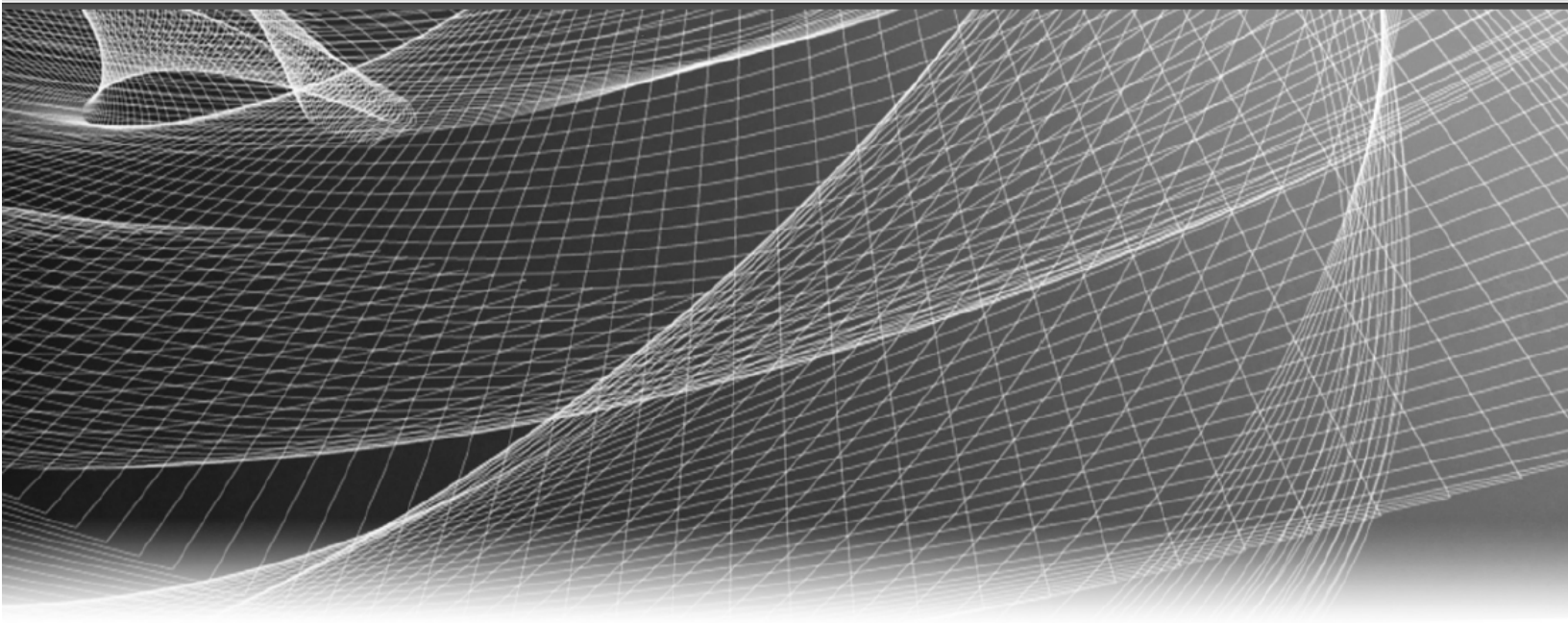


RSA Security Analytics

Decoder et Log Decoder
Guide de configuration

pour la version 10.6

RSA

EMC²

Marques commerciales

Contrat de licence

Licences tierces

Remarque sur les technologies de chiffrement

Distribution

Sommaire

Guide de configuration de Decoder et Log Decoder

Cette rubrique présente le Decoder et le Log Decoder ainsi que la méthode pour les configurer dans Security Analytics.

Topics

Fondamentaux de Decoder et Log Decoder

Cette rubrique présente le Decoder et le Log Decoder dans RSA Security Analytics.

Security Analytics prend en charge deux types de Decoders :

- Le Decoder, qui capture les données réseau sous forme de paquets.
- Le Log Decoder, qui capture les données de log sous forme d'événements.

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.

Lorsqu'un Decoder est ajouté, il devient visible et utilisable avec Security Analytics Administration, Live et Investigation. Pour ajouter un service dans Security Analytics, sélectionnez le type de service, fournissez les informations de connexion et validez que le service peut être accessible.

La configuration du Decoder pour capturer des données implique de sélectionner un adaptateur de capture et de choisir les paramètres du cache et de la capture.

Lorsque le Decoder est disponible dans Security Analytics, il est prêt à capturer le trafic. Vous pouvez configurer chaque Decoder pour contrôler le type de trafic capturé à l'aide de règles, de feeds et de parsers.

Procédures requises

Il s'agit des étapes de configuration requises pour un nouveau Decoder ou Log Decoder, et de modification de la configuration d'un Decoder existant. Sauf indication contraire, Decoder se rapporte au paquet et aux logs Decoders. Suivez les étapes de la section dans l'ordre où elles sont indiquées.

Étape 1 : Vérifier la configuration système

La vérification de la configuration du système est la première étape qui doit être réalisée quand un nouveau service est ajouté à Security Analytics.

Certaines valeurs par défaut des paramètres de configuration du système sont déjà en vigueur. Ces valeurs peuvent être modifiées et affinées pour une performance optimale.

Étape 2 : Configurer les paramètres de capture

Ensuite, vous pouvez configurer l'adaptateur pour la capture de données, activer le démarrage automatique de capture de données, sélectionner les analyseurs qui sont appliqués aux données saisies et optimiser la capture de données en configurant les paramètres de capture.

Étape 3 : Activer ou désactiver les analyseurs

Vérifiez les analyseurs qui ont été téléchargés et déployés depuis Live et gérez ceux qui sont activés ou désactivés.

Étape 4 : 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. 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.

Par défaut, aucune règle n'est définie lors de la première installation de Security Analytics. 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 de couche réseau, règles de couche application et règles de corrélation.

Étape 5 : 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.

Topics

Étape 1. Vérifier la configuration système

Cette rubrique présente une procédure pour vérifier la configuration système d'un Decoder ou Log Decoder.

Lorsqu'un service est ajouté pour la première fois à Security Analytics, les valeurs par défaut des paramètres de configuration système s'appliquent. Vous pouvez modifier ces valeurs pour optimiser les performances.

System Configuration

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

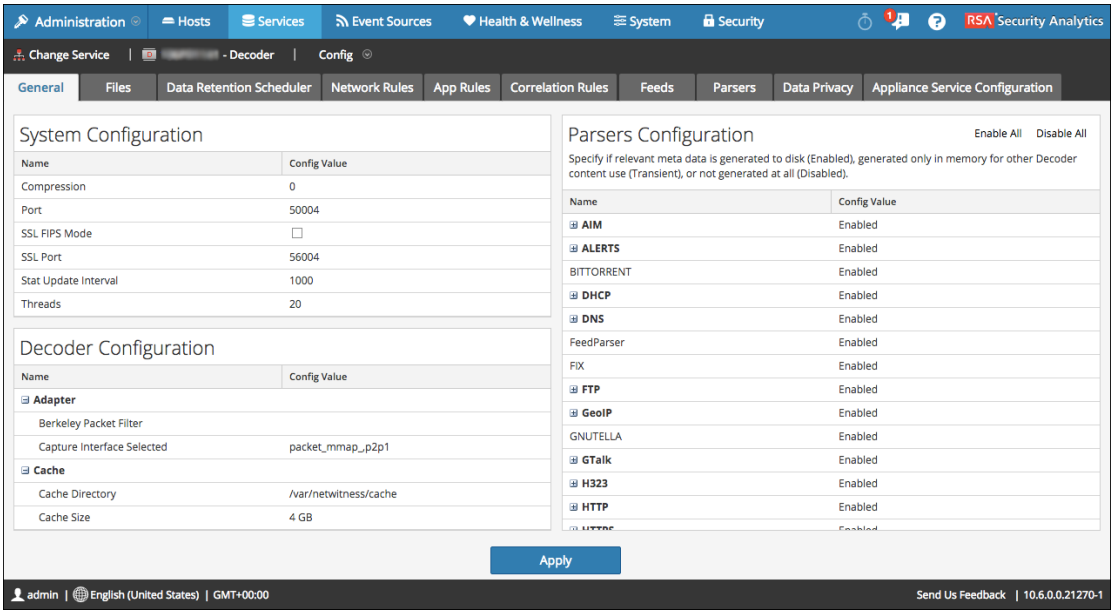
Dans la plupart des cas, les valeurs par défaut pour la compression, l'intervalle de mise à jour des statistiques et le nombre de threads dans le pool de threads sont configurées de façon à optimiser les performances système. Vous souhaiterez peut-être modifier le paramètre SSL de votre environnement, 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.

Procédure

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

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services**, sélectionnez un service Decoder ou Log Decoder et cliquez sur  **>>Vue > Config**.

La vue Configuration des services correspondant à ce service s'ouvre sur l'onglet Général.



3. Dans **Configuration système**, cliquez dans un champ que vous souhaitez modifier et saisissez la nouvelle valeur.
4. Lorsque la modification est terminée, cliquez sur **Appliquer.**

Étape 2. Configurer les paramètres de capture

Cette rubrique présente une procédure pour la configuration de la capture de données sur les Decoders et Log Decoders.

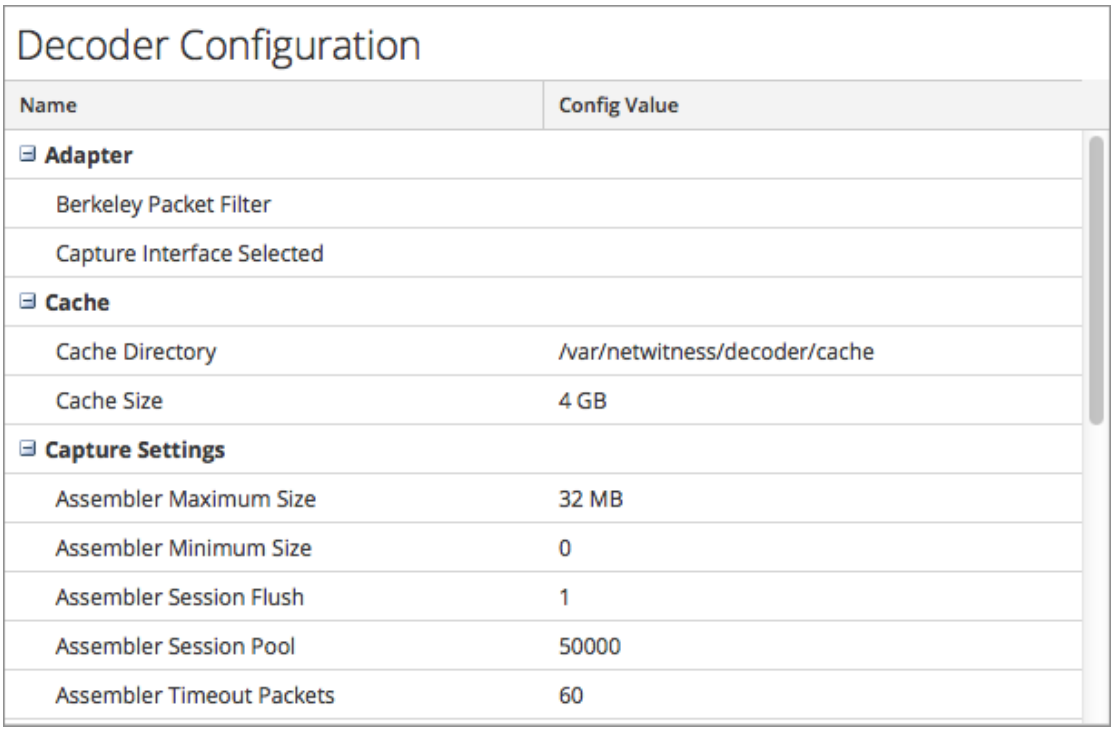
Dans RSA Security Analytics, vous pouvez configurer l'adaptateur pour la capture de données, activer le démarrage automatique de la capture des données, sélectionner les parsers qui sont appliqués aux données capturées et régler la capture.

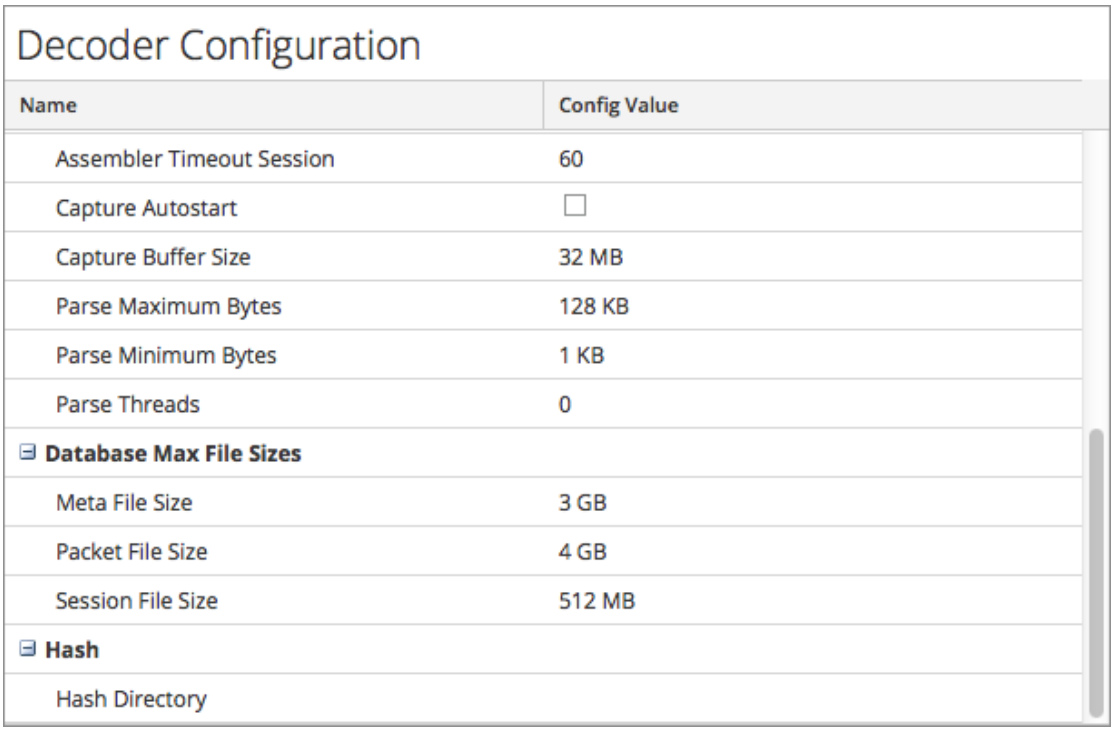
Procédure

Pour configurer un Decoder en vue de la capture de données :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services d'administration**, sélectionnez un service Decoder, puis  **> Vue > Config.**

   La vue Configuration des services affiche l'onglet Général. Les paramètres de services les plus couramment utilisés pour un Decoder ou un Log Decoder peuvent être modifiés sous Configuration de Decoder.





3. Dans la section relative aux **paramètres de l'adaptateur**, configurez l'interface réseau pour la capture des données.
4. Dans la section **Cache**, vérifiez le répertoire et la taille du cache. Si nécessaire, modifiez ces paramètres.
5. Dans les sections **Paramètres de capture**, vérifiez les valeurs par défaut et modifiez-les si nécessaire.
6. Pour que le Decoder commence automatiquement la capture des données au démarrage, cochez l'option de **démarrage automatique de la capture**.
7. Dans la section **Tailles de fichier maximales de la base de données**, vérifiez les valeurs par défaut et modifiez-les si nécessaire.
8. Dans la section relative au **hachage**, définissez un répertoire pour les fichiers de hachage si vous utilisez cette fonction.
9. Exécutez l'une des opérations suivantes :
   - Dans le panneau **Configuration des analyseurs**, vérifiez les parsers sélectionnés pour filtrer le trafic et désactivez-les, activez-les ou marquez-les comme transitoires selon vos besoins.

- Si vous configurez un Log Decoder, vérifiez les parsers sélectionnés pour filtrer le trafic dans la section **Configuration des analyseurs de services**, puis désactivez-les, activez-les ou marquez-les comme transitoires selon vos besoins.

10. Pour enregistrer les modifications, cliquez sur **Appliquer**.
11. Si vous devez appliquer les modifications, accédez à la vue **Système des services**, puis redémarrez le service.
    À ce stade, vous pouvez commencer la capture (également dans la vue Système de services).

Configurer le filtrage de paquets BPF au niveau du système

Cette rubrique décrit comment utiliser les Berkeley Packet Filters (BPF) pour contrôler les paquets et logs qui sont traités par un Decoder.

Vous pouvez utiliser les BPF (Berkeley Packet Filter) pour contrôler les paquets et les logs qui sont traités par un Decoder. Decoder prend en charge le filtrage des paquets au niveau système, défini à l'aide de la syntaxe tcpdump/libpcap. La spécification d'un filtre Libpcap peut réduire efficacement le volume du paquet en fonction d'attributs Couche 2 - Couche 4. 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).

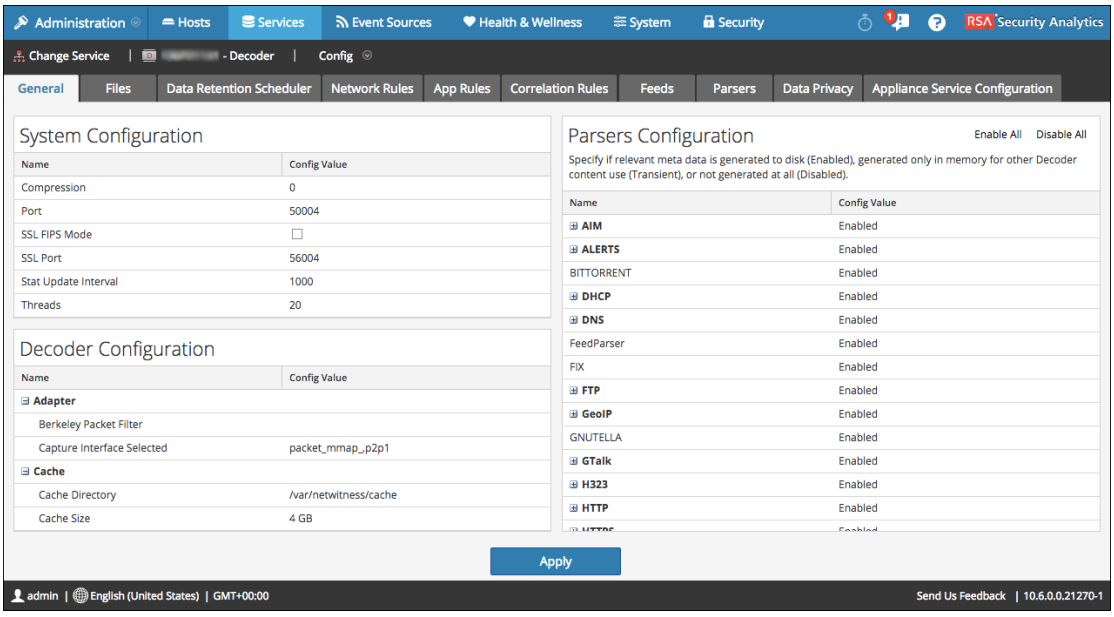
Un filtre libpcap s'avère approprié lorsqu'un Decoder reçoit un volume de trafic qui augmente la charge des ressources physiques de la plateforme. Dans ce scénario, le Decoder peut abandonner les paquets de manière régulière et disposer d'un grand nombre de pages de capture (/decoder/stats/capture.pagefree est élevé).

Ajouter des filtres de paquets niveau système

Pour ajouter un filtre de paquets Berkeley niveau système :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Dans la vue **Services d'administration**, sélectionnez un service Decoder, puis  **> 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 **et**.
   L'interface utilisateur SA 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 l'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 effet important et potentiellement perturbateur sur l'utilisation de filtres de paquets. À titre de 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 formater 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 ça n'est pas le résultat d'une logique au sein du logiciel NetWitness.

Tests

Avant de les mettre en œuvre, et afin de s'assurer qu'ils fourniront 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 niveau système, vous pouvez le convertir. Il y a peu d'éléments à mémoriser lors de la réalisation de conversions.

- **&&** ou **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 **et**.

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 du port UDP 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)**.

Étape 3. Activer et désactiver les parsers de logs

Cette rubrique indique aux administrateurs comment activer ou désactiver les analyseurs de logs sur un Log Decoder.

Cette procédure est utile pour voir quels analyseurs de logs ont été téléchargés et déployés depuis Live, et ceux qui sont activés.

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 des analyseurs, plus vous créez des métas, ce qui influe sur la conservation des données.
- Le fait de ne pas avoir d'analyseurs de logs supplémentaires (inutiles) déployés réduit le risque de mauvaise interprétation des messages.

Conditions préalables

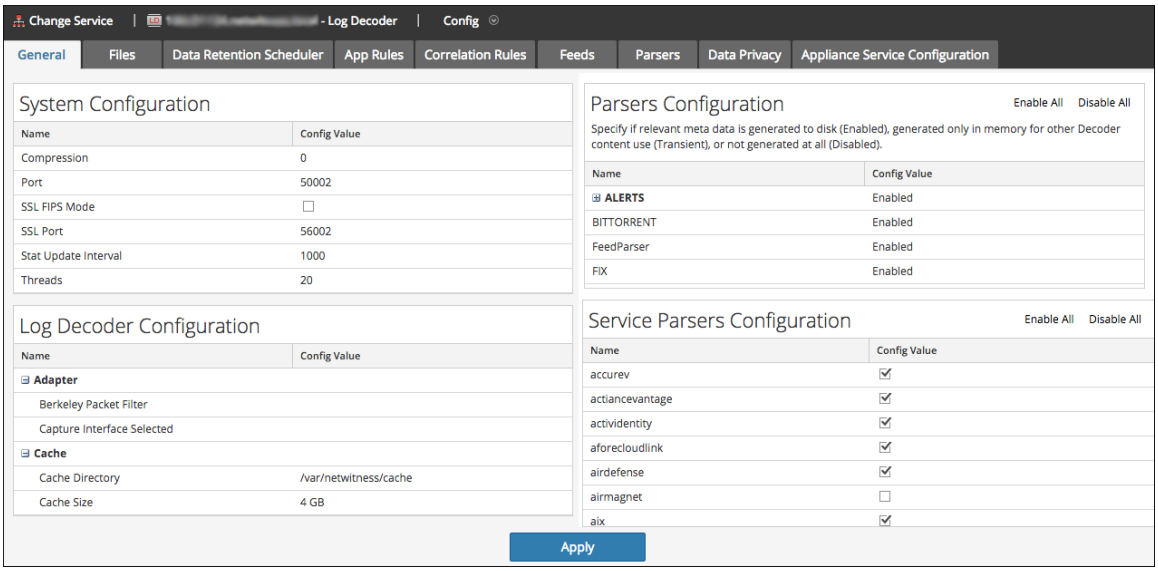
Vous devez avoir déjà déployé des analyseurs de logs depuis Live. Consultez la rubrique **Trouver et déployer des ressources Live** dans *Gestion des services en direct* pour obtenir plus d'informations.

Procédure

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

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans la grille **Services**, sélectionnez un Log Decoder et depuis le menu **Actions** (), choisissez **Vue** > **Configuration**.
3. Dans le panneau **Configuration des analyseurs de services**, recherchez votre source d'événement.
4. Dans la colonne **Valeur de configuration**, notez l'état actuel de votre analyseur.
   - Si l'analyseur est déjà sélectionné, il est activé.
   - S'il n'est pas sélectionné, il est désactivé actuellement

Vous pouvez basculer la valeur pour tout analyseur de log individuel. Sinon, vous pouvez sélectionner **Activer tout** ou **Désactiver tout** pour mettre à jour l'état de tous vos analyseurs de logs à la fois.



5. Cliquez sur **Apply**.

Lorsque vous cliquez sur **Appliquer**, notez que tous les analyseurs sont rechargés dans Security Analytics.

Résultat

L'état de chaque analyseur de log est mis à jour, en fonction de vos sélections.

Étape 4. 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.

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.

Instructions relatives aux règles et requêtes fournit des instructions que toutes les requêtes et conditions de règle des services Security Analytics Core doivent suivre.

Par défaut, aucune règle n'est définie lors de la première installation de Security Analytics. 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 de couche réseau, règles de couche application et règles de corrélation.

Règles de couche réseau

Les règles de couche 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 couche réseau ne sont disponibles que sur les Decoder paquets.

Règles de couche application

Les règles de la couche 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.

Règles de corrélation

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.

Utilisations courantes

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

- alerter, puis 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 ;

Groupes de règles

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 Security Analytics, 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.

Configuration des règles

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.

Syntaxe des règles de capture

La syntaxe d'écriture des règles de capture consiste à comparer un champ à une valeur à l'aide d'un opérateur de comparaison. Les opérateurs de comparaison pris en charge sont l'opérateur d'égalité (=) et l'opérateur de différence (!=).

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. Les plages sont utilisées dans les comparaisons basées sur les opérateurs de supériorité (>) et d'infériorité (<). 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.

Le tableau suivant résume les opérateurs de comparaison pris en charge et la syntaxe d'expression des valeurs.

Syntaxe	Description :
*	Règle par défaut. Si vous utilisez un astérisque (*) en tant que caractère unique dans une règle, celle-ci sélectionne la totalité du trafic.
=	Opérateur égalité.
!=	Opérateur d'inégalité.
&&	Opérateur ET logique.
||	Opérateur OU logique.
-u	Limite supérieure. 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. Par exemple, pour sélectionner tous les ports TCP en dessous du port 40000, la syntaxe est la suivante : `tcp.port = 1-40000`
(tiret)	Désigne une plage. Ceci s'applique uniquement à des 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`

Syntaxe	Description :
, (virgule)	Désigne une liste de valeurs. Vous pouvez combiner l'utilisation de valeurs individuelles, de plages et de limites supérieure ou inférieure. 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)`

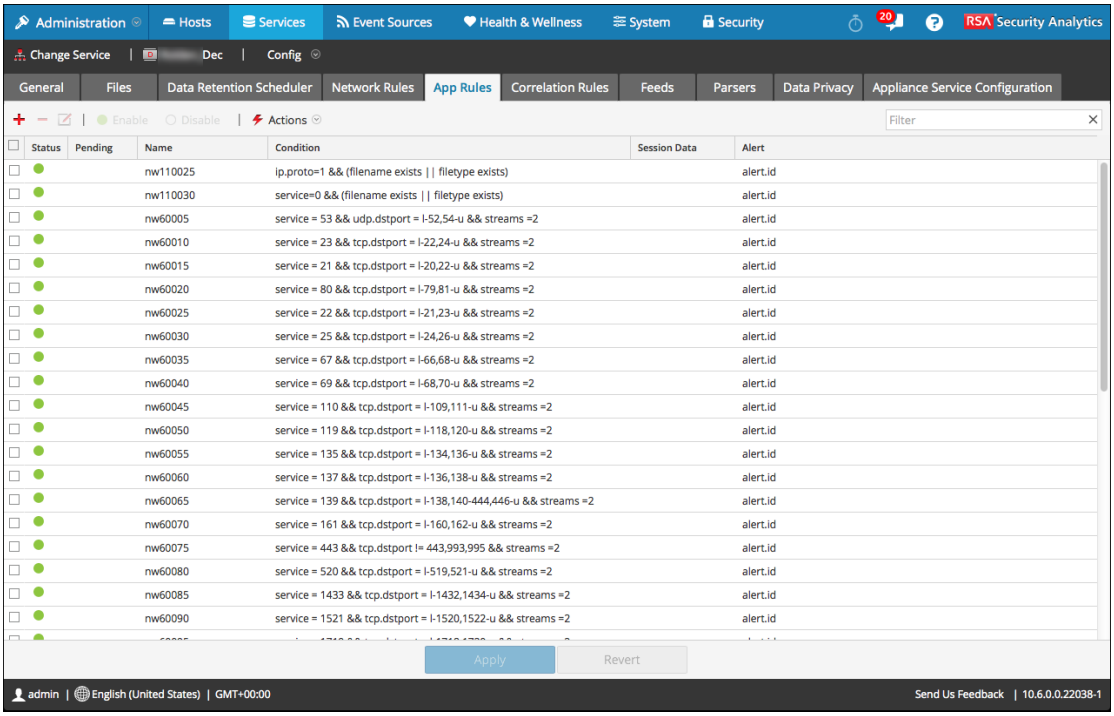
Instructions relatives aux règles et requêtes fournit des instructions que toutes les requêtes et conditions de règle des services Security Analytics Core doivent suivre.

Procédures

Configurer les règles de capture

1. Dans le menu **Security Analytics**, sélectionnez **Administration > 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 grille des règles correspondant au type de règles sélectionné s'affiche.



Chaque type de règles possède une grille 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 grille. Pour changer la séquence d'exécution des règles, effectuez un glisser-déplacer de ces dernières vers l'emplacement approprié dans la grille, ou utilisez les options de menu contextuel pour les réorganiser au sein de la grille.
- Pour sélectionner une seule ligne, cliquez sur celle-ci.
- 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 grille, 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**.

Ajouter une règle

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 audessus** ou **Insérer en dessous** dans le menu contextuel.
  La boîte de dialogue Éditeur de règles s'affiche pour ce type de règle.

Pour obtenir des détails supplémentaires, consultez l'une des sections suivantes :

- Configurer des règles d'application
- Configurer des règles réseau
- Configurer des règles de corrélation

Supprimer une règle

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

Modifier une règle

1. Sous l'onglet Règles, sélectionnez la règle à modifier.
2. Cliquez sur  , ou doubleeliquez sur la ligne de la règle.
   La boîte de dialogue Éditeur de règles s'affiche pour ce type de règle. Pour obtenir des détails supplémentaires, consultez l'une des sections suivantes :

- Configurer des règles d'application
- Configurer des règles réseau
- Configurer des règles de corrélation

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 grille, mais elle est toujours activée dans le service.

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 grille, mais elle est toujours désactivée dans le service.

Importer des règles à partir d'un fichier

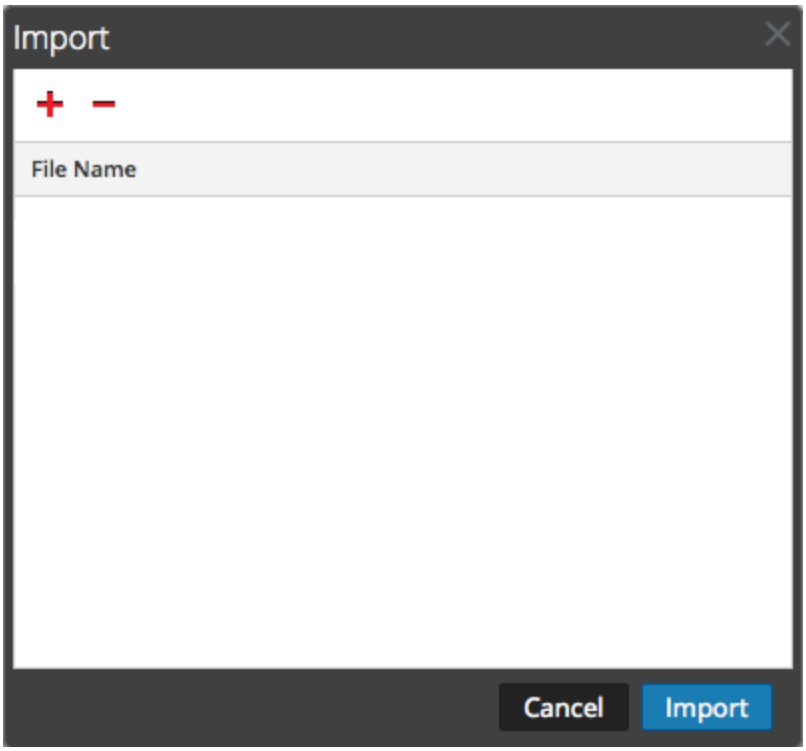
Vous pouvez importer des règles réseau, d'application et de corrélation dans Decoder à partir d'un fichier qui contient des règles du même type. Une fois ces règles importées, vous pouvez les modifier et les gérer comme les autres règles.

Lorsque vous essayez d'importer un groupe de règles, Security Analytics Administration vérifie le type de règles importé. 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 :

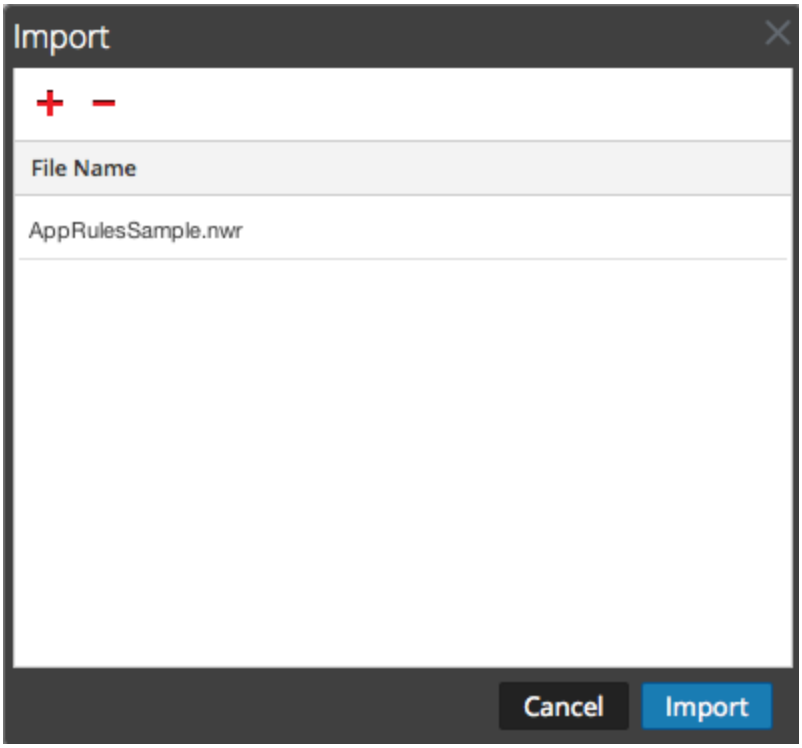
1. Dans l'onglet Règles, sélectionnez Actions > **Importer**.

   La boîte de dialogue Importer s'affiche.



2. Cliquez sur + .
   La structure de 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.

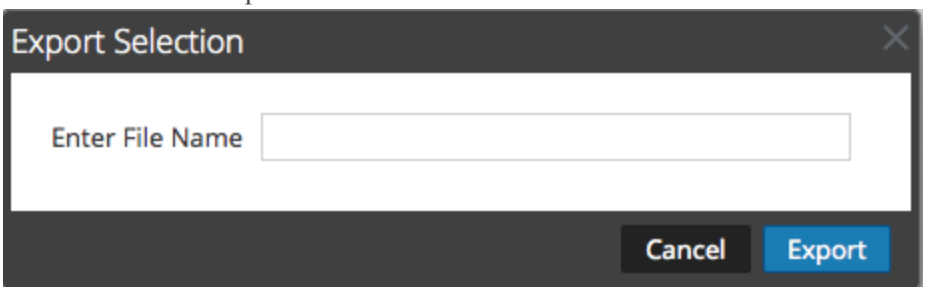


4. Cliquez sur **Importer**.
   Les règles sont importées dans l'interface utilisateur. Les règles importées présentent un angle rouge dans chaque colonne modifiée.
5. Modifiez ou réorganisez les règles, si nécessaire.
6. Pour enregistrer les règles dans le service, cliquez sur **Appliquer**.
   Les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

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 Actions > **Exporter** > **Sélection**. (**Exporter** > **Tout** exporte toutes les règles de la grille, 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

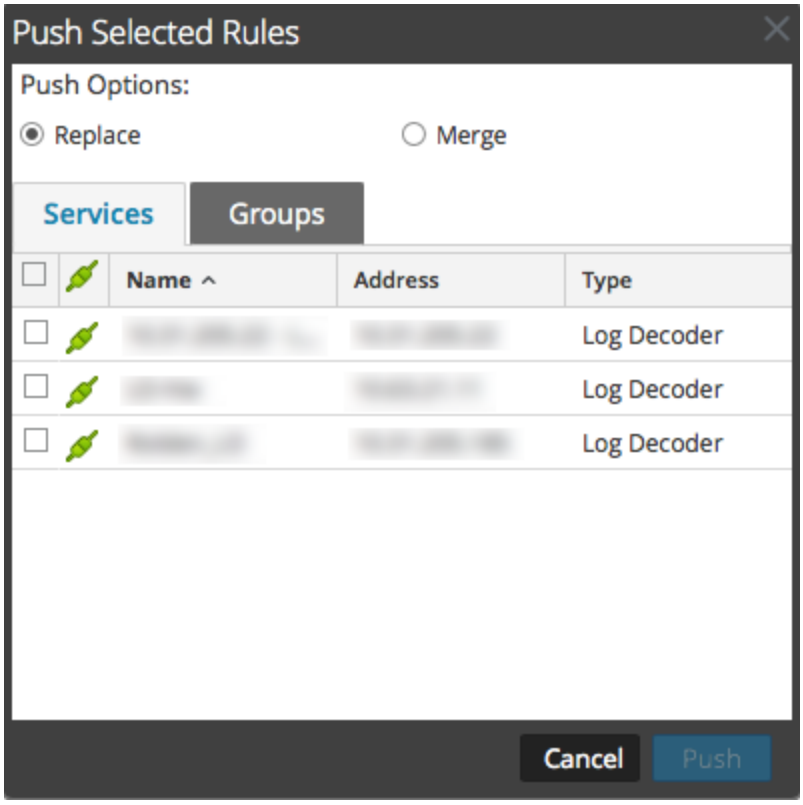
Vous pouvez transmettre (push) des règles ou les règles sélectionnées à d'autres services (Decoder ou Log Decoder) ou groupes de services.

