la case à cocher **Arrêter le traitement des règles**.

d. Dans la section **Données de session**, choisissez l'une des actions suivantes à appliquer lorsqu'un paquet correspondant est trouvé :

- **Conserver** : La charge du paquet et les métadonnées associées sont enregistrées lorsqu'elles correspondent à la règle.
- **Filtrer** : Le paquet n'est pas enregistré lorsqu'il correspond à la règle.
- **Tronquer** : Sélectionnez une option de troncation à exécuter lorsqu'un paquet correspond à la règle. L'exemple utilise l'option **Tout**.
- **Tronquer tout** pour enregistrer les en-têtes de paquet et les métadonnées associées, et ne pas enregistrer la charge utile du paquet.
- **Tronquer après les <n> premiers octets** pour enregistrer les en-têtes de paquet et les métadonnées associées, et ne pas enregistrer la charge utile du paquet après les <n> premiers octets spécifiés, <n> étant un nombre d'octets.
- **Tronquer le handshake SSL/TLS** pour tronquer la charge utile de toutes les sessions, sauf dans le cas d'une session SSL/TLS, où l'échange SSL est conservé, mais le reste de la charge utile n'est pas enregistré. Cette option est utilisée avec les analyseurs SSL.

e. Dans la section **Options de session**, effectuez l'une des tâches suivantes :

- **Pour générer une alerte personnalisée** lorsque des métadonnées de session correspondent à la règle, activez la balise Alerte et sélectionnez le nom des métadonnées d'alerte dans la liste déroulante **Alerte activée**.
- **Pour effectuer un transfert Syslog** lorsque le log correspond à la règle, activez la balise **Transférer**. Vérifiez que :
  - Vous avez activé à la fois les balises Alerte et Transférer pour effectuer le transfert Syslog.
  - Le nom de la règle mentionnée dans la boîte de dialogue Éditeur de règles correspond bien au nom de la destination du transfert Syslog spécifié dans Log Decoder > Vue > Explorer > paramètre `/decoder/config/logs.forwarding.destination`.
- **Pour éviter que les métadonnées de l'alerte qui est créée soient écrites sur le disque**, activez la balise **Transitoire**.

6. Pour enregistrer la règle et l'ajouter à la grille, cliquez sur **OK**.

   La règle est ajoutée à la fin de la grille ou insérée à l'endroit que vous avez indiqué dans le menu contextuel. Le signe plus s'affiche dans la colonne **En attente**.

7. Vérifiez que la séquence d'exécution de la règle est correcte par rapport aux autres règles de la grille. Si nécessaire, déplacez la règle.

8. Pour appliquer la règle mise à jour au Decoder ou Log Decoder, cliquez sur **Appliquer**.

NetWitness Platform enregistre un snapshot des règles en cours d'application, puis applique l'ensemble mis à jour au Decoder et supprime le voyant En attente des règles qui étaient en attente.

Surveiller les règles d'application

Decoder et Log Decoder gardent une trace du nombre de correspondances entre une règle d'application et une session. Ces statistiques peuvent être affichées en se connectant à la vue Explorer de Decoder ou Log Decoder et en affichant les propriétés du dossier `/decoder/config/rules/application`. Ensuite, envoyez la commande "`statdump`" à ce dossier. La sortie de ce message est une liste du nombre d'adéquations avec chacune des règles d'application. La liste est triée dans le même ordre que le contenu des définitions de règle du dossier `/decoder/config/rules/application`. Par exemple, sur un système avec trois règles d'application :

```
0001: hits=6543 loaded=true
0002: hits=9294 loaded=true
0003: hits=43 loaded=true
```

Les compteurs de « hits » des règles d'application sont réinitialisés à chaque fois que les analyseurs sont rechargés.

Configurer des règles de corrélation

Les règles de corrélation de base sont appliquées au niveau de la session et alertent l'utilisateur par rapport à des activités spécifiques pouvant se produire dans leur environnement. NetWitness Platform applique les règles de corrélation sur une période glissante configurable. Lorsque les conditions sont remplies, les métadonnées d'alerte sont créées pour cette activité, et il y a un indicateur visible de l'activité suspecte.

Voici des exemples de règles de corrélation illustrant les deux exemples d'utilisation et la syntaxe.

Objectif : Dans les sessions où tcp.dstport existe, s'il y a une combinaison de ip.src et ip.dst où le nombre d'instances uniques s'élève à `tcp.dstport > 5` en 1 minute, une alerte se déclenche. Pour atteindre cet objectif, créez une règle de la manière suivante :

- Nom de la règle : IPv6 Vertical TCP Port Scan 5
- Règle : `tcp.dstport exists`
- Clé d'instance : `ip.src,ip.dst`
- Seuil : `u_count(tcp.dstport)>5`
- Période : 1 minute

Objectif : Dans les sessions où `action==login` et `error==fail` existent, s'il y a une combinaison de `ip.src` et de `ip.dst` qui s'affiche dans plus de 10 sessions en 5 minutes, une alerte se déclenche. Pour atteindre cet objectif, créez une règle de la manière suivante :

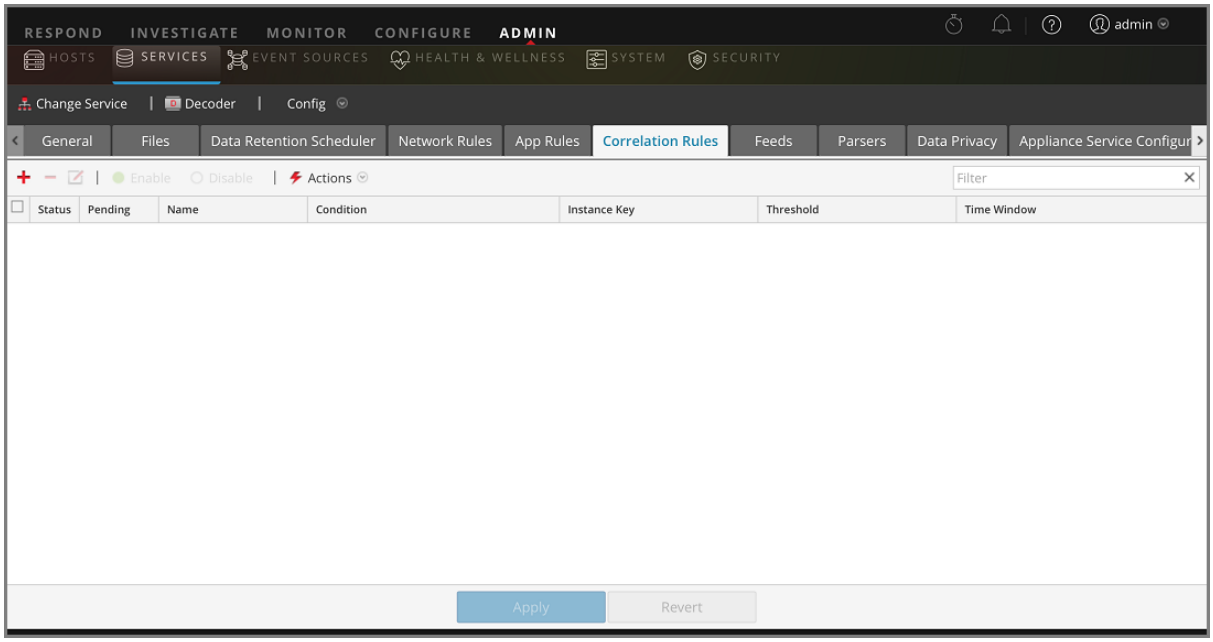
- Nom de la règle : IPv4 Potential Brute Force 10
- Règle : action=`'login' && error='fail'`
- Clé d'instance : `ip.src,ip.dst`
- Seuil : `count()>10`
- Période : 5 minutes

Les deux exemples de règles ont la même clé d'instance : `ip.src` et `ip.dst`. Parce que nous recherchons des combinaisons uniques de `ip.src` et `ip.dst` correspondant à la condition de corrélation, **`ip.src`** et **`ip.dst`** sont des **clés primaires**.
Le seuil peut inclure une **clé associée** qui identifie le type de méta que nous comptons déterminer si la condition est satisfaite. Dans le premier exemple, la clé associée spécifiée dans Seuil est `tcp.dstport`. Nous comptons des instances uniques de `tcp.dstport` pour chaque paire `ip.src/ip.dst`. Dans le deuxième exemple, la clé associée ne précise pas le seuil parce qu'il correspond simplement à un nombre de sessions. Il est utile de penser à ce scénario de comptage des identifiants de session unique et le méta associé est implicitement session.id. Nous comptons des `session.id` uniques pour chaque paire `ip.src/ip.dst`.

Cas d'utilisation incorrects : Pour les sessions where (règle), s'il y a une combinaison de `ip.src` et `ip.dst` avec `ipv6.dst > 5` durant (période), une alerte se déclenche. Ce cas ne fonctionne pas car la clé associée `ipv6.dst` est un type de méta IPv6. Les types de méta IPv4 et IPv6 ne sont pas autorisés à être utilisés en tant que clés associées.

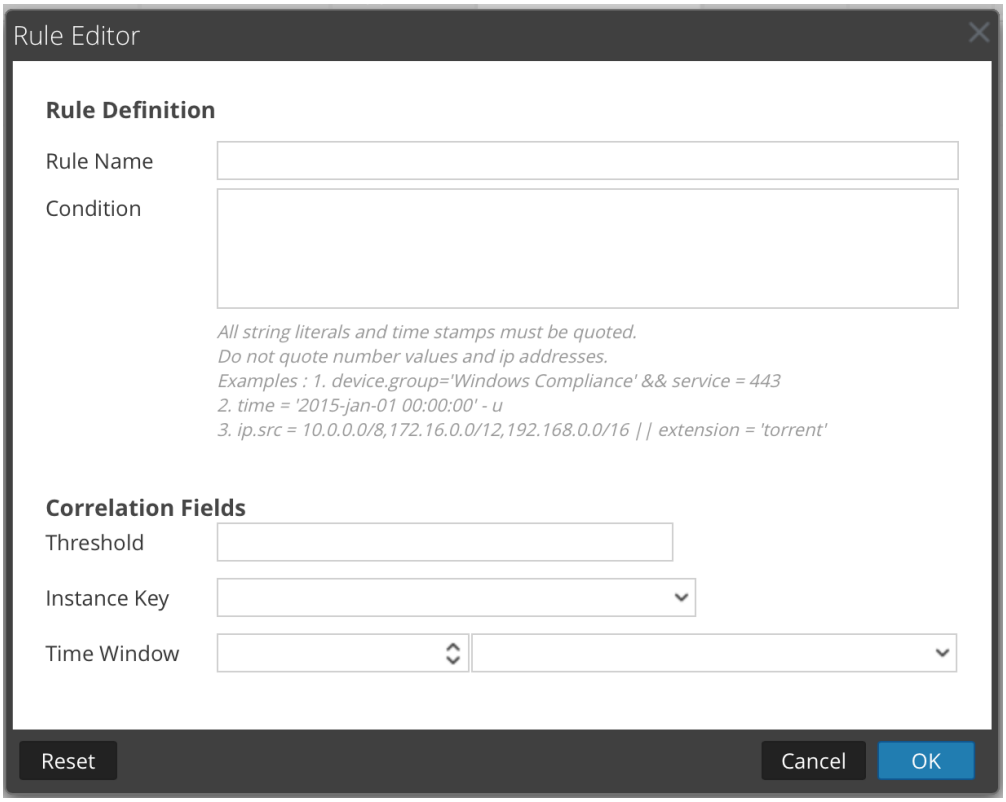
Ajouter ou modifier une règle de corrélation

1. Accédez à **ADMIN > Services,** sélectionnez un service, puis > **Vue > Config**.
   La vue Configuration des services pour le service sélectionné s'affiche.
2. Sélectionnez l'onglet **Règles de corrélation**.



3. Sous l'onglet **Règles de corrélation**, procédez de l'une des façons suivantes :
   - Pour ajouter une nouvelle règle, cliquez sur

- Si vous modifiez une règle, sélectionnez la règle dans la grille de règles, puis cliquez sur . La boîte de dialogue Éditeur de règles s'affiche avec les paramètres des règles de corrélation.



4. Dans le champ **Nom de la règle**, saisissez le nom de la règle. Par exemple, pour créer l'exemple de règle, **IPv6 Vertical TCP Port Scan 5**.
5. Dans le champ **Condition**, élaborez la condition de règle qui déclenche une action lorsqu'elle est remplie. Vous pouvez effectuer votre saisie directement dans le champ ou élaborer la condition dans ce champ à l'aide des métadonnées de la fenêtre Actions. Au fur et à mesure que vous créez la définition de règle, les erreurs de syntaxe et les avertissements sont affichés par NetWitness Platform. Par exemple, pour créer un exemple de règle, saisissez **tcp.dstport exists**. Lorsque cette condition est mise en correspondance, l'action sur les données de session est exécutée.
   Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre et d'adresses IP entre guillemets. Configurer les règles de Decoder fournit des informations supplémentaires.
6. Dans le champ **Seuil**, utilisez l'un des paramètres de seuil pour spécifier le nombre minimum d'occurrences nécessaires pour créer une session de corrélation et une clé associée, si nécessaire. La clé associée ne peut pas être un méta de type IPv4 ou IPv6.
   - `u_count(associated_key)` = nombre de valeurs uniques de la clé spécifiée
   - `sum(associated_key)` = valeurs de la clé spécifiée
   - `count` = nombre de sessions (aucune clé associée spécifiée)
7. Dans le champ **Clé d'instance**, sélectionnez l'indicateur cible sur lequel baser l'événement. Il peut s'agir d'une clé simple ou d'une clé composée (deux clés primaires séparées par une virgule).

8. Dans **Période**, définissez la durée pendant laquelle le seuil doit être atteint pour créer une session de corrélation.
9. Pour enregistrer la règle et l'ajouter à la grille, cliquez sur **OK**.
   La règle est ajoutée à la fin de la grille ou insérée à l'endroit que vous avez indiqué dans le menu contextuel. Le signe plus s'affiche dans la colonne **En attente**.
10. Vérifiez que la séquence d'exécution de la règle est correcte par rapport aux autres règles de la grille. Si nécessaire, déplacez la règle.
11. Pour appliquer la règle mise à jour au service, cliquez sur **Appliquer**.
    NetWitness Platform enregistre un snapshot des règles actuellement appliquées, puis applique l'ensemble mis à jour au Decoder ou Log Decoder.

Configurer des règles réseau

Les règles réseau sont appliquées au niveau des paquets sur un Decoder. Elles sont constituées des groupes de règles de la couche 2, la couche 3 et la couche 4. Vous pouvez appliquer plusieurs règles au niveau des paquets à un Decoder. Les règles réseau peuvent s'appliquer à plusieurs couches (par exemple, lorsqu'une règle réseau filtre des ports spécifiques pour une adresse IP spécifique). Les règles réseau ne s'appliquent pas aux services Log Decoder, mais uniquement aux Network Decoders.

Vous pouvez créer et gérer des règles réseau dans la vue Configuration des services > onglet Règles réseau.

Clés méta prises en charge dans les conditions de règles réseau

Le tableau suivant décrit les clés méta dont NetWitness Platform prend en charge l'utilisation dans les conditions de règle réseau.

Clé méta	Description
eth.addr	Adresse Ethernet source ou de destination. Communément appelée adresse MAC.
eth.dst	Adresse Ethernet de destination. Cette adresse est identique à celle du champ d'adresse Ethernet, sauf qu'elle sélectionne uniquement les paquets dont l'adresse de destination correspond à la valeur ou aux valeurs sélectionnées.
eth.src	Identique à l'adresse Ethernet de destination, sauf qu'elle se concentre sur l'adresse source.
eth.type	Type de frames Ethernet.
hdlc.type	Type de frames du frame HDLC.
ip.addr	Adresse IPv4 source ou de destination au format standard. Vous pouvez saisir les adresses IP en notation CIDR pour les sous‑réseaux.
ip.dst	Adresse IPv4 de destination au format standard. Vous pouvez saisir les adresses IP en notation CIDR pour les sous‑réseaux.
ip.proto	Champ du protocole IPv4.
ip.src	Adresse IPv4 source au format standard. Vous pouvez saisir les adresses IP en notation CIDR pour les sous‑réseaux.
ipv6.addr	Adresse IPv6 source ou de destination au format hexadécimal. En règle générale, les adresses IPv6 sont écrites sous forme de huit groupes de quatre chiffres hexadécimaux, reflétant ainsi la longueur totale d'une adresse 128 bits. Prend en charge la notation pour représenter plusieurs blocs de 0000 dans une adresse. Ne prend pas en charge la notation CIDR.
ipv6.dst	Adresse IPv6 de destination au format hexadécimal.
ipv6.proto	champ du protocole IPv6. Il est mappé au champ d'en‑tête suivant dans l'en‑tête IPv6 et utilise les mêmes valeurs que le champ du protocole IPv4.

Clé méta	Description
ipv6.src	Adresse IPv6 source au format hexadécimal.
tcp.dstport	Port TCP de destination.
tcp.port	Port TCP source ou de destination.
tcp.srcport	Port TCP source.
udp.dstport	Port UDP de destination.
udp.port	Port UDP source ou de destination.
udp.srcport	Port UDP source.

Voici des exemples de règles réseau.

Pour tronquer tous les SSL du port, créez une règle comme suit :

- Nom de la règle : Tronquer SSL
- Condition : `tcp.srcport=443`
- Action de règle : Truncate

Pour filtrer le trafic du sous-réseau, créez une règle de la manière suivante :

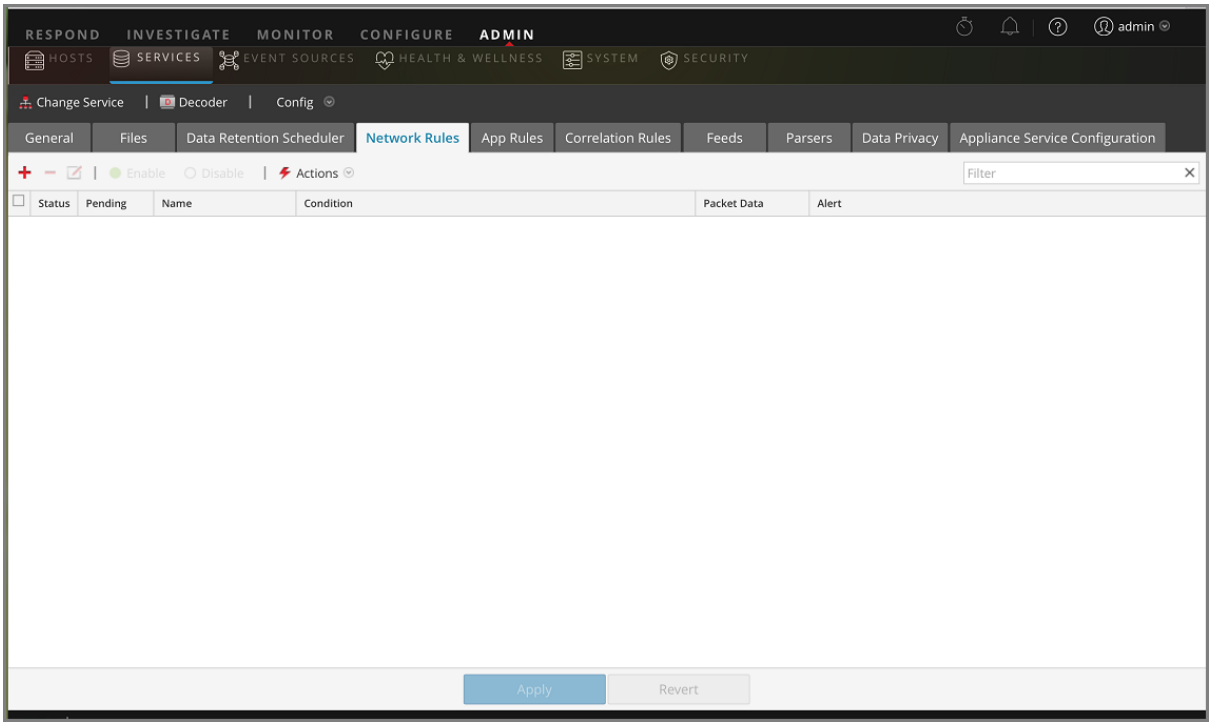
- Nom de la règle : Filtre sous-réseau
- Condition : `ip.addr=192.168.2.0/24`
- Action de règle : Filtrer

Les méta-entités, qui fournissent un moyen de travailler avec plusieurs méta-clés en même temps, peuvent être utilisées dans les règles d'application, mais ne sont pas prises en charge dans les règles de réseau, car les métadonnées disponibles sont trop limitées. Pour plus d'informations sur les méta-entités, reportez-vous au *Guide de réglage de base de données principale*.

Ajouter ou modifier une règle réseau :

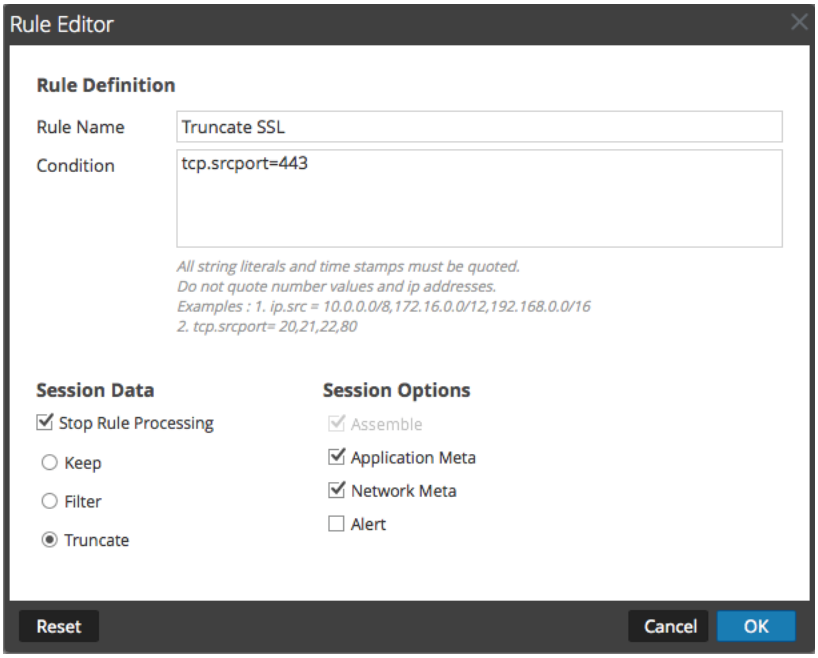
1. Accédez à **ADMIN > Services,** sélectionnez un service Decoder, puis  **> Vue > Config**.
   La vue Configuration des services pour le service sélectionné s'affiche.

2. Sélectionnez l'**onglet Règles réseau**.
   L'onglet Règles réseau s'affiche.



3. Sous l'onglet **Règles réseau**, procédez de l'une des façons suivantes :

   - Pour ajouter une nouvelle règle, cliquez sur  .
   - Si vous modifiez une règle, sélectionnez la règle dans la grille de règles, puis cliquez sur  .
     La boîte de dialogue Éditeur de règles s'affiche.



4. Dans le champ **Nom de la règle**, saisissez le nom de la règle. Par exemple, pour une règle qui tronque tous les SSL du port source, saisissez **Tronquer SSL**.
5. Dans le champ **Condition**, élaborez la condition de règle qui déclenche une action lorsqu'elle est remplie. Vous pouvez effectuer votre saisie directement dans le champ ou élaborer la condition dans ce champ à l'aide des métadonnées de la fenêtre Actions. Lors de l'élaboration de la définition de règle, NetWitness Platform affiche des erreurs et avertissements de syntaxe. Par exemple, pour tronquer tous les SSL à partir du port source, `tcp.srcport=443`.
   Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. N'utilisez pas de guillemets avec les valeurs numériques et les adresses IP. Configurer les règles de Decoder fournit des informations supplémentaires. Clés méta prises en charge dans les conditions de règles réseau décrit les clés méta dont NetWitness Platform prend en charge l'utilisation dans les conditions de règle réseau.
6. Si vous souhaitez mettre fin à l'évaluation de cette règle, activez la case à cocher **Arrêter le traitement des règles**.
7. Dans la section **Données de session**, choisissez l'une des actions suivantes à appliquer lorsqu'un paquet correspondant est trouvé :
   - **Conserver** : La charge du paquet et les métadonnées associées sont enregistrées lorsqu'elles correspondent à la règle.
   - **Filtrer** : Le paquet n'est pas enregistré lorsqu'il correspond à la règle.
   - **Tronquer** : La charge du paquet n'est pas enregistrée lorsqu'elle correspond à la règle, mais les en-têtes des paquets et autres métadonnées associées sont conservées.

8. Dans la section **Options de session**, sélectionnez toutes les options liées à ce qui suit :
   - **Assembler** : L'assembleur assemble la chaîne de paquets lorsqu'elle correspond à la règle.
   - **Méta réseau :** Le paquet génère des métadonnées réseau lorsqu'il correspond à la règle.
   - **Méta application** : Le paquet génère des métadonnées d'application lorsqu'il correspond à la règle.
   - **Alerte** : Le paquet génère une alerte personnalisée lorsque les métadonnées correspondent à la règle.

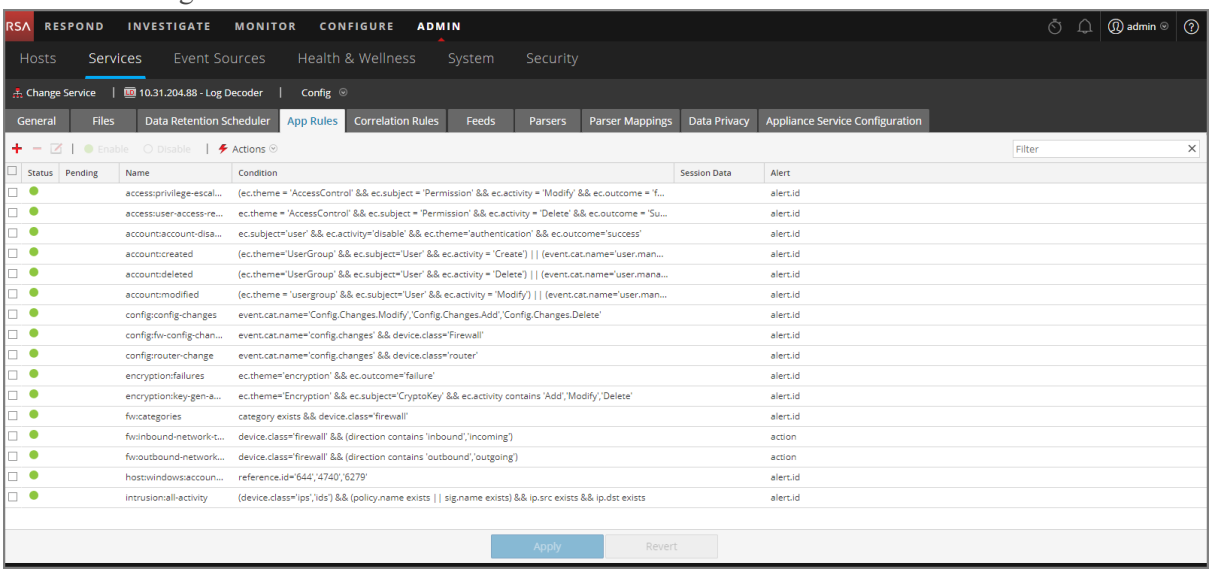
9. Pour enregistrer la règle et l'ajouter à la grille, cliquez sur **OK**.
   La règle est ajoutée à la fin de la liste ou insérée à l'endroit que vous avez indiqué dans le menu contextuel.
10. Vérifiez que la séquence d'exécution de la règle est correcte par rapport aux autres règles de la liste. Si nécessaire, déplacez la règle.
11. Pour appliquer la règle mise à jour au Decoder, cliquez sur **Appliquer**.
    NetWitness Platform enregistre un snapshot des règles actuellement appliquées, puis applique l'ensemble mis à jour au Decoder et supprime l'indicateur en attente des règles qui étaient en attente.

Corriger les règles contenant une syntaxe non valide

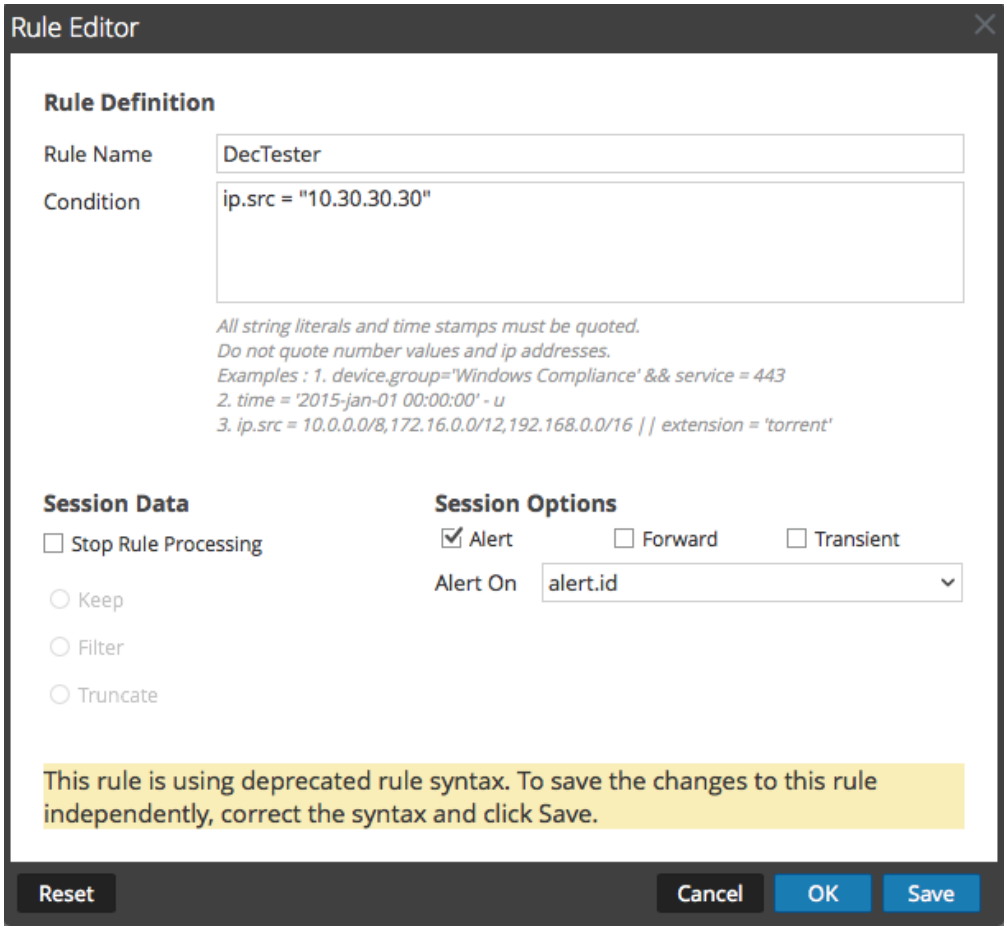
Après la mise à jour vers NetWitness Platform 11.x, l'interface utilisateur signale les règles dont la syntaxe n'est pas valide. L'éditeur de règles fournit des infobulles supplémentaires. Une fois les règles corrigées, les mises en surbrillance disparaissent. La section Configurer les règles de Decoder indique que toutes les requêtes et conditions de règles dans NetWitness Platform doivent suivre.

Pour corriger les règles contenant une syntaxe non valide :

1. Accédez à **ADMIN > Services**.
2. Dans la vue **Services**, sélectionnez un Decoder, puis **> Vue > Configuration**.
3. Dans la vue **Configuration des services**, sélectionnez l'un des onglets Règles : Règles réseau, Règles d'application ou Règles de corrélation.
   L'onglet Règles du type de règle sélectionné affiche le nombre de règles utilisant la syntaxe non valide et les règles non valides sont mises en surbrillance.



4. Sélectionnez une règle non valide, puis cliquez sur .
   L'éditeur de règles affiche des informations supplémentaires pour la règle non valide et comprend une option supplémentaire permettant l'enregistrement.



5. Dans le champ **Condition**, corrigez la syntaxe de la règle.
   Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre et adresses IP entre guillemets. Configurer les règles de Decoder fournit des informations supplémentaires.
   Par exemple, si la condition de règle non valide est `ip.src="10.30.30.30"`, corrigez la syntaxe supprimant les guillemets : `ip.src=10.30.30.30`
6. Exécutez l'une des opérations suivantes :
   - Pour corriger chaque règle, cliquez sur **Enregistrer**.
     La règle corrigée est appliquée indépendamment au Decoder. La règle corrigée s'affiche sous l'onglet Règles sans la mise en surbrillance.
   - Pour corriger la règle et l'appliquer ultérieurement au Decoder avec d'autres règles, cliquez sur **OK**.
     La règle corrigée s'affiche sous l'onglet Règles sans la mise en surbrillance. La règle n'est pas appliquée au Decoder.

Commandes de Decoder pour la gestion des règles

Dans la base de données NetWitness Core, l'arborescence de règles conserve les principales fonctionnalités associées à la gestion des règles pour tous les services Core qui possèdent des règles : Concentrators, Decoders, Log Decoders et Archivers. Bien qu'il soit possible de gérer les règles dans l'interface utilisateur NetWitness Platform, les utilisateurs avancés peuvent également gérer les règles à l'aide d'une ligne de commande pour ajouter, fusionner, remplacer, supprimer et valider les règles sur un service. Cette section fournit un bref tour d'horizon des commandes et de leur utilisation. Voici les commandes disponibles :

- `add` : ajoute une règle unique à la position spécifiée.
- `clear` : supprime toutes les règles existantes sur le nœud actuel du service. Par exemple, la commande utilisée dans le nœud `/decoder/config/rules/application` supprime toutes les règles d'application existantes sur le Decoder.
- `delete` : supprime une ou plusieurs règles à une position et un nombre spécifiés.
- `merge` : fusionne un ensemble de règles transmises avec un ensemble de règles existantes. Les règles existantes qui correspondent aux règles entrantes (par nom ou règle) sont remplacées ; dans le cas contraire, les règles sont insérées à la position indiquée, comme décrit dans Commande Merge.
- `replace` : supprime toutes les règles existantes et les remplace par l'ensemble de règles entrantes.
- `validate` : valide la syntaxe d'une règle, mais ne valide pas les clés méta.

Commande Add

La commande `add` ajoute la règle à l'ensemble de règles existantes. La mise en forme est importante car l'API utilise des guillemets doubles dans le langage de règles et utilise également des guillemets doubles en tant que paramètres pour toutes les API RSA NetWitness® Platform. Par conséquent, vous devez neutraliser les guillemets doubles dans la règle elle-même en les faisant précéder par une barre oblique inversée (\). Voici la syntaxe de la commande :

```
add rule=<string> name=<string> alert=<string, optional> atPos=<<uint32, optional>
```

- `rule` est la règle à ajouter. N'oubliez pas de placer des guillemets doubles autour des règles avec un espace et de neutraliser les guillemets doubles qui font partie de la règle avec une barre oblique inversée.
- `name` est le nom de la règle.
- `alert` est l'alerte pour la règle (le cas échéant).
- `atPos` est la position à laquelle la règle doit être ajoutée (basée sur 1). Zéro correspond à la partie supérieure de la liste et n'importe quel nombre supérieur à la taille actuelle de la liste est ajouté à la liste.

Exemple de commande permettant d'ajouter une règle à l'aide de NwConsole

```
send /decoder/config/rules/application add rule="ip.src exists" order=1
alert=alert.id name=testrule
```

Par exemple, prenons la règle suivante :

```
alias.host = "myPC" && country.src="china","russian federation"
```

Pour ajouter cet élément comme règle, vous devez envoyer les paramètres suivants :

```
rule="alias.host = \"myPC\" && country.src=\"china\",\"russian federation\""
name=myRule filter
```

Remarquez comme tous les guillemets doubles ont été annulés au sein du paramètre d'une règle. Une astuce simple pour optimiser la lisibilité consiste à utiliser des guillemets simples au sein d'une règle. Les guillemets simples et doubles sont interchangeables dans la règle et le langage de la requête, mais pas dans les paramètres de l'API (où seuls les guillemets doubles sont pris en charge). Par conséquent, voici un exemple plus lisible :

```
rule="alias.host = 'myPC' && country.src='china','russian federation'"
name=myRule filter
```

Commande Merge

La commande `merge` est utilisée pour fusionner une liste de règles entrantes avec des règles existantes dans le service. Son fonctionnement est le suivant :

- Elle détecte des règles existantes qui correspondent via le nom ou une règle de correspondance, elle met à jour le nom de la règle existante et conserve la même position.
- Elle insère les nouvelles règles dans la liste des règles en fonction de la position du NUMÉRO. Si le numéro est zéro, elle se place en haut de la liste.
- Elle traite les règles dans l'ordre reçu, donc si vous disposez de deux règles qui portent le numéro zéro, la deuxième règle est traitée après la première et demande la première place. Toutes les règles existantes sont déplacées vers le bas de deux places. Tous les numéros supérieurs aux positions des règles existantes sont ajoutés après la dernière règle existante et numérotés dans l'ordre.
- Toute règle non numérotée est ajoutée après la dernière règle existante et numérotée dans l'ordre.

Voici la syntaxe de la commande Merge :

```
merge --file-data=<string> --file-format<string>
```

- `file-data` est le chemin complet et le nom du fichier de règles à fusionner.
- `file-format` est le format du fichier de règles. Les valeurs valides sont `params-list`, `string`, `params`, `binary` et `params-binary`.

Méthodes d'envoi d'une liste de règles vers un service

Il existe deux façons d'envoyer la liste des règles. Vous pouvez l'envoyer sous forme de fichier `.nwr` (règle NetWitness) ou sous forme d'ensemble numéroté de paramètres, chaque nombre indiquant la position pour insérer la règle, ainsi que la règle codée. Si vous souhaitez voir la liste actuelle de règles sur un service, vous devez exécuter la commande `ls` sur la catégorie de la règle (par exemple, les règles d'application sur un Decoder se trouvent dans `/decoder/config/rules/application`).

Exemple de commandes permettant de répertorier les règles existantes à l'aide de NwConsole :

```
login <hostname>:50004 <username> <password>
cd /decoder/config/rules/application
ls
```

Autre exemple permettant de répertorier les règles existantes avec NwConsole :

```
send /decoder/config/rules/application ls
```

Exemple de la commande permettant de pointer vers les règles réseau dans le port RESTful qui prend en charge une application de base `admin HTML`.

```
http[s]://<decoder>:50104/decoder/config/rules/network
```

Envoyer un fichier de règles NetWitness

Commençons par un exemple de fichier `nwr`, chaque règle doit se trouver sur une ligne distincte :

```
rule="ip.src=192.168.0.1" name=first keep
rule="ip.src=192.168.1.1" name=second alert=risk.info
rule="ip.src=192.168.2.1" name=third filter
```

Pour transmettre et fusionner des règles à l'aide de NwConsole, utilisez les commandes suivantes :

```
login <hostname>:50004 <username> <password>
send /decoder/config/rules/application merge --file-data=/root/App_
Rules.nwr --file-format=params-list
```

Pour remplacer les règles existantes avec les règles contenues dans le fichier, au lieu d'utiliser la commande `merge`, utilisez la commande `replace`.

```
send /decoder/config/rules/application replace --file-
data=<pathname> --file-format=params-list
```

Pour fusionner les règles dans un fichier `nwr` en utilisant le port RESTful, vous pouvez utiliser la commande `curl` qui transmet les règles :

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-
stream" --data-binary @<pathname> -X POST
"http://<hostname>:50104/decoder/config/rules/application?msg=merge"
```

Les exemples transmettent les règles d'application. Pour pousser les règles du réseau, envoyez les règles à `/decoder/config/rules/network`. Pour les règles de corrélation, envoyez les règles à `/decoder/config/rules/correlation`.

Envoyer des paramètres numérotés

L'autre méthode permettant d'envoyer une liste de règles consiste à les envoyer sous forme de paramètres numérotés. La difficulté de cette méthode réside dans le fait d'utiliser obligatoirement un caractère d'échappement avec les guillemets au sein de chaque règle numérotée. Cependant, cela ne représente un problème que si vous essayez de le faire à la main. Par exemple, pour envoyer les règles ci-dessus sous forme de paramètres via NwConsole, utilisez la commande suivante :

```
send /decoder/config/rules/application merge
1="rule=\"ip.src=192.168.0.1\" name=first keep"
2="rule=\"ip.src=192.168.1.1\" name=second alert=risk.info"
3="rule=\"ip.src=192.168.2.1\" name=third filter"
```

Cette commande est difficile à lire parce que vous devez utiliser la barre oblique inversée (\) comme caractère d'échappement pour les guillements internes. Dans le cas contraire, ces deux commandes ont le même résultat. Fusion ou ajout de trois règles aux positions 1, 2 et 3. Si vous pensez que cela manque de lisibilité, voici à quoi ressemble la commande `curl` :

```
curl -u "<username>:<password>"
"http://<hostname>:50104/decoder/config/rules/application?msg=merge&1=rule%3D%
22ip.src%3D192.168.0.1%22%20name%3Dfirst%20keep&2=rule%3D%22ip.src%3D192.168.1
.1%22%20name%3Dsecond%20alert%3Drisk.info&3=rule%3D%22ip.src%3D192.168.2.1%22%
20name%3Dthird%20filter"
```

Pour plus d'informations sur la façon de neutraliser les guillemets doubles à l'intérieur des paramètres, reportez-vous à la section Commande Add.

Règles de tri applicables lors de la transmission

Les règles transmises sont triées de l'une des deux manières suivantes. Lors du passage sous forme de paramètres, le numéro de chaque paramètre détermine l'ordre d'insertion. Sans véritable numéro, `merge` vérifie le paramètre `order` au sein de la règle elle-même et utilise cette valeur si elle s'y trouve.

Remarque : L'utilisation de `order` est le seul moyen de définir l'ordre dans un fichier `.nwr`. Si aucun nombre ou paramètre `order` n'est trouvé, il n'existe aucune garantie sur l'ordre d'insertion.

Exemple

Decoder dispose toujours des règles d'application suivantes installés. Notez que la numérotation est TOUJOURS consécutive et commence à 1 :

```
0001 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-
PC'" name=first keep
0002 : rule="ip.src=192.168.1.1" name=second alert=risk.info
0003 : rule="ip.src=192.168.2.1" name=third filter
```

Et vous souhaitez fusionner les quatre règles suivantes :

```
rule="ip.src=192.168.3.1" name=third keep
rule="ip.dst=192.168.4.1" name=NewRule filter order=0
rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append
rule="service=80,443" name=web filter order=3
```

Utilisez n'importe quelle méthode pour transmettre vos règles et voici le résultat :

```
0001 : rule="ip.dst=192.168.4.1" name=NewRule filter order=1
0002 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-
PC'" name=first keep order=2
0003 : rule="service=80,443" name=web filter order=3
0004 : rule="ip.src=192.168.1.1" name=second alert=risk.info order=4
0005 : rule="ip.src=192.168.3.1" name=third keep order=5
0006 : rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=6
```

Des surprises ? Voici le traitement qui a été réservé à chaque règle.

```
1. rule="ip.src=192.168.3.1" name=third keep
```

Cette règle présente le même nom qu'une règle existante sur le Decoder (troisième). Ainsi, la règle a mis à jour la règle existante, `changing _filter_ to _keep_`.

```
2. rule="ip.dst=192.168.4.1" name=NewRule filter order=0
```

Cette règle est nouvelle et comporte `order=0`, ce qui implique une insertion tout en haut.

```
3. rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append
```

Cette règle comporte un `append` non numérique pour `order`. Par conséquent, elle est passée à la fin de la liste. Vous pouvez obtenir le même résultat en donnant un nombre très élevé, comme `999999`.

```
4. rule="service=80,443" name=web filter order=3
```

Cette règle est la dernière mais elle comporte `order=3`, par conséquent, si elle ne correspond pas à une règle existante par le nom ou le texte de la règle lui-même, elle doit être placée dans la position 3. Et voici la troisième règle de la liste. Toutes les règles suivantes ont été transférées plus bas.

Commande Replace

La commande `replace` supprime toutes les règles existantes et les remplace par la liste de règles entrantes. Reportez-vous à la section Commande Merge pour obtenir plus d'informations sur la façon de mettre en forme la liste de règles entrantes et sur le fonctionnement du tri.

Voici un exemple de la commande `replace` utilisant un fichier de règles NetWitness :

```
send /decoder/config/rules/application replace --file-data=/root/Decoder-
AppRules.nwr --file-format=string
```

Voici un exemple de la commande `replace` utilisant les paramètres numérotés :

```
send /decoder/config/rules/application replace 1="rule=\"ip.src exists\"
name=\"test rule\" order=1 alert=alert.id"
```

Commande Clear

La commande `clear` supprime toutes les règles existantes sur le service. Voici un exemple de la commande :

```
send /decoder/config/rules/application clear
```

Commande Delete

La commande `delete` supprime une ou plusieurs règles sur le service.

```
delete atPos <uint32> count <uint32, optional>
```

- `atPos` supprime la règle à la position donnée. Les règles sont numérotées à partir de 1 et dans un ordre séquentiel.
- `count` supprime une ou plusieurs règles en commençant par `atPos`. Il s'agit d'un paramètre facultatif qui définit le nombre de règles à supprimer en commençant par `atPos`. La valeur par défaut est 1.

Cet exemple de la commande supprime les quatre règles commençant à la position 0003 :

```
send /decoder/config/rules/application delete atPos=0003 count=4
```

Commande Validate

La commande `validate` prend la règle fournie et vérifie qu'elle est correctement analysée. N'oubliez pas que cette commande ne peut pas vérifier si les clés de langue et les entités sont valides.

```
validate rule <string>
```

`rule` est le nom de la règle de validation. Veillez à placer des guillemets doubles autour des règles avec un espace.

Configurer les feeds et les parsers

Les feeds et les analyseurs sont responsables de l'analyse des paquets et des logs lors de la capture ou de l'import dans un Decoder ou Log Decoder. Généralement, ils sont utilisés pour l'extraction de métadonnées statiques et l'identification des services. La définition flexible permet l'extension personnalisée des services définis par le Core pour fournir une identification du type de service supplémentaire et une extraction des métadonnées. Elle est importante à cause du volume d'applications personnalisées qui sont utilisées sur les réseaux.

Remarque : Sauf indication contraire, toutes les références aux Decoders s'appliquent également aux Log Decoders.

Configurer les analyseurs

NetWitness Platform dispose d'un ensemble d'analyseurs de base qui sont définis par le système, et offre la possibilité d'ajouter des analyseurs supplémentaires. Chaque analyseur est configurable dans la Vue Configuration des services - onglet Général. Le panneau Configuration des analyseurs permet d'activer ou de désactiver les analyseurs à utiliser sur le Decoder en plus de limiter les métadonnées créées par l'analyseur.

En outre, il existe plusieurs types d'analyseurs personnalisés configurables :

- GeoIP ou GeoIP2 : cet analyseur associe les adresses IP aux emplacements géographiques. Pour les nouvelles installations et mises à niveau, l'analyseur GeoIP2 est activé par défaut. Un seul de ces analyseurs peut être activé à la fois. Pour plus d'informations sur ces analyseurs, voir Parsers GeoIP2 et GeoIP.
- Search : cet analyseur est configuré par l'utilisateur pour générer des métadonnées par analyse des mots clés prédéfinis et des expressions régulières.
- FLEXPARSE (obsolète) : il s'agit d'un langage de définition d'analyseur générique pour étendre la prise en charge du protocole de l'application actuelle du Decoder. Cet analyseur est désactivé par défaut (reportez-vous à la section Activer ou désactiver les systèmes d'analyse Lua et Flex).
- Lua : cet analyseur est défini à l'aide du langage de script Lua pour étendre la prise en charge du protocole d'application en cours du Decoder.
- enVision : cet analyseur d'application prend en charge le Log Decoder et est configuré pour générer des métadonnées en analysant les fichiers logs.
- Snort® : cet analyseur prend en charge les capacités de détection de la charge utile des règles Snort IDS. Les règles et la configuration de Snort sont ajoutées au répertoire `parsers/snort` pour l'investigation et le décodeur (voir Parsers Snort).

Dans la vue Configuration des services > onglet Analyseurs, vous pouvez visualiser les analyseurs déployés sur un Decoder, télécharger les analyseurs et supprimer les analyseurs déployés. L'interface utilisateur comprend un indicateur si l'analyseur provient de Live Services, installé par NetWitness Platform ou téléchargé manuellement. Les parsers peuvent être ajoutés et supprimés alors qu'un Decoder est en cours d'exécution sans que cela ait d'impact sur la capture.

De plus, vous pouvez télécharger les analyseurs à l'aide de NetWitness Platform Live Services.

Configurer les feeds

NetWitness Platform utilise des feeds pour créer les métadonnées en fonction des valeurs de métadonnées définies en externe. Un feed est une liste de données qui sont comparées à des sessions au fur et à mesure de leur capture ou de leur traitement. Pour chaque correspondance, des métadonnées supplémentaires sont créées. Ces données pourraient identifier et classer les adresses IP malveillantes ou intégrer des informations supplémentaires telles que le département et l'emplacement en fonction des affectations du réseau interne. Certains exemples de feeds comprennent les feeds de menaces pour identifier les BOTNets, les mappages DHCP ou même des informations Active Directory comme les emplacements physiques ou les départements logiques.

Vous pouvez utiliser le module Live dans NetWitness Platform pour obtenir des feeds de sources extérieures. La rubrique « Contenu Live dans NetWitness Platform » du *Guide de gestion des services Live* fournit une présentation de l'outil de gestion du contenu Live.

L'interface utilisateur de NetWitness Platform vous permet de consulter la liste des feeds actuellement déployés, avec un indicateur si le feed provenant de Live a été installé via NetWitness Platform, ou manuellement. Les feeds peuvent être ajoutés, supprimés et mis à jour alors qu'un Decoder est en cours d'exécution sans que cela ait d'impact sur la capture.

L’assistant de feed personnalisé permet la création et le déploiement de feeds Decoder personnalisés en fonction d'une logique déterministe qui offre les clés métas spécifiques aux Decoders et Log Decoders sélectionnés. Bien que l'assistant guide les utilisateurs tout au long du processus pour créer à la fois des feeds à la demande et périodiques, il est utile de comprendre la forme et le contenu d'un fichier de feed lorsque vous créez un feed.

NetWitness Platform dispose d'un assistant Feed personnalisé, qui rationalise la tâche de création et de gestion des feeds personnalisés, ainsi que le renseignement des feeds pour les Decoders et Log Decoders sélectionnés. Par ailleurs, vous pouvez télécharger et modifier les fichiers de feeds existants, puis modifier le feed ou en créer un nouveau à l'aide du fichier modifié.

Structure des fichiers de définition des feeds personnalisés

L'assistant Feed personnalisé de NetWitness Platform permet la création et le déploiement rapides de feeds Decoder personnalisés en fonction d'une logique déterministe qui offre les clés métas spécifiques aux Decoders et Log Decoders sélectionnés. Bien que l'assistant guide les utilisateurs tout au long du processus pour créer à la fois des feeds à la demande et périodiques, il est utile de comprendre la forme et le contenu d'un fichier de feed lorsque vous créez un feed.

Les noms de fichier de feed dans RSA NetWitness Platform se présentent sous la forme `<filename>.feed`. Pour créer un feed, NetWitness Platform a besoin d'un fichier de données de feed au format `csv` ou `.xml` et un fichier de définition de feed au format `.xml`, décrivant la structure d'un fichier de données de feed. L'assistant Feed personnalisé peut créer le fichier de définition de feed en se basant sur un fichier de données de feed, ou en se basant sur un fichier de données de feed et le fichier de définition de feed correspondant.

Les fichiers que vous utilisez pour créer un feed sur demande doivent être stockés sur votre système de fichiers local. Les fichiers utilisés pour créer un feed récurrent doivent être stockés sur une URL accessible, où NetWitness Platform peut récupérer la dernière version du fichier pour chaque récurrence. Après la création d'un feed NetWitness Platform, vous pouvez télécharger le feed sur votre système de fichiers local, modifier les fichiers de feed, puis modifier le feed NetWitness Platform afin qu'il utilise les fichiers de feed mis à jour.

Échantillon de fichier de définition de feed

Voici un exemple de fichier de définition de feed nommé `dynamic_dns.xml`, que NetWitness Platform crée en se basant sur vos entrées dans l'assistant Feed personnalisé. Il définit la structure du fichier de données de feed intitulé `dynamic_dns.csv`.

Remarque : Le chemin d'accès du fichier de feed doit être `.csv`, quel que soit le type de feed (par défaut ou STIX).

```
<?xml version="1.0" encoding="utf-8"?>
 <FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

   <FlatFileFeed name="Dynamic DNS Domain Feed"
   path="dynamic_dns.csv"
   separator=","
   comment="#"
   version="1">

   <MetaCallback
   name="alias.host"
   valuetype="Text"
   apptype="0"
   truncdomain="true"/>

   <LanguageKeys>
            <LanguageKey name="threat.source" valuetype="Text" />
            <LanguageKey name="threat.category" valuetype="Text" />
            <LanguageKey name="threat.desc" valuetype="Text" />
   </LanguageKeys>
```

```
    <Fields>
    <Field index="1" type="index" key="alias.host" />
    <Field index="4" type="value" key="threat.desc" />
    <Field index="2" type="value" key="threat.source" />
    <Field index="3" type="value" key="threat.category" />
    </Fields>
    </FlatFileFeed>