Transmettre les règles sélectionnées

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 Actions > **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 **Remplacer** pour supprimer toutes les règles sur les services de destination et les remplacer par les règles sélectionnées. il s'agit de 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 **Push**.
   Les règles sont transmises aux services sélectionnés, puis entrent en vigueur immédiatement.

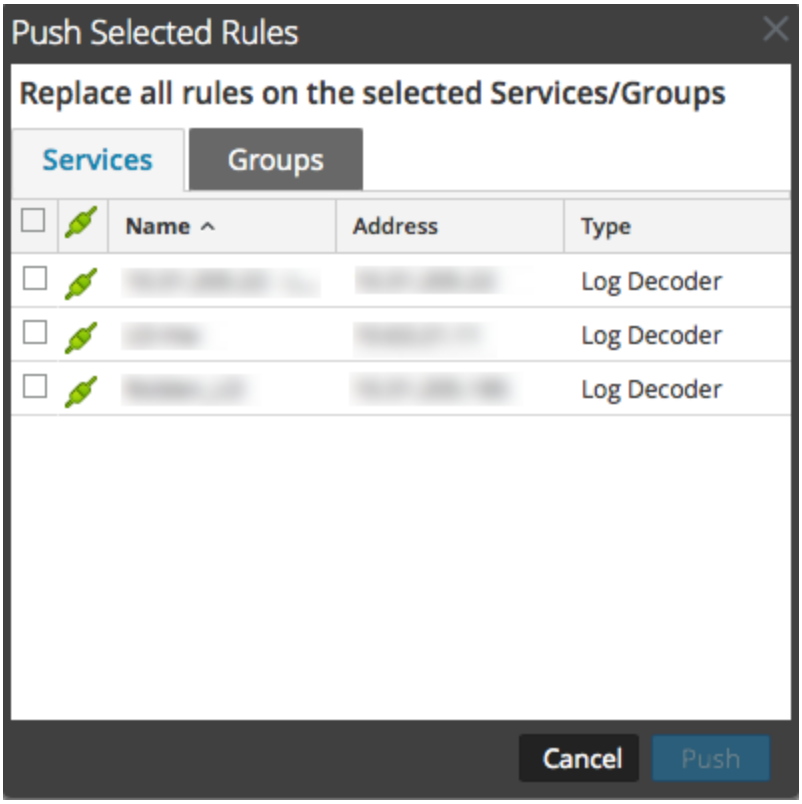
Transmettre toutes les règles

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

1. Dans un onglet Règles, sélectionnez Actions > **Transmettre** > **Tout**.
   (**Transmettre** > **Tout** transmet toutes les règles de la grille même si vous avez sélectionné

un sousensemble 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 **Push**.
   Toutes les règles des services de destination sont supprimées et remplacées par toutes les règles des services source. Les règles prennent effet immédiatement.

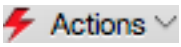
Changer la séquence d'exécution des règles

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

- Effectuez un glisserdéplacer des règles vers l'emplacement approprié dans la grille.
- 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

Security Analytics conserve les dix derniers snapshots de règle appliqués à un service. Pour restaurer un snapshot de règles à partir de l'historique :

1. Sélectionnez  > **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 grille, 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

Cette rubrique présente des règles d'application et donne des instructions pour créer des règles d'application.

Les règles de la couche application sont appliquées au niveau de la session.

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 : Truncate

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 : Filtre

Procédures

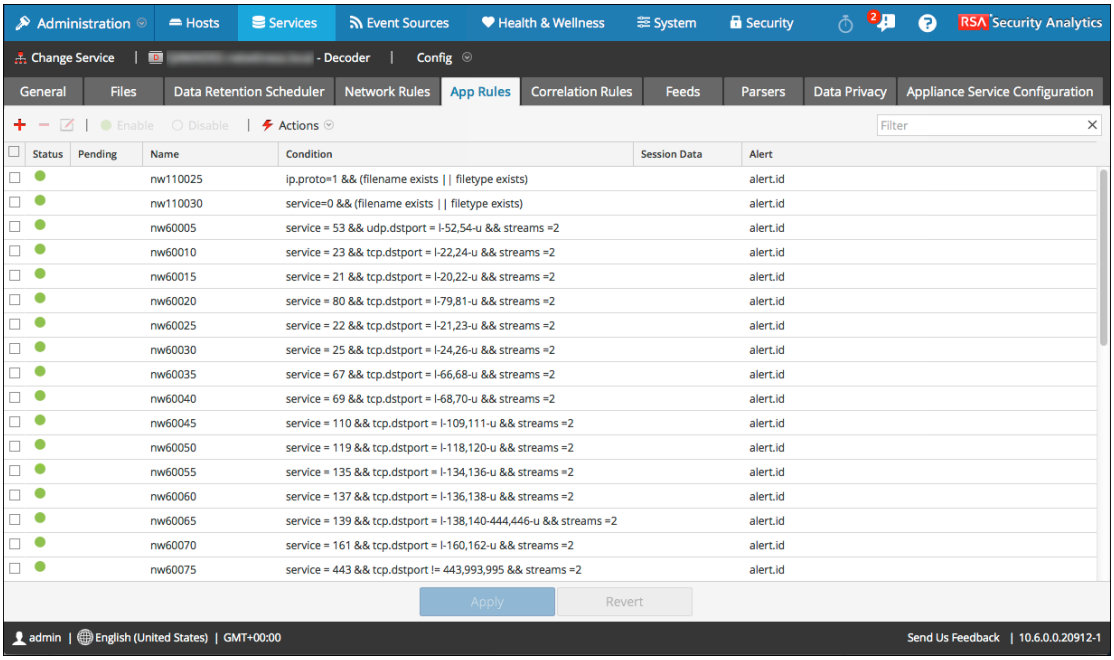
Accéder à l'onglet Règles d'application

L'accès à l'onglet Règles d'application est toujours la première étape dans la définition des règles d'application. Pour accéder à l'onglet Règles d'application :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service Decoder ou Log Decoder, puis **> Vue > Config**.

   La vue Configuration des services pour le service sélectionné s'affiche.

3. Sélectionnez l'onglet **Règles d'application**.

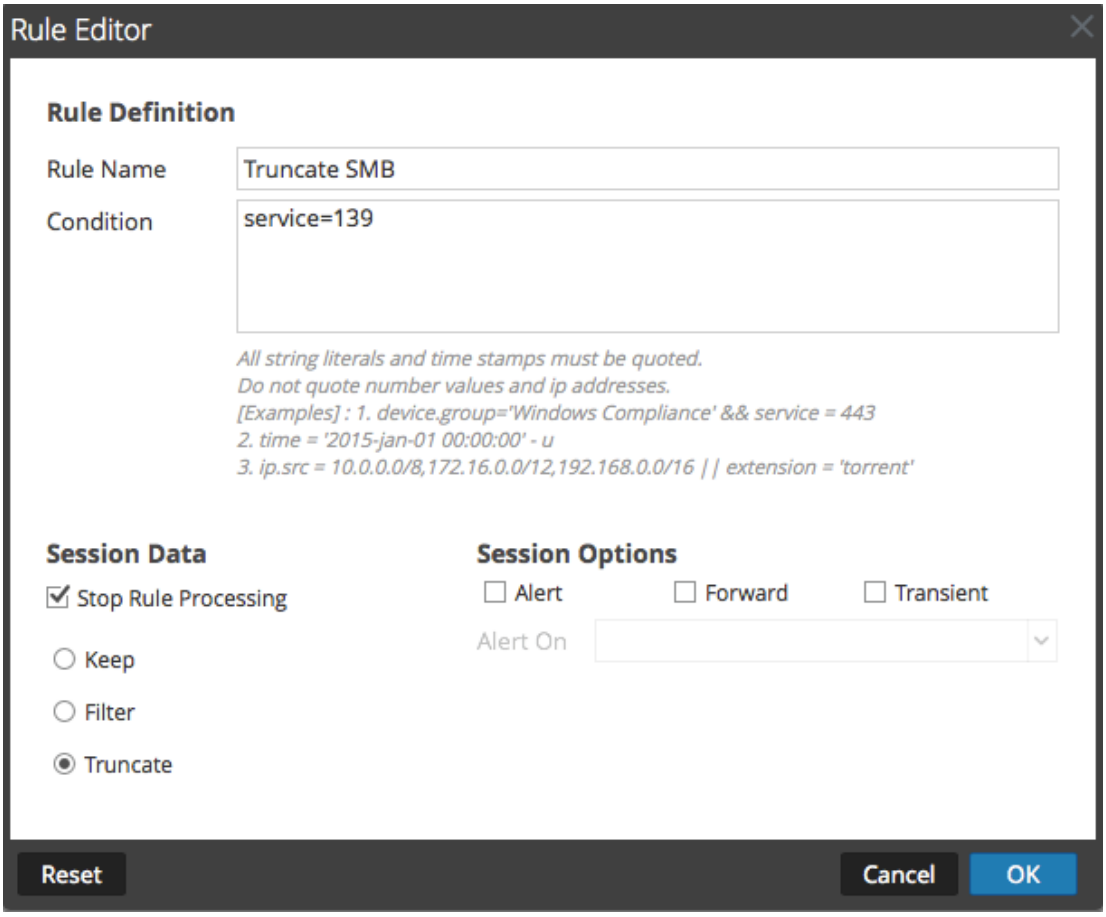


Ajouter ou modifier une règle d'application

Sous l'onglet Règles d'application :

1. 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 
     .

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



3. 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**.
4. 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, Security Analytics 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 ni les adresses IP entre guillemets. La section Instructions relatives aux règles et requêtes fournit des informations supplémentaires.
5. Si vous souhaitez mettre fin à l'évaluation de cette règle, activez la case à cocher **Arrêter le traitement des règles**.
6. 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.

7. 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**.

     Remarque : 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 destination du transfert Syslog spécifié dans le paramétrage Log Decoder > Vue > Explorer > /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**.

8. 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**.
9. Vérifiez que la séquence d'exécution de la règle est correcte par rapport aux autres règles de la grille. Si nécessaire, déplacez la règle.
10. Pour appliquer la règle mise à jour au Decoder ou Log Decoder, cliquez sur **Appliquer**.
    Security Analytics enregistre un snapshot des règles en cours d'application, puis applique l'ensemble mis à jour au Decoder et supprime l'indicateur En attente des règles qui étaient en attente.

Configurer des règles de corrélation

Cette rubrique présente les règles de corrélation et propose des procédures pour créer 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. Security Analytics 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.

Exemples de règles de corrélation

Objectif : Dans les sessions where tcp.dstport exists, s'il y a une combinaison de ip.src et ip.dst avec le nombre d'instances uniques 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
- Rule: tcp.dstport exists
- Instance Key: ip.src,ip.dst
- Threshold: u_count(tcp.dstport)>5
- Période : 1 minute

Objectif : Dans les sessions where action==login et error==fail, s'il y a une combinaison de ip.src avec 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
- Rule: action='login' && error='fail'
- Instance Key: ip.src,ip.dst
- Threshold: count()>10
- Période : 5 minutes

Explication

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 qui correspondent 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 au seuil spécifié est **tcp.dstport**. Nous comptons des cas 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 avons alors une session.id unique 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.

Procédures

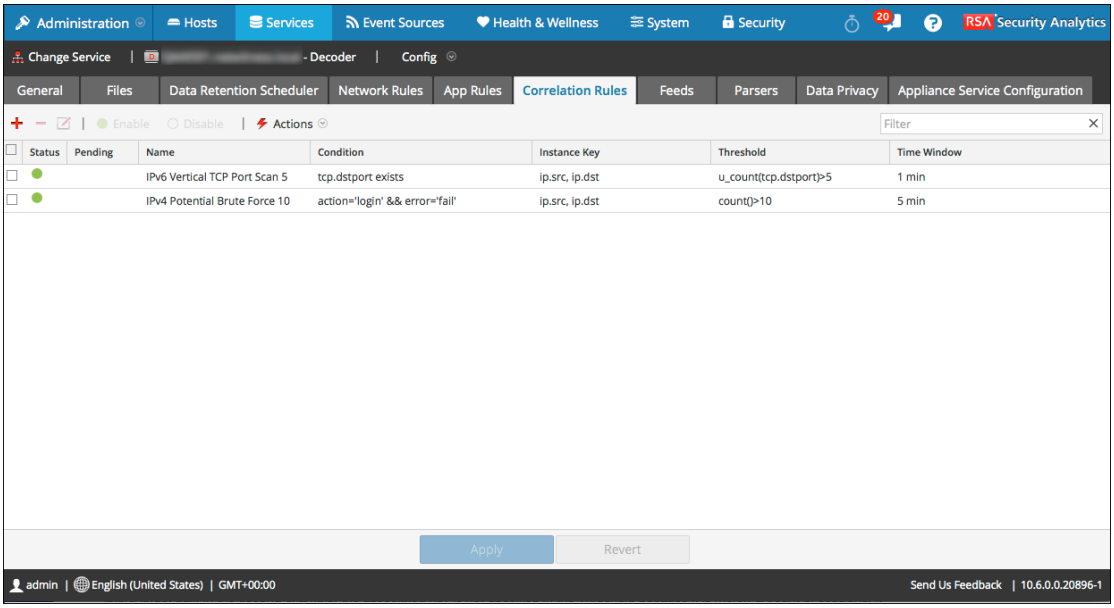
Accéder à l'onglet Règles de corrélation

La première étape dans l'utilisation des règles de corrélation consiste à accéder à l'onglet Règles de corrélation :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service et  **>>Vue > Configuration**.

   La vue Configuration des services pour le service sélectionné s'affiche.

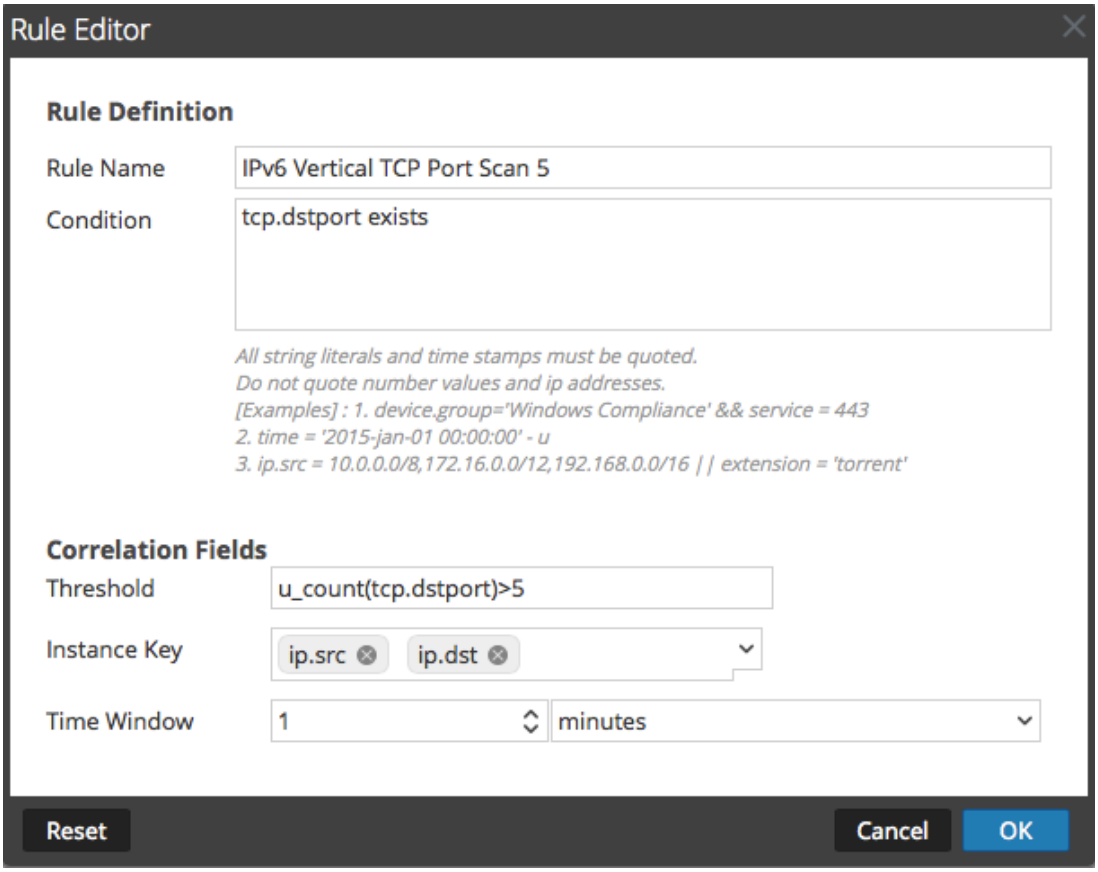
3. Sélectionnez l'onglet **Règles de corrélation**.



Ajouter ou modifier une règle de corrélation

1. 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 des règles et cliquez sur 
     .
     La boîte de dialogue Éditeur de règles s'affiche avec les paramètres de la règle de

corrélation.



2. 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**.
3. 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 Security Analytics. 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 ni les adresses IP entre guillemets. La section Instructions relatives aux règles et requêtes fournit des informations supplémentaires.
4. 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)

5. 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).
6. Dans **Période**, définissez la durée pendant laquelle le seuil doit être atteint pour créer une session de corrélation.
7. 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**.
8. Vérifiez que la séquence d'exécution de la règle est correcte par rapport aux autres règles de la grille. Si nécessaire, déplacez la règle.
9. Pour appliquer la règle mise à jour au service, cliquez sur **Appliquer**.

   Security Analytics enregistre un snapshot des règles actuellement appliquées, puis applique l'ensemble mis à jour au Decoder ou Log Decoder.

Configurer des règles réseau

Cette rubrique présente les règles et procédures du réseau pour configurer des règles réseau.

Les règles de couche réseau sont appliquées au niveau des paquets sur un Decoder. Elles sont constituées des groupes de règles de la couche 2 à la couche 4. 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 décodeurs de paquets.

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 : Filtre

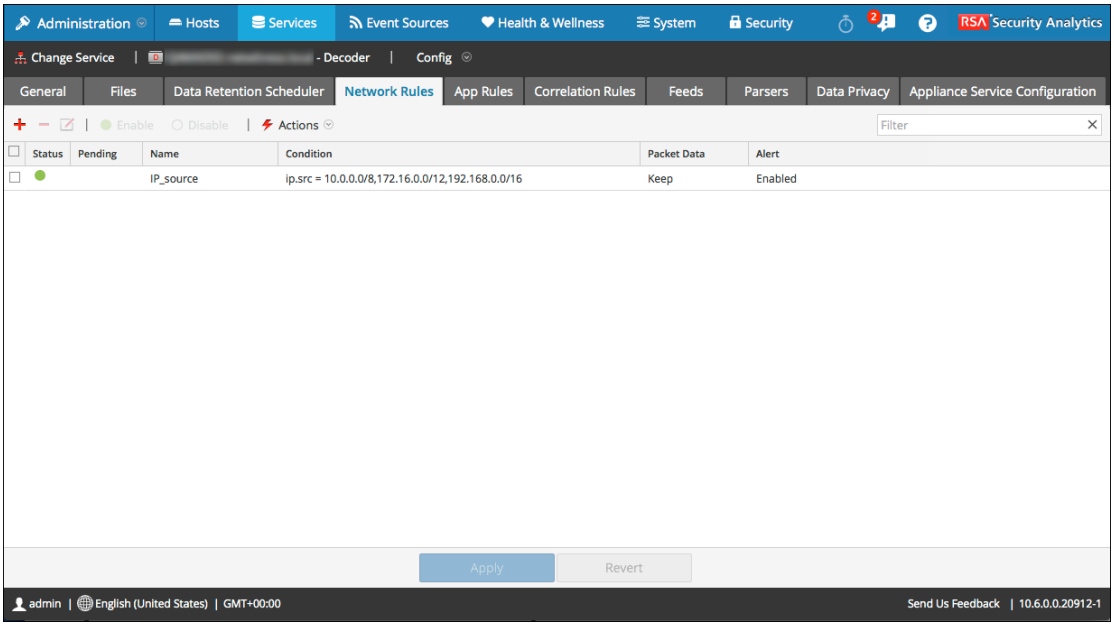
Procédures

Accédez à l'onglet Règles réseau.

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service Decoder et  **>>Vue > Config**.

   La vue Configuration des services pour le service sélectionné s'affiche.

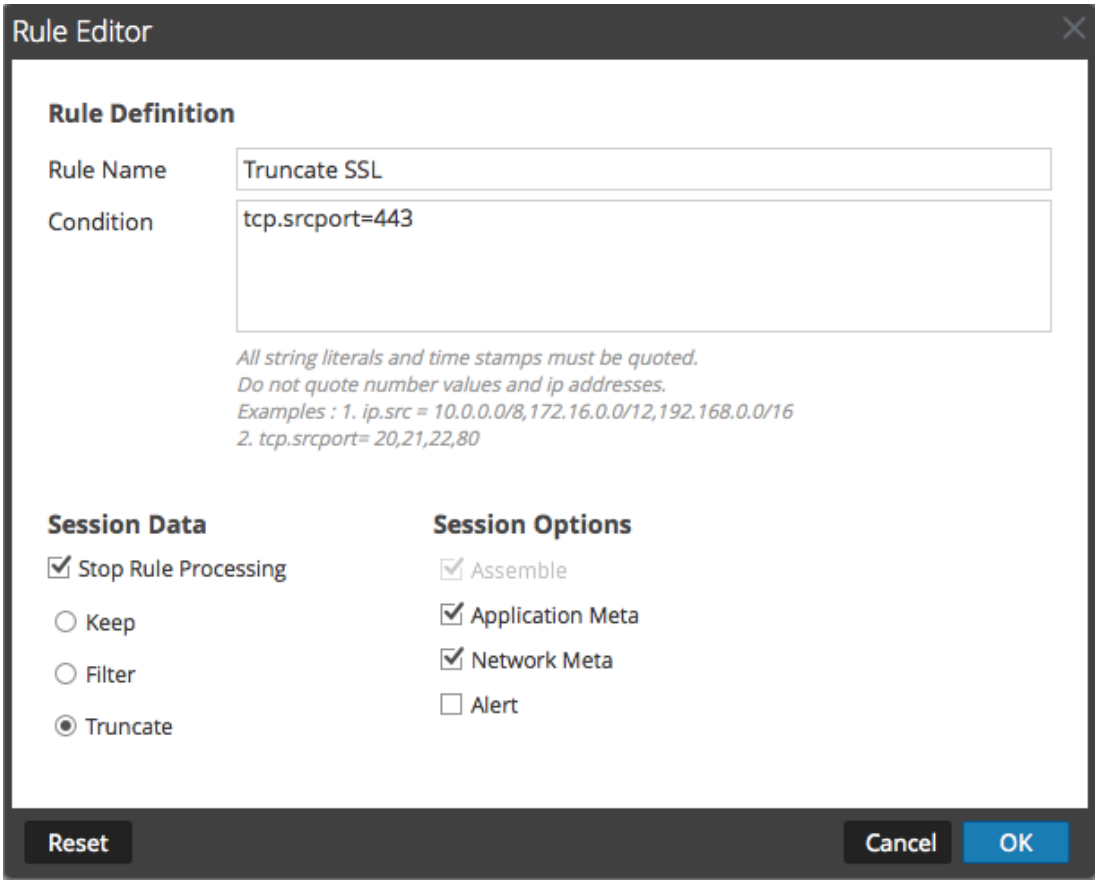
3. Sélectionnez l'onglet **Règles réseau**.
   L'onglet Règles réseau s'affiche.



Ajouter ou modifier une règle réseau

1. 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 des règles et cliquez sur .

La boîte de dialogue Éditeur de règles s'affiche.



2. 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**.
3. 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, Security Analytics affiche des erreurs et avertissements de syntaxe. Par exemple, pour tronquer tous les SSL du port source, **tcp.srcport=443**.

   Tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre ni les adresses IP entre guillemets. La section Instructions relatives aux règles et requêtes fournit des informations supplémentaires. Clés méta prises en charge dans les conditions de règles réseau décrit les clés méta dont Security Analytics prend en charge l'utilisation dans les conditions de règle réseau.
4. Si vous souhaitez mettre fin à l'évaluation de cette règle, activez la case à cocher **Arrêter le traitement des règles**.

5. 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.

6. 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.

7. 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.
8. Vérifiez que la séquence d'exécution de la règle est correcte par rapport aux autres règles de la grille. Si nécessaire, déplacez la règle.
9. Pour appliquer la règle mise à jour au Decoder, cliquez sur **Appliquer**.

   Security Analytics enregistre un snapshot des règles en cours d'application, puis applique l'ensemble mis à jour au Decoder et supprime l'indicateur En attente des règles qui étaient en attente.

Étape 5. Démarrer et arrêter la capture de données

Cette rubrique contient une procédure pour démarrer et arrêter la capture de données sur les Decoders.

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.

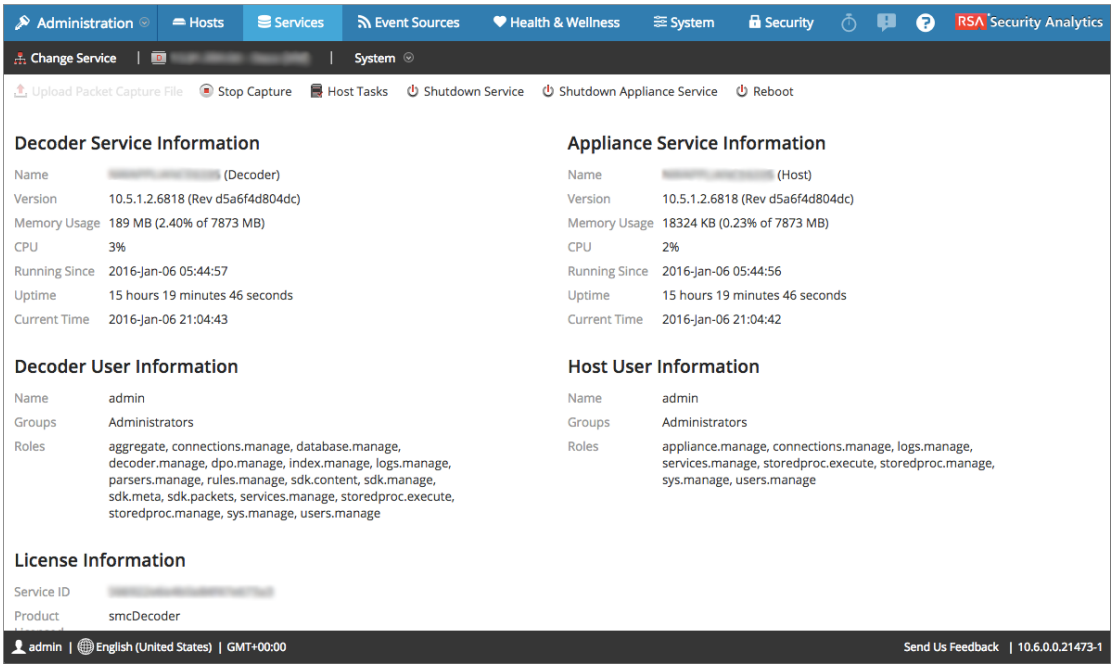
Remarque : Les paramètres de configuration de la capture dans la vue Configuration des services pour un Decoder détermine si Capture Autostart est activé, ainsi que les paramètres d'adaptateur, de cache, de base de données et de hachage.

Procédure

Pour démarrer et arrêter la capture :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > 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.



Procédures supplémentaires

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.

Cette rubrique permet de trouver des informations supplémentaires sur les Decoders et les Log Decoders dans Security Analytics.

Topics

Configurer les feeds et les parsers

Cette rubrique présente les feeds et les parsers, et propose des procédures pour travailler avec les feeds et les parsers de Decoder et Log Decoder.

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.

Procédures

Configurer les analyseurs

Security Analytics 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.

Il existe plusieurs types d'analyseurs personnalisés configurables :

- GeoIP : cet analyseur associe les adresses IP aux emplacements géographiques réels.
- Search : cet analyseur est configuré par l'utilisateur pour générer des métadonnées par analyse des mots clés prédéfinis et des expressions régulières.
- FLEXPARSE : 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.
- 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.

Sous l'onglet Parsers de la vue Configuration des services, vous pouvez afficher les parsers déployés sur un Decoder, télécharger des parsers et supprimer les parsers déployés. L'interface utilisateur comprend un indicateur si l'analyseur provient de Live, qui est installé par Security Analytics 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 Security Analytics Live.

Configurer les feeds

Security Analytics 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 Security Analytics pour obtenir des feeds de sources extérieures. La rubrique **Contenu Live dans Security Analytics** de *Gestion des services Live* fournit une présentation de l'outil de gestion de contenu Live.

L'interface utilisateur de Security Analytics vous permet de consulter la liste des feeds actuellement déployés, avec un indicateur si le feed provenant de Security Analytics Live a été installé via Security Analytics, 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.

Security Analytics 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.

Topics

- Créer et déployer un Feed personnalisé à l'aide de l'assistant
- Utiliser des parsers personnalisés

Créer et déployer un Feed personnalisé à l'aide de l'assistant

Cette rubrique fournit des instructions sur l'utilisation de l'assistant Feed personnalisé dans RSA Security Analytics, afin de renseigner rapidement les Decoders avec des feeds personnalisés.

RSA Security Analytics est doté d'un assistant Feed personnalisé pour permettre 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 Security Analytics se présentent sous la forme `<filename>.feed`. Pour créer un feed, Security Analytics a besoin d'un fichier de données de feed au format `.csv` 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 Security Analytics peut récupérer la dernière version du fichier pour chaque récurrence. Après la création d'un feed Security Analytics, vous pouvez télécharger le feed sur votre système de fichiers local, modifier les fichiers de feed, puis modifier le feed Security Analytics 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 Security Analytics 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**.

```
<?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>

<Champs>
<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 Security Analytics 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 de Security Analytics	Équivalent du fichier de définition de feed
(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 maintenant 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.

Paramètre de Security Analytics	Équivalent du fichier de définition de feed
(Onglet Options avancées) **Fichier de feed XML**	Le nom du fichier de définition de feed. Par exemple : `dynamic_dns.xml`.
(Onglet Options avancées) **Séparateur**	Caractère de séparation utilisé pour séparer les attributs dans le fichier de données du feed. Il correspond à l'attribut **`flatfeedfile 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.

Paramètre de Security Analytics	Équivalent du fichier de définition de feed
(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, ι) **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.exemple.com, elle est tronquée à exemple.com. La valeur **Faux** ne sélectionne pas de troncation, et la valeur **Vrai** sélectionne la troncation.
(onglet Définir des colonnes, ι) **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.

Paramètre de Security Analytics	Équivalent du fichier de définition de feed
(onglet Définir des colonnes, ‹) **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 **Clé de champ** dans le fichier de définition de feed. Une clé s'applique uniquement à un champ dont le type est défini sur **valeur**. Dans le fichier de définition de feed, se trouve une liste de LanguageKeys provenant de **index.xml**, ou un nom récapitulatif si le Nom de la source et le Nom de la destination sont utilisés. Par exemple, **réputation** est un nom de résumé pour **réputation.src** et **réputation.dst**. Cette valeur est référencée par l'attribut Clé de champ.

Créer un Feed personnalisé

Vous pouvez facilement 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`. 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.

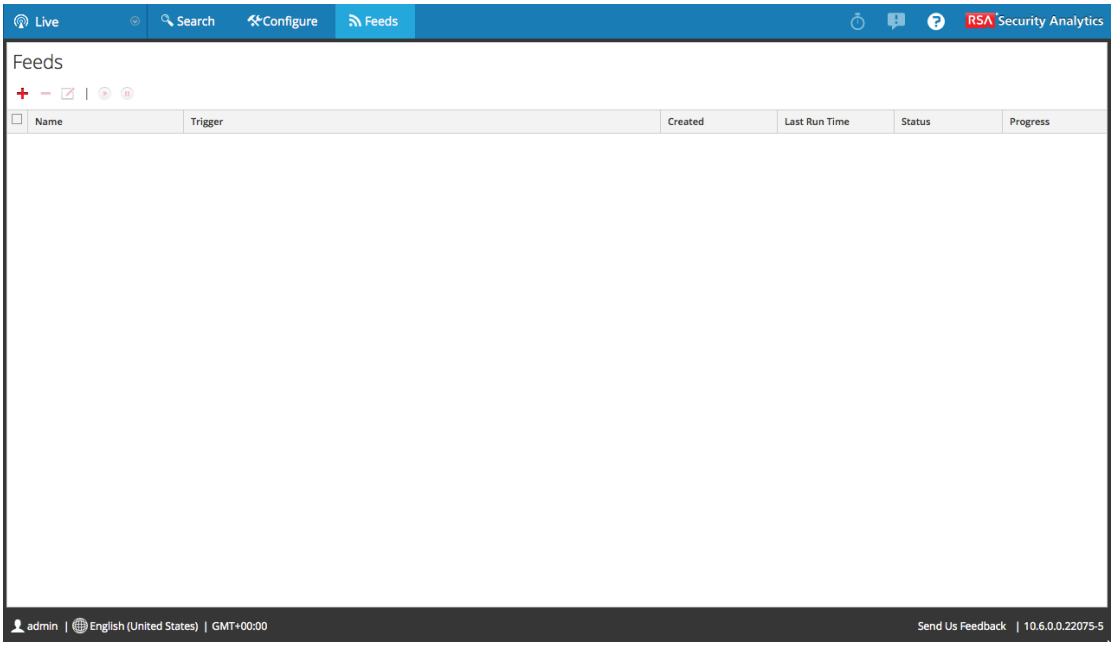
À la fin de cette procédure, vous aurez créé un feed personnalisé.

Le fichier de données de feed (`.csv`) 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 Security Analytics.

Pour créer un feed personnalisé :

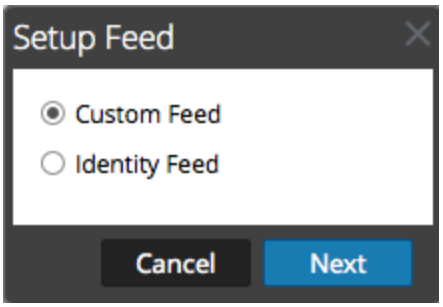
1. Dans le menu **Security Analytics**, sélectionnez **Live > Feeds**.

   La vue Feeds s'affiche.



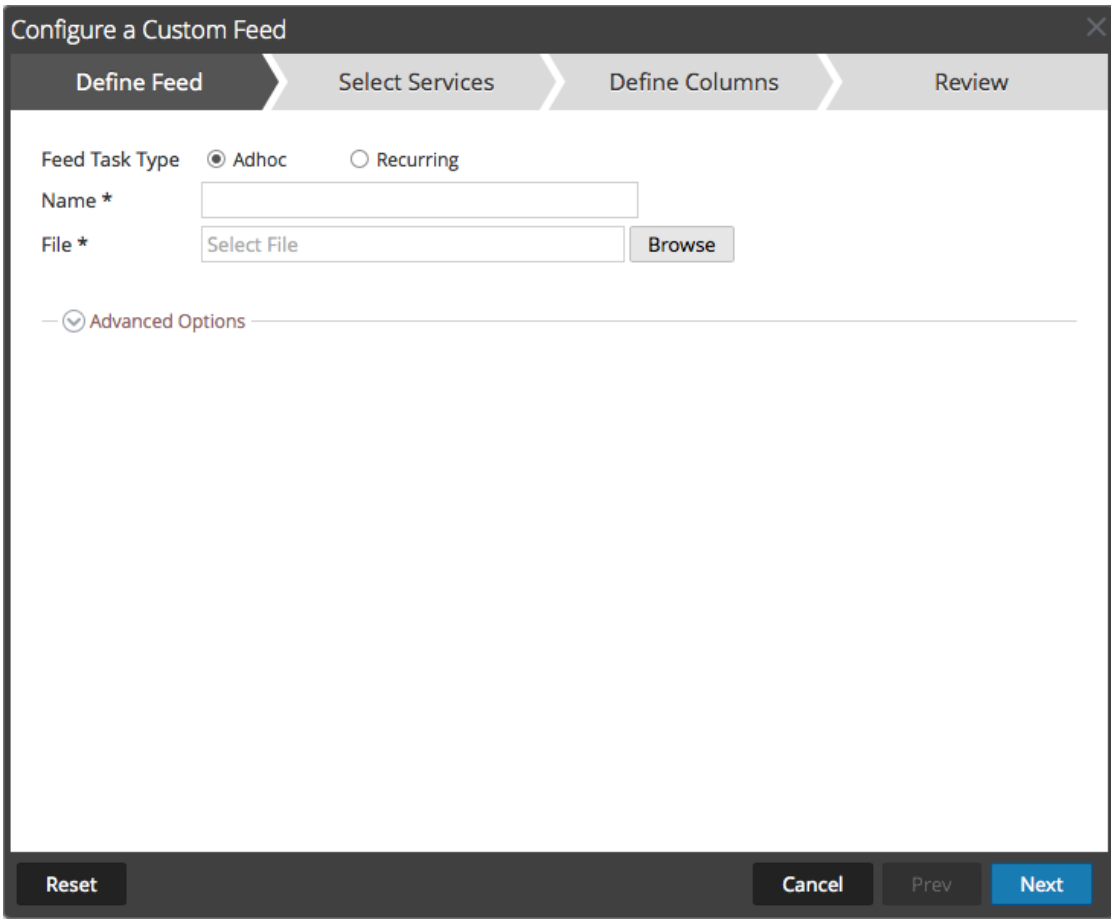
2. Dans la barre d'outils, cliquez sur  .

   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.



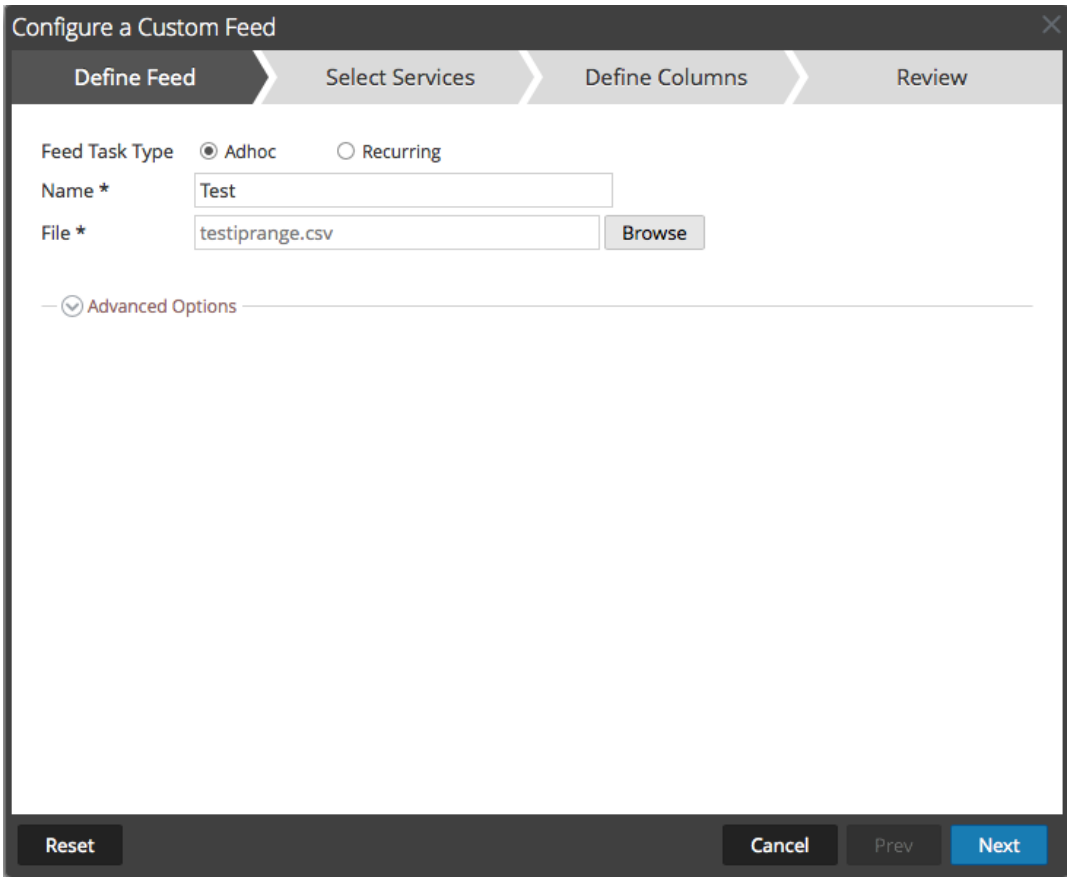
4. Pour définir une tâche de feed à la demande qui s'exécute une fois, sélectionnez **Ad hoc** dans le champ **Type de tâche par défaut** et procédez d'une des manières suivantes :

   a. (Conditionnel) Pour définir un feed basé sur un fichier de données de feed au format .csv, saisissez le **Nom** du feed, sélectionnez un **fichier** de contenu .csv dans le système de fichiers local, puis cliquez sur **Suivant**.

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

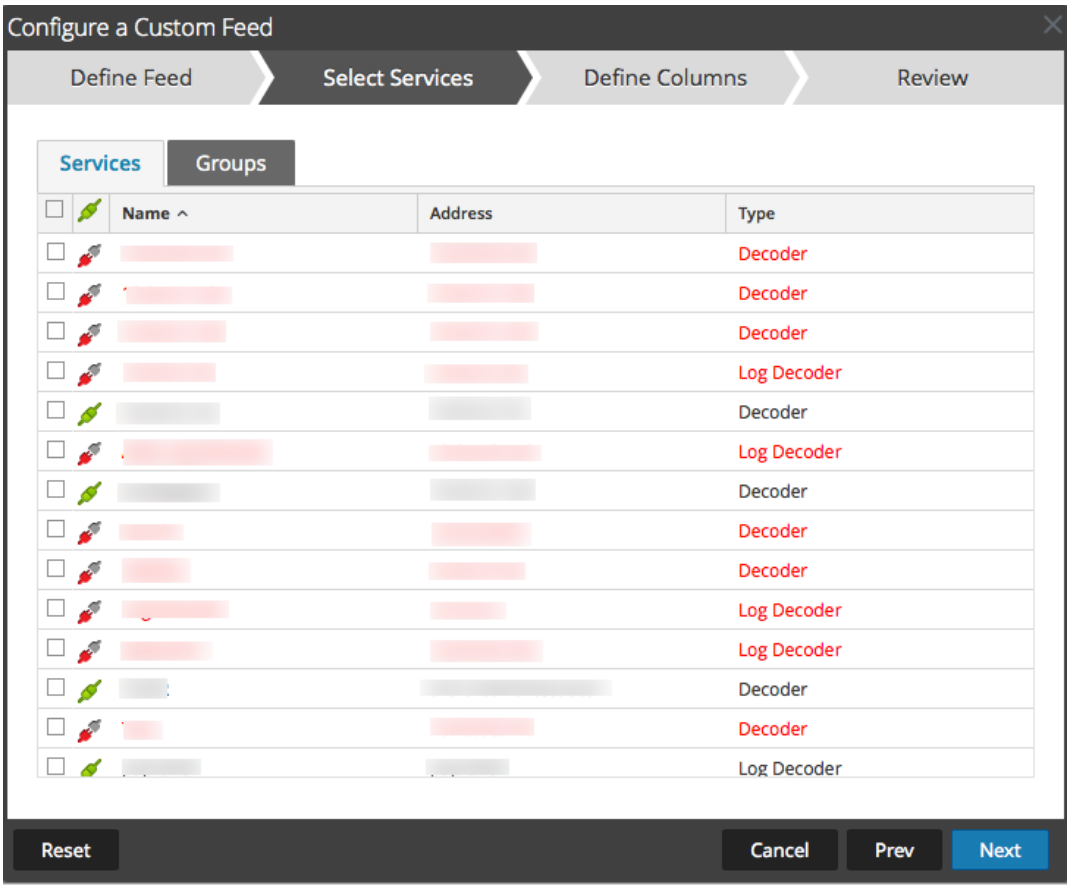
Options avancées.

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**.

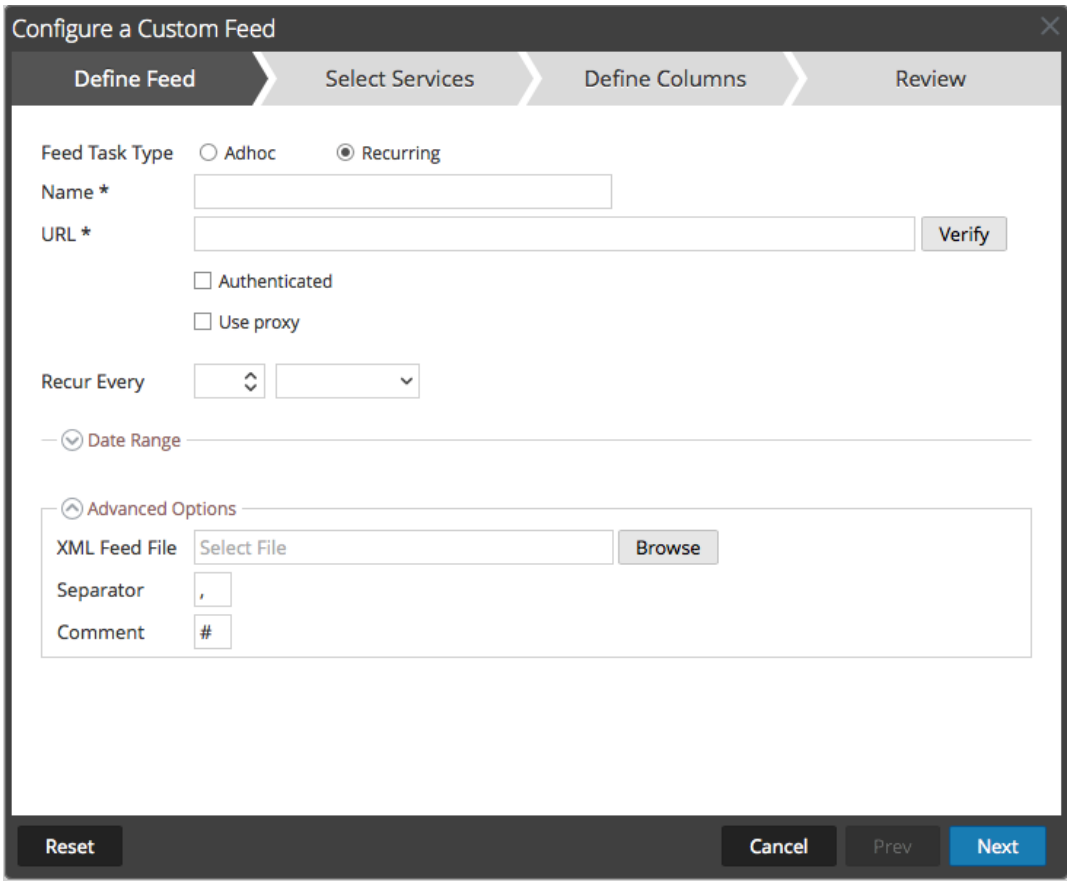
d. Le formulaire Sélectionner des services s'affiche. Voici un exemple de formulaire pour un feed basé sur un fichier de données de feed, sans fichier de définition de feed. Si vous définissez un feed basé sur un fichier de définition de feed, l'onglet Définir des colonnes n'est pas nécessaire.



5. 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'URL de l'emplacement du fichier de données feed, par exemple, `http://<hostname>/<feeddatafile>.csv` et cliquez sur **Vérifier**.

   Security Analytics vérifie l'emplacement de stockage du fichier afin que Security Analytics puisse vérifier automatiquement le dernier fichier 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**.

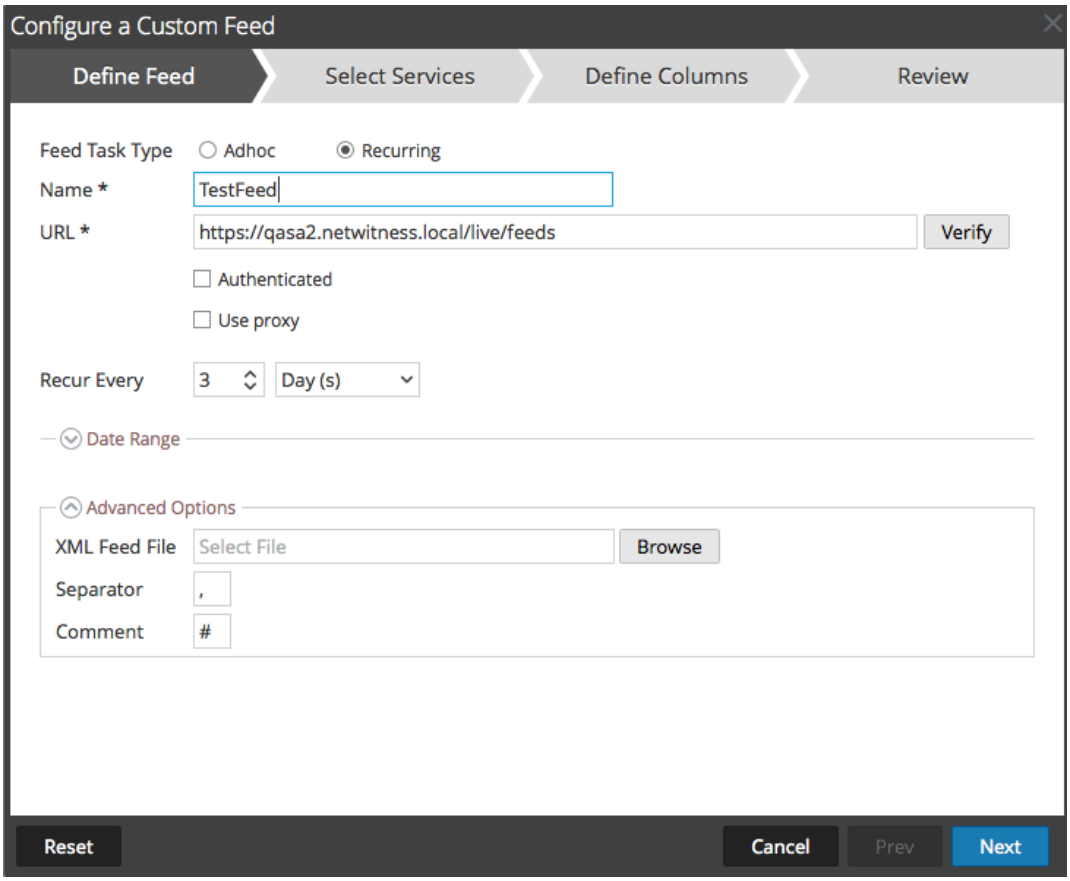
   Security Analytics fournit votre nom d'utilisateur et mot de passe pour l'authentification auprès de l'URL.

d. Si vous souhaitez que le serveur Security Analytics 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 Security Analytics** 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.

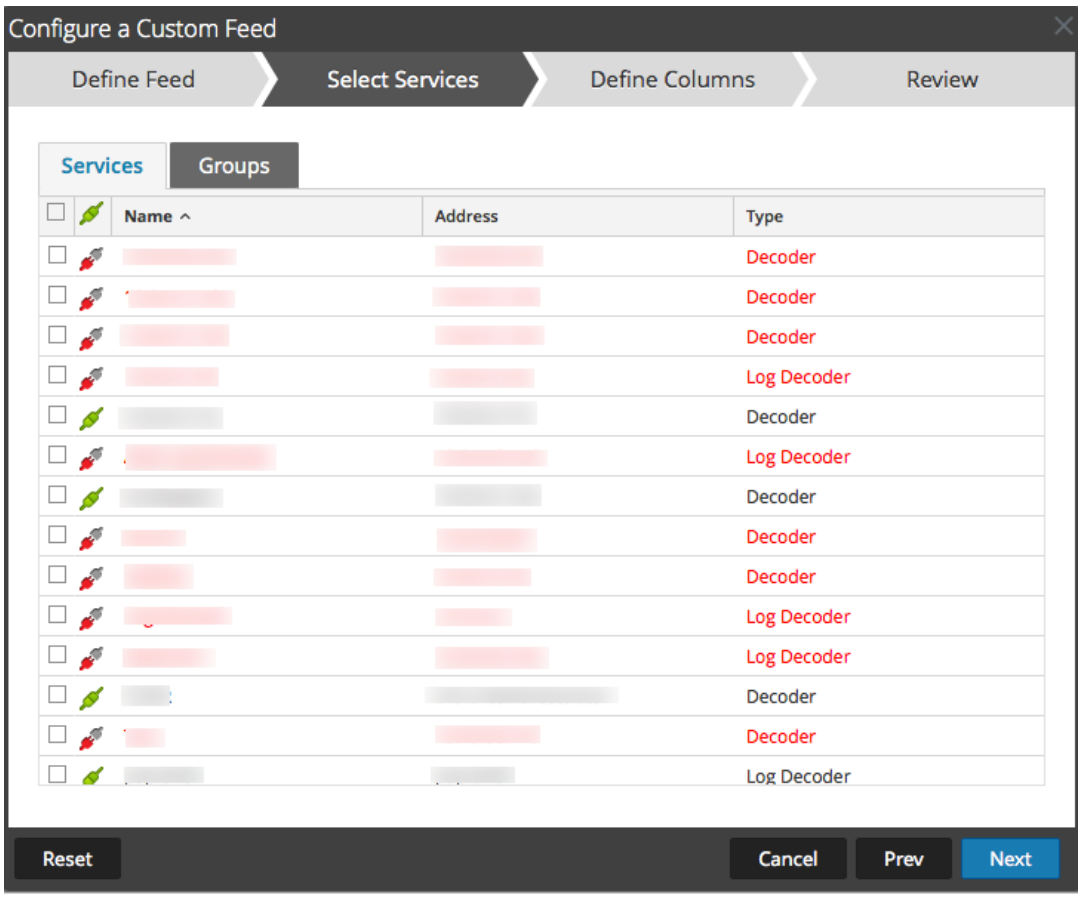


6. (Conditionnel) Si vous souhaitez définir un feed basé sur un fichier de feed XML :

- 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.



7. 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 **Next**.

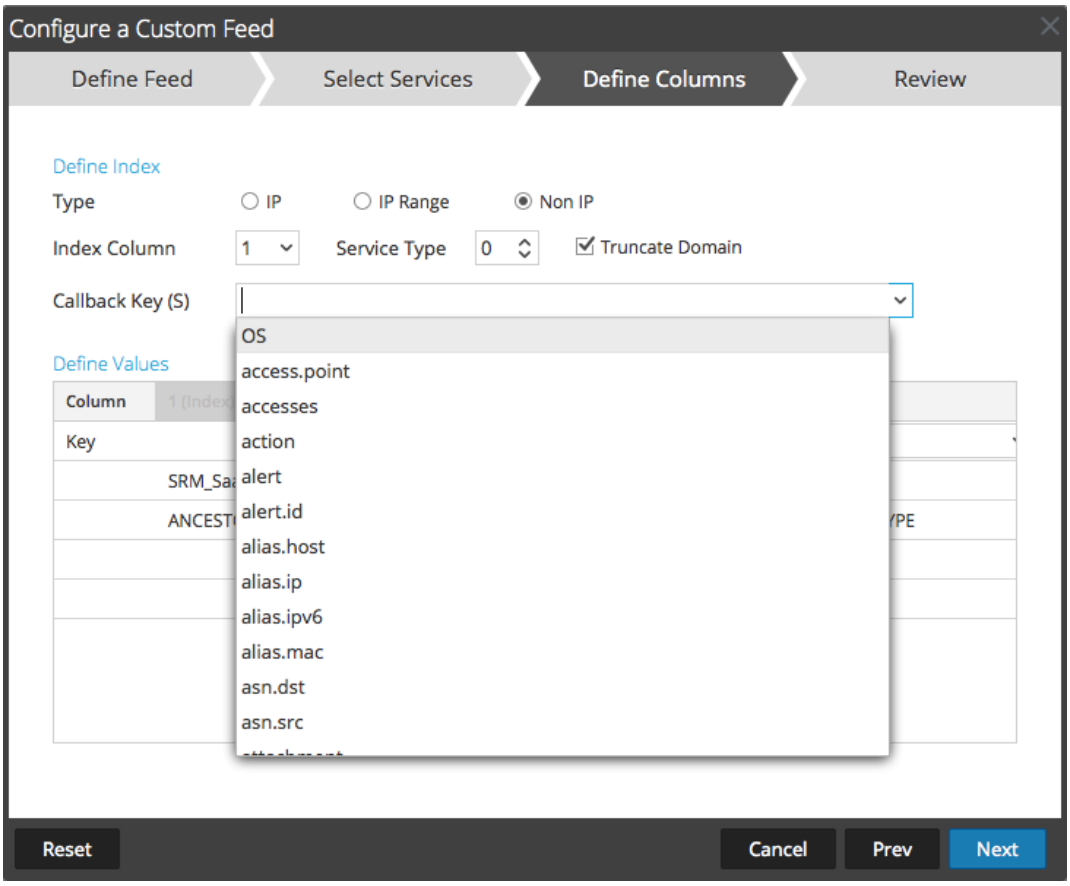
      Le formulaire Définir des colonnes s'affiche.

8. Pour mapper les colonnes dans le formulaire Définir des colonnes :

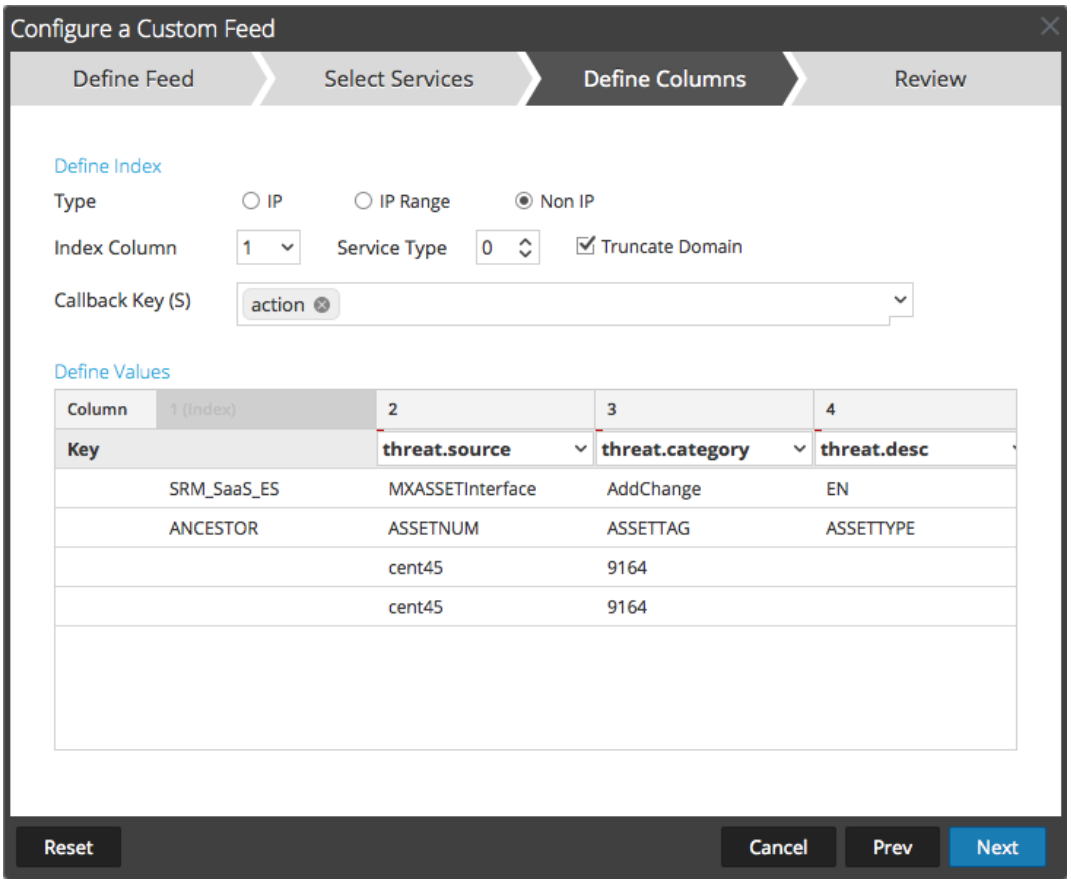
   a. Définir le type d'index : **IP**, **Plage IP** ou **Non IP**, et sélectionnez la colonne index.

   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**.

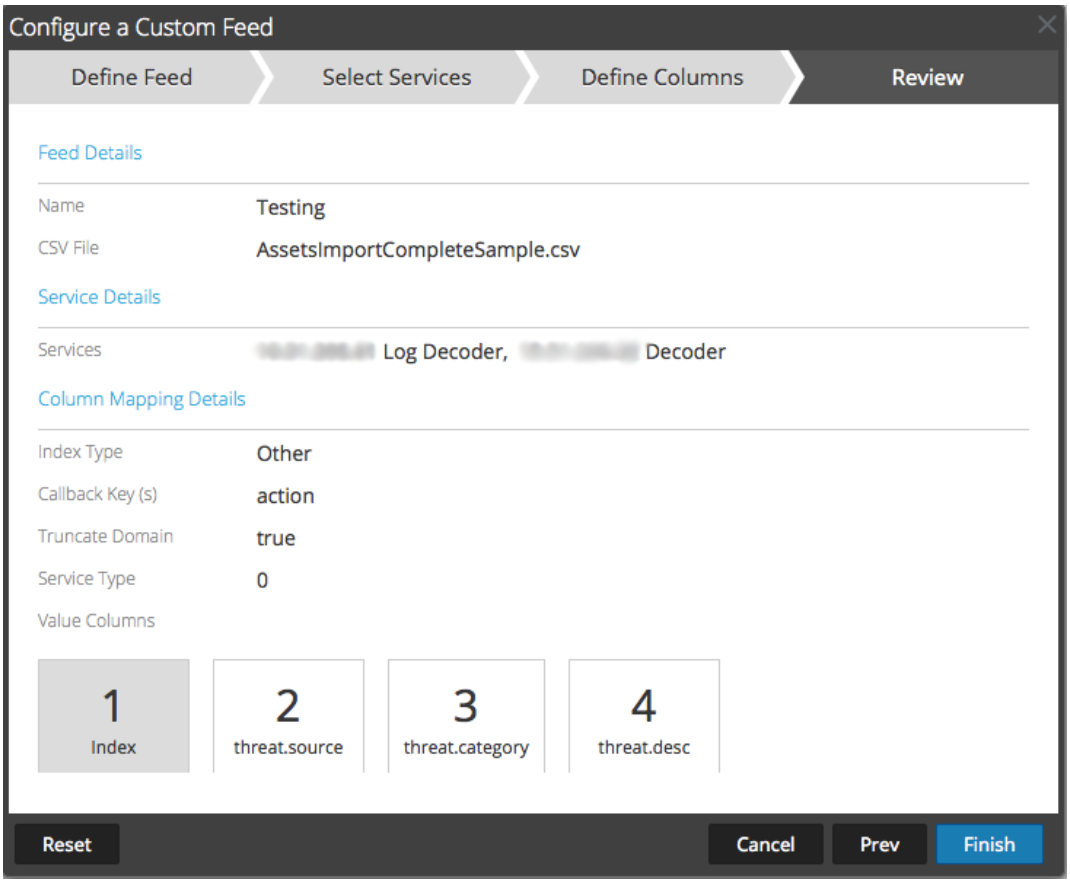


d. Sélectionnez la clé de langue à appliquer aux données de chaque colonne à partir de la liste déroulante. Le méta affiché dans la liste déroulante est basé sur les valeurs définies par le service. Si vous avez des compétences solides, vous pouvez également ajouter d'autres méta.



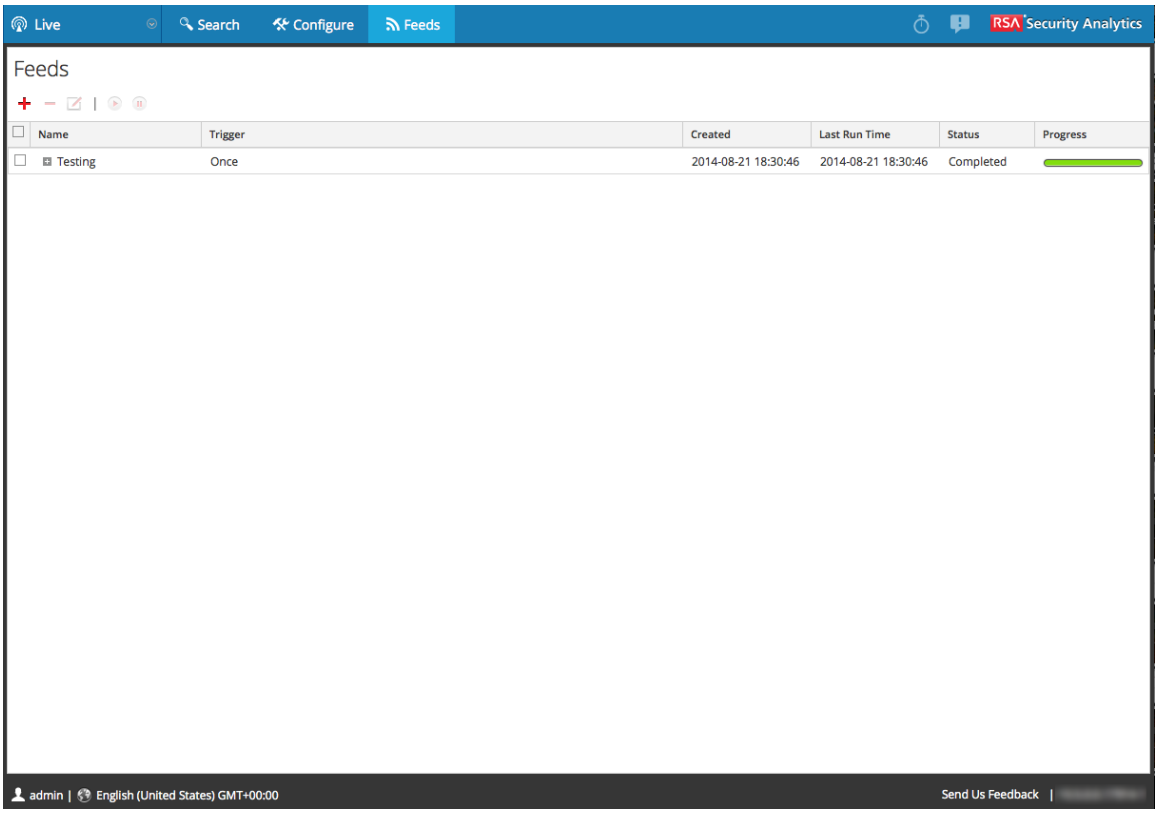
e. Cliquez sur **Suivant**.

Le formulaire Révision s'affiche.



9. 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).

10. Passez en revue les informations du feed et, si elles sont correctes, cliquez sur **Terminer**.
11. 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.


Live
Search
Configure
Feeds
RSA Security Analytics
Feeds
Name
Trigger
Created
Last Run Time
Status
Progress
Testing
Once
2014-08-21 18:30:46
2014-08-21 18:30:46
Completed
admin | English (United States) GMT+00:00
Send Us Feedback |

Créer un feed d'identité

Vous pouvez facilement créer un feed d'identité et le renseigner dans les Decoders et Log Decoders. À la fin de cette procédure, vous aurez créé un feed d'identité.

Conditions préalables

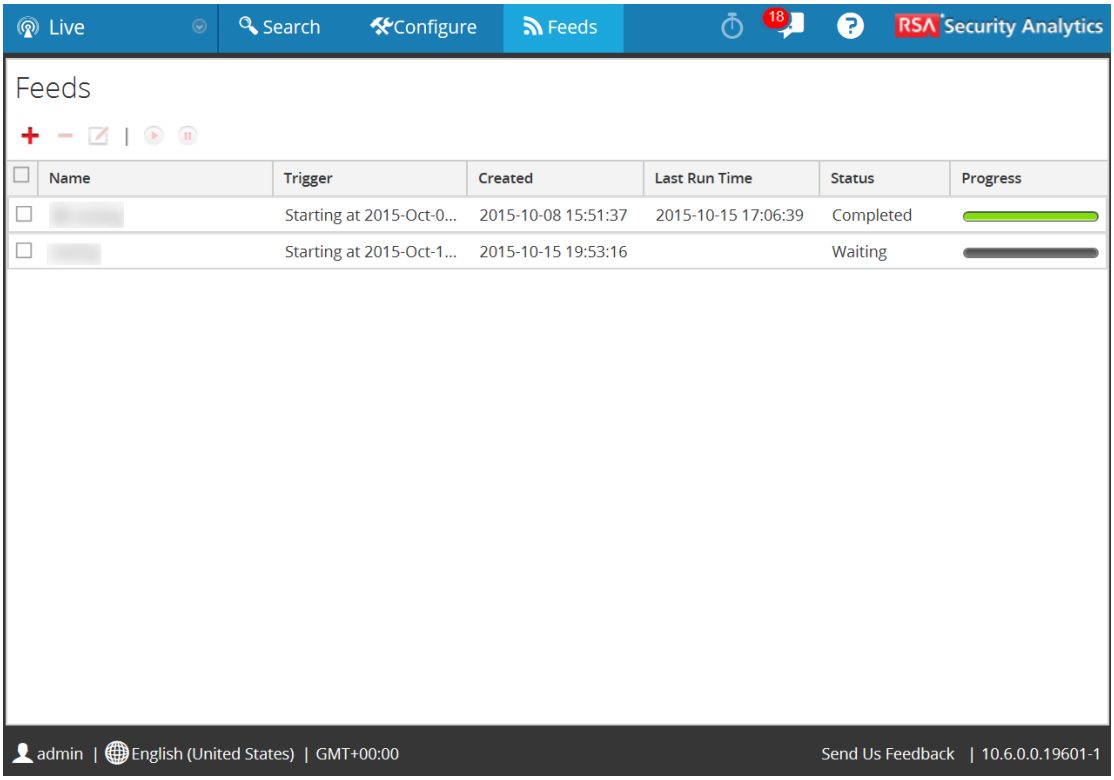
Dans le but de créer un feed d'identité, il vous faut :

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

Créer un feed d'identité

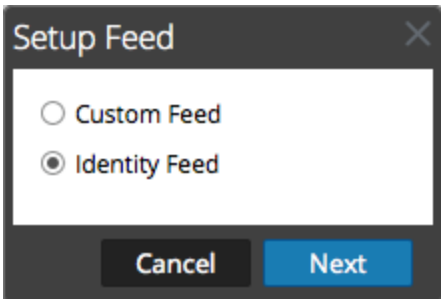
1. Dans le menu **Security Analytics**, sélectionnez **Live > Feeds**.

   La grille Feeds s'affiche.



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

   La boîte de dialogue Configurer le feed s'affiche, avec Identity Feed sélectionné par défaut.



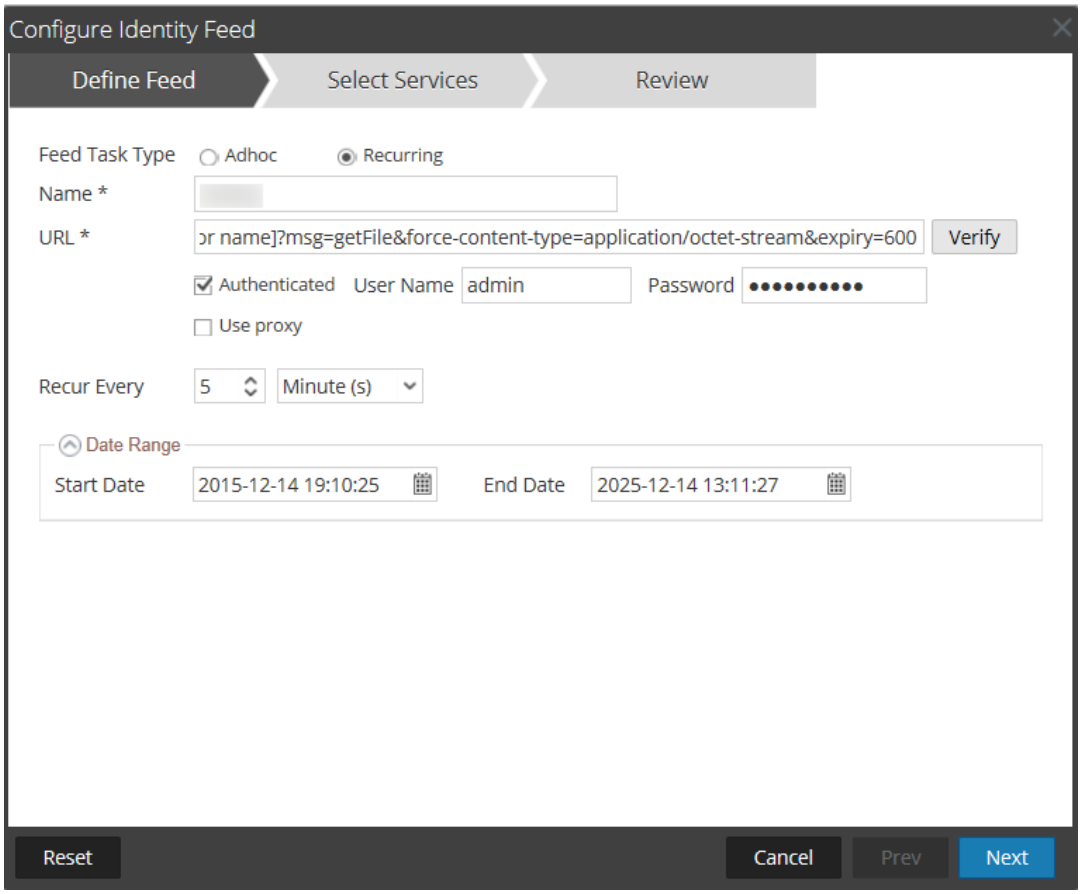
3. Sélectionnez **Feed d'identité**, puis cliquez sur **Suivant**.

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

4. (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**.

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



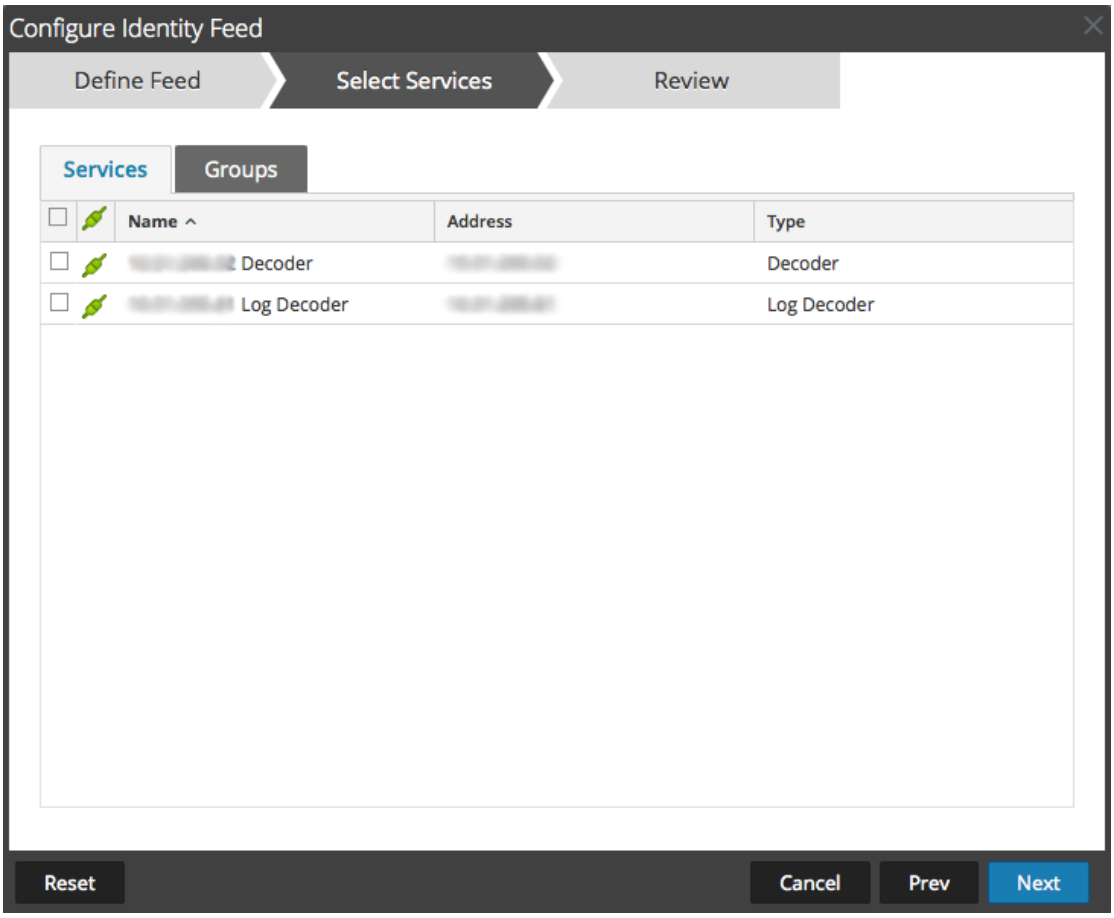
Remarque : Security Analytics vérifie l'emplacement de stockage du fichier pour pouvoir rechercher automatiquement le dernier fichier avant chaque récurrence.

Dans le champ **URL**, saisissez l'URL de l'emplacement du fichier de données de feed. Par exemple :

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

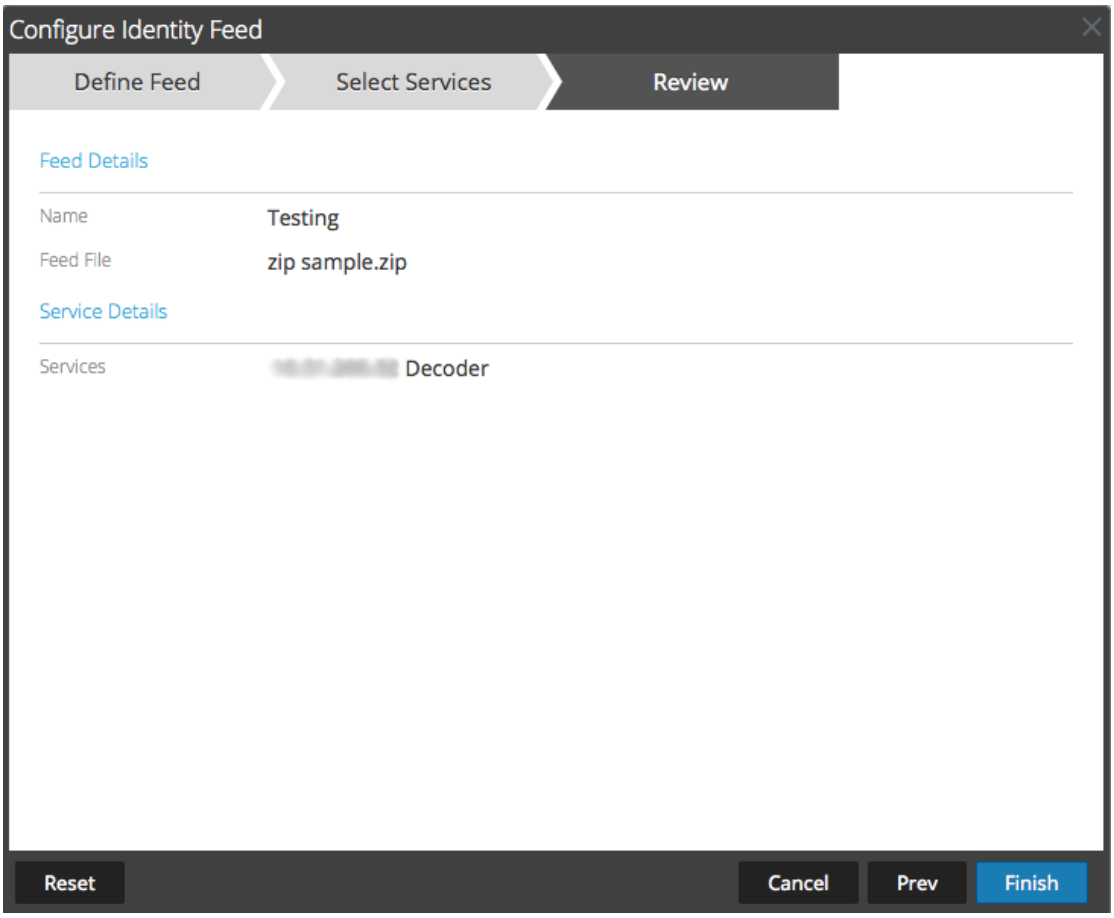
5. (Facultatif) Si l'URL présente un accès restreint et requiert une authentification à l'aide de votre nom d'utilisateur et mot de passe, sélectionnez **Authentifié**. Security Analytics fournit votre nom d'utilisateur et mot de passe pour l'authentification auprès de l'URL.
6. Pour définir l'intervalle 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.
7. Cliquez sur **Vérifier** pour vérifier votre configuration du feed identité avant de procéder au formulaire Sélectionner des services.
8. Cliquez sur **Suivant**.

   Le formulaire Sélectionner des services s'affiche.



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

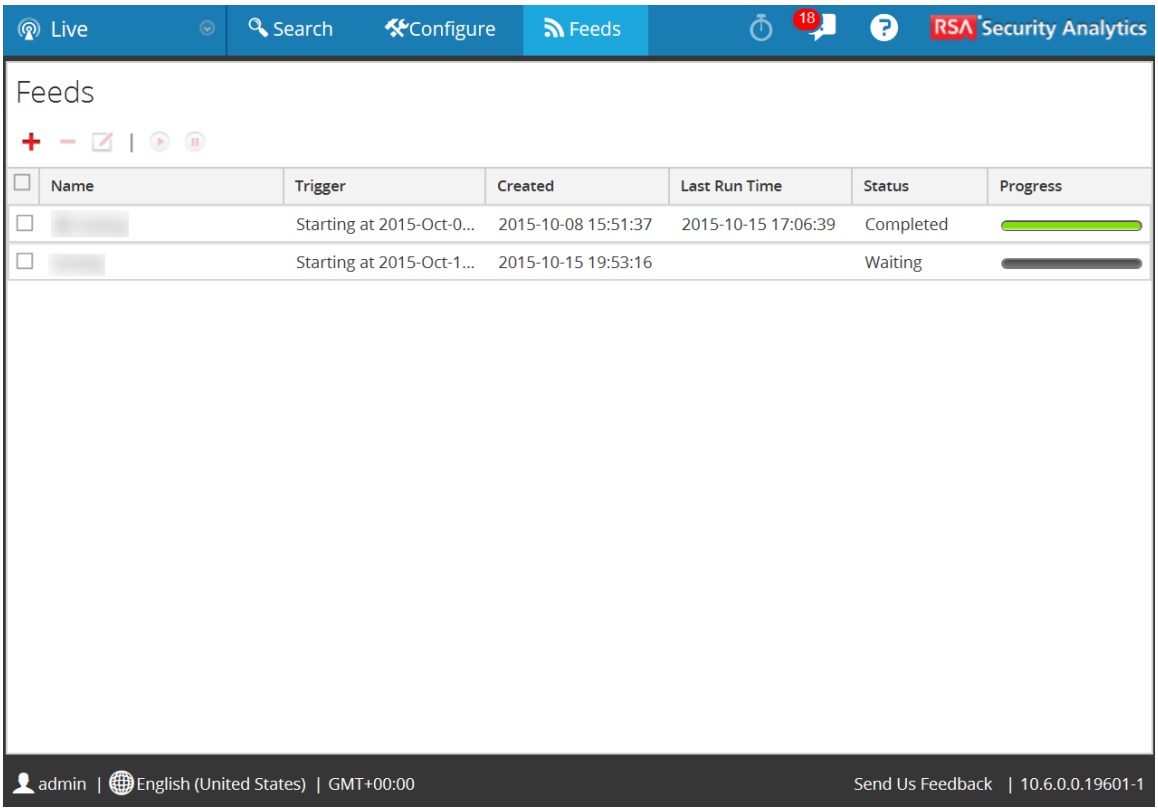
    Le formulaire Révision s'affiche.



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.

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).
12. 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.


Live
Search
Configure
Feeds
18
RSA Security Analytics
Feeds
Name
Trigger
Created
Last Run Time
Status
Progress
Starting at 2015-Oct-0...
2015-10-08 15:51:37
2015-10-15 17:06:39
Completed
Starting at 2015-Oct-1...
2015-10-15 19:53:16
Waiting
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.19601-1

Modifier un Feed personnalisé

Cette rubrique fournit les instructions permettant de modifier un feed personnalisé à l'aide de l'assistant Feed personnalisé.

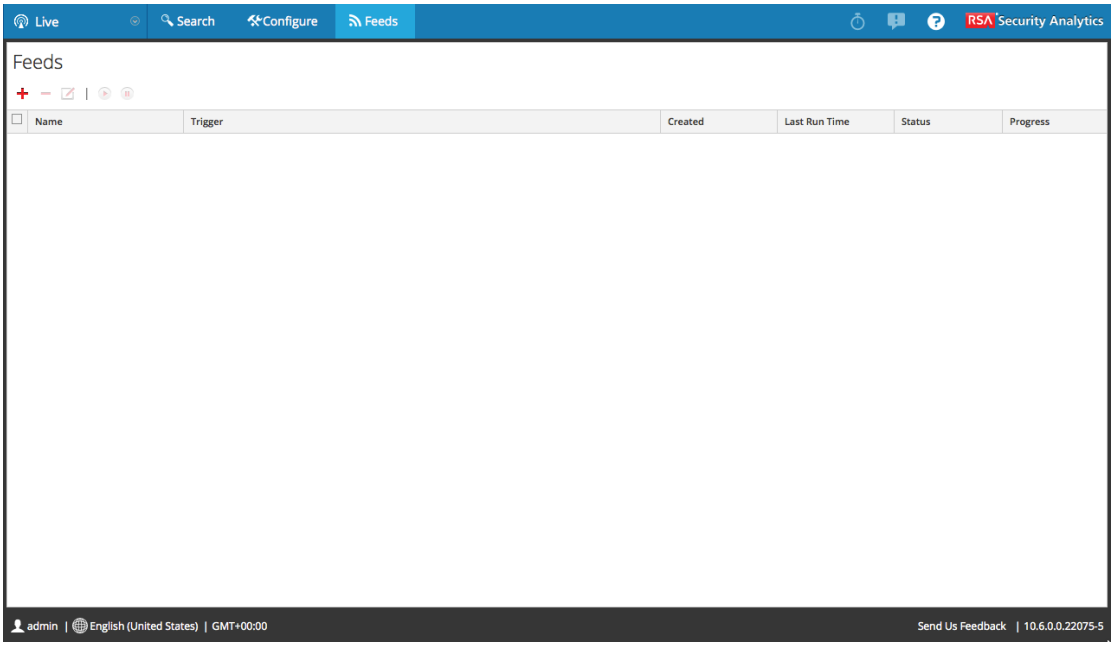
L'exécution de cette procédure aura pour résultat :

- Ouverture d'un feed personnalisé existant.
- Téléchargement et modification du feed (format **.zip**) ou du fichier utilisé pour créer le feed (**.csv** ou **.xml**).
- Recréation du feed avec le fichier mis à jour et les nouvelles spécifications du feed.