</FDF>
```

Équivalents de définition de feed pour les paramètres de l'assistant de feed personnalisé

L'assistant Feed personnalisé de NetWitness Platform fournit des options permettant de définir la structure du fichier de feed de données. Ils correspondent directement aux attributs du fichier de définition de feed (.xml).

Paramètre NetWitness Platform	Équivalent du fichier de définition de feed
(Onglet Définir le feed) Type de feed	Select : **Par défaut** - pour définir un feed basé sur un fichier de données de feed au format .csv. **STIX** - pour définir un feed basé sur un fichier STIX au format .xml.
(Onglet Définir le feed) Type de tâche par défaut	Select : **Ad hoc** - pour créer un feed à la demande. **Récurrent** - pour mettre à jour le fichier .csv ou .xml de manière permanente et le stocker dans un emplacement accessible à NetWitness Platform , de sorte que NetWitness Platform télécharge un fichier à intervalles réguliers et le transmette aux périphériques en aval.
(Onglet Définir le feed) **Nom**	Nom du feed personnalisé dans le fichier de données du feed. Il correspond à l'attribut `flatfeedfile name` dans le fichier de définition de feed. Par exemple, Dynamic DNS Test Feed. **Remarque :** Vous pouvez utiliser des caractères spéciaux pour définir le nom du feed personnalisé.
(Onglet Définir le feed) **Fichier**/ **Parcourir**	Il s'agit du nom du fichier de données du feed. Il correspond à l'attribut `flatfeedfile path` dans le fichier de définition de feed. Par exemple, `dynamic_dns.csv`.
(Onglet Options avancées) **Fichier de feed XML**	Le nom du fichier de définition de feed. Par exemple : `dynamic_dns.xml`.

Paramètre NetWitness Platform	Équivalent du fichier de définition de feed
(Onglet Options avancées) **Séparateur**	Caractère de séparation utilisé pour séparer les attributs dans le fichier de données du feed. Il correspond à l'attribut `latfeedfile separator` dans le fichier de définition de feed. Par exemple, une virgule.
(Onglet Options avancées) **Commentaire**	Caractère utilisé pour identifier un commentaire dans le fichier de données du feed. Il correspond à l'attribut `flatfeedfile comment` dans le fichier de définition de feed. Par exemple, `#`.
(onglet Définir des colonnes, Définir l'index) **Type**	Type de valeur de recherche dans la position d'index du fichier de données de feed. **IP** indique que chaque ligne du fichier de données de feed contient une adresse IP dans la position de valeur de recherche. La valeur IP est au format décimal à points (par exemple, 10.5.187.42). **Plage IP** indique que chaque ligne du fichier de données de feed contient une plage d'adresses IP dans la position de valeur de recherche. La plage IP est au format CIDR (par exemple, 192.168.2.0/24). **Non IP** indique que chaque ligne du fichier de données de feed contient une valeur de métadonnées autre que l'adresse IP dans la position de valeur de recherche. Les champs Type de service, Tronquer le domaine et Clé de retour deviennent actifs dans le cas d'un index Non IP.
(onglet Définir des colonnes, Définir l'index) **CIDR**	Spécifie que la valeur IP dans la position de recherche est au format CIDR. L'attribut **CIDR** définit le format de l'adresse IP dans le champ sur la notation Classless Inter-Domain Routing (CIDR).
(Onglet Définir des colonnes, Définir l'index) **Type de service**	Pour un index Non IP, type de service en nombre entier permettant de filtrer les recherches méta. Il correspond à l'attribut `MetaCallback apptype` dans le fichier de définition de feed. Une valeur de `0` indique qu'il n'y a aucun filtrage par type de service.
(Onglet Définir des colonnes, Définir l'index) **Tronquer le domaine**	Pour un index Non IP, le système peut extraire des données l'élément spécifique à l'hôte pour les métavaleurs qui contiennent les noms de domaine (par exemple, les noms d'hôtes). Tronquer le domaine correspond à l'attribut `MetaCallback truncdomain`. Si la valeur est `www.example.com`, elle est tronquée à `example.com`. Une valeur **Faux** sélectionne aucune troncature et une valeur **Vrai** sélectionne la troncature.

Paramètre NetWitness Platform	Équivalent du fichier de définition de feed
(Onglet Définir des colonnes, Définir l'index) **Clés de rappel**	Pour un index Non IP, les métaclés disponibles à mettre en correspondance à la place de ip.src/ip.dst (les valeurs par défaut pour le type d'index IP) peuvent être sélectionnées dans la liste déroulante. La Clé de rappel correspond à l'attribut `MetaCallback name`, et la colonne index du fichier csv doit contenir des données pouvant correspondre à la clé méta choisie. Par exemple, si la clé méta du nom d'utilisateur est choisie, la colonne index du fichier csv doit être renseignée avec les utilisateurs à associer.
(Onglet Définir des colonnes, Définir l'index) **Colonne index**	Identifie la colonne du fichier de données de feed qui donne la valeur de recherche pour la ligne. Chaque position de chaque ligne du fichier de données de champ est identifiée par l'attribut **Index de champ** dans le fichier de définition de feed. Un champ dont l'index est **1** indique la première entrée de la ligne. Le second champ représente l'index **2**, le troisième champ l'index **3**, etc.
(DÉFINIR LES VALEURS) **Clé**	Nom de `LanguageKey`, tel qu'il est défini dans le fichier de définition de feed, pour lequel les méta sont créées à partir de cette ligne du fichier de données de feed. Il correspond à l'attribut `Field key` dans le fichier de définition de feed. Une clé ne s'applique qu'à un champ dont le type est défini sur `value`. Dans le fichier de définition de feed se trouve une liste de `LanguageKeys` de `index.xml`, ou un nom de récapitulatif si le Nom de la source et le Nom de destination sont utilisés. Par exemple, `reputation` est un nom de récapitulatif pour `reputation.src` et `reputation.dst`. Cette valeur est référencée par l'attribut clé Champ.

Exemples de fichiers pour un feed MetaCallback à l'aide de la plage d'index CIDR pour IPv4 et IPv6

Ces exemples de fichiers montrent comment utiliser des plages d'index CIDR pour IPv4 et IPv6 dans des feeds personnalisés MetaCallback. Comme avec d'autres feeds personnalisés, vous devez créer le fichier de données de feed au format .csv et un fichier de définition de feed au format .xml.

Remarque : L'utilisation de feeds MetaCallback avec des plages d'index CIDR est prise en charge uniquement par le biais de l'interface REST ou de l'assistant de configuration avancée.

L'exemple suivant affiche le contenu des fichiers `.csv` et `.xml` pour un feed MetaCallback à l'aide des plages d'index CIDR pour IPv4 ou IPv6.

`.csv file:`

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

`.xml file:`

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">
```

```
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0"
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

Remarque : Pour configurer une plage d'index CIDR pour les feeds avec un ou plusieurs MetaCallbacks de type de valeur IPv4 ou IPv6, le champ du type d'index DOIT contenir un attribut avec une plage `range="cidr"`. En outre, la configuration de l'index « cidr » pour des feeds avec MetaCallbacks de plusieurs types de valeur différentes n'est pas prise en charge

Créer un Feed personnalisé

Vous pouvez créer un feed personnalisé à l'aide de l'assistant Feed personnalisé. Pour exécuter cette procédure, vous devez disposer d'un fichier de données de feed au format `.csv` ou `.xml`. Si vous avez également un fichier de définition de feed associé au format `.xml`, qui décrit la structure du fichier de données de feed, vous pourrez utiliser le fichier de définition de feed pour créer un feed. L'assistant Feed personnalisé peut créer le feed en se basant sur un fichier de données de feed, ou en se basant sur un fichier de données de feed et le fichier de définition de feed correspondant.

Remarque : À partir de la version 10.6.1 ou d'une version supérieure, NetWitness Platform prend en charge STIX (un langage structuré qui décrit les informations sur les cybermenaces). Pour plus d'informations sur STIX et la manière de créer un feed STIX personnalisé, reportez-vous à la rubrique Créer un Feed STIX personnalisé dans le *guide de configuration Log Decoder*.

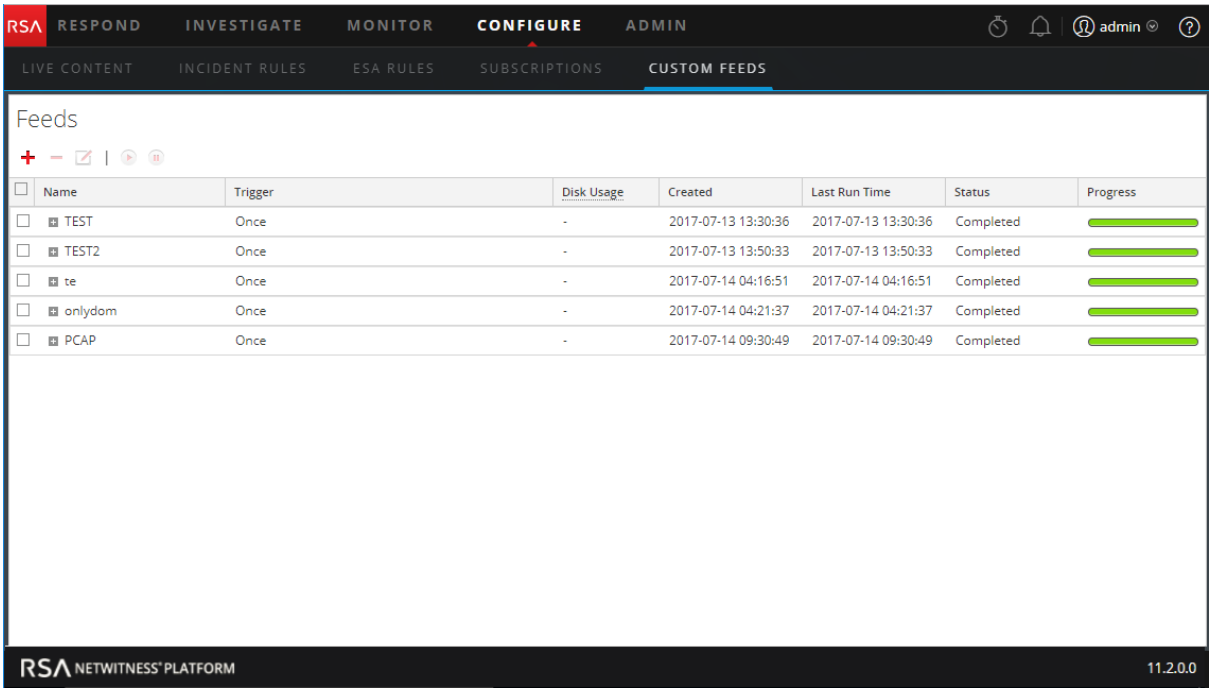
Le fichier de données de feed et éventuellement le fichier de définition de feed (`.xml`) doivent être disponibles sur le système de fichier local pour un feed personnalisé à la demande. Pour un feed personnalisé récurrent, les fichiers doivent être disponibles à une URL accessible au serveur NetWitness Platform.

Remarque : Lors de la création d'une source et d'une destination sur un Log Decoder, seule la clé méta source est renseignée. Vous ne pouvez pas utiliser un flux basé sur une plage ou sur CIDR. Vous devez répertorier chaque adresse IP unique. Pour remédier à ce problème, créez deux flux différents à l'aide des adresses IP et vous pourrez utiliser CIDR dans ces feeds.

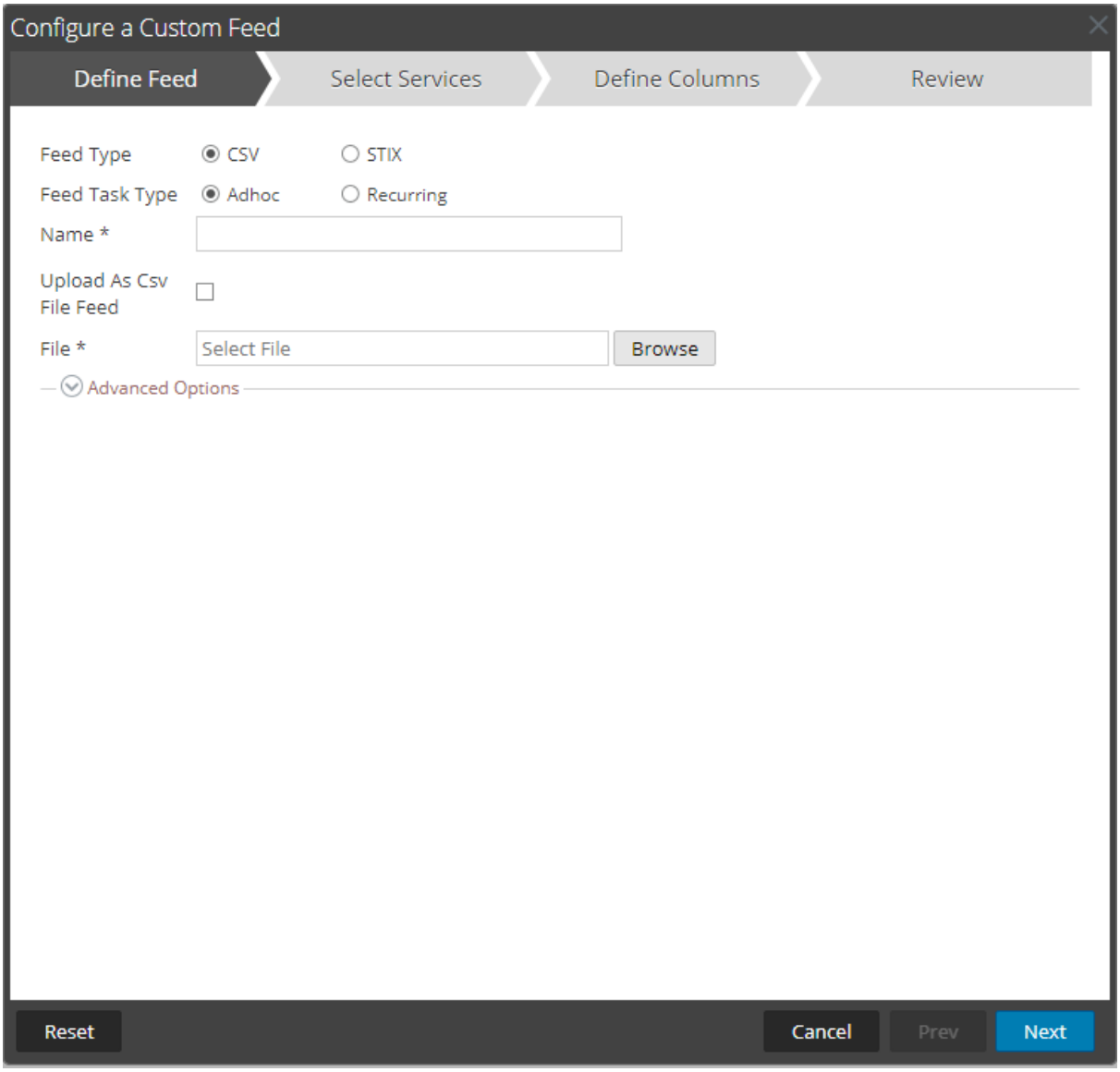
Pour créer un feed personnalisé :

1. Accédez à **CONFIGURER > Feeds personnalisés.**

2. Dans le panneau **Feeds**, cliquez sur +.
   La vue feeds personnalisés s'affiche.



3. Sélectionnez **Feed personnalisé**, puis cliquez sur **Suivant**.
   Le panneau Configurer un feed personnalisé s'affiche avec le formulaire Définir le feed ouvert.



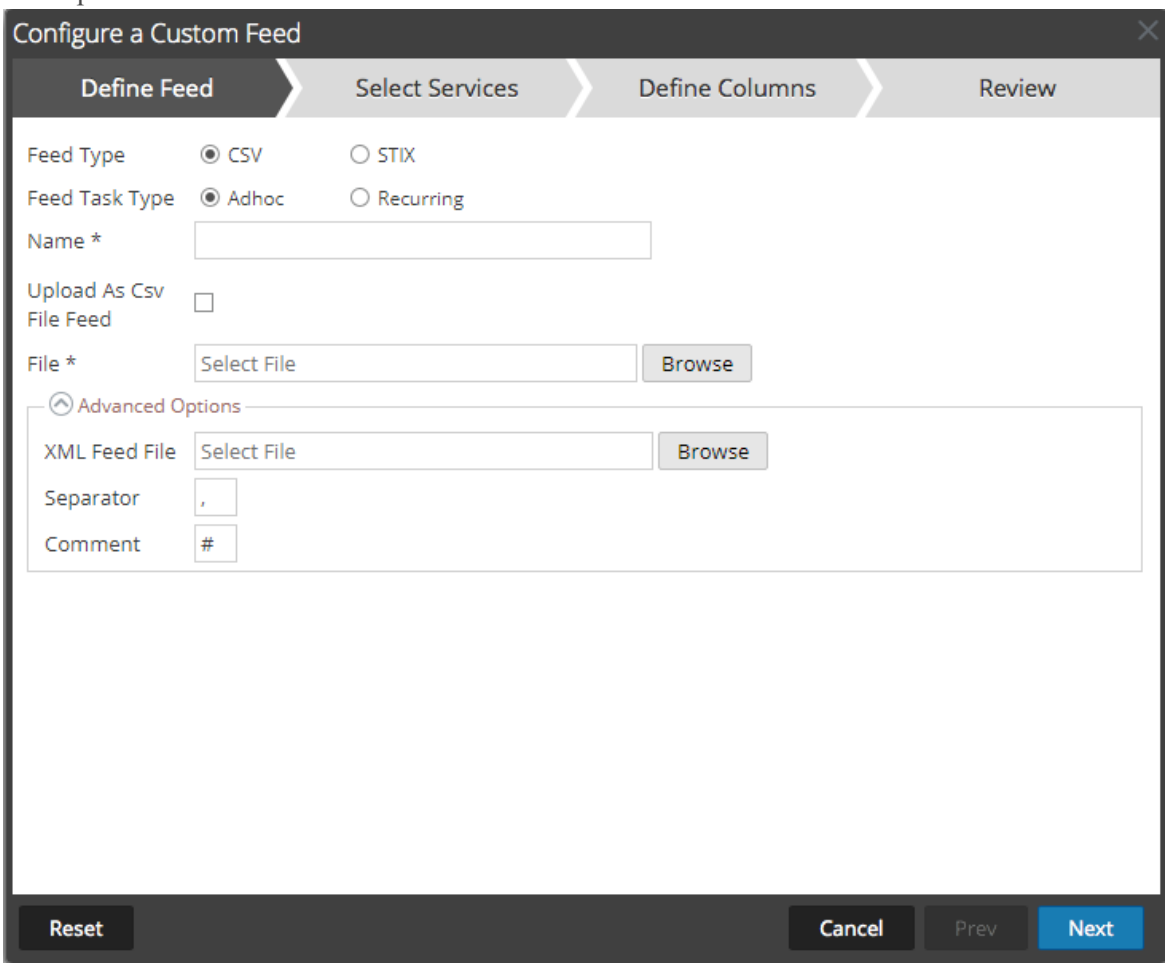
4. Sélectionnez le type de feed : **CSV** ou **STIX**.
5. Pour définir un feed basé sur un fichier de données de feed au format `.csv`, sélectionnez **CSV** (sélectionné par défaut) dans le champ **Type de feed**.
6. Pour définir une tâche de feed à la demande qui s'exécute une fois, sélectionnez **Ad hoc** dans le champ **Type de tâche par défaut** et procédez d'une des manières suivantes :
   a. (Conditionnel) Pour définir un feed basé sur un fichier de données de feed au format .csv, saisissez la case**Télécharger (envoyer) comme fichier Feed CSV**, saisissez le **Nom** du feed, sélectionnez un fichier de contenu au format .csv sur le système de fichiers local, puis cliquez sur **Suivant**. Si vous ne cochez pas la case, le fichier. csv sera un fichier FlatFileFeed.

Remarque : Lorsque vous activez la case à cocher Télécharger (envoyer) comme fichier Feed CSV, les options de feed XML sous la section Avancé ne sont pas disponibles.

b. (Conditionnel) Pour définir un feed basé sur un fichier de feed XML, sélectionnez **Options avancées**.

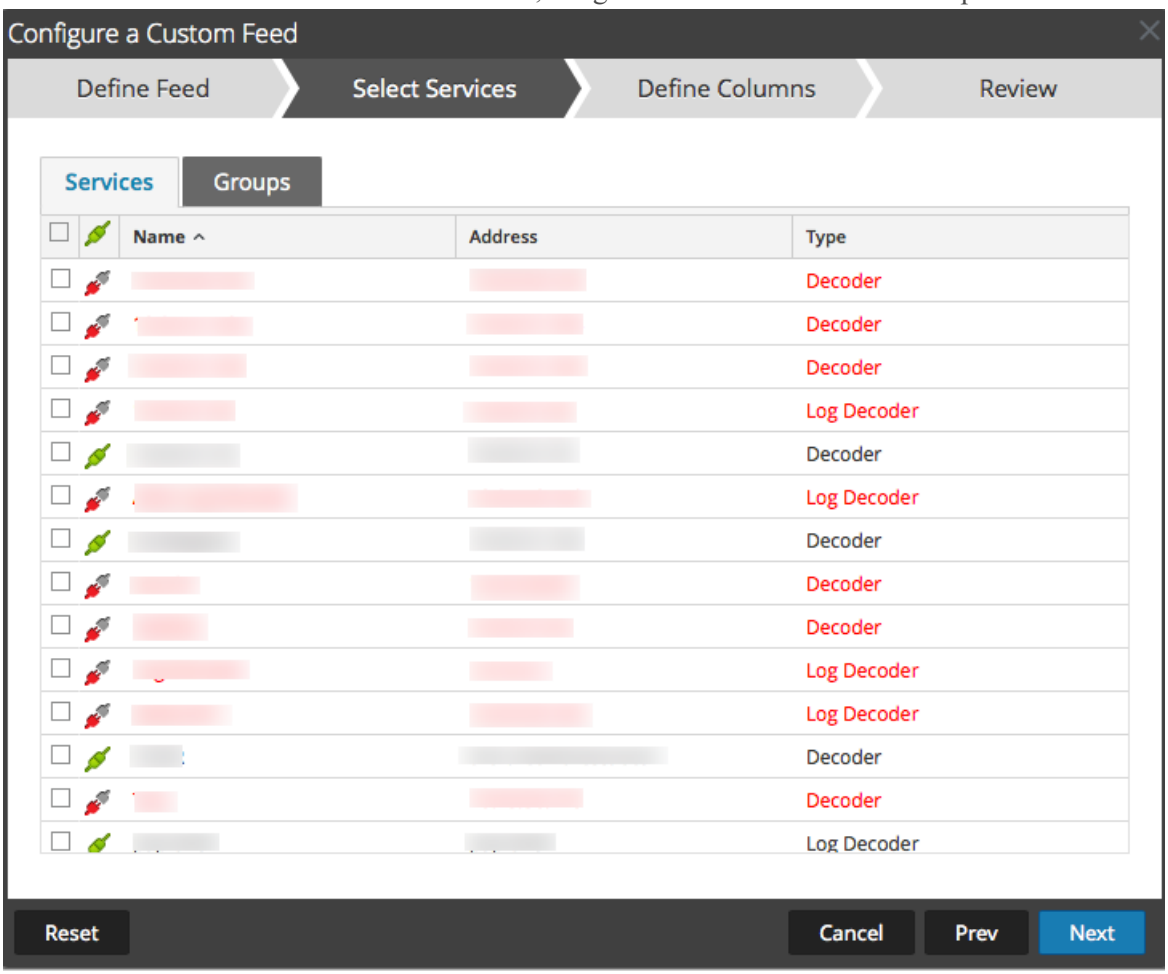
Remarque : Assurez-vous que la case à cocher Télécharger (envoyer) comme fichier Feed CSV est désélectionnée.

c. Les Options avancées s'affichent :



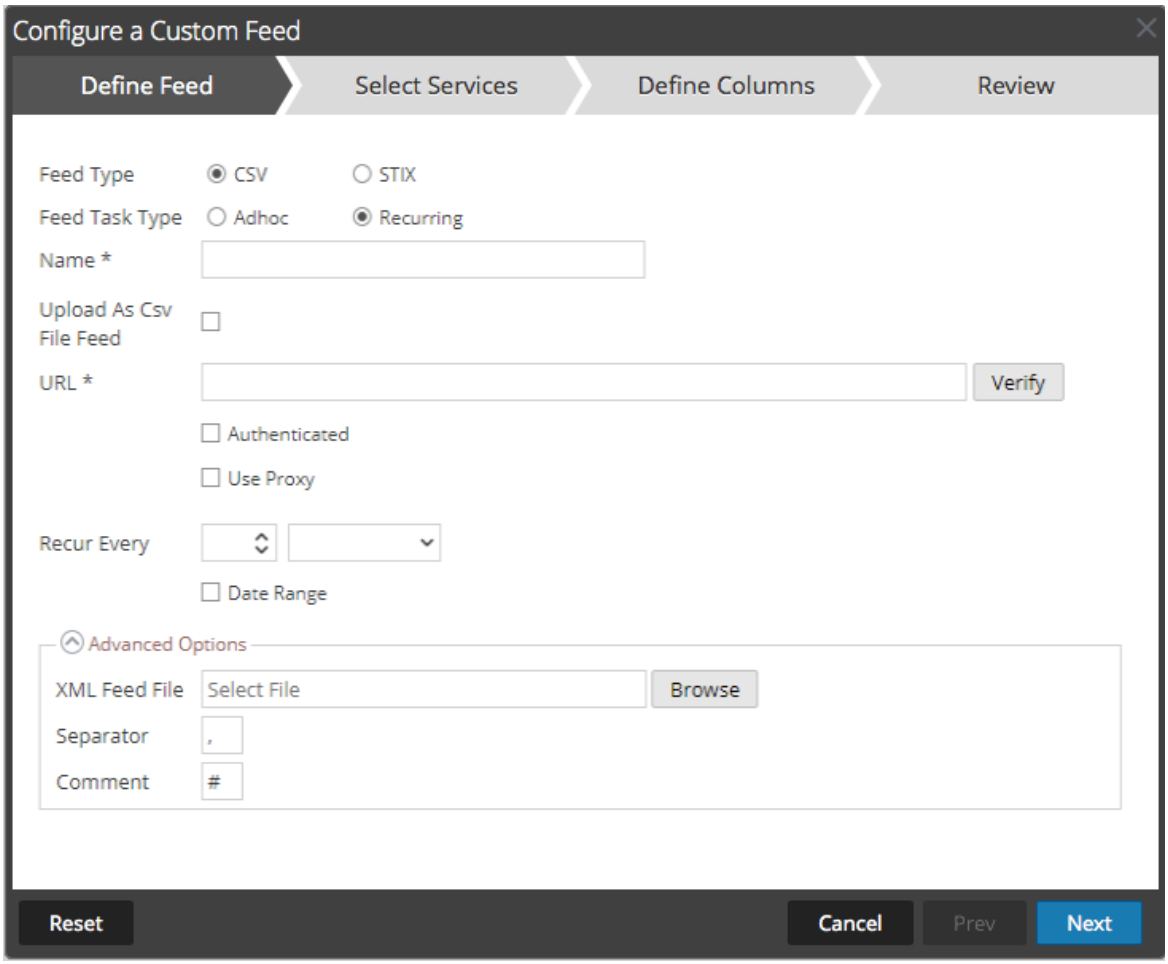
d. Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le Séparateur (par défaut, il s'agit de la virgule), et spécifiez les caractères du Commentaire utilisés dans le fichier de données de feed (la valeur par défaut est #) et cliquez sur **Suivant**.
Le formulaire Sélectionner des services s'affiche. Voici un exemple de formulaire pour un feed basé sur un fichier de données de feed, sans fichier de définition de feed. Si vous définissez un

feed basé sur un fichier de définition de feed, l'onglet Définir des colonnes n'est pas nécessaire.



7. Pour définir une tâche de feed récurrente qui s'exécute de manière répétée à des intervalles spécifiques, pendant une certaine période :

   a. Sélectionnez **Récurrent** dans le champ **Type de tâche de feed.**
   Le formulaire Définir le feed comprend les champs pour un feed récurrent.



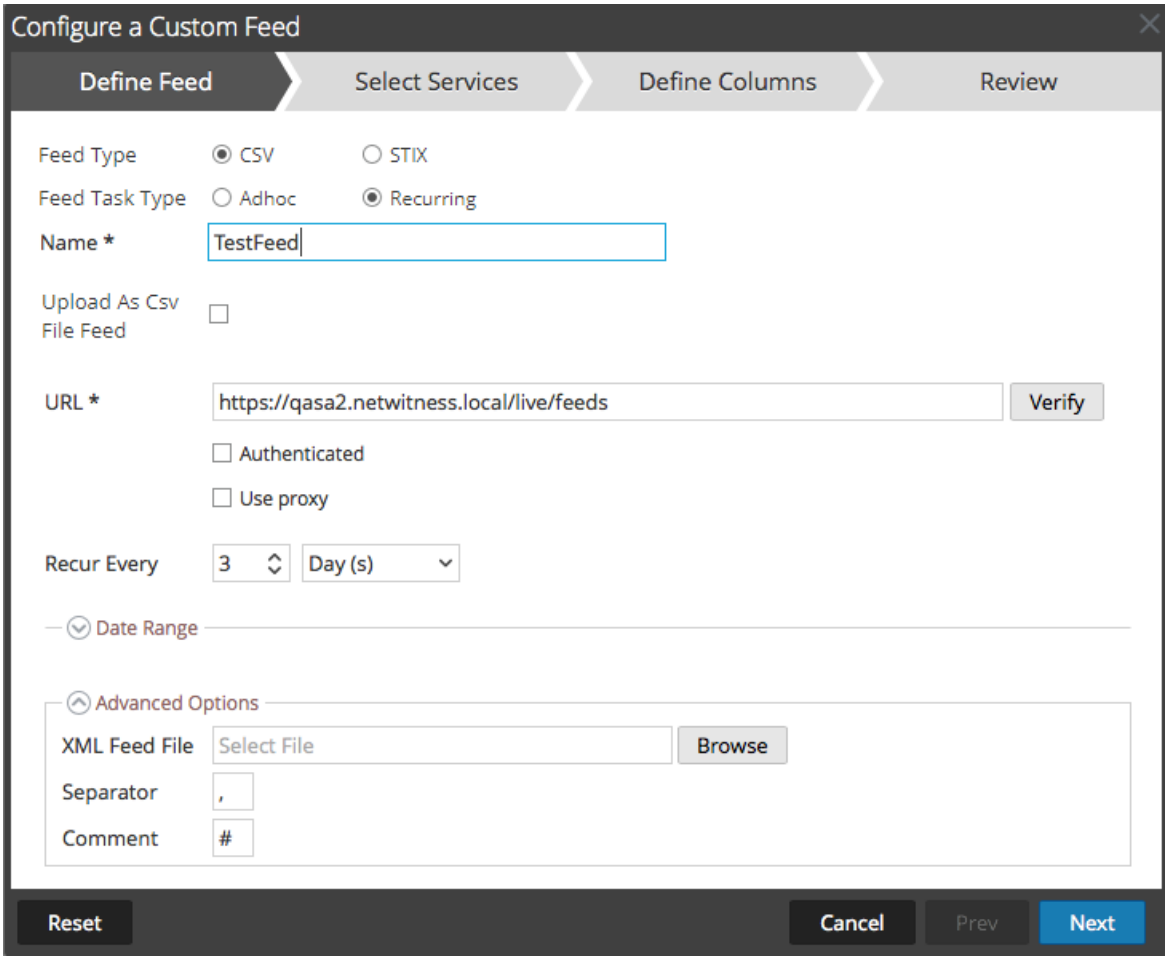
b. Dans le champ **URL**, entrez l'URL où se trouve le fichier de données de feed, par exemple, `http://<hostname>/<feeddatafile>.csv`, et cliquez sur **Vérifier**. NetWitness Platform vérifie l'emplacement où le fichier est stocké afin d'activer la vérification du dernier fichier automatiquement avant chaque récurrence.

c. (Facultatif) Si l'URL présente un accès restreint et requiert une authentification à l'aide de votre nom d'utilisateur et mot de passe, sélectionnez **Authentifié**.
NetWitness Platform fournit votre nom d'utilisateur et mot de passe pour l'authentification auprès de l'URL.

d. Si vous souhaitez que le serveur NetWitness accède à l'URL du feed via un proxy, sélectionnez **Utiliser le proxy**. Pour plus d'informations sur la configuration d'un proxy, reportez-vous à la rubrique « Configurer un serveur proxy » pour NetWitness Platform dans le *Guide de configuration du système*. Par défaut, la case **Utiliser le proxy** n'est pas cochée.

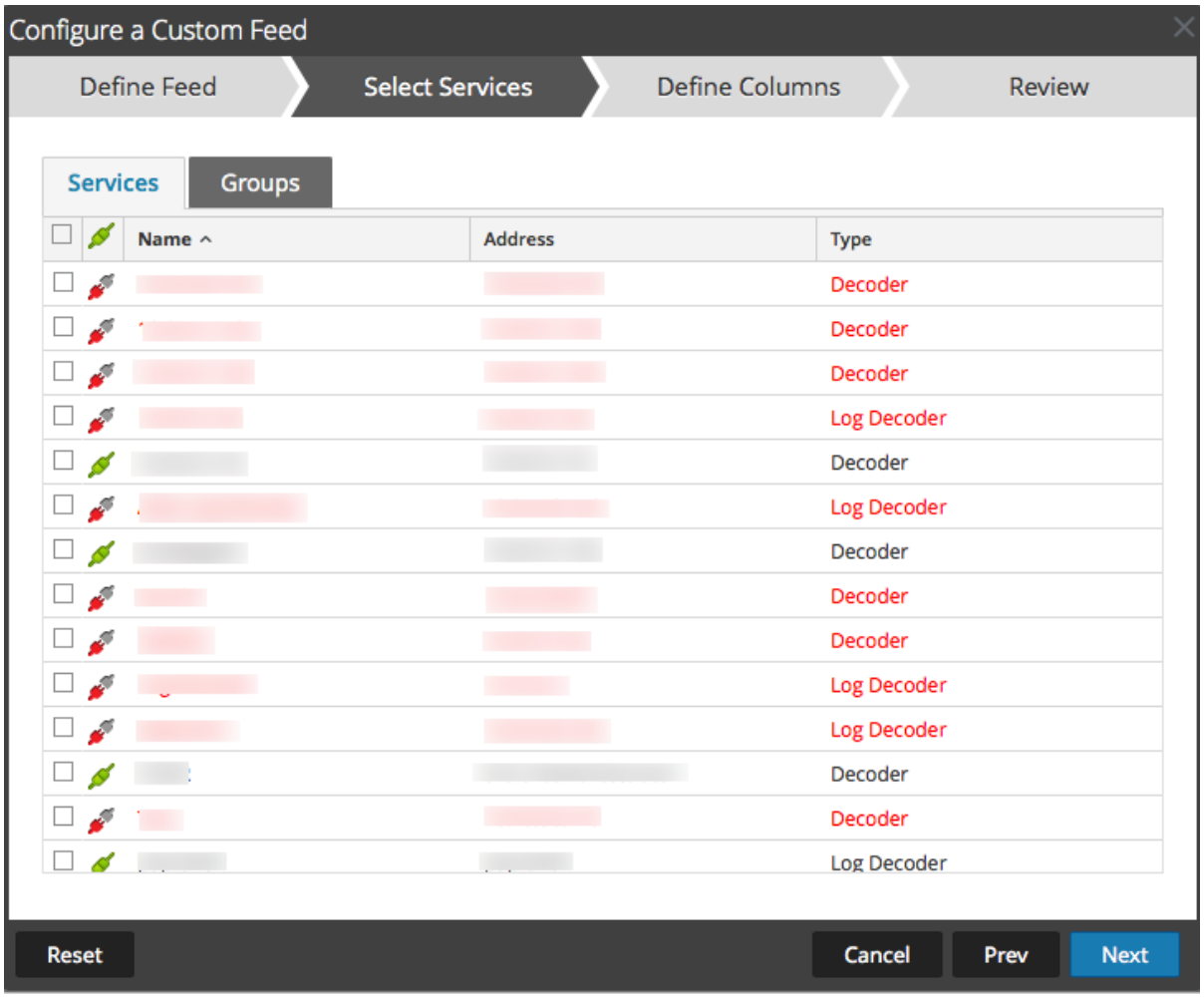
e. Pour définir l'intervalle de récurrence, effectuez l'une des opérations suivantes :
- Spécifiez le nombre de minutes, d'heures ou de jours entre les récurrences du champ.
Spécifiez une récurrence hebdomadaire, puis sélectionnez les jours de la semaine.

f. Pour définir la période pour l'exécution récurrente du feed, spécifiez la **Date de début** et l'heure, ainsi que la **Date de fin** et l'heure.

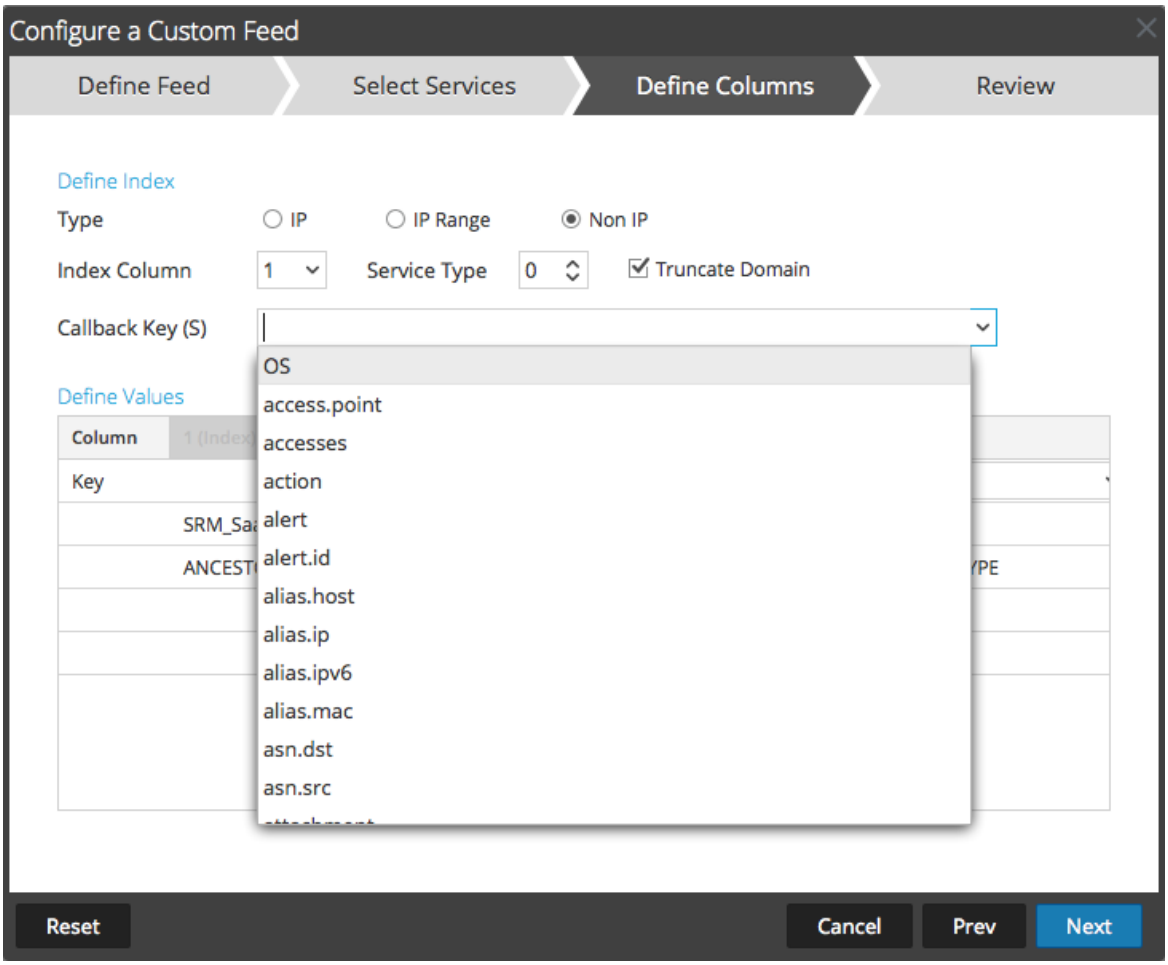


8. (Conditionnel) Si vous souhaitez définir un feed basé sur un fichier de feed XML :
   Saisissez le **Nom** du feed, sélectionnez **Options avancées**. Les champs des Options avancées s'affichent.
   Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le **Séparateur** (par défaut, il s'agit de la virgule), spécifiez les caractères du **Commentaire** utilisés dans le fichier de données de feed (la valeur par défaut est #) et cliquez sur **Suivant**. Le formulaire Sélectionner des

services s'affiche.

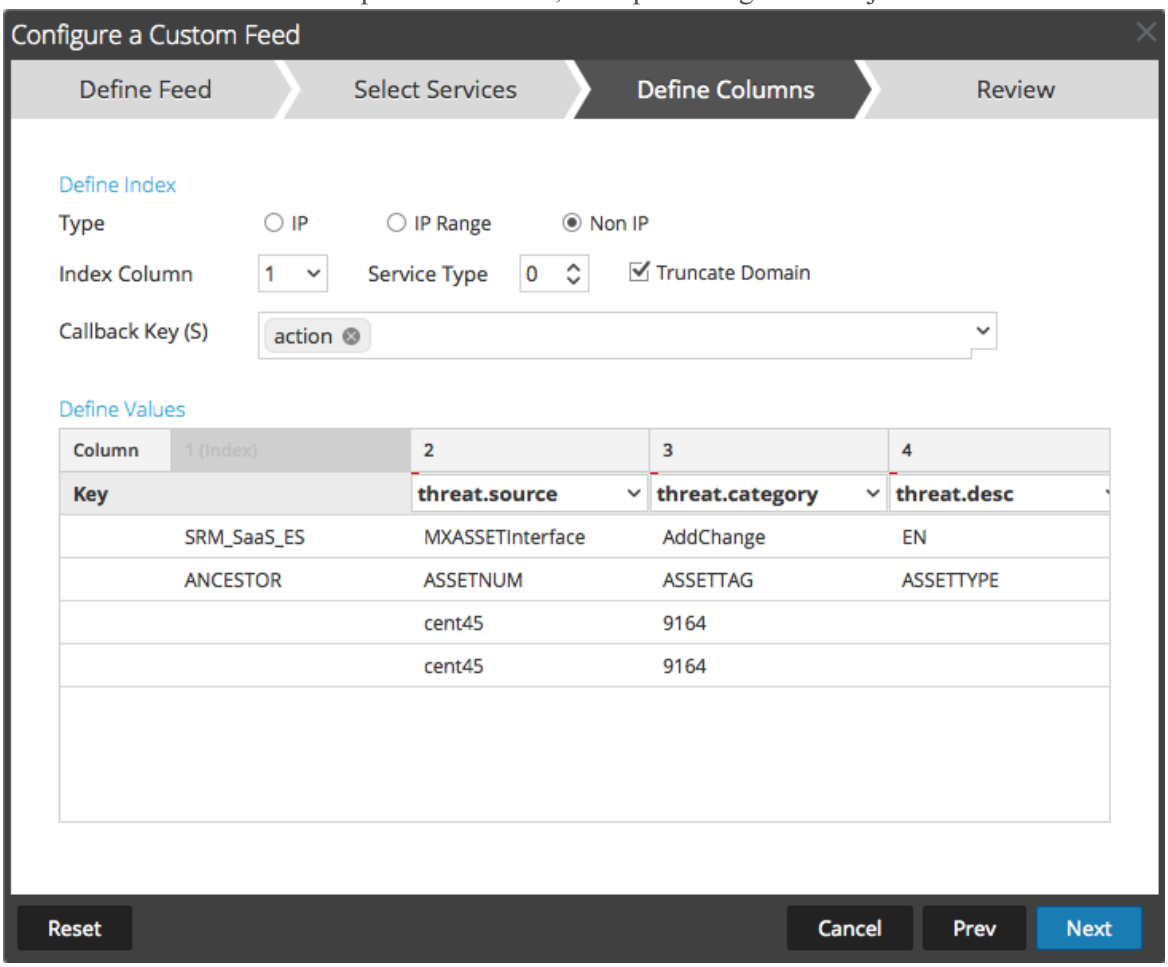


9. Pour identifier les services sur lesquels déployer le feed, effectuez l'une des opérations suivantes :
   a. Sélectionnez un ou plusieurs Decoders et Log Decoders, et cliquez sur **Suivant**
   b. Cliquez sur l'onglet **Groupes** et sélectionnez un groupe. Cliquez sur **Suivant**.
   Le formulaire Définir des colonnes s'affiche.
10. Pour mapper les colonnes dans le formulaire Définir des colonnes :
    a. Définir le type d'index : **IP**, **Plage IP** ou **Non IP**, et sélectionnez la colonne index.
    b. (Conditionnel) Si le type d'index est **IP** ou **Plage IP** et l'adresse IP est au format de notation CIDR, sélectionnez **CIDR**.
    c. (Conditionnel) Si le type d'index est **Non IP**, des paramètres supplémentaires s'affichent. Sélectionnez le type de service et **Clés de rappel**, et éventuellement, sélectionnez l'option **Tronquer le domaine**.

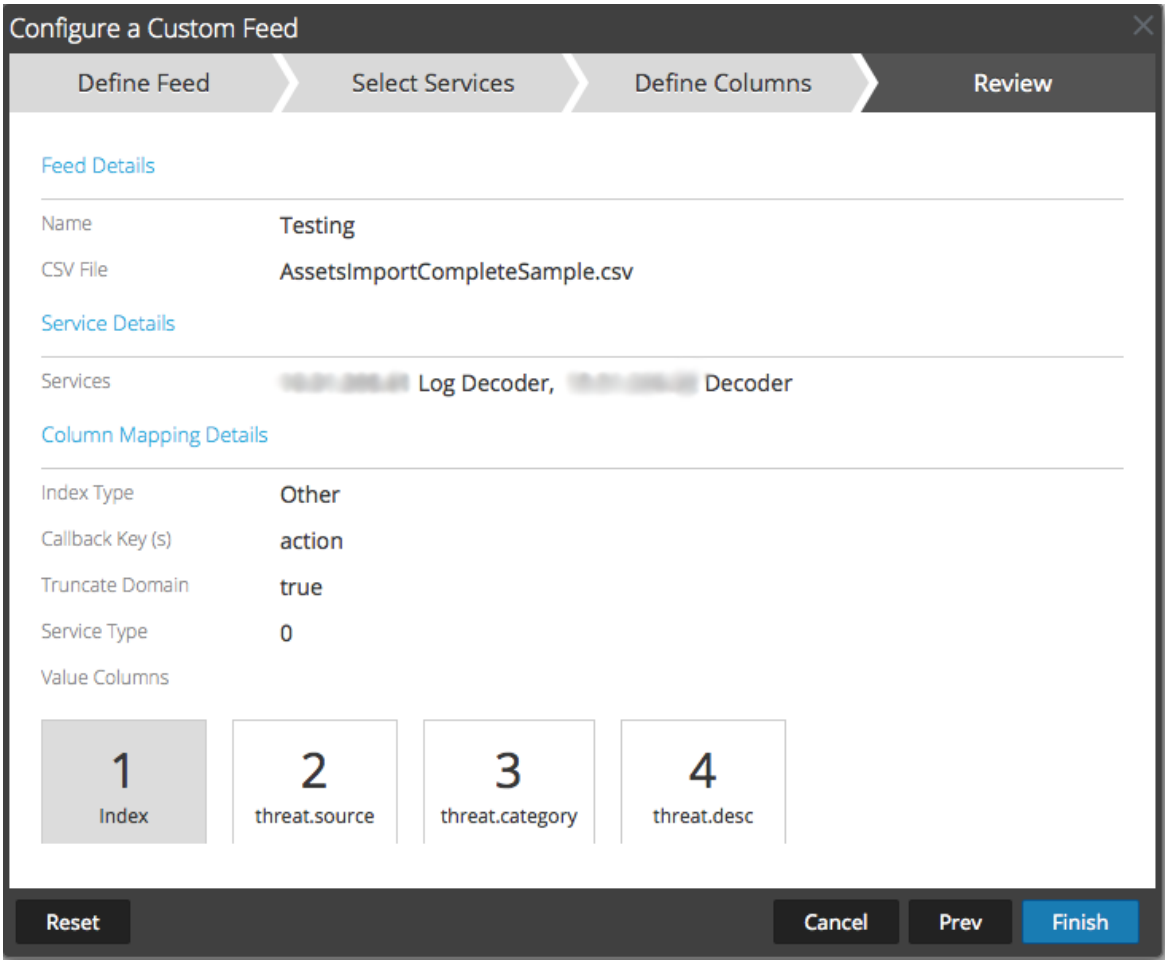


d. Sélectionnez la clé de langue à appliquer aux données de chaque colonne à partir de la liste déroulante. Le méta affiché dans la liste déroulante est basé sur les valeurs définies par le

service. Si vous avez des compétences solides, vous pouvez également ajouter d'autres méta.



e. Cliquez sur **Suivant**.
Le formulaire Révision s'affiche.

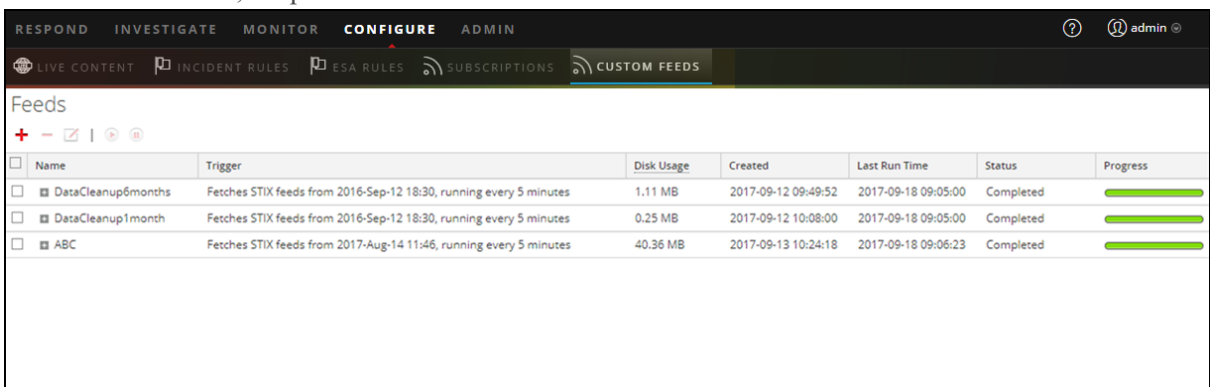


11. À tout moment avant de cliquer sur **Terminer**, vous pouvez :

- Cliquez sur **Annuler** pour fermer l'assistant sans enregistrer votre définition de feed.
- Cliquez sur **Réinitialiser** pour effacer les données de l'assistant.
- Cliquez sur **Suivant** pour afficher le formulaire suivant (si ce n'est pas le dernier formulaire).
- Cliquez sur **Précédent** pour afficher le formulaire précédent (si ce n'est pas le premier formulaire)

11. Passez en revue les informations du feed et, si elles sont correctes, cliquez sur **Terminer**.
12. Lorsque le fichier de définition de feed a été créé avec succès, l'assistant Créer un feed se ferme. Le feed et le fichier de token correspondant sont répertoriés dans la grille de feed et la barre de progression indique l'avancement. Vous pouvez développer ou réduire l'entrée pour voir combien de

services sont inclus, et quels services ont abouti.



Créer un Feed STIX personnalisé

STIX™ (Structured Threat Information Expression) est un langage structuré qui décrit les informations sur les cybermenaces, de façon à ce qu'elles puissent être partagées, stockées et analysées de manière cohérente. Pour plus d'informations sur STIX, consultez https://stixproject.github.io/.

Vous pouvez créer un feed personnalisé à l'aide d'un fichier de données de feed au format STIX (`.xml`) dans RSA NetWitness Platform. NetWitness Platform prend en charge uniquement les versions 1.0, 1.1 et 1.2 de STIX.

Attention : Si un feed récurrent STIX est configuré et que vous mettez à jour Security Analytics de la version 10.6.x vers NetWitness Platform 11.x, vous devez reconfigurer le feed récurrent STIX.

Dans NetWitness Platform, les feeds STIX de type Indicateur ou Observable contenant des propriétés, telles que les adresses IP, les hachages de fichiers, les noms de domaine, les URI et les adresses électroniques sont pris en charge. Les valeurs de propriétés de l'opérateur Égal sont pris en charge. Les attributs tels que le type et le titre sont également lus à partir du STIX. Un fichier STIX avec un seul STIX_Package est pris en charge.

TAXII (Trusted Automated eXchange of Indicator Information) est le mécanisme de transport principal pour les informations sur les cybermenaces représentées dans STIX. À l'aide de services TAXII, les organisations peuvent partager des informations sur les cybermenaces de manière sécurisée et automatisée.

Les communautés STIX et TAXII collaborent étroitement afin de garantir la continuité de ce partage d'informations sur les menaces.

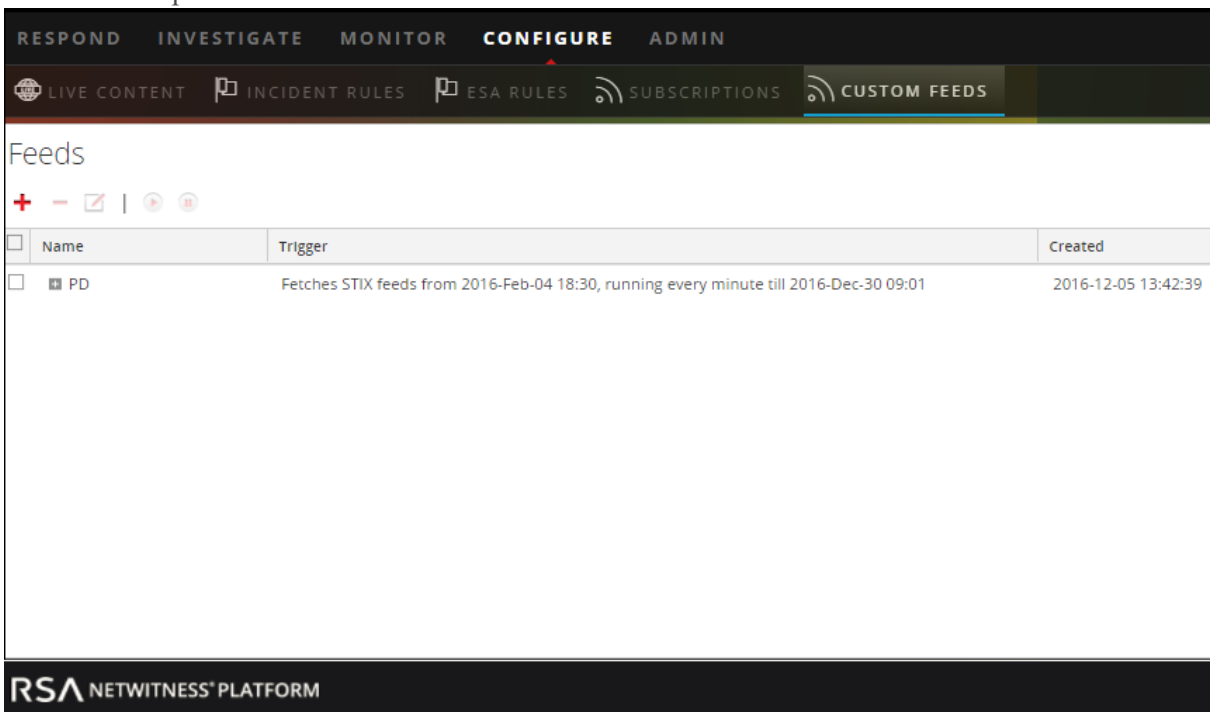
À l'exception du serveur TAXII, les données STIX peuvent également résider sur un serveur REST et vous pouvez extraire le fichier STIX depuis le serveur REST en fournissant l'URL du serveur REST. Par exemple, `http://stixrestserver.internal.com`.

Le fichier de données de feed STIX et éventuellement le fichier de définition de feed, tous deux au format `.xml` doivent être disponibles sur le système de fichier local pour un feed personnalisé à la demande. Pour un feed personnalisé récurrent, les fichiers doivent être disponibles à une URL accessible au serveur NetWitness Platform.

Pour créer un feed STIX personnalisé :

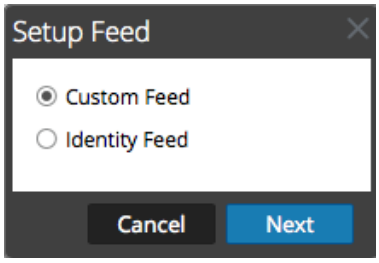
1. Accédez à **Configurer > Feeds personnalisés**.

   La vue Feeds personnalisés s'affiche.



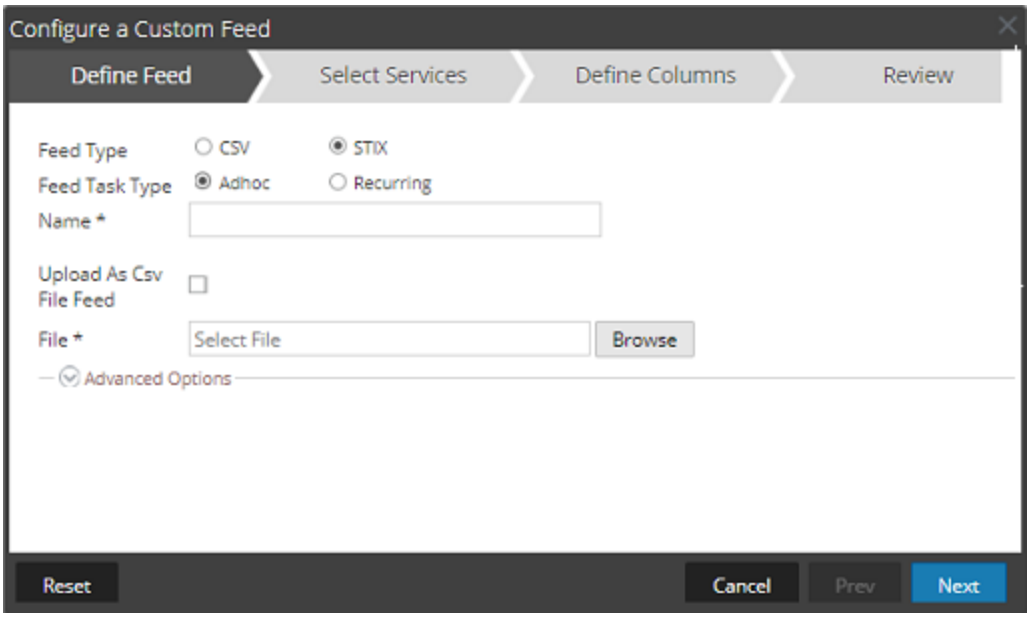
2. Dans la barre d'outils, cliquez sur +.

   La boîte de dialogue Configurer le feed s'affiche.



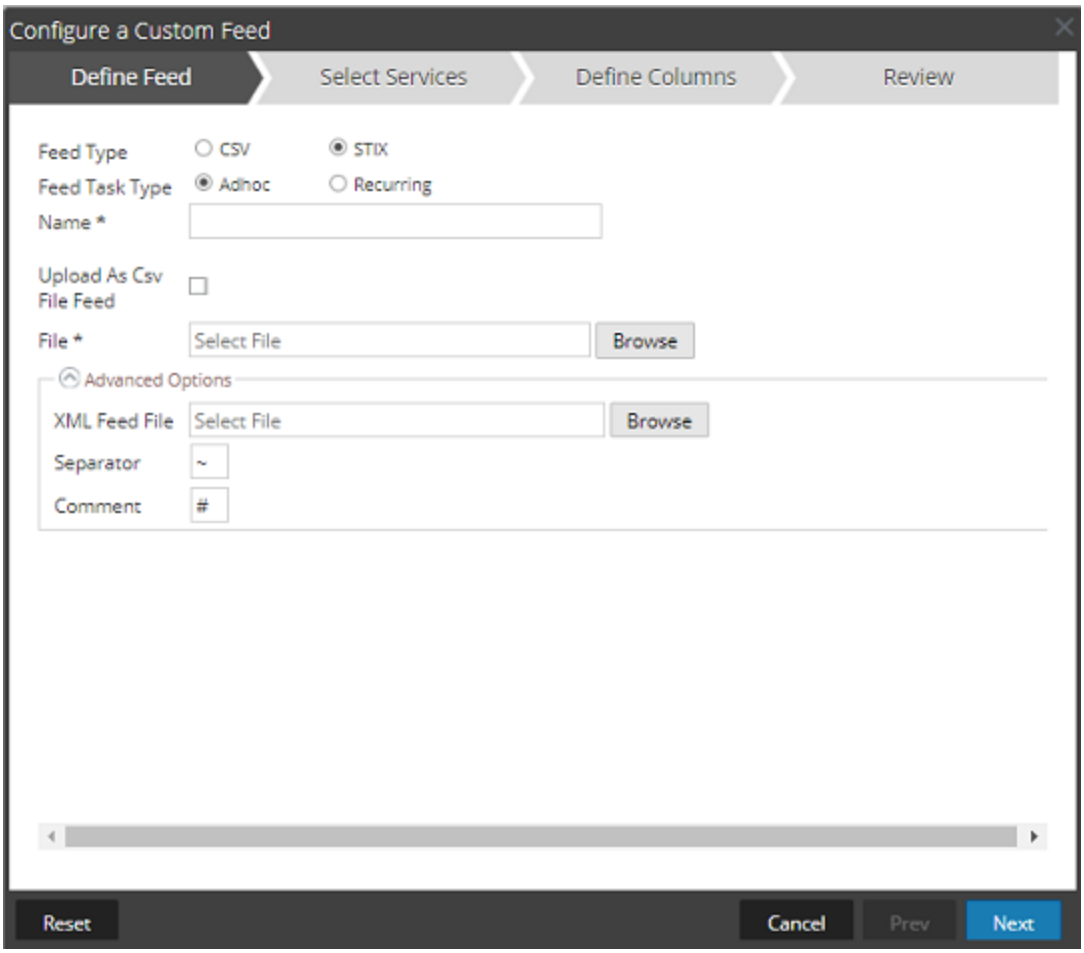
3. Pour sélectionner le type de feed, cliquez sur **Feed personnalisé**, puis sur **Suivant**.

   Le panneau Configurer un feed personnalisé s'affiche avec le formulaire Définir le feed ouvert.

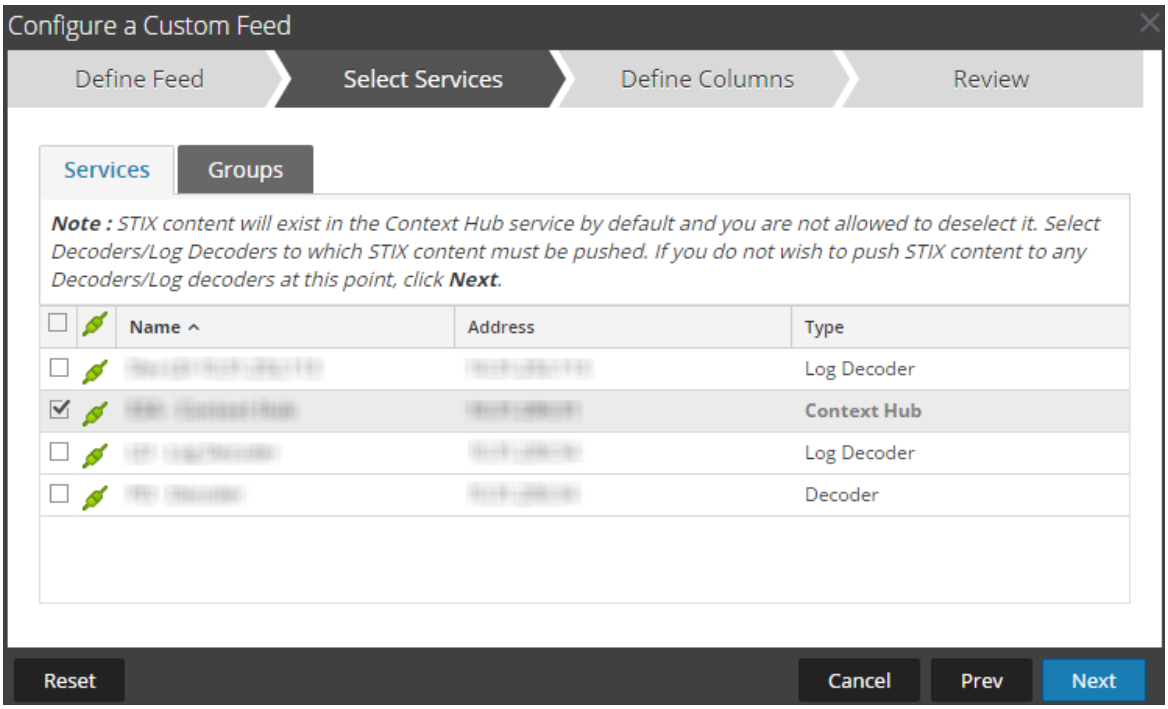


4. Pour définir un feed basé sur un fichier `.xml` au format STIX, sélectionnez **STIX** dans le champ **Type de feed**.
5. Pour définir une tâche de feed à la demande qui s'exécute une fois, sélectionnez **Ad hoc** dans le champ **Type de tâche par défaut** et procédez d'une des manières suivantes :
   a. (Conditionnel) Pour définir un feed basé sur un fichier `.xml` au format STIX, saisissez le **Nom** du feed, sélectionnez un Fichier de contenu `.xml` au format STIX dans le système de fichiers local, puis cliquez sur **Suivant**.
   b. (Conditionnel) Pour définir un feed basé sur un fichier de feed XML, sélectionnez **Options avancées**.

      Les Options avancées s’affichent.



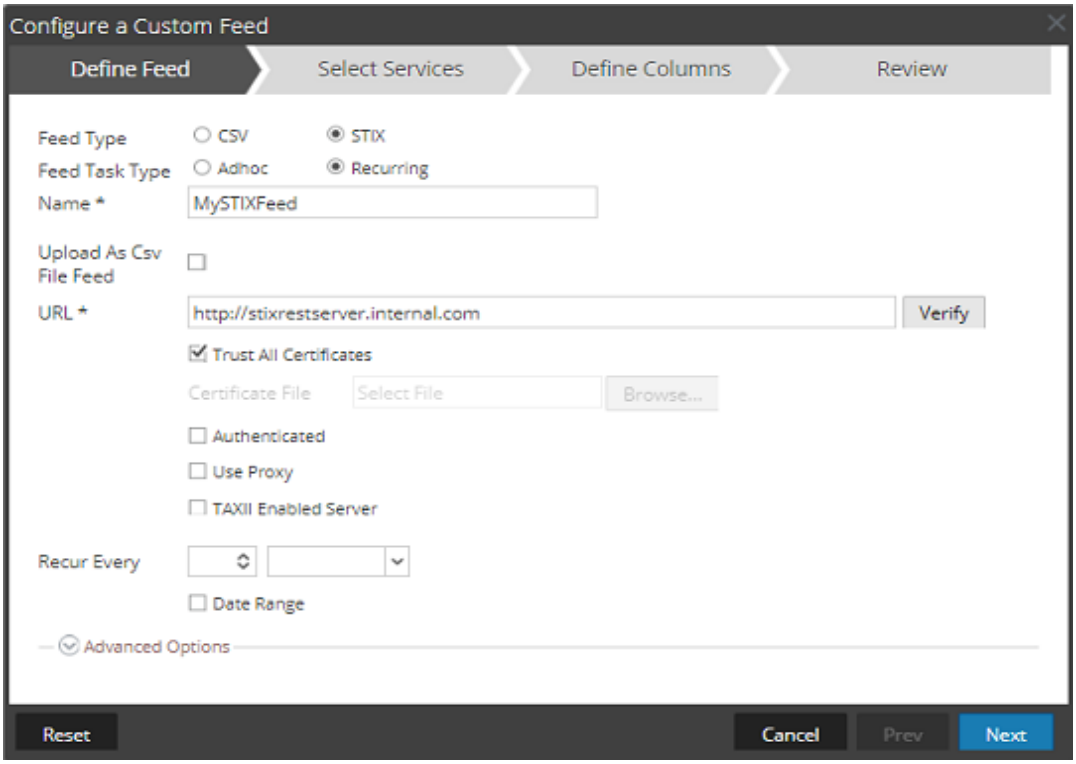
c. Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le Séparateur (par défaut, il s'agit de la virgule), et spécifiez les caractères du Commentaire utilisés dans le fichier de données de feed (la valeur par défaut est #) et cliquez sur **Suivant**.
Le formulaire Sélectionner des services s'affiche. Voici un exemple de formulaire pour un feed basé sur un fichier de données de feed, sans fichier de définition de feed. Si vous définissez un feed basé sur un fichier de définition de feed, l'onglet Définir des colonnes n'est pas nécessaire.



6. Pour définir une tâche de feed récurrente qui s'exécute de manière répétée à des intervalles spécifiques, pendant une certaine période :

   a. Sélectionnez **Récurrent** dans le champ **Type de tâche par défaut**.

   Le formulaire Définir le feed comprend les champs pour un feed récurrent.

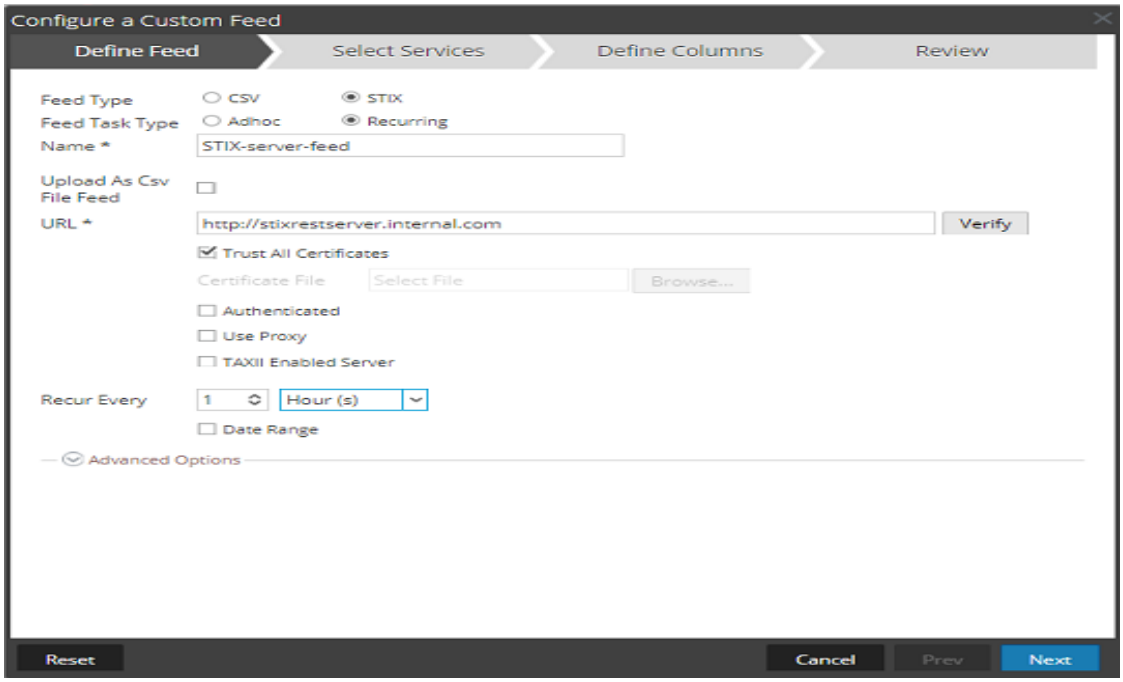


b. Dans le champ **URL**, saisissez l'un des éléments suivants :

- Pour définir un feed récurrent basé sur STIX qui extrait les packages STIX à partir d'un serveur TAXII, saisissez l'URL de service de découverte du serveur TAXII, par exemple, `http://hailataxii.com/taxii-discovery-service`.

  Remarque : Un service Context Hub installé sur un hôte Event Stream Analysis doit être accessible pour le serveur TAXII spécifié.

- Pour définir un feed récurrent basé sur un fichier `.xml` au format STIX à l'aide du serveur REST, saisissez l'URL du serveur REST où le fichier de données STIX se trouve, par exemple, `http://stixrestserver.internal.com`.



NetWitness Platform vérifie la connexion au serveur, afin que NetWitness Platform puisse vérifier le dernier fichier automatiquement avant chaque récurrence.

c. Si vous ne souhaitez pas que NetWitness Platform vérifie le certificat SSL du serveur REST, sélectionnez **Approuver tous les certificats**. Cette option est activée par défaut (cochée).

d. Pour une authentification client avec l'URL REST, dans le champ **Certificat**, cliquez sur **Parcourir** et sélectionnez le certificat auto-signé. Les formats de certificat pris en charge sont `.cer`, `.crt` avec des fichiers codés `Base64` et `DER`.

e. (Facultatif) Si l'URL présente un accès restreint et requiert une authentification à l'aide de votre nom d'utilisateur et mot de passe, sélectionnez **Authentifié**.

NetWitness Platform fournit votre nom d'utilisateur et mot de passe pour l'authentification auprès de l'URL.

f. Sélectionnez **Serveur TAXII activé**, si vous souhaitez sélectionner une collecte TAXII dans la liste.
Pour une adresse URL valide, une ou plusieurs collectes TAXII contenant le fichier de données STIX s'affiche en fonction de vos informations d'identification. Sélectionnez la collecte TAXII

requise dans la liste. Une seule collecte peut être ajoutée à partir d'un serveur TAXII pour un feed.

Remarque : Bien que plusieurs feeds à partir de multiple serveurs TAXII sont pris en charge, un seul compte (nom d'utilisateur et mot de passe) est pris en charge par le serveur TAXII.

g. Si vous souhaitez que le serveur NetWitness Platform accède à l'URL du feed via un proxy, sélectionnez **Utiliser le proxy**. Pour plus d'informations sur la configuration d'un proxy, reportez-vous à la rubrique « Configurer un serveur proxy » pour NetWitness Platform dans le *Guide de configuration du système*. (Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.) Par défaut, la case **Utiliser le proxy** n'est pas cochée.

h. (Facultatif) Cliquez sur **Vérifier** pour tester les paramètres.

Remarque : Assurez-vous que tous les paramètres de connexion requis tels que l'authentification, le proxy, le certificat de fiabilité, le serveur TAXII activé et d'autres, sont configurés avant de cliquer sur Vérifier.

i. Pour définir l'intervalle de récurrence de transfert vers le Decoder ou le Log Decoder, effectuez l'une des opérations suivantes :

- Spécifiez le nombre de minutes, d'heures ou de jours entre les récurrences du champ.
- Spécifiez une récurrence hebdomadaire, puis sélectionnez les jours de la semaine.

j. Pour définir la période pour l'exécution récurrente du feed, spécifiez la **Date de début** et l'heure, ainsi que la **Date de fin** et l'heure. La date de début doit être définie à partir du au moment où vous souhaitez extraire les données.

7. (Conditionnel) Si vous souhaitez définir un feed basé sur un fichier de feed XML :

- Saisissez le **Nom** du feed, sélectionnez **Options avancées**.

  Les champs des Options avancées s'affichent.

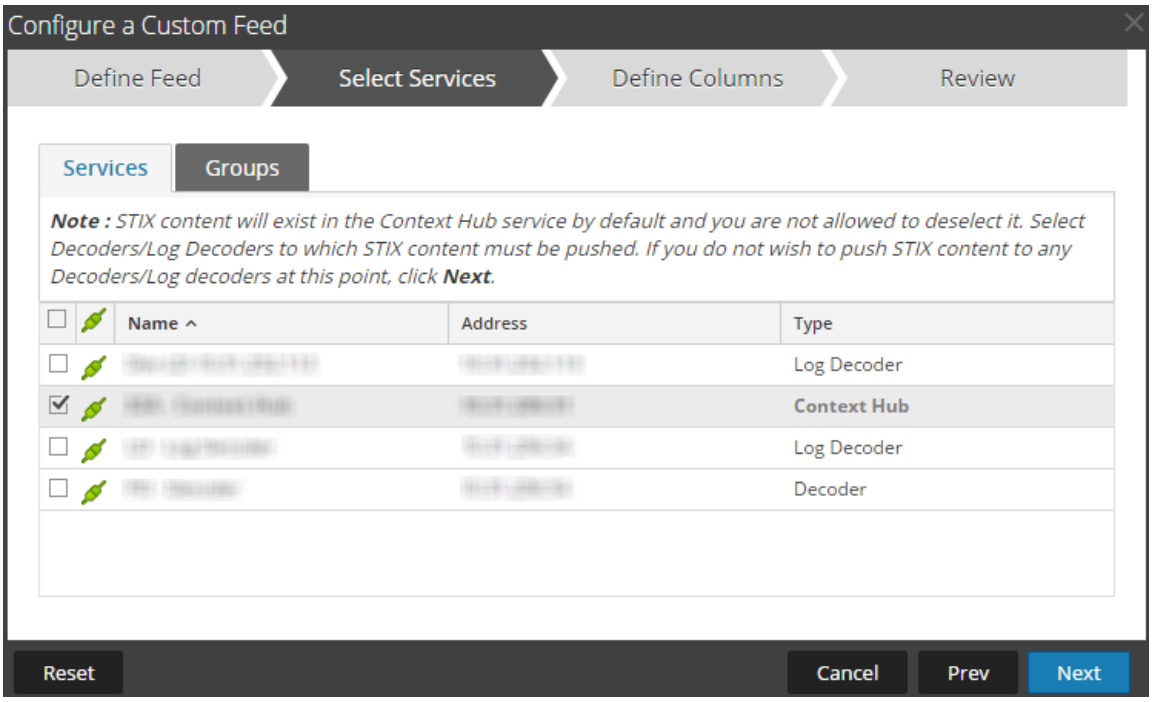
- Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le **Séparateur** (par défaut, il s'agit de la virgule), spécifiez les caractères du **Commentaire** utilisés dans le fichier de données de feed (la valeur par défaut est #).
- Dans le champ **Supprimer les données STIX antérieures à**, indiquez le nombre de jours durant lesquels les packages STIX extraits du serveur TAXII doivent être stockés. Les packages STIX antérieurs au nombre de jours spécifiés sont supprimés automatiquement.
- Cliquez sur **Suivant**.

  Le formulaire Sélectionner des services s'affiche.

8. Pour identifier les services sur lesquels déployer le feed, effectuez l'une des opérations suivantes :

a. Sélectionnez un ou plusieurs Decoders et Log Decoders, et cliquez sur **Suivant**.

b. En cas de feed STIX, Context Hub est sélectionné par défaut et vous n'êtes pas autorisé à le désélectionner. En outre, vous pouvez sélectionner un ou plusieurs Decoders et Log Decoders, cliquer sur **Suivant** ou sur l'onglet **Groupes**, puis sélectionner un groupe. Cliquez sur **Suivant**.

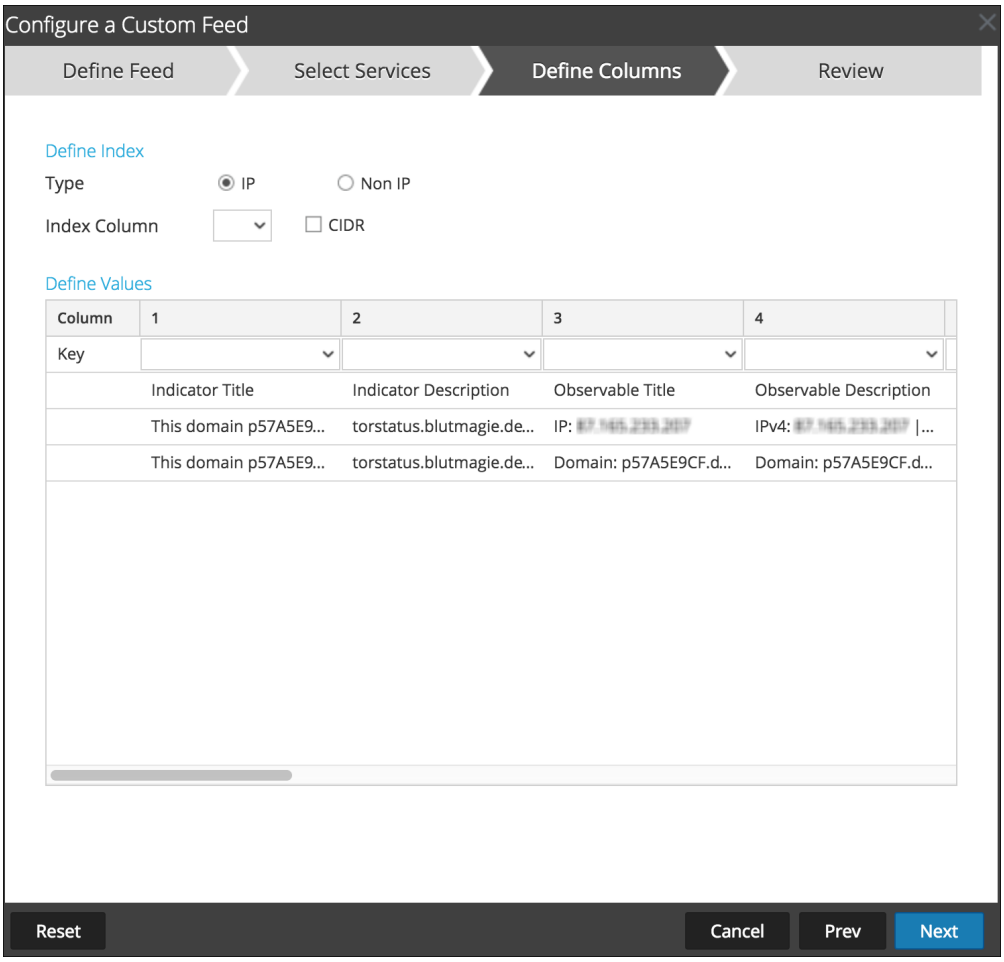


Si les données à partir du serveur STIX sont volumineuses, le message suivant s'affiche : « L'extraction de l'échantillon de données prend plus de temps que prévu. Choisissez une des options suivantes. » Vous avez deux options : vous pouvez continuer à en attendre ou mapper sans l'échantillon de données.

- Si vous cliquez sur **Continuer à en attendre**, l'assistant de feed continue à attendre jusqu'à ce que l'échantillon de données soit extrait ou que le délai expire (10 minutes), selon la première éventualité. Si le délai expire, aucun échantillon de données n'est récupéré.
- Si vous cliquez sur **Mapper sans les échantillons de données**, la colonne de mappage s'affiche sans les échantillons de données.

Le formulaire Définir des colonnes s'affiche.

9. Pour mapper les colonnes dans le formulaire Définir des colonnes :
   a. Définir le type d'index : **IP**, **Plage IP** ou **Non IP**, et sélectionnez la colonne index.
   b. (Conditionnel) Si le type d'index est **IP** ou **Plage IP** et l'adresse IP est au format de notation CIDR, sélectionnez **CIDR**.
   c. (Conditionnel) Si le type d'index est **Non IP**, des paramètres supplémentaires s'affichent. Sélectionnez le type de service et **Clés de rappel**, et éventuellement, sélectionnez l'option **Tronquer le domaine**.

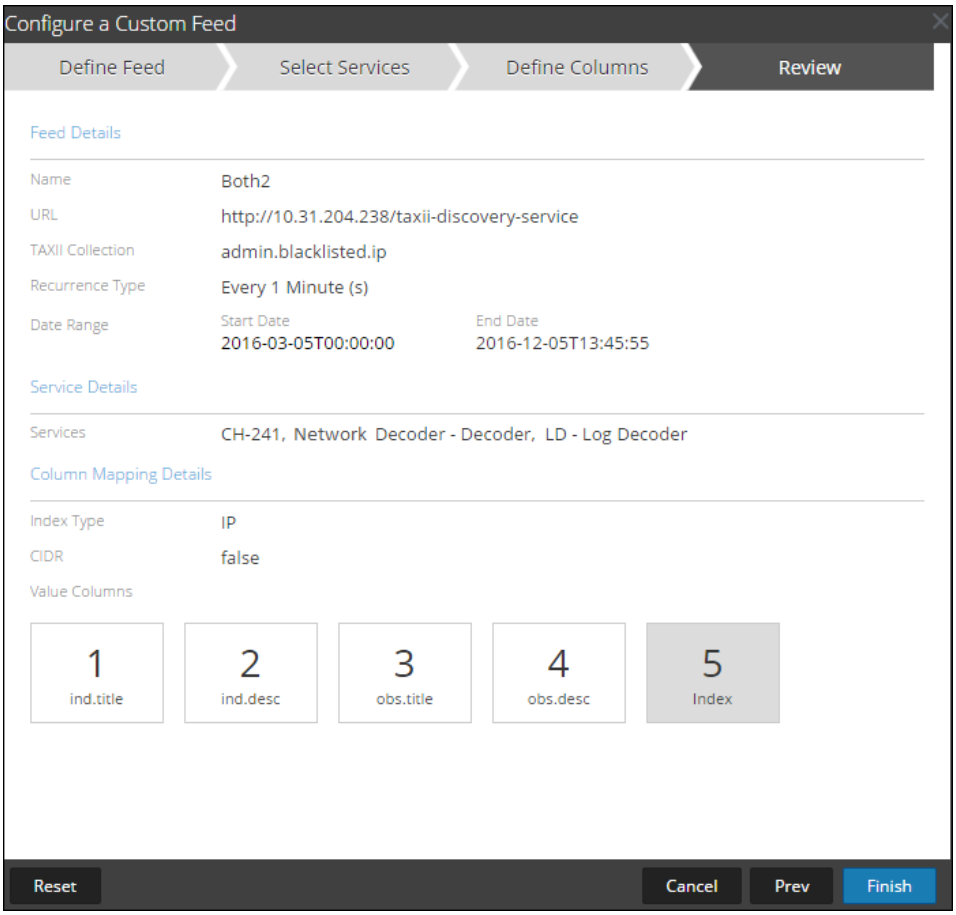


- Si le type d'Index est Non IP, vous pouvez sélectionner plusieurs colonnes d'index dans les colonnes d'Index. Les valeurs de toutes les colonnes sélectionnées sont fusionnées dans la première colonne d'index que vous avez sélectionnée et les valeurs fusionnées sont transférées vers le Log Decoder pour l'analyse. Par exemple, dans les colonnes d'index si vous sélectionnez 2, 4, 7 comme colonnes d'index les valeurs des colonnes 2, 4 et 7 sont fusionnées dans la colonne 2 et les valeurs sont transférées vers Log Decoder pour l'analyse.
- L'indexation n'est pas possible pour les colonnes comme le titre de l'indicateur, le description de l'indicateur, le titre Observable, la description Observables, car la recherche ne peut pas être effectuée pour ces colonnes.

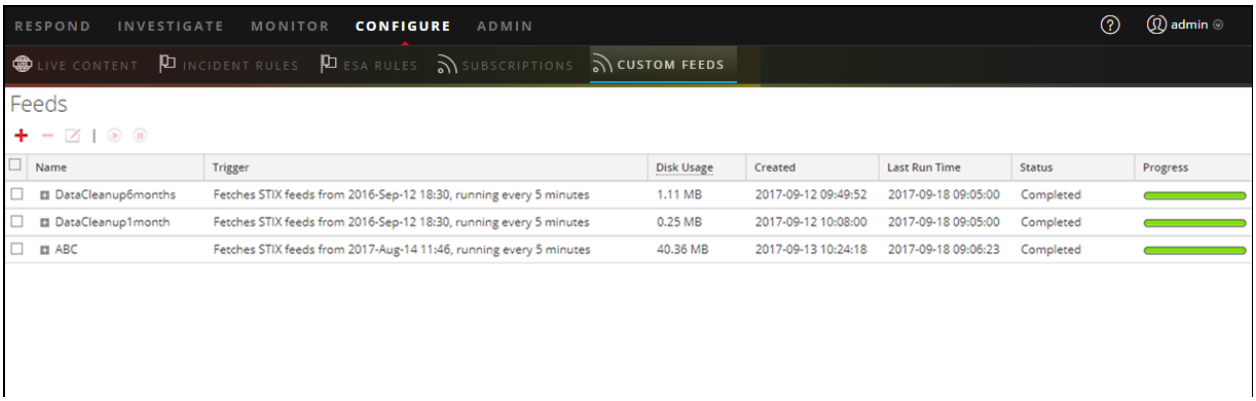
d. Sélectionnez la clé de langue à appliquer aux données de chaque colonne à partir de la liste déroulante. Le méta affiché dans la liste déroulante est basé sur les valeurs définies par le service. Si vous avez des compétences solides, vous pouvez également ajouter d'autres méta.

e. Cliquez sur **Suivant**.

Le formulaire Révision s'affiche.



10. À tout moment avant de cliquer sur **Terminer**, vous pouvez :
    - Cliquez sur **Annuler** pour fermer l'assistant sans enregistrer votre définition de feed.
    - Cliquez sur **Réinitialiser** pour effacer les données de l'assistant.
    - Cliquez sur **Suivant** pour afficher le formulaire suivant (si ce n'est pas le dernier formulaire).
    - Cliquez sur **Précédent** pour afficher le formulaire précédent (si ce n'est pas le premier formulaire).
11. Passez en revue les informations du feed et si elles sont correctes, cliquez sur **Terminer**.
12. Lorsque le fichier de définition de feed a été créé avec succès, l'assistant Créer un feed se ferme. Le feed et le fichier de token correspondant sont répertoriés dans la grille de feed et la barre de progression indique l'avancement. Vous pouvez développer ou réduire l'entrée pour voir combien de services sont inclus, et quels services ont abouti.



Remarque : Intégrité déclenche des alertes lorsque la mémoire disponible du serveur de Context Hub est extrêmement faible. Si l'état du serveur Context Hub est défectueux en raison du manque de mémoire. Pour plus d'informations sur le dépannage de `OutOfMemoryError` sur le serveur `Contexthub`, reportez-vous à la rubrique « Dépannage » le *Guide de gestion des Services Live*.

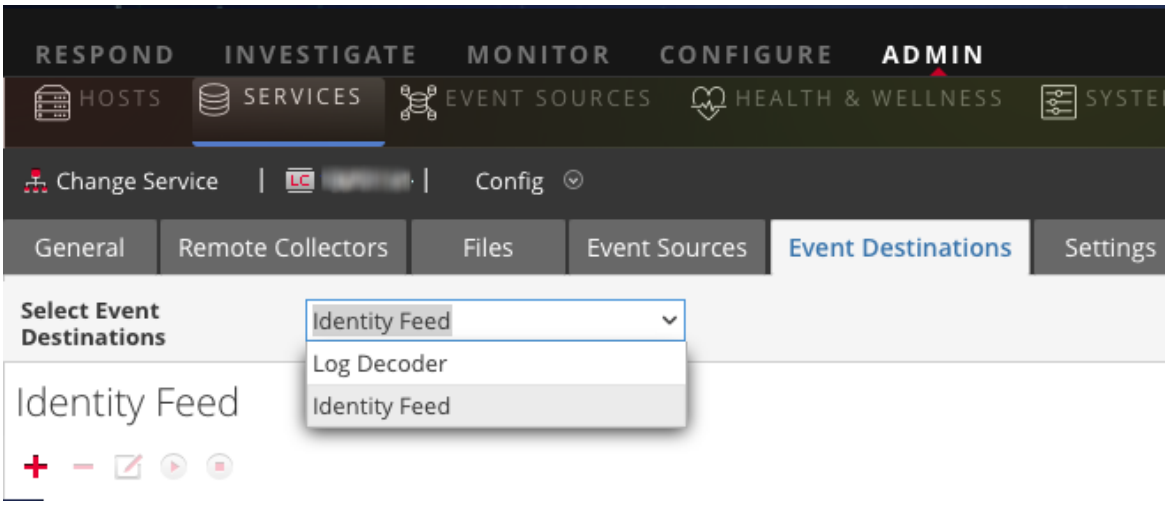
Créer un feed d'identité

Vous pouvez créer un feed d'identité et le renseigner dans les Decoders et Log Decoders. Dans le but de créer un feed d'identité, il vous faut :

- Le service Log Collector avec le processeur d'événements Identity Feed
- Le service Log Collector avec la collection Windows configurée et activée

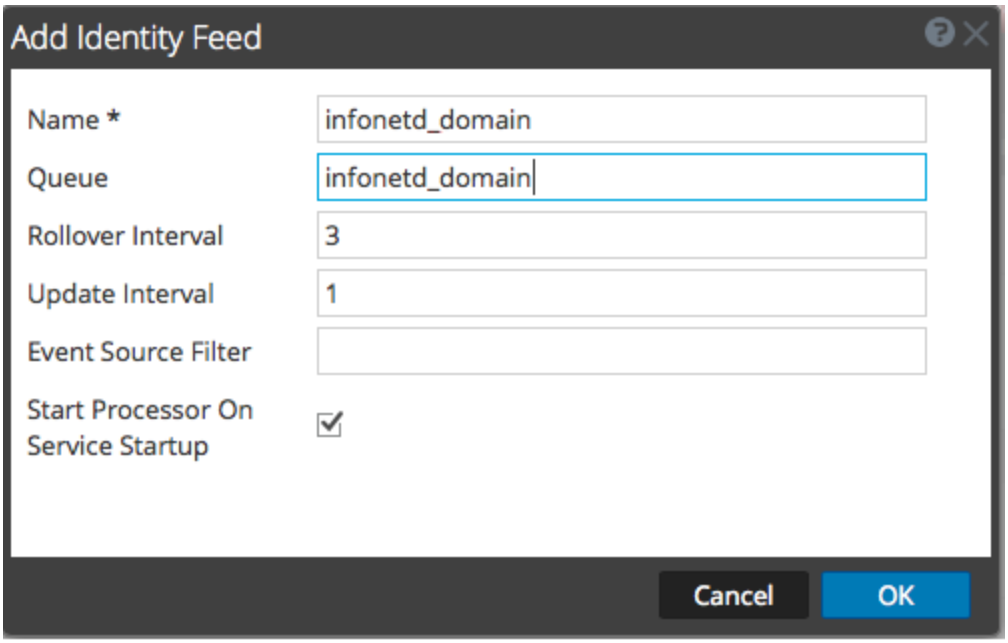
Pour créer un feed d'identité :

1. Ajouter une destination pour le feed.
   a. Accédez à **ADMIN > Services**, puis à la liste **Services**
   b. Sélectionnez un service **Log Collector** et cliquez sur **Vue > Configuration**.
   c. Sélectionnez l'onglet **Destinations d'événements**.
   d. Dans le champs **Sélectionnez les destinations d'événements**, sélectionnez **Identity Feed**.



   e. Cliquez sur + et saisissez un nom unique pour le feed.

      Le nom de la file d'attente identifie le feed dans le Log Collector. Utilisez le nom du feed pour la file d'attente.

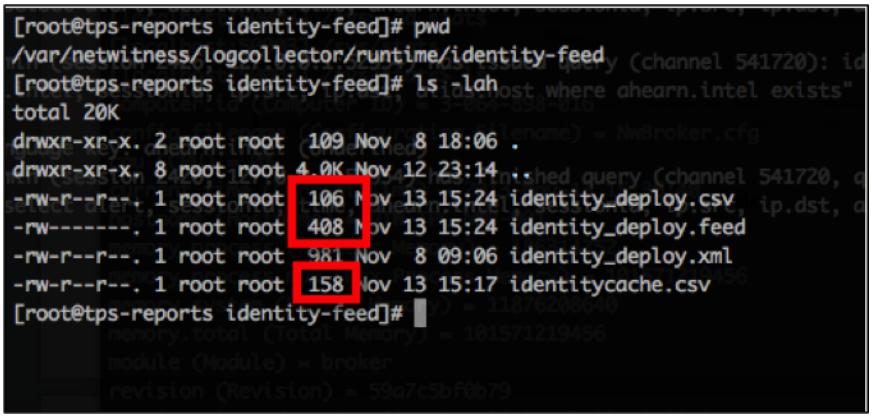


f. Cliquez sur le bouton **OK**.

2. Testez la génération de messages.

a. Invitez des utilisateurs sur le domaine à se connecter à la boite de dialogue Windows et à générer des messages de log appropriés sur les contrôleurs de domaine à des fins de test.

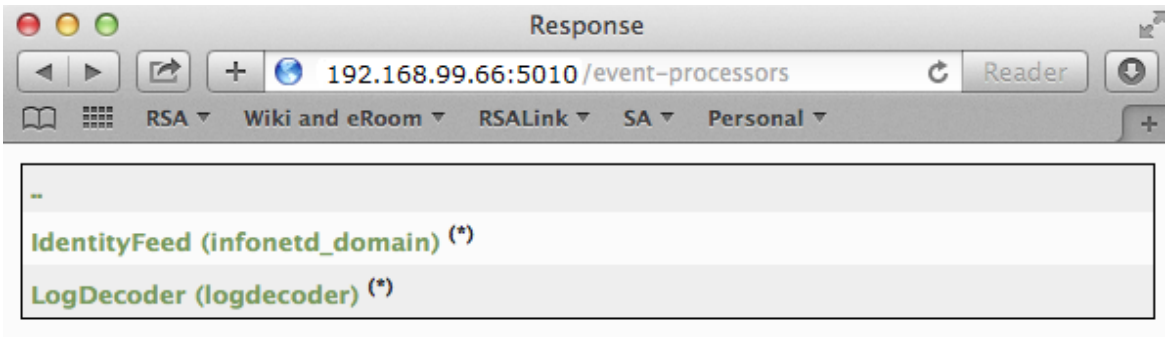
b. Vérifiez que les données sont écrites sur les fichiers de feed. Ouvrez une session SSH sur le Log Decoder/Collector ou sur le Virtual Log Collector en cours de configuration. Accédez à `/var/netwitness/logcollector/runtime/identity-feed` et vérifiez que les fichiers `Identity_deploy` se remplissent de données.



c. Ouvrez un navigateur web (les navigateurs autres que Internet Explorer sont à privilégier) et connectez-vous à l'interface REST du Log Collector. Utilisez les informations d'identification d'administration lors de la connexion. Par exemple, si l'adresse IP de votre collecteur de log est 192.168.99.66, l'adresse URL serait :

- SSL non activé : **http://192.168.99.66:50101/event-processeurs**
- SSL activé : **http://192.168.99.66:50101/event-processeurs**

L'écran du navigateur doit s'afficher comme suit :

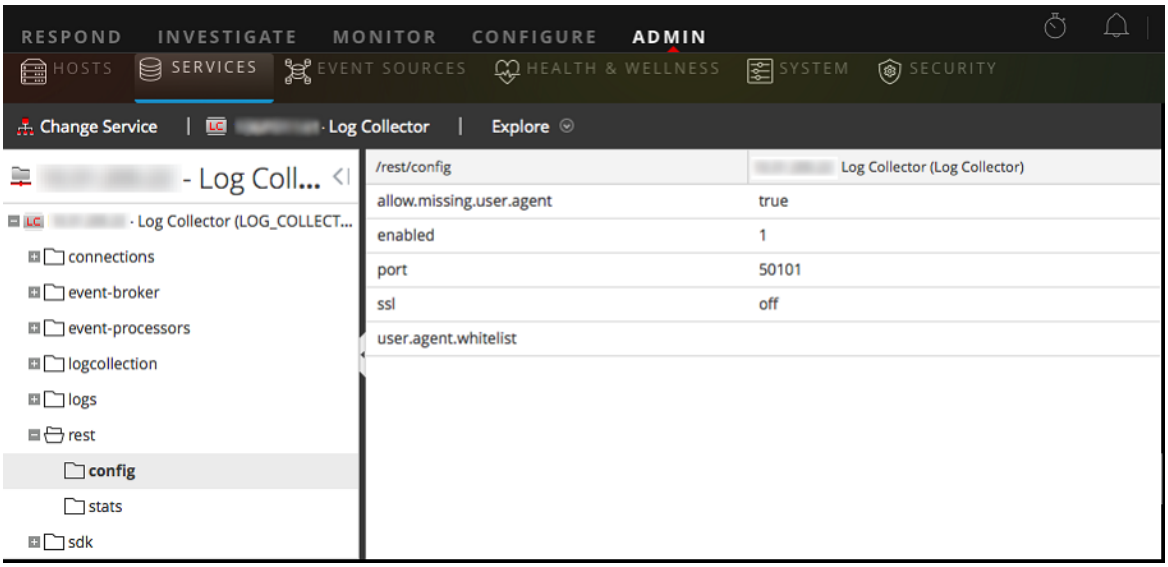


Notez que l'écran affiche le nom de l'identité du feed que vous avez créé précédemment (`infonetd_domain`, dans cet exemple).

Pour que l'identité du feed fonctionne correctement, le port 50101 doit être actif sur le Log Collector, et vous devez déterminer si le chiffrement SSL est actif.

d. Accédez à **ADMIN > Services > < *Log Collector en cours de configuration*** > **Vue > Explorer**.

e. Dans le volet de gauche, développez **rest > config**.



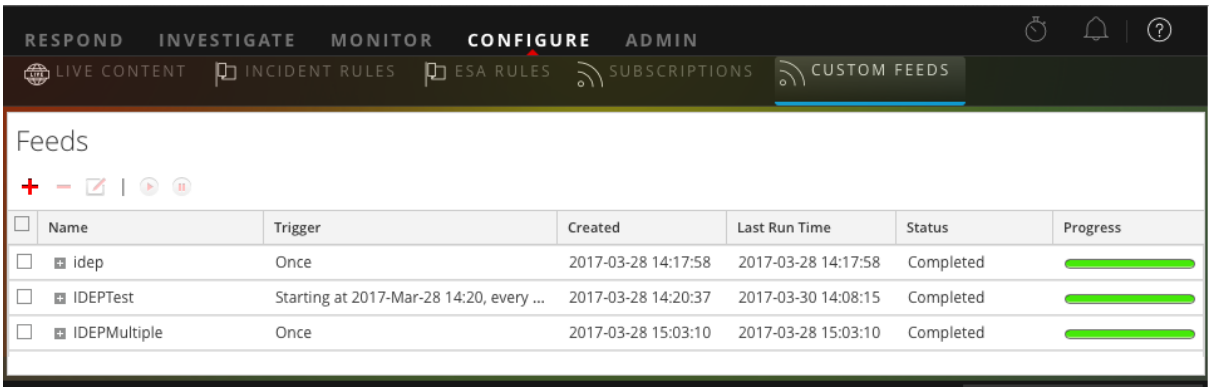
Pour que REST soit actif, **activé** doit être défini sur **1**.

f. Notez la valeur **ssl**. Si SSL doit être activée pour votre environnement, cette option doit être définie sur **activé**.

Remarque : Si vous avez modifié le paramètre pour les options **activé** ou **ssl**, vous devez redémarrer le service Log Collector avant d'aller plus loin.

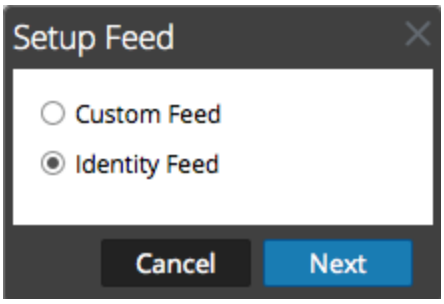
3. Accédez à **CONFIGURER > Feeds personnalisés**.

La boîte de dialogue Feeds s'affiche.



4. Dans la barre d'outils, cliquez sur +.

   La boîte de dialogue Configurer le feed s'affiche.



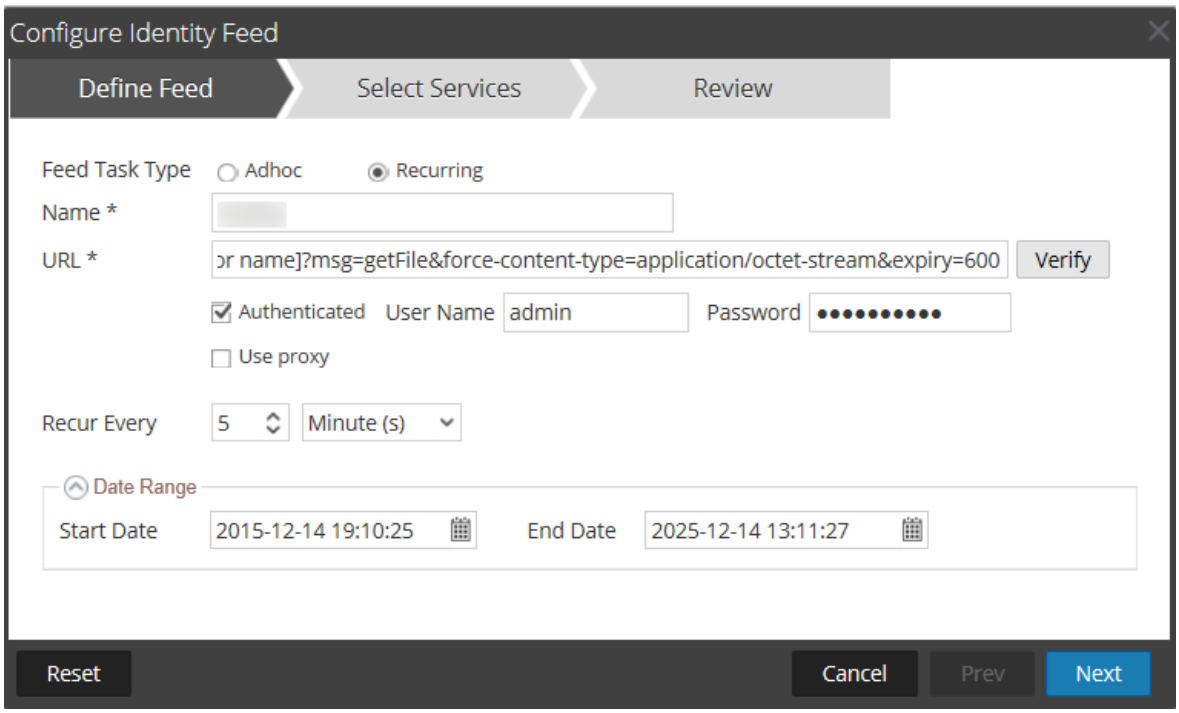
5. Assurez-vous que **Identity Feed** est sélectionné, puis cliquez sur **suivant**.

   Le panneau Configurer Identity Feed s'ouvre avec l'onglet **Définir le feed** affiché.

6. (Conditionnel) Vous pouvez créer un feed à la demande ou récurrent.

   - Pour définir une tâche de feed d'identité à la demande qui s'exécute une fois, sélectionnez **Adhoc** dans le champ **Type de tâche par défaut**, saisissez le **nom** du feed, accédez-y, puis ouvrez-le.
   - Pour définir une tâche Identity Feed récurrente qui s'exécute de manière répétée, sélectionnez **Récurrent** dans le champ **Type de tâche par défaut**.

     La boîte de dialogue **Définir le feed** comprend les champs pour un feed récurrent.



Remarque : RSA NetWitness Platform vérifie l'emplacement de stockage du fichier, de façon à ce que NetWitness Platform puisse vérifier automatiquement le dernier fichier avant chaque récurrence.

7. Renseignez et vérifiez le champ URL.
   a. Dans le champ **URL**, saisissez l'URL de l'emplacement du fichier de données de feed. Il s'agit de l'interface API REST qui a été configurée précédemment. Vous devez avoir connaissance des informations suivantes pour construire l'URL :
      - L'adresse IP du Log Collector utilisée pour créer le fichier Identity Feed.
      - Le nom d'identité de la file d'attente, tel que défini dans l'étape 2c.
      - Si SSL est activé ou non sur le port REST du Log Collector, tel que défini dans l'étape 2f.

      Vous créez cette valeur comme suit :

      - SSL activé : `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
      - SSL désactivé : `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

      Par conséquent, à l'aide de l'exemple précédent, la valeur complète que vous devez saisir dans ce champ est la suivante :

```
http://192.168.99.66:50101/event-processors/infonetd_
domain?msg=getFile&force-content-type=application/octet-
stream&expiry=600?msg=getFile&force-content-
type=application/octet-stream&expiry=600
```

b. Pour que la vérification de l'URL fonctionne correctement, il est important que l'interface utilisateur du serveur NetWitness Platform puisse accéder au port d'API REST du Log Collector (50101). Cela peut être testé en accédant à l'interface utilisateur du serveur NetWitness Platform via le protocole SSH. Exécutez la commande suivante sur l'hôte :

- SSL activé : `curl -vk https://<ip of log collector>:50101`
- SSL désactivé : `curl -v http://<ip of log collector>:50101`

Si la commande `curl` ne se connecte pas, il existe peut-être un problème de routage ou de pare-feu réseau entre l'interface utilisateur du serveur NetWitness Platform et le Log Collector.

Exemple de mauvaise connexion :

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... No route to host
* couldn't connect to host
* Closing connection #0
curl: (7) couldn't connect to host
Example of Good connection:
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... connected
* Connected to 192.168.99.66 (192.168.99.66) port 50105 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2
> Host: 192.168.99.66:50105
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Content-Length: 71
< Connection: Keep-Alive
< Pragma: no-cache
< Expires: -1
< Cache-Control: no-cache, no-store, must-revalidate
< WWW-Authenticate: Basic realm="NetWitness"
< Content-Type: text/xml; charset=utf-8
```

```
<
<?xml version="1.0" encoding="utf-8"?>
<error>401 Unauthorized</error>
* Connection #0 to host 192.168.99.66 left intact
* Closing connection #0
```

8. Un nom d'utilisateur et un mot de passe sont nécessaires à l'API REST pour extraire le fichier `identity_deploy.csv` du Log Collector. Cela peut être n'importe quel nom d'utilisateur et mot de passe disponible sur le service lui-même. Pour plus d'informations, consultez la rubrique « Vue sécurité des services » dans le *Guide des hôtes et des services*.

   Pour afficher les comptes disponibles, accédez à **ADMIN > Services > <Log Collector en cours de configuration> > Actions > Vue > Sécurité**.

   Sous le tableau des utilisateurs, tous les utilisateurs qui peuvent être utilisés dans cette étape s'affichent. Pour une sécurité renforcée, il est recommandé de créer un compte utilisateur spécifiquement pour cette configuration et a n'utiliser nulle part ailleurs dans l'environnement. Pour plus de détails, consultez la section « Ajouter un utilisateur et attribuer un rôle » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*. (Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.)

9. Pour définir l'intervalle de récurrence, effectuez l'une des opérations suivantes :

   - Spécifiez le nombre de minutes, d'heures ou de jours entre les récurrences du champ.
   - Pour définir la période pour l'exécution récurrente du feed, spécifiez la **Date de début** et l'heure, ainsi que la **Date de fin** et l'heure.

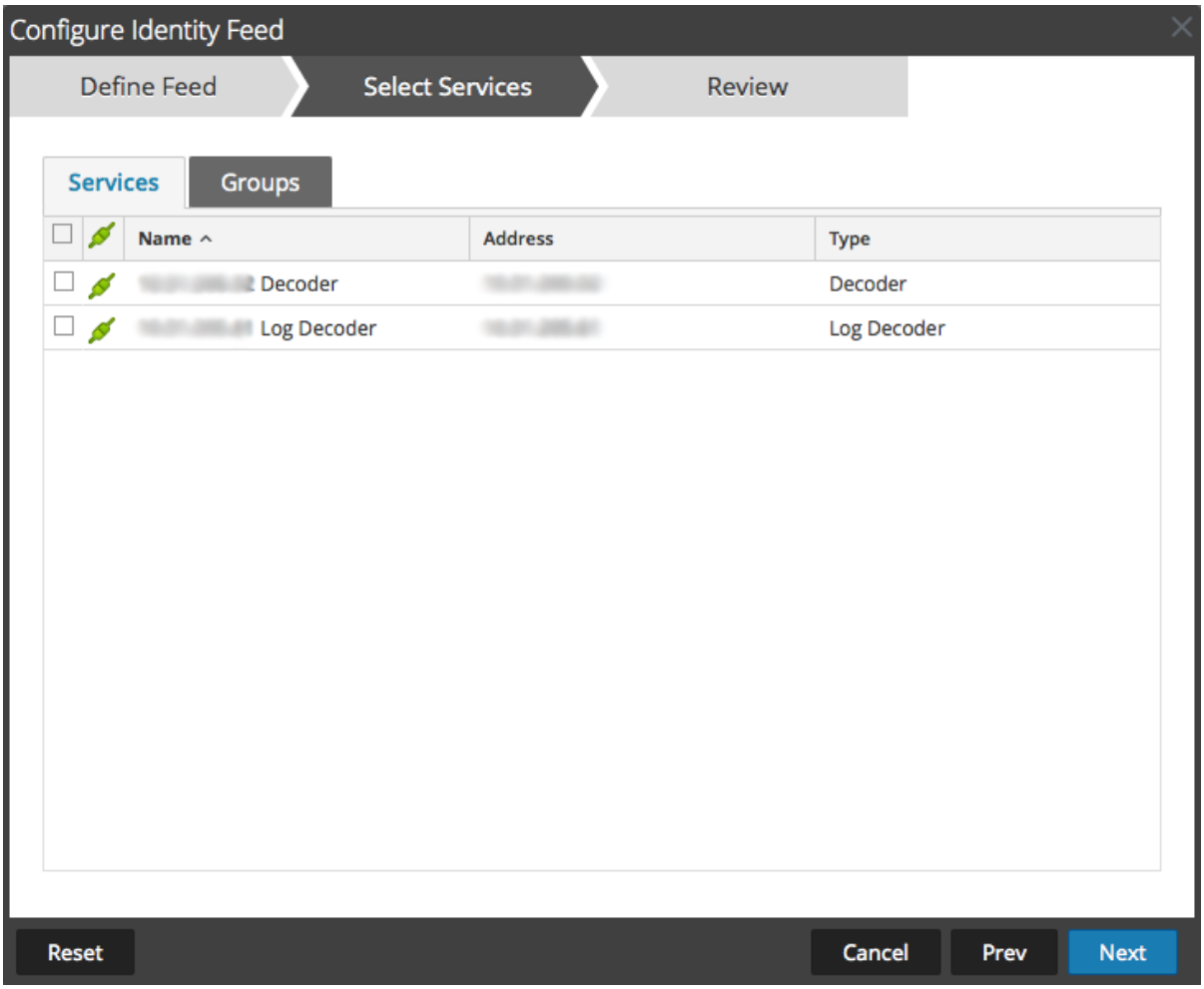
10. Si vous utilisez le chiffrement SSL, vous devez installer le certificat SSL de l'API REST pour le Log Collector dans l'interface utilisateur du serveur NetWitness Platform. Pour plus d'informations sur les certificats SSL, reportez-vous à la rubrique Importer le certificat SSL. .

    Si, après l'importation du certificat SSL, la vérification de l'URL échoue à nouveau, consultez la section Impossible de vérifier l'URL du feed d'identité.

11. Cliquez sur **Vérifier** pour vérifier votre configuration du feed identité avant de procéder à la boîte de dialogue Sélectionner des services.

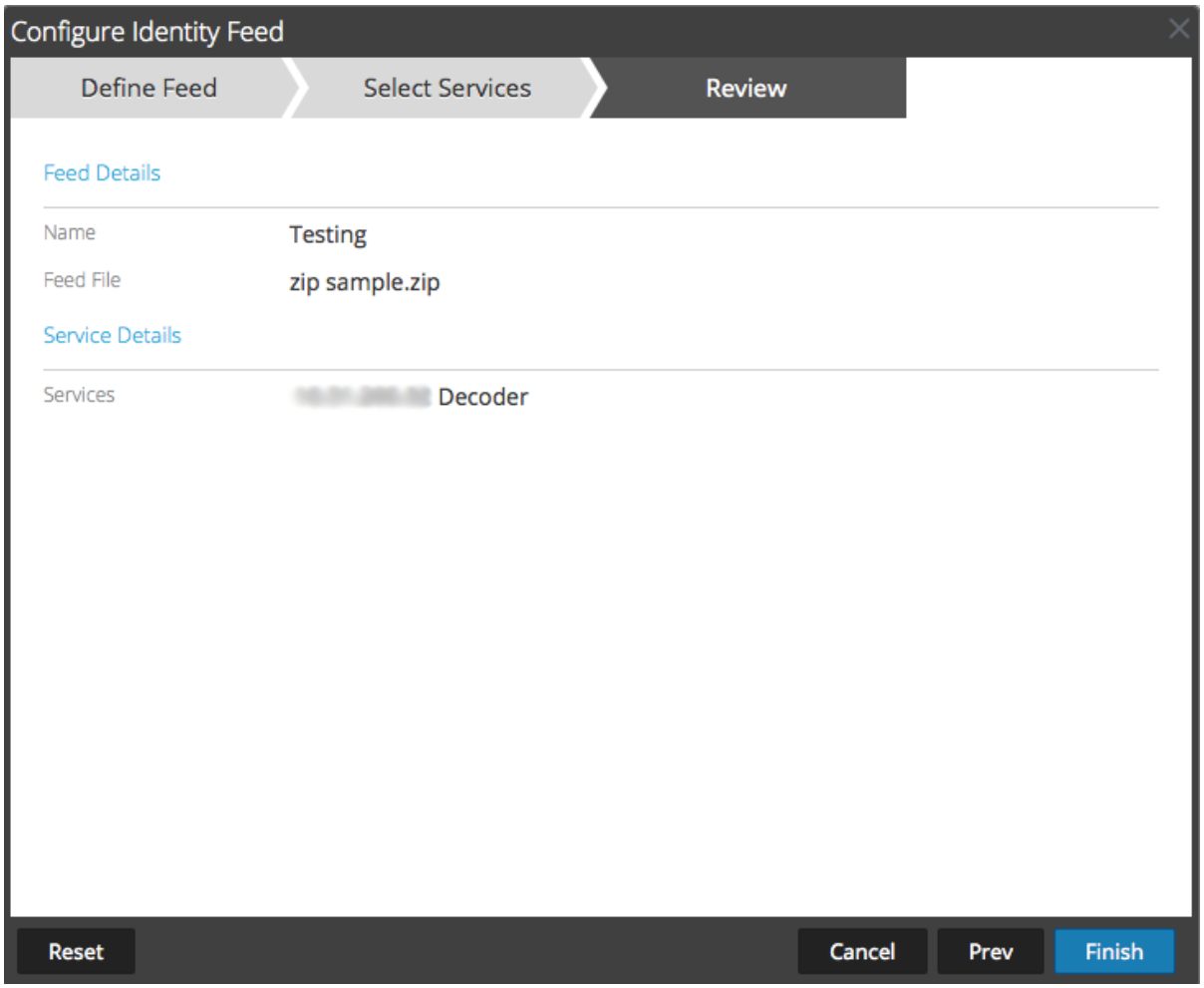
12. Cliquez sur **Suivant**.

    La boîte de dialogue Sélectionner des services s'affiche.



13. Pour identifier les services sur lesquels déployer le feed, sélectionnez un ou plusieurs Decoders et Log Decoders, puis cliquez sur **Suivant**.
14. Cliquez sur l'onglet **Groupes**, sélectionnez un groupe, puis cliquez sur **Suivant**.

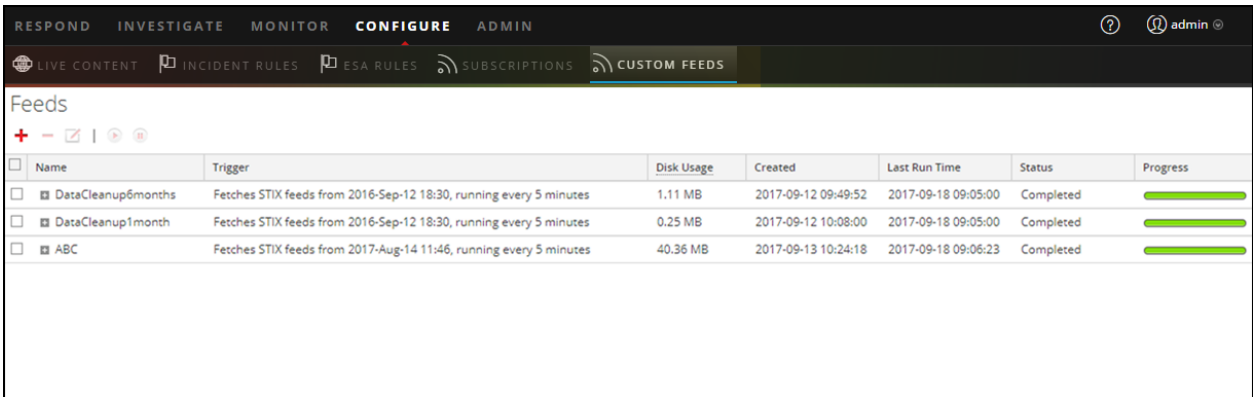
    La boîte de dialogue Examiner s’affiche.



Remarque : Si un groupe de périphériques avec des Decoders et Log Decoders est utilisé pour créer des feeds récurrents ou personnalisés, vous pouvez modifier le feed et ajouter un nouveau groupe au feed.

15. À tout moment avant de cliquer sur **Terminer**, vous pouvez :
    - Cliquez sur **Annuler** pour fermer l'assistant sans enregistrer votre définition de feed.
    - Cliquez sur **Réinitialiser** pour effacer les données de l'assistant.
    - Cliquez sur **Suivant** pour afficher le formulaire suivant (si ce n'est pas le dernier formulaire).
    - Cliquez sur **Précédent** pour afficher le formulaire précédent (si ce n'est pas le premier formulaire).
16. Passez en revue les informations du feed et, si elles sont correctes, cliquez sur **Terminer**.

Lorsque le fichier de définition de feed a été créé avec succès, l'assistant Créer un feed se ferme. Le feed et le fichier de token correspondant sont répertoriés dans la grille de feed et la barre de progression indique l'avancement. Vous pouvez développer ou réduire l'entrée pour voir combien de services sont inclus, et quels services ont abouti.



Importer le certificat SSL

Si SSL est configuré sur le feed d'identité du Log Collector, procédez comme suit pour importer le certificat SSL du Log Collector dans le magasin de clés du serveur de l'interface utilisateur NetWitness Platform. Si ce certificat n'est pas importé, le serveur de l'interface utilisateur NetWitness Platform ne pourra pas extraire le fichier d'Identity feed du Log Collector.

1. Pour extraire le certificat SSL du Log Collector, ouvrez une session SSH sur le serveur de l'interface utilisateur NetWitness Platform et exécutez la commande suivante :

   ```
   echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/<SERVERNAME>.cert
   ```

   Cette commande enregistre le certificat SSL sur `/tmp/<SERVERNAME>.cert`.

   Par exemple :

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/logcollector.cert
   ```

2. Pour importer le certificat SSL du Log Collector, ouvrez une session SSH sur le serveur de l'interface utilisateur NetWitness Platform et exécutez la commande suivante :

   ```
   keytool -importcert -alias <name an alias for the cert> -file <the cert file pathname> -keystore /etc/pki/java/cacerts
   ```

   Par exemple :

   ```
   keytool -importcert -alias logcollector01 -file /tmp/logcollector.cert -keystore /etc/pki/java/cacerts
   ```

3. Le système demande un mot de passe. Saisissez le mot de passe du magasin de clés sur le serveur de l'interface utilisateur NetWitness Platform, et non celui du magasin de clés jetty. Le mot de passe par défaut est **changeit**.

4. Redémarrez **jettysrv** pour autoriser jetty à lire le nouveau certificat dans la zone de stockage.

Impossible de vérifier l'URL du feed d'identité

Si l'URL du feed d'identité ne peut pas être vérifiée, et que vous utilisez SSL, assurez-vous d'avoir suivi les étapes décrites dans Importer le certificat SSL.

Si des problèmes persistent, il est possible que le nom interne du certificat ne corresponde pas au nom d'hôte du Log Collector. La procédure suivante vérifie cette hypothèse.

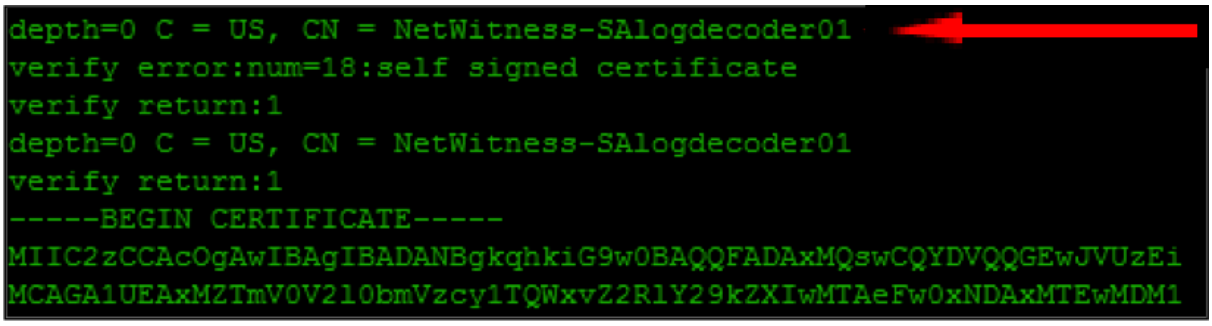
1. Session SSH sur le serveur de l'interface utilisateur NetWitness Platform.
2. Exécutez la commande suivante pour sortir le nom CN du certificat SSL :

   ```
   echo -n | openssl s_client -connect <log decoder>:50101 | sed -ne
   '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

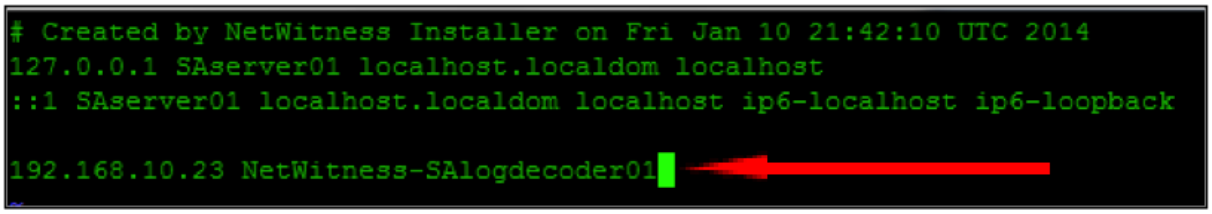
   Exemple :

   ```
   echo -n | openssl s_client -connect salogdecoder01:50101 | sed -ne
   '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

3. Récupérer le nom CN du certificat SSL.

4. Modifier le fichier `/etc/hosts` et ajoutez l'adresse IP et le nom CN dans le fichier.

5. Redémarrez les services de réseau sur l'appliance.
6. Confirmez que le nom placé dans le fichier **/etc/hosts** est utilisé au lieu du nom de domaine complet ou l'adresse IP de l'URL du feed d'identité.
7. Vérifiez à nouveau l'URL du feed d'identité.

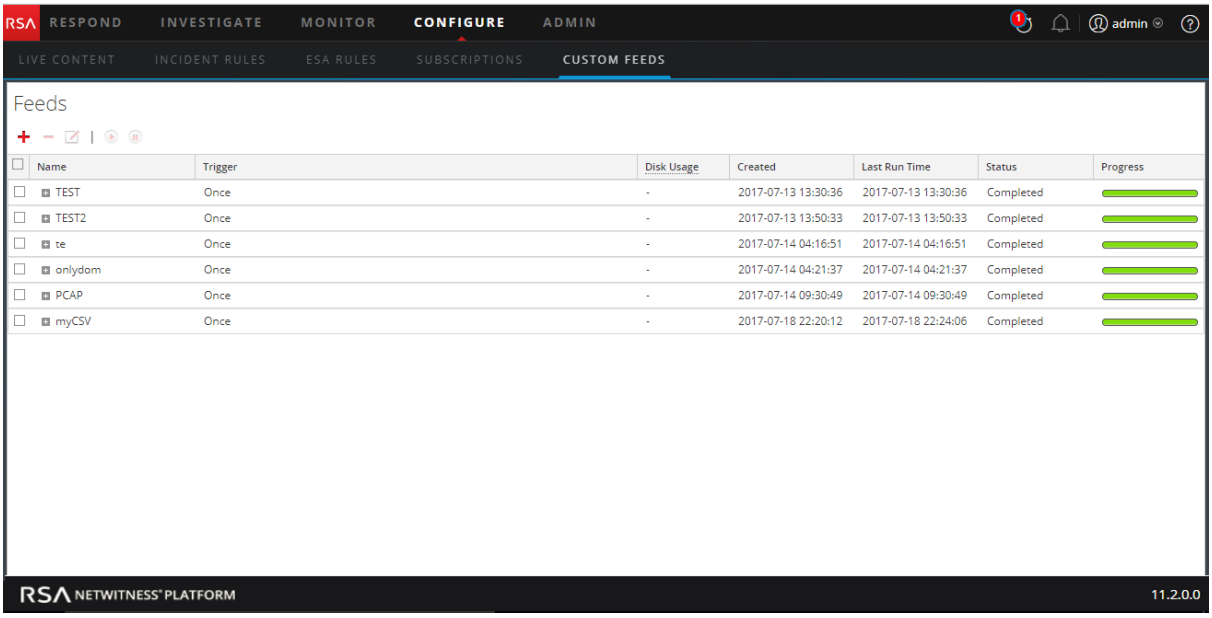
Modifier, télécharger ou supprimer un feed

Vous pouvez télécharger un feed, modifier un feed existant ou supprimer un feed.

Pour modifier un feed existant :

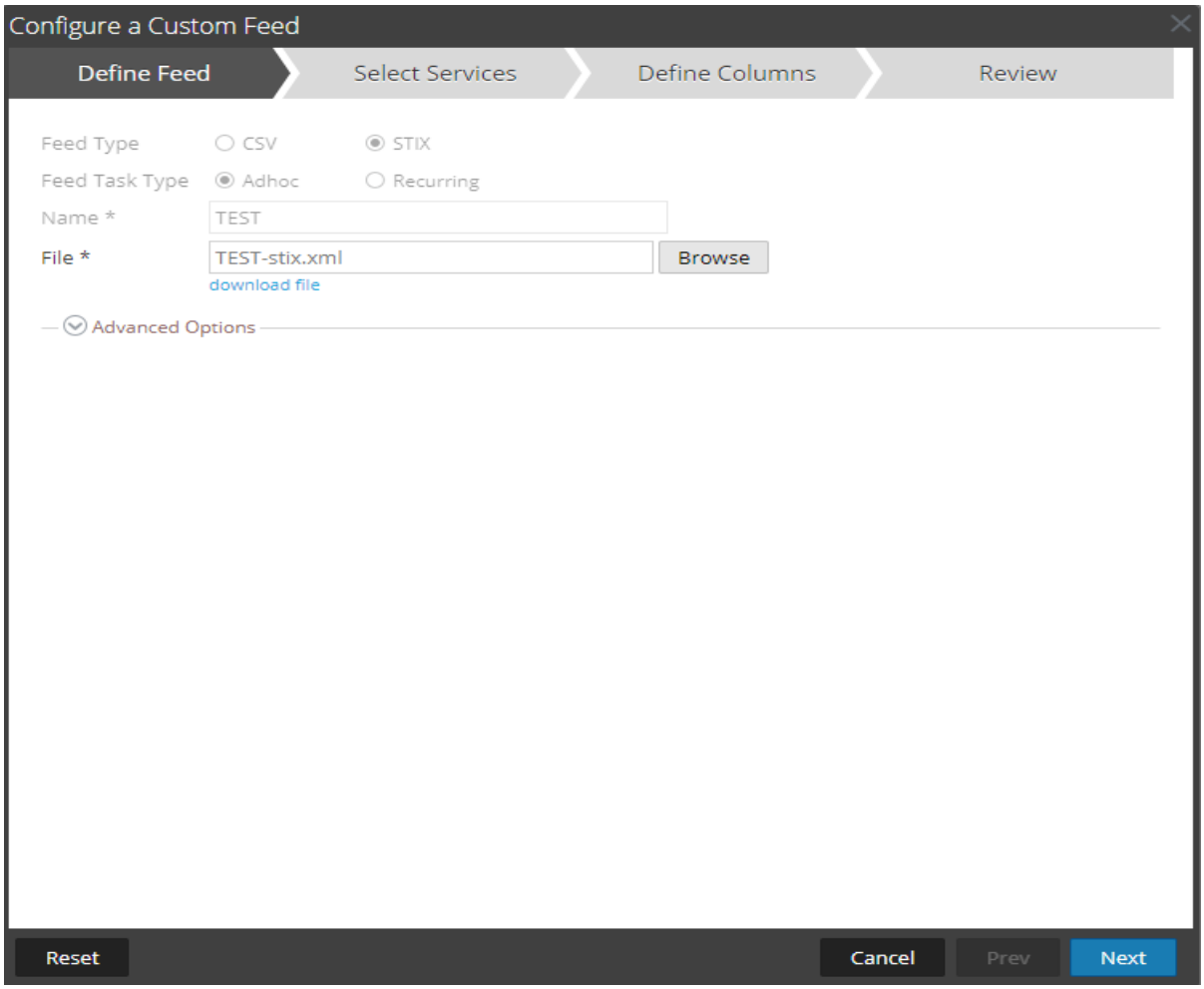
1. Accédez à **CONFIGURER > Feeds personnalisés**.

   La vue Feeds s'affiche.



2. Dans la barre d'outils, sélectionnez un feed, puis cliquez sur .

   Le panneau Configurer un feed personnalisé ou Configurer Identity Feed s'ouvre dans l'assistant Feed personnalisé.



3. Si vous souhaitez modifier le fichier de feed :
   a. Cliquez sur **Télécharger le fichier**.

      Pour le feed Identité, le fichier .zip est téléchargé. Pour un feed personnalisé, le fichier .csv ou .xml est téléchargé sur votre système de fichiers local. Pour un feed STIX, le fichier .xml est téléchargé sur votre système de fichiers local.

   b. Modifiez et enregistrez le fichier.

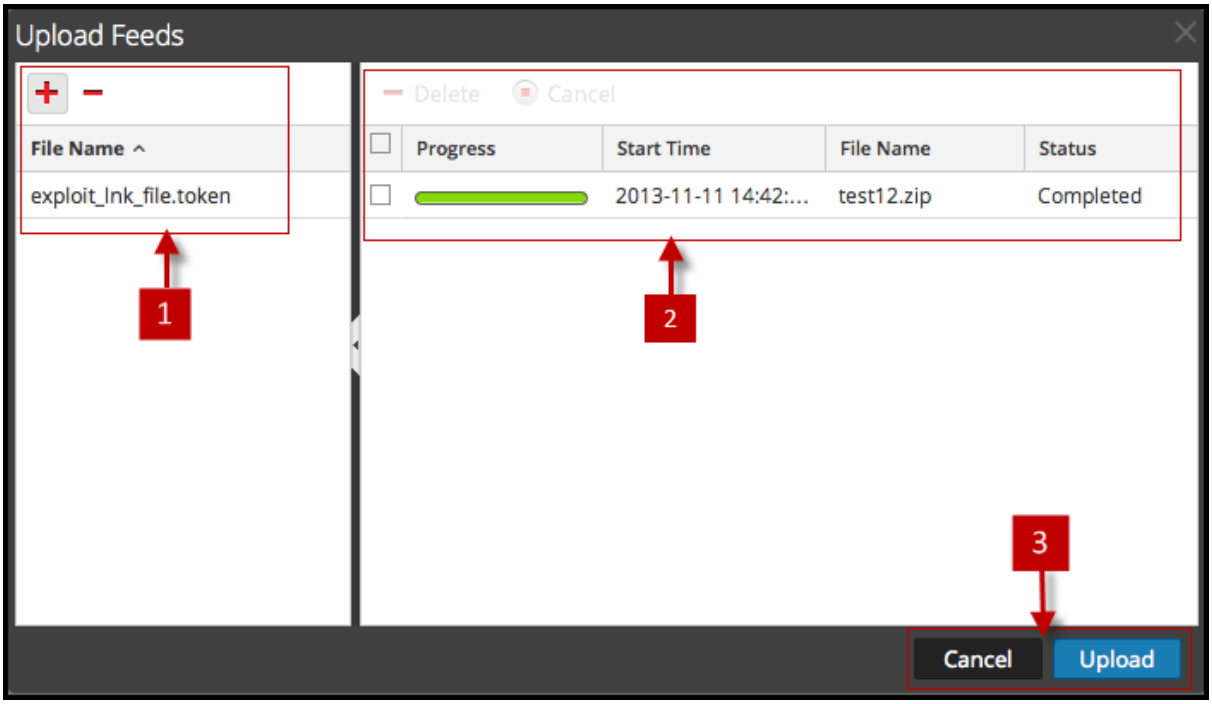
   c. Sous l'onglet **Définir le feed**, recherchez et ouvrez le fichier modifié.
4. Modifiez les autres paramètres s'appliquant au type de feed dans les onglets **Définir le feed**, **Sélectionner des services** et **Définir des colonnes**.
5. À tout moment avant de cliquer sur **Terminer**, vous pouvez :
   - Cliquer sur **Annuler** pour fermer l'assistant sans enregistrer vos modifications.
   - Cliquez sur **Réinitialiser** pour effacer les données de l'assistant.
   - Cliquez sur **Suivant** pour afficher le formulaire suivant (si ce n'est pas le dernier formulaire).
   - Cliquez sur **Précédent** pour afficher le formulaire précédent (si ce n'est pas le premier formulaire).

6. Sous l'onglet **Révision**, passez en revue les informations du feed et, si elles sont correctes, cliquez sur **Terminer**.

Le feed est recréé avec le fichier mis à jour et les nouvelles spécifications du feed. Le feed est ajouté à la liste de feeds et la barre de progression indique l'avancement. Lorsque le fichier de définition de feed est créé avec succès, l'assistant Créer un feed se ferme, et le feed et le fichier de token correspondant sont répertoriés dans la liste Feeds. Vous pouvez développer ou réduire l'entrée pour voir combien de services sont inclus, et quels services ont abouti.

Pour télécharger un feed vers un Decoder ou un Log Decoder :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service, puis cliquez sur > **Vue > Config**.
   La vue Configuration des services s'ouvre sur l'onglet Général.
3. Sélectionnez l'onglet **Feeds**.
4. Dans la barre d'outils Feeds, cliquez sur Upload.
   La boîte de dialogue Télécharger les feeds s'affiche.

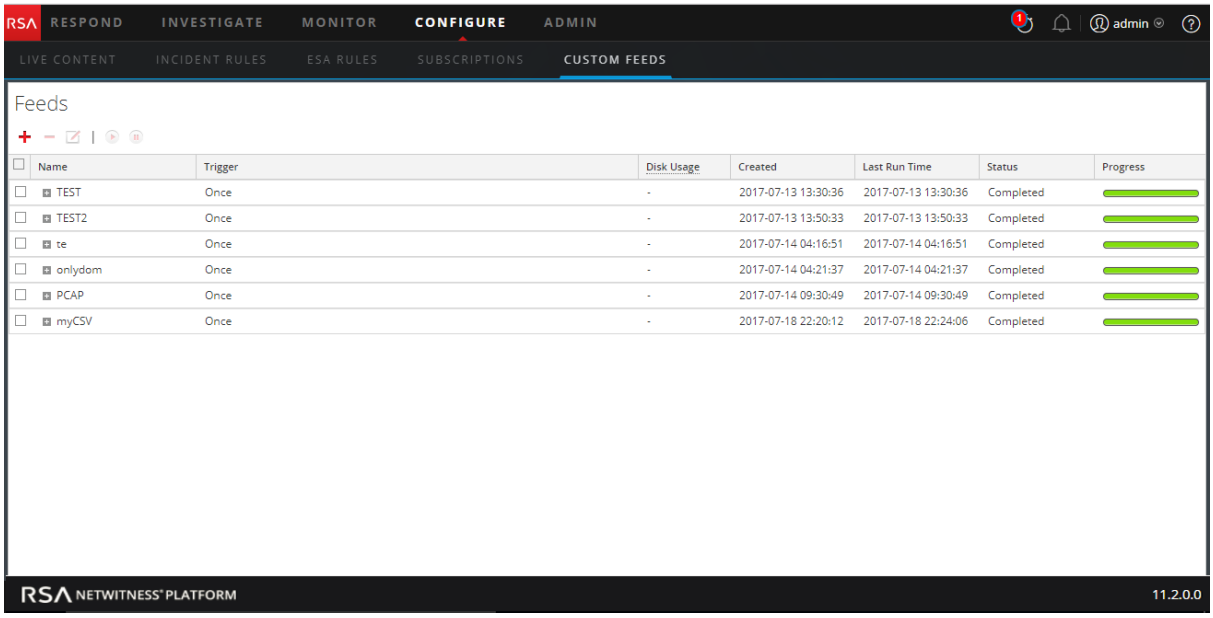


5. Dans la grille **Fichier**, cliquez sur +, puis sélectionnez un fichier de feed. Les fichiers pris en charge sont les suivants: *.feed, *.token et *.filter.
6. Sélectionnez le fichier de feed à partir de la liste **Fichier** et cliquez sur **Télécharger**.
   La liste Télécharger une tâche est mise à jour pour afficher la progression et l'état du feed téléchargé.

Pour supprimer un feed :

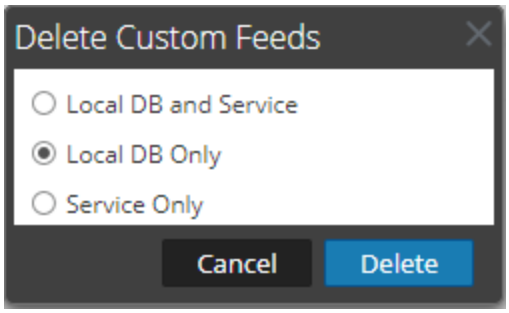
1. Accédez à **CONFIGURER > Feeds personnalisés**.

   La vue Feeds personnalisés s'affiche.



2. Dans la barre d'outils, sélectionnez un feed et cliquez sur .

   La boîte de dialogue Supprimer les feeds personnalisés s'affiche.



   Vous pouvez sélectionner l'une des options suivantes pour supprimer le feed :

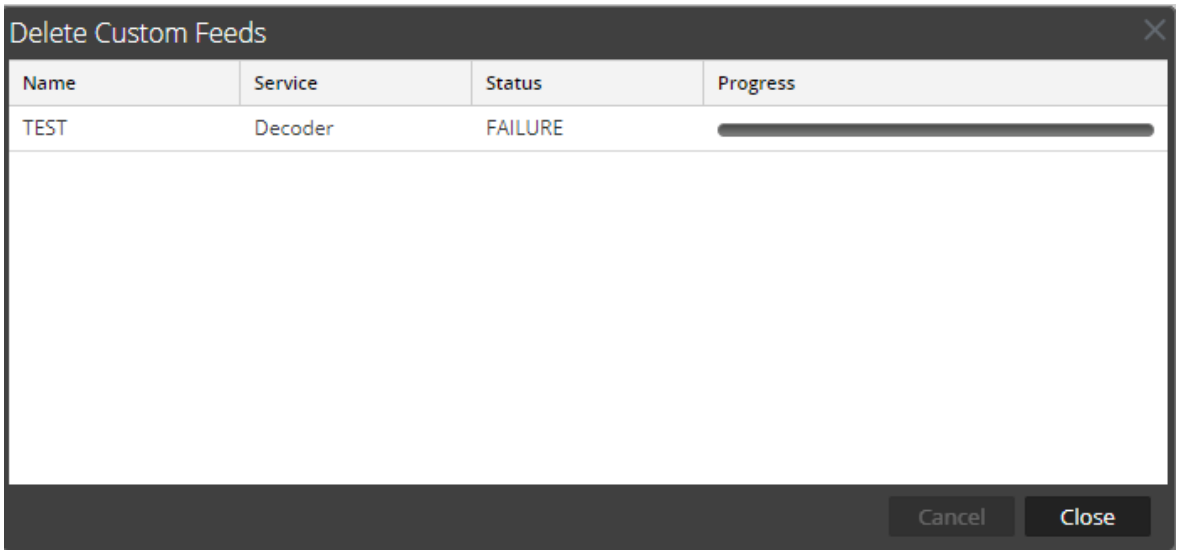
   - Si vous choisissez de supprimer le feed dans **BD locale et Service**, le feed sera supprimé à la fois dans la zone des services et de la zone NetWitness Platform locale. Le feed supprimé n'apparaîtra plus dans l'interface utilisateur NetWitness Platform.
   - Si vous choisissez de supprimer le feed depuis **BD locale uniquement**, le feed sera supprimé de la zone NetWitness Platform locale. Le feed supprimé n'apparaît plus dans l'interface utilisateur NetWitness Platform ; en revanche, la version déployée des feeds reste présente sur le service. Les feeds non déployés seront supprimés pour toujours.
   - Si vous choisissez de supprimer le feed dans **Service uniquement**, le feed est supprimé du service. Le feed supprimé apparaîtra dans l'interface utilisateur NetWitness Platform et peut être redéployé.

3. Choisissez l'emplacement où vous souhaitez supprimer le feed, puis cliquez sur **Supprimer**.

   Une boîte de dialogue d'avertissement s'affiche.

4. Cliquez sur **oui** pour confirmer la suppression du feed des zones sélectionnées.

- Si vous avez choisi de supprimer le feed dans **Base de données uniquement**, le feed est supprimé.
- Si vous avez choisi de supprimer le feed dans **Base de données locale et service** ou **Service uniquement**, la vue Supprimer les feeds personnalisés s'affiche et indique la progression de la suppression au niveau du service.



Créer des clés méta personnalisées à l'aide d'un feed personnalisé

Cette rubrique fournit des informations sur la façon d'ajouter des clés méta personnalisées à l'aide d'un feed personnalisé dans le Log Decoder.

Vous pouvez créer des clés méta personnalisées pour récupérer des données, effectuer des recherches et des analyses dans des logs et des paquets. Les clés méta personnalisées vous permettent d'ajouter un contexte d'enrichissement pour les données de logs et de paquets. Ce document met en évidence les changements de configuration pour refléter les clés méta personnalisées dans le schéma des services Concentrator, ESA, Archiver, Warehouse Connector et Reporting Engine.

Voici un exemple de création de clé méta personnalisée dans le service Log Decoder. Dans ce scénario, une organisation veut suivre l'emplacement d'une ressource, telle qu'une imprimante. Donc, une clé méta personnalisée **source location** est ajoutée pour désigner l'emplacement de la ressource, par exemple Imprimante1, qui est située au « 5ème étage, aile A ».

Remarque : Les clés méta personnalisées peuvent également être créées dans le Decoder. Sélectionnez le fichier `index-decoder-custom.xml` lorsque vous créez une clé méta personnalisée dans le Decoder.

Ajouter une clé méta personnalisée au Log Decoder

Pour ajouter des clés méta personnalisées à l'aide du feed personnalisé :

1. Accédez à **ADMIN** > Services**.**
2. Sélectionnez un service Log Decoder, puis cliquez sur  > **Vue** > **Config** > onglet **Fichiers** > **index-logdecoder-custom.xml.**

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexNone"
name="location.src" format="Text"/>
 </Language>
```

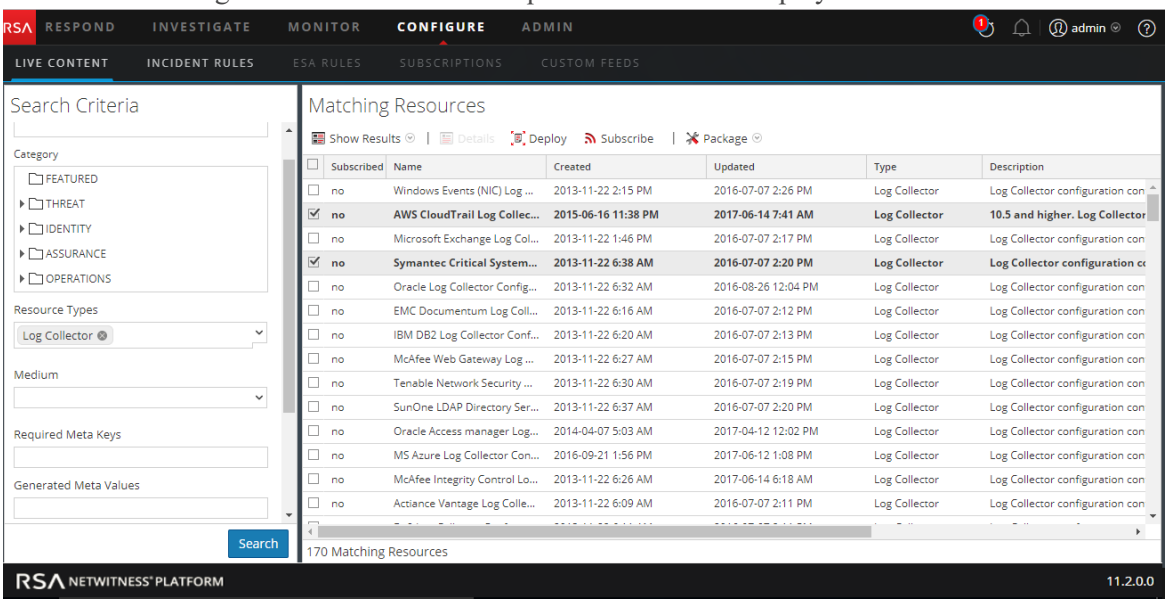
3. Redémarrez le service Log Decoder. Dans la vue Services, cliquez sur  > **Redémarrer**.

Déployer un feed Log Decoder dans Live

Pour déployer le feed dans l'environnement Live :

1. Accédez à **CONFIGURER > Contenu Live.**
2. Sélectionnez un groupe de ressources ou un package de ressources précédemment créé. Pour sélectionner une ressource ou un groupe de ressources :
   a. Dans la **Vue Live Search,** parcourez la ressource Live (par exemple, recherchez le type de ressource **Log Collector**).
   b. Dans le panneau **Ressources correspondantes**, sélectionnez **Afficher les résultats > Grille**.

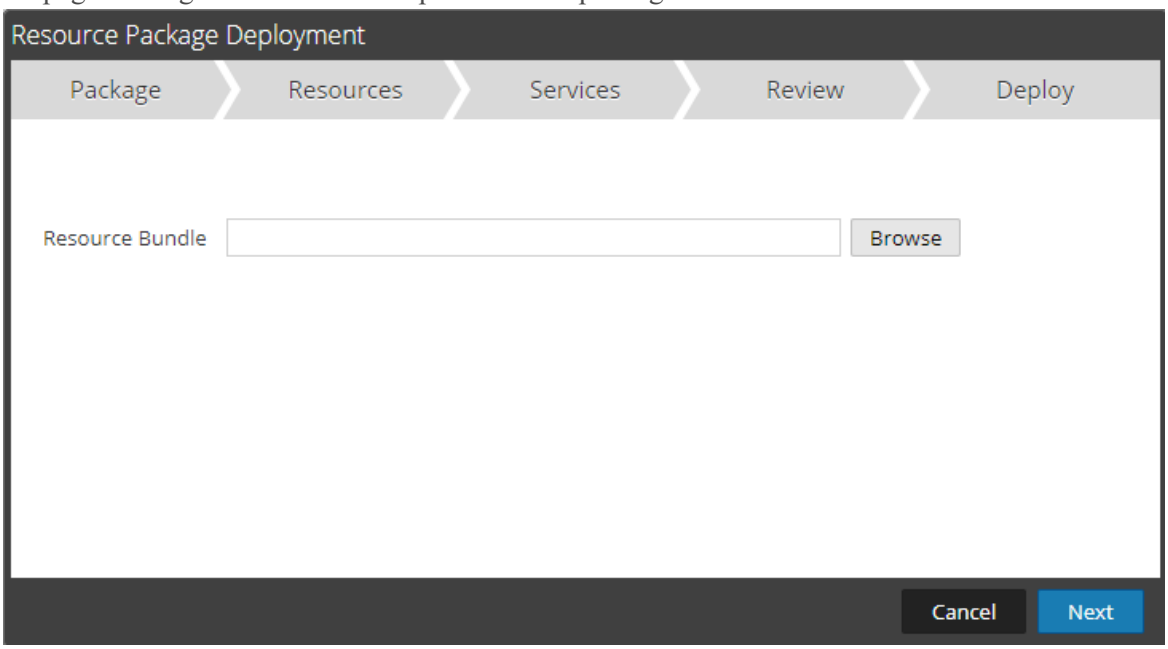
c. Cochez la case à gauche ou les ressources que vous souhaitez déployer.



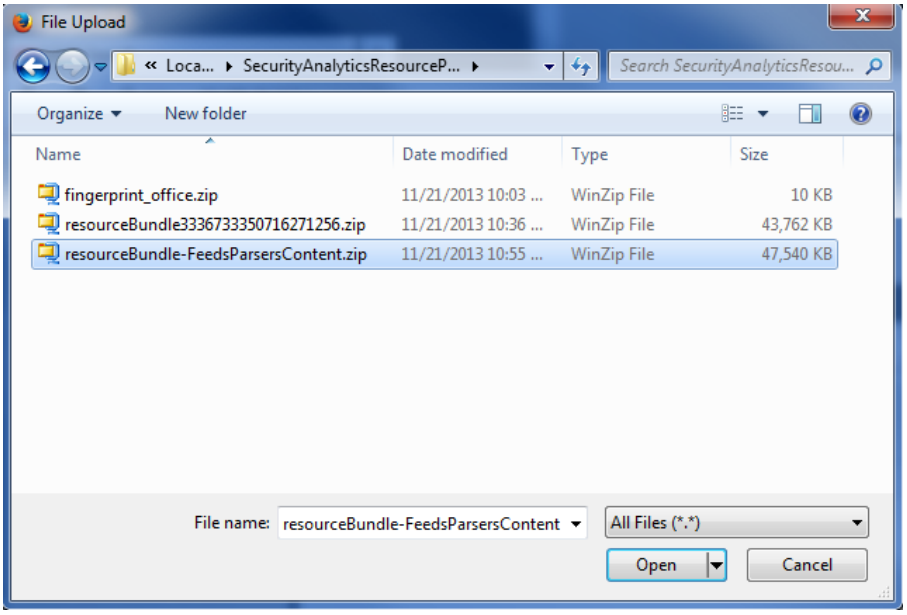
d. Dans la barre d'outils Ressources correspondantes, cliquez sur Deploy.

3. Pour sélectionner un package de ressources à déployer :

a. Dans la vue **Live Search**, dans la barre d'outils **Ressources correspondantes**, sélectionnez **Package** > **Déployer** :
La page Package de l'Assistant Déploiement du package de la ressource s'affiche.



b. Cliquez sur **Parcourir** et sélectionnez un package sur votre réseau (par exemple, **resourceBundle-FeedsParsersContent.zip**).