Pour modifier un feed existant :

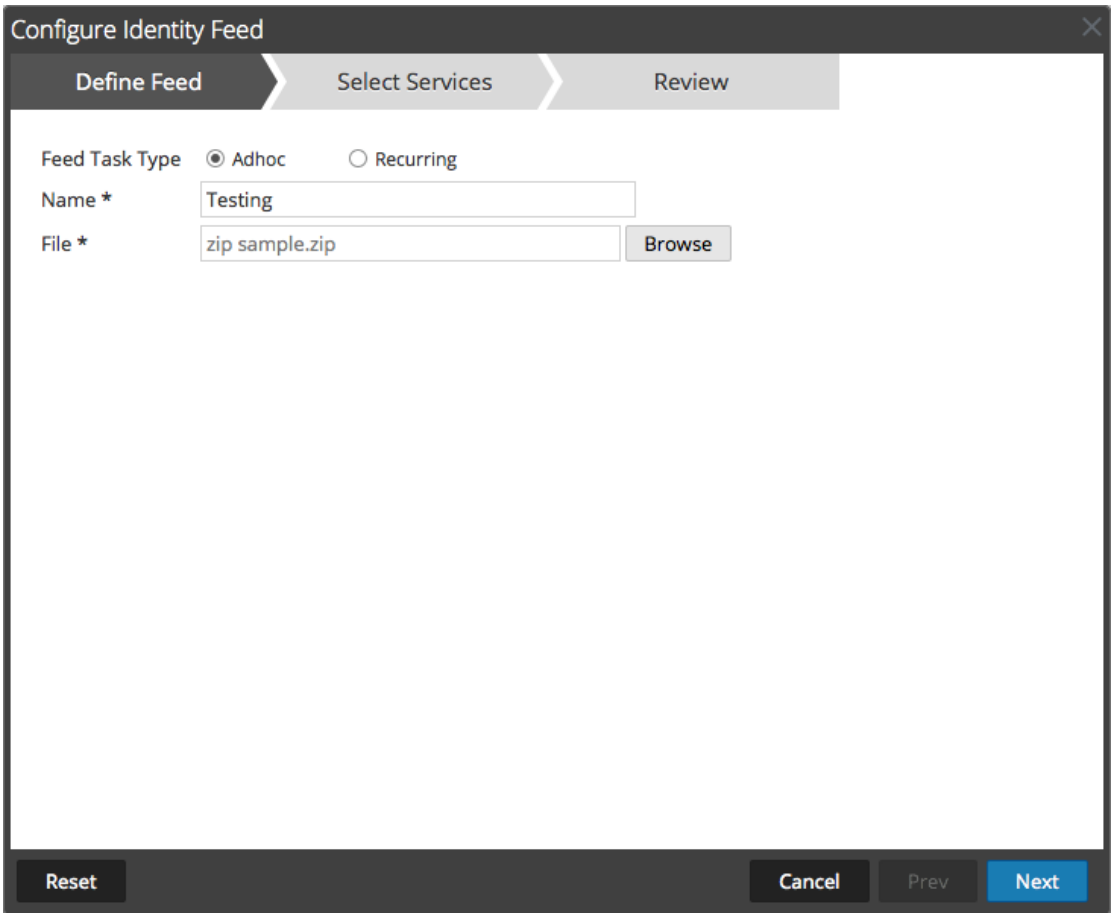
1. Dans le menu **Security Analytics**, sélectionnez **Live > Feeds**.

   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.

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

Utiliser des parsers personnalisés

Cette rubrique fournit des instructions sur l'utilisation d'analyseurs personnalisés dans RSA Security Analytics.

RSA Security Analytics peut télécharger des analyseurs à partir de votre système local et les supprimer.

Procédures

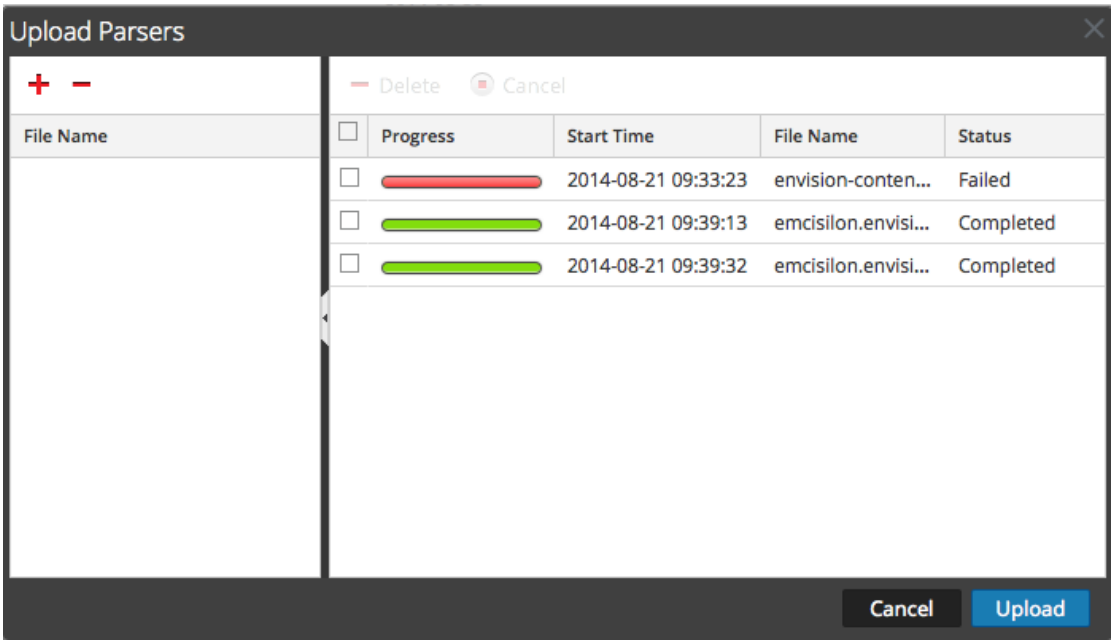
Télécharger des parsers vers un Decoder ou Log Decoder

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 grille Fichier, vous préparez une liste des analyseurs pour téléchargement. 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.

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service et  **> Vue > Configuration.**
   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Parsers**.

4. Cliquez sur Upload.

   La boîte de dialogue Télécharger les analyseurs s'affiche.

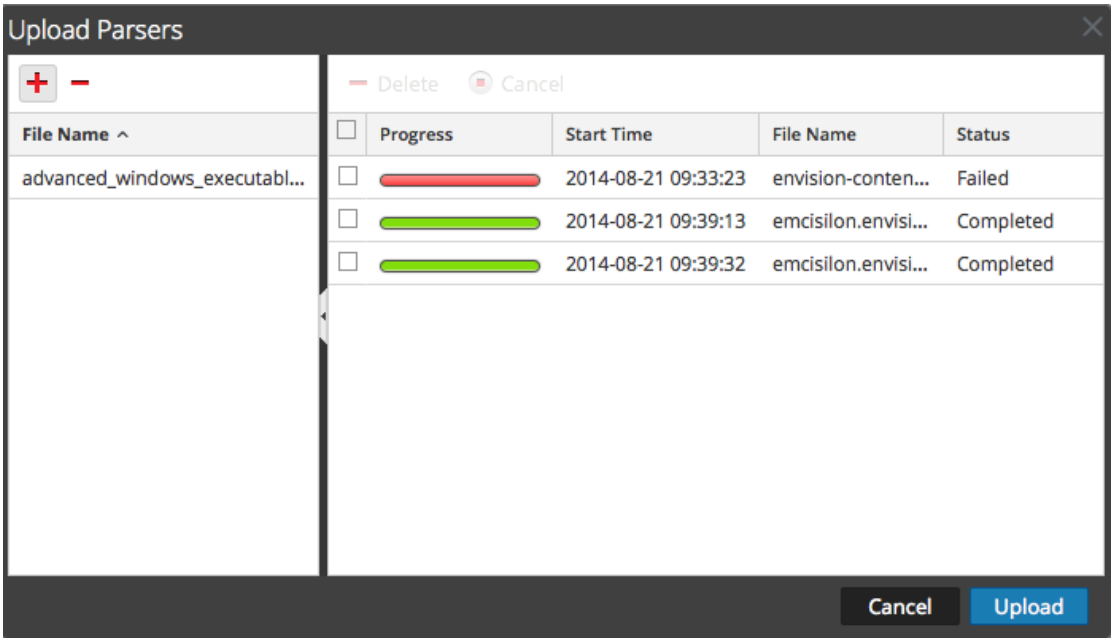


5. Cliquez sur +.

   Une boîte de dialogue de sélection de fichier s'affiche.

6. Sélectionnez les fichiers **.flex**, **.parser** et **.lua** à mettre à jour et cliquez sur **Ouvrir**.

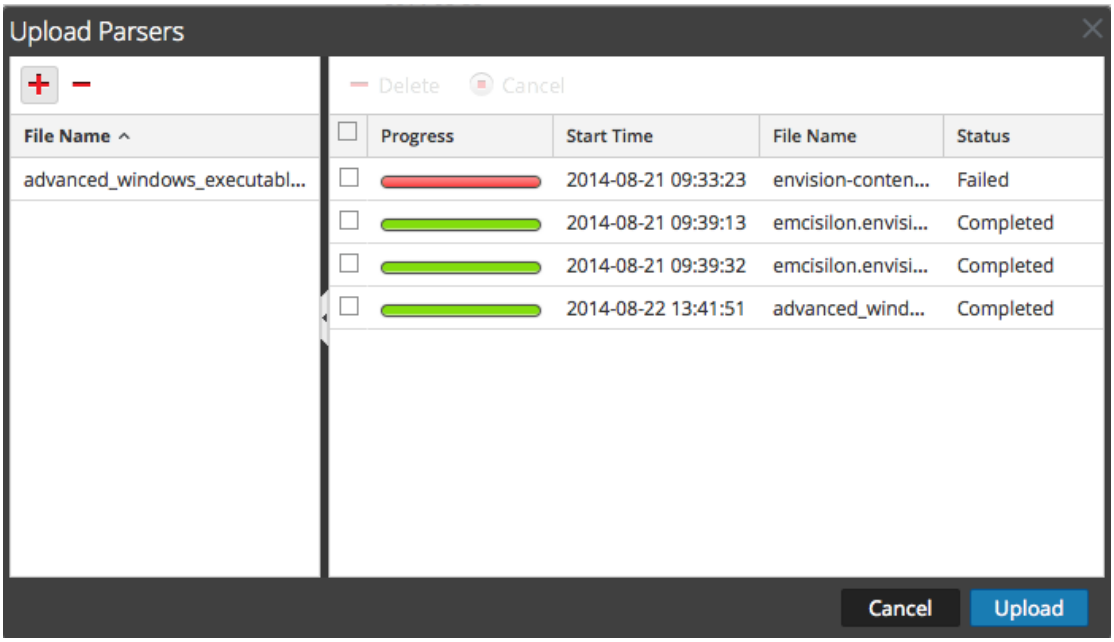
   La boîte de dialogue se ferme et les fichiers sélectionnés s'affichent dans la grille Fichier.



7. Cliquez sur **Télécharger**.

   La grille Télécharger une tâche affiche la progression des tâches de téléchargement, chaque

tâche représentant un fichier à télécharger.



8. 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 Delete.

Supprimer les analyseurs déployés

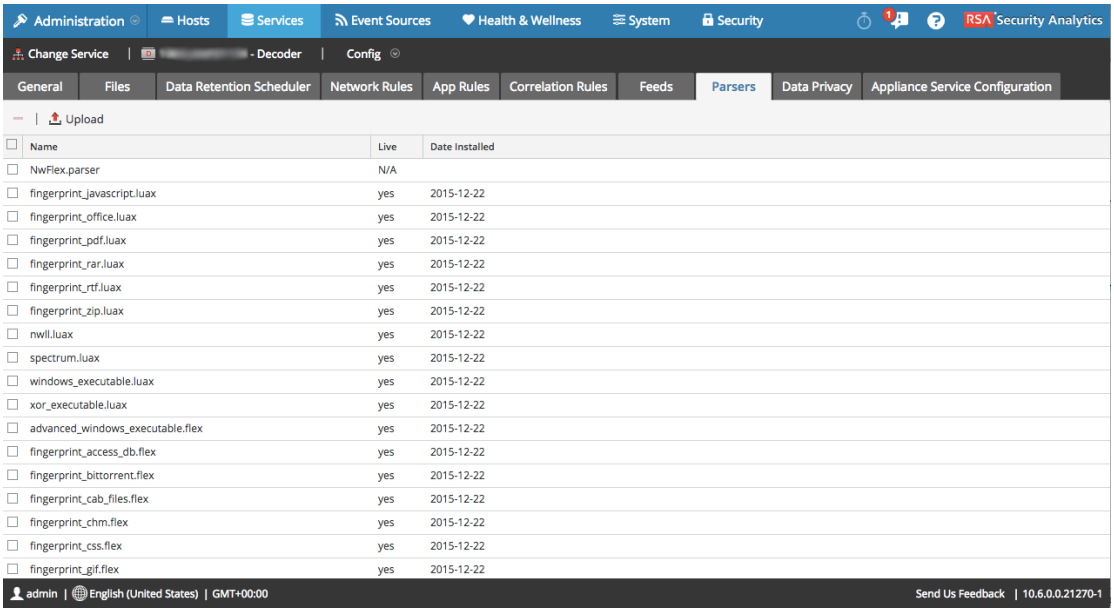
L'option **Supprimer** de la vue Configuration des services > onglet Analyseurs permet de supprimer des analyseurs déployés à partir d'un Decoder ou Log Decoder. Les parsers peuvent être ajoutés et supprimés alors qu'un Decoder est en cours d'exécution sans que cela ait d'impact sur la capture.

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. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service et  **> Vue > Configuration.**

   La vue Configuration des services pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Parsers**.



4. Sous l'onglet **Analyseurs**, sélectionnez un ou plusieurs analyseurs à supprimer.
5. Cliquez sur  .

   Une boîte de dialogue demande une confirmation du fait que vous souhaitez supprimer les analyseurs.
6. Si vous voulez supprimer les analyseurs, cliquez sur **Oui**.

   Les analyseurs sont immédiatement supprimés du Decoder.

Configurer la fonction 10G

Destinée aux administrateurs, cette rubrique explique comment configurer un Packet Decoder spécifiquement pour capturer des paquets à vitesse élevée.

Ce guide s'applique à la capture 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 Security Analytics Version 10.6 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 décodeur de paquets 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 analyseurs et des flux que vous avez activés.

RSA Security a validé le contenu spécifique à analyser à vitesse élevée. Pour plus d'informations Analyse à vitesses élevées pour plus d'informations.

Pour plus d'informations sur la personnalisation des analyseurs avec votre propre contenu, reportez-vous à la section Bonnes pratiques du service 10G ».

Remarque : vous pouvez ignorer l'étape Configuration du service 10G Decoder si vous démarrez avec le nouveau matériel de la gamme 5.

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

• Utilisation de la fonctionnalité du pilote **pf_ring capture** afin d'exploiter les atouts de la carte réseau 10G Intel et d'obtenir des captures à grande vitesse.

• Présentation de la configuration **assembler.parse.valve**. La configuration désactive automatiquement les analyseurs d'application lorsque certains seuils sont dépassés pour limiter les risques de perte de paquets. Une fois désactivés, les analyseurs de la couche réseau restent toujours actifs. Une fois que les statistiques chutent sous les seuils dépassés, les analyseurs d'application sont automatiquement réactivés.

• Présentation de la configuration **parallel.values** sur le service Concentrator pour l'optimisation d'une requête.

Matériel requis

- Decoder série 4S
- Carte Ethernet fibre Intel 82599, comme Intel x520. Toutes les cartes RSA 10G fournies répondent à ces exigences. Plusieurs ports peuvent être utilisés sur une seule carte 10G, mais l'association de 10G avec une carte 1G n'est pas prise en charge.

- 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 la 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.

Logiciels requis

- Module de noyau Linux fourni par RSA. Seuls les modules de noyau Linux fournis par RSA sont pris en charge.
- Package pfring correspondant au noyau installé. La version du noyau doit correspondre exactement à la version du package pfring.

Installation du service Decoder 10G

Procédez comme suit pour installer Security Analytics 10.6 10G Decoder :

Conditions préalables

• Plate-forme SA-S4H-P-DEC ou SMC-S4H-P-DEC intégrée à la plate-forme Dell R620

• Carte réseau fibre SMC-10GE-* 10G Intel 520 (disponible auprès de RSA)

• Décodeurs de paquets avec la mise à jour 10.6

• Chaque décodeur de paquets doit être configuré avec un minimum de 2 DAC ou une connectivité SAN.

Remarque : Reportez-vous aux sections suivantes Considérations relatives au stockage dans ce document avant d'effectuer la mise à jour, car un recâblage physique peut être nécessaire.

• BIOS Dell R620 v1.2.6 ou version ultérieure. 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 supérieure.

Remarque : les révisions du BIOS antérieures à la version 1.2.6 ont du mal à identifier correctement l'emplacement de la carte de capture 10G au sein du système. Il est important de mettre à jour le BIOS avant d'installer des packages, étant donné que les packages utilisent les informations fournies par le BIOS pour initialiser le système.

Éléments à prendre en compte pour l'analyse et le contenu dans le cadre de la capture de paquets

La capture et l'exécution d'un enrichissement sur les paquets bruts peuvent représenter des défis spécifiques à n'importe quel taux de capture. Avec des taux de paquets et de sessions supérieurs en mode 10G, l'efficacité de l'analyse est primordiale. Un seul analyseur peut avoir un effet préjudiciable sur le système, ce qui, au final, entraîne des pertes de paquets. Les tests effectués pour la capture 10G comprenaient des analyseurs de base, ainsi que des combinaisons de flux, des règles et d'autres contenus accessibles via RSA Live. Si un client met à jour un système actuellement déployé ou déploie un nouveau système, il est recommandé qu'il utilise les bonnes pratiques suivantes afin de minimiser les risques de perte de paquets. Il y a cependant une réserve 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 2G ne doit voir aucune différence de performances, sauf si la procédure de mise à jour ajoute un trafic supplémentaire pour la capture.

Bonnes pratiques du service 10G

1. Intégrer les analyseurs de base (sauf SMB/Webmail, qui ont généralement une utilisation CPU élevée) et surveiller les pertes de paquets potentielles.

2. Si vous ajoutez d'autres analyseurs, ajoutez un seul ou de deux analyseurs à la fois.

3. 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 n'activez qu'un seul analyseur à la fois pour mesurer son impact. Cela permet de repérer 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 soit minime, les flux doivent également être réexaminés et ajoutés à une approche progressive afin de mesurer l'impact des performances.

• Généralement, les règles d'application impactent également les performances, donc une fois encore, il est 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

Instructions d’installation du BIOS

1. Téléchargez le BIOS v2.2.3 depuis l’emplacement suivant :

http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04

2. Téléchargez le fichier Update Package for Red Hat Linux.

3. Copiez le fichier sur le serveur Security Analytics.

4. Connectez-vous en tant qu'utilisateur **racine**.

5. Modifiez les autorisations dans le fichier à Exécuter.

6. Supprimez le fichier suivant :

./BIOS_V7P04_LN_2.2.3.BIN

7. Une fois terminé, le système devra être redémarré.

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

Mise à jour 10G Decoder

1. Effectuez une mise à jour de l'appliance Decoder vers la version 10.6, y compris de tous les correctifs du système d'exploitation. La version minimale du correctif de sécurité appliqué est RSA Security Analytics Version 10.6. Cette version nécessite un module de noyau Linux :

`kernel- 2.6.32-573.12.1.el6.x86_64`, qui est la version du noyau de RSA Security Analytics Version 10.6.

2. Vérifiez que les versions kernel, pfring et numactl se présentent comme suit :

- `kernel- 2.6.32-573.12.1.el6.x86_64`
- `pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`
- `numactl-2.0.9-2.el6 .x86_64.rpm`

Installer 10G Decoder

Télécharger la dernière version du module pfring rpm à partir de smcupdate

`pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`

Pour plus d'informations, reportez-vous à la section RSA SecurCare : https://knowledge.rsasecurity.com.

2. Via ssh, installez les packages à l'aide de la commande suivante une fois les fichiers traités par scp dans le Decoder :

rpm -ivh pfring*

Remarque : REMARQUE : effectuez les vérifications suivantes :

a. Recherchez **el6 rpm** à l'aide de la commande suivante :