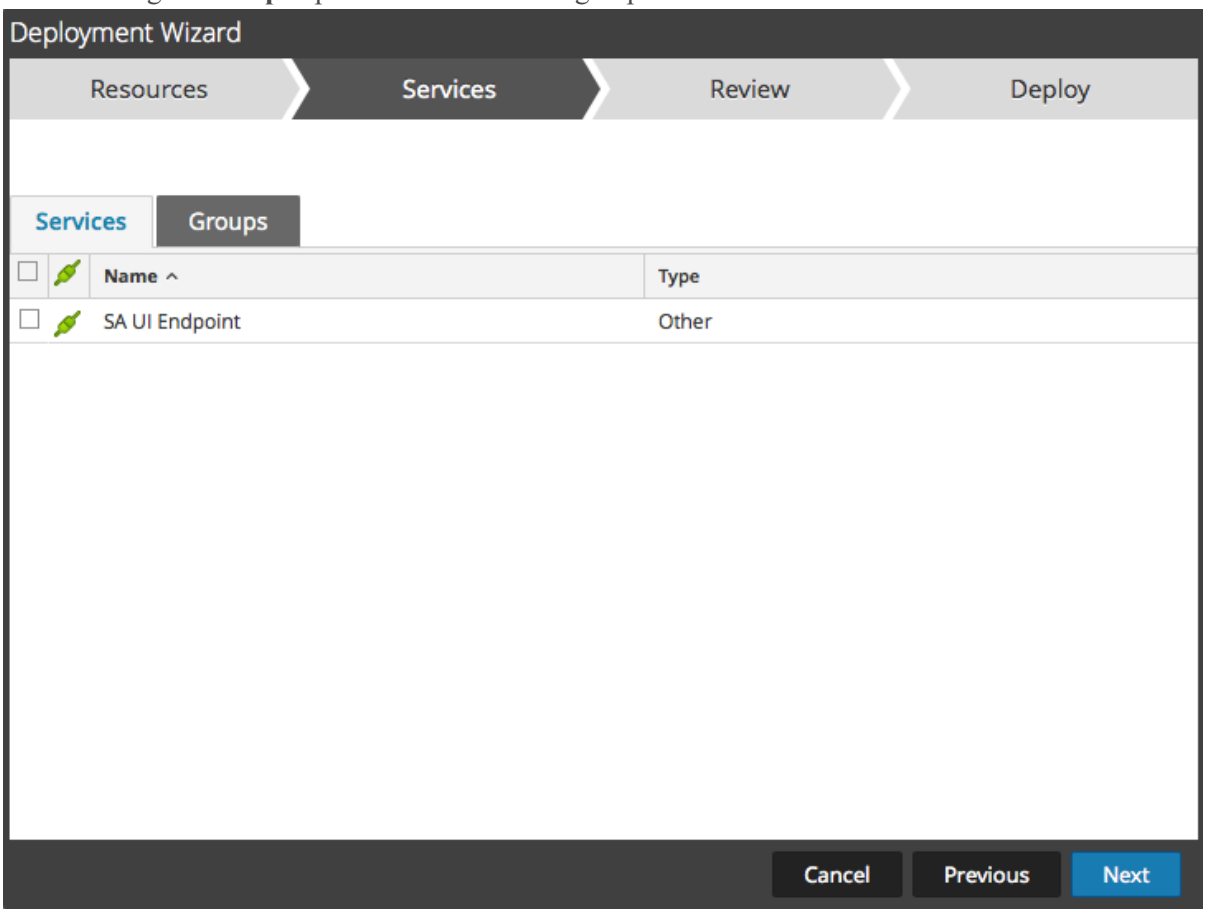
c. Cliquez sur **Ouvrir.**
À ce stade, que vous déployiez un package ou un groupe de ressources, l'Assistant Déploiement s'ouvre et la page Ressources s'affiche.

3. Cliquez sur **Suivant**.
La page **Services** s'affiche et possède deux onglets, **Services** et **Groupes**, qui fournissent une liste de services et groupes de services qui sont configurés dans la vue Administration > Services. Les colonnes représentent un sous-ensemble des colonnes disponibles dans la vue Services.

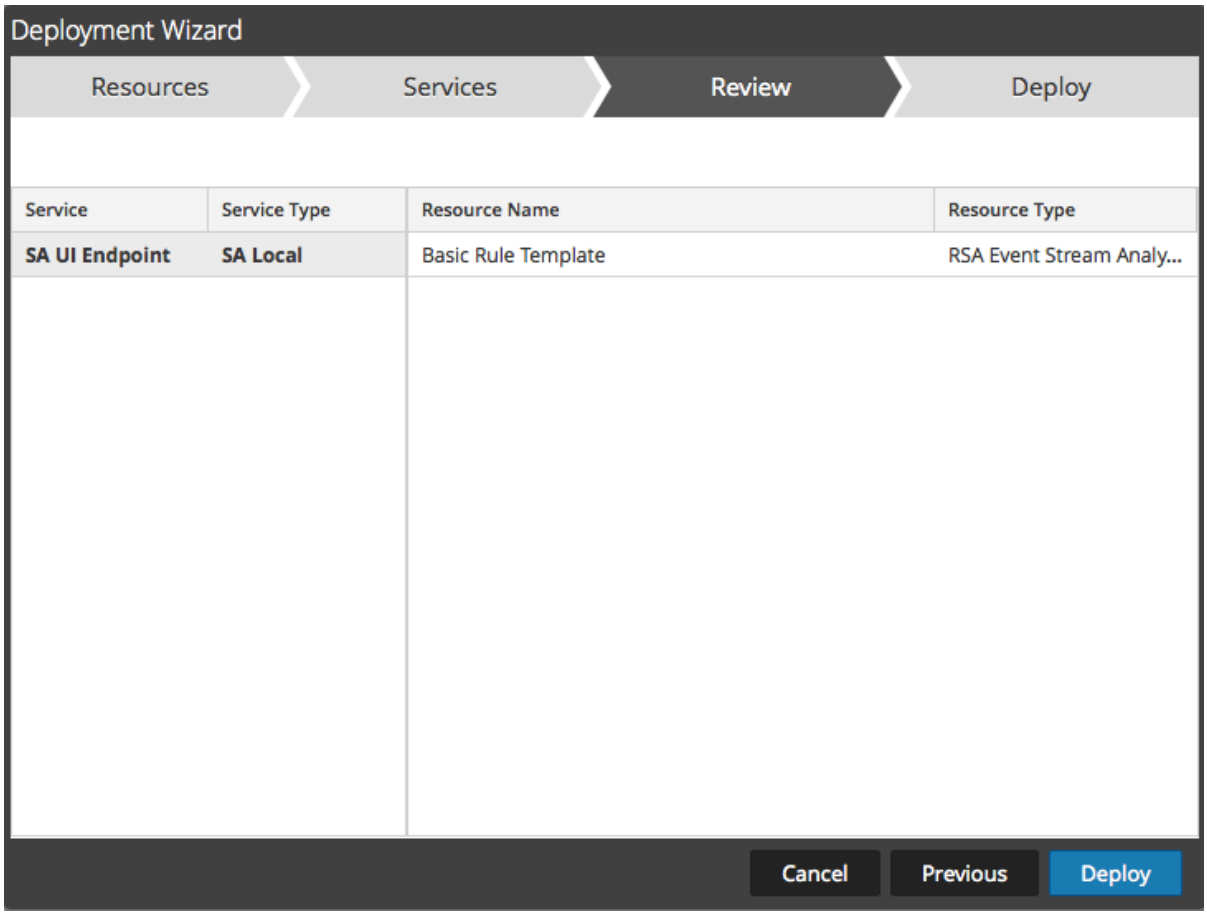
Remarque : Le serveur Live réagit de manière intelligente pour le déploiement des ressources vers les Services. Par exemple, il ne déploie pas de ressources disposant de paquets vers n'importe quel Log Decoder. Cela signifie que seul le contenu applicable est déployé vers chaque service.

4. Sélectionnez les services au niveau desquels vous souhaitez déployer le contenu. Vous pouvez sélectionner une combinaison de services et de groupes de services.
Utilisez l'onglet **Services** pour sélectionner chaque service, la liste des services et des groupes de services qui sont configurés dans la vue Services d'administration.

Utilisez l'onglet **Groupes** pour sélectionner des groupes de services.

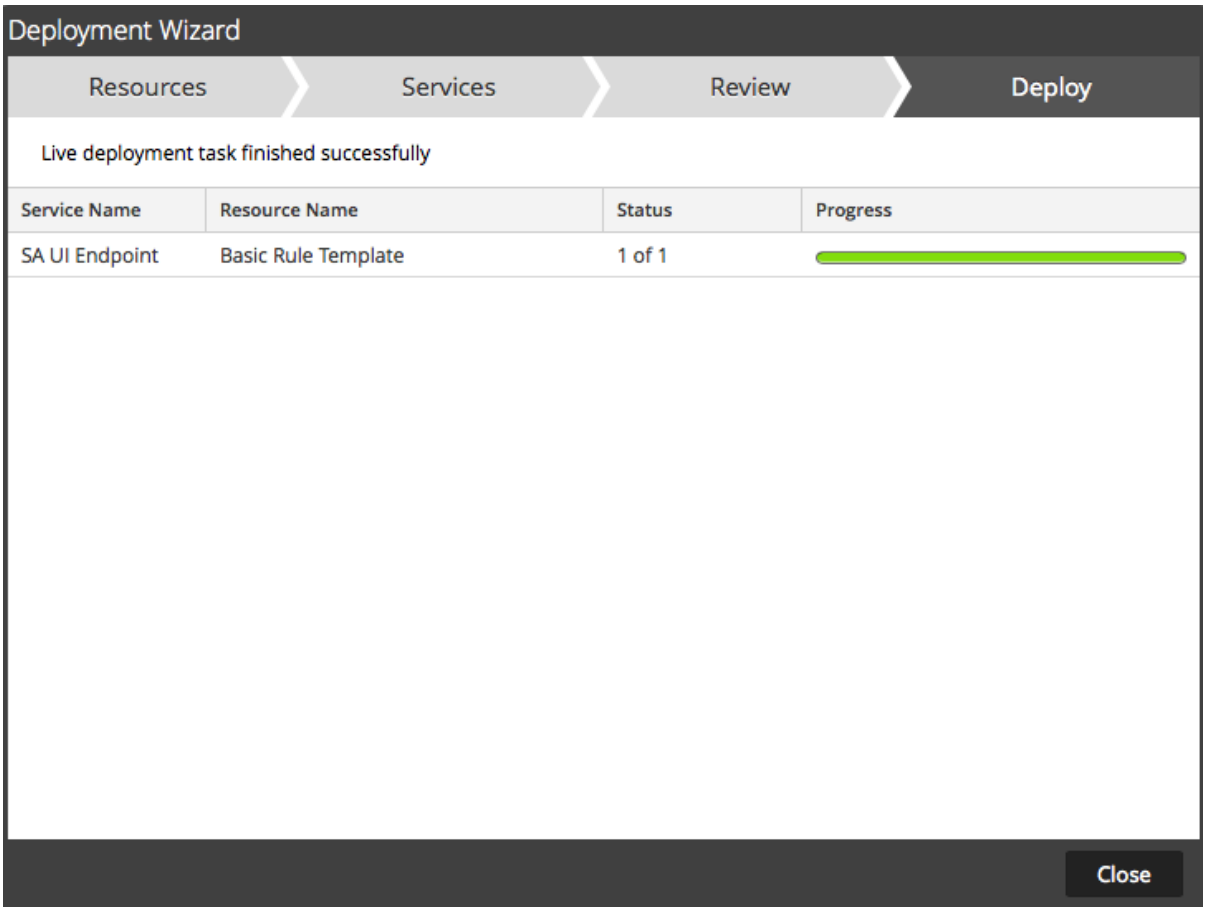


5. Cliquez sur **Suivant**.
   La page **Révision** s'affiche.

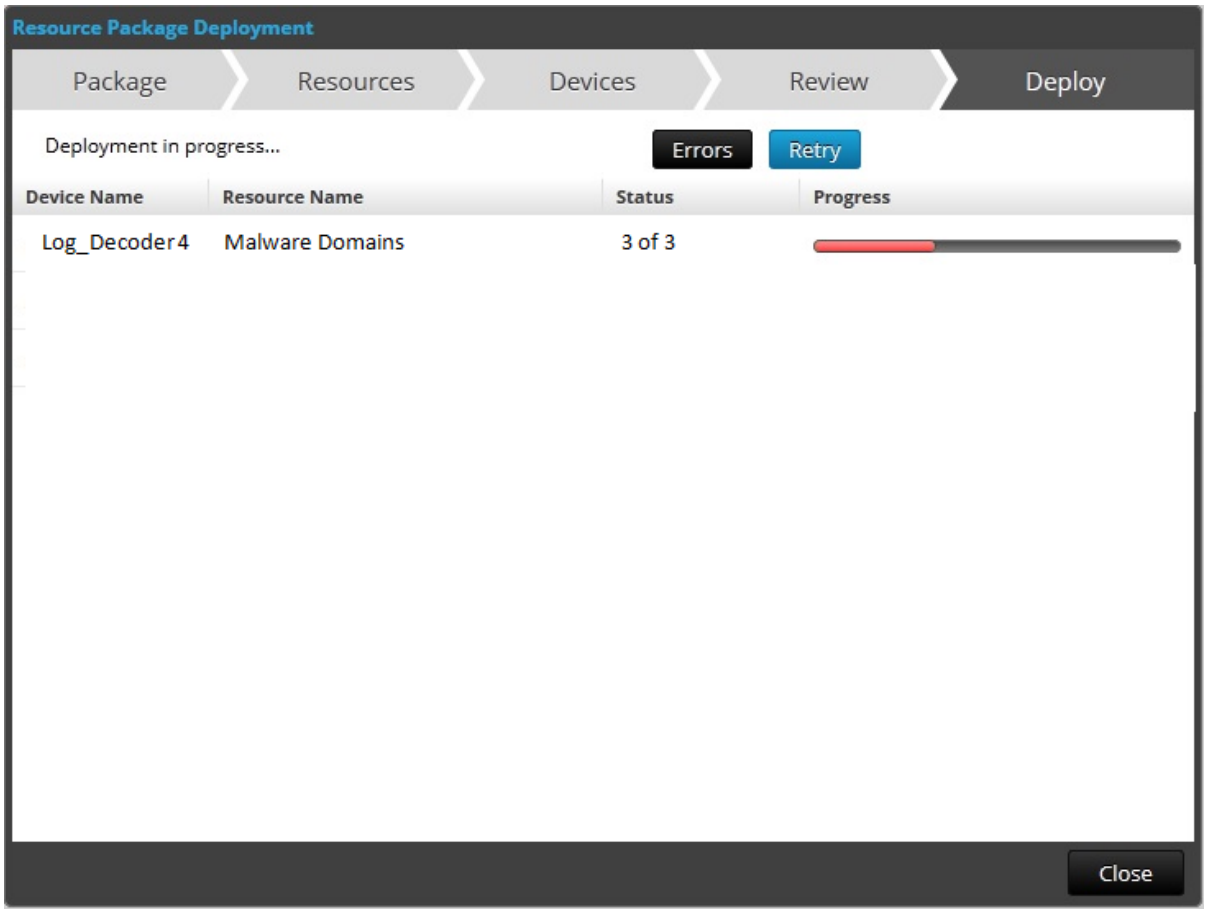


Veillez à sélectionner les ressources appropriées et les services au niveau desquels vous souhaitez effectuer le déploiement.

6. Cliquez sur **Déployer**.
   La page **Déployer** s'affiche. La barre de progression devient verte lorsque vous avez réussi à déployer les ressources au niveau des services sélectionnés.



Si vous tentez de déployer des ressources et des services incompatibles, NetWitness Platform affiche les boutons Erreurs et Réessayer sur lesquels vous pouvez cliquer pour réviser les erreurs et essayer à nouveau d'effectuer le déploiement.



7. Cliquez sur **Fermer**.

Remarque : L'adresse IP source doit être indexée en sélectionnant le type 'IP' car ip.src. et ip.dst sont au format IPv4.

Dans ce scénario, une clé méta personnalisée location.src (source de localisation) est ajoutée par l'indexation du nom d'hôte (alias.host). Dans cet exemple, le nom d'hôte de l'imprimante est renseigné dans la clé méta 'alias.host'. Sélectionnez **alias.host** comme clé de rappel et le type d'index comme 'Non IP' dans l'Assistant Feed, comme indiqué ci-dessous. Dans la section Définissez les valeurs, sélectionnez la clé méta personnalisée dans le menu déroulant.

Ajouter l'entrée de la clé méta personnalisée dans le fichier d'index personnalisé du Concentrator

Pour l'entrée de la clé méta personnalisée dans le fichier d'index personnalisé du Concentrator :

1. Accédez à **ADMIN**> **Services** > **Concentrator**.
2. Cliquez sur > **Vue** > **Config** > **onglet Fichiers** > **index-concentrator-custom.xml.**
3. Ajouter l'entrée de la clé méta personnalisée au fichier d'index du service Concentrator.

```
<Language>
 <?xml version="1.0" encoding="utf-8"?>
 <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location"  level="IndexValues"
name="location.src" format="Text"  valueMax="10000"
defaultAction="Open"/>
 </Language>
```

4. Pour redémarrer le service Concentrator, dans la vue Services, cliquez sur > **Redémarrer**.

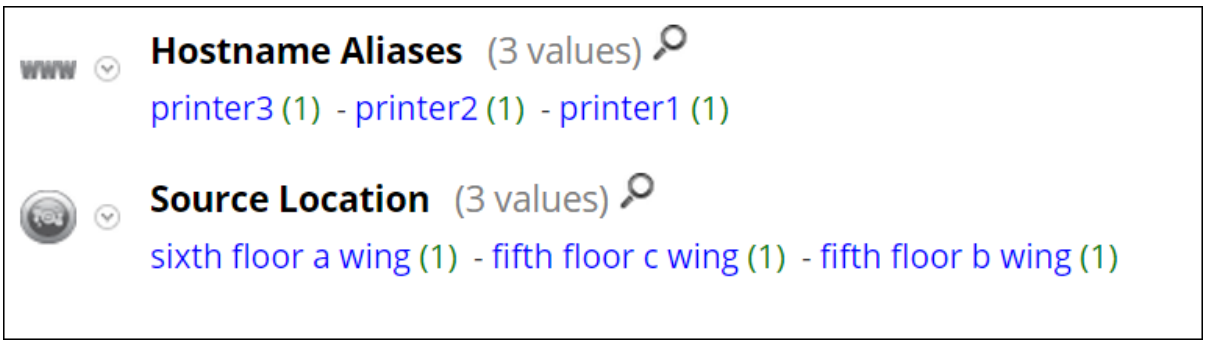
Remarque : Dans le cas du service Broker, ce dernier récupère son index du service Concentrator à partir duquel il effectue l'agrégation. Vous n'avez donc pas besoin de créer un méta personnalisé dans le service Broker. Si vous n'avez pas indexé la clé méta dans le service Concentrator, le service Broker ne sera pas affiché sous Investigation.

Effectuer une recherche de clé méta personnalisée

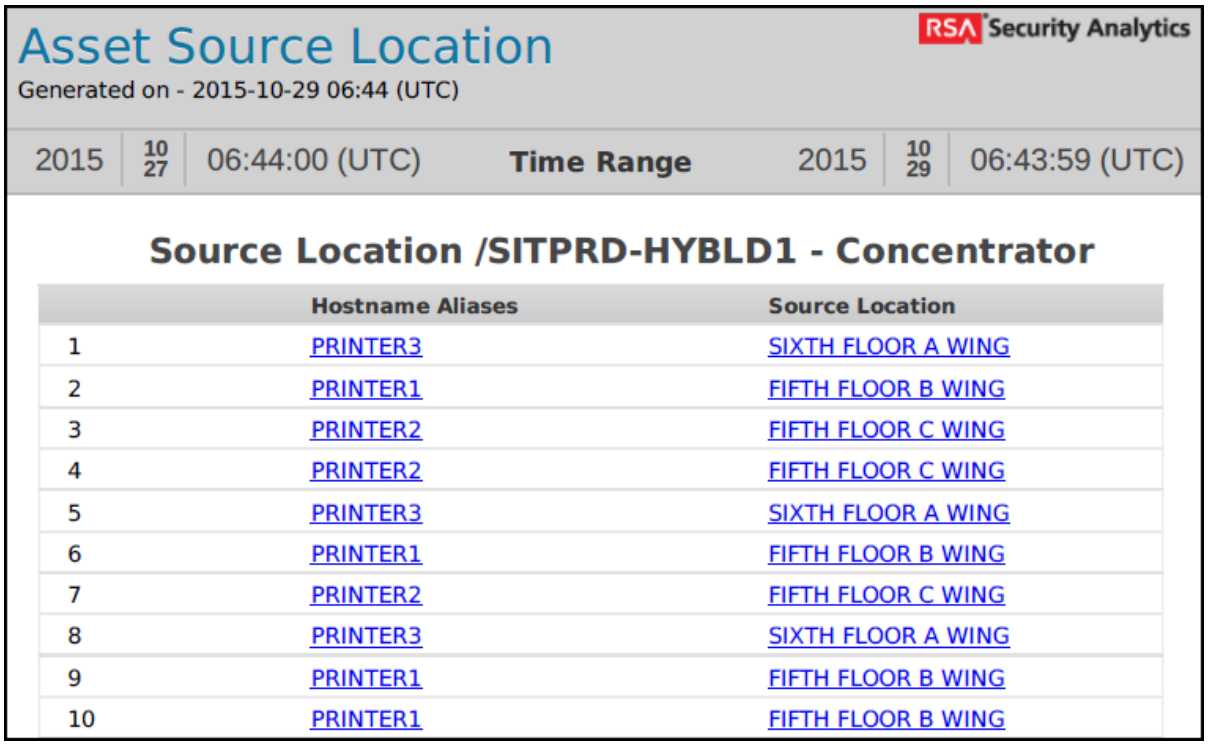
Remarque : Vous devez vous déconnecter et vous reconnecter à partir de l'interface utilisateur de NetWitness Platform, pour pouvoir afficher la clé méta personnalisée dans Investigation.

Pour effectuer la recherche de la clé méta personnalisée :

1. Accédez à **ENQUÊTER**. Une boîte de dialogue qui fournit des services à sélectionner s'affiche.
2. Sélectionnez un service Concentrator, puis cliquez sur **Naviguer**.



Voici un exemple de rapport exécuté sur le service Concentrator.



Asset Source Location

RSA Security Analytics

Generated on - 2015-10-29 06:44 (UTC)

2015	10 27	06:44:00 (UTC)	Time Range	2015	10 29	06:43:59 (UTC)

Source Location /SITPRD-HYBLD1 - Concentrator

	Hostname Aliases	Source Location
1	PRINTER3	SIXTH FLOOR A WING
2	PRINTER1	FIFTH FLOOR B WING
3	PRINTER2	FIFTH FLOOR C WING
4	PRINTER2	FIFTH FLOOR C WING
5	PRINTER3	SIXTH FLOOR A WING
6	PRINTER1	FIFTH FLOOR B WING
7	PRINTER2	FIFTH FLOOR C WING
8	PRINTER3	SIXTH FLOOR A WING
9	PRINTER1	FIFTH FLOOR B WING
10	PRINTER1	FIFTH FLOOR B WING

Procédures supplémentaires

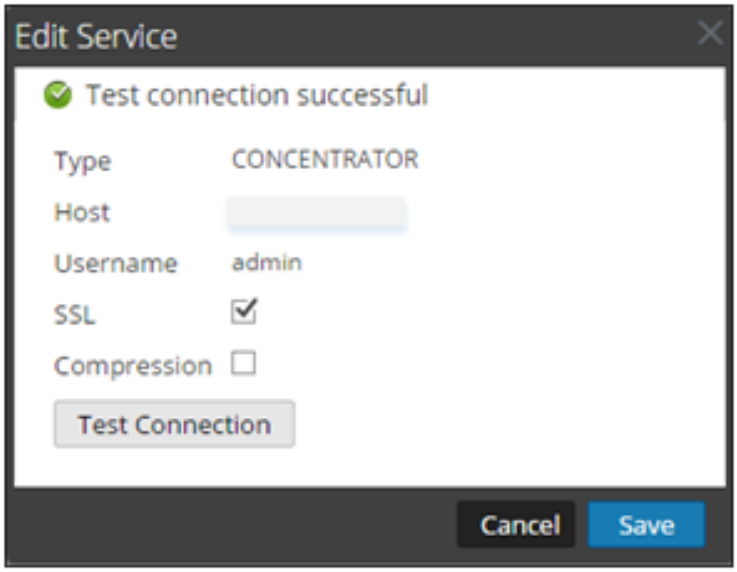
Les procédures suivantes doivent être exécutées si vous avez configuré les services Warehouse Connector, Archiver, Reporting Engine et ESA.

Mettre à jour le schéma dans ESA

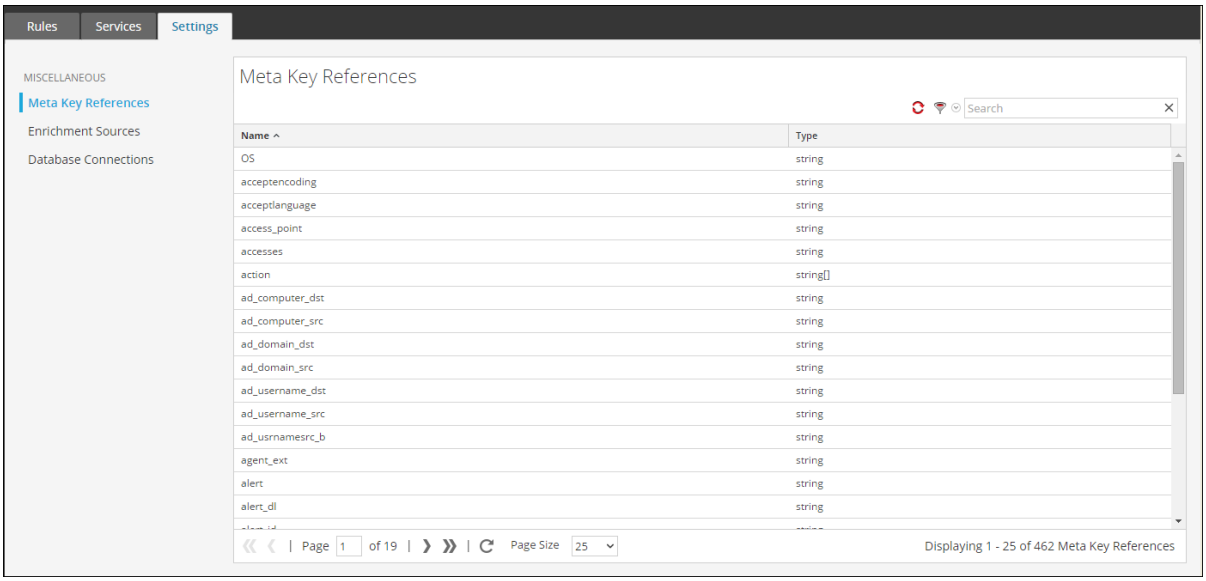
Avant de mettre à jour le schéma dans ESA, la clé méta personnalisée doit être indexée dans le service Concentrator.

Pour mettre à jour les règles ESA du schéma et pouvoir utiliser les nouvelles clés méta personnalisées :

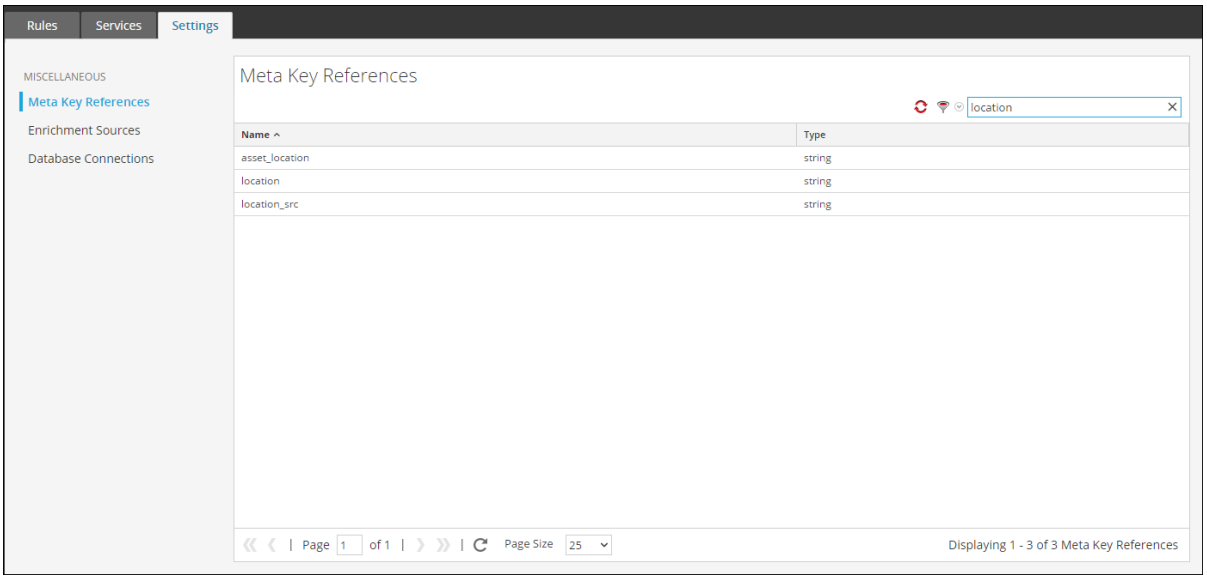
1. Accédez à **ADMIN** > **Services** > **ESA- Event Stream Analysis** > **Vue** > **Config**.
2. Modifiez la source de données Concentrator.
3. Cliquez sur **Tester la connexion**.



4. Cliquez sur **Enregistrer** une fois la connexion établie.
5. Cliquez sur **Appliquer**.
6. Naviguez jusqu'à **Configurer** > **Règles ESA** > **paramètres**.



7. Cliquez sur l'onglet **Rechercher** puis recherchez le nom de la clé méta personnalisée.
   Le nom et le type de la clé méta personnalisée apparaissent.



Mettre à jour le schéma dans Archiver

Si vous souhaitez configurer Archiver, à l'aide des clés méta personnalisées, vous devez mettre à jour le schéma Archiver dans le Reporting Engine. Pour mettre à jour le schéma Archiver dans Reporting Engine :

1. Accédez à **ADMIN** > **Services** > **Archiver**.
2. Sélectionnez > **Vue** > **Config** > **Fichiers** > **index-archiver-custom.xml**.
3. Ajoutez l'entrée de clé méta personnalisée dans le fichier d'index Archiver.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexValues"
name="location.src" format="Text"
  valueMax="10000" defaultAction="Open"/>
 </Language>
```

4. Pour redémarrer le service Archiver, cliquez sur > **Redémarrer.**
   Le schéma Archiver est mis à jour avec la clé méta personnalisée.

Mettre à jour le schéma dans Warehouse Connector

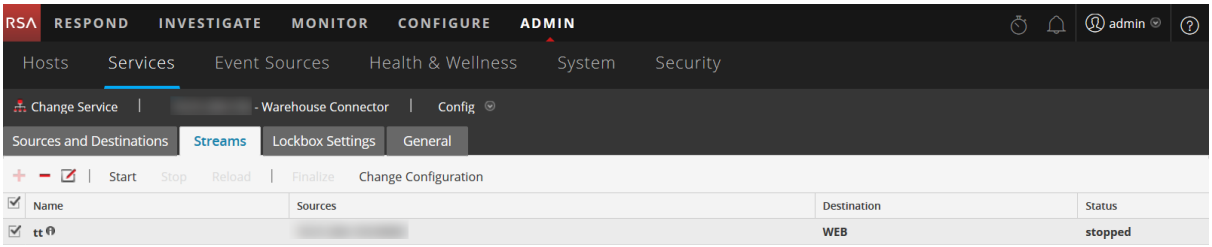
Si vous souhaitez configurer Warehouse Connector avec la métadonnée personnalisée et l'utiliser dans le rapport Warehouse Connector, vous devez mettre à jour le schéma Warehouse Connector dans le Reporting Engine.

Si le service Log Decoder ou Decoder, où la clé méta personnalisée est ajoutée, représente l'une des sources du flux Warehouse Connector, vous devrez mettre à jour le schéma dans Warehouse Connector.

Pour mettre à jour le schéma Warehouse Connector dans Reporting Engine :

1. Accédez à **ADMIN** > **Services** > **Warehouse Connector**.
2. Cliquez sur > **Vue** > **Config** > **onglet Fichiers** > **index-logdecoder-custom.xml.**

3. Sélectionnez le flux, puis cliquez sur **Recharger**.
   Le service Warehouse Connector extrait le schéma des périphériques en aval (Log Decoder/Decoder).



Pour plus d'informations sur les flux, reportez-vous à la rubrique « Configurer les flux » dans le *Guide de configuration de Warehouse Connector*.

Mettre à jour le schéma dans Reporting Engine

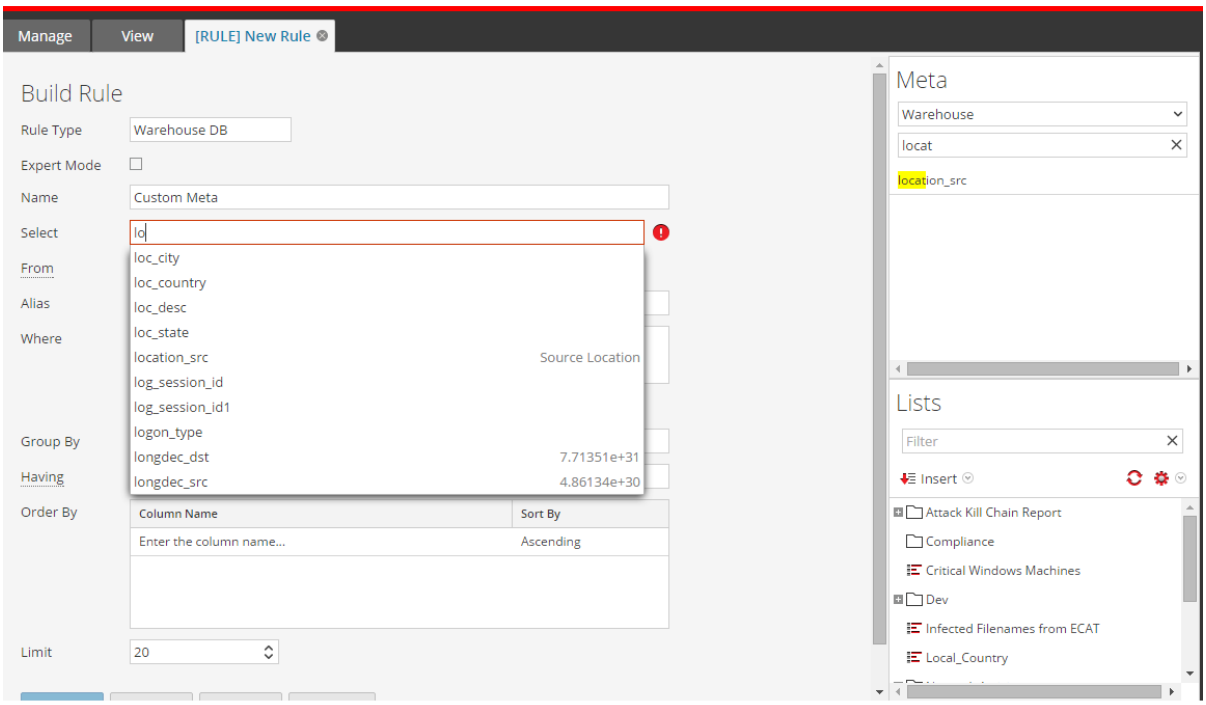
Pour mettre à jour le schéma dans Reporting Engine :

1. Accédez à **ADMIN** > **Services** > **Reporting Engine.**
2. Cliquez sur > **Redémarrer.**

Remarque : Redémarrez le Reporting Engine ou patientez trente minutes pour que le schéma se mette à jour.

Pour afficher la clé méta personnalisée :

1. Accédez à **Moniteur** > **Rapports** > **Règles**.
2. Dans la barre d'outils, cliquez sur .
3. Sélectionnez **Base de données Warehouse**.
4. Sur l'onglet Élaborer une règle, recherchez le méta personnalisé dans le panneau droit de la page.
   La clé méta personnalisée s'affiche.



Télécharger et supprimer des analyseurs personnalisés

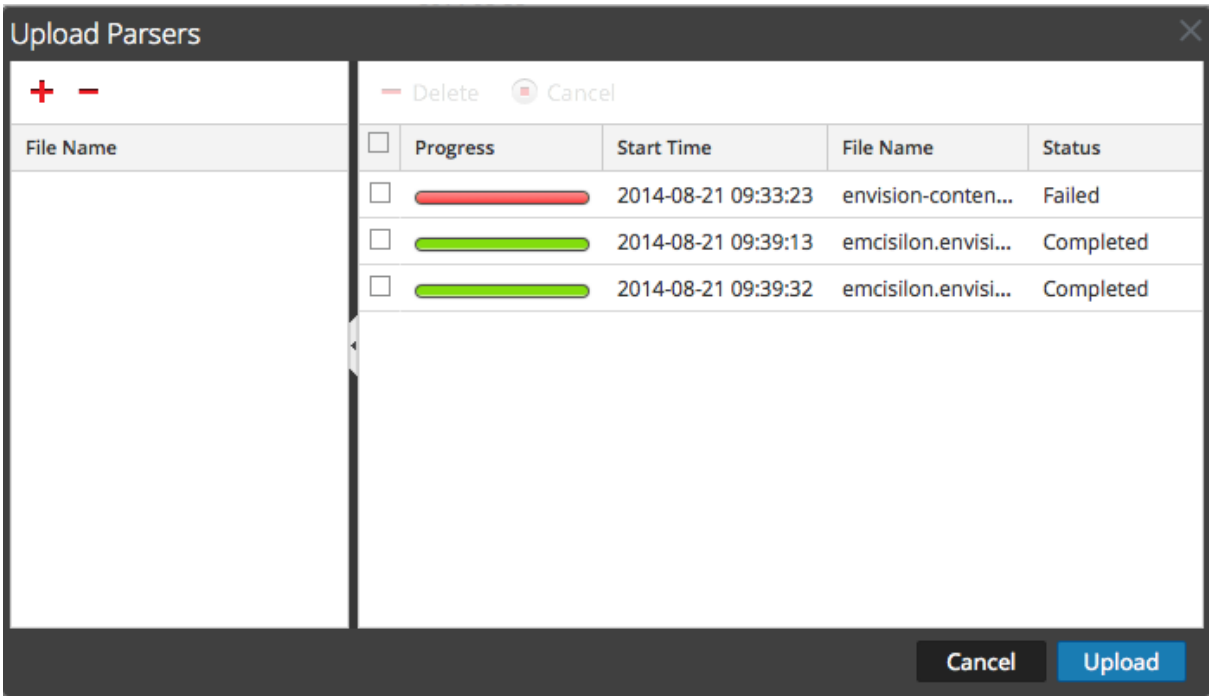
RSA NetWitness Platform peut télécharger des analyseurs à partir de votre système local et de les supprimer.

Télécharger des analyseurs vers un Decoder ou Log Decoder

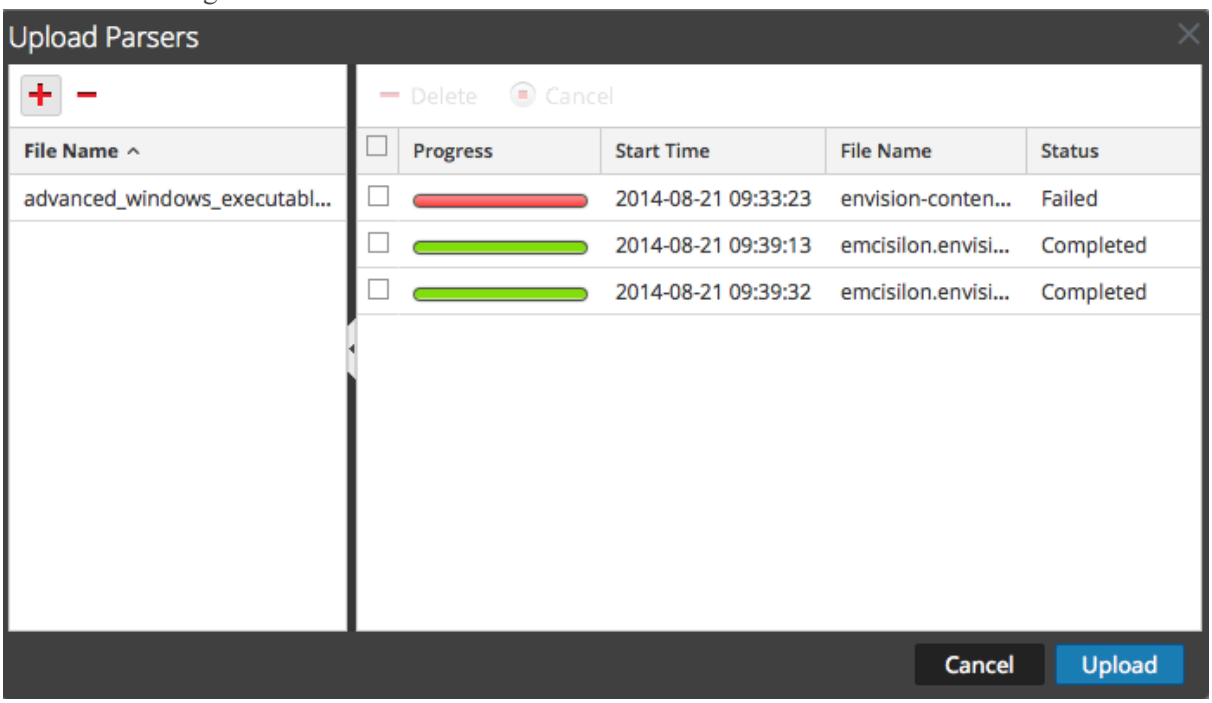
L'option Télécharger de la vue Configuration des services > onglet Analyseurs affiche la boîte de dialogue Télécharger les analyseurs, dans laquelle vous pouvez gérer le téléchargement des analyseurs vers un Decoder ou Log Decoder. Dans la liste Fichier, vous préparez une liste d'analyseurs à télécharger. Vous pouvez ajouter des fichiers à partir d'une structure de répertoire et supprimer des fichiers d'une liste si vous décidez que vous ne souhaitez pas télécharger un fichier particulier. Lorsque cette liste est prête, cliquez sur Télécharger pour lancer le téléchargement.

1. Accédez à **ADMIN > Services**, sélectionnez un service, puis > **Vue > Config.**
   La vue Configuration pour le service sélectionné s'affiche.
2. Cliquez sur l'onglet **Parsers**.

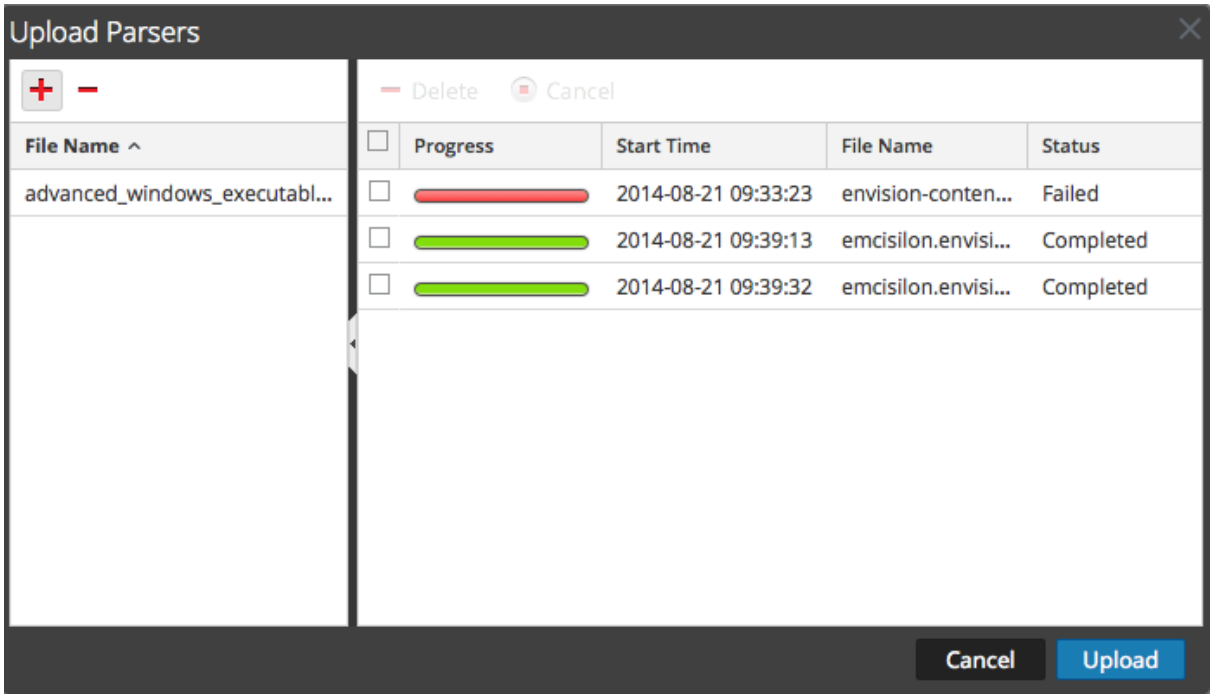
3. Cliquez sur Upload.
   La boîte de dialogue Télécharger les analyseurs s'affiche.



4. Cliquez sur + .
   Une boîte de dialogue de sélection de fichier s'affiche.
5. Sélectionnez les fichiers **.flex**, **.parser** et **.lua** à mettre à jour, puis cliquez sur **Ouvrir**.
   La boîte de dialogue se ferme et les fichiers sélectionnés s'affichent dans la liste Fichier.



6. Cliquez sur **Télécharger**.
   La grille Télécharger une tâche affiche la progression des tâches de téléchargement, chaque tâche représentant un fichier à télécharger.



7. Utilisez l'un des outils de grille Télécharger pour gérer le téléchargement des tâches sélectionnées : mettre en pause et reprendre, annuler et supprimer.
   Une fois qu'une tâche est terminée, elle est déployée sur le Decoder et répertoriée avec les analyseurs déployés sous l'onglet Analyseurs.

Gérer les tâches de téléchargement

Vous pouvez utiliser l'un des outils de grille Télécharger pour gérer le téléchargement des tâches sélectionnées : mettre en pause et reprendre, annuler et supprimer.

- Pour annuler le téléchargement d'un ensemble d'analyseurs pendant que le téléchargement est en file d'attente ou en cours, cliquez sur Cancel.
- Pour mettre en pause le téléchargement d'un ensemble d'analyseurs, si le téléchargement n'est pas encore terminé, cliquez sur Pause.
- Pour reprendre le téléchargement d'un ensemble d'analyseurs après une pause, cliquez sur Resume.
- Pour supprimer une tâche de téléchargement, cliquez sur .

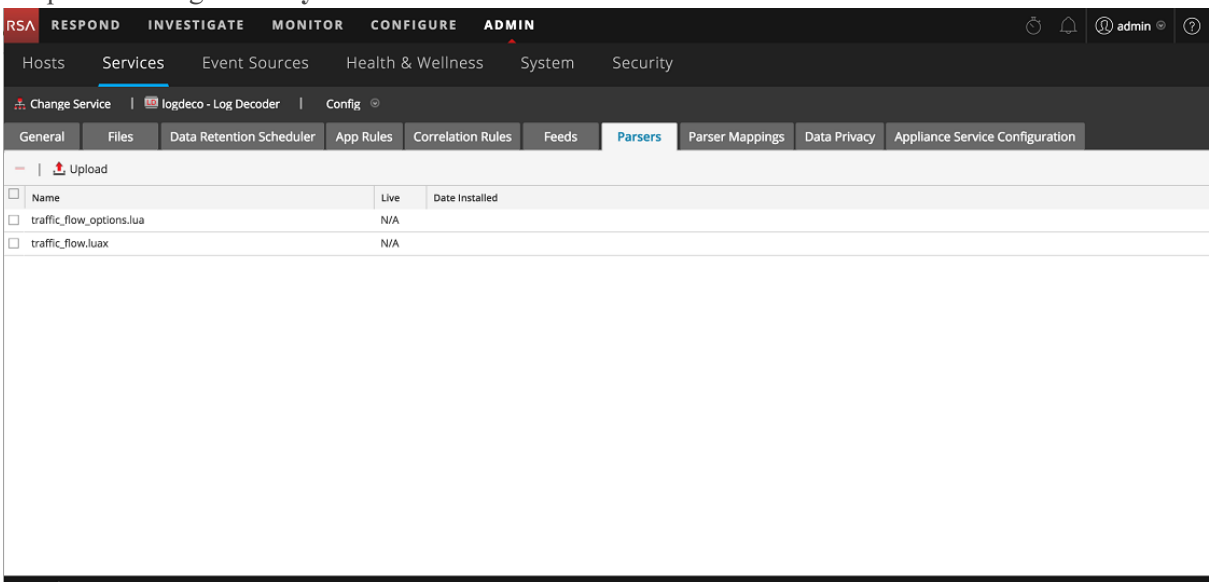
Supprimer les analyseurs déployés

L'option Supprimer de la vue Configuration des services > onglet Analyseurs permet de supprimer des analyseurs déployés à partir d'un Decoder ou Log Decoder. Les parsers peuvent être ajoutés et supprimés alors qu'un Decoder est en cours d'exécution sans que cela ait d'impact sur la capture.

Remarque : Sauf indication contraire, toutes les références aux Decoders s'appliquent également aux Log Decoders.

Pour supprimer un analyseur à partir d'un Decoder :

1. Accédez à **ADMIN > Services**, sélectionnez un service, puis > **Vue > Config.**
   La vue Configuration des services pour le service sélectionné s'affiche.
2. Cliquez sur l'onglet **Analyseurs**.



3. Sous l'onglet **Analyseurs**, sélectionnez un ou plusieurs analyseurs à supprimer.
4. Cliquez sur .
   Une boîte de dialogue demande une confirmation du fait que vous souhaitez supprimer les analyseurs.
5. Si vous voulez supprimer les analyseurs, cliquez sur **Oui**.
   Les analyseurs sont immédiatement supprimés du Decoder.

Activer et configurer du parser Entropy

À partir de la version NetWitness Platform 11.0, l'administrateur peut configurer un Decoder pour utiliser un analyseur natif NetWitness, appelé l'analyseur Entropy. Lorsque l'analyseur Entropy est activé, les analystes ont une visibilité sur les canaux qui tentent de se fondre dans le reste du trafic, mais ne suivent pas le comportement normal du protocole. Cela permet d'identifier les canaux qui ne sont pas conformes à la référence du trafic normal de l'environnement et peuvent faire l'objet d'une procédure d'enquête.

L'analyseur crée des clés méta, basées sur les statistiques collectées par l'analyseur natif NetWitness Platform, qui permettent d'identifier le comportement de tous les canaux qui génèrent beaucoup de trafic réseau. Lorsque l'analyseur est activé pour la première fois, l'analyste doit se familiariser avec le comportement global des différents canaux apparaissant dans une session capturée pour comprendre la fréquence des octets et la charge utile normale du client et du serveur. Dès lors que le comportement normal est connu, les analystes peuvent utiliser les clés méta pour trouver le comportement qui sort de la normale.

Par défaut, l'analyseur Entropy génère 10 clés méta supplémentaires qui n'ajoutent pas de charge significative au Decoder et qui sont utiles pour ce cas particulier. Par défaut, l'analyseur est désactivé.

Activez l'indexation si vous souhaitez explorer certaines sessions en fonction de l'analyse des octets de charge utile des paquets. Par défaut, pour faciliter l'indexation, la valeur `Float32` normale pour `entropy.req` et `entropy.res` est multipliée par 10 000 et stockée dans un `UInt16` (ce qui donne quatre chiffres de précision, entre 0 et 10 000).

Toutefois, si vous définissez les champs `entropy.*` dans le langage du Decoder sur `Float32`, le Decoder le stockera en tant que valeur flottante dans une plage comprise entre 0,0 et 1,0. Veillez à modifier le langage à tous les emplacements si vous décidez de conserver `Float32`.

RSA ne recommande pas l'indexation avec `Float32` en raison du nombre élevé de décomptes uniques dû aux changements de minutes dans la précision.

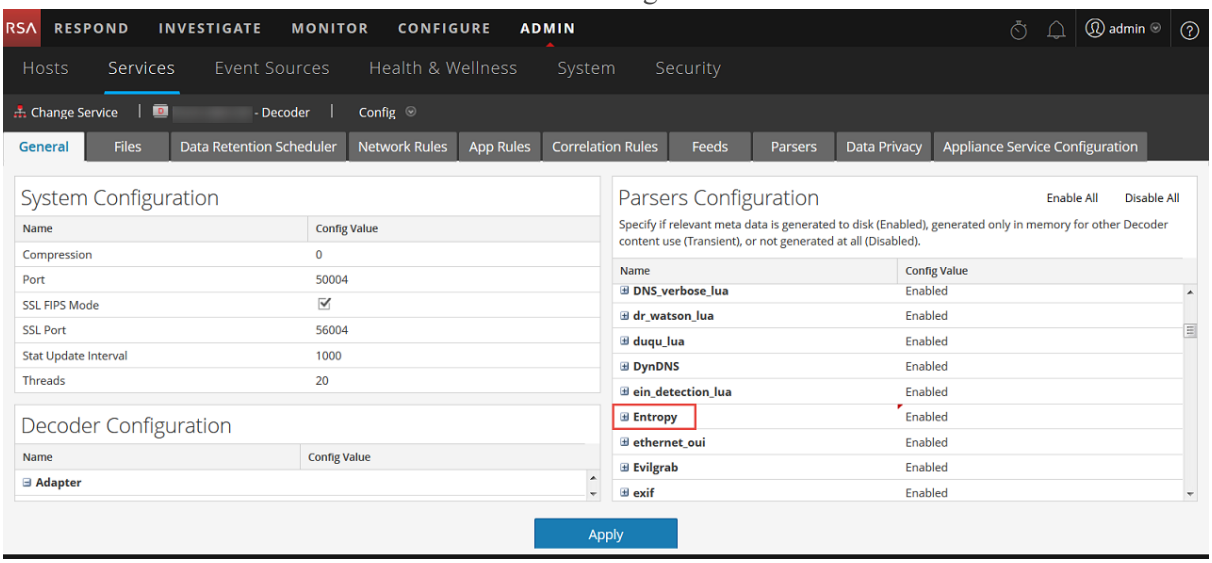
Voici les nouvelles clés méta générées par le parser Entropy par défaut :

- `entropy.req` et `entropy.res` : ces clés méta capturent Entropy à l'aide de l'équation Entropy Shannon qui présente une valeur à virgule flottante comme résultat. La valeur à virgule flottante de 0 à 1 000 est multipliée par 10 000 et écrite dans NetWitness Platform en tant que `UInt 16`, un entier non signé compris entre 0 et 10 000.
- `mcb.req` et `mcb.res` : l'octet le plus courant est simplement celui qui a été le plus rencontré pour chaque côté (entre 0 et 255).
- `mcbc.req` et `mcbc.res` : le nombre d'octets le plus courant est le nombre de fois où l'octet le plus courant (ci-dessus) a été rencontré dans les flux de session.
- `ubc.req` et `ubc.res` : - Le nombre unique d'octets est le nombre d'octets uniques rencontrés dans chaque flux. 256 signifie que toutes les valeurs d'octets entre 0 et 255 ont été rencontrées au moins une fois.

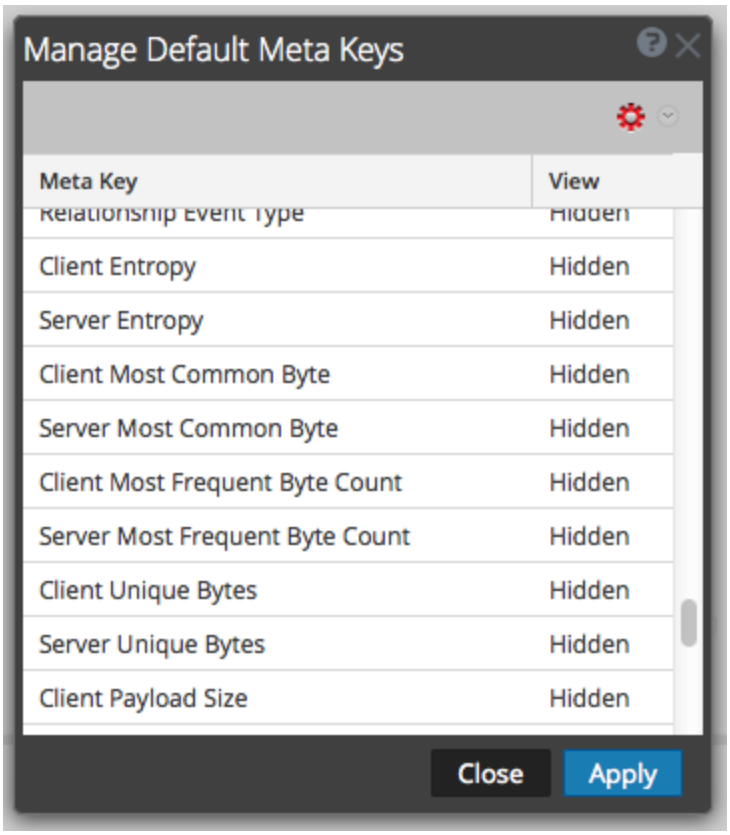
Pour activer et configurer le parser Entropy sur un Decoder :

1. Connectez-vous à RSA NetWitness et sélectionnez **ADMIN > Services** dans le menu NetWitness Platform.
2. Dans la vue Services, sélectionnez le Decoder que vous souhaitez configurer, puis  **Vue > Config**.
   La vue Configuration des services s'affiche pour le Decoder sélectionné.
3. Par défaut, l'analyseur Entropy est désactivé. Cliquez sur la liste déroulante sous **Valeur de configuration** et sélectionnez **Activé**. Si vous souhaitez désactiver certaines des clés méta, cliquez

sur la liste déroulante et sélectionnez **Désactivé** en regard de la clé méta.



4. Cliquez sur **Appliquer**.
   Le parser Entropy est activé et commence à créer les nouvelles clés méta, tel que configuré dans le fichier d'index personnalisé du Concentrator.
5. Dans la vue Configuration des services, sélectionnez le Concentrator qui agrège le trafic à partir de ce Decoder. Sélectionnez **Vue > Fichiers** et ouvrez le fichier d'index personnalisé pour le Concentrator. Recherchez les clés méta de l'analyseur Entropy pour voir si elles sont inclues et non commentées.
   Par défaut, les clés sont commentées et donc non activées. Pour activer cette partie du langage, l'administrateur doit copier cette partie du fichier d'index dans le `index-concentrator-custom.xml` et supprimer le commentaire de la ligne `key description` pour chaque clé méta. Vous trouverez ci-dessous un exemple de fichier d'index personnalisé avec les clés et instructions de l'analyseur Entropy.
6. Lorsque les clés méta Entropy sont activées, elles sont disponibles aux analystes dans Investigate mais masquées par défaut. Pour afficher les clés méta dans la vue Valeurs Investigate, modifiez les clés méta par défaut dans la boîte de dialogue Clés méta par défaut afin qu'elles soient ouvertes et non masquées. Vous pouvez gérer ces clés méta de la même manière que les autres clés méta.



Configuration de l'analyseur Entropy dans le fichier d'index personnalisé Concentrator

Voici un extrait des lignes du fichier d'index Concentrator que l'administrateur doit copier dans le fichier d'index personnalisé. Les commentaires fournissent des informations sur la configuration de l'analyseur.

```
<!-- This section is commented out because it's only used by the Entropy
parser which is disabled by default. To enable this part of the language, copy
to index-concentrator-custom.xml and uncomment the keys. HOWEVER, take note
that depending on how the Entropy parser is configured, the entropy.req and
entropy.res format might be a Float32 instead of a UInt16. So make sure to
change to the correct type if necessary.-->

<!-- Entropy parser meta - enable indexing if you have interest in exploring
this for interesting sessions based on payload byte analysis of the packets.
By default, to make indexing easier, the normal Float32 value for entropy.req
and entropy.res is multiplied by 10k and stored in a UInt16 (thus giving 4
digits of precision, 0 to 10,000). However, if you define the entropy.* fields
in the Decoder language to be Float32, it will store it as a float with a
range of 0.0 to 1.0. Take care to change the language everywhere if you decide
to keep it as a Float32. We do not recommend indexing as a Float32 because of
the high unique counts due to minute changes in precision. -->

<!--

<key description="Entropy Request (Client)" format="UInt16" level="IndexNone"
name="entropy.req" valueMax="10001"/>

<key description="Entropy Response (Server)" format="UInt16" level="IndexNone"
name="entropy.res" valueMax="10001"/>

-->
```

```
<!-- The most common byte is simply which byte for each side (0 thru 255) was
seen the most -->

<!--

<key description="Most Common Byte Request" format="UInt8" level="IndexNone"
name="mcb.req"/>

<key description="Most Common Byte Response" format="UInt8" level="IndexNone"
name="mcb.res"/>

-->

<!-- The most common byte count is the number of times the most common byte
(above) was seen in the session streams -->

<!--

<key description="Most Common Byte Count Request" format="UInt32"
level="IndexNone" name="mcbc.req" valueMax="500000"/>

<key description="Most Common Byte Count Response" format="UInt32"
level="IndexNone" name="mcbc.res" valueMax="500000"/>

-->

<!-- Unique byte count is the number of unique bytes seen in each stream. 256
would mean all byte values of 0 thru 255 were seen at least once -->

<!--

<key description="Unique Byte Count Request" format="UInt16" level="IndexNone"
name="ubc.req"/>

<key description="Unique Byte Count Response" format="UInt16"
level="IndexNone" name="ubc.res"/>

-->

<!-- The payload size metrics are the payload sizes of each session side at
the time of parsing. However, in order to keep indexing from having high
unique counts (bad for performance), the two payload size metas below are
indexed in buckets. -->

<!--

<key description="Payload Size Request" format="UInt32" level="IndexNone"
bucket="true" name="payload.req" valueMax="500000"/>

<key description="Payload Size Response" format="UInt32" level="IndexNone"
bucket="true" name="payload.res" valueMax="500000"/>