```
rpm -qa |grep numactl*
```

b. Vérifiez que la version correspond à `numactl-2.0.9-2.el6. x86_64.rpm`

Remarque : si l'étape de mise à jour ci-dessus est exécutée avant la mise à niveau du BIOS, les étapes suivantes devront être effectuées :

• Désinstaller les modules via la commande **rpm –e**.

• Mettre à jour le BIOS vers la version 2.2.3

• Exécuter les commandes rpm pour installer à nouveau les packages requis.

3. Vérifiez que les versions **kernel**, **pfring** et **numactl** se présentent comme suit :

• `kernel- 2.6.32-573.12.1.el6.x86_64`

• `pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`

• `numactl-2.0.9-2.el6 .x86_64.rpm`

4. Redémarrez l'appliance Decoder (le redémarrage du système complet est nécessaire pour s'assurer que les pilotes pf_ring sont chargés correctement).

5. Au redémarrage du Decoder, vous pouvez vérifier que l'installation est réussie si vous voyez d'autres interfaces **PFRINGZC** disponibles sous les options de l'Interface de capture sélectionnée (voir ci-dessous).

Configurer 10G Decoder

Une fois la mise à jour effectuée, procédez comme suit pour configurer 10G Decoder :

1. Dans la vue Explorateur de Decoder, cliquez avec le bouton droit sur **Decoder** et sélectionnez **Propriétés**.

2. Dans le menu déroulant des propriétés, sélectionnez **reconfig** et saisissez les paramètres suivants :

update=1 op=10g

3. Dans la vue Explorateur de Decoder, cliquez avec le bouton droit sur **database** et sélectionnez **Propriétés**.

4. Dans le menu déroulant des propriétés, sélectionnez **reconfig** et saisissez les paramètres illustrés dans la capture d'écran suivante :

`update=1 op=10g`

5. Sélectionnez l'adaptateur de port de capture. Les options disponibles sont :

a. Capture de port unique : **PFRINGZC,p1p1 ou PFRINGZC,p1p2**

b. Capture désactivée sur les deux ports :

i. **Sélectionnez PFRINGZC,P1P1**

ii. Dans la vue Explorateur, définissez **capture.device.params = device=zc:p1p2,zc:p1p1**

c. Assurez-vous que le matériel de capture sélectionné est sur le nœud NUMA correct.

À partir d'une session ssh sur l'appliance, exécutez l'instruction suivante :

cat /sys/class/net/<interface_name>/device/numa_node

où **<interface_name>** est l'interface de capture sélectionnée (par exemple, **p1p1**).

Si le résultat est **0** (zéro), aucune configuration supplémentaire n'est nécessaire.

Si ce n'est pas le cas, ajoutez le résultat en tant que paramètre principal aux paramètres de capture, comme indiqué ci-dessous :

/decoder/config/capture.device.params: core=1

Cette modification nécessite un redémarrage du service pour prendre effet.

Remarque : REMARQUE : Selon la configuration matérielle, les ports de capture peuvent être identifiés avec un nom différent autre que **p1p1/p1p2** mais toujours avec le préfixe **PFRINGZC**. Par exemple, sur certaines appliances, ces ports peuvent être identifiés en tant que **eth4 / eth5**. Pour effectuer une capture à partir de **eth4**, sélectionnez **PFRINGZC,eth4**. Pour effectuer une capture à partir de **eth5**, sélectionnez **PFRINGZC,eth5**.

6. Si le thread d'écriture rencontre des difficultés à maintenir la vitesse de capture, vous pouvez procéder comme suit :

Passez **/datebase/config/packet.integrity.flush** en mode normal.

Remarque : Vous pouvez essayer d'ajuster le paramètre **packet.file.size** pour qu'il soit supérieur, mais conservez la taille du fichier à moins de 10 Go, comme tout le fichier est mis en mémoire tampon à ces vitesses-là.

7. (Facultatif) L'analyse d'application sollicite de manière très intensive le CPU et peut entraîner le Decoder à supprimer des paquets. Pour atténuer les suppressions induites par l'analyse d'application d'analyse, le paramètre /**decoder/config/assembler.parse.valve** peut être défini sur la valeur **true**. Ce qui engendre les conséquences suivantes :

• 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 interrompues lorsque les analyseurs d'applications sont désactivés, mais la fidélité de l'analyse réalisée sur ces sessions peut laisser à désirer.

• Les sessions analysées lorsque les analyseurs d'application sont désactivés ont toujours un méta-réseau associé (Analyseur RÉSEAU).

• La statistique **/decoder/parsers/stats/blowoff.count** affiche le nombre total de sessions ayant contourné les analyseurs d'application (l'analyse réseau est toujours effectuée).

• Lorsque l'analyse des sessions n'est plus à l'état de goulot d'étranglement, les analyseurs d'application sont automatiquement réactivés.

8. Le pool de sessions de l'assembleur doit être suffisamment grand pour ne pas contraindre les sessions.

• Pour déterminer si les sessions sont contraintes par la statistique **/decoder/parsers/stats/blowoff.count** (augmentation) et **/decoder/stats/assembler.sessions** sera compris entre plusieurs centaines de **/decoder/stats/assembler.sessions**.

• Le site de test RSA Security utilisait la configuration suivante à un peu moins de 10G :

/decoder/config/assembler.session.pool a été défini sur 1000000

et **/decoder/stats/assembler.sessions** avoisinerait 630K.

Une autre méthode pour les étapes 1 à 4 présentées ci-dessus peut être utilisée pour configurer 10G Decoder en exécutant les étapes 1, 2, 3 et 4 décrites ci-dessous. Les étapes 5 à 8 ci-dessus sont obligatoires si vous utilisez cette méthode.

1. Effectuez une mise à jour des paramètres des pools de sessions et de paquets en utilisant les valeurs suivantes (sous **/decoder/config**) :

a. **pool.packet.pages = 1000000**

b. **pool.session.pages = 300000**

2. Il convient de définir la taille de bloc d'écriture de paquets (**/database/config/packet.write.block.size**) à 4 Go exactement, ou pour la version 10.6+, d'utiliser **filesize**.

Remarque : Cela permet de configurer le Decoder pour mettre en mémoire tampon les pages volumineuses du fichier et d'y accéder en écriture à l'aide des E/S directes pour des performances maximales.

3. Effectuez une mise à jour des paramètres des threads d'analyse en utilisant les valeurs suivantes (sous **/decoder/config**).

a. **parse.threads =12**

4. Sélectionnez l'adaptateur de port de capture. Les options disponibles sont :

a. Port de capture unique - **PFRINGZC,p1p1** ou **PFRINGZC,p1p2**

b. Capture désactivée sur les deux ports –

i. Sélectionnez **PFRINGZC, P1P1**

ii. Dans la vue Explorateur, **définissez capture.device.params = capture=zc:p1p2,zc:p1p1**

Remarque : Selon la configuration matérielle, les ports de capture peuvent être identifiés avec un nom différent autre que **p1p1/p1p2** mais toujours avec le préfixe **PFRINGZC**. Par exemple, sur certaines appliances, ces ports peuvent être identifiés en tant que **eth4 / eth5**. Pour effectuer une capture à partir de **eth4**, sélectionnez **PFRINGZC,eth4**. Pour effectuer une capture à partir de **eth5**, sélectionnez **PFRINGZC,eth5**.

Considérations relatives au stockage

Lors d'opérations de capture à une cadence 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. Les options prises en charge pour les configurations DAC et SAN sont présentées ci-dessous.

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

L'unité de tête de lecture du Decoder est équipée d'une carte contrôleur matériel-RAID SAS fournissant la connectivité à l'unité DAC. Dans la plupart des déploiements, elles sont configurées de sorte que les unités DAC ne sont pas reliées en cascade à un port unique de la carte SAS. Pour prendre en charge les environnements de vitesse supérieure, un minimum de deux DAC est requis par Decoder, et chacun doit être connecté directement à la carte SAS. Pour prendre en charge deux DAC, connectez le premier DAC à un port de la carte SAS et ensuite connectez 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 (par exemple, si vous ajoutez trois DAC, alors le script doit être exécuté trois fois), en les ajoutant 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 du stockage SAN

Le Decoder accepte toutes les configurations de stockage pouvant satisfaire les besoins en débit soutenu. Notez que la liaison FC 8 Gbits standard sur un SAN n'est pas suffisante pour lire et écrire des données de paquet avec 10G. Par conséquent, les environnements utilisant un SAN doivent configurer la connectivité pour le SAN en utilisant plusieurs FC.

Agrégation d'un 10G Decoder à d'autres composants de Security Analytics

Avec la version initiale, l'agrégation entre le décodeur de paquets et un Concentrator est prise en charge. Les déploiements utilisant Malware Analytics, Event Stream Analysis, Warehouse Connector et Reporting Engine sont susceptibles d'avoir un impact sur les performances et peuvent entraîner une perte de paquets. En raison du volume élevé de taux de sessions, les modifications de configuration suivantes sont recommandées :

• L'agrégation nice sur le Concentrator limite l'impact sur les performances sur le 10G Decoder

/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 attribuant la valeur true au paramètre `/sdk/config/parallel.values`. Cela permet d'améliorer les performances de la procédure d'enquête lorsque le nombre de sessions par seconde est supérieur à 30 000.

Une révision du contenu et analyse ultérieures seront requises pour les déploiements où vous souhaitez obtenir les taux d'utilisation des autres composants SA (par exemple, Warehouse, Malware Analysis, ESA et Reporting Engine).

Un Decoder 10G peut assurer l'agrégation sur un seul Concentrator tout en fonctionnant à des vitesses de 10G.

1. Le Concentrator agrège les données à une cadence de 45 à 70 000 sessions/s.
2. Le Decoder 10G 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 méta/s.
3. Activez l'option Agrégation simple sur le Concentrator pour limiter l'impact sur les performances du Decoder
   /concentrator/config/aggregate.nice=true
4. En raison du volume élevé de sessions sur le Concentrator, vous pouvez envisager d'activer le mode **Valeurs parallèles** sur le Concentrator en attribuant la valeur **true** au paramètre **/sdk/config/parallel.values**. 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 sera moindre lorsque l'agrégation est réalisée sur le Decoder.

Analyse à vitesses élevées

Il va sans dire que l'analyse de paquets bruts à vitesses élevées présente des défis spécifiques. Étant donnés les forts débits 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 sont éludés au niveau de la carte. Pour réaliser un test initial à 10G, lancez uniquement les analyseurs natifs (sauf SMB/WebMail). Utilisez les analyseurs natifs pour déterminer les performances de base, avec un nombre limité ou nul de paquets éludés. 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. Les performances peuvent considérablement varier en fonction des analyseurs. Voici quelques règles d'or :

Contenu Live testé

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

- Contenu MA (7 analyseurs lua, 1 feed, 1 règle d'application)
- 4 feeds (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 en le faisant passer 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.

Configurer le transfert Syslog vers la destination

Cette rubrique fournit des instructions pour le transfert des messages Syslog collectés à partir d'un Log Decoder vers un autre récepteur Syslog.

En plus de collecter des messages Syslog, vous pouvez configurer le Log Decoder pour qu'il transmette des messages Syslog à un autre récepteur Syslog. Security Analytics transfère des messages Syslog après avoir analysé les messages et avant de les écrire 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**.

Conditions préalables

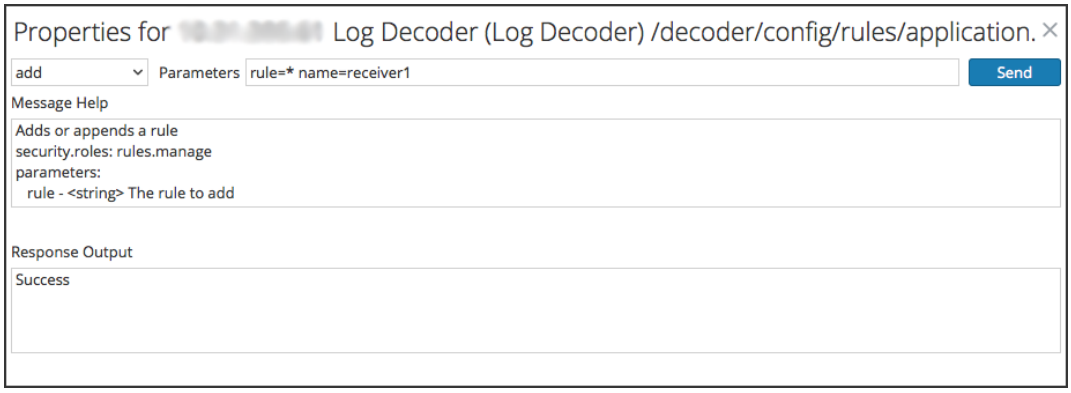
Le Log Decoder doit posséder l'état **Démarré**.

Procédure

Pour configurer le transfert Syslog :

1. Configurez les règles de couche d'application Log Decoder (règles d'application) pour indiquer les messages Syslog possédant des métadonnées indiquant à Security Analytics 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>** (Example 1, **rule=*name=receiver1,** Example 2, **rule="device.type='winevent_nic'" name=receiver1**)

d. Cliquez sur **Send**.



Security Analytics crée la règle **name=receiver1 rule=* order=<n>**. Security Analytics 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.

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 dans la colonne **Actions**, sélectionnez  **> Vue > Explorer**.

b. Dans le paramètre **/decoder/config/logs.forwarding.destination**, spécifiez la destination. Par exemple :
Connexions TLS : **receiver1=tls:receiver1.netwitness.local:6514**
Connexions 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 section **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.

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

logs.forwarding.enabled	true

Rubrique connexe

- Configurer des règles d'application

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 au service Log Decoder.

Vous pouvez créer des clés méta personnalisées pour récupérer des données, rechercher et analyser les logs et les paquets. Les clés méta personnalisées vous permettent d'ajouter un contexte d'enrichissement pour les données des logs et des 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 introduite pour désigner l'emplacement de la ressource, par exemple l'Imprimante1, qui est située au « 5ème étage - Aile A ».

Remarque : Les clés méta personnalisées peuvent également être créées dans le service Decoder. Veillez à sélectionner le fichier index.decoder.xml lorsque vous créez un méta personnalisé dans le service Decoder.

Procédure

Ajouter une clé méta personnalisée au service Log Decoder

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

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services** > **Log Decoder.**
2. Sélectionnez un service, puis cliquez sur  > **Vue** > **Config** > onglet **Fichiers** > **index-logdecoder-custom.xml.**

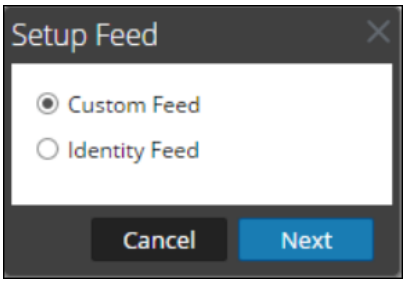
```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexNone"
name="location.src" format="Text"/>
 </Language>
```

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

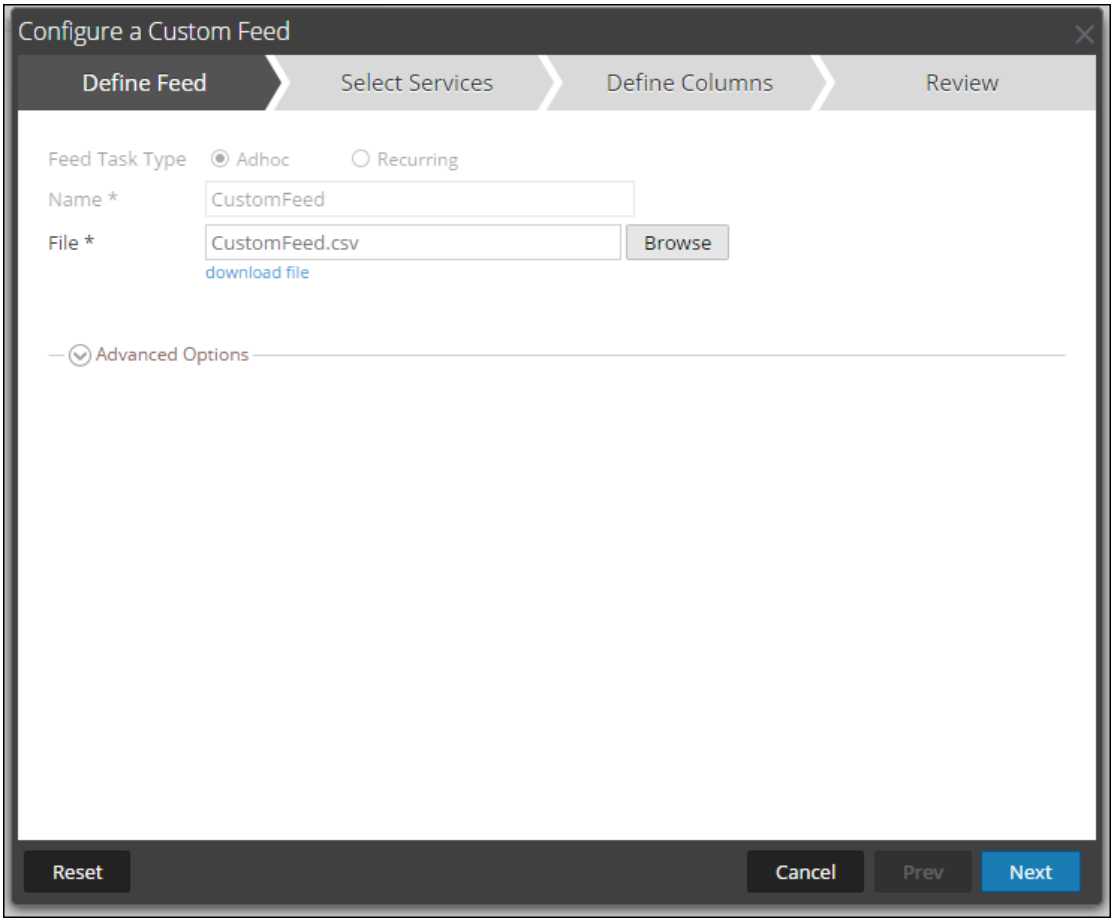
Déployer des ressources dans Live

Pour déployer le feed dans l'environnement Live :

1. Dans le menu **Security Analytics**, sélectionnez **Live** > **Feed**.
2. Dans la barre d'outils, cliquez sur  .
   La boîte de dialogue Configurer le feed s'affiche.

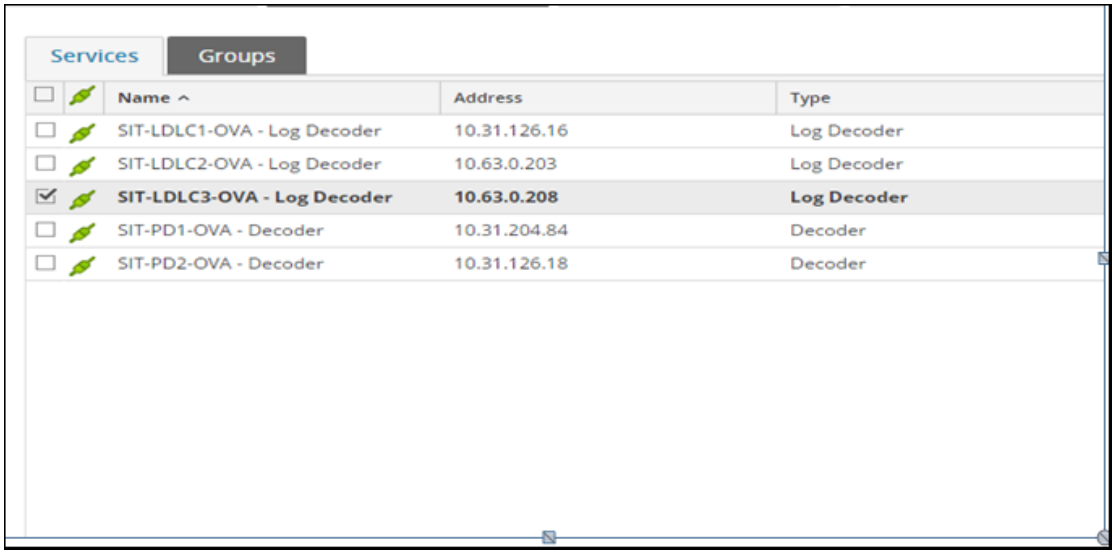


3. Pour sélectionner le type de feed, cliquez sur **Feed personnalisé** puis sur **Suivant**.
   Le panneau Configurer un feed personnalisé s'affiche avec le formulaire Définir le feed ouvert.
   Saisissez le nom et téléchargez le fichier CSV du feed.



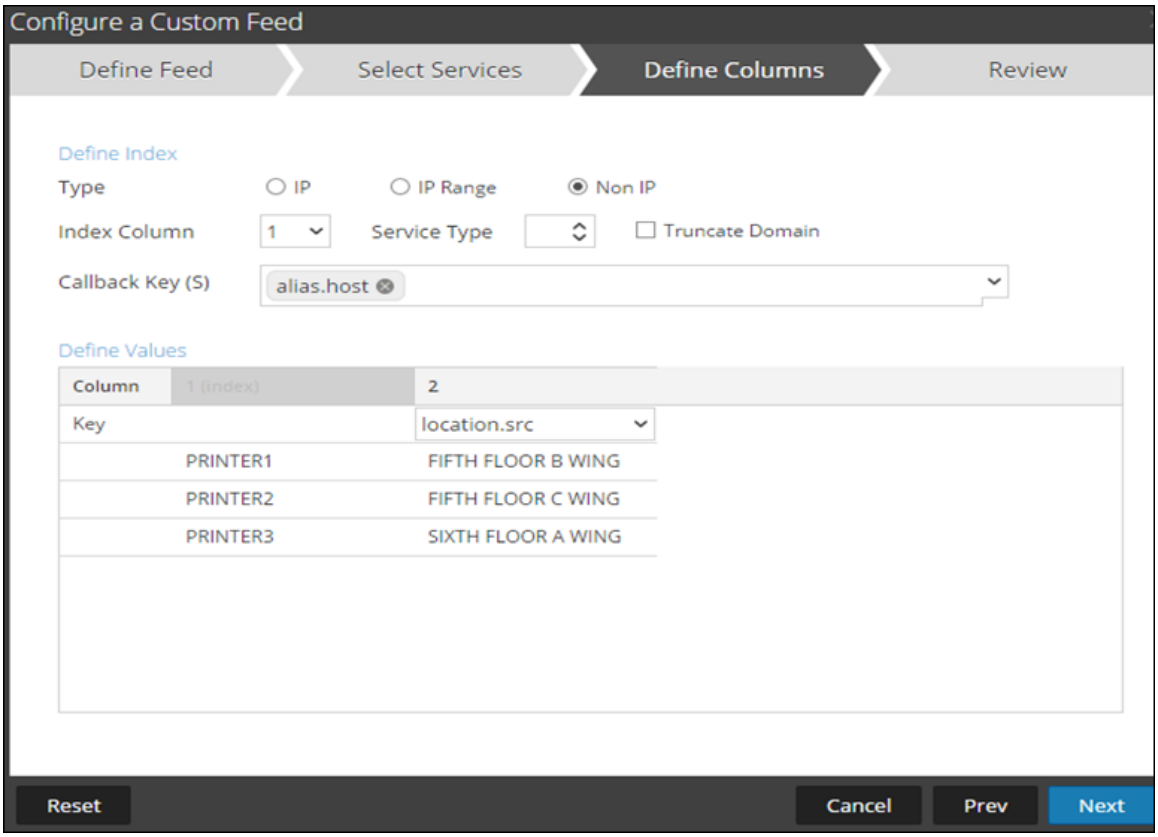
4. Cliquez sur **Suivant**.

5. Sélectionnez le service **Log Decoder**, où le feed doit être téléchargé.



6. Dans la section Définir l'index, sélectionnez le type d'index, la colonne de l'index et la clé de rappel. Dans la section Définir les valeurs, saisissez la clé méta personnalisée.
   Le contenu du fichier .csv s'affiche dans l'assistant de configuration d'un feed. Dans ce cas, la première colonne indique le nom d'hôte de la ressource et la deuxième colonne indique l'emplacement de la ressource.

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'. Par conséquent, 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 Définir les valeurs, sélectionnez la clé méta personnalisée dans le menu déroulant.

7. Cliquez sur **Suivant**.
8. Cliquez sur **Terminé**.

Pour plus d'informations sur l'assistant de configuration des feeds, reportez-vous à la rubrique Créer et déployer un Feed personnalisé à l'aide de l'assistant.

Ajouter l'entrée méta personnalisée au fichier d'index du service Concentrator

Pour ajouter l'entrée méta personnalisée au fichier d'index du service Concentrator :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services** > **Concentrator**.
2. Cliquez sur > **Vue** > **Config** > **onglet** Fichiers > **index-concentrator-custom.xml.**
3. Ajouter l'entrée 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. Redémarrez les services Concentrator. Dans la vue Services, cliquez sur  > **Redémarrer**.

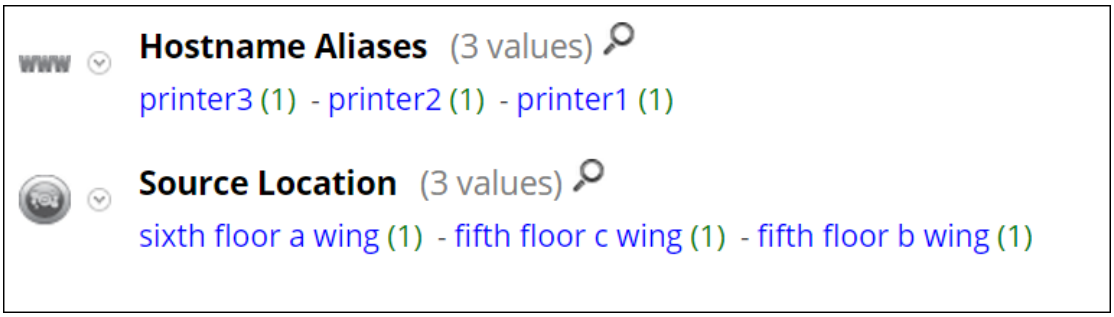
Remarque : Dans le cas du service Broker, ce dernier récupère son index du service Concentrator à partir duquel il effectue l'agrégation. Vous n'avez donc pas besoin de créer un méta personnalisé dans le service Broker. Si vous n'avez pas indexé la clé méta dans le service Concentrator, le service Broker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

Rechercher

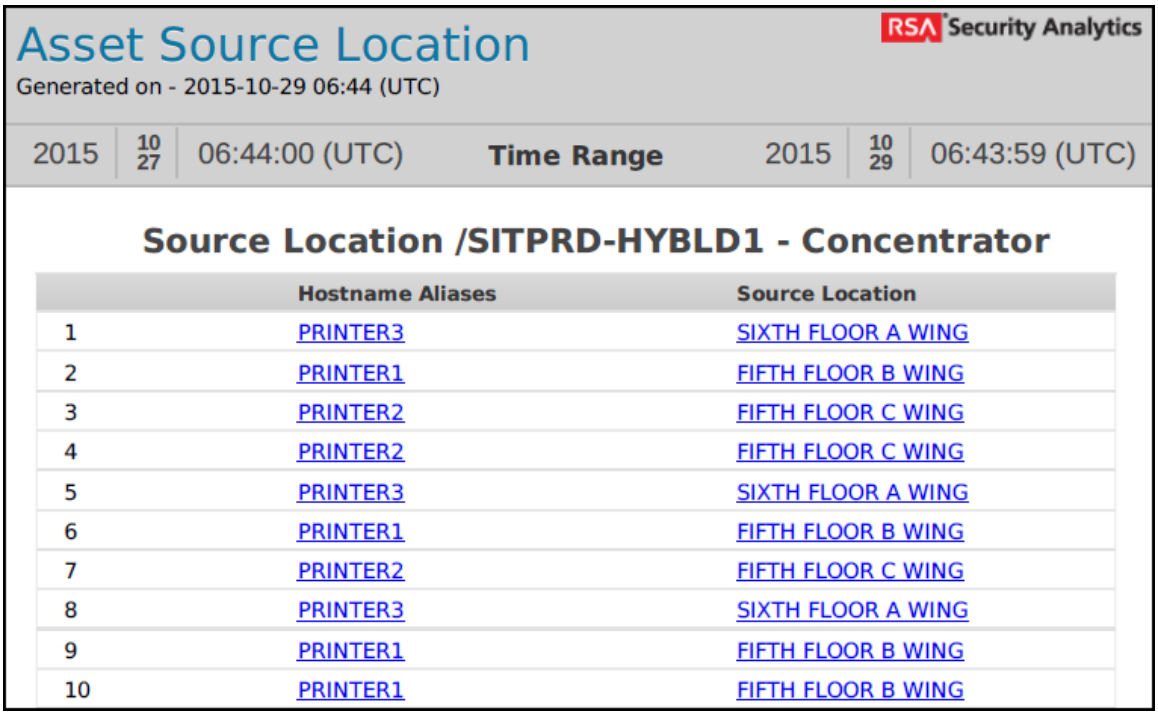
Remarque : Veillez à vous déconnecter et vous reconnecter à partir de l'interface utilisateur de Security Analytics, pour pouvoir afficher la clé méta personnalisée dans Investigation.

Pour effectuer la recherche de la clé méta personnalisée :

1. Dans le menu **Security Analytics**, sélectionnez **Investigation** > **Naviguer**.
2. Sélectionnez un service Concentrator.
3. 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

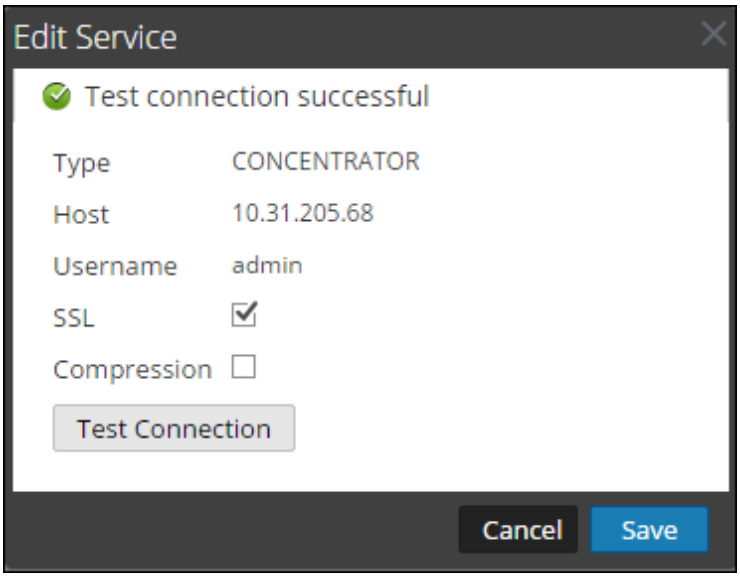
Les procédures suivantes doivent être exécutées si vous avez configuré les services Warehouse Connector, Archiver, Reporting Engine et ESA.

Mettre à jour le schéma dans ESA

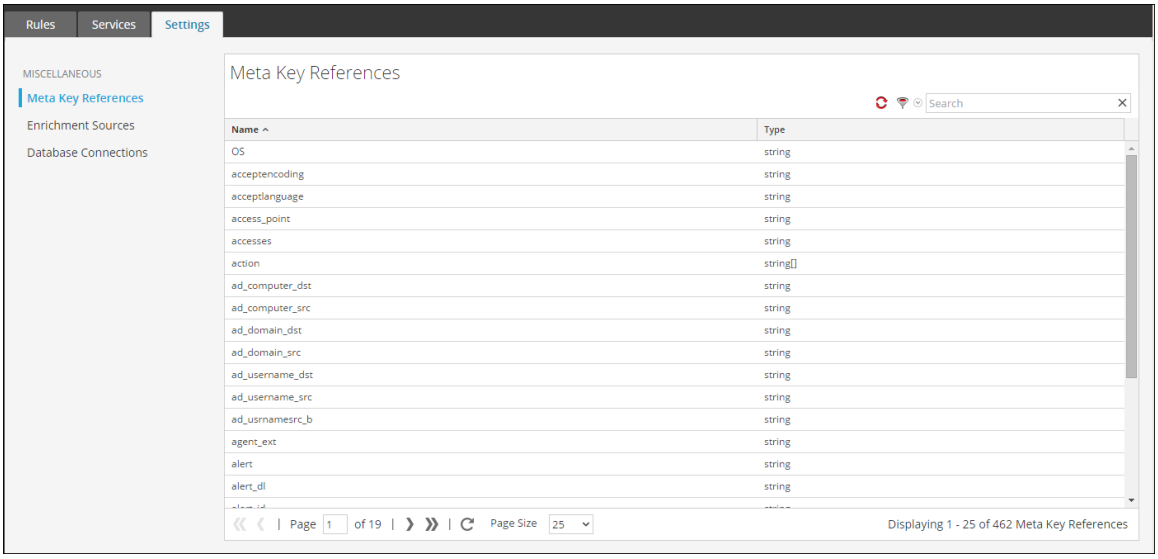
Avant de mettre à jour le schéma dans ESA, la clé méta personnalisée doit être indexée dans le service Concentrator.

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

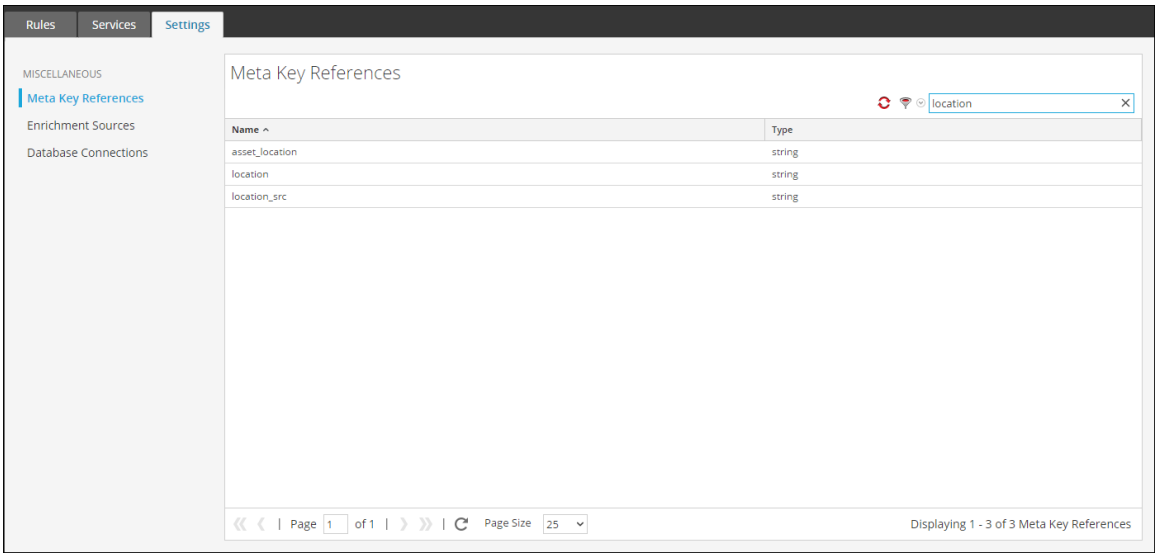
1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**> **ESA- Event Stream Analysis** > **Vue** > **Config**.
2. Modifiez la source de données Concentrator.
3. Cliquez sur **Tester la connexion**.



4. Cliquez sur **Enregistrer** une fois la connexion établie.
5. Cliquez sur **Appliquer**.
6. Accédez à **Alertes** > **Configurer** > **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 Security Analytics 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. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services** > **Archiver**.
2. Cliquez sur > **Vue** > **Config** > **Fichiers** > **index-archiver-custom.xml**.
3. Ajoutez l'entrée 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. Redémarrez le service Archiver. Cliquez sur > **Redémarrer.**

   Le schéma Archiver est mis à jour avec la clé méta personnalisée.

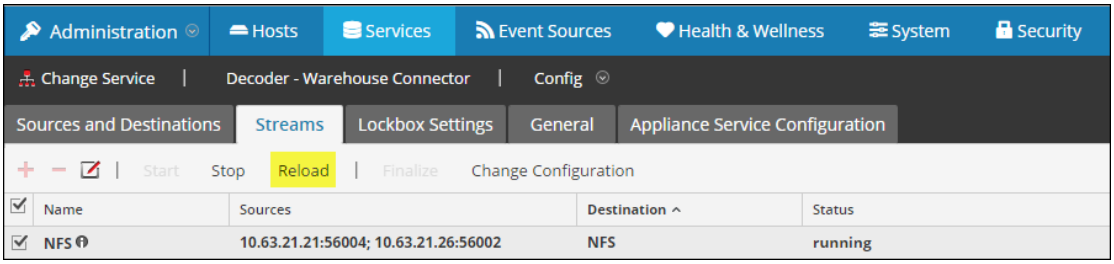
Mettre à jour le schéma dans Warehouse Connector

Si vous souhaitez configurer Security Analytics Warehouse avec le méta personnalisé et l'utiliser dans le rapport Warehouse, vous devez mettre à jour le schéma Warehouse 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 dans Reporting Engine :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **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

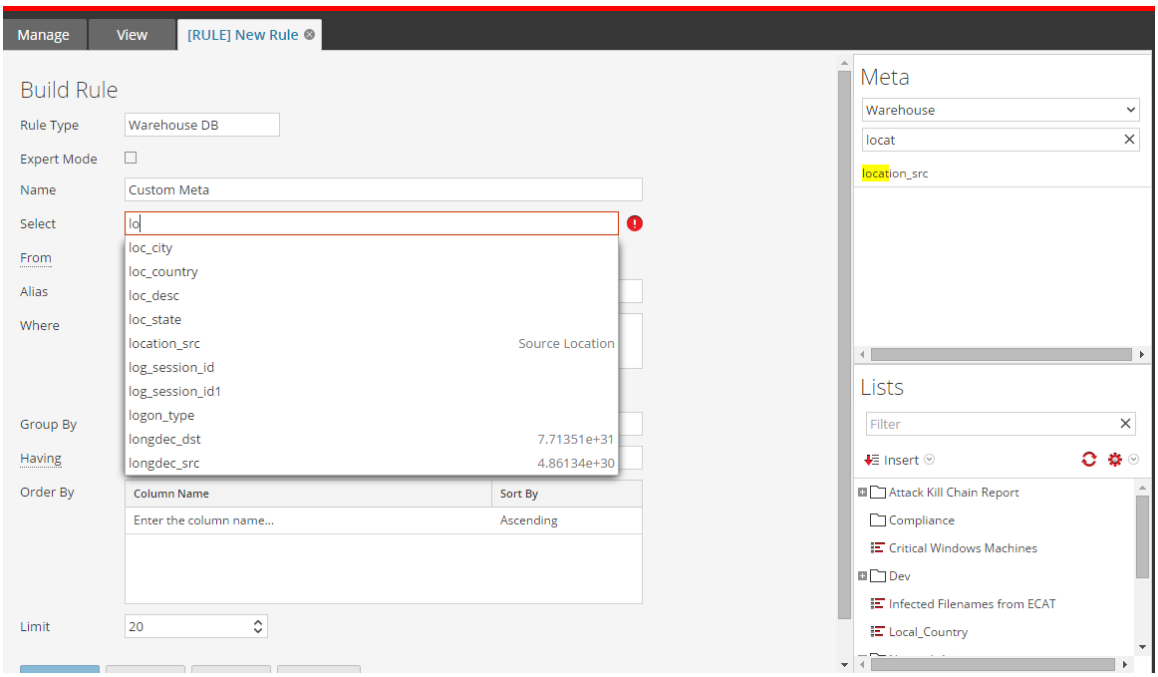
Pour mettre à jour le schéma dans Reporting Engine :

1. Dans le menu **Security Analytics**, sélectionnez **Administration**> **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 **Rapports** > **Règles**.
2. Dans la barre d'outils, cliquez sur .
3. Sélectionnez Base de données Warehouse.
4. Dans la page Élaborer une règle, recherchez le méta personnalisé dans le panneau droit de la page.
   La clé méta personnalisée s'affiche.


Manage
View
[RULE] New Rule
Build Rule
Rule Type
Warehouse DB
Expert Mode
Name
Custom Meta
Select
lo
From
Alias
Where
loc_city
loc_country
loc_desc
loc_state
location_src
Source Location
log_session_id
log_session_id1
logon_type
longdec_dst
7.71351e+31
longdec_src
4.86134e+30
Group By
Having
Order By
Column Name
Sort By
Enter the column name...
Ascending
Limit
20
Meta
Warehouse
locat
location_src
Lists
Filter
Insert
Attack Kill Chain Report
Compliance
Critical Windows Machines
Dev
Infected Filenames from ECAT
Local_Country

Mappages d'analyseur d'accès

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, les messages communs entre les types de sources d'événements seront mal classés. 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.

Procédures

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

Pour activer une adresse IP pour le mappage de sources d'événements :

1. Dans le menu Security Analytics, sélectionnez **Administration > Système > Mappages de l'analyseur de log**.
2. Sélectionnez Log Decoder, puis **Vue > Config**.
   L'onglet Mappage d'analyseurs 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. Dans le menu Security Analytics, sélectionnez **Administration > 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'analyseurs**.

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 **Sources d'événements(**s), saisissez le type de source d'événement.
  Par exemple :`apache`

Un hôte et un ou plusieurs types de source d'événement
- Dans le champ **Hôte**, saisissez le nom d'hôte.
  Par exemple : `10.0.0.1`
- Dans le champ **Sources 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 **Sources 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 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 **Sources 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.

6. Cliquez sur **OK**.

   Le mappage des analyseurs est ajouté.

7. Pour accepter la sélection des mappages des analyseurs, cliquez sur **Appliquer**.
8. Pour annuler la sélection des mappages d'analyseurs, 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. Dans le menu Security Analytics, sélectionnez **Administration > Services.**
2. Sélectionnez un service Log Decoder.
3. Dans la colonne Actions, sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.
   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. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service Log Decoder.
3. Dans la colonne Actions, sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.
5. Sélectionnez le mappage que vous souhaitez modifier.
6. Cliquez sur 
7. Dans le champ **Source(s) d'événement(s)** , saisissez la ou les sources d'événements.
8. Cliquez sur **OK** pour accepter la source d'événement modifiée.
9. Pour accepter la source d'événement modifiée, cliquez sur **OK**.
10. 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. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service Log Decoder.

3. Dans la colonne Actions, sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.
5. Sélectionnez le mappage que vous souhaitez supprimer.
6. Cliquez sur .
   Le mappage est supprimé.
7. 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 :

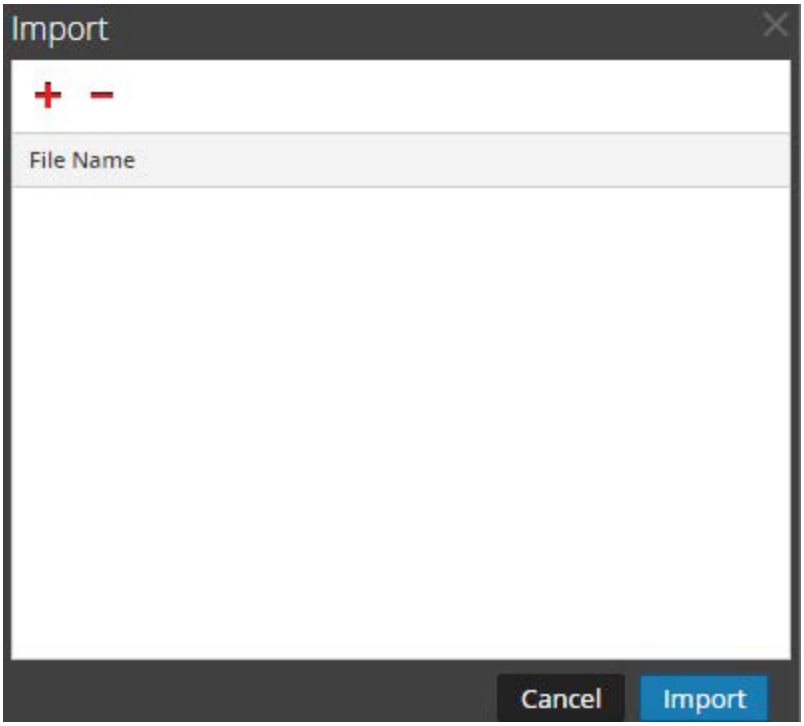
1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service Log Decoder.
3. Dans la colonne Actions, sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.
5. Pour trier une colonne, cliquez 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 parsers dans l'ordre, qu'elles sont répertoriées.

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. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service Log Decoder.
3. Dans la colonne Actions, sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.

5. Sélectionnez **Actions > Importer**.
   La boîte de dialogue Importer s'affiche.



6. Cliquez sur +.
7. Sélectionnez le fichier à importer, puis cliquez sur **OK**.
8. 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. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service Log Decoder.
3. Dans la colonne Actions, sélectionnez **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.
5. Sélectionnez les mappages à exporter.

6. Sélectionnez **Actions > Exporter > Sélection**.
   La boîte de dialogue Sélections pour l'exportation s'affiche.

7. 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. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service Log Decoder.
3. Dans la colonne Actions, sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'affiche.
4. Sélectionnez l'onglet **Mappages d'analyseurs**.
5. Dans la barre d'outils Mappage d'analyseurs, saisissez l'hôte ou la source d'événement dans le champ **Filtrer**.
6. Cliquez sur **Enter**.
   Les hôtes ou les sources d'événements qui correspondent aux noms saisis dans le champ **Filtrer** s'affichent.

Corriger les règles dont la syntaxe est obsolète

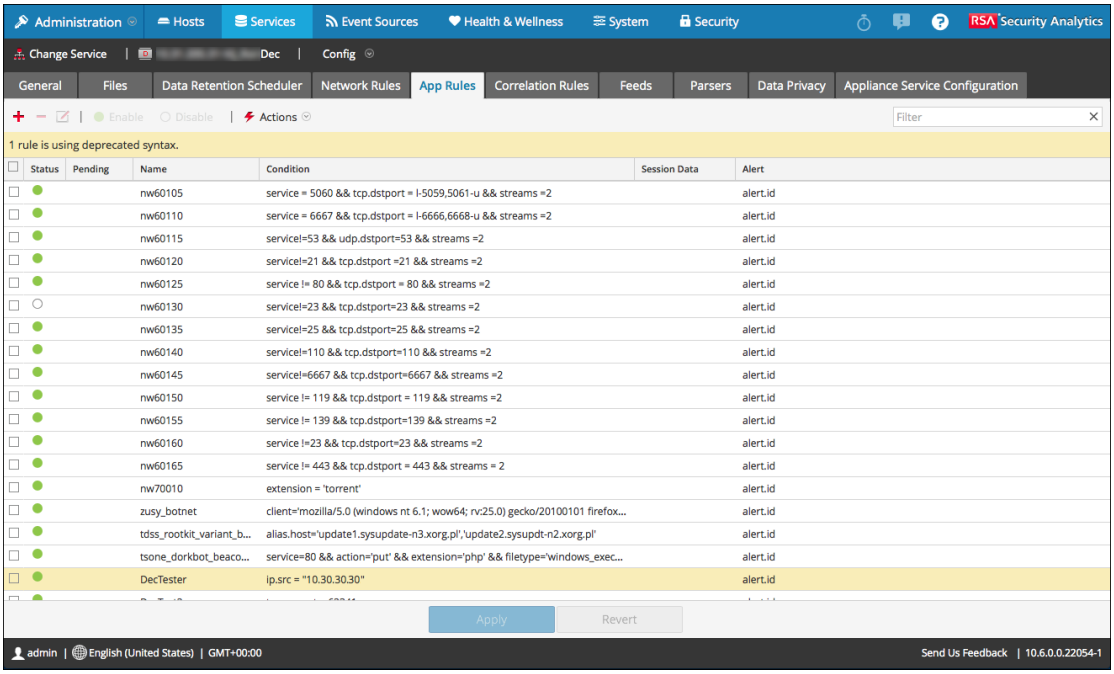
Après avoir effectué une mise à jour vers Security Analytics 10.6, l'interface utilisateur met en surbrillance les règles contenant une syntaxe obsolète. Il est important de corriger la syntaxe des règles mises en surbrillance car elles peuvent contenir une syntaxe ambiguë pouvant provoquer des résultats inattendus. L'Éditeur de règles fournit des info-bulles supplémentaires. Une fois les règles corrigées, les mises en surbrillance disparaissent.

Instructions relatives aux règles et requêtes Cette rubrique fournit des instructions que toutes les requêtes et conditions de règle de Security Analytics doivent suivre. Elle fournit également des informations sur la configuration du mode strict, ainsi que sur les syntaxes valide et obsolète.

Procédure

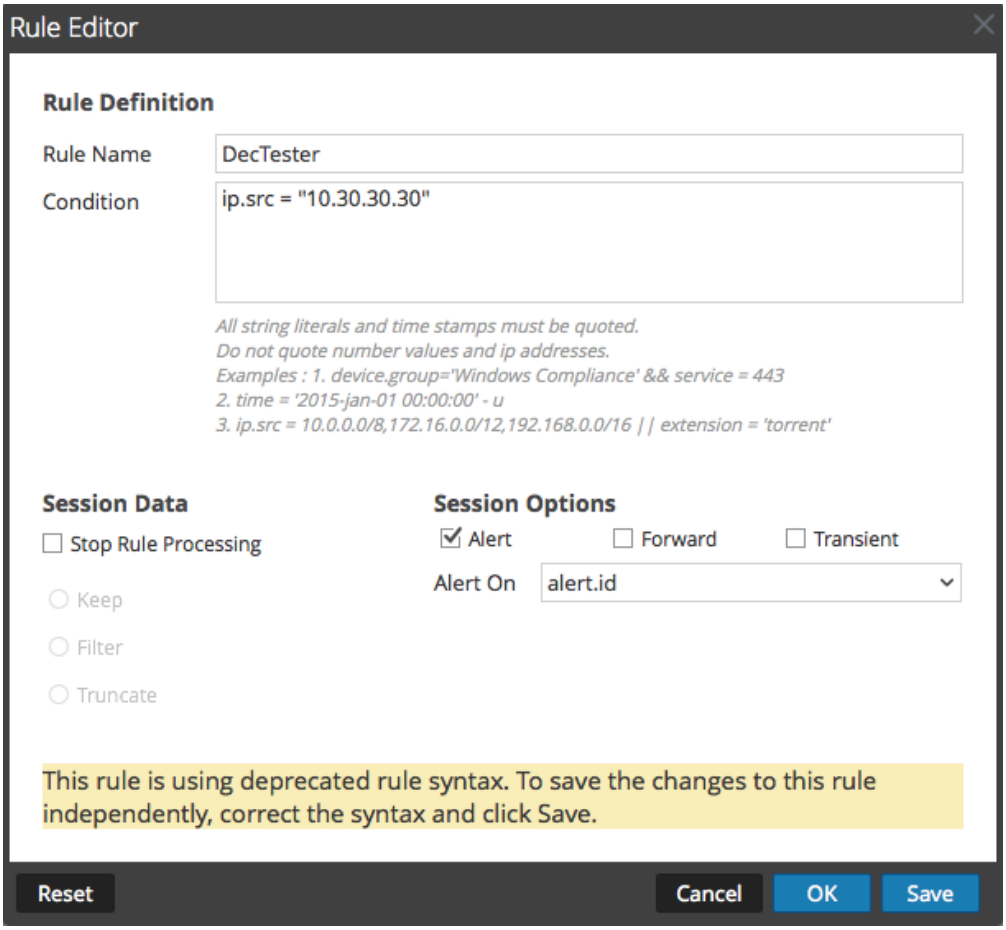
Pour corriger les règles contenant une syntaxe obsolète :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > 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.
   L'onglet Règles du type de règle sélectionné affiche le nombre de règles utilisant la syntaxe obsolète ; les règles obsolètes sont mises en surbrillance.



4. Sélectionnez une règle obsolète et cliquez sur .
   L'Éditeur de règles affiche des informations supplémentaires pour la règle obsolète et inclut

une autre option Enregistrer.



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 ni les adresses IP entre guillemets. Instructions relatives aux règles et requêtes fournit des informations supplémentaires.
   Par exemple, si la condition de règle obsolète 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 service Decoder. La règle corrigée s'affiche sous l'onglet Règles sans la mise en surbrillance.
   - Pour corriger la règle et l'appliquer ultérieurement au service 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 service Decoder.

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 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/Flex, il sera désactivé et aucun analyseur Lua/Flex ne sera chargé.
- Si vous **activez** le système d'analyse Lua/Flex, il sera activé et chaque analyseur Lua/Flex sera activé et désactivé en fonction des configurations individuelles définies.

Procédure

Pour activer ou désactiver les systèmes d'analyse Lua et Flex sur un service Decoder ou Log Decoder :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > 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, sélectionnez **/decoder/parsers/config**.
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

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.

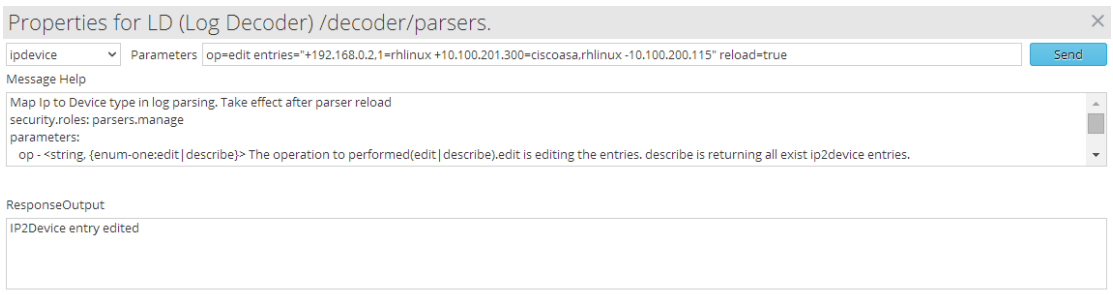
Si vous mappez une adresse IP à ses services, le Log Decoder peut identifier le service à partir duquel le log est généré. Lorsque les messages sont dans le Log Decoder à partir d'un service mappé, les analyseurs affectés sont chargés de trouver les correspondances d'événements.

Vous pouvez attribuer des types de services à la valeur du nom d'hôte, IPV4 et IPV6 de l'événement source. 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.

Procédure

Pour mapper une adresse IP à un type de service, procédez comme suit :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > 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=edit entries="+/-ipaddress=service”reload=true` (par exemple, `op=edit entries="+10.100.201.300=ciscoasa" reload=true`)
5. Cliquez sur **Envoyer**.



Commande IPdevice

Dans la commande ipdevice, deux opérations sont disponibles :

- Edit : Vous pouvez utiliser cette opération pour ajouter et supprimer des entrées dans le mappage ipdevice.
  - Pour ajouter une entrée, spécifiez :
    `+<IP value> = <service type>`
  - Pour supprimer une entrée, spécifiez :
    -<IP value> = <service type>
- Décrire : Cette opération renvoie les valeurs actuellement présentes dans le mappage ipdevice.

Commande reload

Vous devez recharger l'analyseur après avoir modifié le mappage ipdevice à l'aide de la commande `reload=true`. En revanche, cette opération ne doit pas être effectuée après chaque entrée, mais uniquement à la fin de la tâche. Vous pouvez également remplacer une configuration existante en modifiant la valeur. La nouvelle valeur prend effet après le rechargement de l'analyseur.

Résultat

Security Analytics mappe l'adresse IP aux types de services dans le Log Decoder.

Exemples

Les exemples suivants fournissent différentes instances pour le mappage de l'adresse IP aux types de services :

- Si vous souhaitez mapper deux entrées différentes avec des valeurs IPV4 et des types de services différents, saisissez le paramètre suivant dans la commande **ipdevice**, puis cliquez sur **Envoyer**.
  `op=edit entries="+10.5.245.9=ciscoasa +10.5.245.45=vmware_vcloud"`
- Si vous souhaitez supprimer une entrée pour une valeur IPV4 et un type de service uniques, saisissez le paramètre suivant dans la commande **ipdevice**, puis cliquez sur **Envoyer**.
  `op=edit entries="-10.5.245.9=ciscoasa"`
- Si vous souhaitez créer une entrée unique pour une valeur IPV6 et un type de service, saisissez le paramètre suivant dans la commande **ipdevice**, puis cliquez sur **Envoyer**.