-->
```

Procédures supplémentaires de Decoder et Log Decoder

Cette rubrique explique les procédures supplémentaires qu'un administrateur peut choisir de suivre, et qui ne sont pas indispensables à la configuration du Decoder ou Log Decoder.

Rubriques

Configurer la fonction 10G

Destinée aux administrateurs, cette rubrique explique comment configurer un Network Decoder spécifiquement pour capturer des paquets à vitesse élevée à l'aide de NetWitness Platform 11.x. Elle traite de la capture de paquets sur une carte d'interface 10G. La capture de paquets à vitesse élevée nécessite une configuration minutieuse et pousse le matériel du Decoder jusqu'à ses dernières limites. Aussi, lisez attentivement cette rubrique lorsque vous mettez en œuvre une solution de capture 10G.

RSA NetWitness Platform permet d'effectuer une collecte à grande vitesse sur le Decoder. Vous pouvez capturer des données de paquets réseau issues de réseaux de vitesse supérieure et optimiser votre Network Decoder pour capturer le trafic réseau pouvant atteindre 8 Gbits/s en débit soutenu et 10 Gbits/s lors d'un pic de charge, en fonction des parsers et des flux que vous avez activés.

Voici les améliorations apportées pour faciliter la fonctionnalité de capture dans ces environnements :

- Utilisation de la fonctionnalité du pilote de capture `pf_ring` afin d'exploiter les atouts de la carte réseau 10G Intel pour obtenir des captures à grande vitesse.
- Introduction de la configuration `assembler.parse.valve`, qui désactive automatiquement les analyseurs d'application lorsque certains seuils sont dépassés, afin de limiter les risques de perte de paquets. Lorsque les analyseurs d'application sont désactivés, les analyseurs de la couche réseau restent actifs. Lorsque les statistiques chutent sous les seuils dépassés, les analyseurs d'application sont automatiquement réactivés.

Matériel requis

- Decoder de la gamme 4S ou 5
- Carte Ethernet basée sur Intel 82599, comme Intel x520. Toutes les cartes RSA 10G fournies répondent à ces exigences. Voici deux exemples :
  - Toutes les cartes SMC-10GE fournies par RSA.
  - Une carte réseau fille de Dell utilisant un contrôleur Intel pour fournir des interfaces réseau 10G. Elle est incluse dans tout le matériel de la gamme 5.
- Pour la gamme 4S / Dell R620 uniquement : 96 Go de mémoire DD3-1600 sous forme de modules DIMM à **double rangée**. Les modules DIMM à simple rangée peuvent réduire les performances à hauteur de 10 %. Pour déterminer la vitesse et le nombre de rangées des modules DIMM installés, exécutez cette commande :
  `dmidecode -t 17.`
- Espace de stockage suffisamment volumineux et rapide pour répondre aux besoins de capture. Les considérations relatives au stockage sont abordées plus loin dans cette rubrique.
- Chaque Network Decoder doit être configuré avec un minimum de 2 DAC ou une connectivité SAN.

Logiciels requis

- Les systèmes Dell R620 tels que la gamme 4S doivent subir une mise à jour de leur BIOS vers la version 1.2.6 ou supérieure.
- La fonction 10G Decoder est uniquement prise en charge sur les images d'installation du Decoder fournies par RSA. Tout logiciel requis est installé par défaut.
- Si vous procédez à la mise à niveau depuis une version précédente, effectuez d'abord la mise à niveau avant de procéder à la configuration.

Installer le 10G Decoder

Remarque : vous pouvez ignorer l'étape « Configurer le 10G Decoder » si vous démarrez avec le nouveau matériel de la gamme 5.

Pour installer NetWitness 10G Decoder, procédez comme suit :

Téléchargez et mettez à jour le BIOS

Remarque : les révisions du BIOS antérieures à la version 1.2.6 peinent à identifier correctement l'emplacement de la carte de capture 10G au sein du système. Il est recommandé que les clients effectuent une mise à jour vers le tout-dernier BIOS v2.2.3, mais il n'est pas nécessaire pour 10G s'ils exécutent la version 1.2.6 ou ultérieure.

1. Téléchargez le BIOS v2.2.3 depuis le lien suivant :

   http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04
2. Téléchargez le package de mise à jour du fichier Red Hat Linux.
3. Copiez le fichier sur le serveur NetWitness.
4. Connectez-vous en tant que `root`.
5. Modifiez les autorisations dans le fichier à exécuter.
6. Exécutez le fichier suivant :

   ```
   ./BIOS_V7P04_LN_2.2.3.BIN
   ```
7. Redémarrez le système lorsque l'exécution est terminée et qu'un redémarrage est demandé.

Remarque : la procédure d'installation du BIOS dure environ 10 minutes.

Localiser les packages 10G Decoder

Les packages requis pour configurer le 10G Decoder doivent déjà être présents sur l'image d'installation du Decoder. Vous ne devriez pas avoir besoin d'installer des packages supplémentaires.

Vérifier l'installation des packages 10G Decoder

L'installation des packages 10G Decoder est gérée automatiquement. Par conséquent, aucune action n'est nécessaire pour activer la fonctionnalité 10G.

- Si vous avez mis à niveau les packages de noyau dans le cadre d'une mise à niveau, un redémarrage est nécessaire. Le système d'exploitation recompile et installe les pilotes pour le noyau mis à niveau.
- Vous pouvez vérifier que l'installation a réussi si vous voyez des interfaces `PFRINGZC` supplémentaires lorsque vous sélectionnez l'adaptateur de port de capture décrit ci-dessous.

Configurer le 10G Decoder

Procédez comme suit pour configurer le 10G Decoder :

1. Dans la vue **Explorateur de Decoder**, cliquez avec le bouton droit de la souris sur **Decoder** et sélectionnez **Propriétés**.
2. Dans le menu déroulant des propriétés, sélectionnez **reconfig** et saisissez les paramètres suivants : `update=1 op=10g`
   Ces paramètres ajustent le pipeline de traitement du paquet Decoder pour permettre une vitesse de transfert de données brutes supérieure, mais une capacité d'analyse moindre.
3. Dans la vue **Explorateur de Decoder**, cliquez avec le bouton droit de la souris sur **base de données** et sélectionnez **Propriétés**.
4. Dans le menu déroulant **Propriétés**, sélectionnez **reconfig** et saisissez les paramètres suivants : **`update=1 op=10g`**
   Ces paramètres ajustent la base de données de paquets pour utiliser les tailles des fichiers très volumineux et les E/S directes.
5. Sélectionnez l'adaptateur de port de capture. Les options sont les suivantes (dans les exemples suivants, « p1p1 » et « p1p2 » sont des espaces réservés et doivent être remplacés par vos propres noms d'interface) :
   - Port de capture unique - **PFRINGZC,p1p1** ou **PFRINGZC,p1p2**
   - Capture des deux ports - Sélectionnez **PFRINGZC,P1P1** et dans la vue **Explorateur**, définissez `capture.device.params = device=zc:p1p2,zc:p1p1`
6. Si le thread d'écriture rencontre des difficultés à maintenir la vitesse de capture, vous pouvez procéder comme suit :

   Remplacez `/datebase/config/packet.integrity.flush` par `normal`.

   Remarque : vous pouvez ajuster `packet.file.size` en lui attribuant une valeur plus élevée, mais inférieure à 10 Go, car le fichier entier est mis en mémoire tampon.
7. (Facultatif) L'analyse d'application sollicite de manière très intensive le CPU et peut entraîner le Decoder à supprimer des paquets. Pour limiter les suppressions causées par l'analyse d'application, définissez `/decoder/config/assembler.parse.valve` sur `true`. Cela génère les résultats ci-dessous :
   - Lorsque l'analyse de sessions provoque un goulot d'étranglement, les analyseurs d'applications (HTTP, SMTP, FTP, etc.) sont temporairement désactivés.
   - Les sessions ne sont pas supprimées lorsque les analyseurs d'applications sont désactivés ; mais la fidélité de l'analyse réalisée sur ces sessions peut être remise en cause.

- Les sessions analysées lorsque les analyseurs d'application sont désactivés ont toujours un méta-réseau associé (depuis l'analyseur de réseau).
- La statistique `/decoder/parsers/stats/blowoff.count` affiche le nombre total de sessions ayant contourné les analyseurs d'applications (l'analyse de réseau est toujours effectuée).
- Lorsque l'analyse des sessions n'est plus à l'état de goulot d'étranglement, les analyseurs d'applications sont automatiquement réactivés.
- Le pool de sessions de l'assembleur doit être suffisamment large pour ne pas contraindre les sessions.
- Vous pouvez déterminer si des sessions sont forcées par la statistique `/decoder/stats/assembler.sessions.forced` (elle augmentera). En outre, `/decoder/stats/assembler.sessions` se trouvera parmi plusieurs centaines de `/decoder/config/assembler.session.pool`.

8. (Facultatif) Si vous avez besoin d'ajuster la taille de MTU pour la capture, ajoutez le paramètre `snaplen` à `capture.device.params`. Contrairement aux versions précédentes, `snaplen` ne doit pas être arrondi à une limite spécifique. Le Decoder ajuste automatiquement l'ensemble MTU sur les interfaces de capture.
9. Les paramètres de configuration suivants sont obsolètes et ne sont plus nécessaires :
   - `core= parameter` dans `capture.device.params`
   - Tous les fichiers de configuration sous le répertoire `/etc/pf_ring`

   Remarque : un périphérique Ethernet installé après la création d'images ne nécessite pas de configuration pour une utilisation en tant que périphérique de capture. Il ne requiert pas de configuration s'il est utilisé comme interface réseau ou pour que les outils système y accèdent sans configuration manuelle.

Paramètres de configuration par défaut

Les paramètres de configuration par défaut sont répertoriés ci-dessous. Les paramètres réels peuvent varier selon la quantité de mémoire et les ressources de CPU disponibles.

1. Paramètres de pool des paquets et sessions (sous `/decoder/config`) :
   - `pool.packet.pages` = `1000000`
   - `pool.session.pages` = `300000`
2. Taille de blocs d'écriture des paquets sous (`/database/config/packet.write.block` taille) définie sur `filesize`.

   Remarque : cela permet de configurer le Decoder pour mettre en mémoire tampon les fichiers volumineux et y accéder en écriture à l'aide des E/S directes pour des performances maximales.
3. Nombre de threads de l'analyse (sous `/decoder/config`).

   `parse.threads =12`

Considérations relatives au stockage

Lors d'opérations de capture à un débit de 10G, le système de stockage qui héberge les bases de données de paquets et de méta doit être en mesure de supporter un débit d'écriture de 1 400 Mo/s.

Utilisation du matériel de la gamme 4S (avec deux ou plusieurs unités DAC)

Le matériel de la série 4S est équipé d'un contrôleur SAS RAID autorisant un débit d'E/S agrégé de 48 Gbits/s. Il est doté de 8 ports externes de 6 Gbits, organisés en 2 câbles SAS à 4 voies. La configuration recommandée pour 10G consiste à répartir au moins deux unités DAC sur ces deux connecteurs externes. Par exemple, connectez un DAC à un port de la carte SAS, puis un autre DAC à l'autre port de la carte SAS.

Pour les environnements comportant plus de deux DAC, ne les reliez pas à chaque port de manière équilibrée. Un recâblage des DAC dans un déploiement existant peut être nécessaire, mais sans avoir d'incidence sur les données qui ont déjà été capturées sur le Decoder.

Si vous souhaitez renforcer la capacité de stockage, utilisez le script actuellement disponible `NwMakeArray` pour provisionner les unités DAC. Le script ajoute automatiquement un DAC par exécution (c'est-à-dire que si vous ajoutez trois DAC, le script doit être exécuté trois fois), en ajoutant les DAC à la configuration de `NwDecoder10G` comme points de montage distincts. Les points de montage indépendants sont importants, car ils permettent à `NwDecoder10G` de distinguer les E/S en écriture de la capture des E/S en lecture requises pour répondre aux demandes de contenu de paquet.

Utilisation de SAN et d'autres configurations de stockage

Le Decoder accepte toutes les configurations de stockage pouvant satisfaire les besoins en débit soutenu. La liaison FC de 8 Gbits standard vers un réseau SAN ne suffit pas pour stocker des données de paquets à 10G. Pour utiliser un réseau SAN, il faut parfois réaliser une agrégation sur plusieurs cibles à l'aide d'un schéma RAID logiciel. Par conséquent, les environnements utilisant un SAN doivent configurer la connectivité vers le SAN à l'aide de plusieurs FC.

Considérations relatives à l'analyse et au contenu

L'analyse de paquets bruts à vitesses élevées présente des défis spécifiques. Étant donné les débits élevés de sessions et de paquets, l'efficacité de l'analyse est fondamentale. Si la productivité d'un seul analyseur n'est pas satisfaisante (examen trop long des paquets), le système entier peut être ralenti au point que des paquets soient supprimés au niveau de la carte.

Pour réaliser un test initial à 10G, lancez uniquement les analyseurs natifs (excepté SMB/WebMail). Utilisez les analyseurs natifs pour établir les performances de base, avec un nombre limité ou nul de paquets supprimés. Ne téléchargez pas de contenu Live avant cette opération. Il convient de vérifier que le système ne rencontre pas de problèmes au cours de la capture à vitesses élevées.

Dès que le système est opérationnel et fonctionne parfaitement, vous pouvez ajouter peu à peu du contenu Live, notamment des analyseurs.

Bonnes pratiques

Si vous mettez à jour un système actuellement déployé ou déployez un nouveau système, il est recommandé d'utiliser les bonnes pratiques suivantes afin de minimiser les risques de perte de paquets. Une réserve est émise dans le cas de la mise à jour d'un déploiement 10G sans ajouter de trafic supplémentaire. Par exemple, un Decoder actuel capturant une carte 10G avec un débit soutenu de 2G ne doit voir aucune différence de performances, excepté si la mise à jour comprend l'ajout d'un trafic supplémentaire pour la capture.

- Intégrer les analyseurs de base (excepté SMB/Webmail, qui ont généralement une utilisation CPU élevée) et surveiller les pertes de paquets potentielles.
- Si vous ajoutez d'autres analyseurs, ajoutez-en un ou deux à la fois.
- Mesurer l'impact sur les performances du contenu nouvellement ajouté, particulièrement durant les pics de trafic.
- Si des suppressions surviennent alors qu'il n'y en avait pas auparavant, désactivez tous les analyseurs nouvellement ajoutés et activez un seul analyseur à la fois pour mesurer son impact. Cela permet d'identifier individuellement les analyseurs à l'origine des effets préjudiciables sur les performances. Pour obtenir des performances optimales, remaniez ou réduisez les fonctionnalités de chaque analyseur en fonction des besoins du client.
- Bien que leur impact sur les performances soient minimes, les flux doivent également être réexaminés et ajoutés à une approche progressive afin de mesurer l'impact sur les performances.
- Les règles d'application ont également tendance à impacter les performances dans une faible mesure ; il est donc une fois encore conseillé de ne pas ajouter un grand nombre de règles en une seule fois, sans mesurer au préalable leur impact.

Enfin, les modifications de configuration recommandées décrites dans la section Configuration permettent de réduire les problèmes potentiels.

Contenu Live testé

Les analyseurs suivants peuvent tous (mais pas individuellement) être exécutés à 10G sur le jeu de données de test :

- Contenu MA (7 analyseurs Lua, 1 flux, 1 règle d'application)
- 4 flux (alert ids info, nwmalwaredomains, warning et suspicious)
- 41 règles d'application
- DNS_verbose_lua (disable DNS)
- fingerprint_javascript_lua
- fingerprint_pdf_lua
- fingerprint_rar_lua
- fingerprint_rtf_lua
- MAIL_lua (disable MAIL)
- SNMP_lua (disable SNMP)
- spectrum_lua
- SSH_lua (disable SSH)
- TLS_lua
- windows_command_shell
- windows_executable

NON TESTÉ :

- SMB_lua, SMB natif désactivé par défaut
- html_threat

AUTRE :

- HTTP_lua réduit le taux de capture de > 9G à < 7G. À un débit tout juste inférieur à 5G, cet analyseur peut remplacer le natif sans dégrader les performances (en plus des éléments répertoriés dans la liste ci-dessus).
- Avec xor_executable, les ressources de CPU seront utilisées à 100 % lors de l'analyse, et les performances du système peuvent considérablement chuter au moment de la sauvegarde.

Ajustements de l'agrégation sur la base du contenu Live testé

Un Decoder 10G peut assurer l'agrégation sur un seul Concentrator tout en fonctionnant à des vitesses de 10G. Les déploiements utilisant Malware Analysis, Event Stream Analysis, Warehouse Connector et Reporting Engine sont susceptibles d'avoir un impact sur les performances et peuvent entraîner une perte de paquets.

Pour le scénario testé, le Concentrator agrège les données à un débit de 45 à 70 000 sessions/s. Le 10G Decoder capture des données à un débit de 40 à 50 000 sessions/s. Avec le contenu défini ci-dessus, cela représente environ 1,5 à 2 millions de métas/s. En raison du volume élevé des taux de sessions, les modifications de configuration suivantes sont recommandées :

- L'agrégation nice sur le Concentrator limite l'impact des performances sur le 10G Decoder. La commande suivante active l'agrégation nice.
  `/concentrator/config/aggregate.nice = true`
- En raison du volume élevé de sessions sur le Concentrator, vous pouvez envisager d'activer le mode Valeurs parallèles sur le Concentrator en définissant `/sdk/config/parallel.values` sur `16`. Cela améliore les performances d'Investigation lorsque le nombre de sessions par seconde dépasse 30 000.
- Si des flux d'agrégation multiples sont nécessaires, l'impact sur le Decoder est moindre lorsque l'agrégation est réalisée à partir du Concentrator.
- Une révision ultérieure du contenu et de l'analyse est requise pour les déploiements où vous souhaitez utiliser d'autres composants NetWitness Platform (par exemple, Warehouse Connector, Malware Analysis, ESA et Reporting Engine).

Optimiser les opérations de lecture/écriture lors de l'ajout d'un nouveau stockage

Un décodeur 10G est optimisé pour décaler les opérations de lecture et d'écriture sur plusieurs volumes afin que le fichier en cours de rédaction soit sur un volume différent du fichier suivant qui sera écrit. Cela permet d'obtenir un débit maximal sur le volume RAID lors de la lecture des données du dernier fichier écrit lors de l'écriture du fichier actuel sur un volume différent. Toutefois, si les volumes sont ajoutés après qu'un Decoder a été utilisé, la capacité de décaler est limitée parce qu'un ou plusieurs volumes sont déjà pleins, de sorte que le nouveau volume est le seul endroit où de nouveaux fichiers peuvent être écrits.

Pour remédier à cette situation, un administrateur peut exécuter une commande `stagger` sur une base de données NetWitness Platform existante (paquet, log, métadonnées ou session), qui possède au moins deux volumes, pour décaler les fichiers sur tous les volumes dans le modèle de lecture/écriture le plus optimal. Le principal cas d'utilisation est lorsque le nouveau stockage est ajouté à un Decoder existant et que vous souhaitez décaler les volumes AVANT de redémarrer la capture.

Les nœuds de configuration de cette commande sont les bases de données de sessions, métadonnées et paquets. Chacune d'elles se trouve sous `/database/config`, qui est généralement un nœud racine. Les nœuds de configuration d'un Decoder sont :

- `/database/config/packet.dir`
- `/database/config/meta.dir`
- `/database/config/session.dir`

Le *Guide d'optimisation de la base de données principale de NetWitness Platform* contient des informations sur la mise en forme de ces configurations.

La commande `stagger` n'est généralement utile que pour un Decoder 10G et généralement uniquement pour la base de données de paquets. Des performances maximales sont obtenues pour stocker et récupérer des paquets lorsque plusieurs volumes sont présents. Dans ce scénario, le Decoder remplit toujours le volume en conservant le plus d'espace disponible possible. Lorsque les volumes sont à peu près de la même taille, il en résulte un motif d'écriture échelonnée, qui permet un débit maximal pour la lecture et l'écriture sur tous les volumes. Toutefois, cela se produit naturellement lorsque plusieurs volumes de stockage de paquets sont présents au moment où le Decoder est déployé pour la première fois.

Un exemple d'utilisation typique consiste à ajouter plus de stockage à un Decoder existant pour augmenter la rétention. Toutefois, lors de l'ajout de stockage à un déploiement qui a déjà rempli les volumes existants avec des paquets stockés, le Decoder occupera naturellement le nouveau stockage avec des paquets avant de déployer tous les paquets sur le stockage existant. Il en résulte un modèle de lecture/écriture sous-optimal, car la plupart des lectures se produiront sur le même volume que celui en cours de rédaction. Lors d'un déploiement 10G, les lectures sont bloquées à partir du volume lorsque les écritures se produisent. Cela n'arrête pas TOUTES les lectures sur ce volume, car le fichier est mis en mémoire tampon avant d'être écrit, mais il entraîne des performances de lecture non optimales.

Avec la commande `stagger`, vous pouvez ajouter plus de stockage et obtenir ensuite du service qu'il répartisse naturellement les fichiers sur TOUS les volumes (existants et nouveaux) afin que les performances de lecture soient optimisées.

Attention : Cette commande ne doit être exécutée qu'APRÈS le montage du stockage et la configuration du Decoder effectués pour l'utiliser (par exemple, après avoir ajouté le ou les points de montage à `packet.dir`).

L'inconvénient de cette commande est qu'elle peut prendre un certain temps à répartir les données et le Decoder ne doit pas effectuer de captures pendant l'opération de répartition.

Flux de travail recommandé :

1. Ajoutez tout le stockage et configurez les points de montage.
2. Ajoutez de nouveaux points de montage du stockage à `packet.dir` (ou `session.dir`/`meta.dir`) et redémarrez le service (très important !).
3. Assurez-vous que la capture est arrêtée.

4. Exécutez l'opération de répartition, mais assurez-vous que la connexion qui a initié l'opération ne s'interrompe pas avant la fin de l'opération. Si la connexion est terminée, l'opération de répartition sera annulée. Si l'opération est annulée, les fichiers déjà répartis resteront en place. L'opération peut être reprise en exécutant de nouveau la même commande (le travail déjà fait n'aura pas besoin d'être refait). Si vous exécutez stagger à partir de nwconsole, exécutez la commande `timeout 0` avant d'envoyer la commande `stagger`. Cela empêchera que le délai de temporisation normal de 30 secondes ne s'exécute.
5. Démarrez la capture après la fin de la commande `stagger`.

Voici les paramètres de la commande :

- `type` : la base de données qui sera répartie (session, métadonnée ou paquet). En général, seule la base de données de paquets est utile pour la répartition, mais il est possible d'exécuter la session ou la base de données de métadonnées lorsque plusieurs volumes sont présents pour ces bases de données. Étant donné que la session et les bases de données de métadonnées écrivent beaucoup moins de données que la base de données de paquets, en général la répartition de ces bases de données se traduit par des gains de performances beaucoup moins perceptibles.
- `dryRun` - Si `true` (la valeur par défaut), seule une description des opérations en passe d'être exécutées sera renvoyée. Si `false`, alors les fichiers seront effectivement déplacés vers un modèle de lecture/écriture optimal. Vous DEVEZ transmettre false pour répartir réellement les fichiers.

Exemple d'utilisation de NwConsole :

```
login <decoder>:50004 <username> <password>
timeout 0
send /database stagger type=packet dryRun=false
```

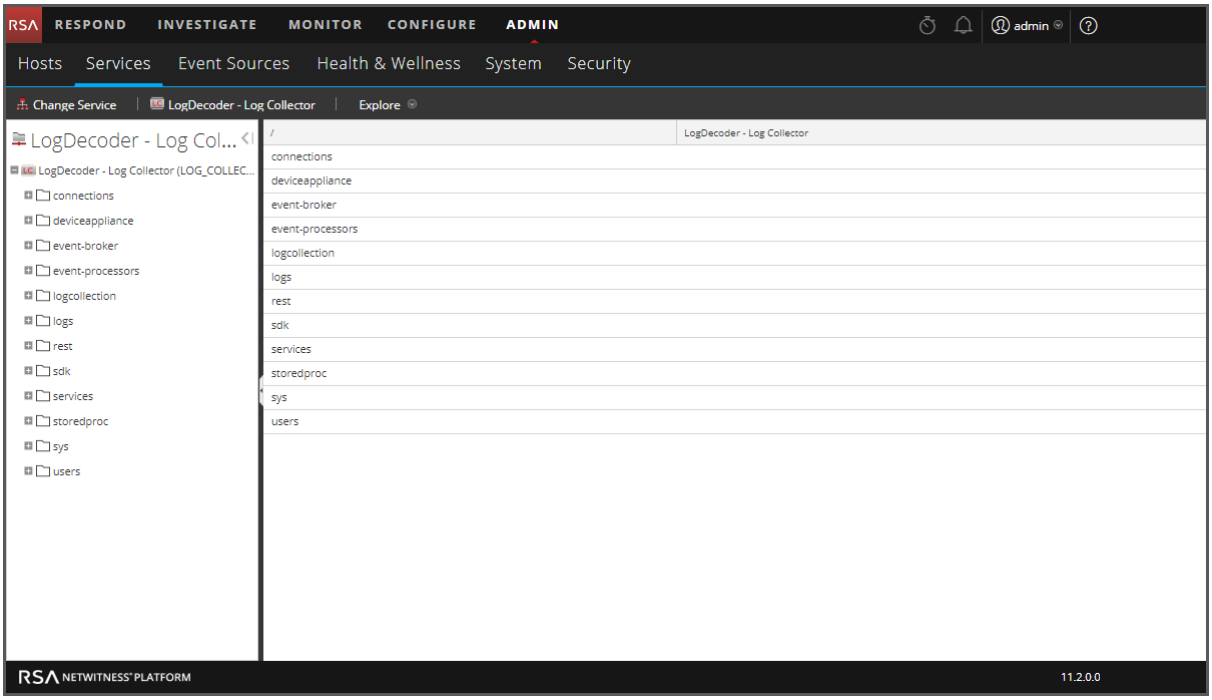
Si vous exécutez cette commande via l'API RESTful, veuillez passer le paramètre `expiry=0` supplémentaire pour empêcher un délai d'attente du service. Vous devez également vous assurer que le client HTTP ne se déconnecte pas avant la fin de l'opération.

Configurer un Log Decoder pour qu'il accepte le format protobuf

Il peut arriver que vous souhaitiez analyser des fichiers log au format protobuf (Protocol Buffer). Vous pouvez configurer un Log Decoder avec un service Log Collector pour qu'il accepte les logs au format protobuf (Protocol Buffer).

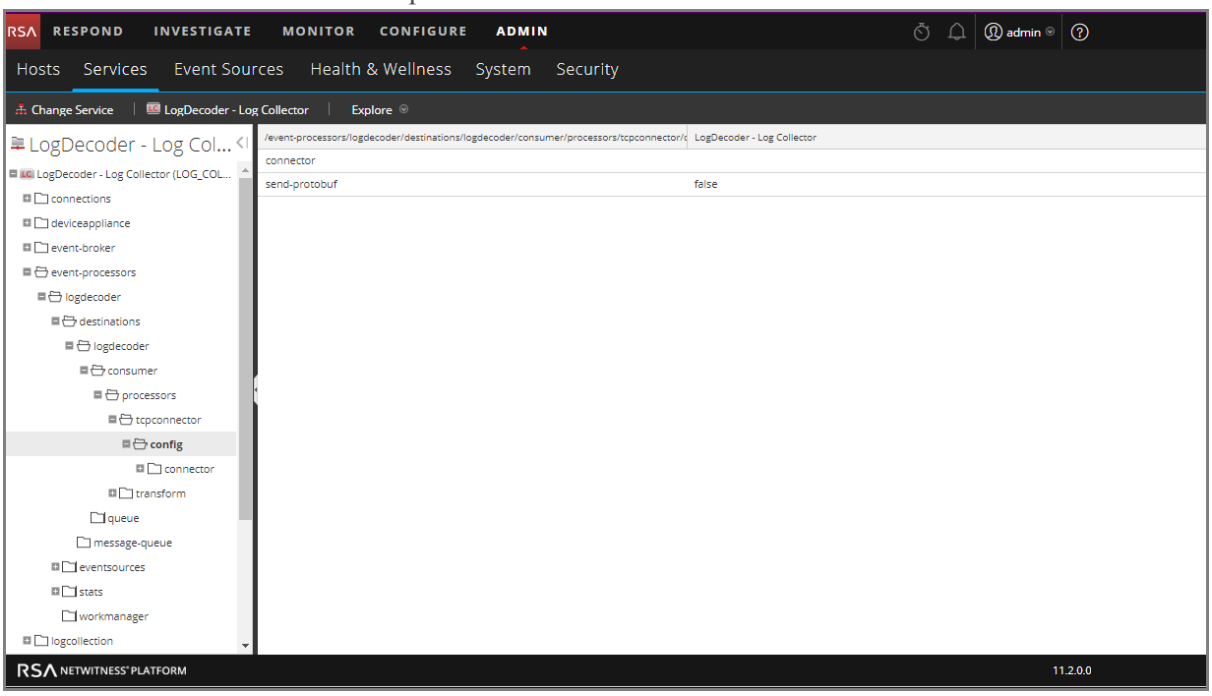
Pour importer un fichier log dans un Log Decoder :

1. Accédez à **ADMIN** > **Services**.
2. Sélectionnez un Log Decoder avec un service Log Collector dans la liste **Service**, puis sélectionnez > **Vue** > **Explorer**.
   La vue Explorer du Log Decoder - Log Collector s'affiche.



3. Accédez à **`event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config`**

Votre écran doit ressembler à ce qui suit.



4. Dans le champ **send-protobuf**, sélectionnez **false** (faux) et remplacez la valeur par **true** (vrai).
5. Accédez à `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/channel/tcp` et remplacez la valeur du **port** par **50202**.
6. Accédez à `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/event` et modifiez les paramètres suivants :
   - Effacez le champ **delimiter**
   - Remplacez **format** par **%text%**

Configurer l'expiration du délai de fractionnement des sessions

Le comportement par défaut du Decoder est de mettre fin automatiquement aux sessions qui dépassent une taille configurée ou qui ont été inactives pendant une période donnée. Lorsque la session est terminée en raison du délai d'expiration, tous les paquets suivants reçus dans cette session sont stockés dans une nouvelle session. Vous pouvez réduire l'effet du fractionnement de la session dû aux longues périodes d'inactivité entre les paquets à l'aide de cette procédure.

Lorsqu'une session Decoder dépasse une taille configurée (32 Mo par défaut, le `/decoder/config/assembler.max.size`) ou a été inactive pendant une période de temps, la session est fractionnée. NetWitness Platform contient le paquet précédent et le paquet suivant et peut propager l'état de session à partir du fragment de session initial vers le fragment de session suivant.

Chaque fragment de session est annoté (métadonnée `session.split`) de façon à ce qu'il soit identifié et associé à d'autres fragments de la session réseau en cours. La direction, telle que déterminée par la session initiale, réduit l'occurrence de fragments ayant des directions inversées.

S'il existe un écart de temps suffisamment grand entre les paquets pour qu'il n'y en ait plus dans la session en mémoire, la session est supprimée du Decoder. Si un paquet ultérieur arrive après cela, une nouvelle session est créée sans lien avec la session précédente. Le problème réside dans l'incapacité à continuer une session lorsque nous rencontrons un écart entre les paquets d'une session qui dépasse les paquets que nous avons mis en mémoire tampon (en fonction des configurations disponibles pour la mémoire et le délai d'expiration). Lorsque le dernier paquet d'une session est supprimé de la mémoire, la session est également supprimée et, avec elle, le contexte nécessaire pour garantir une direction cohérente.

Il existe deux paramètres de délai d'attente dans un Network Decoder `/decoder/config/assember.timeout.session` et `assembler.timeout.packet`. Les deux sont paramétrés par défaut sur 60 secondes. Le paramètre `assembler.timeout.session` contrôle le temps que dure une session dans Assembler sans recevoir d'autre paquet. Le paramètre `assembler.timeout.packet` contrôle combien de temps une session attend avant d'être analysée. Si la session est exclue de l'Assembler avant ce délai, elle passe automatiquement à l'analyse.

Le délai d'expiration de session représente le nombre de secondes depuis que le dernier paquet a été ajouté à cette session. Par conséquent, ce délai est réinitialisé pour chaque paquet ajouté à la session. Le délai d'expiration du paquet représente le nombre de secondes depuis que le tout premier paquet à été ajouté à cette session (c'est-à-dire, le paquet qui a créé la session). Il n'est jamais réinitialisé et, après l'expiration du délai, la session est analysée.

Point important : une session peut être analysée tout en restant dans l'Assembler. Une session dans l'Assembler peut faire l'objet d'ajout de paquets, même si elle a déjà été analysée. Les paquets ajoutés après l'analyse de la session ne sont jamais vérifiés par les analyseurs, mais ils sont rattachés à la session et peuvent être affichés par un appel `/sdk content` ou `/sdk packets` ultérieur.

Après l'analyse d'une session, la session ET ses métadonnées sont écrites sur le disque. À ce stade, elles peuvent être agrégées et « affichées » par les commandes `sdk`. Les paquets sont écrits dans l'ordre de capture et ne sont pas réorganisés par la session à laquelle ils appartiennent. Ils ne sont pas non plus nécessairement écrits lorsque la session et les métadonnées sont écrites.

Vous pouvez désactiver les deux nœuds d'expiration du délai, `/decoder/config/assembler.timeout.session` et `assembler.timeout.packet`, en les définissant sur zéro dans la Vue Explorer les services.

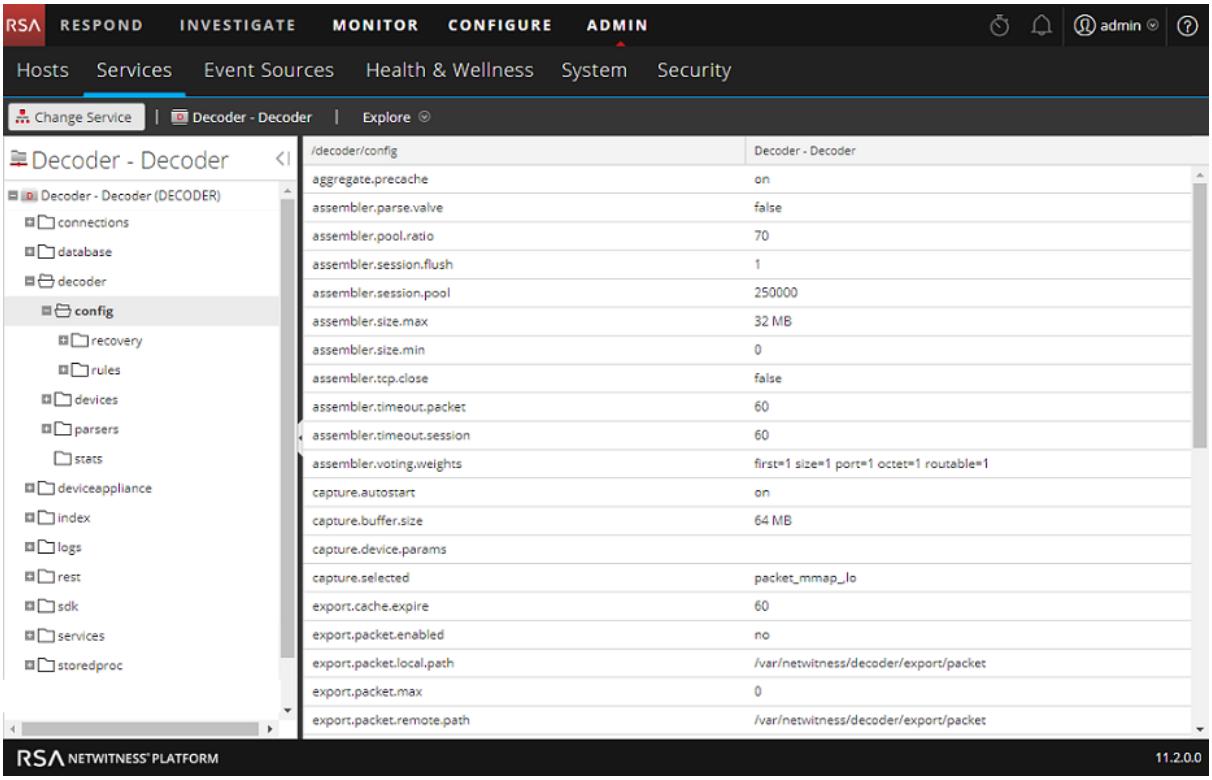
Si les deux expirations de délai sont désactivées, les sessions sont quand même fractionnées en raison de l'expiration de la taille ou du délai. Toutefois, le Decoder assure le suivi du flux réseau tant qu'il dispose de suffisamment de mémoire. Par conséquent, lorsque plus de paquets arrivent sur le même flux réseau, le Decoder ajoute des éléments méta `split` aux sessions ultérieures. À l'aide d'une combinaison de métadonnées `split` et la clé du flux, il est possible de reconstituer le flux réseau à partir de plusieurs sessions.

La durée pendant laquelle les sessions sont suivies est limitée par le nombre d'entrées de pools de sessions disponibles sur le Decoder, et par conséquent, la période réelle varie en fonction de la vitesse à laquelle de nouvelles sessions sont ajoutées. Si de nouvelles sessions sont ajoutées à un débit élevé, la durée de la période diminue. La taille du pool est définie à l'aide de l'entrée de configuration `/decoder/config/assembler.session.pool`, qui définit le nombre maximal de sessions qui peuvent être suivies à la fois.

La statistique `/decoder/stats/assembler.timespan` vous permet de savoir quand le Decoder n'effectue plus le suivi des fractionnements de sessions car le taux d'acquisition est trop élevé et le Decoder ne dispose pas de suffisamment de mémoire pour effectuer le suivi. Cette statistique indique le nombre de secondes suivies au sein du tableau des sessions. C'est en fait la période effective pendant laquelle le Decoder peut rattacher des sessions. Dans des conditions normales de fonctionnement, cette statistique correspond à la valeur de `/decoder/config/assembler.timeout.session`, mais lors de l'exécution en mode de fractionnement du temps, la statistique `/decoder/stats/assembler.timespan` augmente ou diminue en fonction du taux d'acquisition.

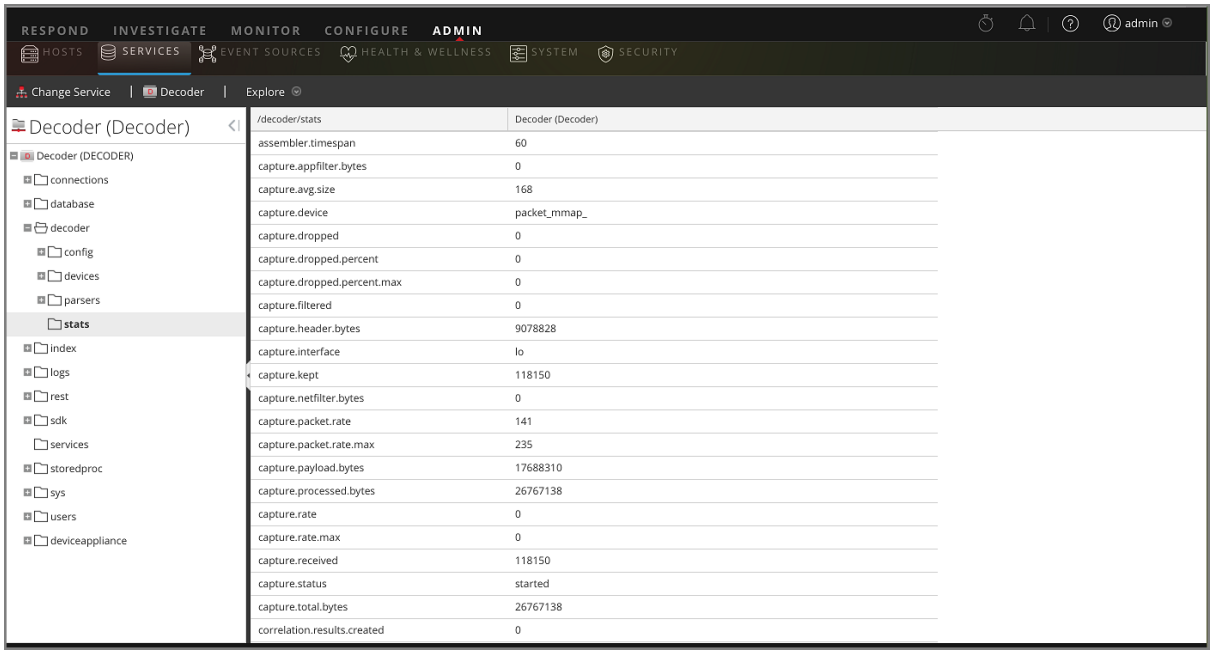
Pour configurer le mode Fractionnement du temps, définissez les paramètres de configuration suivants et redémarrez le Decoder :

1. Dans la vue Admin > Services, sélectionnez un service Decoder, puis  **> Vue > Explorer.**
2. Dans la Vue Explorer les services, sélectionnez **decoder** > **config**.



3. Cliquez dans la colonne **Valeur** en regard du paramètre et définissez ces deux paramètres :
   `/decoder/config/assembler.session.flush = 0`
   `/decoder/config/assembler.timeout.session = 0`

4. Pour savoir lorsque Decoder n'effectue plus le suivi des fractionnements de sessions car le taux d'acquisition est trop élevé et le Decoder n'a pas assez de mémoire pour effectuer le suivi, affichez la statistique `/decoder/stats/assembler.timespan`. Dans la Vue Explorer les services, sélectionnez **decoder** > **stats**.



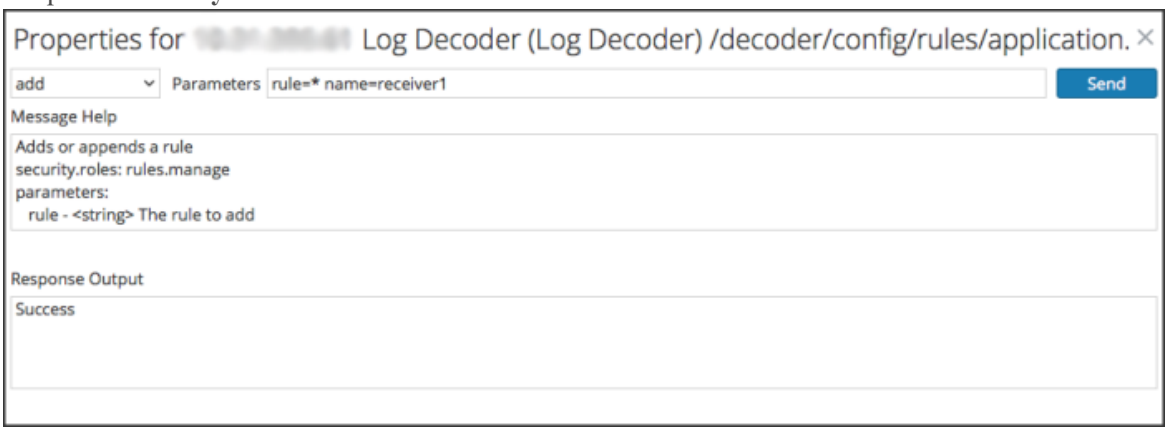
Configurer le transfert Syslog vers la destination

En plus de collecter des messages Syslog, vous pouvez configurer le Log Decoder pour transférer les messages Syslog vers un autre récepteur Syslog. NetWitness Platform transfère des messages Syslog après avoir analysé les messages et avant qu'il écrive les messages dans le Log Decoder.

Remarque : Vous devez configurer le transfert Syslog en suivant les étapes définies dans cette rubrique sous **Procédure,** à l'aide de la vue **Explorer**.

Le Log Decoder doit se trouver à l'état **Démarré** avant que vous puissiez configurer le transfert Syslog. Pour configurer le transfert Syslog :

1. Configurez les règles de couche d'application Log Decoder (règles d'application) pour signaler les messages Syslog possédant des métadonnées indiquant à NetWitness Platform de transmettre les messages :
   a. Dans la vue **Services**, sélectionnez un Log Decoder, et dans la colonne Actions, sélectionnez > **Vue** > **Explorer**.
   b. Accédez au nœud **/decoder/config/rules/application**, cliquez avec le bouton droit sur **application,** puis cliquez sur **Propriétés**.
   c. Dans la vue **Propriétés**, spécifiez la commande **add** avec les paramètres suivants :
   `rule=<query> name=<name>`
   Exemple 1 : `rule=*name=receiver1`
   Exemple 2 `rule="device.type='winevent_nic'" name=receiver`)
   d. Cliquez sur **Envoyer**.



   NetWitness Platform crée la règle `name=receiver1 rule=* order=<n>`. NetWitness Platform insère le numéro d'ordre (par exemple, `order=49`) d'après le moment où vous définissez la règle.

   e. Accédez au nœud `/decoder/config/rules/application` et cliquez sur la règle `name=receiver1 rule=* order=49`.

f. Ajoutez les paramètres **alert forward** aux paramètres de la règle.

```
rule=* name=receiver1 order=49 alert forward
```

Tous les autres paramètres de règle possèdent la même signification que dans les autres règles d'application.

L'exemple de règle Application suivant sélectionne tous les logs avec la règle `*`. Il crée une métadonnée d'alerte avec la valeur « **`receiver1`** » et marque tout le log pour le transférer à la destination de transfert de syslog. Vous pouvez définir autant de règles de transfert que vous le souhaitez avec le même nom ou avec des noms uniques.

2. Définissez les destinations de transfert Syslog et activez le transfert.

   a. Dans la vue **Services**, sélectionnez un Log Decoder et  > **Vue** > **Explorer**.

   b. Les destinations de transfert syslog sont définies dans le nœud de configuration `/decoder/config/logs.forwarding.destination`.
   Ce nœud de configuration contient une ou plusieurs paires nom/valeur. Le nom correspond au paramètre de nom dans la règle d'application que vous avez utilisé pour appliquer des balises aux logs avec les métadonnées de transfert. La valeur est un triplet séparé par une virgule contenant le transport, l'hôte et le port, suivi par un paramètre facultatif de mise en forme.
   `name=(udp|tcp|tls):host:port[:(retainsource|rfc3164)]`
   Le premier paramètre indique le protocole de transport et doit être tls, tcp ou udp. Si vous spécifiez udp, les logs seront transférés via le protocole UDP Syslog RFC 3164 / RFC 5426. Si vous spécifiez tcp, les logs seront transférés via une connexion TCP avec une gestion des trames RFC 6587. Si vous spécifiez tls, les logs seront transférés conformément à RFC 5425. L'hôte est une adresse IPv4, une adresse IPv6 ou un nom d'hôte.

   Le port est le port auquel les logs sont envoyés. Il s'agit généralement du port 514 pour UDP syslog et du port 6514 pour les connexions TLS. Il n'existe pas de port standard attribué à syslog via TCP.

   Si vous le souhaitez, `retainsource` ou `rfc3164` peuvent être spécifiés à la fin de la chaîne de destination pour indiquer d'inclure de la mise en forme et des informations supplémentaires avec chaque log transmis. Si vous spécifiez `retainsource`, des en-têtes z-connector seront intégrées au début du log et seront générées par les métadonnées `time`, `device.(ip|ipv6|host)` et `lc.cid` dont l'utilisation est idéale pour le transfert vers d'autres services log Decoder. L'option `rfc3164` ajoutera un en-tête RFC3164 valide pour tous les événements transmis, constitués des métadonnées `syslog.pri`, `time` et `device.(ip|ipv6|host)`. Dans les deux cas, le texte du log d'origine n'est pas modifié.

   Exemple de transfert de destination :

   ```
   gears=tls:gears.netwitness.local:6514
   ```

   Exemple de transfert via tcp sur blackout sur le port 514 avec en-têtes z-connector :

   ```
   fwdrule=tcp:blackout.netwitness.local:514:retainsour
   ```

   Dans le paramètre `/decoder/config/logs.forwarding.destination`, spécifiez la destination. Par exemple :
   Connexions TLS : `receiver1=tls:receiver1.netwitness.local:6514`
   Connexion UDP : `receiver1=udp:receiver1.netwitness.local:514`
   Connexions TCP : **`receiver1=tcp:receiver1.netwitness.local:514`**

logs.forwarding.destination	receiver1=tcp:10.31.244.44:514 receiver2=tcp:10.31.244.46:514 receiver3=tcp:10.31.244.48:514

Remarque :
Vous pouvez configurer :
- Plusieurs règles pour transférer des logs vers la même destination.
- Plusieurs règles pour transférer des logs vers plusieurs destinations.

Pour les connexions TLS, le certificat de la destination de transfert doit être validé. L'autorité de certification qui a signé le certificat de la destination doit être présent dans le magasin de certificats de confiance CA du Log Decoder et le certificat doit résider sur la destination ou le récepteur Syslog. Reportez-vous à la rubrique « Configurer les certificats » dans le *Guide de configuration de Log Collection* pour plus d'informations sur la manipulation du magasin de confiance CA du Log Decoder (Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.).

c. Dans le paramètre `/decoder/config/logs.forwarding.enabled`, spécifiez **true**.

logs.forwarding.enabled	true

Configurer la gestion des transactions sur un Decoder

À partir de la version 11.0, les administrateurs peuvent configurer un Decoder afin de subdiviser les sessions entrantes dans des sessions de transactions plus petites lors de l'utilisation d'analyseurs LUA conçus pour créer des transactions. Cette fonction permet aux analystes d'effectuer une analytique sur les sessions fractionnées dans les services en aval comme Investigate.

Gestion des transactions

Le nœud de configuration du service Decoder dispose d'un nouveau paramètre pour la configuration de la gestion des transactions : `/decoder/parsers/config/parser.transaction.mode`. Ce nœud contrôle le comportement du Decoder lorsqu'un analyseur définit une transaction dans une session réseau.

Les valeurs de `parser.transaction.mode` correspondent aux modes de fonctionnement :

- `off` (transactions désactivées)
- `meta` (transactions représentées sous forme de métaéléments)
- `split` (sessions fractionnées de transactions)

Transactions désactivées

Lorsque le mode Transactions est désactivé, toutes les transactions au niveau des applications créées par les analyseurs sont ignorées, et rien n'est stocké dans la collection pour représenter la transaction.

Transactions représentées sous forme de métaéléments

Dans ce mode de fonctionnement, lorsqu'un analyseur génère une transaction au niveau des applications, un nouveau métaélément de type `{{trans}}` est ajouté à la session dans laquelle la transaction s'est produite. Le métaélément `{{trans}}` contient une liste d'autres métaéléments qui constituent la transaction.

Sessions fractionnées de transactions

Dans ce mode de fonctionnement, lorsqu'un analyseur génère une transaction au niveau des applications, la session est fractionnée. Le fractionnement de la session est effectué par :

1. Un nouvel élément de session est créé.
2. Les métaéléments réseau sont copiés à partir de la session analysée dans la nouvelle session.
3. Les métaéléments de la transaction sont déplacés à partir de la session d'origine vers la nouvelle session.

Les métaéléments suivants sont dupliqués dans la session fractionnée à partir de la session qui a été analysée :

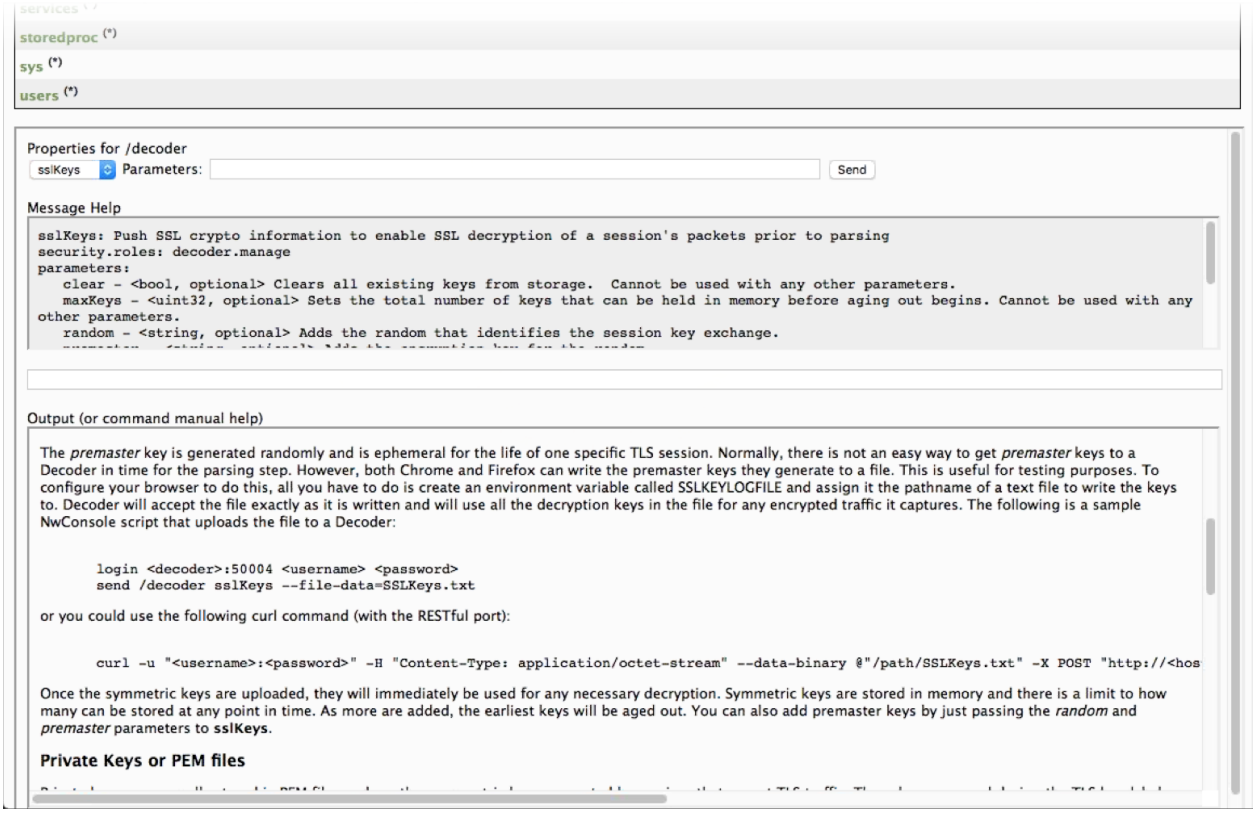
- `time`
- `medium`
- `eth.src`
- `eth.dst`
- `eth.type`
- `ip.proto`
- `ip.src`
- `ip.dst`
- `ipv6.src`
- `ipv6.dst`
- `ipv6.proto`
- `tcp.srcport`
- `tcp.dstport`
- `tcp.flags`
- `udp.srcport`
- `udp.dstport`
- `service`
- `udp.srcport`
- `udp.srcport`
- `tls.premaster`

Déchiffrer les paquets entrants

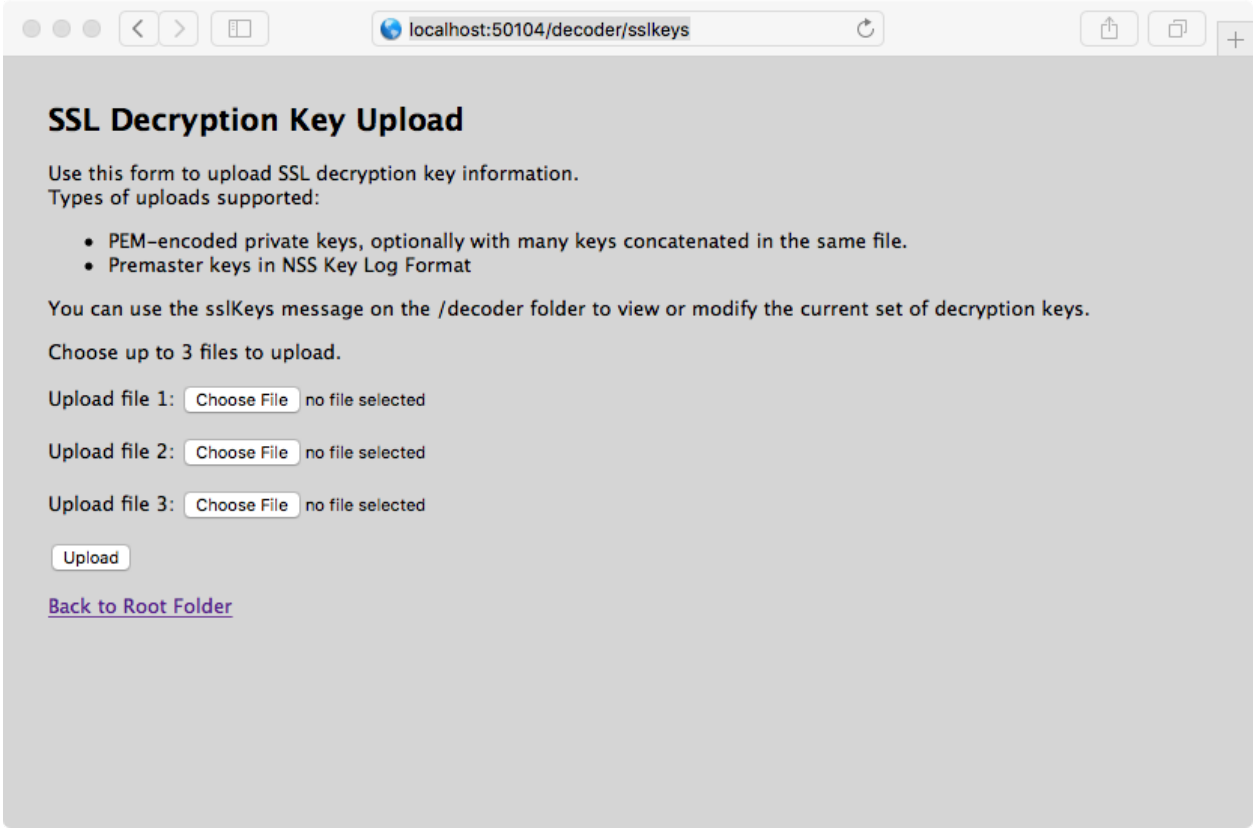
À partir de la version NetWitness Platform 11.0, les administrateurs peuvent configurer un Network Decoder pour déchiffrer les paquets entrants à l'aide de la commande `sslKeys`. Les analyseurs activés pourront voir la charge utile du paquet non chiffré et créer des métadonnées en conséquence. Si le Decoder n'est pas configuré pour déchiffrer les paquets entrants, la plupart des analyseurs activés ne verront que du garbage chiffré et ne pourront pas créer de métadonnées significatives.

Remarque : Si FIPS est activé, la liste des chiffrements permettant le déchiffrement se limite à ceux approuvés par FIPS.

La commande `sslKeys` permet de télécharger des clés premaster ou des clés privées sur le Decoder, afin que la capture des paquets chiffrés qui correspondent aux clés puissent être déchiffrés avant l'analyse. Les administrateurs peuvent configurer le Decoder en saisissant la commande `sslKeys` à l'aide de l'interface de ligne de commande NwConsole ou de l'interface RESTful Decoder.



Le formulaire de l'interface RESTful à l'emplacement : `/decoder/sslkeys` permet de télécharger une clé privée unique au format d'encodage PEM, un fichier unique contenant plusieurs clés privées concaténées, ou un fichier unique contenant plusieurs clés premaster.



Bien que les paquets soient déchiffrés durant la phase d'analyse, seuls les paquets chiffrés sont écrits sur le disque. La clé premaster correspondante, utilisée pour le déchiffrement, est écrite sur la clé méta `tls.premaster`, que les analystes peuvent ensuite utiliser à la demande pour afficher les paquets non chiffrés.

Vous trouverez ci-dessous des détails permettant aux administrateurs de configurer le déchiffrement des paquets entrants et aux analystes de visualiser les paquets non chiffrés à la demande.

Considérations relatives aux performances

Le déchiffrement des paquets en temps réel requiert un travail supplémentaire en phase d'analyse. Avant d'implémenter cette fonction, planifiez soigneusement pour vous assurer que la bande passante de trafic entrant n'excède pas la puissance de calcul disponible. Vous aurez peut-être besoin de plus de Decoders pour déchiffrer le trafic que si vous n'utilisez pas le déchiffrement.

Les paquets capturés sur un Decoder ont généralement un délai d'expiration de 60 secondes en phase d'assemblage avant d'être envoyés à l'étape d'analyse. Si le Decoder est sous pression au niveau de la mémoire en raison d'une utilisation très élevée de la bande passante, il se peut que la durée de vie des paquets dans l'assembleur soit raccourcie. Pour résoudre cette situation, vous pouvez configurer une valeur plus longue du délai d'expiration et augmenter la quantité de mémoire disponible pour conserver les paquets dans l'assemblage. En outre, pour effectuer le déchiffrement des paquets, le Decoder doit recevoir la clé de déchiffrement avant l'étape d'analyse.

Remarque : Actuellement, seuls les protocoles TLS 1.2 et les protocoles antérieurs peuvent être déchiffrés.

Lorsqu'aucun feed n'est chargé, que les analyseurs suivants sont activés et que 50 % des sessions sont déchiffrées, un Decoder peut traiter le trafic à 3 Gbit/s.

Nom de l'analyseur	Description
SYSTEM	Détails de la session
NETWORK	Couche réseau
ALERTS	Alertes
GeoIP	Données géographiques basées sur ip.src et ip.dst
GeoIP2	Données géographiques par défaut basées sur les clés META IPv4 (ip.src, ip.dst) et IPv6 (ipv6.src, ipv6.dst)
HTTP	Hyper Text Transport Protocol (HTTP)
HTTP_Lua	Hyper Text Transport Protocol (HTTP) Lua
FTP	File Transfer Protocol (FTP)
TELNET	Protocole TELNET
SMTP	Simple Mail Transport Protocol (SMTP)
POP3	Post Office Protocol (POP3)
NNTP	Network News Transport Protocol (NNTP)
DNS	Domain Name Service (DNS)
HTTPS	Protocole Secure Socket Layer (SSL)
MAIL	Format d'e-mail standard (RFC822)
VCARD	Extrait les informations de nom complet et d'e-mail de VCARD
PGP	Identifie les blocs PGP au sein du trafic réseau
SMIME	Identifie les blocs SMIME au sein du trafic réseau
SSH	Secure Shell (SSH)
TFTP	TFTP (Trivial File Transfer Protocol)
DHCP	Dynamic Host Configuration Protocol (DHCP et BOOTP)
NETBIOS	Extrait les informations de nom d'ordinateur NETBIOS.
SNMP	Simple Network Management Protocol (SNMP)
NFS	Protocole Network File System (NFS)
RIP	Routing Information Protocol (RIP).

Nom de l'analyseur	Description
TDS	Protocole de base de données MSSQL et Sybase (TDS)
TNS	Protocole de base de données Oracle (TNS)
IRC	Protocole Internet Relay Chat (IRC)
RTP	Real Time Protocol (RTP) pour l'audio et la vidéo
SIP	Session Initiation Protocol (SIP)
H323	Protocole de téléconférence H.323
SCCP	Protocole Cisco Skinny Client Control
GTalk	Google Talk (GTalk)
VlanGre	Vlan ID et adresses de tunnel GRE/EtherIP
BITTORRENT	Protocole de partage de fichiers BitTorrent
FIX	Protocole Financial Information eXchange
GNUTELLA	Protocole de partage de fichiers Gnutella
IMAP	Internet Message Access Protocol
MSRPC	Protocole Microsoft Remote Procedure Call
RDP	Remote Desktop Protocol
SHELL	Identification de Shell de commande
TLSv1	TLSv1
SearchEngines	Analyseur qui extrait des termes de recherche
FeedParser	Analyseur de feed externe

Clés de chiffrement

La commande `sslKeys` accepte deux types de clés de chiffrement :

- Clé premaster : clé symétrique utilisée dans le flux de charge utile TLS pour le chiffrement et le déchiffrement.
- Clé privée : clé privée asymétrique utilisée lors de la négociation TLS qui chiffre la clé premaster.

Clé premaster

La clé premaster est générée de manière aléatoire et éphémère pour la durée de vie d'une session TLS spécifique. En règle générale, il n'existe pas de manière idéale pour transférer les clés premaster vers un Decoder à temps pour l'étape d'analyse. Toutefois, Chrome et Firefox peuvent tous deux écrire les clés premaster qu'ils génèrent dans un fichier. Cela est utile à des fins de test. Pour configurer votre navigateur à cet effet, créez une variable d'environnement appelée SSLKEYLOGFILE et attribuez-lui le chemin d'accès du fichier dans lequel les clés seront écrites. Le Decoder accepte le fichier exactement tel qu'il a été écrit et utilise toutes les clés de déchiffrement dans le fichier pour tout le trafic chiffré qu'il capture.

Exemple de script NwConsole qui télécharge le fichier sur un Decoder :

```
login <decoder>:50004 <username> <password>
send /decoder sslKeys --file-data=SSLKeys.txt
```

Exemple d'utilisation d'une commande curl (avec le port RESTful) pour télécharger le fichier vers un Decoder :

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --
data-binary @"/path/SSLKeys.txt" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys"
```

Lorsque les clés symétriques sont téléchargées, elles sont immédiatement utilisées pour n'importe quel déchiffrement nécessaire. Les clés symétriques sont stockées dans la mémoire et il existe une limite quant au nombre de clés pouvant être stockées à un moment donné. Lorsque de nouvelles clés sont stockées, les plus anciennes expirent. Vous pouvez également ajouter des clés premaster en transmettant uniquement les paramètres `random` et `premaster` vers `sslKeys`.

Clés privées ou fichiers PEM

Les clés privées sont généralement stockées dans des fichiers au format PEM et sont les clés asymétriques générées par les services qui acceptent le trafic TLS. Ces clés sont utilisées lors de la négociation TLS pour chiffrer la clé symétrique premaster qui sera utilisée pour le reste du chiffrement de la charge utile.

Par exemple, si vous disposez d'un serveur Web sur lequel vous souhaitez une visibilité, vous devez télécharger la clé privée qu'il utilise pour chiffrer le trafic. Il vous suffit d'effectuer cette procédure une seule fois car elle est stockée de manière permanente (ou jusqu'à ce qu'elle soit supprimée par la commande de suppression). Les clés privées sont automatiquement chiffrés avant leur stockage afin de les protéger. Après le téléchargement, vous devez émettre une commande destinée à recharger l'analyseur afin que la clé nouvellement installée devienne visible pour l'analyseur HTTPS. Ainsi, toutes les négociations TLS qui utilisent cette clé privée pourront être déchiffrées par le Decoder.

Remarque : Toutes les suites de chiffrement n'utilisent pas de clé privée « connue » (par exemple, Diffie Hellman éphémère). Le trafic ainsi chiffré ne peut pas être déchiffré à moins qu'une clé premaster soit téléchargée sur le Decoder avant l'analyse de la session.

Voici quelques exemples de commandes qui téléchargent un fichier PEM à utiliser pour le déchiffrement.

À l'aide de NwConsole :

```
send /decoder sslKeys pemFilename=MyKey.pem --file-data=/path/MyKey.pem
```

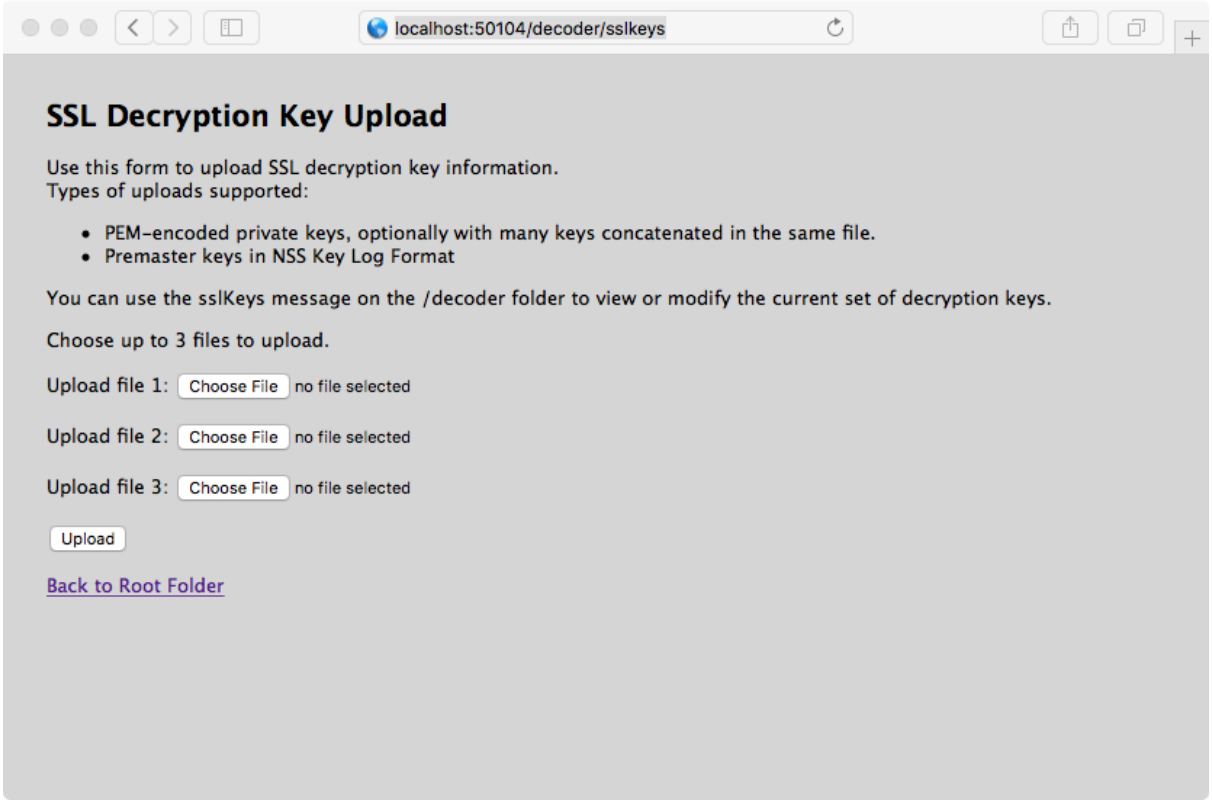
À l'aide de l'interface RESTful (vous devez fournir le paramètre `pemFilename` dans l'URL) :

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --
data-binary @"/path/MyKey.pem" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys&pemFilename=MyKey.pem"
```

Télécharger plusieurs clés premaster et clés privées

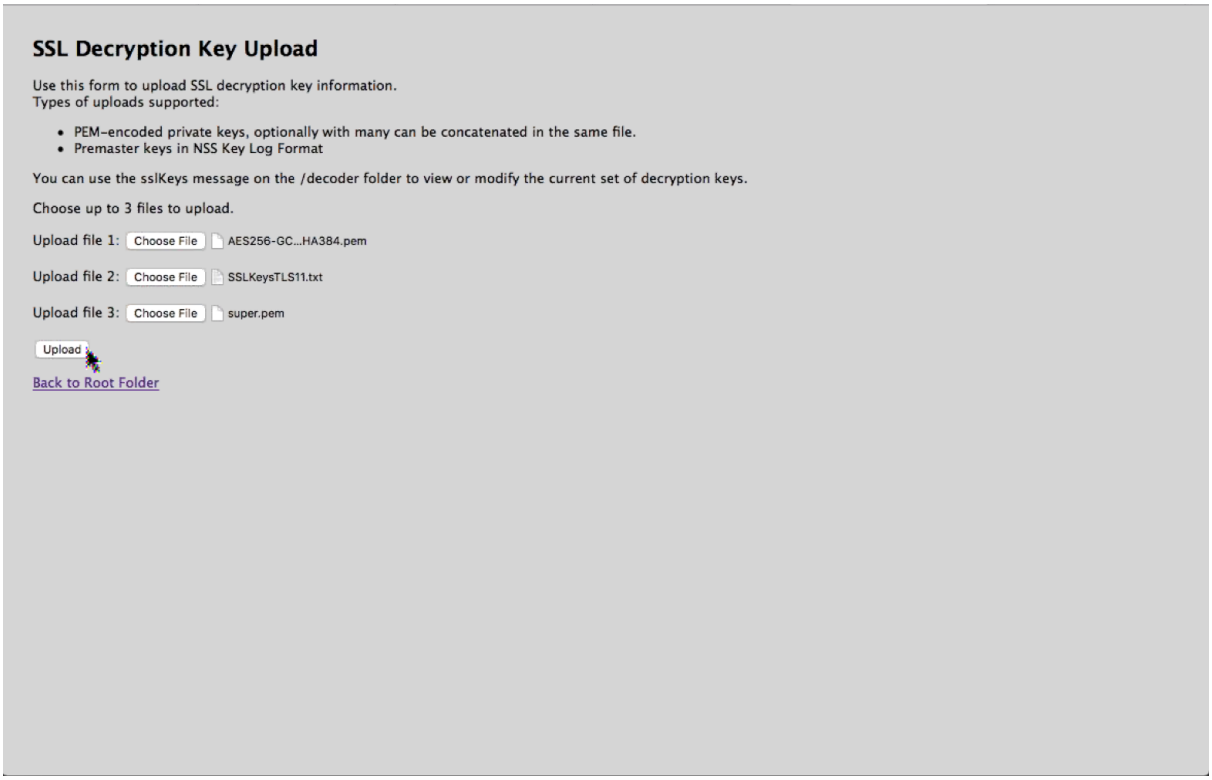
Vous pouvez utiliser le formulaire de l'interface RESTful pour faciliter le chargement de plusieurs clés (premaster et privées) en même temps.

1. Ouvrez l'API RESTful dans votre navigateur et accédez à ce chemin d'accès sur le Decoder que vous souhaitez configurer : `/decoder/sslkeys`.

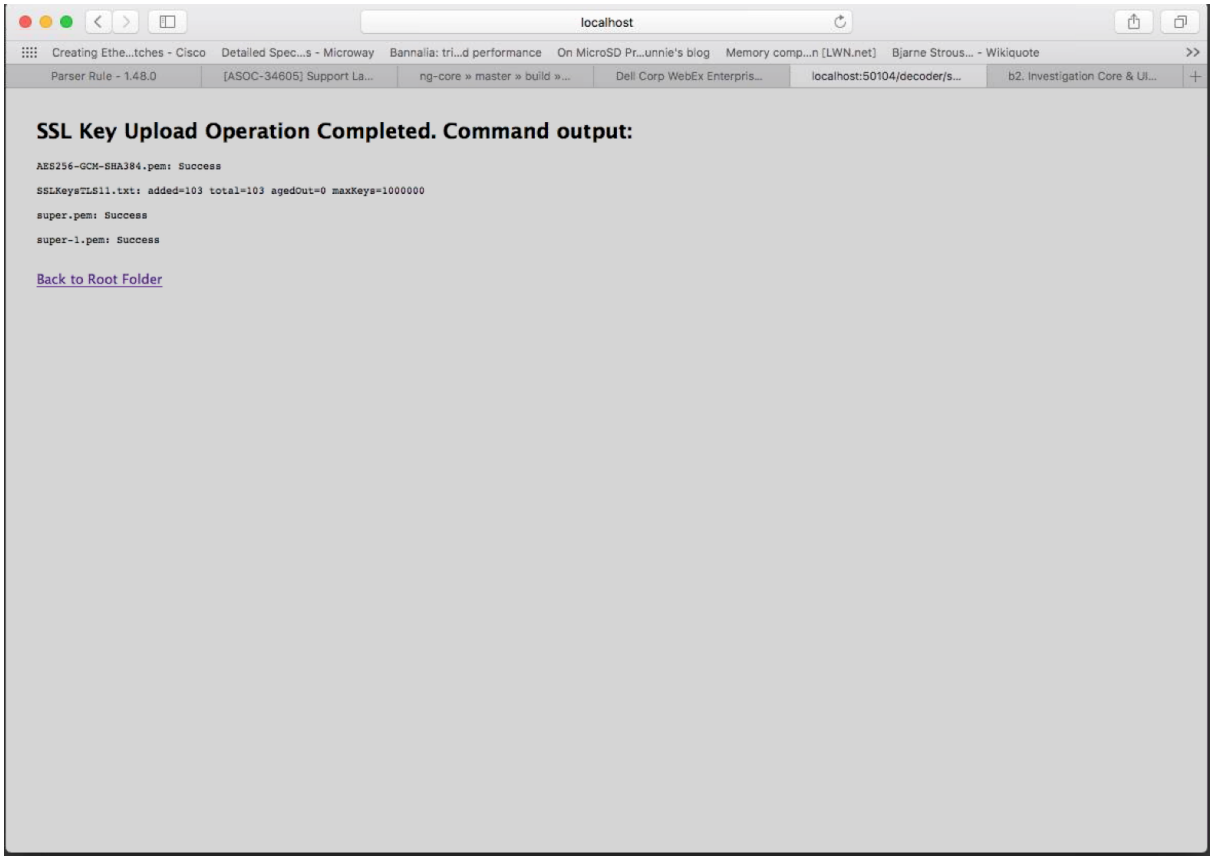


2. En regard de **Télécharger le fichier 1**, cliquez sur **Choisir le fichier** et recherchez le fichier de clé premaster ou le fichier PEM que vous souhaitez télécharger sur votre système de fichiers local.

3. (Facultatif) Répétez cette étape pour **Télécharger le fichier 2** et **Télécharger le fichier 3**.



4. Cliquez sur **Télécharger**.
   Les fichiers sont téléchargés vers Decoder et les résultats s'affichent dans le formulaire.



Paramètres pour la gestion des clés

La commande `sslKeys` dispose de plusieurs paramètres pour gérer les clés premaster et privées. Voici la liste complète des paramètres :

Paramètre	Description
`clear`	Supprime toutes les clés premaster de la mémoire. Ne supprime aucun fichier PEM installé sur le système.
`maxKeys`	Modifie le nombre maximal de clés premaster qui sont stockées dans la mémoire.
`listPems`	Renvoie une liste de tous les fichiers PEM de clés privées installées.
`deletePem`	Supprime le fichier PEM nommé à partir du système de fichiers. Vous pouvez passer ce paramètre plusieurs fois pour supprimer plusieurs fichiers.
`random`	Valeur de hachage aléatoire permettant d'identifier la clé premaster.

Paramètre	Description
premaster	Clé premaster qui est installée pour le paramètre random précédent. Ils doivent s'afficher par paires et random doit être le premier.

Valeurs renvoyées

La plupart des commandes sslKeys renvoient des paires nom/valeur de statistiques sur les clés premaster en mémoire. Les statistiques sont répertoriées dans le tableau suivant.

Nom	Description
added	Nombre de clés premaster qui viennent d'être ajoutées pendant cette commande.
total	Nombre total de clés premaster chargées en mémoire.
agedOut	Nombre total de clés premaster qui ont été supprimées pendant cette commande ; il ne s'agit pas d'une statistique de durée de vie.
maxKeys	Nombre maximal actuel de clés premaster autorisées

Affichage du trafic non chiffré

Si des paquets sont déchiffrés durant la phase d'analyse, des paquets chiffrés sont écrits sur le disque et la clé premaster correspondante, utilisée pour le déchiffrement, est écrite sur la clé méta tls.premaster. Les analystes peuvent afficher les paquets non chiffrés à l'aide de la clé méta tls.premaster.

Le service /sdk/content RESTful est une API de Decoder que vous pouvez utiliser pour voir les paquets déchiffrés. Vous devez connaître l'identifiant de session des paquets chiffrés et le paramètre flags masqué pour la valeur 128 (ou 0 x 80 au format hexadécimal). Avec votre navigateur, accédez à l'interface RESTful du Decoder et saisissez la commande suivante, en remplaçant l'identifiant de session réel pour <id> :

http://<decoder>:50104/sdk/content?session=<id>&flags=128&render=text

Le Decoder renvoie à une simple page Web affichant les paquets une fois qu'ils sont déchiffrés.

Si vous souhaitez voir à quoi ressemblent les paquets chiffrés, saisissez l'une des commandes suivantes, en remplaçant l'identifiant de session pour <id> :

http://<decoder>:50104/sdk/content&session=<id>&render=text

http://<decoder>:50104/sdk/content&session=<id>&flags&render=text

Pour plus d'informations sur le service /sdk/content, reportez-vous à la page du manuel relative au contenu /sdk/.

Suites de chiffrement prises en charge

Le tableau suivant répertorie les suites de chiffrement prises en charge à l'aide de clés privées.

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	[0xc030]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	[0xc02c]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	[0xc028]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	[0xc024]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	[0xc014]	SSLv3	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	[0xc00a]	SSLv3	Kx=ECDH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384	[0xa3]	TLSv1.2	Kx=DH	Conforme	Non pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	[0x9f]	TLSv1.2	Kx=DH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	[0x6b]	TLSv1.2	Kx=DH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256	[0x6a]	TLSv1.2	Kx=DH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	[0x39]	SSLv3	Kx=DH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA	[0x38]	SSLv3	Kx=DH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	[0x88]	SSLv3	Kx=DH	Non conforme	Non pris en charge
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE-DSS-CAMELLIA256-SHA	[0x87]	SSLv3	Kx=DH	Non conforme	Non pris en charge
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384	[0xc032]	SSLv3	Kx=ECDH/RSA	Conforme	Non pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384	[0xc02e]	TLSv1.2	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	ECDH-RSA-AES256-SHA384	[0xc02a]	TLSv1.2	Kx=ECDH/RSA	Conforme	Non pris en charge
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	ECDH-ECDSA-AES256-SHA384	[0xc026]	TLSv1.2	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	[0xc00f]	SSLv3	Kx=ECDH/RSA	Conforme	Non pris en charge
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	[0xc005]	SSLv3	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	[0x9d]	TLSv1.2	Kx=RSA	Conforme	Pris en charge
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	[0x3d]	TLSv1.2	Kx=RSA	Conforme	Pris en charge
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	[0x35]	SSLv3	Kx=RSA	Conforme	Pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	[0x84]	SSLv3	Kx=RSA	Non conforme	Pris en charge
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	[0xc012]	SSLv3	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	[0xc008]	SSLv3	Kx=ECDH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	[0x16]	SSLv3	Kx=DH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA	[0x13]	SSLv3	Kx=DH	Conforme	Non pris en charge
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	ECDH-RSA-DES-CBC3-SHA	[0xc00d]	SSLv3	Kx=ECDH/RSA	Conforme	Non pris en charge
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH-ECDSA-DES-CBC3-SHA	[0xc003]	SSLv3	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	[0x0a]	SSLv3	Kx=RSA	Conforme	Pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	[0xc02f]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	[0xc02b]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	[0xc027]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	[0xc023]	TLSv1.2	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	[0xc013]	SSLv3	Kx=ECDH	Conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	[0xc009]	SSLv3	Kx=ECDH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256	[0xa2]	TLSv1.2	Kx=DH	Conforme	Non pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	[0x9e]	TLSv1.2	Kx=DH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	[0x67]	TLSv1.2	Kx=DH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256	[0x40]	TLSv1.2	Kx=DH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	[0x33]	SSLv3	Kx=DH	Conforme	Non pris en charge
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA	[0x32]	SSLv3	Kx=DH	Conforme	Non pris en charge
TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE-RSA-SEED-SHA	[0x9a]	SSLv3	Kx=DH	Non conforme	Non pris en charge
TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE-DSS-SEED-SHA	[0x99]	SSLv3	Kx=DH	Non conforme	Non pris en charge
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	[0x45]	SSLv3	Kx=DH	Non conforme	Non pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE-DSS-CAMELLIA128-SHA	[0x44]	SSLv3	Kx=DH	Non conforme	Non pris en charge
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	ECDH-RSA-AES128-GCM-SHA256	[0xc031]	TLSv1.2	Kx=ECDH/RSA	Conforme	Non pris en charge
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH-ECDSA-AES128-GCM-SHA256	[0xc02d]	TLSv1.2	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	ECDH-RSA-AES128-SHA256	[0xc029]	TLSv1.2	Kx=ECDH/RSA	Conforme	Non pris en charge
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH-ECDSA-AES128-SHA256	[0xc025]	TLSv1.2	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	[0xc00e]	SSLv3	Kx=ECDH/RSA	Conforme	Non pris en charge
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	[0xc004]	SSLv3	Kx=ECDH/ECDSA	Conforme	Non pris en charge
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	[0x9c]	TLSv1.2	Kx=RSA	Conforme	Pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	[0x3c]	TLSv1.2	Kx=RSA	Conforme	Pris en charge
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	[0x2f]	SSLv3	Kx=RSA	Conforme	Pris en charge
TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA	[0x96]	SSLv3	Kx=RSA	Non conforme	Pris en charge
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	[0x41]	SSLv3	Kx=RSA	Non conforme	Pris en charge
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA	[0x07]	SSLv3	Kx=RSA	Non conforme	Pris en charge
TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	[0xc011]	SSLv3	Kx=ECDH	Non conforme	Non pris en charge
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	[0xc007]	SSLv3	Kx=ECDH	Non conforme	Non pris en charge
TLS_ECDH_RSA_WITH_RC4_128_SHA	ECDH-RSA-RC4-SHA	[0xc00c]	SSLv3	Kx=ECDH/RSA	Non conforme	Non pris en charge

Nom de la suite de chiffrement (RFC)	Nom (OpenSSL)	Suites de chiffrement	Version de TLS	KeyExch.	FIPS	Clé privée
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	ECDH-ECDSA-RC4-SHA	[0xc002]	SSLv3	Kx=ECDH/ECDSA	Non conforme	Non pris en charge
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	[0x05]	SSLv3	Kx=RSA	Non conforme	Pris en charge
TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA	[0x15]	SSLv3	Kx=RSA	Non conforme	Non pris en charge
TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-DES-CBC-SHA	[0x12]	SSLv3	Kx=DSS	Non conforme	Non pris en charge
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA	[0x09]	SSLv3	Kx=RSA	Non conforme	Pris en charge
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA	[0x14]	SSLv3	Kx=DSS	Non conforme	Non pris en charge
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA	[0x11]	SSLv3	Kx=DSS	Non conforme	Non pris en charge
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA	[0x08]	SSLv3	Kx=DES	Non conforme	Pris en charge

Hachage du certificat TLS

Le Network Decoder peut produire des hachages de certificats qui sont visibles dans le flux de paquets. Ces hachages sont la valeur SHA-1 de tout certificat codé DER rencontré lors d'une négociation TLS. Les hachages produits peuvent être utilisés pour comparer le trafic réseau avec les hachages des listes noires SSL publiques, comme celle de sslbl.abuse.ch.

La fonctionnalité de hachage de certificat TLS est désactivée par défaut. Elle peut être activée en ajoutant l'option du parser :