```
op=edit entries=”+ 2001:0db8:85a3:0000:0000:8a2e:0370:7353=vmware_
esx_esxi"
```

- Si vous souhaitez créer une entrée unique pour une valeur IPV4 unique qui dispose de deux types de service, et si vous souhaitez envoyer chaque type de service à des collecteurs différents, saisissez le paramètre suivant dans la commande **ipdevice**, puis cliquez sur **Envoyer**.

  ```
  op=edit entries="+10.168.0.2,nwappliance20819=rhlinux
  +10.168.0.2,nwappliance3014=apache"
  ```

- Si vous souhaitez créer une entrée pour un nom d'hôte unique avec deux types de service différents, et si vous souhaitez charger l'analyseur, saisissez le paramètre suivant dans la commande **ipdevice**, puis cliquez sur **Envoyer**.

  ```
  op=edit entries=”+RS214Server-2=rhlinux,apache” reload=true
  ```

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 dans Security Analytics un fichier log capturé d'un autre service. Les noms des fichiers log portent l'extension **.log**.

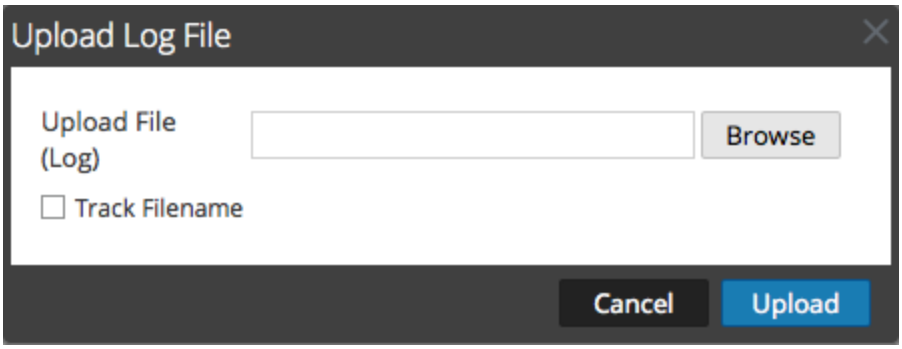
Si vous téléchargez un fichier log dans un Log Decoder, ce dernier l'analyse et génère des métadonnées pour chacun des logs qu'il contient. Ces logs sont ajoutés aux logs déjà décodés dans le Log Decoder et sont disponibles pour analyse. Security Analytics inclut une option de suivi des noms de fichier 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 quand d'autres opérations du Log Decoder empêchent une telle action. Ce peut ainsi être le cas lorsque le Log Decoder capture des logs.

Procédure

Pour importer un fichier log dans un Log Decoder :

1. Dans le **menu Security Analytics**, sélectionnez **Administration > 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 le fichier de capture de paquets

Cette rubrique explique comment importer un fichier de capture de paquet vers un Decoder.

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 dans Security Analytics un fichier capturé d'un autre service. Les fichiers de capture de paquet pris en charge sont au format **pcap** et **pcap.gz**.

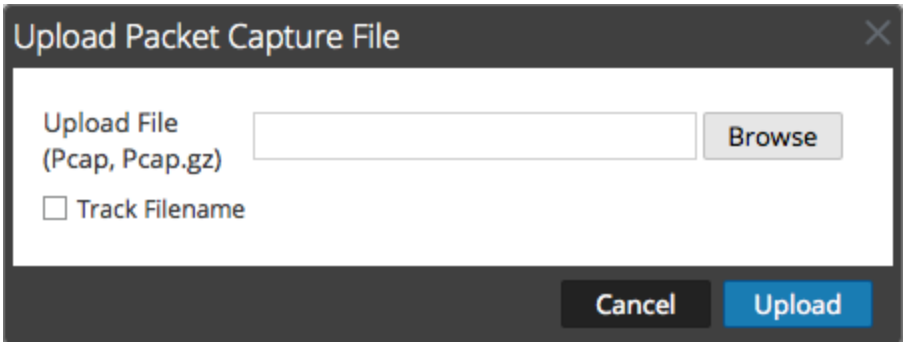
Quand un fichier de capture de paquet est téléchargé dans un décodeur, ce dernier crée des sessions à partir des paquets du fichier. Ces sessions sont ajoutées aux sessions déjà décodées dans le décodeur et sont disponibles pour analyse. Security Analytics inclut une option de suivi des noms de fichier qui facilite la recherche d'un jeu de sessions donné. Une fois le fichier de capture de paquet téléchargé avec cette option, le décodeur 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 décodeur empêchent une telle action. Ce peut être le cas lorsque le décodeur capture des paquets.

Procédure

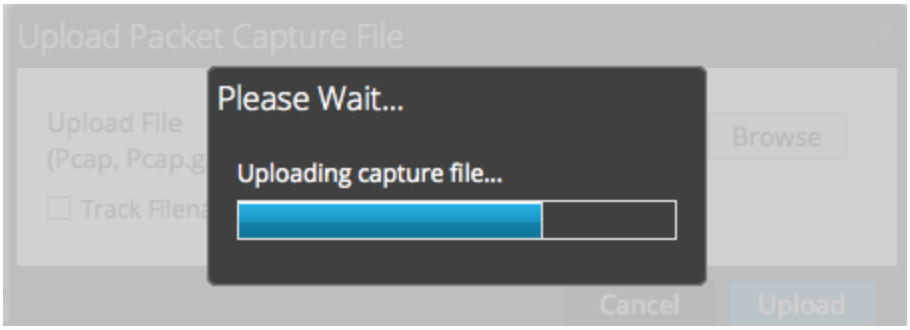
Pour sélectionner et télécharger un fichier de capture de paquet :

1. Dans le menu **Security Analytics**, sélectionnez **Administration >Services**.
   La vue Services Administration s'affiche.
2. Sélectionnez le nom du décodeur, puis  **> Vue > Système**.
   La vue Système de services du décodeur 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 décodeur 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.

Vérifier les informations système du Decoder

Cette rubrique présente les fonctions de la vue Système qui appartiennent spécifiquement aux Decoders et Log Decoders.

Lorsqu'un service est ajouté pour la première fois à Security Analytics, les valeurs par défaut des paramètres de configuration système s'appliquent. Vous pouvez modifier ces valeurs pour optimiser les performances.

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	☐
SSL Port	56005
Stat Update Interval	1000
Threads	20

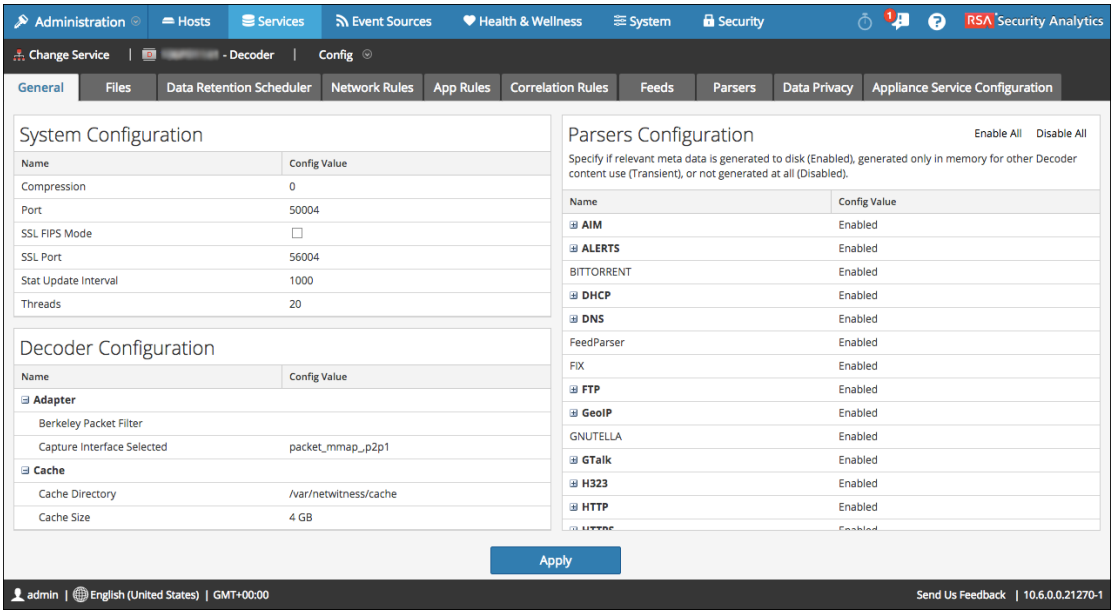
Dans la plupart des cas, les valeurs par défaut pour la compression, l'intervalle de mise à jour des statistiques et le nombre de threads dans le pool de threads sont configurées de façon à optimiser les performances système. Vous souhaiterez peut-être modifier le paramètre SSL de votre environnement, 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.

Procédure

Pour modifier les paramètres de configuration système :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services**, sélectionnez un service Decoder ou Log Decoder et cliquez sur  **>Vue > Config**.

La vue Configuration des services pour le service sélectionné s'affiche.



3. Dans **Configuration système**, cliquez sur le champ que vous souhaitez modifier et saisissez la nouvelle valeur.
4. Lorsque la modification est terminée, cliquez sur **Appliquer.**

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

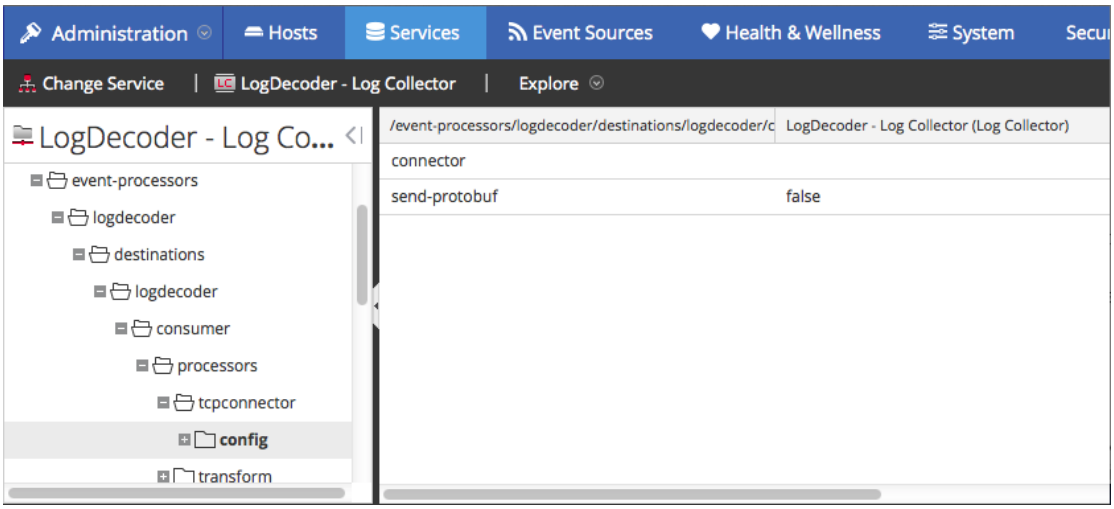
Cette rubrique décrit la méthode à suivre pour configurer un Log Decoder afin qu'il accepte les logs au format protobuf (Protocol Buffer).

Il peut arriver que vous souhaitiez analyser des fichiers log au format protobuf (Protocol Buffer).

Procédure

Pour importer un fichier log dans un Log Decoder :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un Log Decoder dans la grille **Service**, puis sélectionnez  **> Vue > Explorer**.
   La vue Explorer du Log Decoder 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%**

Références

Cette rubrique rassemble des références qui décrivent l'interface utilisateur des Decoders et Log Decoders dans Security Analytics. Ces rubriques sont présentées par ordre alphabétique.

Utilisez cette section si vous recherchez la description des attributions de droits et définitions des fonctions de l'interface utilisateur.

La vue Configuration des services Security Analytics met à disposition une interface utilisateur pour configurer des Decoders et des Log Decoders afin de capturer des données et pour contrôler le type de trafic capturé à l'aide de règles, flux et analyseurs.

Topics

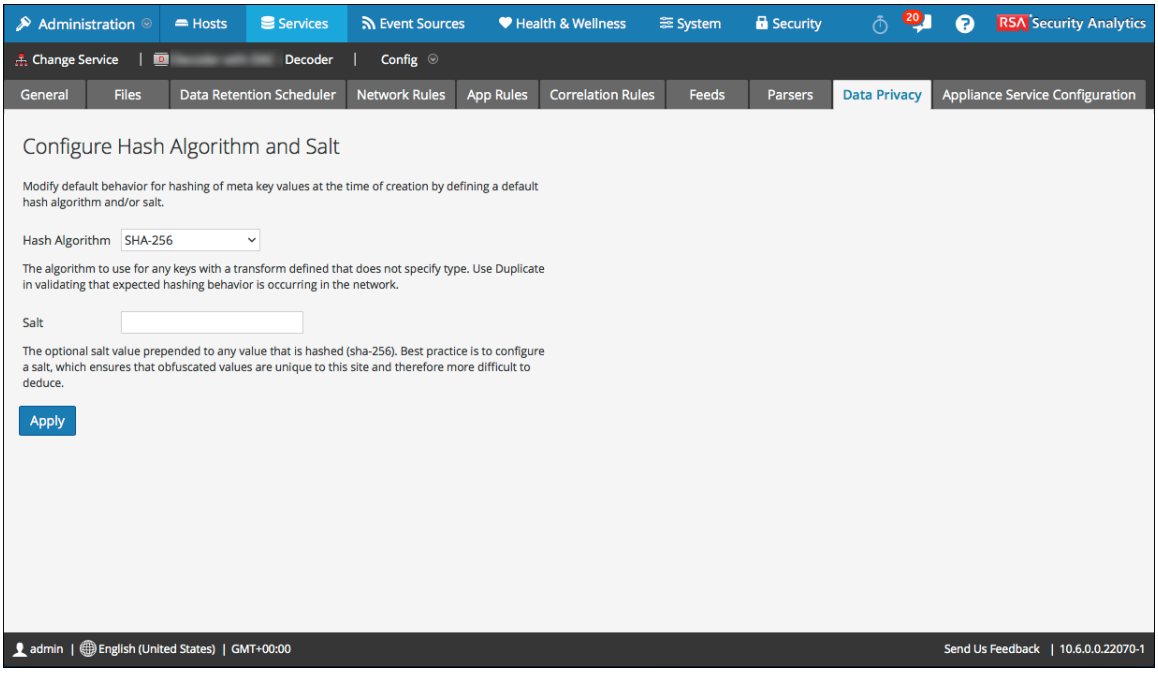
Vue Configuration des services - onglet Confidentialité des données

Cette rubrique propose une description des options configurables pour un Decoder ou Log Decoder sous l'onglet Confidentialité des données.

Sous l'onglet Confidentialité des données, les administrateurs peuvent configurer les paramètres de confidentialité des données de certains services Core. Pour Decoder et Log Decoder, vous pouvez définir l'algorithme de hachage par défaut et la valeur salt.

Pour accéder à cet onglet :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service Decoder ou Log Decoder, puis cliquez sur > **Configuration**.
   L'onglet Général s'affiche.
3. Cliquez sur l'onglet **Confidentialité des données**.



Fonctions

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 Security Analytics 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 - onglet Feeds

Cette rubrique décrit les fonctions de la vue Configuration des services Decoder > onglet Feeds.

Les feeds et les analyseurs sont des programmes FLEXPARSE 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 décodeurs. Généralement, ils sont utilisés pour l'extraction de métadonnées statiques et l'identification des services.

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

Security Analytics utilise des feeds pour créer des métadonnées sur la base des valeurs méta 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.

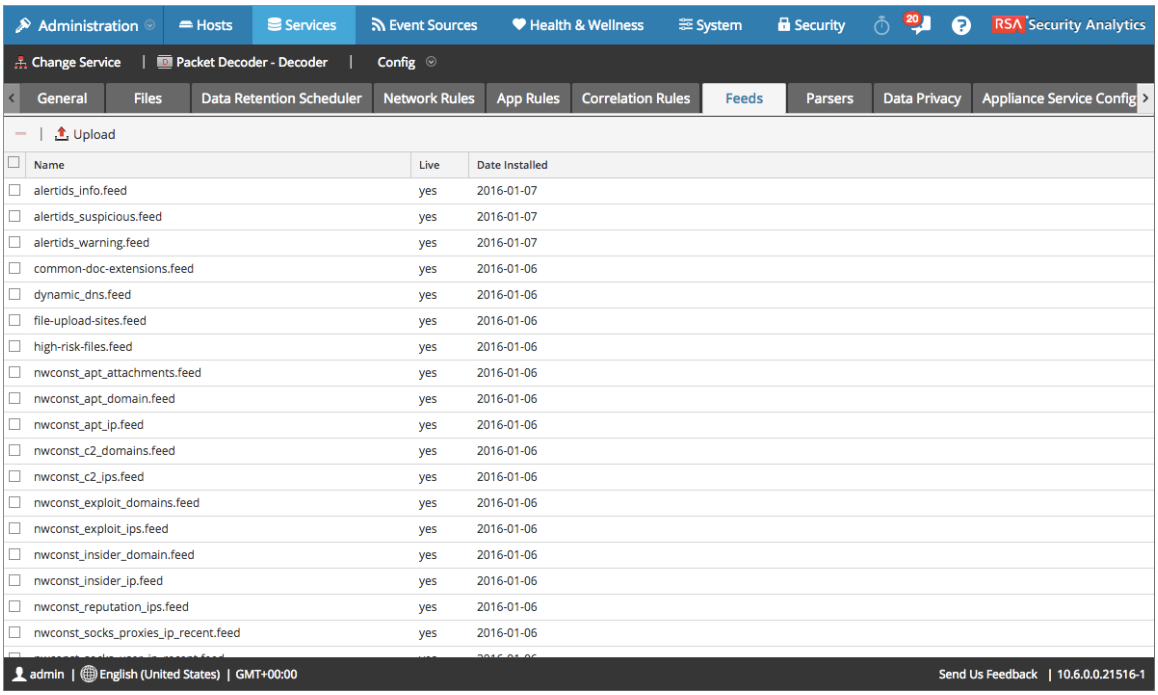
Les feeds peuvent être ajoutés, supprimés et mis à jour alors qu'un Decoder est en cours d'exécution sans que cela ait d'impact sur la capture. La vue Configuration des services > onglet Feeds propose une interface utilisateur qui permet de gérer les feeds sur les Decoders.

Pour accéder à cette vue, procédez comme suit :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis  **>Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Feeds**.

Voici un exemple de l'onglet Feeds.



Fonctions

La grille Feed répertorie tous les feeds actuellement déployés sur le Decoder. La barre d'outils de l'onglet Feeds comporte des options permettant d'utiliser les feeds dans la grille.

Barre d'outils de l'onglet Feeds

Fonctionnalité	Description :
Upload	Affiche la boîte de dialogue Télécharger les feeds.
	Supprime les feeds sélectionnés.

Grille Feed

La grille Feed répertorie tous les feeds actuellement déployés sur le Decoder.

Colonne	Description :
Name	Nom du feed ou fichier de feed.

Colonne	Description :
Live	Indique si le feed provient de Live. Les valeurs possibles sont **Oui**, **Non** ou **N/A**. • **Oui** = Installé via Live • **Non** = Installé via Security Analytics • **N/A** = Le feed n'a pas de fichier d'attribut créé par Security Analytics pour effectuer le suivi de la date d'installation. Il se peut que le feed ait été installé manuellement et non via Security Analytics ou Live. Les feeds installés manuellement fonctionnent encore correctement.
Date d'ins-tallation	Date à laquelle le feed a été transmis au service.

Section

- Boîte de dialogue Télécharger les feeds

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.

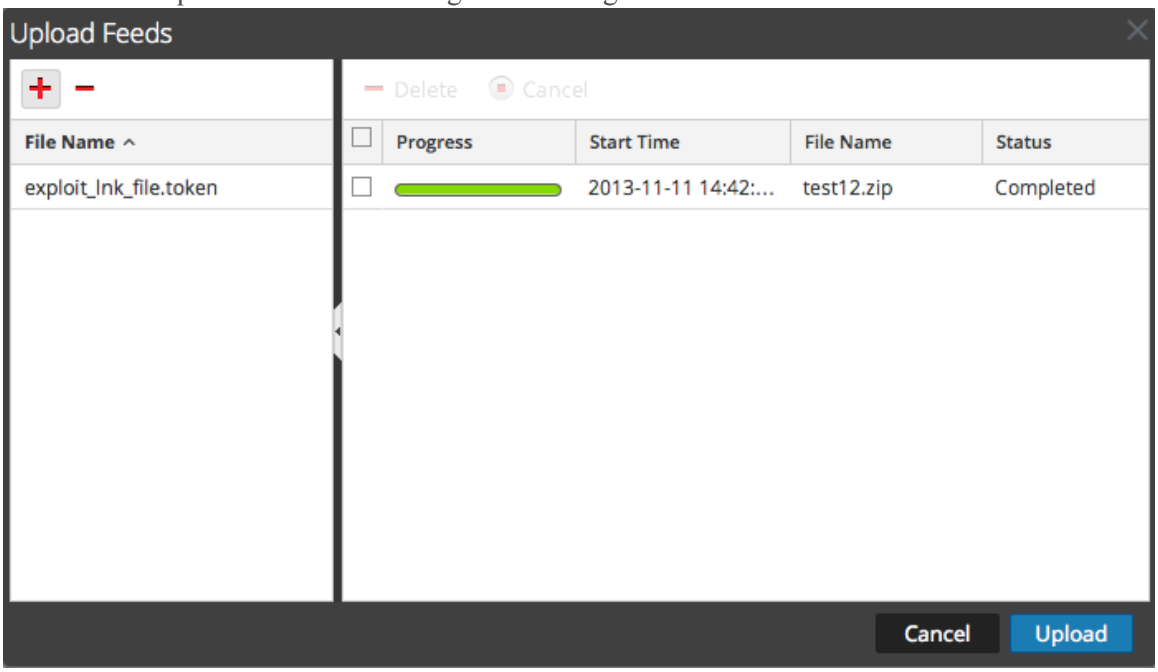
Dans la vue Configuration des services, cliquez sur l'option **Télécharger** de l'onglet Feeds pour accéder à la boîte de dialogue Télécharger les feeds. Vous pouvez y gérer le téléchargement des feeds sur un Decoder ou un Log Decoder.

Vous pouvez accéder à cette vue de la manière suivante :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis >**Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Feeds**.
4. Cliquez sur Upload.

Voici un exemple de la boîte de dialogue Télécharger les feeds.



Fonctions

Grille File

La grille File 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 grille File.
	Supprime les fichiers sélectionnés dans la grille File.
Nom de 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.

Grille Télécharger une tâche

La grille Télécharger une tâche répertorie les tâches de téléchargement que vous avez lancées en cliquant sur **Télécharger**.

Fonction/Colonne	Description :
	Supprime une tâche de téléchargement.
Progress	Affiche l'avancée d'une tâche de téléchargement.
Start Time	Affiche l'heure de début d'une tâche de téléchargement.
Nom de 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.
Chargement	Démarre le téléchargement des fichiers de feed répertoriés dans la grille File. Chaque feed est indiqué dans une ligne distincte dans la grille Processus de téléchargement.

Vue Configuration des services - onglet Fichiers

Cette rubrique présente les fichiers de configuration de Decoder et Log Decoder qui sont visibles dans la 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.

À l'instar des autres services Security Analytics Core, le Decoder et le Log Decoder comportent un fichier d'index, et peuvent également avoir un crashreporter, un netwitness et un planificateur. Les fichiers d'index du Decoder et du Log Decoder sont nommés **index-decoder.xml** et **index-logdecoder.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 apparaissent désormais mais seulement si table-map.xml a été trouvé sur le système de fichiers (par exemple, s'il s'agit d'un log decoder avec un contenu Envision installé).

Filename	Description :
GeoPrivate.ipl	Cet analyseur fixe prend les adresses IP et les convertit en lieux géographiques. Les emplacements s'affichent via Google Earth.
NwFlex.parser	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.
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** .
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 analysant des mots-clés prédéfinis et des expressions régulières.
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.

Rubriques connexes

- Fichier de définition de feed
- Parser Flex

- Parser Geo IP
- Parsers Lua
- 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 le Guide de l'administration système NextGen.

Parser Flex

Cette rubrique présente les analyseurs Flex.

L'un des fichiers qu'il est possible de modifier dans la vue Configuration des services > onglet Fichiers est **NwFlex.xml**, l'analyseur 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**.

Topics

- Définition de langage de fonctions générales
- Définition de langue
- Définition linguistique des nœuds
- Définition de langue
- Définition de langue
- Définition de langage de 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 :
et		Effectue une opération AND au niveau du bit entre deux nombres.
	nom	Variable dans laquelle effectuer une opération AND du résultat.
	value	Nombre auquel effectuer une opération AND dans le résultat.
ou		Effectue une opération OR au niveau du bit entre deux nombres.
	nom	Variable dans laquelle effectuer une opération OR du résultat.
	value	Nombre auquel effectuer une opération OR dans le résultat.
incrément		Effectue l'ADDITION de deux nombres.
	nom	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.
	nom	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.

Node Name	Nom de l'attribut	Description :
	nom	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.
	nom	Variable contenant la valeur initiale AND pour recevoir les résultats de l'opération MODULO.
	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.
	nom	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.
	nom	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.
	nom	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 de langage de fonctions générales

Node Name	Nom de l'attribut	Description :
apptype		Obtient le type de service actuellement défini pour la session en cours.
	nom	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.
attribuer		Attribue une valeur à une variable.
	nom	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.
	nom	Variable pour recevoir la valeur de la métadonnée qui a généré le rappel.
gettoken		Renvoie le token associé actuel.
	nom	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.

Node Name	Nom de l'attribut	Description :
Fin		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.
	nom	Identifiant unique variable attribué à l'objet dans la section de **déclaration**.
	equal notequal moins lessequal greater greaterequal et ou	Valeur d'opération à comparer. Si la valeur est vraie, une sous-action est exécutée.
register		Ajoute des métadonnées à la session.
	nom	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.
	nom	Identifiant unique variable attribué à l'objet dans la section de déclaration.

Node Name	Nom de l'attribut	Description :
	equal notequal moins lessequal greater greaterequal et ou	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		Exécutez 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 :
Échec		Consigne un message dans le log système avec le niveau de log **Échec.**
	value	Chaîne à inclure en tant que message de log.
avertissement		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.

Node Name	Nom de l'attribut	Description :
	nom	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	Ce nœud fournit une description conviviale de la fonction de l'analyseur.
	service	Il s'agit d'un numéro unique attribué à la session, lorsqu'il est identifié.
declaration		Nœud qui décrit la définition. Chacune de ces définitions peut avoir une entrée **match** correspondante.
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.
	nom	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**).

Node Name	Nom de l'attribut	Description :
meta-call-back		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).
	nom	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.
	nom	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.
	nom	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.
	nom	Il s'agit d'un identifiant unique pour la déclaration.
	value	Il s'agit du numéro de port à identifier.

Node Name	Nom de l'attribut	Description :
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.
	nom	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.
	nom	Il s'agit d'un identifiant unique pour la déclaration
	value	Indique que le traitement a lieu au début ou à la fin d'un flux (**begin** ou **end**).
fonction		Définit une section **match** qui peut être utilisée en tant que fonction générique. Aucun rappel n'est associé à cette déclaration.
	nom	Il s'agit d'un identifiant unique pour la déclaration.
méta		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.

Node Name	Nom de l'attribut	Description :
	format	Spécifie le type de variante (par exemple,. **Texte, 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**
	nom	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 **l'attribut scope** 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 match : • General • 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.
	nom	Variable **numérique** 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. 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.

Node Name	Nom de l'attribut	Description :
	type	Type de décodeur à installer. Les options valides sont : gzip, deflate, chunked, chunked-gzip, chunked-deflate.
	Décalage	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.
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.
	nom	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.

Node Name	Nom de l'attribut	Description :
	nom	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.
	nom	Nom d'une variable de **chaîne** ou **numérique** permettant de recevoir des données de flux. Si une variable **numérique** 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. L'attribut n'est pas valide lors de la lecture dans une variable de chaîne.

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 :
nom	Variable **numérique** 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**.
	nom	Identifiant unique d'une variable de chaîne à laquelle la valeur spécifiée est rattachée.
	value	Chiffre ou chaîne à rattacher.
rechercher		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.
	nom	Variable sous forme de **chiffre** pour recevoir la position basée sur zéro, dans laquelle la chaîne de valeur fournie a été trouvée dans la chaîne **in**.
	value	Chaîne à trouver.
	de	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 **chiffre**.
	nom	Variable **chiffre** pour recevoir la longueur de la chaîne spécifiée.

Node Name	Nom de l'attribut	Description :
	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.
	nom	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.
	value	Expression régulière à rechercher.
	de	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.
	nom	Identifiant unique d'une variable de chaîne pour recevoir la valeur extraite.
	value	Valeur de chaîne à partir de laquelle extraire une sous-chaîne.

Node Name	Nom de l'attribut	Description :
	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.
	nom	Nom d'une variable **string** à traiter.
toupper		Convertit une chaîne en lettres en majuscules uniquement.
	nom	Nom d'une variable **string** à traiter.
urldecode		Décode une chaîne contenant des caractères codés URL.
	nom	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne d'URL chiffrée à décoder.
base64decode		Décode une chaîne codée base 64.
	nom	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne d'URL chiffrée à décoder.
uudecode		Décode une chaîne uuencode.
	nom	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.
	nom	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne codée Quoted-printable.
convert-ebcdic		Convertit une chaîne EBCDIC en son équivalent ASCII.
	nom	Variable de chaîne qui recevra la chaîne décodée.
	value	Chaîne d'URL chiffrée à décoder.

Parser Geo IP

Cette rubrique présente le parser Geo IP pour les Decoders.

L'un des fichiers modifiables dans la vue Configuration des services > onglet Fichiers est **GeoPrivate.ipl**, le parser Geo IP.

GeoPrivate.ipl

Le parser Geo IP est un parser fixe qui prend les adresses IP et les convertit en lieux géographiques. Les emplacements s'affichent via Google Earth.

Les métadonnées de géolocalisation figurant 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

Cette rubrique présente les 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 SecurCare Online (SCOL) 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

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 Syntaxe.

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>|Pat-
tern=<expression>Case=0|1
Proximity=<number_of_bytes>Recon=0|1
Raw=0|1
```

Parameters

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\ Inves-
tigations\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)
- Radiota1p avec en-tête 802.11
- Absolute Value Systems (AVS) avec en-tête 802.11
- Prism II avec en-tête 802.11
- Per Packet Information (PPI) de CACE 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.

Vous trouverez une présentation complète de ce fichier de configuration dans le chapitre sur la capture des paquets sans fil figurant dans le Guide de l'administration système NextGen.

Vue Configuration des services - onglet Général

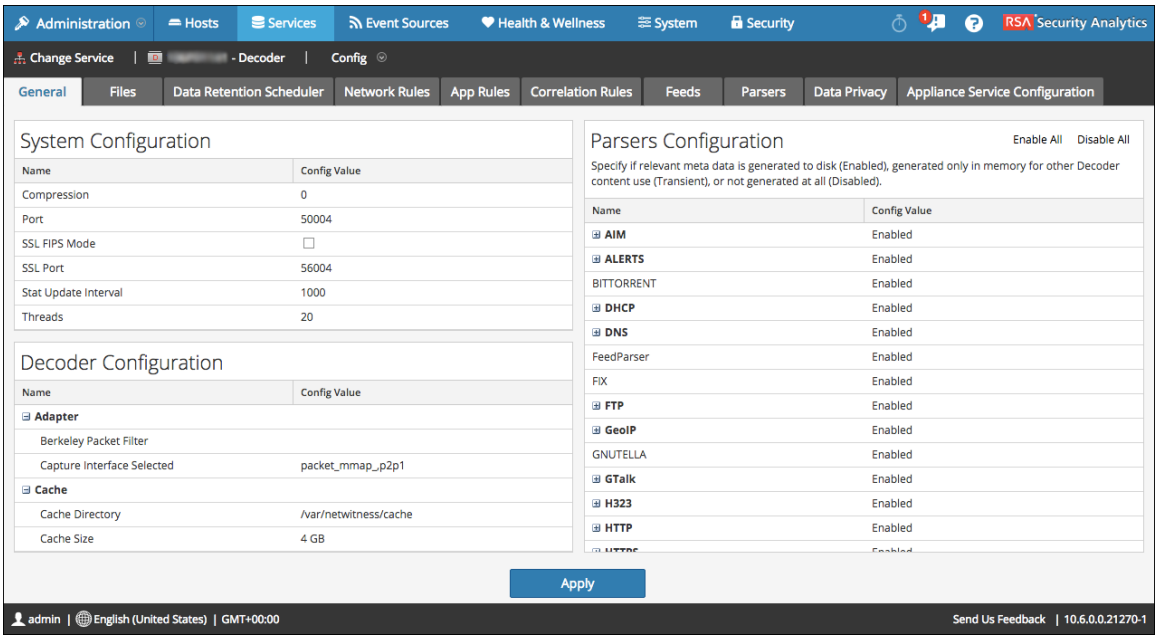
Cette rubrique présente les fonctions de la vue Configuration des services > onglet Général pour les Decoders et Log Decoders.

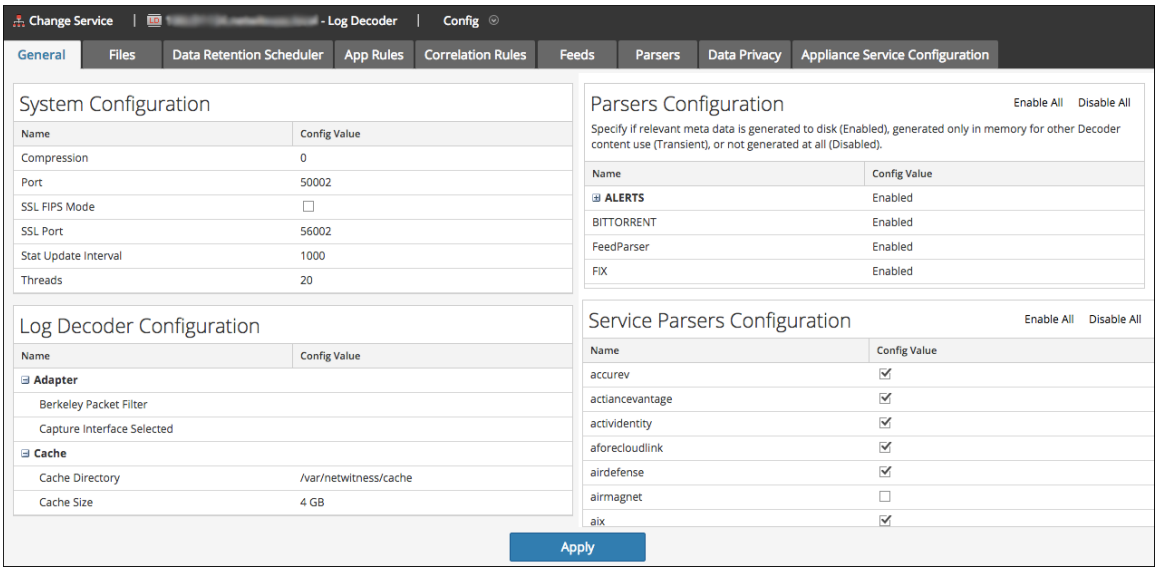
L'onglet Général de Decoder dans la vue Configuration des services vous permet de gérer la configuration de base des services, de configurer la capture des données et de sélectionner les parsers appliqués aux données capturées.

Les paramètres de configuration et d'ajustement de la capture des données sont les suivants :

- sélection d'adaptateur ;
- spécification du cache ;
- démarrage automatique et autres paramètres de capture affectant le cache, les sessions et les expirations du délai ;
- tailles des fichiers de base de données ;
- emplacement du répertoire de hachage.

La première figure est un exemple d'onglet Général pour un Decoder. La seconde est un exemple d'onglet Général pour un Log Decoder.





Fonctions

Voici les quatre sections principales de l'onglet Général pour les Decoders et les Log Decoders :

- Configuration système
- Configuration des Decoder
- Configuration des analyseurs
- Configuration des analyseurs de servicess (Log Decoders uniquement)

Configuration système

La section Configuration système gère la configuration de service d'un Decoder. Lorsqu'un service est ajouté pour la première fois, les valeurs par défaut s'appliquent. Vous pouvez modifier ces valeurs pour optimiser les performances.

System Configuration

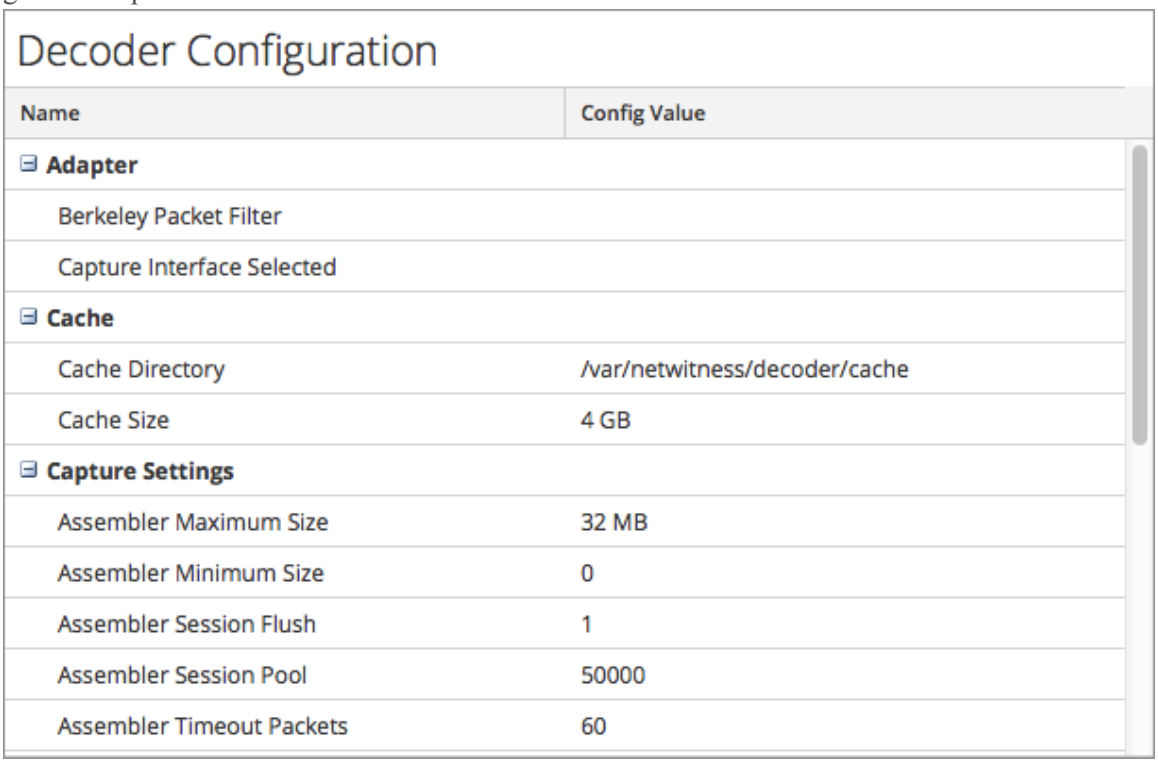
Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	☐
SSL Port	56004
Stat Update Interval	1000
Threads	20

La Configuration système dispose des paramètres suivants.

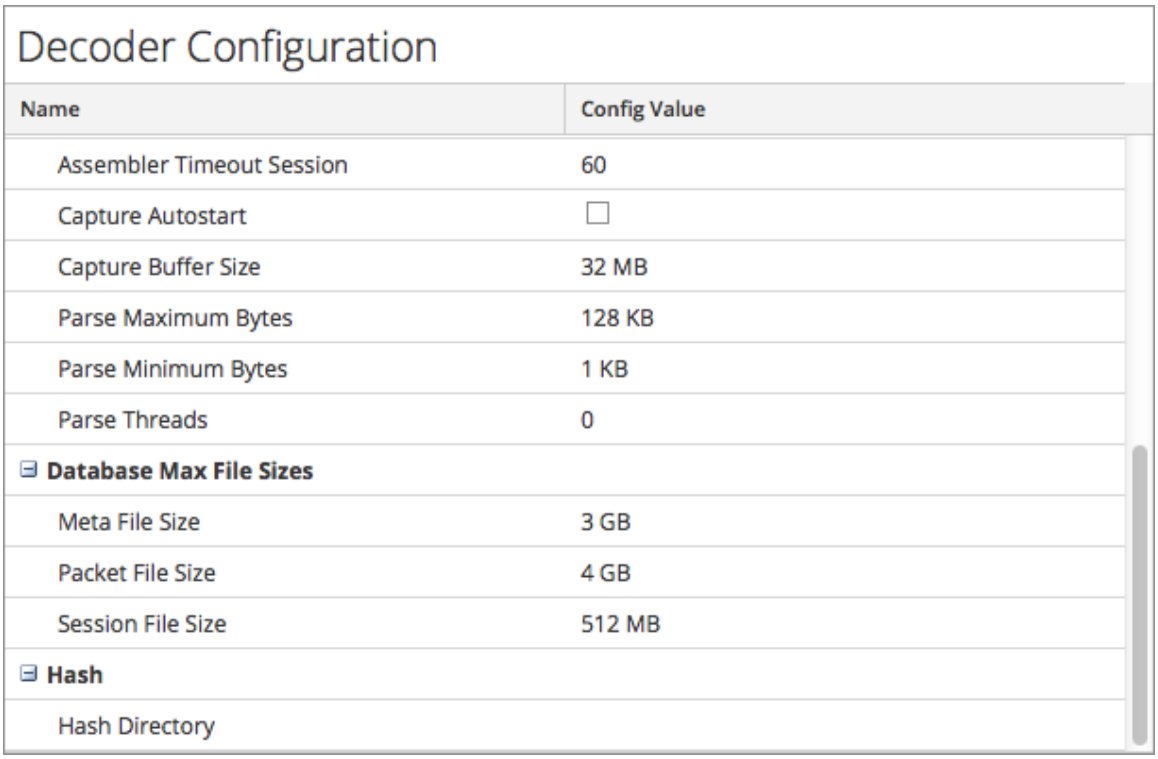
Paramètre	Description :
Compression	Le nombre minimum d'octets devant être transmis par réponse avant la compression. Le paramètre 0 désactive la compression. La valeur par défaut est **0**. La modification d'une valeur prend effet immédiatement pour toutes les connexions suivantes.
Port	Détermine le 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 **1 000**. 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.

Configuration des Decoder

La section Configuration des Decoder 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.



Adaptateur

Les paramètres d'adaptateur vous permettent de configurer l'interface réseau de la capture. Le tableau ci-dessous décrit les paramètres d'adaptateur Decoder. Les adaptateurs réseau par défaut sont définis lors de l'installation. 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)

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/man-page/FreeBSD/7/pcap-filter/).

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.

Paramètre du cache	Description :
Répertoire cache	Répertoire où sont stockés les fichiers du cache de session. La valeur par défaut est **/var/netwitness/decoder/cache**. La modification prend effet immédiatement.
Cache Size	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.

Paramètres de capture

La section Paramètres de capture vous permet de configurer les paramètres de capture opérationnels.

Remarque : Par défaut, aucune règle n'est définie lors de la première installation de Security Analytics. À moins que des règles ne soient spécifiées, les paquets ne sont pas filtrés. Vous pouvez définir des règles de capture avant de commencer à capturer les données (voir Configurer des règles réseau, Configurer des règles d'application et Configurer des règles de corrélation).

Ce tableau décrit les paramètres de capture.

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.

Paramètres de capture	Description :
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.

Paramètres de capture	Description :
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.
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.

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. Le tableau suivant décrit les paramètres.

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.

Hachage

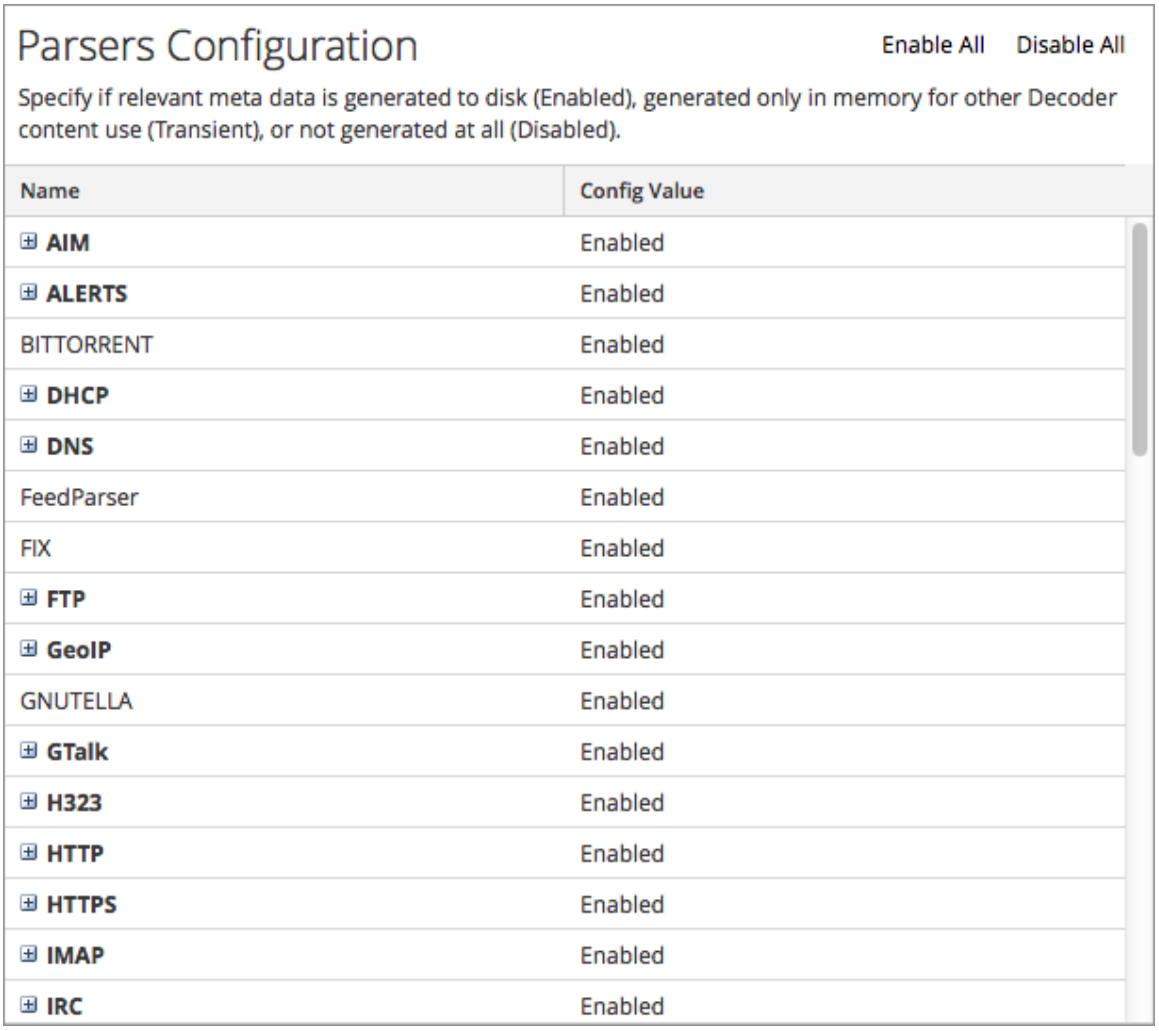
Contrôle les options de hachage des fichiers de base de données. Il y a une petite pénalité de performance lors du hachage. Le tableau suivant décrit les options de hachage.

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.

Configuration des analyseurs

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.

Security Analytics offre la possibilité de configurer des parsers individuels qui ne stockent pas les métadonnées générées sur disque (option Transitoire). Cela permet aux administrateurs de protéger certaines données. Elle est généralement mise en œuvre dans le cadre d'un plan de confidentialité des données (reportez-vous à *Gestion de la confidentialité des données*).



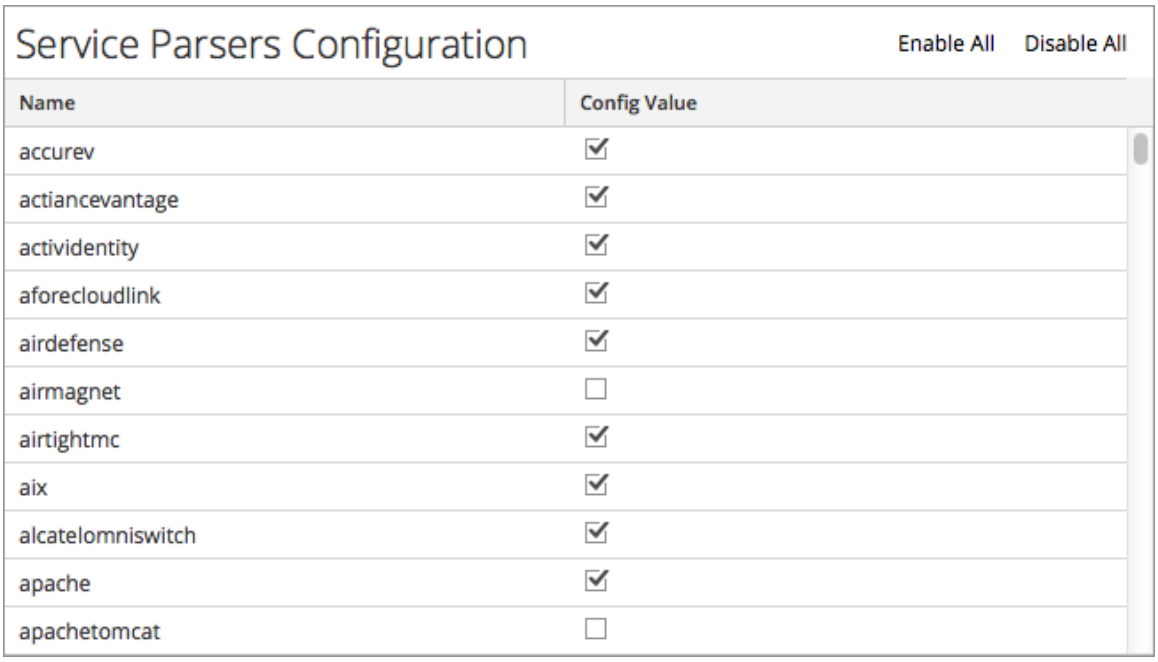
Le tableau suivant décrit les fonctions de la section Configuration des analyseurs.

Fonctionnalité	Description :
Activer toutes **Désactiver toutes**	Ces options donnent la possibilité de sélectionner rapidement la totalité des parsers ou aucun d'entre eux.

Fonctionnalité	Description :
Name	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. Dans l'exemple ci-dessus, CMS_windows_executable a trois métadonnées sélectionnables que le parser peut créer : alert.id, error et filetype.
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. • Lorsque l'option est **Désactivé**, 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.

Configuration de parsers de services supplémentaires pour Log Decoder

La section Configuration des analyseurs de services vous permet de sélectionner les parsers de services à utiliser dans Log Decoder.