```
HTTPS="cert.sha1=true"
```

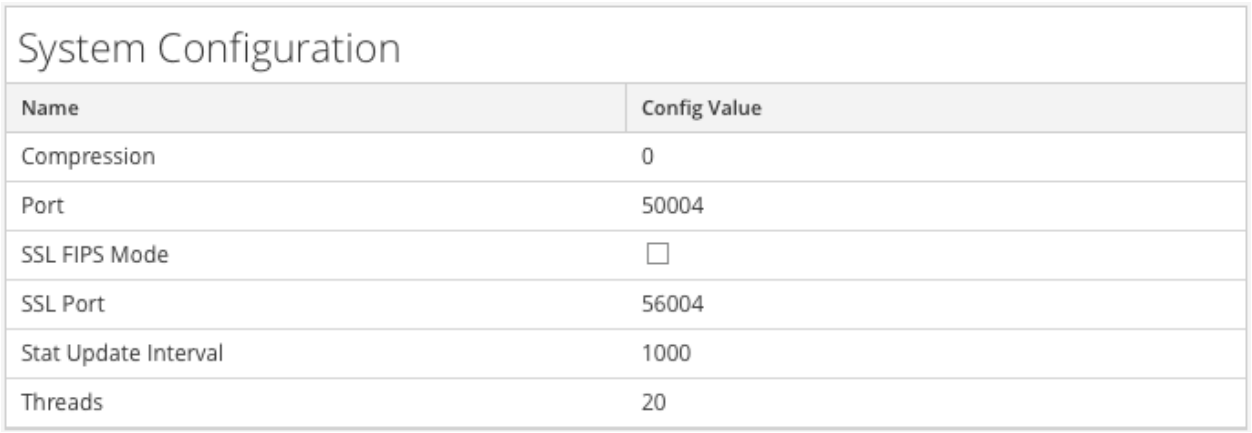
à la configuration `/decoder/parsers/config/parsers.options` d'un Network Decoder.

Lorsque cette option est activée, le SHA-1 est stocké sous la forme d'une valeur de texte dans la méta-clé :

```
cert.checksum
```

Modifier la configuration système de Decoder

Lorsqu'un service est ajouté pour la première fois à NetWitness Platform, les valeurs par défaut des paramètres de configuration système s'appliquent. Dans la plupart des cas, les valeurs par défaut pour la compression, l'intervalle de mise à jour des statistiques et le nombre de threads dans le pool de threads sont configurées de façon à optimiser les performances système. Il est inutile de modifier ces paramètres, sauf si un technicien du support client RSA vous le demande.


System Configuration

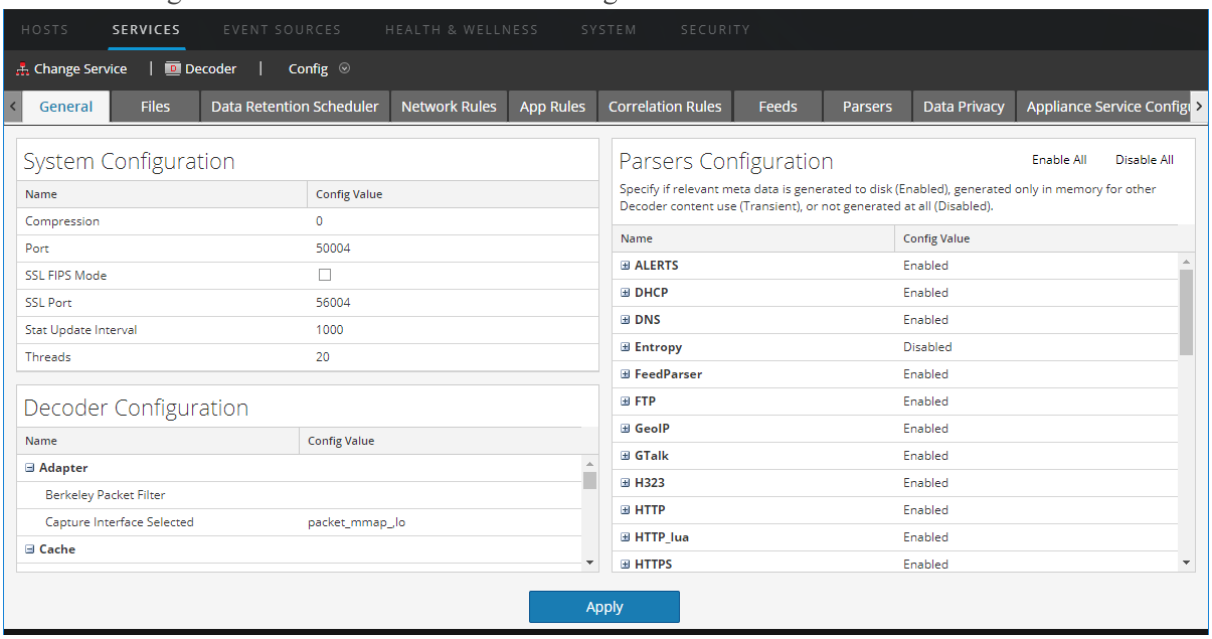
Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	☐
SSL Port	56004
Stat Update Interval	1000
Threads	20

Vous souhaiterez peut-être modifier le paramètre SSL de votre environnement, qui est désactivé par défaut. Lorsqu'il est activé, la sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL.

Pour modifier les paramètres de configuration d'un Decoder ou d'un Log Decoder :

1. Accédez à**ADMIN > Services**.
2. Dans la vue Admin > System, sélectionnez un service Decoder ou Log Decoder, puis sélectionnez  **> Vue > Config**.

La Vue Configuration des services s'ouvre sur l'onglet Général.



3. Sous **Configuration du système**, cliquez sur un champ que vous voulez modifier **(Compression**, **Port**, **Mode FIPS SSL**, **Port SSL**, **Intervalles de mise à jour des statistiques** ou **Threads**). Saisissez une nouvelle valeur.
4. Lorsque la modification est terminée, cliquez sur **Appliquer.**
   Les paramètres prennent effet immédiatement.

Activer les statistiques d'utilisation du CPU pour le contenu installé

À partir de la version RSA NetWitness® Platform 11.0, le Decoder fournit des statistiques d'utilisation du CPU pour tous les contenus installés, que vous pouvez utiliser pour découvrir le temps de CPU utilisé par les parsers, les feeds, les règles d'application et l'analyse lexicale. Les statistiques apparaissent sous forme de nœuds Statistiques dans l'arborescence des services de la vue Explorer lorsque `/decoder/parsers/config/detailed.stats` est activé et que le Decoder capture les statistiques.

Chaque élément de contenu est comptabilisé comme une valeur unique en pourcentage (0-100), quel que soit le nombre de threads d'analyse en cours d'exécution. Le pourcentage représente une moyenne mensuelle de l'utilisation du CPU pour le contenu sur tous les threads.

Pour activer la surveillance des statistiques d'utilisation :

1. Accédez à la vue Explorer du Decoder et sélectionnez le paramètre `/decoder/parsers/config/detailed.stats`.
2. Remplacez la valeur par **Activé**. Si le Decoder ne capture pas de données, démarrez la capture. Lorsque vous ouvrez le nœud Statistiques du Decoder dans la vue Explorer, la nouvelle statistique s'affiche.

Activer les mappages d'analyseur

Cette rubrique indique aux administrateurs comment activer le mappage des sources d'événements sur un Log Decoder.

Le Log Collector découvre le type de source d'événement de chaque message. Si l'analyseur approprié n'est pas identifié pour la source d'événement, un faible pourcentage de logs peut être mal identifié. Les messages mal classés ne renseignent pas les règles et les alertes de sources d'événements, et les rapports ne disposent pas des données correctes. En outre, s'il y a plusieurs types de sources d'événements associés à une adresse IP, il peut être difficile pour les analyseurs d'identifier la source d'événement exacte à partir de laquelle les logs sont générés.

Si vous mappez une adresse IP à son type de source d'événement, le Log Decoder peut identifier la source d'événement à partir de laquelle le log est généré. Lorsque les messages sont remis au Log Decoder à partir d'une source d'événement mappée, les analyseurs affectés sont interrogés pour trouver les correspondances d'événements.

Vous pouvez attribuer des types de sources d'événements pour IPV4, IPV6, ou la valeur de nom d'hôte de la source d'événement. Vous pouvez également affecter plusieurs types de sources d'événements à une seule adresse IP. Vous pouvez aussi utiliser un ID Log Collector lorsque différentes sources d'événements avec la même adresse IP sont envoyées à différents services Log Collector.

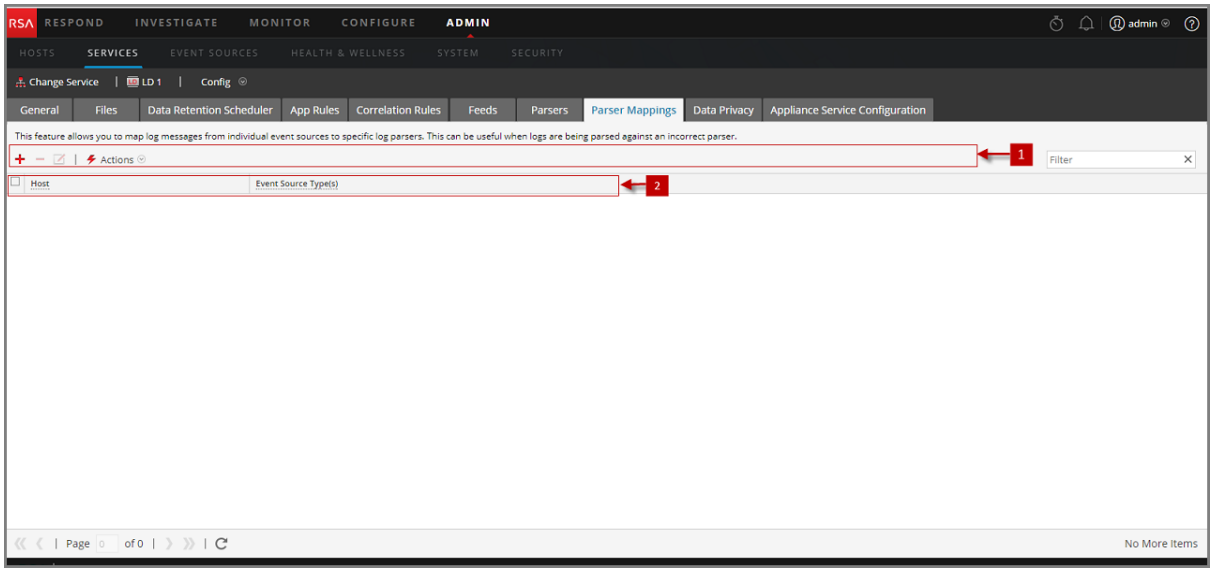
Remarque : Vous pouvez également activer les fonctions de mappage de l'analyseur en accédant à **ADMIN > Sources d'événements > Découverte.**

Activer une adresse IP pour le mappage de sources d'événements

Pour activer une adresse IP pour le mappage de sources d'événements :

1. Accédez à **ADMIN > Services**, puis sélectionnez un Log Decoder.
2. Sélectionnez  **> Vue > Config**.

3. Sur la page Configuration, sélectionnez l'onglet **Mappages d'analyseur**.
   L'onglet Mappages d'analyseur s'affiche dans la vue Configuration des services.

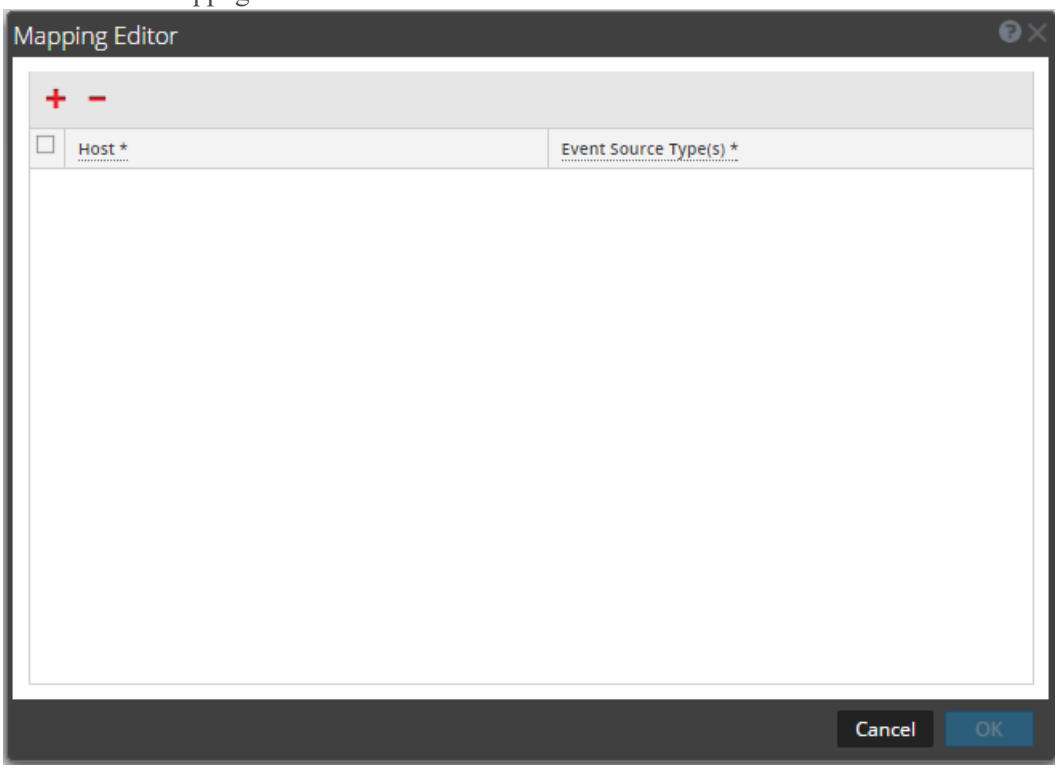


Mettre à jour une adresse IP pour le mappage de sources d'événements

Pour mettre à jour une adresse IP pour le mappage de sources d'événements :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un **Log Decoder**, puis dans la colonne **Actions**, sélectionnez  **> Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseur**.
4. Cliquez sur  .

L'Éditeur de mappage s'affiche.



5. Les mappages suivants peuvent être définis :

- **Un hôte et un type de source d'événement**
  Dans le champ **Hôte** saisissez le nom d'hôte.
  Par exemple :`10.0.0.1`
- Dans le champ **Source(s) d'événements**, saisissez le type de source d'événement.
  Par exemple :`apache`
- **Un hôte et un ou plusieurs types de sources d'événements**
  Dans le champ **Hôte**, saisissez le nom d'hôte.
  Par exemple : `10.0.0.1`
- Dans le champ **Source(s) d'événements**, saisissez le type de source d'événement.
  Par exemple :`apache,sap,aix`
- **Un hôte, un Log Collector et un type de source d'événement**
  Dans le champ **Hôte**, saisissez le nom d'hôte et l'ID de Log Collector.
  Par exemple : `10.0.0.1,LC-1`
- Dans le champ **Source(s) d'événements**, saisissez le type de source d'événement.
  Par exemple : `apache`
- **Un hôte, un ID de Log Collector et un ou plusieurs types de sources d'événements**
  Dans le champ **Hôte**, saisissez le nom d'hôte et l'ID de Log Collector.
  Par exemple : `10.0.0.1,LC-1`

- Dans le champ **Source(s) d'événements**, saisissez le type de source d'événement.
  Par exemple : `apache,sap,aix`

> **Remarque :** Les types de sources d'événements sont traités dans l'ordre où vous saisissez les analyseurs et si un ou plusieurs analyseurs correspondent à un log, le premier analyseur de la liste est interrogé. L'hôte/l'adresse IP peut être de type IPv4, IPv6 ou un nom d'hôte.

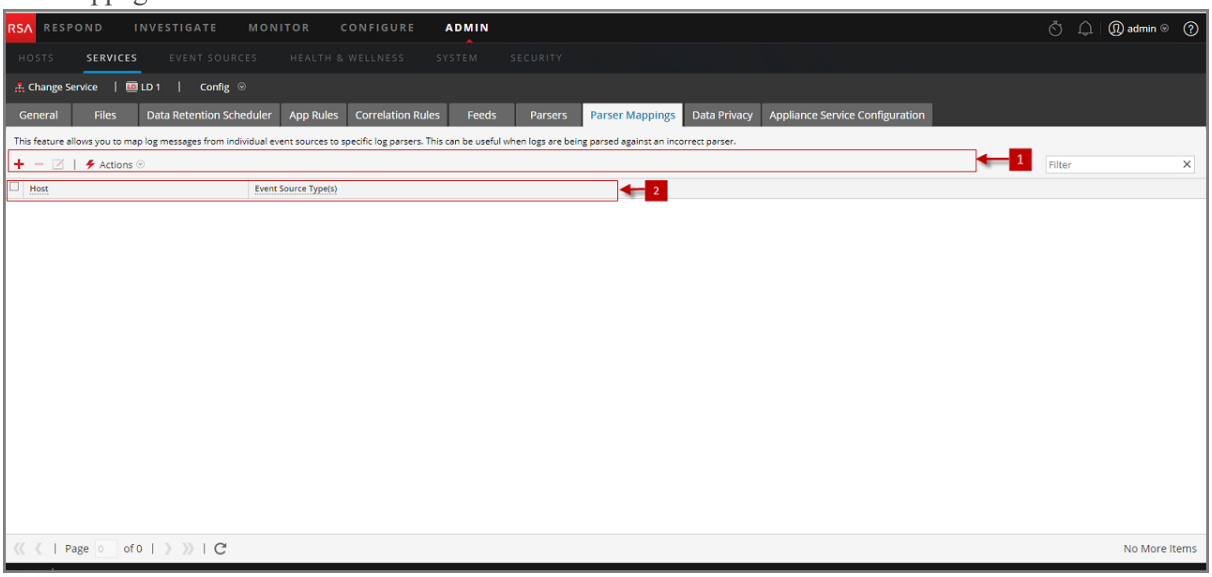
9. Cliquez sur **OK**.
   Le mappage des analyseurs est ajouté.

7. Pour annuler la sélection des mappages d'analyseur, cliquez sur **Annuler**.

Lire l'adresse IP dans les mappages de types de sources d'événements

Pour lire l'adresse IP dans les mappages de types de sources d'événements :

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez > **Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseur**.
   Les mappages sont affichés.



Modifier l'adresse IP dans le mappage de types de sources d'événements

Pour modifier l'adresse IP dans le mappage de types de sources d'événements :

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez > **Vue > Config**.
   La vue Configuration des services s'affiche.

3. Sélectionnez l'onglet **Mappages d'analyseurs**.
4. Sélectionnez le mappage que vous souhaitez modifier.
   Remarque : Vous ne pouvez modifier qu'une seule liste à la fois.
5. Cliquez sur 
6. Dans le champ **Source(s) d'événement(s)** , saisissez la ou les sources d'événements.
   Remarque : L'hôte n'est pas modifiable et le champ est désactivé.
7. Cliquez sur **OK** pour accepter la source d'événement modifiée.
8. Pour annuler les modifications, cliquez sur **Annuler**.

Supprimer l'adresse IP dans le mappage de types de sources d'événements

Pour supprimer l'adresse IP dans le mappage de types de sources d'événements :

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez  **> Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseurs**.
4. Sélectionnez le mappage que vous souhaitez supprimer.
5. Cliquez sur .
   Le mappage est supprimé et la grille est actualisée.
6. Pour annuler les modifications, cliquez sur **Annuler**.

Trier le nom d'hôte ou le type de source d'événement

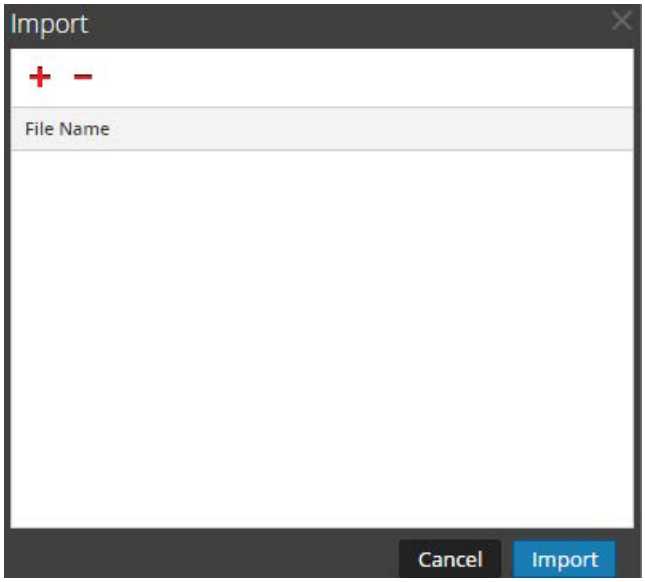
Pour trier le nom d'hôte ou le type de source d'événement :

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez  **> Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseurs**.
4. Pour trier une colonne, cliquez sur
   sur l'en-tête de cette colonne.Le ou les types de source d'événement sont appliqués à l'adresse IP sélectionnée. Les fichiers log sont analysés par rapport aux analyseurs dans l'ordre dans lequel ils sont répertoriés.

Importer une adresse IP pour les entrées de mappage de sources d'événements

Pour importer une adresse IP pour les entrées de mappage de sources d'événements :

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez > **Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseurs**.
4. Sélectionnez **Actions > Importer**.
   La boîte de dialogue Importer s'affiche.



5. Cliquez sur .
6. Sélectionnez le fichier à importer, puis cliquez sur **OK**.
7. Pour charger l'analyseur, cliquez sur **Importer**.

Remarque : Vous ne pouvez importer qu'un seul fichier .csv à la fois.

Exporter une adresse IP pour les entrées de mappage de sources d'événements

Pour exporter une adresse IP pour les entrées de mappage de sources d'événements :

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez > **Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseurs**.
4. Sélectionnez les mappages à exporter.

5. Sélectionnez **Actions > Exporter > Sélection**.
   La boîte de dialogue Sélections pour l'exportation s'affiche.

6. Saisissez un nouveau nom et cliquez sur **Exporter**.

Rechercher une adresse IP pour les entrées de mappage de sources d'événements

Pour rechercher une adresse IP pour les entrées de mappage de sources d'événements

1. Accédez à **ADMIN > Services**, puis sélectionnez un service Log Decoder.
2. Dans la colonne Actions, sélectionnez > **Vue > Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Mappages d'analyseurs**.
4. Dans la barre d'outils Mappage d'analyseurs, saisissez l'hôte ou la source d'événement dans le champ **Filtrer**.
5. Cliquez sur **Entrée**.
   Les hôtes ou les sources d'événements qui correspondent aux noms saisis dans le champ **Filtrer** s'affichent.

Activer ou désactiver les systèmes d'analyse Lua et Flex

Cette rubrique indique aux administrateurs comment activer ou désactiver les systèmes d'analyse Lua et Flex sur un service Decoder ou Log Decoder. Les analyseurs Flex sont obsolètes et désactivés par défaut.

Les paramètres permettant d'activer ou de désactiver ces systèmes d'analyse sont déjà configurés par défaut et en règle générale, vous n'avez pas besoin de les modifier. En revanche, vous pouvez les ajuster à la demande du Support Clients RSA ou à des fins de dépannage.

En plus de la configuration de chaque analyseur, vous pouvez activer et désactiver tous les analyseurs Lua, ainsi que tous les analyseurs Flex dans la vue Explorer les services. Vous pouvez effectuer les opérations d'activation et de désactivation de ces deux systèmes d'analyse séparément, même s'ils fonctionnent de la même manière.

- Si vous **désactivez** le système d'analyse Lua ou Flex, le système d'analyse correspondant sera désactivé et aucun analyseur ne sera chargé.
- Si vous **activez** le système d'analyse Lua ou Flex, le système d'analyse correspondant sera activé et chaque analyseur sera activé et désactivé en fonction des configurations individuelles définies.

Pour activer ou désactiver les systèmes d'analyse Lua et Flex sur un service Decoder ou Log Decoder :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service Decoder ou Log Decoder, puis  **> Vue > Explorer.**
   La vue Explorer les services pour le service sélectionné s'affiche.
3. Dans la liste Nœud, naviguez jusqu'à **`/decoder/parsers/config`** et sélectionnez-le.
4. Dans le panneau Surveillance :
   - Pour activer le système d'analyse Lua, dans le champ de valeur `lua.enabled`, saisissez **yes**.
   - Pour désactiver le système d'analyse Lua, dans le champ de valeur `lua.enabled`, saisissez **no**.
   - Pour activer le système d'analyse Flex, dans le champ de valeur `flex.enabled`, saisissez **yes**.
   - Pour désactiver le système d'analyse Flex, dans le champ de valeur `flex.enabled`, saisissez **no**.

Mapper l'adresse IP avec le type de service pour l'analyse de log

Cette rubrique décrit la procédure pour mapper une adresse IP à un type de service pour l'analyse de log.

Le Log Collector découvre le type de source d'événement de chaque message. Si l'analyseur n'est pas approprié à la source d'événement spécifiée, les messages qui sont communs entre les types de sources d'événements seront mal classés. Les messages mal identifiés ne renseignent pas les règles ni les alertes de service, et les rapports ne contiennent pas les informations appropriées. En outre, s'il y a plusieurs services associés à une adresse IP, il peut être difficile pour les analyseurs d'identifier le service exact à partir duquel le log est généré.

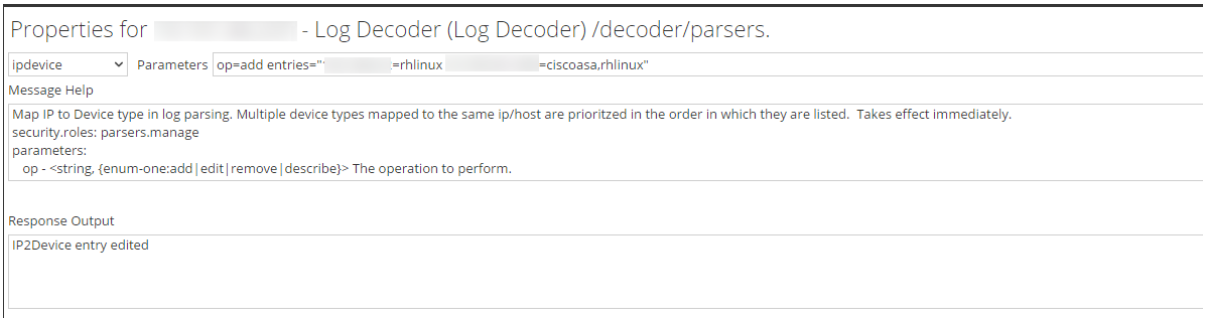
Si vous mappez une adresse IP à ses services, le Log Decoder peut identifier le service à partir duquel le log est généré. Lorsque les messages sont dans le Log Decoder à partir d'un service mappé, les analyseurs affectés sont chargés de trouver les correspondances d'événements.

Vous pouvez attribuer des types de service pour IPV4, IPV6, ou la valeur de nom d'hôte de la source d'événement. Vous pouvez également affecter plusieurs types de services à une seule adresse IP. Vous pouvez aussi utiliser CollectorID lorsque différents types de services avec la même adresse IP sont envoyés à différents collecteurs.

Mapper une adresse IP à un type de service

Pour mapper une adresse IP à un type de service, procédez comme suit :

1. Accédez à **ADMIN > Services**.
2. Dans la vue **Services**, sélectionnez un Log Decoder, et dans la colonne **Actions**, sélectionnez  **> Vue > Explorer**.
3. Accédez au nœud **/decoder/parsers**, cliquez avec le bouton droit sur **parsers**, puis sélectionnez **Propriétés**.
4. Dans la vue **Propriétés**, spécifiez la commande **ipdevice** avec les paramètres suivants : `op=add/remove entries="ipaddress=service”` (par exemple, `op=add entries="10.100.201.300=ciscoasa"`)
5. Cliquez sur **Envoyer**.



Commande IPdevice

Dans la commande `ipdevice`, trois opérations sont disponibles :

- `add` : Cette opération ajoute ou met à jour des entrées dans le mappage ipdevice. Vous pouvez spécifier plusieurs paires adresse/type séparées par des espaces.
  `op=add entries="<address>=<service type>"`
- `remove` : Cette opération supprime les entrées du mappage ipdevice. Vous pouvez spécifier plusieurs paires adresse/type séparées par des espaces.
  `op=remove entries="<address>"`
- `describe` : Cette opération renvoie les valeurs actuellement présentes dans le mappage ipdevice.

Mapper une adresse IP à un fuseau horaire

Souvent les journaux de temps ne spécifient pas entièrement les horodatages et il peut manquer des informations sur le fuseau horaire. Pour normaliser correctement ces horodatages en UTC, le Log Decoder offre la possibilité d'associer les périphériques à partir d'une adresse spécifique (IPv4 ou IPv6) ou du nom d'hôte à un fuseau horaire ou un écart fixe.

Il existe actuellement trois formats de fuseau horaire acceptés et ils sont présentés dans les exemples suivants :

- Format Olson : Amérique/Anguilla
- Format POSIX : AST2:45ADT0:45,M4.1.6/1:45,M10.5.6/2:45
- Format avec écart d'heures : = -500

NetWitness Platform mappe l'adresse du périphérique (IPv4 ou IPv6) ou le nom d'hôte à un fuseau horaire ou écart. Les métas liées au temps de l'événement qui sont analysées à partir d'un log provenant d'une adresse mappée et ne comprenant pas d'écart ou de fuseau horaire dans l'horodatage sont ajustées en heure UTC en fonction du mappage.

Pour mapper une adresse IP à un fuseau horaire, procédez comme suit :

1. Accédez à **ADMIN > Services**.
2. Dans la vue **Services**, sélectionnez un Log Decoder, et dans la colonne **Actions**, sélectionnez  **> Vue > Explorer**.
3. Accédez au nœud **/decoder/parsers**, cliquez avec le bouton droit sur **Parsers**, puis sélectionnez **Propriétés**.
4. Dans la vue **Propriétés**, spécifiez la commande `iptmzone` avec les paramètres suivants :
   `op=add entries="ipaddress=timezone" (par exemple, op=add entries="10.10.10.10=Africa/Addis Ababa")`
5. Cliquez sur **Envoyer**.

Commande iptmzone

Dans la commande `iptmzone`, trois opérations sont disponibles :

- `add` : Cette opération ajoute ou met à jour des entrées dans le mappage iptmzone. Vous pouvez spécifier plusieurs paires adresse/type séparées par des espaces.
  `op=add entries="<address>=<time zone>"`

- `remove` : Cette opération supprime des entrées dans le mappage iptmzone. Vous pouvez spécifier plusieurs paires adresse/type séparées par des espaces.
  `op=remove entries="<address>"`
- `describe` : Cette opération renvoie les valeurs actuellement présentes dans le mappage iptmzone.

Exemples

Les exemples suivants proposent des instances de mappage des adresses IP à des fuseaux horaires :

- Si vous souhaitez mapper deux entrées différentes avec des valeurs IPV4 et des fuseaux horaires différents, saisissez le paramètre suivant dans la commande **iptmzone**, puis cliquez sur **Send**
  `"op=add entries=”10.10.10.10=America/Anguilla 10.10.10.11=Pacific/Rarotonga”`
- Si vous souhaitez supprimer une entrée pour une valeur IPV4 et un fuseau horaire unique, saisissez le paramètre suivant dans la commande **iptmzone**, puis cliquez sur **Envoyer**.
  `"op=remove entries=10.5.245.9"`
- Si vous souhaitez créer une entrée unique pour une valeur IPV6 et un fuseau horaire, saisissez le paramètre suivant dans la commande **iptmzone**, puis cliquez sur **Envoyer**.
  `op=add entries=”2001:DB8:85A3::8A2E:370:7334=America/Anguilla”`
- Si vous souhaitez créer une entrée unique pour mapper un nom d’hôte, IPV4 ou IPV6 au format d’écart en minutes, Olson ou POSIX, saisissez le paramètre suivant dans la commande **iptmzone**, puis cliquez sur **Envoyer**.
  `op=add entries="10.168.0.2=America/Anguilla 2001:DB8:85A3::8A2E:370:7334=0500nwappliance21=EST5EDT,M3.2.0/2,M11.1.0'`

Obtenir des fichiers Log à partir d’un Log Decoder pré-11.0

NetWitness 11.0 a ajouté la possibilité d’afficher un petit échantillon des logs récents pour certains périphériques via des onglets de détails de la vue Découverte. Par défaut, les versions de Log Decoders antérieures à 11.0 ne possèdent pas la configuration requise pour activer cette fonction, mais quelques changements mineurs peuvent la rendre disponible.

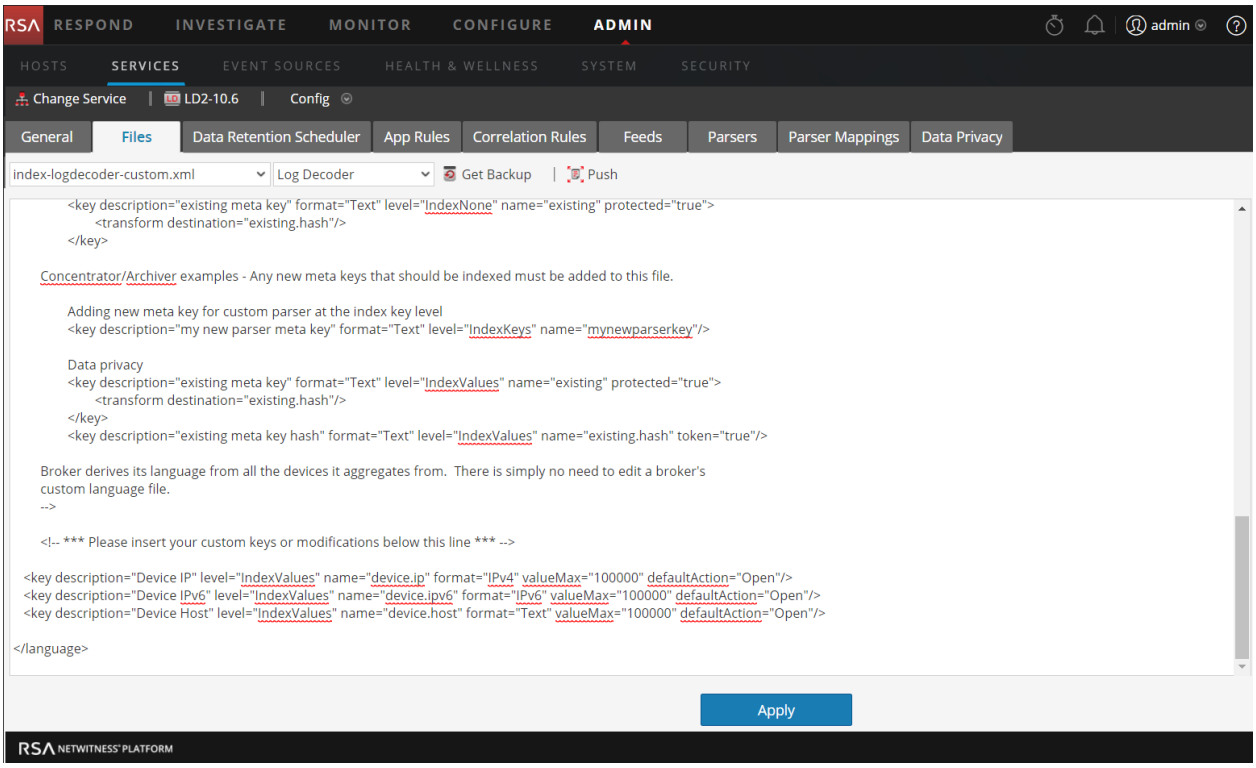
Pour activer l’aperçu des logs pour une version de Log Decoder antérieure à 11.0, suivez ces étapes dans le Log Decoder :

1. Accédez à **ADMIN > Services >**, sélectionnez un **Log Decoder**, puis  **> Vue > Config**.
2. Cliquez sur l'onglet **Fichiers**, puis dans le menu déroulant, sélectionnez **index-logdecoder-custom.xml**.
3. Ajoutez les trois lignes suivantes à la fin du fichier (avant la balise de langue fermante) :

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4" valueMax="100000"
defaultAction="Open"/>
<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

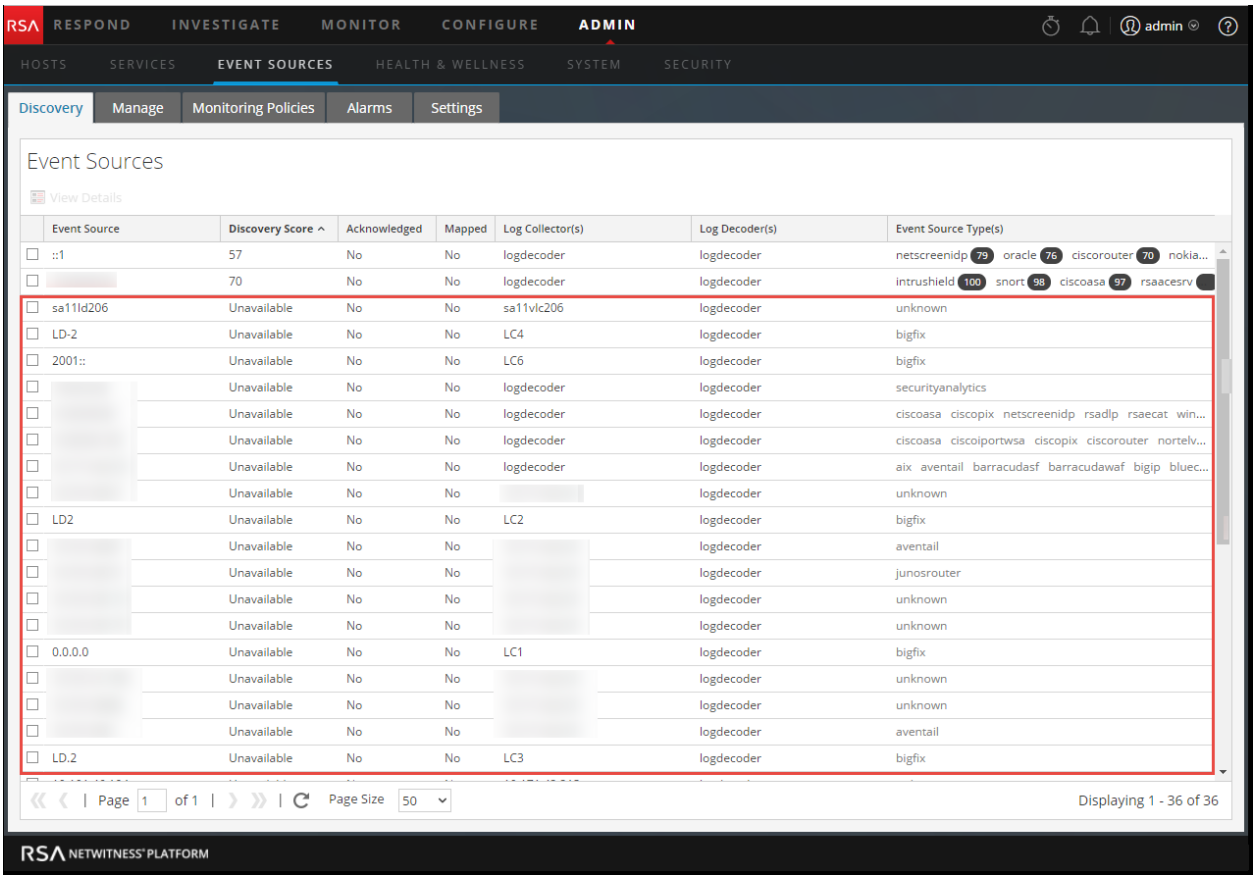
4. Cliquez sur **Appliquer**.
5. Redémarrez le Log Decoder comme suit.
   Sélectionnez le service Log Decoder **> Explorer > decoder > Propriétés > Réinitialiser**
   Sélectionnez **réinitialiser** dans un menu déroulant. Cliquez sur **Envoyer** après avoir sélectionné réinitialiser.

Exemple de fichier **index-logdecoder-custom.xml**.



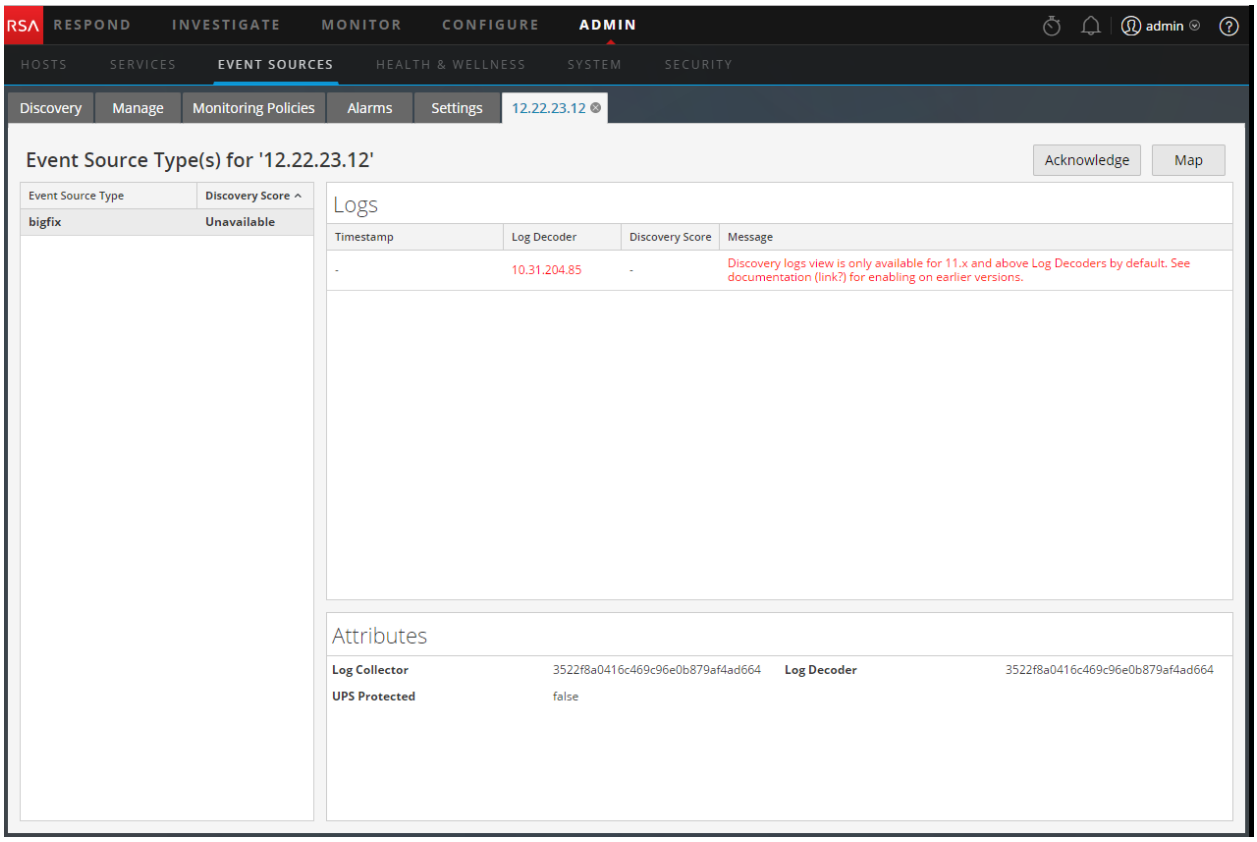
Remarque : Les scores de découverte ne sont disponibles que pour les services Log Decoder 11.x et version supérieure. Les scores de découverte pour les versions Log Decoders antérieures à 11.x s'affichent comme étant non disponibles.

L'exemple suivant affiche un score de découverte considéré comme **Non disponible** dans la vue **Détails** pour une version de Log Decoder antérieure à 11.0.



Remarque : Les logs de périphériques sont uniquement disponibles pour les versions de Log Decoder 11.x et ultérieures.

L'exemple suivant affiche le message qui s'affiche dans le volet Logs pour une version de Log Decoder antérieure à 11.0.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Discovery
Manage
Monitoring Policies
Alarms
Settings
12.22.23.12
Event Source Type(s) for '12.22.23.12'
Acknowledge
Map
Event Source Type
Discovery Score
bigfix
Unavailable
Logs
Timestamp
Log Decoder
Discovery Score
Message
-
10.31.204.85
-
Discovery logs view is only available for 11.x and above Log Decoders by default. See documentation (link?) for enabling on earlier versions.
Attributes
Log Collector
3522f8a0416c469c96e0b879af4ad664
Log Decoder
3522f8a0416c469c96e0b879af4ad664
UPS Protected
false

Télécharger un fichier log vers un Log Decoder

Cette rubrique décrit la méthode permettant d'importer un fichier log dans un Log Decoder.

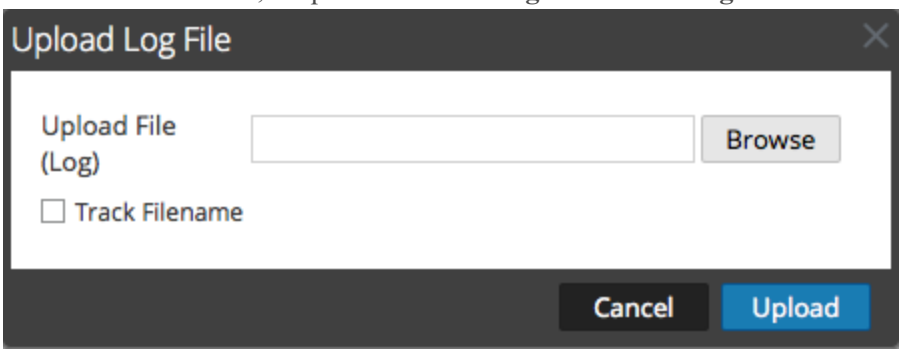
Il se peut parfois que vous souhaitiez analyser un fichier log qui n'est pas disponible pour le service utilisé. Vous pouvez télécharger un fichier log capturé d'un autre service vers NetWitness Platform. Les noms des fichiers log portent l'extension **.log**.

Si vous téléchargez un fichier log dans un Log Decoder, ce dernier l'analyse et génère des métadonnées pour chacun des logs qu'il contient. Ces logs sont ajoutés aux logs déjà décodés dans le Log Decoder et sont disponibles pour analyse. NetWitness Platform inclut une option de suivi des noms de fichier qui facilite la recherche d'un jeu de logs donné. Une fois le fichier log téléchargé avec cette option, le Log Decoder ajoute des métadonnées à chaque log en fonction du nom de fichier téléchargé. Vous pouvez ensuite filtrer les sessions à analyser à l'aide de ces métadonnées.

L'option de téléchargement d'un fichier log est grisée lorsque d'autres opérations du Log Decoder empêchent une telle action. Ce peut être le cas lorsque le Log Decoder capture des logs.

Pour importer un fichier log dans un Log Decoder :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un Log Decoder dans la grille **Service**, puis sélectionnez > **Vue > Système**.
   La vue Système de services du Log Decoder s'affiche.
3. Dans la barre d'outils, cliquez sur **Télécharger le fichier log**.



4. Pour choisir un fichier log, cliquez sur **Parcourir**.
   La vue du répertoire s'affiche.
5. Sélectionnez le fichier log à télécharger.
   Le nom du fichier s'affiche dans le champ **Télécharger le fichier**.
6. Pour que le Log Decoder ajoute des métadonnées aux logs d'après leur nom de fichier, cochez la case située à côté de **Suivre le nom de fichier**.
7. Pour télécharger le fichier, cliquez sur **Télécharger**.
   Le fichier sélectionné est téléchargé et un message d'état confirme que l'opération a réussi. Le fichier log est disponible pour l'analyse.

Télécharger un fichier de capture de paquets

Il se peut parfois que vous souhaitiez analyser un fichier de capture de paquet qui n'est pas disponible pour le service utilisé. Vous pouvez télécharger un fichier log capturé d'un autre service vers NetWitness Platform. Les fichiers de capture de paquet pris en charge sont au format `pcap` et `pcap.gz`.

Quand un fichier de capture de paquet est téléchargé dans un Decoder, ce dernier crée des sessions à partir des paquets du fichier. Ces sessions sont ajoutées aux sessions déjà décodées sur le Decoder et sont disponibles pour l'analyse. NetWitness Platform inclut une option de suivi du nom de fichier qui facilite la recherche d'un ensemble particulier de sessions. Une fois le fichier de capture de paquet téléchargé avec cette option, le Decoder ajoute des métadonnées aux sessions en fonction du nom de fichier téléchargé. Vous pouvez ensuite filtrer les sessions à analyser à l'aide de ces métadonnées.

L'option de téléchargement d'un fichier de capture de paquet est grisée lorsque d'autres opérations du Decoder empêchent une telle action. Ce peut être le cas lorsque le Decoder capture des paquets.

Pour sélectionner et télécharger un fichier de capture de paquet :

1. Accédez à **ADMIN** > **Services**.

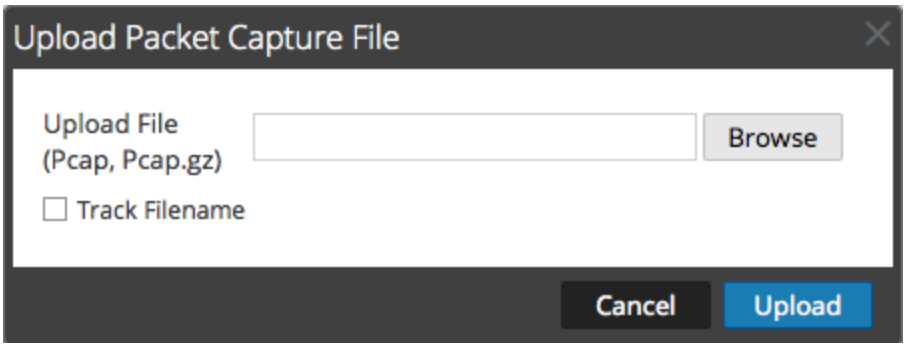
   La vue Services d'administration s'affiche.

2. Sélectionnez le nom du Decoder, puis > **Vue** > **Système**.

   La vue Système de services du Decoder s'affiche.

3. Dans la barre d'outils, cliquez sur **Télécharger le fichier de capture de paquets**.

   La boîte de dialogue **Télécharger le fichier de capture de paquets** s'affiche.



4. Pour choisir un fichier de capture, cliquez sur **Sélectionner**.

   La vue du répertoire s'affiche.

5. Dans le répertoire, sélectionnez le fichier de capture de paquet à télécharger.

   Son nom est affiché dans le champ **Télécharger le fichier(pcap,pcap.gz)**.

6. Pour que le Decoder ajoute des métadonnées aux sessions d'après leur nom de fichier, cochez la case située à côté de **Suivre le nom de fichier**.

7. Pour télécharger le fichier, cliquez sur **Télécharger**.

   Une barre de progression affiche l'avancée du téléchargement.

Le temps de téléchargement varie en fonction de la taille du fichier. Une fois le fichier téléchargé, un message d'état s'affiche. Le fichier peut à présent faire l'objet d'une procédure d'enquête.

Références de feed et d'analyseur

Cette rubrique fournit plus d'informations sur les feeds et les analyseurs utilisés par Decoder.

- Fichier de définition de feed
- Parsers Flex
- Parsers GeoIP2 et GeoIP
- Parsers Lua
- Parsers Snort
- Parser Search
- Configuration LAN sans fil

Fichier de définition de feed

Cette rubrique présente le fichier de définition de feed, qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers.

L'un des fichiers qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers est **`feed-definitions.xml`**, le fichier de définition de feed.

feed-definitions.xml

Vous pouvez définir des feeds dans le fichier `feed-definitions.xml`. Le Decoder utilise un schéma XML pour définir des messages feed lors de la création d'un fichier binaire .feed à partir des feeds définis ici.

Pour plus d'informations sur le langage de définition de feed, consultez la section « Gérer les feeds personnalisés » du *Guide de gestion des services en direct*.

Parsers Flex

L'un des fichiers qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers est `NwFlex.xml`, le parser Flex.

NwFlex.xml

Il existe deux types d'analyseurs Flex :

- **L'identification de service basée uniquement sur le port.** Il s'agit d'analyseurs qui utilisent uniquement des ports source ou de destination pour identifier le type d'application de session (le service). Ce sont les plus simples et plus faciles à définir.
- **L'identification de service basée sur un jeton ou des jetons trouvés.** Ces analyseurs utilisent des jetons pour identifier le type de service. Cette technique permet de développer facilement les types de services identifiés. Ces derniers sont importants lors de l'identification d'applications standards hors internet. Ces analyseurs nécessitent que le protocole dispose d'un token défini qui peut identifier de manière unique le type de service.

Voici cinq opérations courantes de parser :

- Faire correspondre le port et identifier immédiatement
- Faire correspondre le port et retarder l'identification
- Faire correspondre le token et identifier immédiatement
- Faire correspondre plusieurs tokens
- Faire correspondre le token et créer les métadonnées

Des informations et des exemples de langue détaillés sont fournis dans cette rubrique. Cette rubrique décrit le schéma XML utilisé pour définir un fichier FlexParse. Le nœud SML, l'attribut et les valeurs mentionnés dans le texte descriptif sont en **gras**. Le nœud racine de chaque fichier doit être le nœud **analyseurs**. Sous ce nœud, il peut y avoir un certain nombre de nœuds analyseurs. Chaque nœud analyseur définit un analyseur unique. Un nœud analyseur peut comporter un nœud **declaration** et un nombre illimité de nœuds **match**.

Rubriques

- Regex
- Fonctions de chaîne

Fonctions arithmétiques

Cette rubrique donne les définitions linguistiques des fonctions arithmétiques du parser Flex.

Cette rubrique donne les définitions linguistiques des fonctions arithmétiques du parser Flex. Tous les nombres sont des valeurs non signées de 64 bits, soumis à la fois au soupassement et au dépassement de capacité, selon l'opération.

Définition de langue

Le tableau suivant fournit des définitions linguistiques.

Node Name	Nom de l'attribut	Description
and		Effectue une opération AND au niveau du bit entre deux nombres.
	name	Variable dans laquelle effectuer une opération AND du résultat.
	value	Nombre auquel effectuer une opération AND dans le résultat.
or		Effectue une opération OR au niveau du bit entre deux nombres.
	name	Variable dans laquelle effectuer une opération OR du résultat.
	value	Nombre auquel effectuer une opération OR dans le résultat.
increment		Effectue l'ADDITION de deux nombres.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de l'ADDITION.
	value	Nombre à AJOUTER à la valeur initiale.
decrement		Effectue la SOUSTRACTION de deux nombres.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de la SOUSTRACTION.
	value	Nombre à SOUSTRAIRE de la valeur initiale.
divide		Effectue la DIVISION de deux nombres.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de la DIVISION.
	value	Nombre par lequel diviser la valeur initiale. La division par zéro génère une erreur et arrête le traitement de la session actuelle par ce parser.
modulo		Effectue une opération MODULO de deux nombres.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de l'opération MODULO.

Node Name	Nom de l'attribut	Description
	value	Nombre par lequel diviser la valeur initiale. La division par zéro génère une erreur et arrête le traitement de la session actuelle par ce parser.
multiply		Effectue une MULTIPLICATION de deux nombres.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de la MULTIPLICATION.
	value	Nombre par lequel MULTIPLIER la valeur initiale.
shiftleft		Effectue un décalage à gauche binaire.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de l'opération de décalage.
	value	Nombre de bits du déplacement.
shiftright		Effectue un décalage à droite binaire.
	name	Variable contenant la valeur initiale AND pour recevoir les résultats de l'opération de décalage.
	value	Nombre de bits du déplacement.

Opérations courantes des parsers

Cette rubrique donne des exemples d'opérations courantes des parsers.

Cette rubrique présente cinq opérations courantes des parsers.

Faire correspondre le port et identifier immédiatement

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
          <parser name="CustApp" desc="Acme Custom App" service="45324">
               <declaration>
                    <port name="port" value="45324" />
               <declaration>
               </match name="port">
                    <identify />
               </match>
          </parser>
</parsers>
```

Faire correspondre le port et retarder l'identification

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MSRPC" desc="Microsoft RPC protocol" service=135">
          <declaration>
               <port name="port" value="135" />
               <number name="state" scope="session" />
               <session name="end" value="end" />
          </declaration>
          <match name="port">
               <assign name="state" value="1" />
          </match>
          <match name="end">
               <if name="state" equal="1" />
                    <identify />
               </if>
          </match>
     </parser>
</parsers>
```

Faire correspondre le token et identifier immédiatement

```
<?xml version="1.0" encoding="utf-8?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="RDP" desc="Remote Desktop Protocol" service="3389">
          <declaration>
               <token name="signature" value="Cookie: mstshash=" />
          </declaration>
          <match name="signature">
               <identify />
          </match>
     </parser>
</parsers>
```

Faire correspondre plusieurs tokens

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MyServiceMultiToken" desc="Multiple Tokens" service="333">
          <declaration>
               <number name="state" scope="stream" />
               <token name="user" value="USER " />
               <token name="pass" value="PASS " />
               <session name="session" value="end" />
          </declaration>
          <match name="user">
               <or name="state" value="1" />
          </match>
          <match name="pass">
               <or name="state" value="2" />
          </match>
          <match name="session">
               <if name="state" equal="3">
                    <identify />
               </if>
          </match>
     </parser>
</parsers>
```

Faire correspondre le token et créer les métadonnées

```
<?xml version="1.0" encoding="utf-8"?>
<parsers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="SHELL" desc="Command Shell Identification">
          <declaration>
               <token name="cmd.exe" value=" (C) Copyright 1985-2001 Microsoft
               Corp" options="linestart" />
               <meta name="client" key="client" format="Text" />
          </declaration>
          <match name="cmd.exe"
               <register  name="client" value="MS Command Shell" />
          </match>
     </parser>
</parsers>
```

Fonctions générales

Cette rubrique donne les définitions linguistiques des fonctions générales du parser Flex.

Définition linguistiques de fonctions générales

Node Name	Nom de l'attribut	Description
apptype		Obtient le type de service actuellement défini pour la session en cours.
	name	Variable sous forme de nombre pour recevoir le type de service en cours.
identify		Marque la session avec le type de service de l'analyseur si le type de service n'a pas déjà été identifié.
assign		Attribue une valeur à une variable.
	name	Identifiant unique attribué à l'objet dans la section de déclaration.
	value	Facultatif. Si elle est spécifiée, l'action définie dans la correspondance n'est appliquée que lorsque la déclaration correspond à la valeur donnée.
getmeta		Récupère la valeur de la métadonnée qui a généré un rappel. Cette fonction renverra des résultats vides (0, chaîne de longueur zéro) si elle est appelée en l'absence de rappel de métadonnées.
	name	Variable pour recevoir la valeur de la clé méta qui a généré le rappel.
gettoken		Renvoie le token associé actuel.
	name	Variable sous forme de chaîne pour recevoir le jeton associé actuel. S'il n'existe aucun jeton actuel, une chaîne vide est attribuée à la variable.
end		Termine l'exécution de la section **match** actuelle.
if		Compare deux valeurs. Si la comparaison est vraie, exécute une sous-action. Les comparaisons peuvent être de type **nombre** ou **chaîne**, à partir du moment où les deux valeurs sont du même type.
	name	Identifiant unique variable attribué à l'objet dans la section de **déclaration**.

Node Name	Nom de l'attribut	Description
	equal notequal less lessequal greater greaterequal and or	Valeur d'opération à comparer. Si la valeur est vraie, une sous-action est exécutée.
register		Ajoute des métadonnées à la session.
	name	Identifiant unique d'une variable de métadonnées à créer, tel que le définit la section **déclaration**.
	value	Valeur des métadonnées à créer.
while		Compare deux valeurs et exécute une sous-action si la comparaison est vraie. Les comparaisons peuvent être de type **nombre** ou **chaîne**, à partir du moment où les deux valeurs sont du même type.
	name	Identifiant unique variable attribué à l'objet dans la section de déclaration.
	equal notequal less lessequal greater greaterequal and or	Spécifie la valeur d'opération à comparer. Si la valeur est vraie, une sous-action est exécutée. Les attributs **and** et **or** indiquent des opérations au niveau du bit et ne peuvent être appliqués qu'à des variables **number**.
call		Exécute l'élément **match** spécifié. Il peut s'agir de tout élément de correspondance défini dans le même parser flex, quel que soit son mode de déclaration.
	value	Nom de l'élément de correspondance, ou variable de chaîne contenant le nom d'un élément de correspondance. • Si le nom de l'élément de correspondance est spécifié, l'analyseur ne se chargera pas si l'élément associé nommé n'existe pas. • Si une variable de chaîne est spécifiée, l'élément **call** exécutera tous les éléments enfants qu'il peut avoir si la valeur de chaîne se résout à un élément d'association après l'exécution de l'élément de correspondance nommé. • Si aucun élément **match** correspondant à la valeur de chaîne n'est trouvé, aucune action n'est exécutée.

Fonctions de consignation

Cette rubrique donne les définitions de langue des fonctions de consignation du parser Flex.

Les fonctions de consignation permettent à un parser flex d'écrire dans un log système. Les fonctions de consignation peuvent être extrêmement utiles pour créer un parser flex, mais doit être maintenu à un minimum absolu lorsqu'un parser flex est déployé sur un système de production.

Définition de langue

Node Name	Nom de l'attribut	Description
failure		Consigne un message dans le log système avec le niveau de log **Échec.**
	value	Chaîne à inclure en tant que message de log.
warning		Consigne un message dans le log système avec le niveau de log **Avertissement.**
	value	Chaîne à inclure en tant que message de log.
info		Consigne un message dans le log système avec le niveau de log **Info.**
	value	Chaîne à inclure en tant que message de log.
debug		Consigne un message dans le log système avec le niveau de log **Débogage.**
	value	Chaîne à inclure en tant que message de log.

Nodes

Cette rubrique donne les définitions linguistiques des nœuds du parser Flex.

Définition linguistique des nœuds

Node Name	Nom de l'attribut	Description
parsers		Nœud racine de chaque fichier de définition.
	xmins:xsi	Définit l'espace de nommage à utiliser pour l'inclusion du schéma. Cet attribut n'est pas requis. Toutefois, la définition linguistique n'est pas possible sans lui. Ce nœud doit avoir la valeur suivante : http://www.w3.org/2001/XMLSchema-instance
	xsi:noNamespaceSchemaLocation	Définit le fichier de validation du schéma XSD permettant de valider la définition linguistique. Cet attribut n'est pas requis. Toutefois, la définition linguistique n'est pas possible sans lui. Ce nœud doit avoir la valeur suivante : parsers.xsd
parser		Nœud qui définit une seule définition d'analyseur. Ce nœud doit se trouver directement sous le nœud parsers. Il peut y en avoir plusieurs par fichier.
	name	Nom qui identifie de manière unique l'analyseur. Ce nom doit être court et succinct. Il est utilisé par le système pour l'activation et la désactivation. Il ne doit contenir que les lettres [a-z] et [A-Z].
	desc	Fournit une description conviviale de la fonction de l'analyseur.
	service	Le numéro unique attribué à la session, lorsqu'il est identifié.
declaration		Détermine la définition. Chacune de ces définitions peut avoir une entrée match correspondante.

Node Name	Nom de l'attribut	Description
token		Spécifie une définition permettant d'identifier un token au sein du protocole de session. Définit un rappel `match` lorsque les tokens spécifiés figurent dans une session de charge utile. La position `read` est définie sur l'octet immédiatement après la correspondance de token.
	name	Il s'agit d'un identifiant unique pour la déclaration.
	value	Il s'agit de la valeur de token exacte à identifier.
	options	Les options spécifient que le token doit commencer sur une nouvelle ligne ou à une extrémité de ligne (`linestart` ou `linestop`).
meta-callback		Enregistre un rappel pour l'analyseur flex à chaque création d'un méta de format spécifique. Il peut être plus qualifié pour générer des rappels uniquement pour les sessions qui ont été identifiées en tant que apptype spécifique (par exemple, 80 pour HTTP).
	name	Nom de la correspondance d'élément à exécuter lorsqu'un rappel se produit. (Chaîne)
	key	Nom de la clé méta qui génère des rappels. (Chaîne)
	format	Type de données de la clé méta qui génèrera la méta.
	apptype	Le rappel de méta est uniquement généré si la session en cours d'analyse a été identifiée avec le paramètre apptype spécifié. (Entier non signé, facultatif)
number		Définit une variable numérique qui peut être référencée à un autre endroit de la définition de parser. Toutes les valeurs numériques sont des valeurs non signées de 64 bits.
	name	Il s'agit d'un identifiant unique pour la déclaration.

Node Name	Nom de l'attribut	Description
	`scope` (facultatif)	Spécifie quand réinitialiser la variable. Cela peut être pour chaque côté d'une session bilatérale ou uniquement après la détection d'une nouvelle session. Les valeurs possibles sont **`global`**, **`constant`**, **`stream`**, et `session` (par défaut).
`string`		Définit une variable numérique qui peut être référencée à un autre endroit de la définition de parser.
	`name`	Il s'agit d'un identifiant unique pour la déclaration.
	`scope` (facultatif)	Spécifie quand réinitialiser la variable. Cela peut être pour chaque côté d'une session bilatérale ou uniquement après la détection d'une nouvelle session. Les valeurs possibles sont **`global`**, **`constant`**, **`stream`**, et `session` (par défaut).
port		Définit un rappel **match** lorsqu'une session est trouvée à l'aide du port spécifié. La position **read** est définie sur le premier octet du premier flux (client) de la session.
	`name`	Il s'agit d'un identifiant unique pour la déclaration.
	`value`	Il s'agit du numéro de port à identifier.
`session`		Définit un rappel `match` pour les événements de début/fin de session. Ces événements ne se produisent que si un token de l'analyseur est trouvé dans la session.
	`name`	Il s'agit d'un identifiant unique pour la déclaration.
	`value`	Indique que le traitement a lieu au début d'une nouvelle session ou à la fin d'une session (`begin` ou `end`).
`stream`		Définit un rappel `match` pour les événements de début/fin de flux. Ces événements ne se produisent que si un token de l'analyseur est trouvé dans le flux.
	`name`	Il s'agit d'un identifiant unique pour la déclaration

Node Name	Nom de l'attribut	Description
	value	Indique que le traitement a lieu au début ou à la fin d'un flux (begin ou end).
function		Définit une section match qui peut être utilisée en tant que fonction générique. Aucun rappel n'est associé à cette déclaration.
	name	Il s'agit d'un identifiant unique pour la déclaration.
meta		Définit le type de données créé par l'analyseur.
	key	Spécifie le nom de la clé. La clé doit avoir une taille de 1-16 octets.
	format	Spécifie le type de variante (par exemple, **Text**, **IPv4**, **UInt32**). Reportez-vous à la documentation SDK pour obtenir la liste complète.
pattern		Définit une variable d'expression régulière à utiliser par la fonction regex
	name	Il s'agit d'un identifiant unique pour la déclaration.
	scope (facultatif)	Spécifie quand réinitialiser la variable. Cela peut être pour chaque côté d'une session bilatérale ou uniquement après la détection d'une nouvelle session. Les valeurs possibles sont **global**, **constant**, **stream**, et session (par défaut).
	value (facultatif)	Spécifie une expression régulière à attribuer au modèle de variable. Cet attribut n'est valide que si **scope attribute** est défini sur constant.

Node Name	Nom de l'attribut	Description
match		Entrées possibles pour prendre une mesure lorsqu'un critère de correspondance a été trouvé pour une déclaration. Ces nœuds peuvent être imbriqués pour fournir une logique plus profonde. Il existe plusieurs catégories d'éléments d'exécution (fonctions) qui peuvent apparaître en tant qu'enfants d'un élément : • Général • Arithmétique • String • Payload

Fonctions de charge utile

Cette rubrique donne les définitions de langue des fonctions de charge utile du parser Flex.

Ces fonctions agissent en position `read`, définie au début d'un élément `match` .

Définition de langue

Node Name	Nom de l'attribut	Description
`find`		Recherche la charge utile de flux à partir de la position read pour une valeur de chaîne fournie. Si la valeur est trouvée, le décalage par rapport à la position read est renvoyée. Tous les éléments enfants s'exécutent alors. Si la valeur n'est pas trouvée, aucun élément enfant ne s'exécutera.
	`name`	Variable `number` permettant d'avoir un décalage par rapport à la position `read` où la correspondance commence.
	`value`	Chaîne à trouver.
	`length` (facultatif)	La limite de longueur de la charge utile sera recherchée. Si aucune limite n'est indiquée, le reste de la charge utile est recherchée. Il est recommandé de toujours utiliser ici la plus faible valeur possible afin de réduire l'impact sur les performances.
`install-decoder`		Permet d'activer les jetons pour correspondre aux données de charge utile pouvant être fragmentées ou chiffrées. Un décodeur d'analyse peut être installé sur une section de pré-traitement de la charge utile avant analyse pour les jetons. Par exemple, une réponse HTTP qui utilise le codage de transfert segmenté avec le chiffrage de contenu gzip. En analysant l'en-tête HTTP, les paramètres de type, de décalage et de longueur nécessaires peuvent tous être définis, après quoi la charge utile de la réponse HTTP s'afficherait dans l'analyse des tokens, comme si aucun chiffrement n'avait été appliqué. Toutefois, cela entraîne un temps système significatif.
	`type`	Type de décodeur à installer. Les options valides sont : gzip, deflate, chunked, chunked-gzip, chunked-deflate.
	`offset`	Décalage par rapport à la position read pour commencer le décodage.
	`length`	Longueur de charge utile maximale à décoder.
`isdecoding`		Teste si un décodeur installé est actuellement actif. Si c'est le cas, tous les enfants de cette fonction s'exécutent. Cette fonction ne comporte pas de paramètres.

Node Name	Nom de l'attribut	Description
move		Déplace la position read vers l'avant dans le flux actuel en fonction d'un nombre spécifié d'octets. Si le flux contient suffisamment de données, la position read est mise à jour et tous les éléments enfants s'exécuteront par la suite. Si la valeur n'est pas trouvée, la position read reste inchangée et aucun élément enfant ne s'exécutera.
	value	Nombre d'octets pour déplacer la position read.
	direction (facultatif)	Sens de déplacement de la position read actuelle. Peut être forward (par défaut) ou **reverse.**
packetid		Renvoie l'ID du paquet de la position read actuelle. Le résultat peut être 0, ce qui indique que l'ID de paquet ne pourrait pas être déterminé.
	name	Variable numérique permettant de recevoir l'ID de paquet actuel.
payload-position		Renvoie la position read actuelle. Il s'agit d'un index basé sur zéro dans la charge utile de flux.
	name	Variable numérique permettant de recevoir la position read actuelle.
read		Lit un nombre spécifié d'octets commençant à la position read dans une variable. Si le flux contient suffisamment de données, la position read est mise à jour, la lecture des données est définie, et tous les éléments enfants s'exécutent. Si la valeur n'est pas trouvée, la position read reste inchangée et aucun élément enfant ne s'exécutera.
	name	Nom d'une variable string ou number permettant de recevoir des données de flux. Si une variable number est fournie, les octets lus sont interprétés comme une valeur numérique non signée unique.
	length	Nombre d'octets à lire à partir d'un flux.
	endianess (facultatif)	Ordre des octets à utiliser lors de la lecture dans une variable numérique. Peut être big (par défaut) ou little. L'attribut n'est pas valide lors de la lecture dans une variable string.

Regex

Cette rubrique donne les définitions linguistiques du nœud regex du parser Flex.

Dans la charge utile de flux commençant à la position `read`, Regex recherche les occurrences d'une expression régulière fournie. Si des occurrences sont trouvées, le décalage par rapport à la position `read`, et éventuellement la chaîne correspondante, est retournée. Tous les éléments enfants s'exécutent. Si aucune occurrence n'est trouvée, les éléments enfants ne s'exécutent pas.

Définition de langue

Nom de l'attribut	Description
`name`	Variable `number` permettant d'avoir un décalage par rapport à la position `read` où la correspondance commence.
`value`	Expression régulière à trouver.
`length` (facultatif)	La limite de longueur de la charge utile sera recherchée. Si aucune limite n'est indiquée, le reste de la charge utile est recherchée. Il est recommandé de toujours utiliser ici la plus faible valeur possible afin de réduire l'impact sur les performances.
`found` (facultatif)	Nom d'une variable `string` qui reçoit une chaîne correspondante.

Fonctions de chaîne

Cette rubrique donne les définitions linguistiques des fonctions de chaîne du parser Flex.

Définition de langage de fonctions de chaîne

Node Name	Nom de l'attribut	Description
append		Ajoute un chiffre ou une chaîne à la fin d'une variable string.
	name	Identifiant unique d'une variable de chaîne à laquelle la valeur spécifiée est rattachée.
	value	Chiffre ou chaîne à rattacher.
find		Recherche la valeur de chaîne fournie dans une chaîne. Si elle est trouvée, la position est renvoyée et tous les éléments enfants s'exécuteront. Autrement, les éléments enfants ne s'exécuteront pas.
	name	Variable number permettant de recevoir la position basée sur zéro, dans laquelle la chaîne de valeur fournie a été trouvée dans la chaîne **in**.
	value	Chaîne à trouver.
	in	Chaîne à rechercher.
	length (facultatif)	Limite de longueur de la chaîne **in** à rechercher. Si aucune limite n'est fournie, la recherche sera effectuée dans toute la chaîne **in**.
length		Attribue la longueur d'une chaîne à une variable number.
	name	Variable number pour recevoir la longueur de la chaîne spécifiée.
	value	Valeur de la chaîne dont la longueur doit être déterminée.
regex		Recherche des correspondances avec l'expression régulière fournie dans une chaîne. Si une correspondance est trouvée, la position et, éventuellement, la chaîne correspondante sont renvoyées. Tous les éléments enfants s'exécutent alors. Si la valeur n'est pas trouvée, aucun élément enfant ne s'exécutera. Les opérations d'expression régulière peuvent avoir un impact négatif sur les performances système.
	name	Variable sous forme de chiffre pour recevoir la position basée sur zéro, dans laquelle l'expression régulière fournie avait une correspondance dans la chaîne in.

Node Name	Nom de l'attribut	Description
	value	Expression régulière à rechercher.
	in	Chaîne à rechercher.
	length (facultatif)	Limite de longueur de la chaîne in à rechercher. Si aucune limite n'est fournie, la recherche sera effectuée dans toute la chaîne **in**.
	found (facultatif)	Nom de la variable de chaîne pour recevoir la chaîne associée.
substring		Au moins l'un des attributs facultatifs from et length doit être spécifié.
	name	Identifiant unique d'une variable de chaîne pour recevoir la valeur extraite.
	value	Valeur de chaîne à partir de laquelle extraire une sous-chaîne.
	from (facultatif)	Position basée sur zéro à partir de laquelle la sous-chaîne commence. Si elle n'est pas spécifiée, sa valeur est de zéro par défaut.
	length (facultatif)	Nombre de caractères à extraire. S'il n'est pas spécifié, la valeur par défaut est la longueur restante de la chaîne.
tolower		Convertit une chaîne en lettres en minuscules uniquement.
	name	Nom d'une variable string à traiter.
toupper		Convertit une chaîne en lettres en majuscules uniquement.
	name	Nom d'une variable string à traiter.
urldecode		Décode une chaîne contenant des caractères codés URL.
	name	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne d'URL chiffrée à décoder.
base64decode		Décode une chaîne codée base 64.
	name	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne d'URL chiffrée à décoder.
uudecode		Décode une chaîne uuencode.
	name	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne uuencode. Les lignes d'en-tête et de fin ne doivent pas être incluses.

Node Name	Nom de l'attribut	Description
quotedprintabledecode		Décode une chaîne codée Quoted-printable.
	name	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne codée Quoted-printable.
convert-ebcdic		Convertit une chaîne EBCDIC en son équivalent ASCII.
	name	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne d'URL chiffrée à décoder.

Parsers GeoIP2 et GeoIP

Cette rubrique décrit les parsers GeoIP2 et GeoIP pour les décodeurs. Vous ne pouvez activer qu'un seul de ces parsers à un moment donné. Ces deux parsers convertissent les adresses IP en emplacements géographiques, tels que le nom du pays et la ville où l'adresse IP est généralement située.

Parser GeoIP2

Disponible dans NetWitness Platform la version 11.2 ou ultérieure, le parser GeoIP2 est activé par défaut pour les mises à niveau et les nouvelles installations. Le parser GeoIP2 fournit le dernier package MaxMind GeoIP et prend en charge les adresses IPv6, ainsi que IPv4.

La configuration du parser GeoIP2 peut être modifiée en procédant comme suit :

1. Accédez à **ADMIN** > **Services**.
2. Dans la vue **Services d'administration**, sélectionnez un Log Decoder ou un Decoder.
3. Cliquez sur l'icône Paramètres () et sélectionnez **Vue** > **Configuration**. Le panneau Configuration des parseurs s'affiche, à partir duquel vous pouvez sélectionner **GeoIP2** pour afficher et mettre à jour les options de configuration.

Vous pouvez définir les adresses IP à rechercher. Le parseur GeoIP2 active les adresses IP suivantes par défaut : `ip.src`, `ip.dst`, `ipv6.src` et `ipv6.dst`. Vous pouvez toutefois mettre à jour les options en utilisant `parsers.options` pour supprimer ou ajouter de nouvelles adresses IP. Par exemple, vous pouvez modifier `parsers.options` et passer une liste d'adresses IP séparées par des virgules à utiliser comme suit :
`GeoIP2="ipaddr=ip.src,ip.dst,ipv6.src,ipv6.dst,ip.addr"`
Cela ajoutera une nouvelle adresse IP à la recherche appelée `ip.addr`. Toutefois, `ip.addr` ne se termine pas par `.src` ou `.dst`. Le parseur choisira donc de placer les métadonnées GeoIP2 générées dans les métadonnées sans suffixe `.src` ou `.dst`. Ainsi, vous pouvez voir le pays, la ville, et ainsi de suite, après les métadonnées `ip.addr`.

Remarque : La liste que vous transmettez pour `ip.addr` remplace la liste par défaut. Donc, si vous transmettez `ipaddr=ip.src`, il générera des métadonnées GeoIP2 uniquement pour `ip.src` à l'exclusion de toute autre adresse IP.

Remarque : `parsers.options` est utilisé pour transmettre des options à plusieurs parsers. Donc, si vous ajoutez GeoIP2, vous ne devez pas supprimer les autres options transmises à d'autres parser (comme l'entropie).

Le tableau suivant fournit la liste complète des métadonnées que le parseur GeoIP2 peut potentiellement générer et indique quelles métadonnées sont ou non activées par défaut :

Activée par défaut	Non activée
country, country.src, country.dst	latdec, latdec.src, latdec.dst
	longdec, longdec.src, longdec.dst
domain, domain.src, domain.dst	isp, isp.src, isp,dst
org, org.src, org.dst	city, city.src, city.dst

Vous pouvez activer les autres métadonnées à l'aide des configurations de parser standard.

Remarque : En désactivant certaines métadonnées par défaut, le parser GeoIP2 ne fonctionne pas de la même façon que le parser GeoIP (qui n'a pas, par défaut, désactivé les métadonnées qu'il a générées). Si vous avez besoin d'une des métadonnées désactivées, vous devrez les activer (une seule fois) pour chaque Decoder, après la mise à niveau vers 11.2 ou une version ultérieure. Gardez à l'esprit que les champs de métadonnées `isp` et `org` produisent généralement une valeur équivalente à `domain`.

Parser GeoIP

Le parser GeoIP est un parser plus ancien disponible dans les versions précédentes de NetWitness Platform, mais il est toujours pris en charge en plus du parser GeoIP2 plus récent. Pour modifier la configuration du parser, les utilisateurs peuvent modifier ses options à partir d'ici : Vue Configuration des services > Fichiers > `GeoPrivate.ipl`.

Les métadonnées de géolocalisation dans `GeoPrivate.ipl`, sont ajoutées pour `ip.src` et `ip.dst`. Le parser utilise deux fichiers de données externes, `GeoCity.dat` et `GeoCountry.dat`, qui sont tous deux stockés dans le répertoire de l'application. Comme indiqué dans le tableau ci-dessous, il existe jusqu'à huit métadonnées pour chaque adresse IP.

Métadonnées	Description
city.dst	Ville de destination
city.src	Ville source
country.dst	Pays de destination
country.src	Pays source
latdec.dst	Latitude décimale de destination
latdec.src	Latitude décimale source
longdec.dst	Longitude décimale de destination
longdec.src	Longitude décimale source

Parsers Lua

L'un des fichiers qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers est **`NwLua.xml`**, le parser Lua.

Liste des parsers Lua

Il existe un certain nombre de parsers Lua disponibles dans Live. Voir Contenu RSA pour :

- la liste complète de ces parsers ;
- leurs interdépendances ;
- les parsers Flex intégrés par chaque parser Lua.

Voici cinq opérations courantes de parser :

- Faire correspondre le port et identifier immédiatement
- Faire correspondre le port et retarder l'identification
- Faire correspondre le token et identifier immédiatement
- Faire correspondre plusieurs tokens
- Faire correspondre le token et créer les métadonnées

Parsers Snort

Les règles et la `parsers/snort` configuration Snort® sont ajoutées au répertoire pour la procédure d'enquête et le Decoder. Le Decoder prend en charge les capacités de détection de charge utile des règles Snort. Les fichiers de règles doivent avoir l'extension `.rules` et les fichiers de configuration doivent avoir l'extension `.conf`. L'implémentation par le Decoder des règles Snort est centrée sur l'utilisation des chaînes de contenu définies dans une règle Snort en tant que token. Une fois qu'un token est associé, l'en-tête de règle et les options de règle supplémentaires peuvent être évalués. Actuellement, les règles qui ne définissent pas de contenu (via les options de règle `content` ou `uricontent`) ne sont pas prises en charge.

Configuration

Les fichiers de configuration sont chargés avant les règles de chargement.

Options de configuration	Description
Définitions de variable	**Description**
`ipvar`	Le langage complet de définition des variables d'adresse IP est pris en charge, y compris les listes, CIDR et la négation.
`portvar`	Le langage complet de définition des variables d'adresse IP est pris en charge, y compris les listes, les plages et la négation.
`var`	Non supporté ; utiliser `ipvar` ou `portvar`.
Définitions d'action	**Description**
`ruletype`	La définition de `ruletypes` supplémentaire est prise en charge. Toutefois, seules les règles qui ont un type de règle de base `alert` sont prises en charge.
Configuration générale	**Description**
`nopcre`	Cette option de configuration désactive toutes les règles avec `pcre`.

Règles

Les règles Snort sont analysées et chargées lorsque PCS est chargé (toute importation ou capture dans l'Enquêteur, début de capture initiale et recharge du parser dans Decoder).

- Toute règle qui n'est pas correctement analysée est ignorée.
- Toute règle Snort valide doit effectuer des analyses réussies ; toutefois, il existe des options de règle, qui ne sont pas prises en charge par Decoder, qui ne sont pas entièrement analysées.

Section	Description
En-tête	Les conditions d'en-tête sont évaluées lorsqu'une règle reçoit le premier rappel de token pour un flux. L'en-tête est évalué une fois par flux et empêche toute prise en compte d'une règle par rapport à un flux spécifique si les conditions ne sont pas remplies.
Actions	L'action spécifiée ou une règle doit être définie (soit l'une des actions Snort natives, soit définie dans la configuration à l'aide de l'instruction `ruletype`) pour que la règle soit considérée comme valide. Decoder utilise uniquement des règles avec des actions d'alerte.
Protocoles	Decoder prend en charge les mots clés du protocole Snort actuel (`tcp`, `udp`, `icmp`, `ip`).
Adresses IP	Le langage complet de définition des adresses IP est pris en charge, y compris les listes, CIDR et la négation.
Numéros de port	Le langage complet pour la définition des numéros de port est pris en charge, y compris les listes, les plages et la négation.
Opérateur directionnel	L'opérateur directionnel prend en charge les valeurs from-to ('->') et bidirectionnelles (‘<>’). La valeur to-from ('<-') n'est pas valide et entraînera un échec du chargement de la règle.

Options générales

Decoder utilise les options de règle générales Snort suivantes :

Option	Description
`msg`	Si la règle correspond, la valeur `msg` est ajoutée en tant que métadonnée `risk.info`, `risk.warning` ou `risk.suspicious`, selon la priorité de la règle.
`sid`	Si la règle correspond, la valeur `sid` est ajoutée en tant que métadonnée.
`classtype`	Si la règle correspond, le nom `classtype` est ajouté en tant que métadonnée `threat.cat`.
`priority`	Si la règle correspond et qu'elle a une option `priority`, elle est utilisée pour déterminer le type de métadonnée à risque associé à la valeur `msg`.

Options de charge utile

Decoder prend en charge les options de règle de charge utile suivantes.

Option	Description
`content`	L'option `content` crée un token pour faire correspondre Decoder. Seuls les tokens de trois octets ou plus sont acceptés. Il est également important de noter que Decoder diffère de Snort en ce que les règles sont évaluées par rapport à la charge utile du flux reconstruit et non pas seulement d'un seul paquet. Cela peut entraîner des différences dans les correspondances de règles entre Snort et Decoder, en particulier lors de l'examen des options de position.
`nocase`	Actuellement non pris en charge. Cette option est ignorée et la sensibilité à la casse est utilisée.
`depth`	Cette option est appliquée à la distance du token depuis le début du flux. Si la position du token est supérieure à cette valeur, il ne s'agit pas d'une correspondance.
`offset`	Cette option est appliquée à la distance du token depuis le début du flux. Si la position du token est inférieure à cette valeur, il ne s'agit pas d'une correspondance.
`distance`	Cette option est appliquée à la distance du token depuis la fin de la correspondance de token précédente. Si la position de token relative est inférieure à cette valeur, il ne s'agit pas d'une correspondance.
`within`	Cette option est appliquée à la distance du token depuis la fin de la correspondance de token précédente. Si la position de token relative est supérieure à cette valeur, il ne s'agit pas d'une correspondance.
`http_uri`	Tout token qui se démarque est vérifié afin qu'il s'inscrive dans les limites de `http_uri`, comme indiqué par le parser HTTP. Aucune normalisation d'URI n'est appliquée.
`uricontent`	Aucune normalisation d'URI n'est appliquée. Sinon, cela équivaut à l'option de contenu avec le modificateur `http_uri`.
`pcre`	Actuellement, les PCREs ne sont appliqués qu'aux URI et doivent spécifier l'option U.

Options non liées à la charge utile

Option	Description
`flow`	Vérifie que la règle est appliquée uniquement au flux de client ou de serveur.
`to_client`	Limite la règle à la correspondance uniquement sur un flux défini par Decoder comme étant un flux serveur.

Option	Description
from_server	Synonyme de to_client.
from_client	Limite la règle à la correspondance uniquement sur un flux défini par Decoder comme étant un flux client.
flowbits	Maintient un état de session et sont réinitialisés à la fin de chaque session.
set	Lorsque la règle correspond, le flowbit spécifié est défini.
unset	Lorsque la règle correspond, le flowbit spécifié est effacé.
toggle	Lorsque la règle correspond, le flowbit spécifié est inversé.
isset	Lorsque la règle est évaluée, l'état du flowbit spécifié doit être défini pour que la règle corresponde.
isnotset	Lorsque la règle est évaluée, l'état du flowbit spécifié ne doit pas être défini pour que la règle corresponde.
noalert	Empêche la règle de générer des métadonnées si elle correspond.

Parser Search

Cette rubrique explique comment configurer un parser personnalisé utilisé sur un Decoder pour générer des métadonnées en recherchant les mots-clés et les expressions régulières prédéfinis dans la vue configuration des services > onglet Fichiers.

L'un des fichiers qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers est **search.ini**, le parseur Search.

search.ini

Le parser Search est un parser personnalisé utilisé pour générer des métadonnées en recherchant des mots-clés et expressions régulières prédéfinis. Dans la charge utile d'une session reconstruite, le parser recherche des occurrences de chaîne et peut exécuter une recherche d'expression régulière. Vous pouvez configurer le parser en modifiant le fichier search.ini.

Attention : Le parser Search peut impacter sensiblement les performances système. Il importe de bien comprendre le mécanisme de recherche et les données auxquelles il est appliqué avant de créer des définitions de recherche et d'activer le parser Search.

La définition de recherche est utilisée pour tous les protocoles. Il existe trois méthodes de recherche de base :

- Mot-clé : Recherche un ensemble de mots spécifique dans un flux
- Pattern: Recherche une occurrence d'expression régulière dans un flux
- Mot-clé + Modèle : Recherche une expression régulière dans un flux s'il contient un ensemble de mots-clés.

Pour consulter une explication détaillée, reportez-vous à Parser Search dans la rubrique Syntaxe de chaîne Search search.ini.

Syntaxe de chaîne Search search.ini

Cette rubrique présente les méthodes de recherche et la syntaxe à utiliser dans le parser Search.

Le parser Search utilise trois méthodes de recherche de base :

- Mot-clé : Recherche un ensemble de mots spécifique dans un flux.
- Pattern: Recherche une occurrence d'expression régulière dans un flux.
- Mot-clé + Modèle : Recherche une expression régulière dans un flux s'il contient un ensemble de mots-clés.

Syntaxe

```
Maxrecon=<max_size>Maxsearch=<max_ssearch_length>MatchLimit=<max_matches_per_
stream
Search Name
Services=<service_id_list>Keywords=<keyword_list>|Pattern=<expression>Case=0|1
Proximity=<number_of_bytes>Recon=0|1
Raw=0|1
```

Paramètres

Paramètres utilisés dans cette commande :

Paramètre	Description
`autocheck`	Corrige automatiquement tous les problèmes en mode sans invite
`header Only`	Vérifie/affiche l'en-tête de chaque fichier
`chatty`	Affiche un vidage hexadécimal de chaque objet du fichier (quantité importante de données)
`dump#-#`	Indique à un objet ou une plage d'objets de base zéro du fichier de sortir en hexadécimal sur la console

Exemple

Voici un exemple de la commande :

Vérifier tous les fichiers de la base de données NetWitness situés dans la collection nommée Default. Si des problèmes sont trouvés, la commande décrira le problème et vous demandera si vous souhaitez le corriger.

```
dbcheck C:\Documents and Settings\User\My Documents\NetWitness\
Investigations\Default\*.nw*
```

Configuration LAN sans fil

Cette rubrique présente le fichier de configuration LAN sans fil pour les Decoders, qui se trouve dans la vue Configuration des services > onglet Fichiers.

wlan-config.xml

L'un des fichiers qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers est **`wlan-config.xml`**, le fichier de configuration LAN sans fil.

Il contrôle les parsers 802.11. Son objectif principal est de contrôler le déchiffrement de trames brutes 802.11 capturées par le Decoder. Ce fichier est facultatif. Si le déchiffrement du trafic 802.11 n'est pas souhaité, il n'est pas nécessaire de créer le fichier.

Il existe cinq parsers de liaison liés à la capture de paquets LAN sans fil :

- Parser IEEE 802.11 (trames et balises de données uniquement)
- Radiotap avec en-tête 802.11
- Absolute Value Systems (AVS) avec en-tête 802.11
- Prism II avec en-tête 802.11
- CACE's ″Per Packet Information″ (PPI) avec en-tête 802.11

Les parsers sans fil 802.11 introduits dans la version 9.8 partagent le même fichier de configuration. Ce fichier wlan-config.xml est utilisé pour définir les points d'accès sans fil dont l'utilisateur peut disposer sur le réseau, et son objectif principal est de contrôler le déchiffrement. Le BSSID du point d'accès et le SSID pour lequel il fait autorité est ajouté à ce fichier ainsi que toutes les clés par défaut actives utilisées par le point d'accès.

Références de Decoder et Log Decoder

Il s'agit d'un ensemble de références qui fournissent des informations sur l'interface utilisateur pour les Decoders et Log Decoders dans NetWitness Platform, avec des références aux procédures qui décrivent le travail que vous pouvez effectuer dans cette partie de l'interface utilisateur. Ces rubriques sont présentées par ordre alphabétique.

Rubriques

Vue Configuration des services - onglet Confidentialité des données

Dans l'onglet Confidentialité des données (**ADMIN > Services > Sélectionner un Decoder ou un Log Decoder >** ⚙ **> Config > onglet Confidentialité des données)**, les administrateurs peuvent configurer les paramètres de confidentialité des données pour certains services Core. Pour Decoder et Log Decoder, vous pouvez définir l'algorithme de hachage par défaut et la valeur salt.

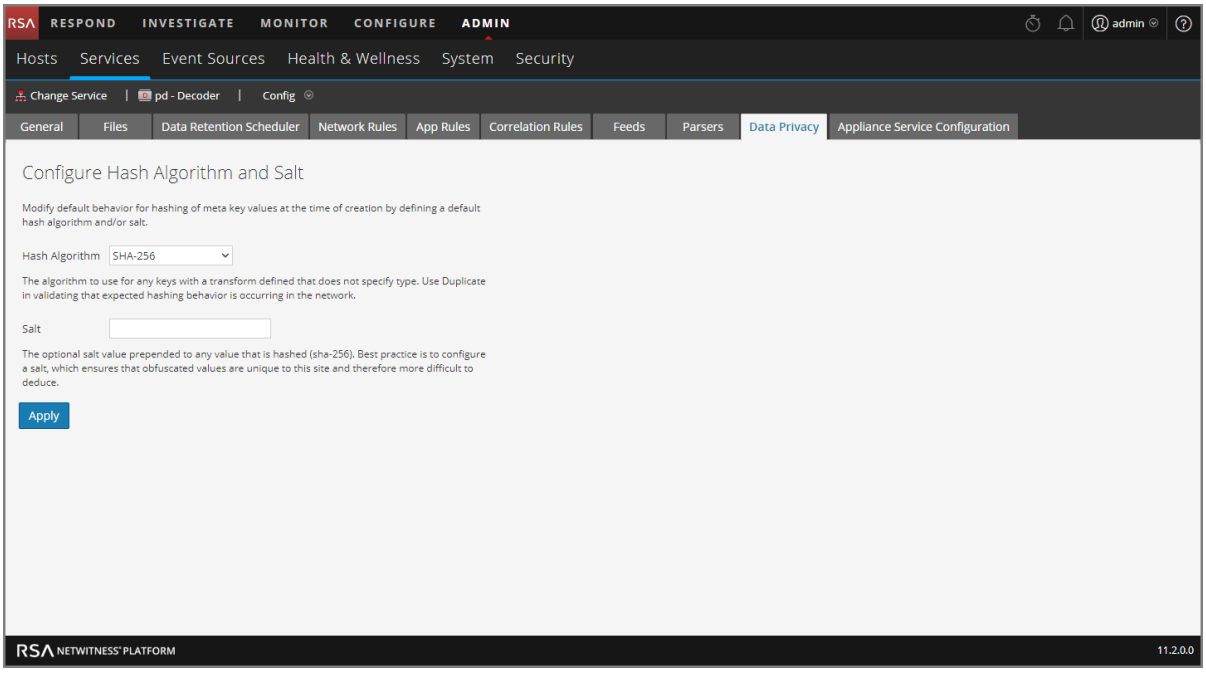
Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	configurer l'algorithme de hachage et la valeur Salt	« Configurer l'algorithme de hachage et la valeur Salt » dans le *Guide de gestion de la confidentialité des données*. (Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.)

Rubriques connexes

- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder

Aperçu rapide



L'onglet Confidentialité des données comporte les paramètres de configuration Configurer l'algorithme de hachage et le sel. Le tableau suivant décrit les paramètres de ce menu.

Paramètre	Description
Algorithme de hachage	Affiche une liste déroulante des algorithmes de hachage à utiliser pour toutes les clés avec une transformation qui ne précise pas le type d'algorithme. Les valeurs possibles sont SHA-256 et Duplicate. Duplicate est un algorithme spécial, disponible aux administrateurs pour valider que le comportement de ce hachage doit bien se produire sur le réseau. Dans les versions de NetWitness Platform antérieures à 10.5, SHA-1 était disponible comme algorithme de hachage, mais RSA ne recommande pas l'utilisation de SHA-1.
Salt	Indique la valeur salt facultative à ajouter comme préfixe à une valeur qui est hachée. Les bonnes pratiques de sécurité recommandent une valeur salt de 100 bits minimum ou 16 caractères de long. La configuration d'une valeur assure que les valeurs obscurcies sont uniques à ce site et donc plus difficiles à déduire. Pour plus d'informations sur ce champ, consultez la rubrique « Configurer l'obfuscation des données » dans le *Guide de gestion de la confidentialité des données*.
Appliquer	Applique les modifications.

Vue Configuration des Services - Planificateur de rétention des données

Sous l'onglet Vue Configuration des Services - Planificateur de rétention des données, vous pouvez définir les critères de déploiement pour supprimer des enregistrements de base de données à partir du stockage principal à l'aide d'un seuil d'âge. Vous pouvez également planifier un délai pour vérifier si le seuil est atteint.

Pour accéder à l'onglet Planificateur de rétention des données, accédez à **ADMIN** > **Services** > sélectionnez un service **Decoder** ou **Log Decoder** zt cliquez sur > **Vue** > **Config** > **Rétention de données**.

Que voulez-vous faire ?

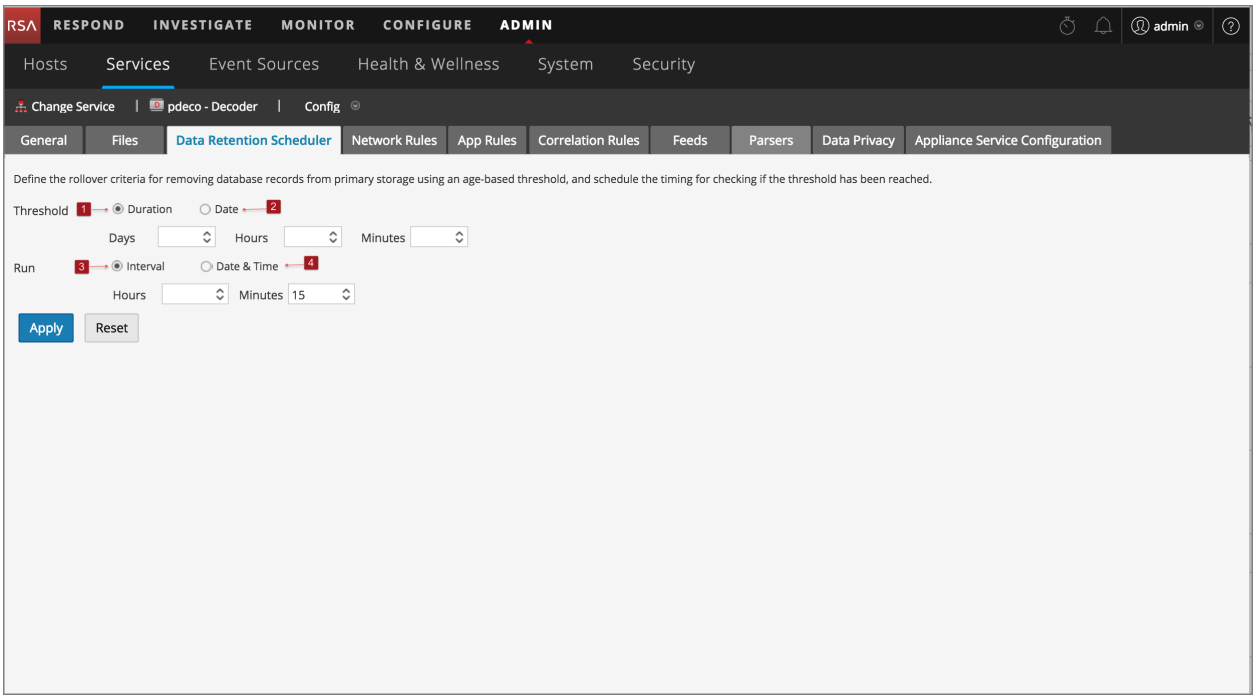
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	planifier un délai pour vérifier si le seuil est atteint.	Configurer la gestion des transactions sur un Decoder

Rubriques connexes

- Configurer les paramètres communs sur un Decoder
- Configuration rapide de Decoder et de Log Decoder

Aperçu rapide

Il s'agit d'un exemple de l'onglet Planificateur de rétention des données.



1	**Durée du seuil** : Supprime les fichiers de base de données plus anciens que le nombre de jours, minutes ou heures sélectionné.
2	**Date du seuil** : Supprime les fichiers de base de données plus anciens que la date UTC sélectionnée (AAAA-MM-JJ HH:MM:SS), qui ne sont pas compatibles avec les paramètres de minutes, heures ou jours.
3	**Intervalle d'exécution** : Indique le nombre d'heures entre les exécutions.
4	**Date et heure de l'exécution** : Définit quels jours de la semaine doit s'exécuter le planificateur, et l'heure de l'exécution au format HH:MM:SS pour l'heure locale du service.

Vue Configuration des services - onglet Feeds

Les feeds et les analyseurs sont des programmes Lua qui sont chargés et compilés lors du traitement des fichiers de capture dans le module Investigation ou lors de la capture de données avec des Decoders. Généralement, ils sont utilisés pour l'extraction de métadonnées statiques et l'identification des services.

Remarque : Les versions de NetWitness antérieures à 11.0 utilisaient des programmes FLEXPARSE en plus des programmes Lua ; les flexparsers sont obsolètes dans NetWitness Platform 11.0. Sauf indication contraire, toutes les références aux Decoders s'appliquent également aux Log Decoders.

NetWitness Platform utilise des feeds pour créer des métadonnées sur la base des métadonnées définies en externe. Un feed est une liste de données qui sont comparées à des sessions au fur et à mesure de leur capture ou de leur traitement. Pour chaque correspondance, d'autres métadonnées sont créées. Ces données permettent d'identifier et de classer les adresses IP malveillantes ou d'intégrer les informations complémentaires comme les noms de services et les emplacements en fonction des assignations de réseau internes. Certains exemples de feeds comprennent les feeds de menaces pour identifier les BOTNets, les mappages DHCP ou même des informations Active Directory comme les emplacements physiques ou les départements logiques.

Les feeds peuvent être ajoutés, supprimés et mis à jour alors qu'un Decoder est en cours d'exécution sans que cela ait d'impact sur la capture. L'onglet Feeds (**ADMIN > Services >** sélectionnez un service et cliquez sur > **Vue > Config > onglet Feeds**) propose une interface utilisateur pour gérer les feeds sur les Decoders.

Que voulez-vous faire ?

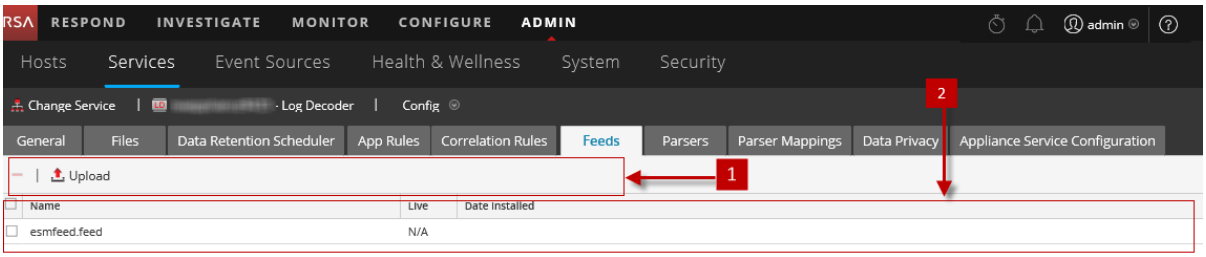
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	configurer les feeds	Configurer les feeds et les parsers
Administrateur	activer et désactiver les analyseurs	Activer et désactiver les analyseurs et les analyseurs de logs

Rubriques connexes

- Configurer les paramètres communs sur un Decoder
- Configuration rapide de Decoder et de Log Decoder
- Boîte de dialogue Télécharger les feeds
- Références de feed et d'analyseur

Aperçu rapide

Voici un exemple de l'onglet Feeds.



1 Barre d'outils de l'onglet Feeds - Comporte des options permettant d'utiliser les feeds dans la grille

2 Grille Feed - Répertorie tous les feeds actuellement déployés sur le Decoder

Barre d'outils de l'onglet Feeds

Fonctionnalité	Description
Upload	Affiche la boîte de dialogue Télécharger les feeds.
−	Supprime les feeds sélectionnés.

Liste de feeds

La liste Feeds répertorie tous les feeds actuellement déployés sur le Decoder.

Colonne	Description
Nom	Nom du feed ou fichier de feed.
Live	Indique si le feed provient de Live. Les valeurs possibles sont **Oui**, **Non** ou **N/A**. • **Oui** = Installé via Live • **Non** = Installé via NetWitness Platform • **N/A** = Le feed n'a pas de fichier d'attribut créé par NetWitness Platform pour effectuer le suivi de la date d'installation. Il se peut que le feed ait été installé manuellement et non via NetWitness Platform ou Live Services. Les feeds installés manuellement fonctionnent encore correctement.
Date d'installation	Date à laquelle le feed a été transmis au service.

Boîte de dialogue Télécharger les feeds

Cette rubrique décrit les fonctions de la boîte de dialogue Télécharger les feeds dans la vue Configuration des services > onglet Feeds.

Dans la vue Configuration des services, cliquez sur l'option **Télécharger** de l'onglet Feeds pour accéder à la boîte de dialogue Télécharger les feeds. Vous pouvez y gérer le téléchargement des feeds sur un Decoder ou un Log Decoder.

Que voulez-vous faire ?

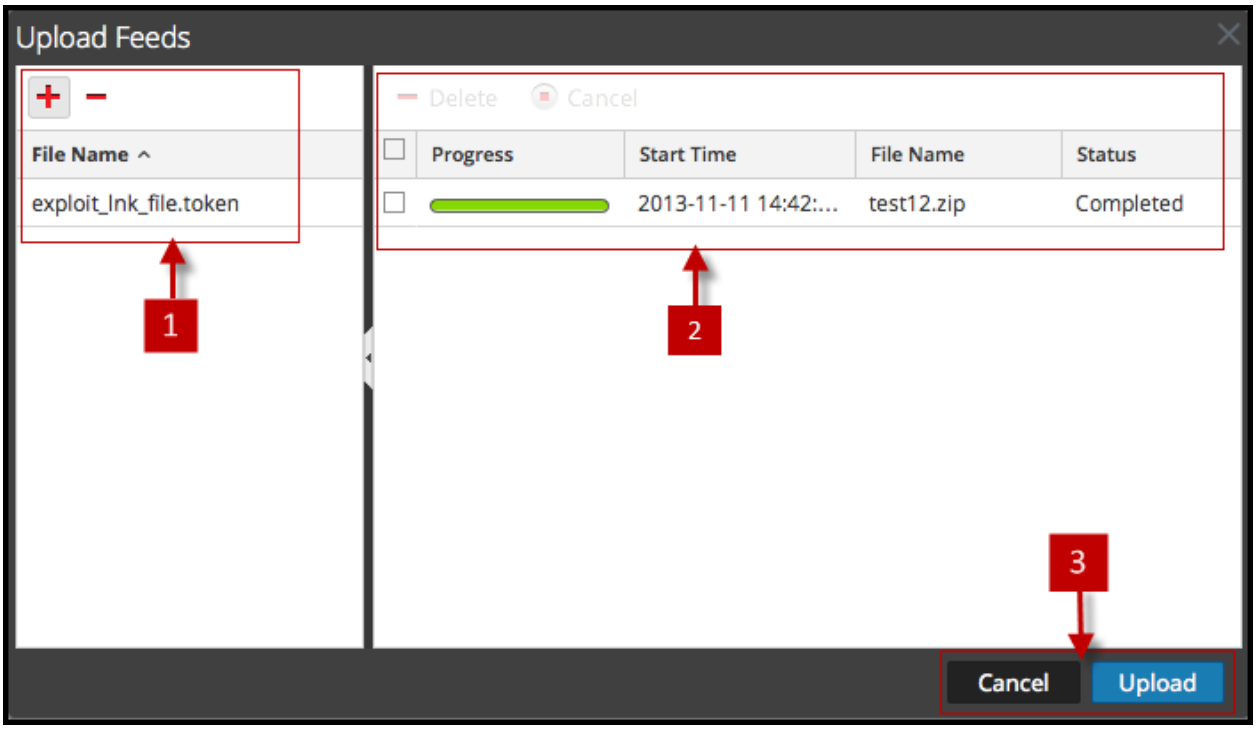
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	préparer une liste de feeds à télécharger	Modifier, télécharger ou supprimer un feed
Administrateur	afficher et supprimer des tâches de téléchargement	Modifier, télécharger ou supprimer un feed

Rubriques connexes

- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder
- Références de feed et d'analyseur

Aperçu rapide

Voici un exemple de la boîte de dialogue Télécharger les feeds.



1 Liste de fichiers - Permet de préparer une liste de feeds à télécharger
2 Liste de tâches de téléchargement - Fournit une vue des tâches de téléchargement
3 Boutons de la boîte de dialogue Télécharger les feeds

Liste de fichiers

La liste de fichiers permet de préparer la liste des feeds à télécharger. Vous pouvez ajouter des fichiers à partir d'une structure de répertoire, et supprimer des fichiers d'une grille si vous décidez que vous ne souhaitez pas télécharger un fichier particulier. Lorsque cette liste est prête, cliquez sur **Télécharger** pour lancer le téléchargement.

Fonctionnalité	Description
+	Ouvre une vue de la structure de répertoires dans laquelle vous pouvez sélectionner les fichiers à ajouter à la liste de fichiers.
−	Supprime les fichiers sélectionnés de la liste de fichiers.
Nom du fichier	Répertorie les fichiers de feed d'un système de fichiers que vous avez ajoutés en vue de leur téléchargement dans un Decoder. Lorsque vous cliquez sur **Télécharger**, les fichiers répertoriés ici sont téléchargés.

Liste de tâches de téléchargement

La liste de tâches de téléchargement affiche les tâches de téléchargement que vous avez lancées en cliquant sur **Télécharger**.

Fonction/Colonne	Description
Delete	Supprime une tâche de téléchargement.
Progression	Affiche l'avancée d'une tâche de téléchargement.
Heure de début	Affiche l'heure de début d'une tâche de téléchargement.
Nom du fichier	Répertorie les noms de fichiers du feed téléchargé.
État	Affiche l'état de la tâche de téléchargement.

Boutons de la boîte de dialogue Télécharger les feeds

Fonctionnalité	Description
Annuler	Ferme la boîte de dialogue Télécharger les feeds.
Télécharger	Démarre le téléchargement des fichiers de feed répertoriés dans la liste de fichiers. Chaque feed est indiqué sur une ligne distincte dans la liste Processus de téléchargement.

Vue Configuration des services - onglet Fichiers

Les fichiers de configuration de Decoder et Log Decoder sont visibles et modifiables dans la vue Configuration de services > onglet Fichiers. La section « Modifier les fichiers de configuration des services Core » dans le *Guide de mise en route des hôtes et des services* fournit des instructions générales sur la modification des fichiers. (Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.)

À l'instar des autres services Core, le Decoder et le Log Decoder comportent un fichier d'index, et peuvent également avoir un rapporteur d'incidents, un netwitness et un planificateur. Les fichiers d'index Decoder et Log Decoder sont nommés **`index-decoder-custom.xml`** et **`index-logdecoder-custom.xml`.**

Remarque : Ce type de fichier est disponible uniquement pour Log Decoder avec un contenu Envision installé. `Table-map.xml` et `table-map-custom.xml` ne s'affichent désormais que si `table-map.xml` a été détecté sur le système de fichiers (par exemple, il peut s'agir d'un Log Decoder avec un contenu envision installé).

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	obtenir des fichiers logs à partir d'une version antérieure à 11.0Log Decoder	Obtenir des fichiers Log à partir d'un Log Decoder pré-11.0
Administrateur	modifier les fichiers et les analyseurs	Références de feed et d'analyseur

Rubriques connexes

- Configurer les paramètres communs sur un Decoder
- Configuration rapide de Decoder et de Log Decoder
- Créer des clés méta personnalisées à l'aide d'un feed personnalisé

Aperçu rapide

Nom de fichier	Description
`GeoPrivate.ipl`	Cet analyseur fixe prend les adresses IP et les convertit en lieux géographiques. Les emplacements s'affichent via Google Earth.
`feed-definitions.xml`	Utilisé pour créer des feeds personnalisés, il s'agit du schéma XML utilisé par le Decoder pour définir un message **feed** lors de la création d'un fichier **.feed** .

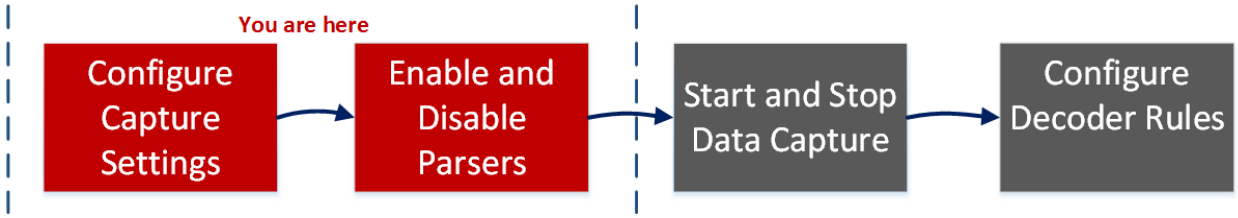
Nom de fichier	Description
`traffic_flow_options.lua`	Utilisé pour fournir des informations d'orientation. Mettez à jour ce fichier avec des sous-réseaux internes et externes propres à l'environnement pour l'analyseur Lua pour créer une orientation appropriée dans les métadonnées. L'analyseur est décrit dans RSA Content for RSA NetWitness Platform.
`search.ini`	Il s'agit du fichier de configuration de l'analyseur Search. L'analyseur Search est un analyseur personnalisé utilisé pour générer des métadonnées en recherchant des mots-clés et expressions régulières prédéfinis.
`wlan-config.xml`	Il s'agit du fichier de configuration LAN (9/9/2009). Ce fichier contrôle les analyseurs 802.11. Son objectif principal est de contrôler le déchiffrement de trames brutes 802.11 capturées par le Decoder.

Vue Configuration des services - onglet Général

L'onglet Général de Decoder dans la vue Configuration des services vous permet de gérer la configuration de base des services, de configurer la capture des données et de sélectionner les analyseurs appliqués aux données capturées. Pour accéder à l'onglet Général, accédez à **ADMIN** > **Services** > sélectionnez un Decoder ou un Log Decoder, puis cliquez sur > **Vue** > **Config**> **onglet Général**.

Workflow

La figure suivante illustre les tâches courantes de configuration de Decoder avec les étapes que vous pouvez effectuer dans cette vue mises en surbrillance.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	configurer les paramètres de capture*	Configurer les paramètres de capture
Administrateur	gérer les analyseurs et les analyseurs de logs*	Activer et désactiver les analyseurs et les analyseurs de logs
Administrateur	démarrer et arrêter la capture de données	Démarrer et arrêter la capture de données
Administrateur	configurer des règles	Configurer les règles de Decoder

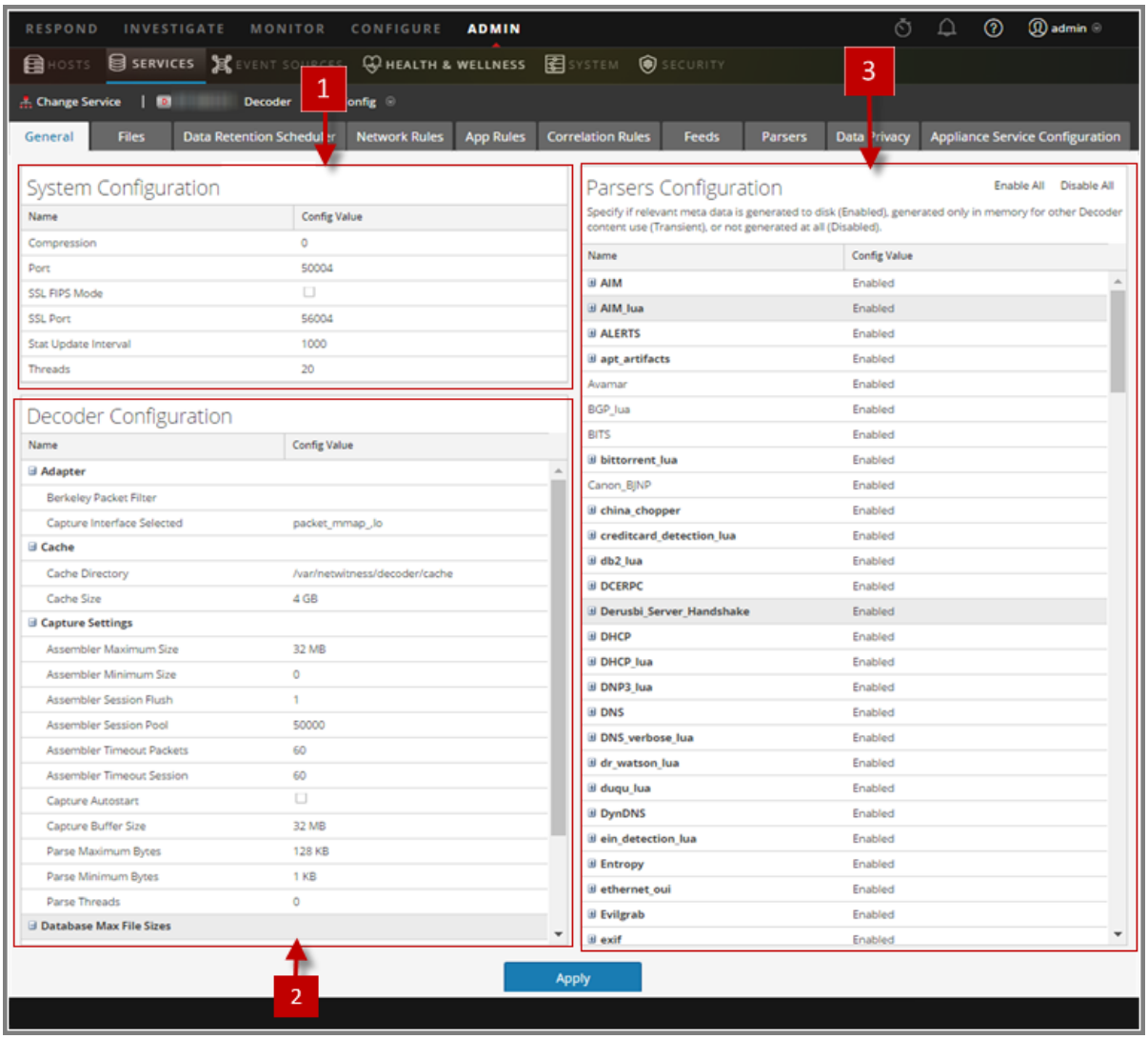
*Vous pouvez effectuer ces tâches ici.

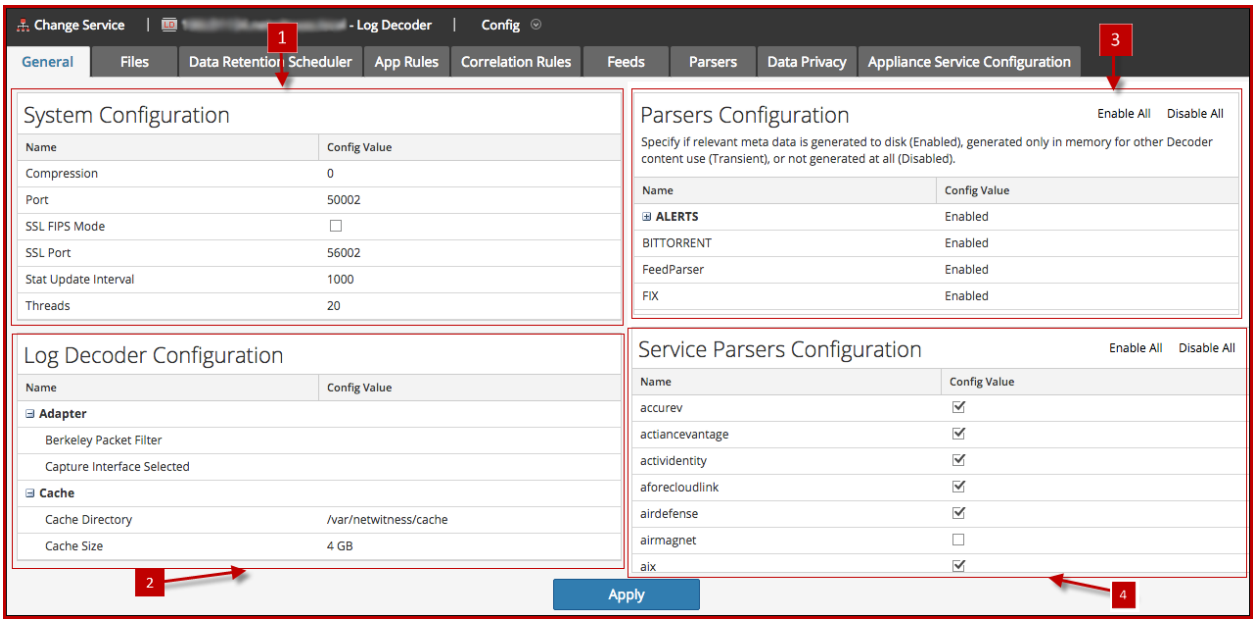
Rubriques connexes

- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder
- Configurer les feeds et les parsers

Aperçu rapide

La première figure est un exemple d'onglet Général pour un Decoder. La seconde est un exemple d'onglet Général pour un Log Decoder.





1 Configuration système - Gère la configuration de service d'un Decoder.

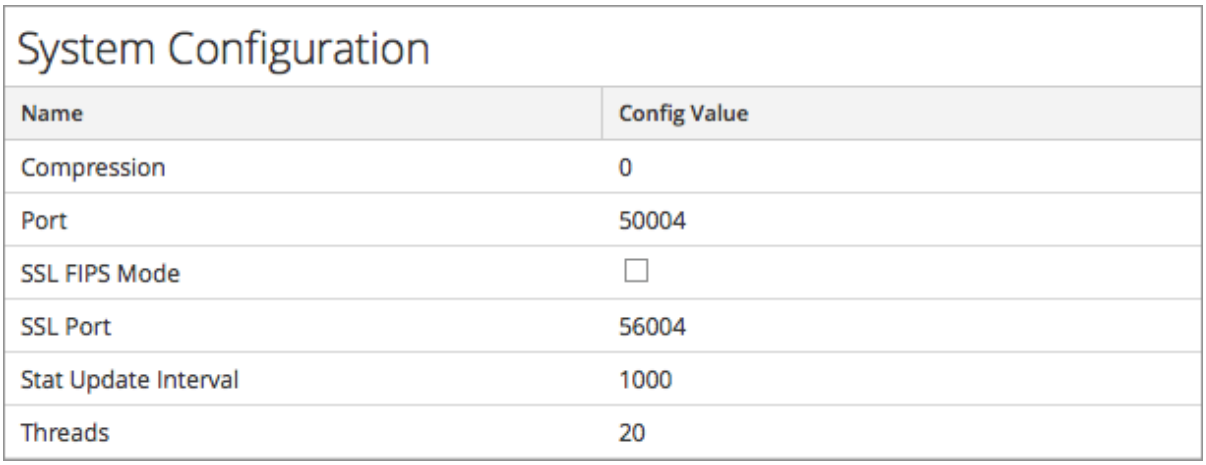
2 Configuration de Decoder ou Configuration de Log Decoder - Vous permet d'afficher et de modifier les paramètres de configuration de service pour un Decoder ou un Log Decoder.

3 Configuration des analyseurs - Vous permet de sélectionner les analyseurs à utiliser sur le Decoder.

4 Configuration des analyseurs de service (Log Decoders uniquement) - Vous permet de sélectionner les analyseurs de service à utiliser sur le Log Decoder.

Section Configuration système

La section Configuration système gère la configuration de service d'un Decoder. Lorsque vous ajoutez un service pour la première fois, les valeurs par défaut sont en vigueur et doivent être modifiées uniquement dans des circonstances particulières, par exemple, si le support client conseille une modification.

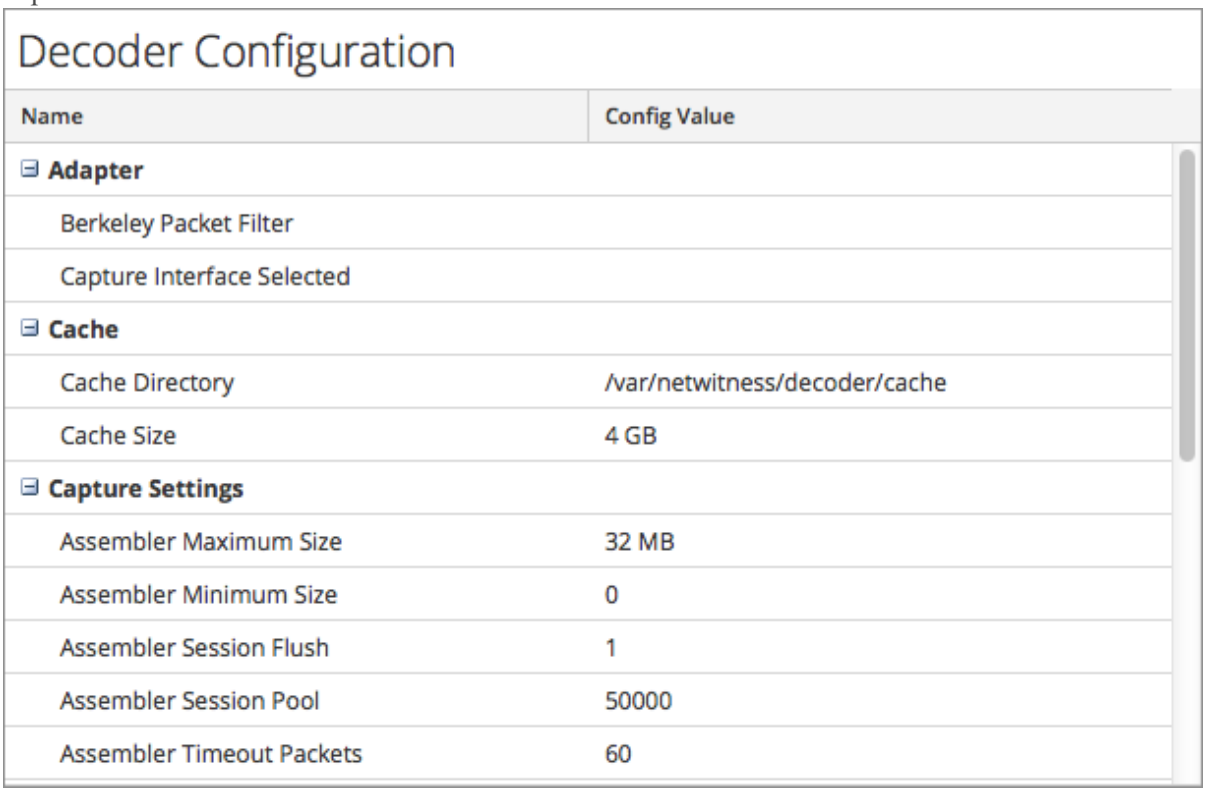


La Configuration système dispose des paramètres suivants.

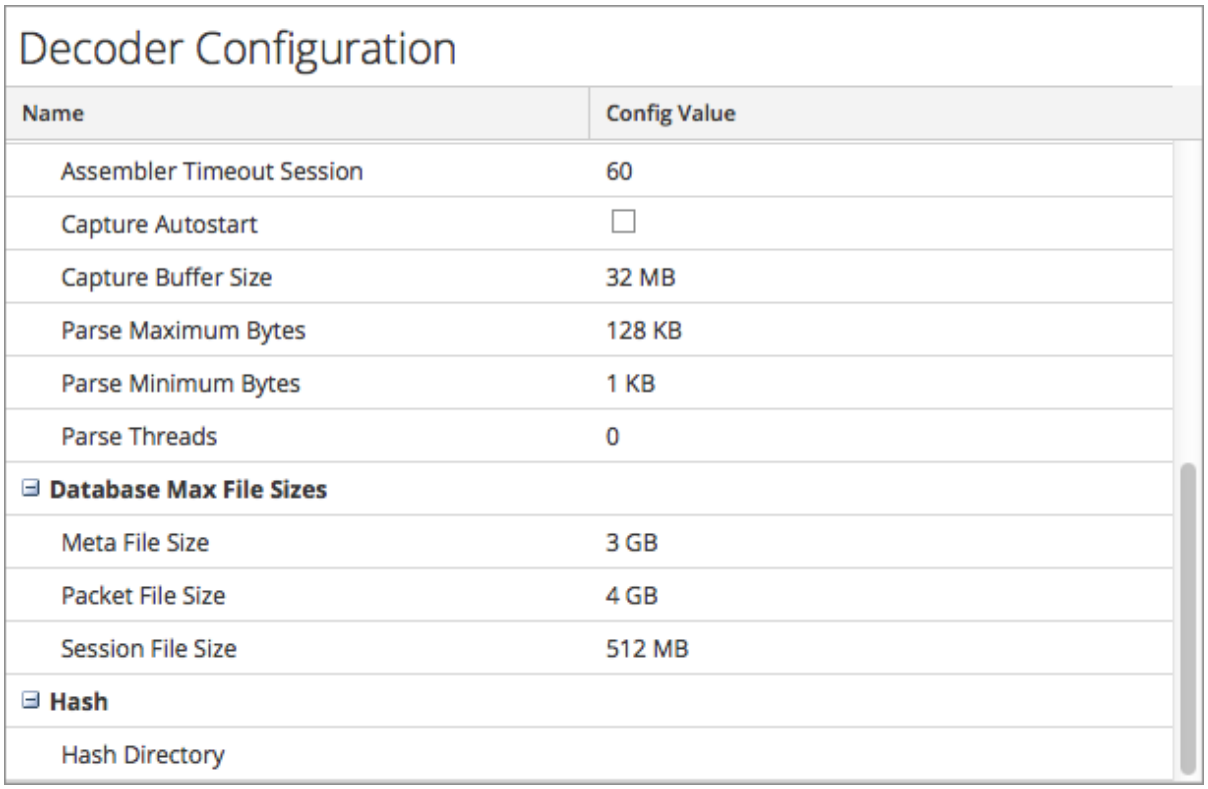
Paramètre	Description
Compression	Le nombre minimum d'octets devant être transmis par réponse avant la compression. Le paramètre 0 désactive la compression. La valeur par défaut est **0**. La modification d'une valeur prend effet immédiatement pour toutes les connexions suivantes.
Port	Détermine le port utilisé par le service. **Remarque :** Si vous modifiez le numéro de port, assurez-vous de redémarrer le service.
Mode FIPS SSL	En cas d'activation, toutes les données transférées dans le réseau seront chiffrées via SSL.
Port SSL	Désigne le port utilisé pour le chiffrement SSL.
Intervalle de mise à jour des statistiques	Nombre de millisecondes entre les mises à jour statistiques sur le système. Les petites valeurs engendrent des mises à jour plus fréquentes et peuvent ralentir d'autres processus. La valeur par défaut est **1000**. La modification de la valeur prend effet immédiatement.
Threads	Nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. Le paramètre **0** laisse le système décider. Les modifications prendront effet au redémarrage du service.

Section Configuration des Decoders

La section Configuration des Decoders vous permet de visualiser et modifier les paramètres de configuration de service pour un Decoder ou un Log Decoder. Lorsqu'un service est ajouté pour la première fois, les valeurs par défaut s'appliquent. Vous pouvez modifier ces valeurs pour gérer la capture du trafic.



Faites défiler la fenêtre vers le bas de la section pour afficher les paramètres de configuration supplémentaires de Decoder.



Sélection Adaptateur

Les paramètres de l'adaptateur configurent l'interface réseau pour la capture, comme décrit dans la rubrique Configurer les paramètres de capture.

Section Cache

Les paramètres du cache vous permettent de configurer le répertoire cache et la taille des fichiers du cache de session. Le tableau suivant décrit les paramètres du cache. Lorsque vous ajoutez un service pour la première fois, les valeurs par défaut sont en vigueur et doivent être modifiées uniquement dans des circonstances particulières, par exemple, si le support client conseille une modification.

Paramètre du cache	Description
Répertoire cache	Le répertoire où sont stockés les fichiers du cache de session. La valeur par défaut est `/var/netwitness/decoder/cache`. Les modifications prennent effet automatiquement.
Taille du cache	Taille maximale, en mégaoctets (Mo), que tous les fichiers du répertoire cache peuvent atteindre avant la suppression des fichiers les plus anciens. Une fois le seuil atteint, la taille du cache est réduite de 10 %. La valeur par défaut est **4 Go**. La modification prend effet immédiatement.

Section Paramètres de capture

La section Paramètres de capture vous permet de configurer les paramètres de capture opérationnels. Lorsque vous ajoutez un service pour la première fois, les valeurs par défaut sont en vigueur et doivent être modifiées uniquement dans des circonstances particulières, par exemple, si le support client conseille une modification.

Paramètres de capture	Description
Taille maximale de l'assembleur	Spécifie la valeur maximale (en octets) que la taille des données de paquets dune session peut atteindre. La valeur par défaut est **32 Mo**. La modification prend effet immédiatement.
Taille minimale de l'assembleur	Spécifie la taille minimale (en octets) qu'une session doit avoir pour générer des métadonnées. La valeur **0** signifie que chaque session génère des métadonnées. La valeur par défaut est **0.** La modification prend effet immédiatement.
Vidage de session de l'assembleur	Spécifie si une session est supprimée de l'assembleur lorsque la dernière chaîne de la session est supprimée de lassembleur. La valeur par défaut est **1**. • **2** = si le délai du premier paquet d'une session expire de l'assembleur, la session est supprimée de l'assembleur à la fin de l'analyse. Tous les paquets suivants de cette session créent une nouvelle session dans l'assembleur. • **1** = si le délai de la dernière chaîne d'une session expire de l'assembleur, la session est supprimée de l'assembleur. Tous les paquets suivants de cette session créent une nouvelle session dans l'assembleur. • **0** = si le délai de la dernière chaîne d'une session expire de l'assembleur, la session est laissée dans l'assembleur jusqu'à ce qu'elle expire. Tous les paquets suivants de cette session sont filtrés Les modifications prendront effet au redémarrage du service.
Pool de sessions de l'assembleur	Spécifie le nombre d'entrées dans le pool de sessions. La valeur par défaut est **350 000**. Les modifications prendront effet au redémarrage du service.
Expiration du délai des paquets de l'assembleur	Spécifie le nombre de secondes avant l'expiration du délai d'un paquet ou d'une chaîne. La valeur par défaut est **60**. La modification prend effet immédiatement.
Expiration du délai de session de l'assembleur	Spécifie le nombre de secondes avant l'expiration du délai d'une session. La valeur par défaut est **60**. La modification prend effet immédiatement.
Démarrage automatique de la capture	Spécifie si la capture commence automatiquement chaque fois que Decoder démarre. Lorsque ce paramètre est activé, la valeur est oui. Lorsque cette option est désactivée, la valeur = no. La valeur par défaut est **no**. La modification prend effet immédiatement.

Paramètres de capture	Description
Taille du tampon de capture	Taille allouée à la mémoire tampon de capture en mégaoctets. La valeur par défaut est **64 Mo**. Les modifications prendront effet au redémarrage du service.
Nombre maximal d'octets à analyser	Nombre maximal d'octets à analyser pour rechercher des jetons supplémentaires dans un flux. Lorsque le premier jeton est trouvé, le flux est analysé à hauteur du nombre d'octets défini, mais pas au-delà. Le paramètre **0** supprime l'achèvement anticipé et tout le flux est scanné, quelle que soit sa taille. La valeur par défaut est **128 Ko**. La modification prend effet immédiatement.
Nombre minimal d'octets à analyser	Nombre minimal d'octets à analyser pour rechercher le premier jeton dans un flux. Si aucun jeton n'est trouvé dans le nombre d'octets défini, l'analyse prend fin. Le paramètre **0** supprime l'achèvement anticipé et tout le flux est scanné, quelle que soit sa taille. La valeur par défaut est **1 Ko**. La modification prend effet immédiatement.
Threads d'analyse	Nombre de threads d'analyse à utiliser pour l'analyse de session. La valeur **0** signifie que la décision revient au serveur. La valeur par défaut est **0**. Les modifications prendront effet au redémarrage du service.

Section Tailles de fichier maximales de la base de données

La section Tailles de fichier maximales de la base de données vous permet de contrôler la taille maximale des fichiers des diverses bases de données. Lorsque vous ajoutez un service pour la première fois, les valeurs par défaut sont en vigueur et doivent être modifiées uniquement dans des circonstances particulières, par exemple, si le support client conseille une modification.

Paramètre de taille des fichiers	Description
Taille des fichiers méta	Taille maximale des fichiers de base de données méta en mégaoctets. La valeur par défaut est **10 Mo**. Les modifications prendront effet au redémarrage du service.
Taille des fichiers de paquets	Taille maximale des fichiers de base de données des paquets en mégaoctets. La valeur par défaut est **10 Mo**. Les modifications prendront effet au redémarrage du service.
Taille des fichiers de session	Taille maximale des fichiers de base de données de session en mégaoctets. La valeur par défaut est **100 Mo**. Les modifications prendront effet au redémarrage du service.

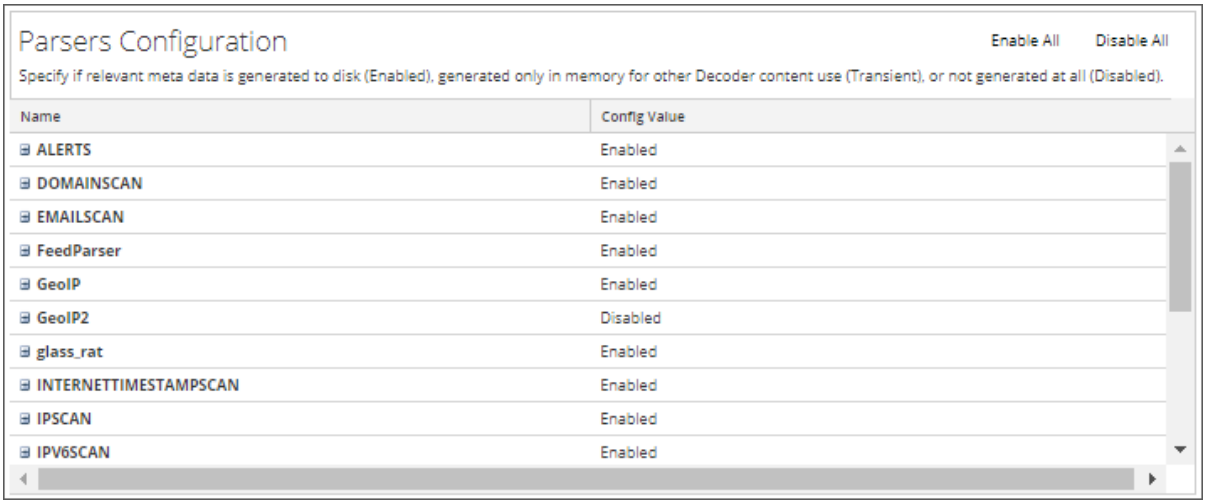
Section Hachage

Les paramètres de la section Hachage contrôlent les options de hachage des fichiers de base de données des options de hachage. Il y a une petite pénalité de performance lors du hachage.

Paramètre de hachage	Description
Répertoire de hachage	Répertoire du serveur où sont écrits tous les fichiers de hachage. En l'absence de valeur, chaque fichier de hachage est écrit dans le même répertoire que le fichier en cours de hachage. La valeur par défaut est vide. Les modifications prendront effet au redémarrage du service.

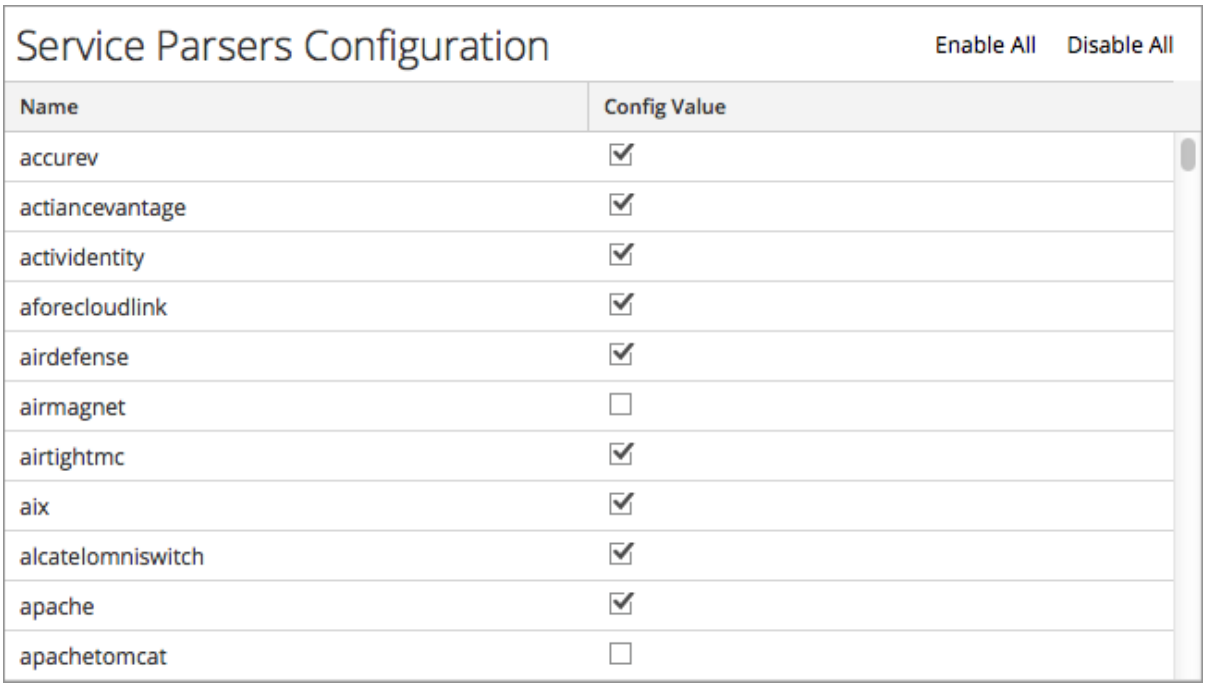
Panneau Configuration des analyseurs

Le panneau Configuration des analyseurs vous permet de sélectionner les analyseurs à utiliser dans Decoder. Dans certains analyseurs, vous pouvez également configurer les métadonnées créées par l'analyseur. Reportez-vous à la section Activer et désactiver les analyseurs et les analyseurs de logs pour des informations détaillées et des procédures.



Section Configuration des analyseurs de services pour Log Decoder

La section Configuration des analyseurs de services vous permet de sélectionner les analyseurs de services à utiliser dans Log Decoder.



Vue Configuration des services - onglet Analyseurs

Sous l'onglet Analyseurs de la vue Configuration des Services, vous pouvez afficher les analyseurs déployés sur Decoder ou Log Decoder, télécharger des analyseurs et supprimer les analyseurs déployés. Les analyseurs peuvent être ajoutés et supprimés alors que Decoder ou Log Decoder est en cours d'exécution sans que cela ait d'impact sur la capture.

Pour accéder à l'onglet Analyseurs, accédez à **ADMIN** > **Services** > sélectionnez un service **Decoder** ou **Log Decoder** et cliquez sur > **Afficher** > **Config** > **Onglet Analyseurs**.

Que voulez-vous faire ?

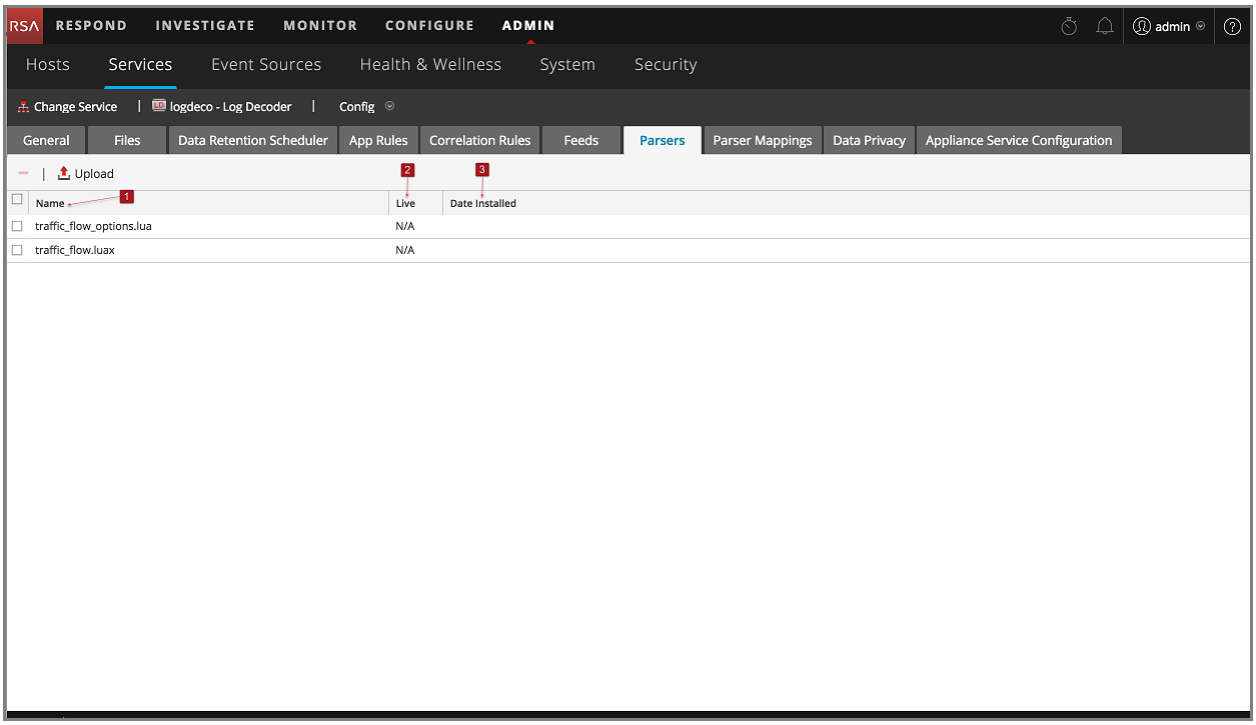
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	Afficher les analyseurs déployés.	Activer et désactiver les analyseurs et les analyseurs de logs
Administrateur	Télécharger des analyseurs vers un Decoder ou Log Decoder.	Activer et désactiver les analyseurs et les analyseurs de logs

Rubriques connexes

- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder
- Télécharger et supprimer des analyseurs personnalisés

Aperçu rapide

Voici un exemple de l'onglet Analyseurs. La grille Analyseur répertorie tous les analyseurs actuellement déployés sur le Decoder.



1 **Nom** : Nom de l'analyseur ou fichier d'analyseur.

2 **Live** : Indique si l'analyseur provient de Live. Les valeurs possibles sont **Oui**, **Non** ou **N/A**.

- **Oui** = Installé via Live Services.
- **Non** = installé via NetWitness.
- **N/A** = L'analyseur n'a pas de fichier d'attribut créé par NetWitness pour effectuer le suivi de la date d'installation. Il se peut que l'analyseur ait été installé manuellement et non via NetWitness ou Live Services.

3 **Date d'installation** : Date à laquelle l'analyseur a été transmis au service.

Barre d'outils de l'onglet Analyseurs

La barre d'outils de l'onglet Analyseurs comporte des options permettant d'utiliser les analyseurs dans la grille.

Fonctionnalité	Description
Upload	Vous permet de télécharger des analyseurs vers un Decoder ou Log Decoder.
	Vous invite à confirmer la suppression des analyseurs sélectionnés. Vous pouvez sélectionner **Non** pour annuler la suppression ou **Oui** pour supprimer les analyseurs sélectionnés.

Vue Configuration des services - Onglet Mappages d'analyseur

Cette rubrique propose une description des options configurables pour un Log Decoder sous l'onglet Mappages d'analyseur.

Sous l'onglet Mappages d'analyseur, les administrateurs peuvent configurer des mappages d'analyseurs de logs pour les services Log Decoder. Pour accéder à l'onglet Mappages d'analyseur, accédez à **ADMIN** > **Services** > sélectionnez un service et cliquez sur > **Afficher** > **Config** > **onglet Mappages d'analyseur**.

Remarque : Vous pouvez également configurer des mappages d'analyseur de log pour les services Log Decoder en accédant à **ADMIN > Services > Sources d'événements > Découverte**.

Cette fonction est conçue pour effectuer le suivi d'un sous-ensemble de sources d'événements dont l'analyse se fait avec l'analyseur incorrect.

Que voulez-vous faire ?

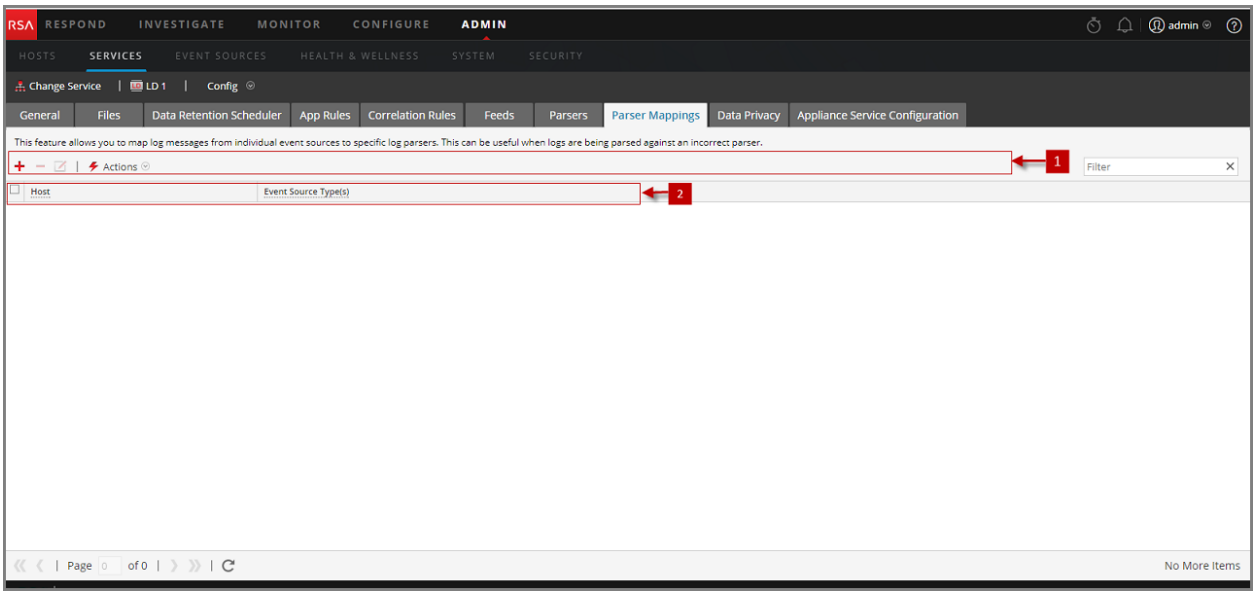
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	Gérer les adresses IP pour le mappage de source d'événement.	Activer les mappages d'analyseur

Rubriques connexes

- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder

Aperçu rapide

Voici un exemple de l'onglet.



1 Barre d'outils Mappages d'analyseur - Comporte des options permettant d'utiliser les mappages d'analyseur dans la grille

2 Grille Mappages d'analyseur - Répertorie tous les analyseurs actuellement mappés sur le Log Decoder

Barre d'outils Mappages d'analyseur

La barre d'outils Mappages d'analyseur comporte des options permettant d'utiliser les mappages d'analyseur dans la grille.

Fonctionnalité	Description
	Ajoute un mappage d'analyseur.
	Supprime le mappage d'analyseur sélectionné.
	Modifie un mappage d'analyseur.
	Actualise la liste des mappages d'analyseurs.
	Affiche le Menu Actions. • **Importer** - Importe un mappage d'analyseur vers un fichier. • **Exporter** - Exporte un mappage d'analyseur vers un fichier.

Liste Mappages d'analyseur

La liste Mappages d'analyseur répertorie tous les analyseurs actuellement mappés sur le Log Decoder.

Paramètre	Description
Hôte	Affiche l'adresse IP de l'hôte.
Source d'événement	Affiche les sources d'événements qui sont analysées de manière incorrecte.

Boîte de dialogue Éditeur de mappages d'analyseur

La boîte de dialogue Éditeur de mappages d'analyseur vous permet de mettre à jour une adresse IP en fonction du mappage de source d'événement.

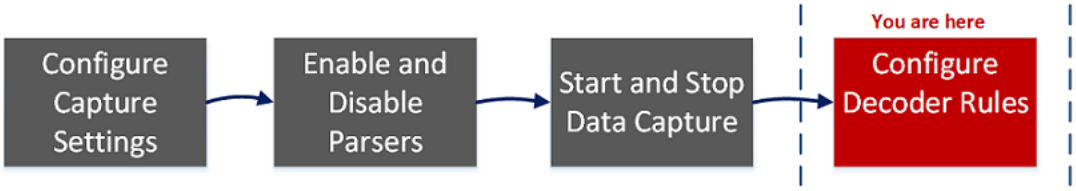
Pour accéder à la boîte de dialogue Éditeur de mappages d'analyseur, dans la vue Configuration des services d'un Log Decoder, sélectionnez l'onglet Mappages d'analyseur.

Vue Configuration des services - onglets Règles

Les onglets Règles de la vue Configuration des Services (**ADMIN > Services >** , sélectionnez un service et cliquez sur > **Vue > Config**) vous permettent de définir et de gérer les règles de capture. Chaque type de règles possède une grille avec des colonnes et des paramètres légèrement différents dans la boîte de dialogue Éditeur de règles. Les règles d'application et de corrélation s'appliquent aux services Decoder et Log Decoder. Les règles réseau ne s'appliquent qu'aux Decoders de réseaux.

Workflow

La figure suivante illustre les tâches courantes de configuration de Decoder avec les étapes que vous pouvez effectuer dans cette vue mises en surbrillance.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	configurer les paramètres de capture	Configurer les paramètres de capture
Administrateur	gérer les analyseurs et les analyseurs de logs*	Activer et désactiver les analyseurs et les analyseurs de logs
Administrateur	démarrer et arrêter la capture de données	Démarrer et arrêter la capture de données
Administrateur	configurer des règles*	Configurer les règles de Decoder
Administrateur	importer, exporter ou appliquer une règle*	Configurer les règles de Decoder
Administrateur	activer ou désactiver des règles*	Configurer les règles de Decoder
Administrateur	ajouter, modifier et supprimer des règles*	Configurer les règles de Decoder

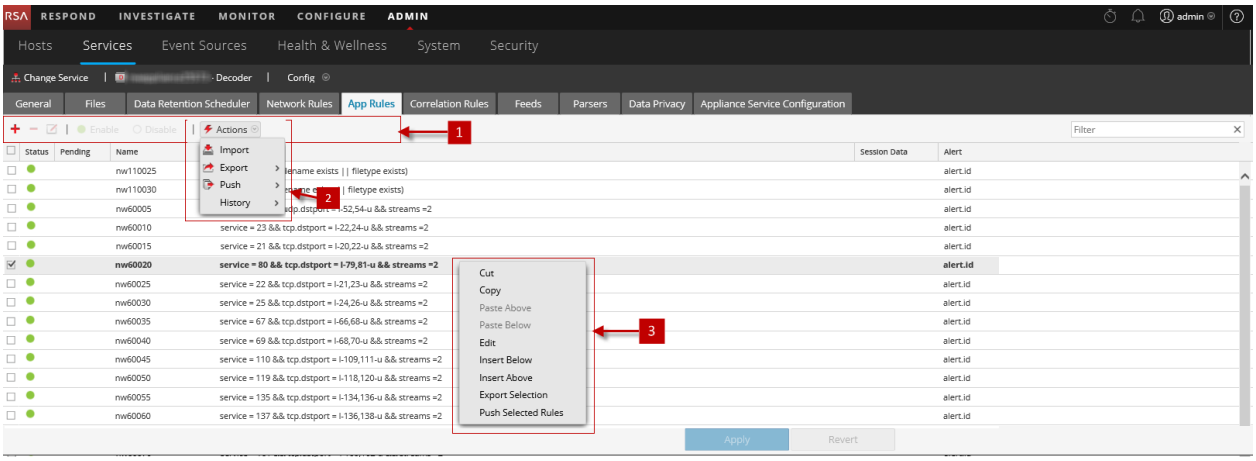
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer les paramètres communs sur un Decoder
- Configuration rapide de Decoder et de Log Decoder
- Onglet Règles d'application
- Onglet Règles de corrélation
- Onglet Règles réseau

Aperçu rapide

Voici un exemple de l'onglet Règles d'application.



1	Barre d'outils de l'onglet Règles - Comporte des options permettant d'utiliser les règles dans la grille
2	Menu Actions de règles - Comporte des options permettant de gérer des ensembles de règles
3	Actions de contexte de liste de règles - Affiche le menu contextuel Liste de règles

Barre d'outils onglet Règles

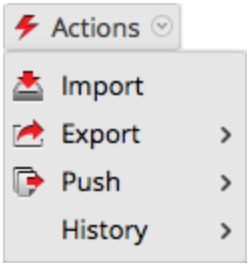
La barre d'outils est identique pour tous les onglets Règles de la vue Config.

Fonctionnalité	Description
Actions	Affiche le menu **Actions**.
+	Ajoute une nouvelle règle à un service.
−	Supprime une règle d'un service.
	Autorise la modification de règle.

Fonctionnalité	Description
Disable	Désactive une règle (sans la supprimer).
Enable	Active (réactive) une règle.
Filtrer	Champ de saisie pour une chaîne de recherche. NetWitness Platform filtre les règles de manière dynamique à mesure que vous tapez une chaîne de recherche. Le fait de cliquer sur **x** efface le champ de saisie et restaure la vue non filtrée.
Appliquer	Enregistre les modifications apportées aux règles et applique les règles configurées à un service. Avant l'application des modifications, il est possible de recharger les règles à leur état précédant les modifications actuelles.
Rétablir	Supprime les modifications non sauvegardées sur la grille et rétablit les règles non modifiées.

Menu Actions de règles

Le menu Actions possède des options qui aident à gérer des ensembles de règles.



Option	Description
Import	Importe un ensemble de règles dans l'interface utilisateur de sorte qu'il puisse être appliqué à un service. Vous pouvez modifier les règles avant de les appliquer.
Exporter	Enregistre les règles sélectionnées ou toutes les règles dans un fichier .nwr sur la machine client.

Option	Description

Insertion	Autorise l'application des règles à d'autres services (Decoder ou Log Decoder) ou à un service Decoder appartenant à un groupe de services. Lors de la transmission, les règles peuvent être fusionnées (mise à jour des règles existantes et ajout de nouvelles règles) ou remplacées.
	• **Transmettre > Tout.** Transmet toutes les règles aux autres services. Toutes les règles des services de destination sont supprimées et remplacées par toutes les règles du service source.
	• **Transmettre > Sélection.** Transmet toutes les règles sélectionnées à d'autres services. Deux options s'offrent à vous :
	  • **Remplacer.** Supprime toutes les règles sur les services cibles et les remplace par les règles sélectionnées par le service de source.
	  • **Fusionner.** Fusionne les règles sélectionnées avec les règles existantes sur les services cibles

Historique	Affiche les dix derniers instantanés de règles appliqués dans NetWitness Platform. Vous pouvez sélectionner et appliquer (restaurer) un instantané dans le Decoder à tout moment.

Actions de contexte de liste de règles

Dans une grille de règles, le fait de cliquer sur une ligne avec le bouton droit affiche le menu contextuel de la grille de règles.

Option	Description
Couper	Supprime la règle actuelle.
Copy	Copie la règle actuelle.
Coller au-dessus	Colle la règle copiée au-dessus de la règle actuelle.
Coller en dessous	Colle la règle copiée en dessous de la règle actuelle.
Modifier	Modifie la règle actuelle.
Insérer en dessous	Insère les règles importées en dessous de la règle actuelle.
Insérer au dessus	Insère les règles importées au-dessus de la règle actuelle.
Sélections pour l'exportation	Exporte les règles sélectionnées.
Transmettre les règles sélectionnées	Transmet les règles sélectionnées à d'autres services.

Onglet Règles d'application

L'onglet Règles d'application (**ADMIN > Services >**, puis cliquez sur sélectionnez un Decoder ou un Log Decoder et cliquez sur > **Vue > Config > onglet Règles d'application**) vous permet de gérer les règles d'application. NetWitness Platform applique les règles d'application au niveau de la session.

Que voulez-vous faire ?

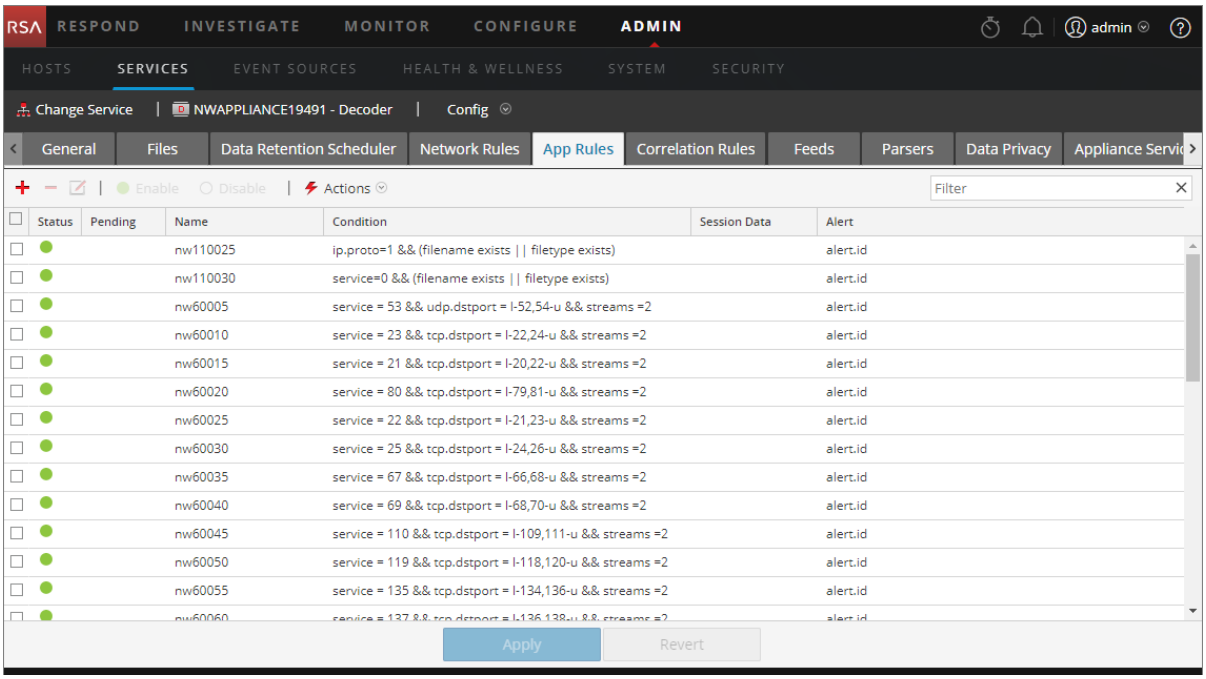
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	ajouter ou modifier des règles d'application	Configurer des règles d'application

Rubriques connexes

- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder
- Configurer les règles de Decoder
- Vue Configuration des services - onglets Règles

Aperçu rapide

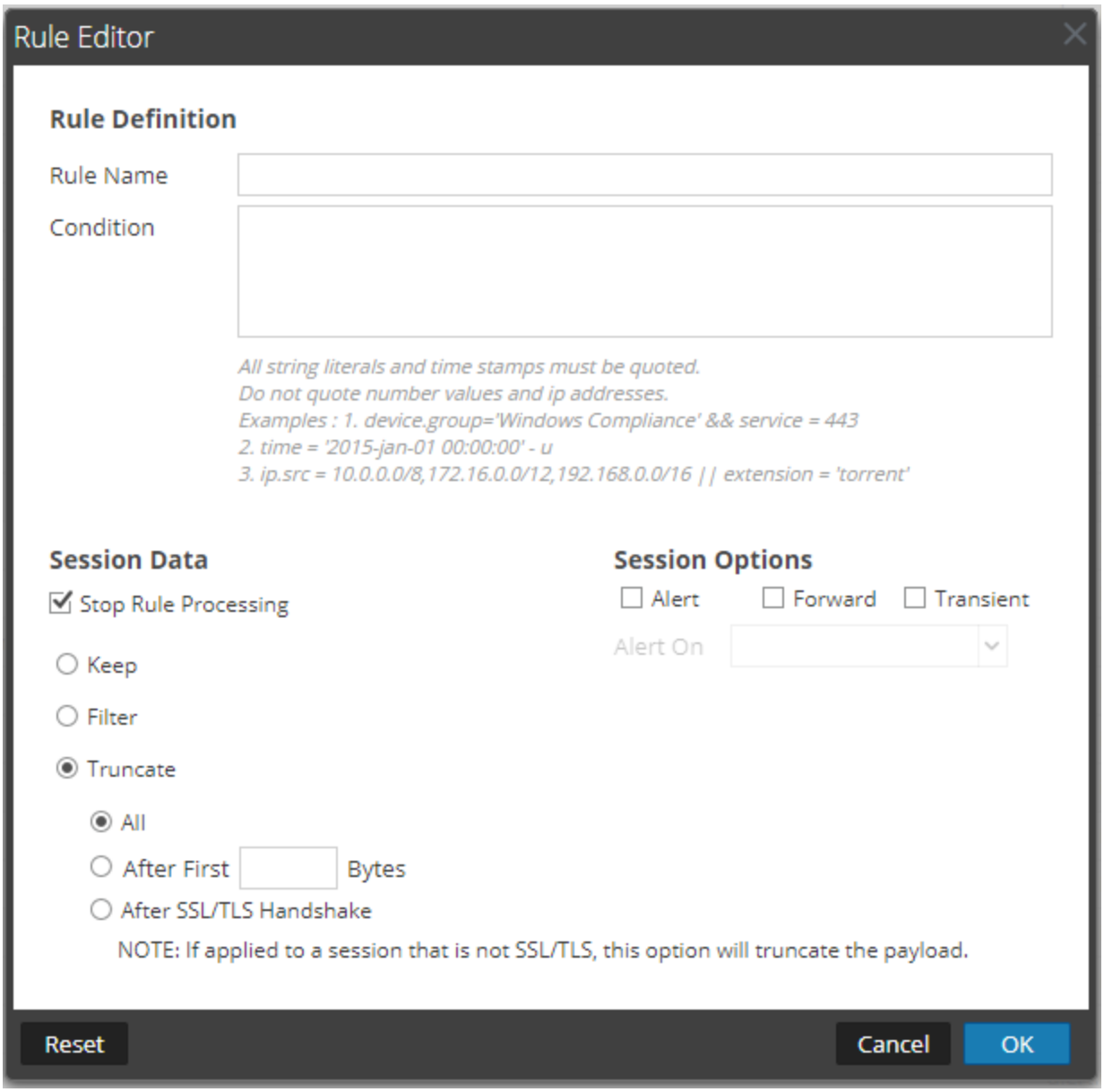
La figure suivante illustre l'onglet Règles d'application et le tableau décrit les colonnes.



Colonne	Description
En attente	Cette colonne indique si une règle dispose de modifications en attente. Les règles actuellement actives sur le Decoder ne disposent pas d'indicateur. Si la règle est nouvelle ou a subi une modification, la colonne affiche . Lorsque les règles sont appliquées, l'indicateur En attente est supprimé.
Name	Il s'agit du nom de la règle, un identifiant descriptif de la règle.
Condition	Il s'agit de la définition de la condition qui déclenche une action lorsqu'elle est rencontrée.
Données de session	Cette colonne affiche l'action des Données de session qui est réalisée lorsqu'un paquet correspond à la règle. Les valeurs possibles sont **Filtrer**, **Conserver** ou **Tronquer**.
Alert	Cette colonne affiche le nom de l'alerte personnalisée que le service Decoder génère en cas de correspondance entre les métadonnées et la règle.
État	Cette colonne indique si la règle est activée ou désactivée à l'aide d'une icône circulaire. Si le cercle est vert, la règle est activée. Si le cercle est vide, la règle est désactivée.

Boîte de dialogue Éditeur de règles

La figure suivante affiche la boîte de dialogue Éditeur de règles pour une règle d'application.



La boîte de dialogue Éditeur de règles propose les champs et options nécessaires pour définir une règle d'application.

Champ	Description
Nom de la règle	Nom descriptif qui identifie la règle.

Champ	Description
Condition	Définition de la condition qui déclenche une action lorsqu'elle est rencontrée. Vous pouvez effectuer une saisie directement dans le champ ou élaborer une condition dans ce champ à l'aide des métadonnées provenant des actions de la fenêtre Intellisense. Lors de l'élaboration de la définition de règle, Intellisense affiche des erreurs et avertissements de syntaxe. Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre et d'adresses IP entre guillemets.Configurer les règles de Decoder fournit des informations supplémentaires.

Le tableau suivant décrit les actions et options de la section Données de session.

Action	Description
Arrêter le traitement d'une règle	Si cette option est cochée, aucune nouvelle évaluation de règle ne se produira en cas de correspondance avec la règle, et la session sera enregistrée comme indiqué par l'action de la session. Si cette option n'est pas cochée, l'évaluation des règles continue jusqu'à ce que toutes les règles soient évaluées.
Conserver	La charge utile du paquet et les métadonnées associées sont enregistrées lorsqu'elles correspondent à la règle.
Filtrer	Le paquet n'est pas enregistré lorsqu'il correspond à la règle.
Tronquer	**Tronquer tout** – tronque tous les octets de la charge utile de la session. La charge utile du paquet n'est pas enregistrée lorsqu'elle correspond à la règle, mais les en-têtes des paquets et les autres métadonnées associées sont conservés. Il s'agit de l'option de troncature par défaut. **Tronquer après les premiers octets < n >** : tronque les octets de la charge utile de la session après les premiers octets < n > spécifiés, où < n > est un nombre entier. La charge utile du paquet n'est pas enregistrée après <n> octets lorsqu'elle correspond à la règle, mais les en-têtes des paquets et les autres métadonnées associées sont conservés. **Tronquer SSL/TLS après le handshake** pour tronquer la charge utile de toutes les sessions, sauf dans le cas d'une session SSL/TLS, où l'échange SSL est conservé, mais le reste de la charge utile n'est pas enregistré. Cette option est utilisée avec les analyseurs SSL.
Alerter et **Alerte activée**	Si l'option **Alerter** est activée, le paquet génère une alerte personnalisée lorsque les métadonnées correspondent à la règle. Vous pouvez sélectionner le nom de l'alerte dans le champ **Alerte activée**.
Faire suivre	Active les performances de transfert Syslog lorsque le log correspond à la règle.
Transitoire	Empêche les métadonnées de l'alerte qui est créée d'être écrites sur le disque.

Le tableau suivant décrit les actions de la boîte de dialogue Éditeur de règles.

Action	Description
Réinitialiser	Réinitialise le contenu de la boîte de dialogue aux valeurs précédant la modification ; les modifications sont ignorées.
Annuler	Annule toute modification et ferme la boîte de dialogue Éditeur de règles.
OK	Enregistre la nouvelle règle ou la règle modifiée, et l'ajoute à la grille de règles. La boîte de dialogue Éditeur de règles se ferme.
Enregistrer	(Règles avec une syntaxe obsolète uniquement) Applique une règle corrigée de manière individuelle au service Decoder. Reportez-vous à la section Corriger les règles contenant une syntaxe non valide.

Onglet Règles de corrélation

L'onglet Règles de corrélation (**ADMIN > Services>** , sélectionnez un service et cliquez sur > **Vue > Config > onglet Règles de corrélation**) vous permet de gérer les règles de corrélation. Les règles de corrélation de base sont appliquées au niveau de la session et alertent l'utilisateur par rapport à des activités spécifiques pouvant se produire dans leur environnement. NetWitness Platform applique les règles de corrélation sur une période glissante configurable.

Que voulez-vous faire ?

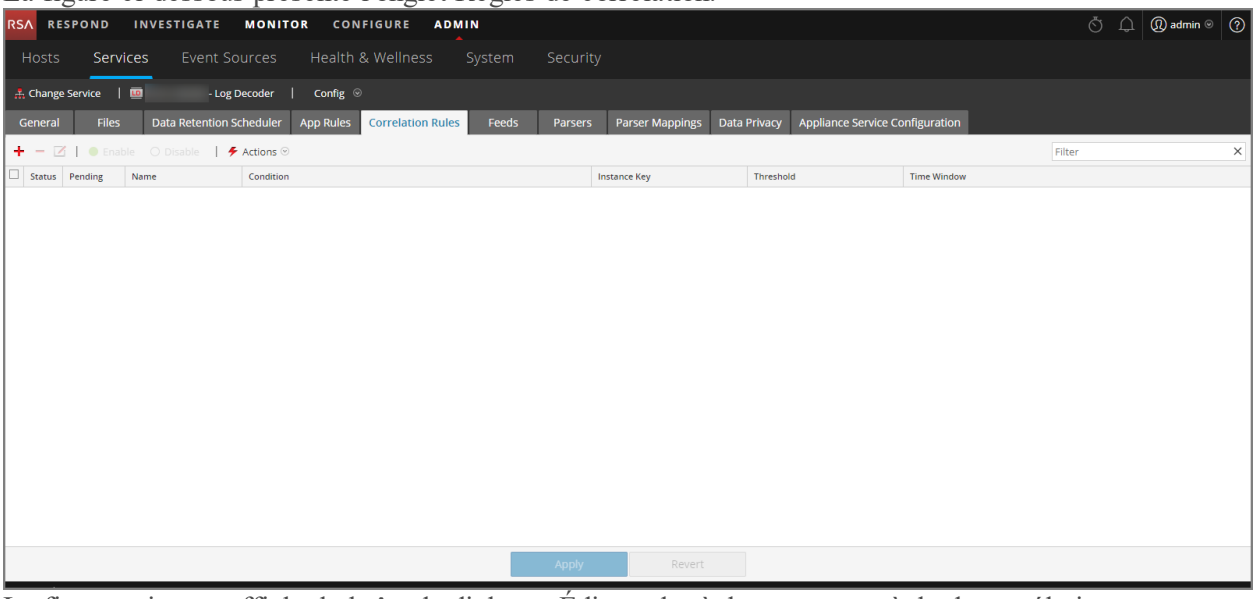
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	ajouter ou modifier une règle de corrélation	Configurer des règles de corrélation

Rubriques connexes

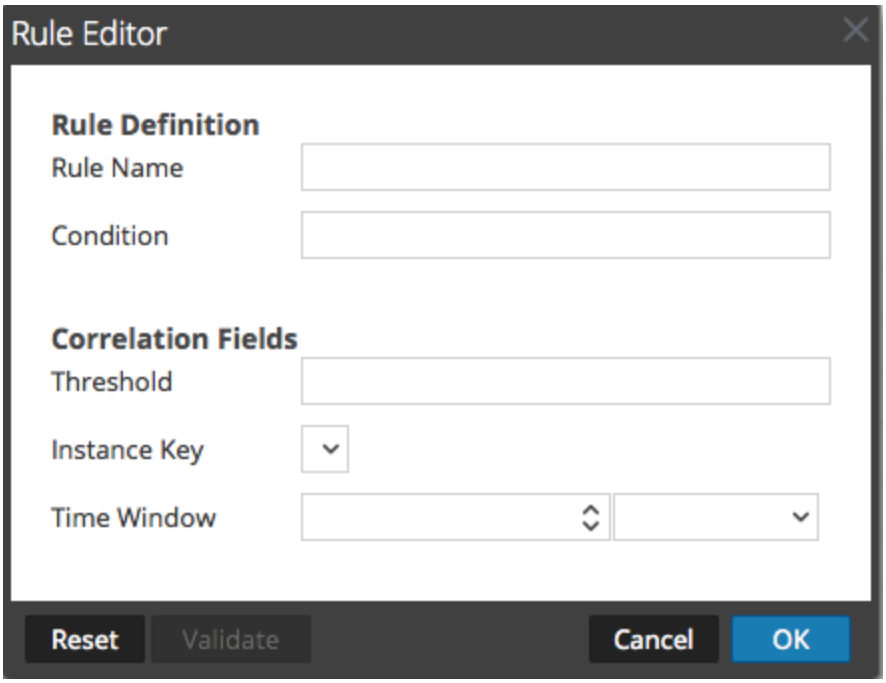
- Configurer les paramètres communs sur un Decoder
- Configuration rapide de Decoder et de Log Decoder
- Configurer les règles de Decoder
- Vue Configuration des services - onglets Règles

Aperçu rapide

La figure ci-dessous présente l'onglet Règles de corrélation.



La figure suivante affiche la boîte de dialogue Éditeur de règles pour une règle de corrélation.



Le tableau suivant décrit les colonnes de l'onglet Règles de corrélation.

Colonne	Description
En attente	Cette colonne indique si une règle dispose de modifications en attente. Les règles actuellement actives sur le Decoder ne disposent pas d'indicateur. Si la règle est nouvelle ou a subi une modification, la colonne affiche . Lorsque les règles sont appliquées, l'indicateur En attente est supprimé.
Nom	Il s'agit du nom descriptif de la règle.
Condition	Il s'agit de la définition de la condition qui déclenche une action lorsqu'elle est rencontrée. Dans les conditions, tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre et adresses IP entre guillemets. Configurer les règles de Decoder fournit des informations supplémentaires.
Clé d'instance	Il s'agit de l'indicateur cible sur lequel l'événement s'appuie. Il peut s'agit d'une clé primaire unique, telle qu'ip.src, ou d'une clé primaire composée, telle qu'ip.src,ip.dst.

Colonne	Description
Seuil	Il s'agit du nombre minimum d'occurrences requis pour déclencher une session de corrélation, qui peut inclure une clé associée identifiant le type de métadonnée compté pour déterminer si la condition est satisfaite. Le moteur de corrélation ne peut pas utiliser IPv4 ou IPv6 en tant que type de métadonnées associé. Utilisez l'un de ces trois arguments : • `u_count(associated_key)` = nombre de valeurs uniques de la clé spécifiée Une clé est requise. • `sum(associated_key)` = les valeurs de la clé spécifiée. Une clé est requise. • `count()` = nombre de sessions, aucune clé associée utilisée. S'il est inclus, il est ignoré.
Période	Il s'agit de la durée en heures, minutes ou secondes pendant laquelle le seuil doit être atteint pour qu'une session de corrélation soit déclenchée.
État	Cette colonne indique si la règle est activée ou désactivée à l'aide d'une icône circulaire. Si le cercle est vert, la règle est activée. Si le cercle est vide, la règle est désactivée.

La boîte de dialogue **Éditeur de règles** propose les champs et options nécessaires pour définir une règle réseau. Les champs correspondent exactement aux colonnes de grille.

Action	Description
Réinitialiser	Réinitialise le contenu de la boîte de dialogue aux valeurs précédant la modification ; les modifications sont ignorées.
Annuler	Annule toute modification et ferme la boîte de dialogue Éditeur de règles.
OK	Enregistre la nouvelle règle ou la règle modifiée, et l'ajoute à la grille de règles. La boîte de dialogue Éditeur de règles se ferme.
Enregistrer	(Règles avec une syntaxe obsolète uniquement) Applique une règle corrigée de manière individuelle au service Decoder. Reportez-vous à la section Corriger les règles contenant une syntaxe non valide.

Onglet Règles réseau

L'onglet Règles réseau (**ADMIN > Services >** sélectionnez un Decoder, puis cliquez sur **> Vue > Config > onglet Règles réseau**) vous permet de gérer les règles réseau. NetWitness Platform applique des règles réseau au niveau des paquets. Les règles réseau comprennent les groupes de règles de la couche 2, de la couche 3 et de la couche 4. Plusieurs règles peuvent s'appliquer à Decoder. Les règles peuvent être appliquées à plusieurs couches (par exemple, lorsqu'une règle réseau filtre des ports spécifiques pour une adresse IP spécifique). Les règles réseau ne s'appliquent qu'aux Network Decoder.

Que voulez-vous faire ?

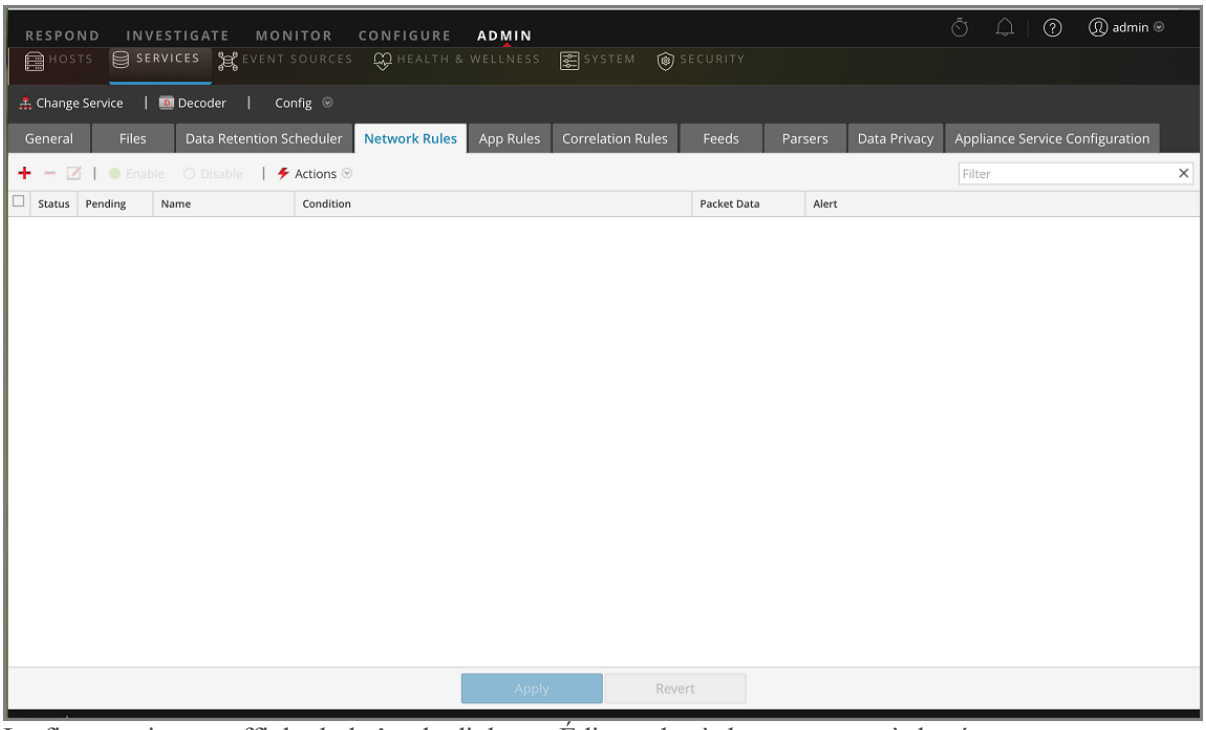
Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	ajouter, modifier ou corriger des règles réseau	Configurer des règles réseau

Rubriques connexes

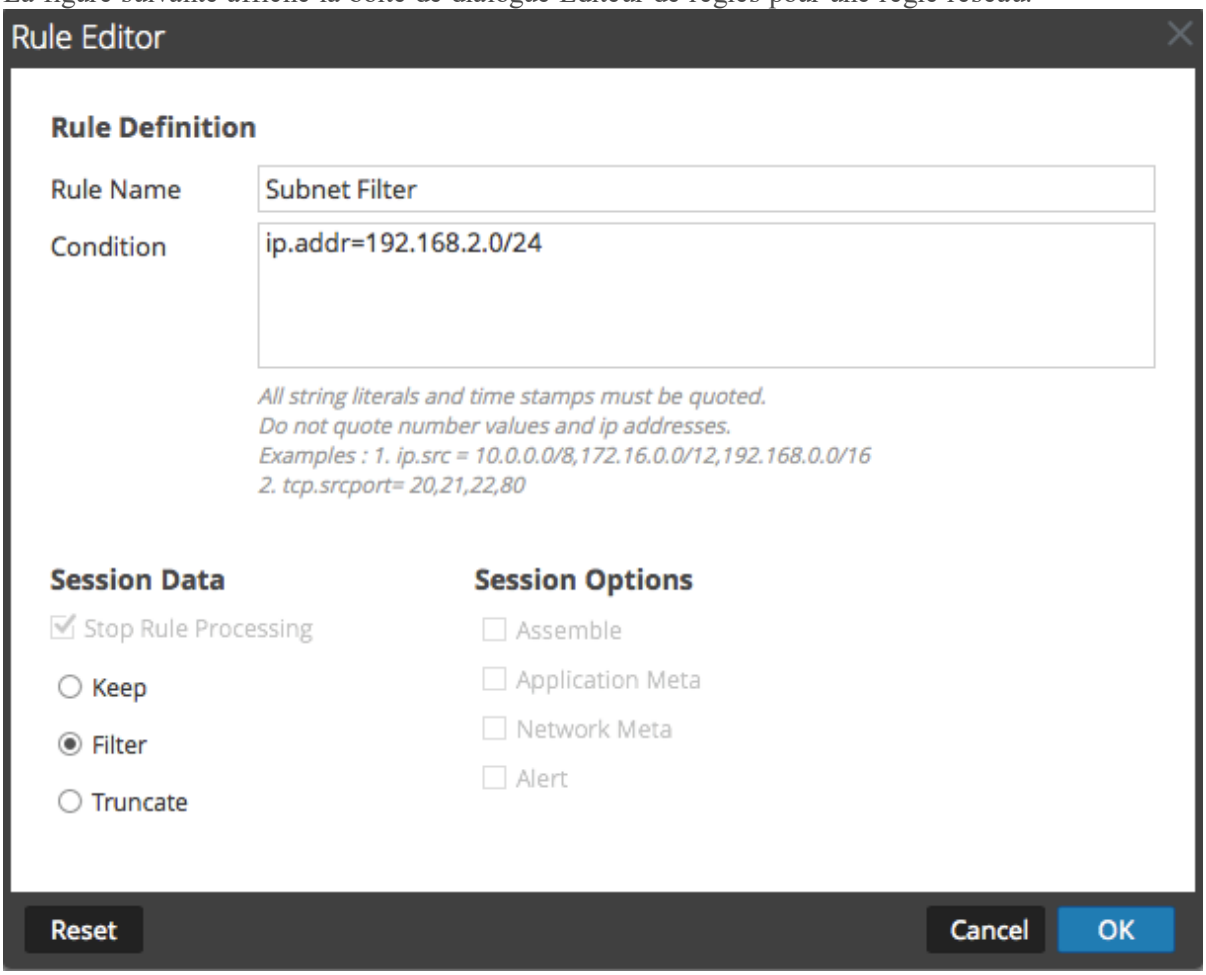
- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder
- Configurer les règles de Decoder
- Vue Configuration des services - onglets Règles

Aperçu rapide

La figure ci-dessous présente l'onglet Règles réseau.



La figure suivante affiche la boîte de dialogue Éditeur de règles pour une règle réseau.



Le tableau suivant décrit les colonnes de la grille Règles réseau.

Colonne	Description
En attente	Cette colonne indique si une règle dispose de modifications en attente. Les règles actuellement actives sur le Decoder ne disposent pas d'indicateur. Si la règle est nouvelle ou a été modifiée, la colonne contient . Une fois que les règles sont appliquées, l'indicateur en attente est supprimé.
Nom	Il s'agit du nom de la règle, un identifiant descriptif de la règle.
Condition	Il s'agit de la définition de la condition qui déclenche une action lorsqu'elle est rencontrée.
Données de paquet	Cette colonne affiche l'action des Données de session qui est réalisée lorsqu'un paquet correspond à la règle. Les valeurs possibles sont **Filtrer**, **Conserver** ou **Tronquer**.
Alerte	Cette colonne indique si le Decoder génère une alerte personnalisée lorsque les métadonnées correspondent à la règle. Les valeurs possibles sont **Activé** ou **Désactivé**.
État	Cette colonne indique si la règle est activée ou désactivée à l'aide d'une icône circulaire. Si le cercle est vert, la règle est activée. Si le cercle est vide, la règle est désactivée.

La boîte de dialogue **Éditeur de règles** propose les champs et options nécessaires pour définir une règle réseau.

Le tableau suivant décrit les champs Définition de règle.

Champ	Description
Nom de la règle	Nom descriptif qui identifie la règle.
Condition	Définition de la condition qui déclenche une action lorsqu'elle est remplie. Vous pouvez effectuer votre saisie directement dans le champ ou élaborer la condition dans ce champ à l'aide des métadonnées de la fenêtre Intellisense. Lors de l'élaboration de la définition de règle, Intellisense affiche des erreurs et avertissements de syntaxe. Dans les conditions, tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre et d'adresses IP entre guillemets.. Configurer les règles de Decoder fournit des informations supplémentaires. Cette section décrit également les clés méta prises en charge par NetWitness Platform pour être utilisées dans les conditions de règle réseau.

Le tableau suivant décrit les actions de la section Données de session.

Action	Description
Arrêter le traitement d'une règle	Si cette option est cochée, aucune nouvelle évaluation de règle ne se produira en cas de correspondance avec la règle, et la session sera enregistrée comme indiqué. Si cette option n'est pas cochée, l'évaluation des règles continue jusqu'à ce que toutes les règles soient évaluées.

Action	Description
Conserver	La charge du paquet et les métadonnées associées sont enregistrées lorsqu'elles correspondent à la règle.
Filtrer	Le paquet n'est pas enregistré lorsqu'il correspond à la règle.
Tronquer	La charge du paquet n'est pas enregistrée lorsqu'elle correspond à la règle, mais les en-têtes des paquets et autres métadonnées associées sont conservées.

Le tableau suivant décrit les options de session.

Action	Description
Assembler	Si l'option est cochée, l'assembleur assemble la chaîne de paquets lorsqu'elle correspond à la règle.
Méta réseau	Le paquet génère des métadonnées réseau lorsqu'il correspond à la règle.
Méta application	Le paquet génère des métadonnées d'application lorsqu'il correspond à la règle.
Alerte	Le paquet génère une alerte personnalisée lorsque les métadonnées correspondent à la règle.

Le tableau suivant décrit les actions de la boîte de dialogue Éditeur de règles.

Action	Description
Réinitialiser	Réinitialise le contenu de la boîte de dialogue aux valeurs précédant la modification ; les modifications sont ignorées.
Annuler	Annule toute modification et ferme la boîte de dialogue Éditeur de règles.
OK	Enregistre la nouvelle règle ou la règle modifiée, et l'ajoute à la grille de règles. La boîte de dialogue Éditeur de règles se ferme.
Enregistrer	(Règles avec une syntaxe obsolète uniquement) Applique une règle corrigée de manière individuelle au service Decoder. Reportez-vous à la section Corriger les règles contenant une syntaxe non valide.

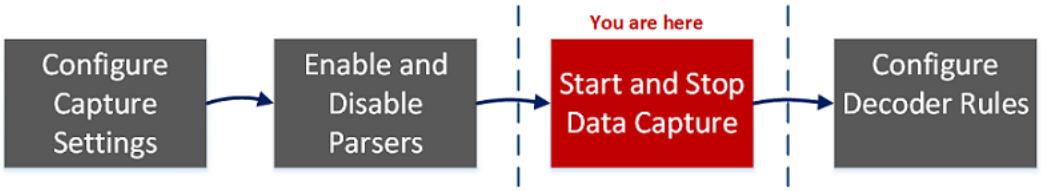
Vue Système de services - Decoders

Un Log Decoder est un type particulier de Decoder, et il est configuré et géré de manière équivalente à un Decoder. Ainsi, la plupart des informations de cette section se rapportent aux deux types de Decoders. Les différences concernant les Log Decoders sont annotées.

Pour accéder à la vue Système de services, accédez à **ADMIN > Services >** sélectionnez un Decoder ou un Log Decoder > > **Vue** > **Système**.

Workflow

La figure suivante illustre les tâches courantes de configuration de Decoder avec les étapes que vous pouvez effectuer dans cette vue mises en surbrillance.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Administrateur	configurer les paramètres de capture	Configurer les paramètres de capture
Administrateur	gérer les analyseurs et les analyseurs de logs*	Activer et désactiver les analyseurs et les analyseurs de logs
Administrateur	démarrer et arrêter la capture de données*	Démarrer et arrêter la capture de données
Administrateur	télécharger des fichiers de capture de paquets et de logs*	Télécharger un fichier log vers un Log Decoder Télécharger un fichier de capture de paquets
Administrateur	réinitialiser les statistiques de log, effectuer des tâches sur l'hôte, arrêter le service, arrêter le service d'appliance et redémarrer l'hôte*	*Guide de mise en route des hôtes et des services*
Administrateur	configurer des règles	Configurer les règles de Decoder

*Vous pouvez effectuer ces tâches ici.

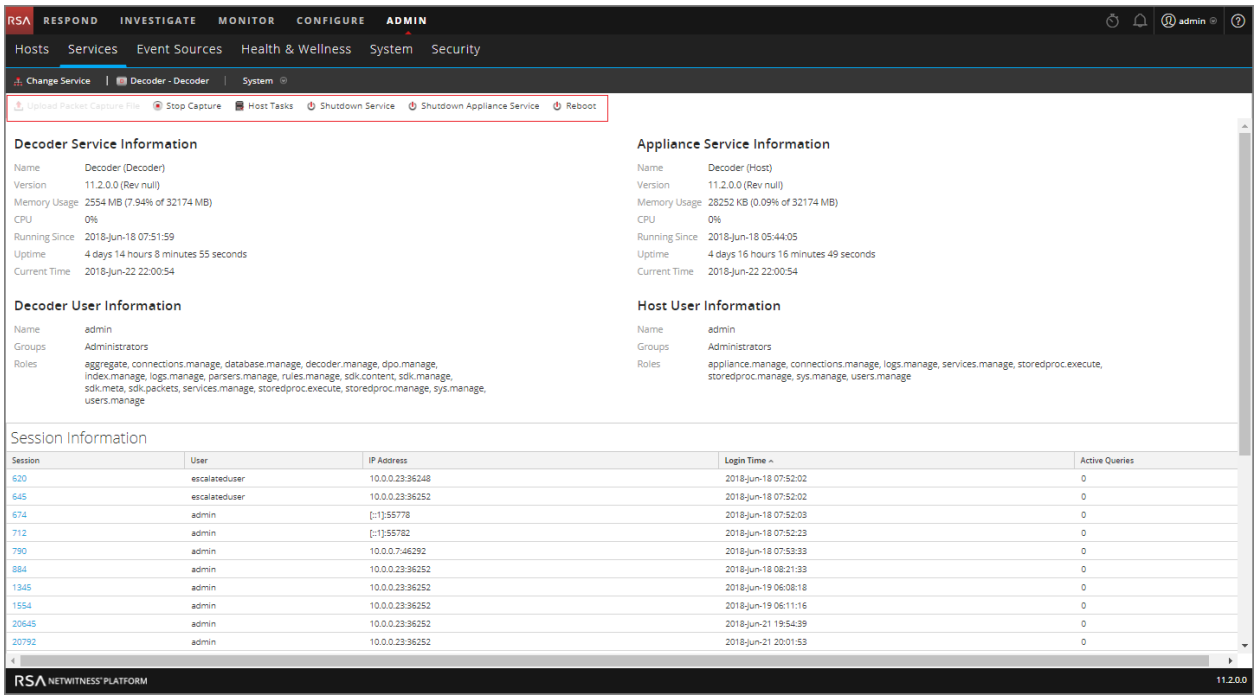
Rubriques connexes

Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

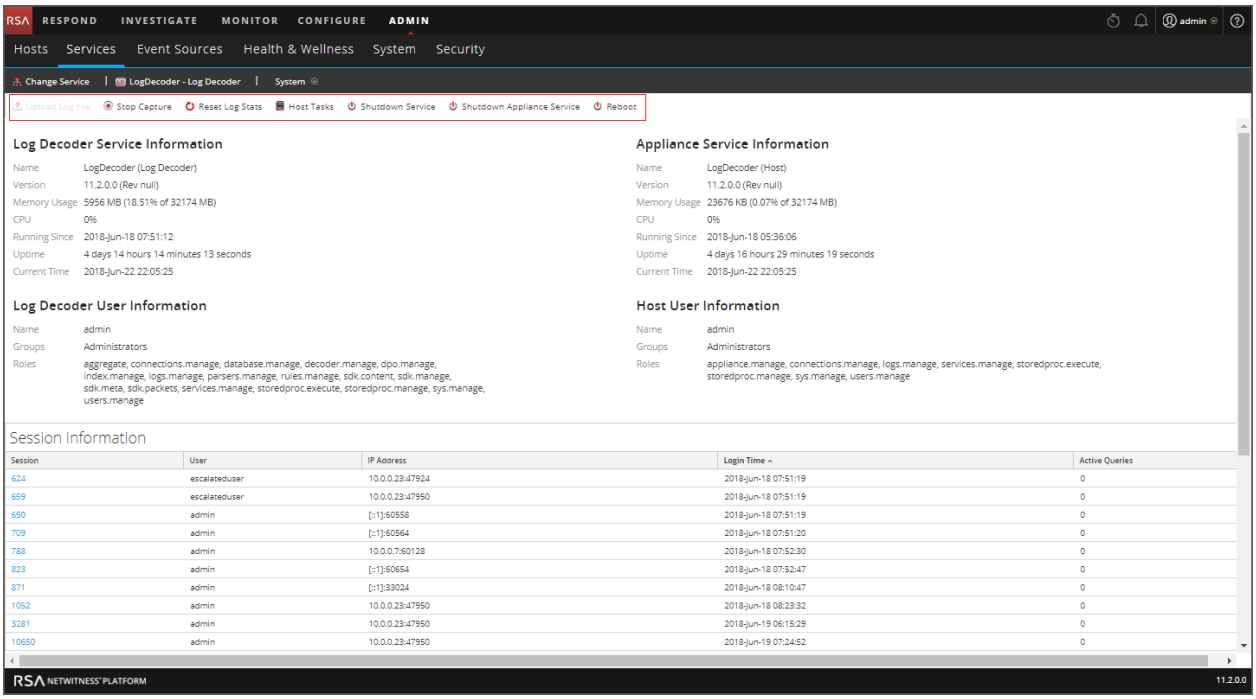
- Configuration rapide de Decoder et de Log Decoder
- Configurer les paramètres communs sur un Decoder
- « Vue Système de services » dans le *Guide de mise en route des hôtes et des services*

Aperçu rapide

Exemple de vue Configuration des services pour un Decoder.

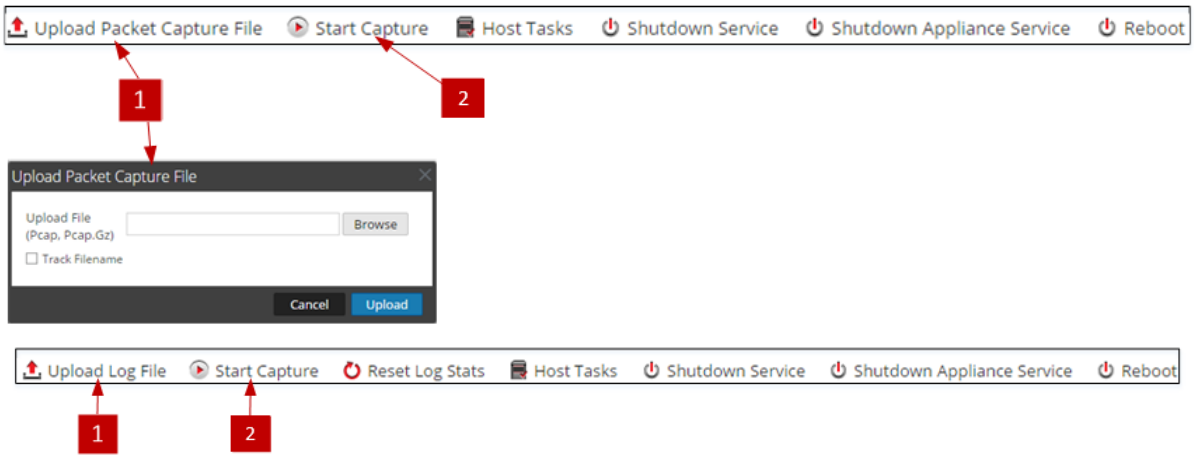


Exemple de vue Système de services pour un Log Decoder.



Barre d'outils Info services

Ces deux barres d'outils illustrent les options propres aux Decoders et aux Log Decoders.



En plus des options classiques dont vous disposez dans la barre d'outils de la vue Système de services, vous pouvez démarrer et arrêter la capture de paquets ou de logs. Les options de téléchargement de fichier sont différentes de celles du Decoder standard (fichier de capture de paquet) et du Log Decoder (fichier log).

Action	Description
Télécharger le fichier de capture de paquets	Affiche une boîte de dialogue qui propose une façon de sélectionner un fichier de capture de paquet (.pcap) à télécharger vers le Decoder sélectionné. Pour plus d'informations, reportez-vous à la rubrique Télécharger un fichier de capture de paquets. **Remarque :** Cette option ne s'applique pas aux Log Decoders.
Télécharger le fichier log	Affiche une boîte de dialogue qui propose un moyen de sélectionner un fichier log (.log) à télécharger vers le Log Decoder sélectionné. Pour plus d'informations, reportez-vous à la ribrique Télécharger un fichier log vers un Log Decoder.
Démarrer/arrêter la capture	Démarre la capture de paquet sur le Decoder sélectionné. Lorsque la capture de paquets est en cours, l'option de la barre d'outils se change en Arrêter la capture, et l'option pour télécharger un fichier est disponible.