Service Parsers Configuration
Enable All
Disable All
Name
Config Value
accurev
actiancevantage
actividentity
aforecloudlink
airdefense
airmagnet
airtightmc
aix
alcatelomniswitch
apache
apachetomcat

Vue Configuration des services - Onglet Mappages des parsers

Cette rubrique propose une description des options configurables pour un Log Decoder sous l'onglet Mappage d'analyseurs.

Sous l'onglet Mappage d'analyseurs, les administrateurs peuvent configurer des mappages d'analyseurs de log pour les services Log Decoder. 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. L'onglet Mappages d'analyseurs doit être activé pour que vous puissiez le visualiser dans la vue Configuration des services.

Les procédures associées à l'onglet Mappages d'analyseurs sont fournies dans Mappages d'analyseur d'accès.

Pour accéder à cet onglet :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis  **>Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Mappages d'analyseurs**.

Voici un exemple de l'onglet.

Fonctions

La grille Parser répertorie tous les analyseurs actuellement mappés sur le Log Decoder. La barre d'outils de l'onglet Parser comporte des options permettant d'utiliser les mappages d'analyseurs dans la grille.

Barre d'outils Mappages d'analyseurs

La barre d'outils de l'onglet Mappages d'analyseurs comporte des options permettant d'utiliser les mappages d'analyseurs 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.

Fonctionnalité	Description :
	Affiche le Menu Actions. • **Importer** - Importe un mappage d'analyseur vers un fichier. • **Exporter** - Exporte un mappage d'analyseur vers un fichier.

Grille Mappages d'analyseurs

La grille Mappages d'analyseurs 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.

Vue Configuration des services - onglet Parsers

Cette rubrique présente les fonctions de la vue Configuration des services > onglet Analyseurs.

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. 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. Reportez-vous à Configurer les feeds et les parsers pour obtenir une présentation générale de l'utilisation des parsers sur les Decoders.

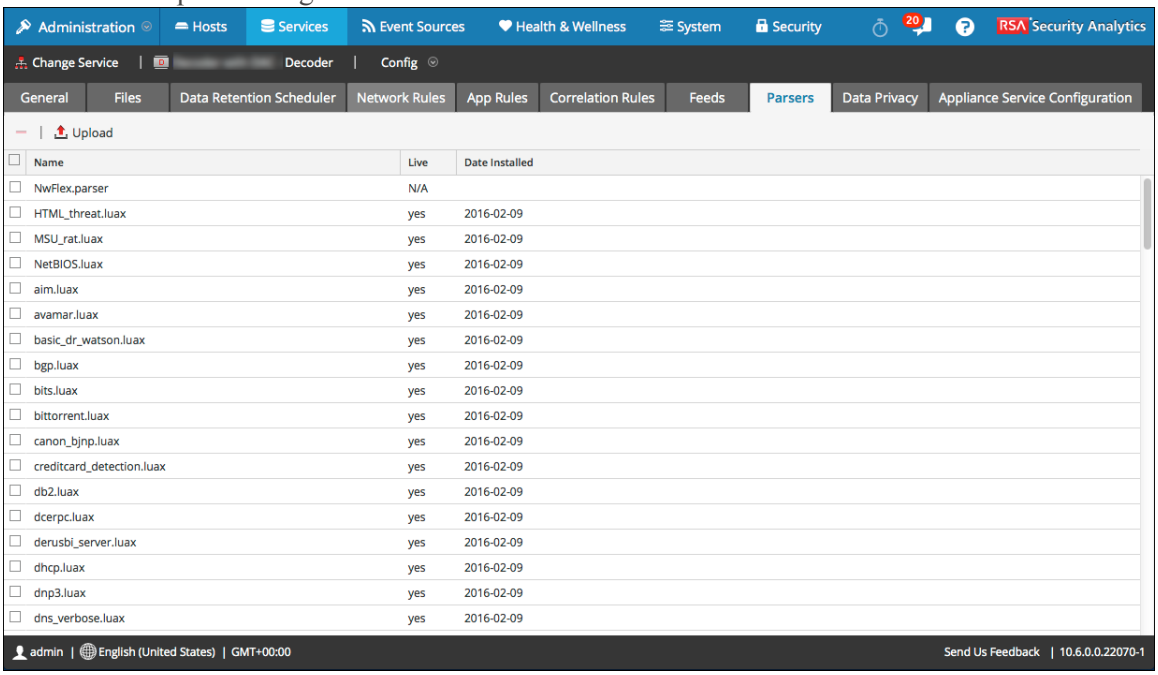
Remarque : Sauf indication contraire, toutes les références aux Decoders s'appliquent également aux Log Decoders.

Vous pouvez accéder à cette vue de la manière suivante :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis **>Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Parsers**

Voici un exemple de l'onglet Parsers.



Fonctions

La grille Parser répertorie tous les parsers actuellement déployés sur le Decoder. La barre d'outils de l'onglet Parsers comporte des options permettant d'utiliser les parsers dans la grille.

Barre d'outils de l'onglet Parsers

Voici un exemple de la barre d'outils.

Fonctionnalité	Description :
Upload	Vous permet de télécharger des parsers vers un Decoder ou Log Decoder
	Vous invite à confirmer la suppression des parsers sélectionnés. Vous pouvez sélectionner **Non** pour annuler la suppression ou **Oui** pour supprimer les parsers sélectionnés.

Grille Parser

La grille Parser répertorie tous les parsers actuellement déployés sur le Decoder.

Colonne	Description :
Name	Nom du parser ou fichier de parser.
Live	Indique si le parser provient de Live. Les valeurs possibles sont **Oui**, **Non** ou **N/A**. • **Oui** = Installé via Live • **Non** = Installé via Security Analytics • **N/A** = Le parser n'a pas de fichier d'attribut créé par Security Analytics pour effectuer le suivi de la date d'installation. Il se peut que le parser ait été installé manuellement et non via Security Analytics ou Live. Les feeds installés manuellement fonctionnent encore correctement.
Date d'installation	Date à laquelle le parser a été transmis au service.

Vue Configuration des services - onglets Règles

Les onglets Règles de la vue Configuration des services 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 paquets.

Étape 4. Configurer les règles de Decoder fournit des informations supplémentaires.

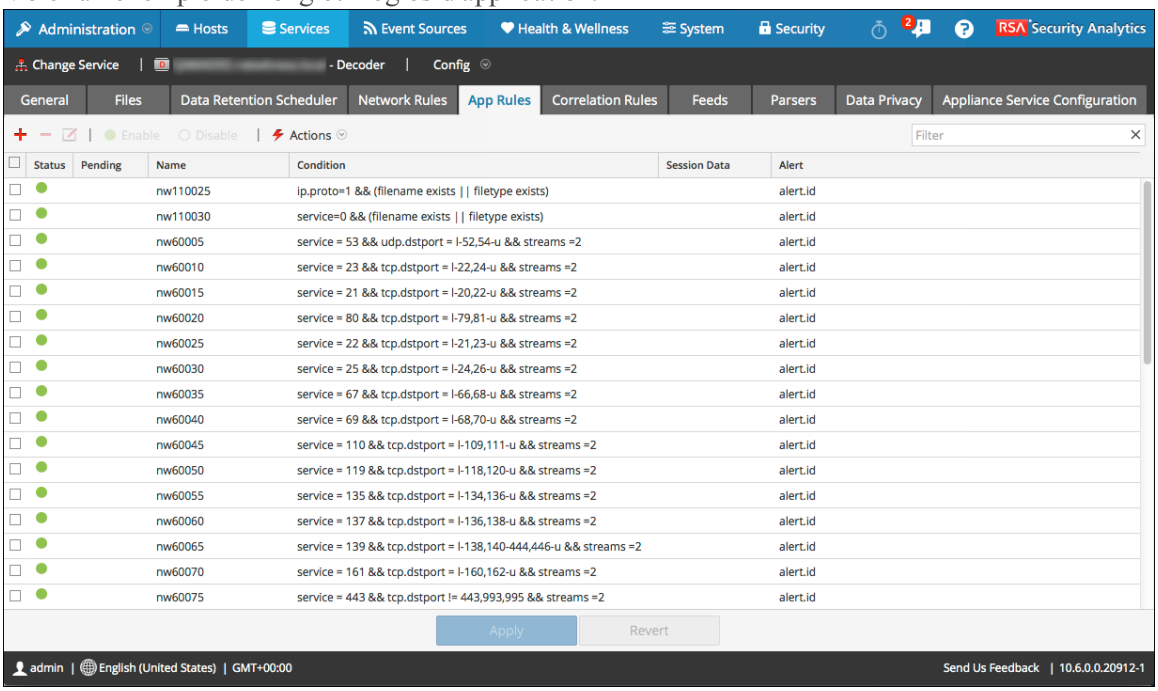
Vous pouvez afficher cette vue de la manière suivante :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis **>Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'un des onglets des règles : **Règles réseau**, **Règles d'application** ou **Règles de corrélation**.

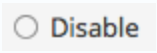
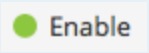
   L'onglet des règles sélectionné s'affiche.

Voici un exemple de l'onglet Règles d'application.



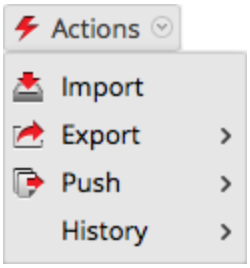
Barre d'outils onglet Règles

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.
	Désactive une règle (sans la supprimer).
	Active (réactive) une règle.
Filtre	Champ de saisie pour la chaîne de recherche. Security Analytics filtre les règles de façon dynamique au fur et à mesure que vous saisissez 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.

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.

History	Affiche les dix derniers instantanés de règles appliqués dans Security Analytics. Vous pouvez sélectionner et appliquer (restaurer) un instantané dans le Decoder à tout moment.

Actions de contexte de grille 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.

Topics

- Onglet Règles d'application
- Onglet Règles de corrélation
- Onglet Règles réseau
- Instructions relatives aux règles et requêtes

Onglet Règles d'application

Cette rubrique décrit les fonctionnalités permettant de créer et de gérer les règles d'application dans la vue Configuration des services > onglet Règles d'application.

L'onglet Règles d'application vous permet de gérer les règles d'application. Security Analytics applique des règles d'application au niveau de la session.

Étape 4. Configurer les règles de Decoder fournit des informations supplémentaires et Configurer des règles d'application fournit des instructions pour la création de règles d'application.

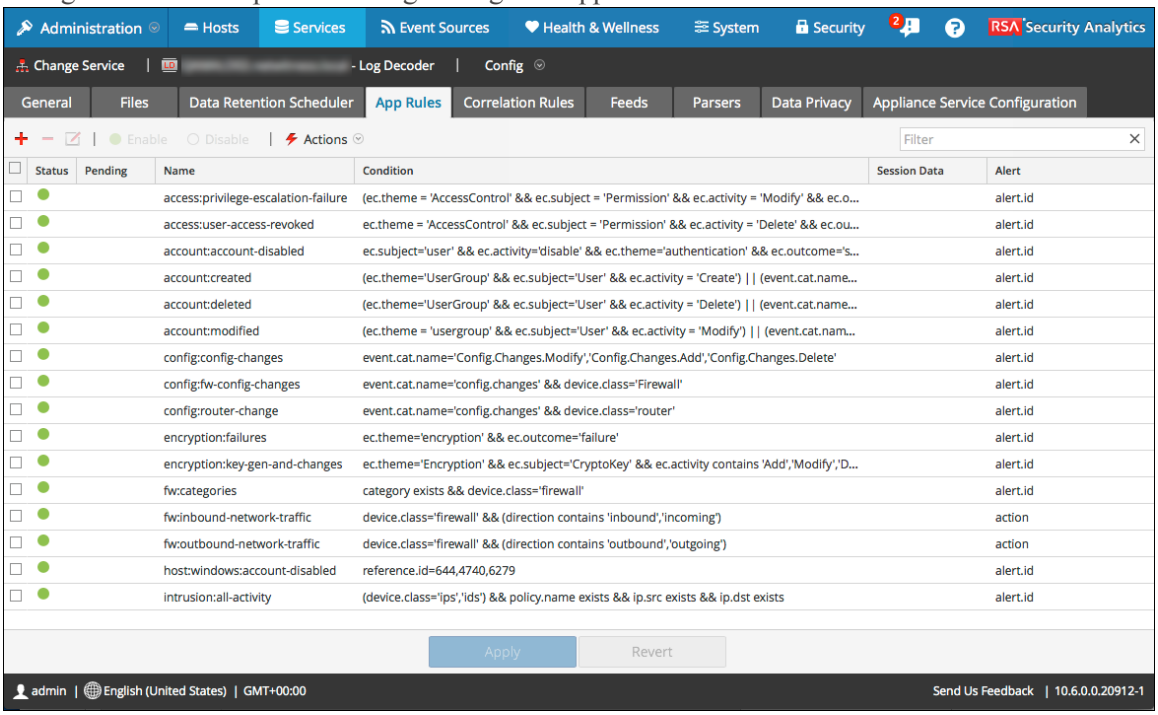
La barre d'outils de l'onglet Règles d'application est commune à toutes les règles. Vue Configuration des services - onglets Règles fournit des informations sur la barre d'outils et les actions courantes.

Pour accéder à l'onglet Règles d'application :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service Decoder ou Log Decoder, puis **>Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Règles d'application**.

La figure ci-dessous présente l'onglet Règles d'application.

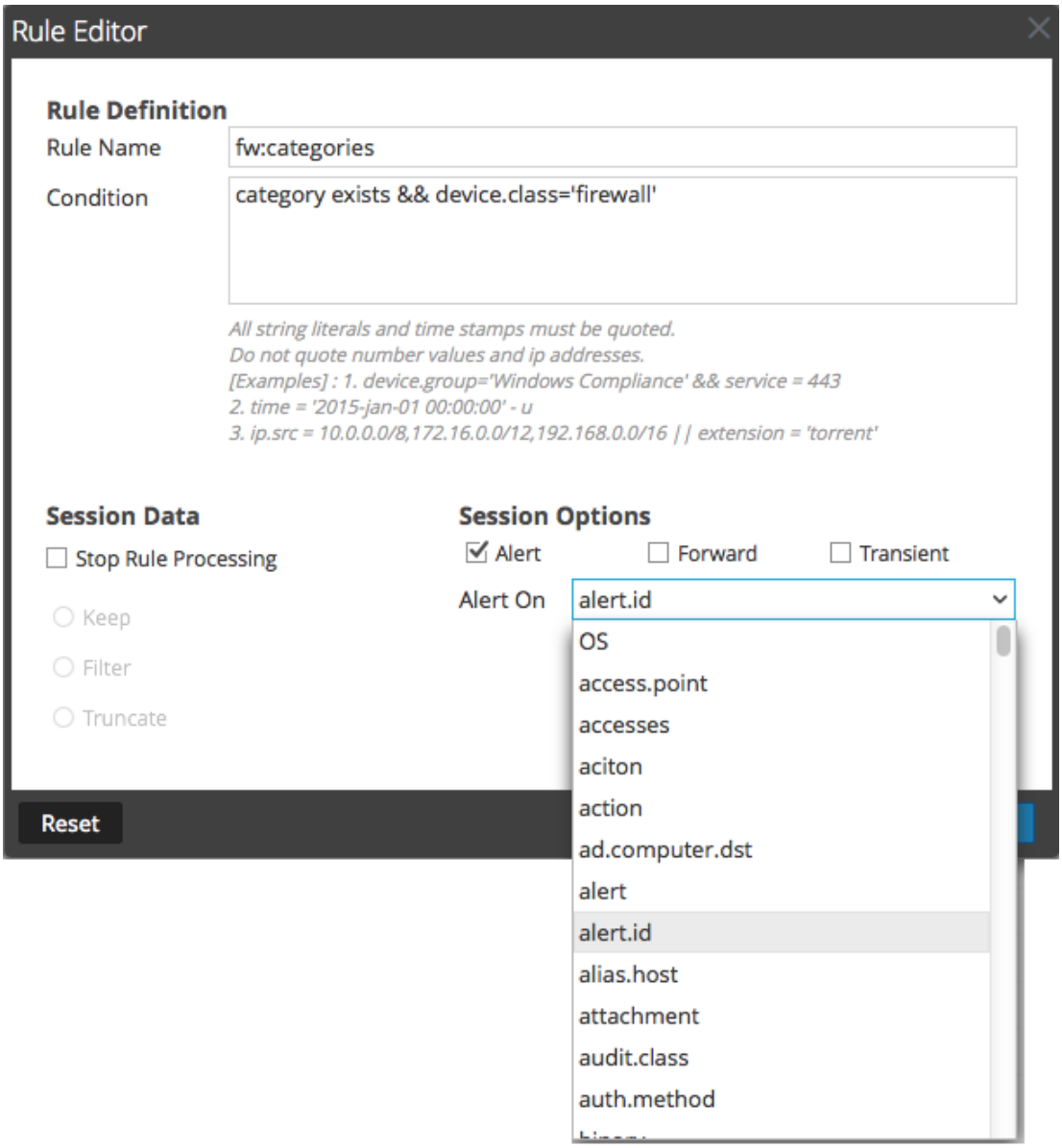


Colonnes de l'onglet Règles d'application

Colonne	Description :
Pending	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.
Donnéesde 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 ni les adresses IP entre guillemets. Instructions relatives aux règles et requêtes 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.
Filtre	Le paquet n'est pas enregistré lorsqu'il correspond à la règle.
Truncate	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.
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. Voir Corriger les règles dont la syntaxe est obsolète.

Onglet Règles de corrélation

Cette rubrique décrit les fonctionnalités permettant de créer et de gérer les règles de corrélation dans la vue Configuration des services > onglet Règles de corrélation.

L'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. Security Analytics applique les règles de corrélation sur une période glissante configurable.

Étape 4. Configurer les règles de Decoder fournit des informations supplémentaires et Configurer des règles de corrélation fournit des instructions pour la création de règles de corrélation.

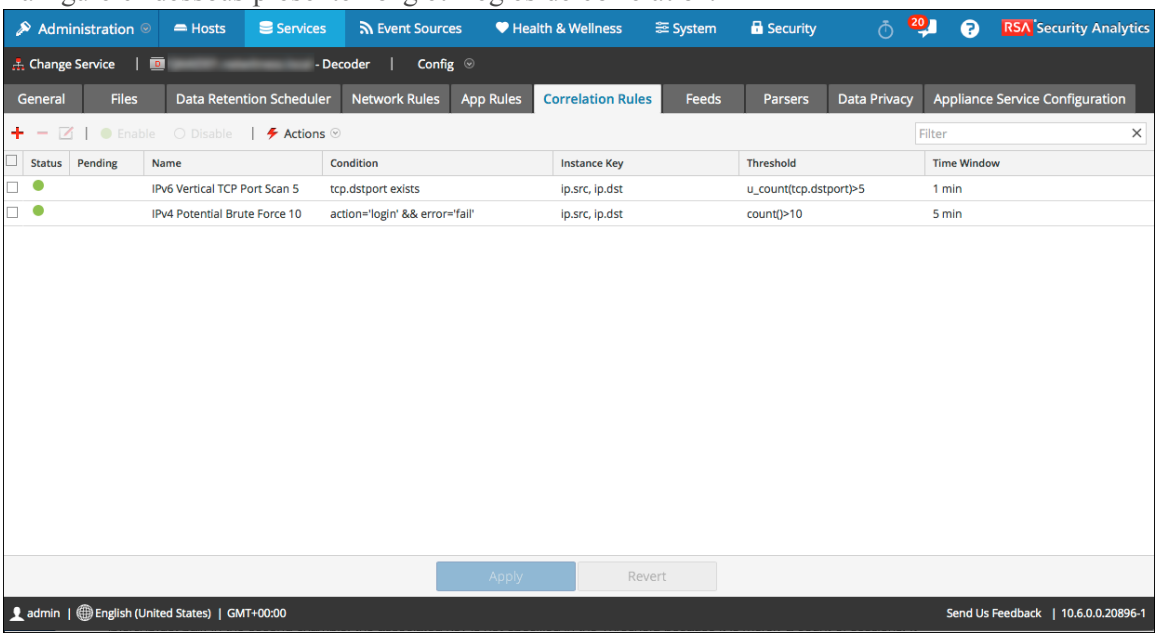
La barre d'outils de l'onglet Règles de corrélation est commune à toutes les règles. Vue Configuration des services - onglets Règles fournit des informations sur la barre d'outils et les actions courantes.

Pour accéder à l'onglet Règles de corrélation :

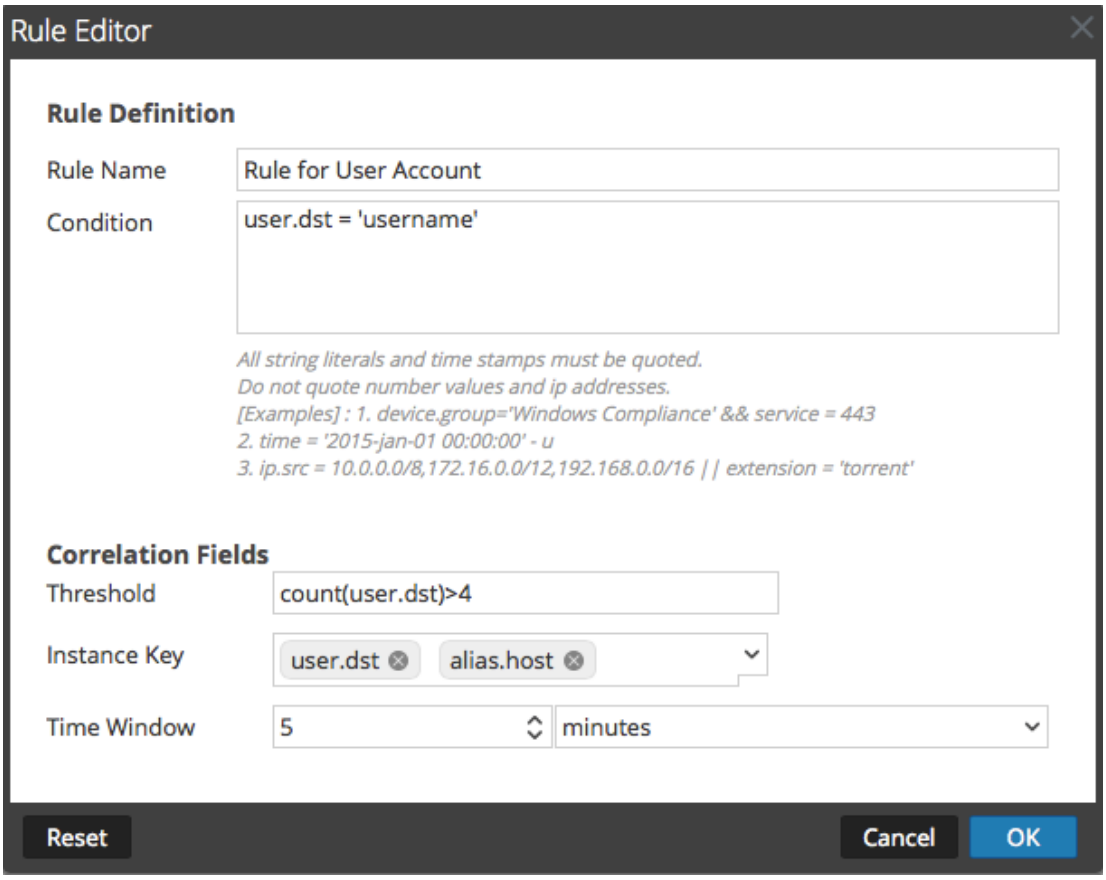
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis **>Vue > Config**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Cliquez sur l'onglet **Règles de corrélation**.

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 :
Pending	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 descriptif de la règle.

Colonne	Description :
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 ni les adresses IP entre guillemets. Instructions relatives aux règles et requêtes 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.
Threshold	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. Voir Corriger les règles dont la syntaxe est obsolète.

Onglet Règles réseau

Cette rubrique décrit les fonctions permettant de créer et de gérer des règles réseau dans la vue Configuration des services > onglet Règles réseau.

L'onglet Règles réseau vous permet de gérer des règles réseau. Security Analytics 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 Decoders de paquets.

Étape 4. Configurer les règles de Decoder fournit des informations supplémentaires et Configurer des règles réseau fournit des instructions pour la création de règles réseau.

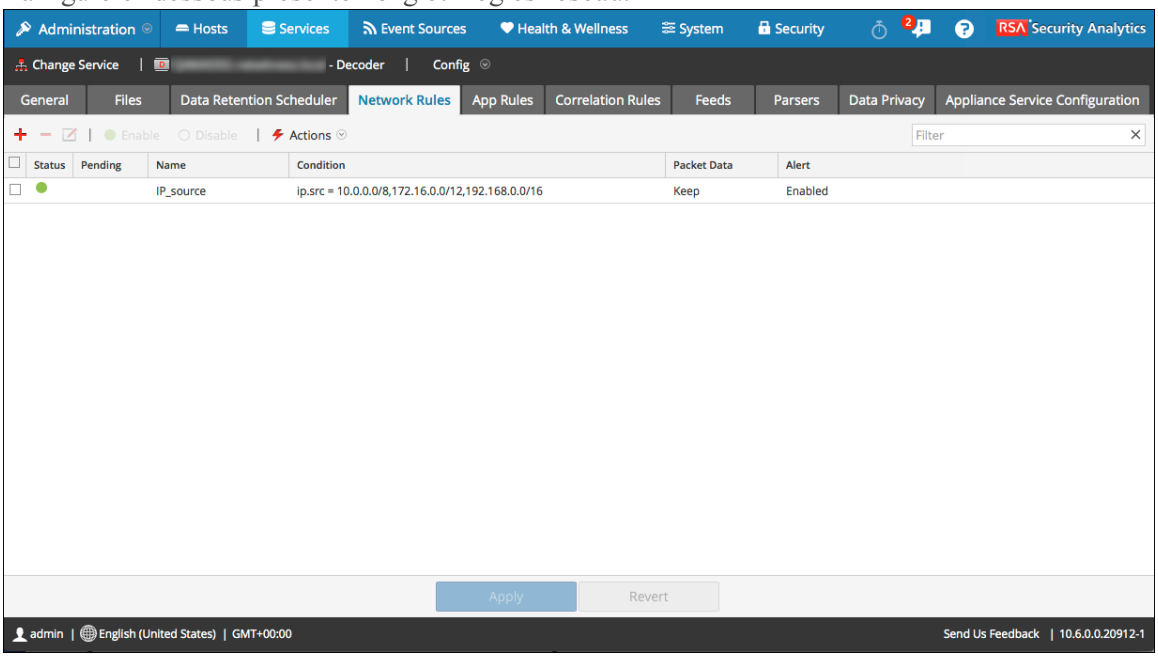
La barre d'outils de l'onglet Règles réseau est commune à tous les types de règles. Vue Configuration des services - onglets Règles fournit des informations sur la barre d'outils et les actions courantes.

Pour accéder à l'onglet Règles réseau :

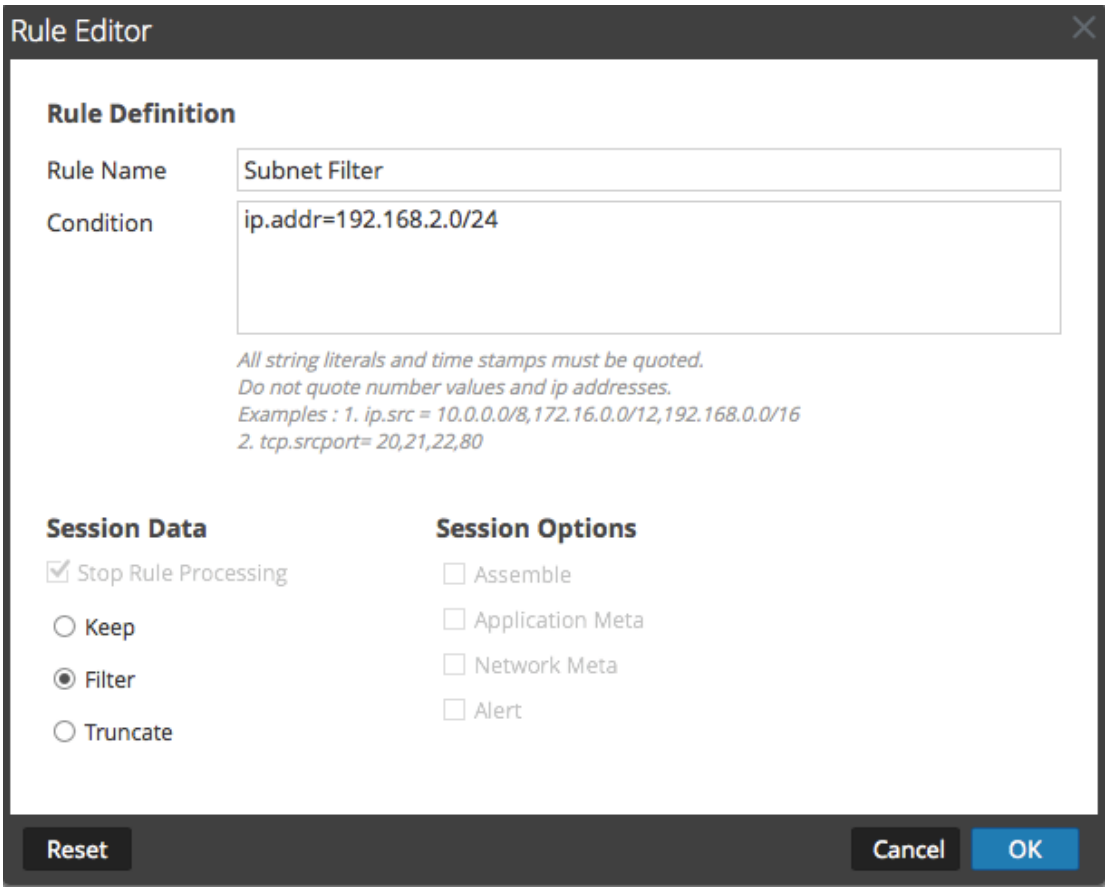
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service Decoder et sélectionnez  **> Vue > Configuration**.

   La vue Configuration pour le service sélectionné s'affiche.
3. Sélectionnez l'**onglet Règles réseau**.

La figure ci-dessous présente l'onglet Règles réseau.



La figure suivante affiche la boîte de dialogue Éditeur de règles pour une règle réseau.



Fonctions

Le tableau suivant décrit les colonnes de la grille Règles réseau.

Colonne	Description :
Pending	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 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**.

Colonne	Description :
Alert	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 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. Dans les conditions, tous les horodatages et valeurs littérales de la chaîne doivent être entre guillemets. Ne mettez pas les valeurs de nombre ni les adresses IP entre guillemets. Instructions relatives aux règles et requêtes fournit des informations supplémentaires. Clés méta prises en charge dans les conditions de règles réseau décrit les clés méta dont Security Analytics prend en charge l'utilisation 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.
Conserver	La charge du paquet et les métadonnées associées sont enregistrées lorsqu'elles correspondent à la règle.
Filtre	Le paquet n'est pas enregistré lorsqu'il correspond à la règle.
Truncate	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.

Option	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.
Alert	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.

Action	Description :
Enregistrer	(Règles avec une syntaxe obsolète uniquement) Applique une règle corrigée de manière individuelle au service Decoder. Voir Corriger les règles dont la syntaxe est obsolète.

Clés méta prises en charge dans les règles réseau

Les règles réseau comprennent les groupes de règles de la couche 2, de la couche 3 et de la couche 4. Vous pouvez appliquer plusieurs règles au niveau des paquets à un Decoder. Les règles peuvent être appliquées à plusieurs couches (par exemple, lorsqu'une règle réseau filtre des ports spécifiques pour une adresse IP spécifique). 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 Security Analytics 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.

Clé méta	Description :
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 de l'adresse entier 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
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.

Instructions relatives aux règles et requêtes

Toutes les requêtes et les conditions de règle définies dans les services de base de RSA Security Analytics doivent suivre 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.

Par exemple :

- `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 utiliser `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 des logs dans un service Archiver et pour les règles d'application, de réseau et de corrélation appliquées à un Decoder, Log Decoder ou Concentrator. Les conditions de règle sont également utilisées dans toutes les clauses `Where` de toutes les requêtes de la base de données principale.

Pour plus d'informations sur la syntaxe de règle dans Security Analytics, reportez-vous à la section **Clauses Where** de la rubrique **Requêtes** dans le *Guide d'optimisation de la base de données principale de RSA Security Analytics*.

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'

Configuration du mode strict pour Security Analytics 10.6

Depuis la version 10.2, Security Analytics utilise un analyseur moderne pour les règles et les requêtes qui définit de manière stricte la syntaxe valide. Lorsqu'un service de base rencontre une syntaxe obsolète, un message d'avertissement à ce propos est consigné dans les logs de Security Analytics. Security Analytics applique désormais une analyse stricte pour les nouvelles règles d'application, de réseau et de corrélation. L'analyseur hérité de la génération précédente, désormais obsolète, autorise l'utilisation d'une syntaxe ambiguë, ce qui peut entraîner des résultats inattendus. Security Analytics 10.6 continue de prendre en charge la syntaxe obsolète, mais les versions futures ne la prendont plus en charge.

Une fois la mise à jour vers Security Analytics 10.6 effectuée, les règles de syntaxe obsolètes sont mises en surbrillance dans l'interface utilisateur. L'éditeur de règles fournit des infobulles supplémentaires. Une fois les règles corrigées, les mises en surbrillance disparaissent. Reportez-vous à la rubrique **Corriger les règles contenant une syntaxe obsolète** dans le *Guide de configuration de Decoder et Log Decoder*.

Les statistiques **/decoder/config/rules/rule.errors** et **/concentrator/config/rules/rule.errors**, introduites dans la version 10.6, indiquent le nombre de règles erronées. Si **rule.errors** est différent de zéro, Security Analytics génère une alerte d'intégrité pour indiquer que vous devez corriger les règles.

De plus, un chemin de migration est disponible pour les requêtes issues de systèmes externes. Après une mise à jour à partir d'une version antérieure, le système fonctionne en mode obsolète (contrôlé par **/sdk/config/query.parse**). En mode obsolète, le service continue à utiliser l'analyseur hérité pour toutes les requêtes qui échoue lors de l'analyse stricte. Les erreurs sont consignées et un message est renvoyé au client pour l'informer de l'échec de l'analyse stricte. Cependant, la requête s'exécute et renvoie les résultats comme pour les versions précédentes. Vous devez surveiller les logs et les clients externes afin d'identifier les rapports, les tableaux de bord, les règles..., qui sont écrits dans la syntaxe obsolète afin de corriger les erreurs potentielles.

Une fois les problèmes résolus, vous pouvez passer tous les services de base (Decoder, Log Decoder, Concentrator, Broker et Archiver) en mode strict afin de surveiller le moindre problème. Le mode strict n'utilise pas l'analyseur hérité et les violations d'analyse renvoient des erreurs. Vous devez effectuer cette tâche avant toute mise à niveau majeure ultérieure à la version 10.6, étant donné que l'analyseur hérité sera supprimé des prochaines versions, et il qu'il n'y aura plus aucune option de fonctionnement en mode obsolète.

Par défaut, toutes les nouvelles installations fonctionnent en mode strict. Si vous prévoyez d'ajouter une nouvelle appliance à l'infrastructure existante en cours d'exécution en mode obsolète, dans la vue Explorer (Administration > Services > Sélectionner un service, puis dans le menu Actions, sélectionnez Afficher > Explorer), vous pouvez basculer **/sdk/config/query.parse** en mode obsolète jusqu'à ce que l'ensemble de la pile soit passé en mode strict.

Dans Security Analytics 10.6, la validation des règles s'appliquera toujours en mode strict, afin d'éviter de créer des problèmes de syntaxe.

Syntaxe valide avec analyseur moderne

Voici les règles de syntaxe valides en utilisant l'analyseur moderne :

- Tous les types de texte doivent utiliser les valeurs littérales entre guillemets. Exemple : `username = 'user1'`
- Les guillemets peuvent être simples ou doubles, mais ils doivent être identiques (vous ne pouvez pas commencer avec un guillemet simple et finir avec des guillemets doubles)
- Si la valeur littérale comporte des guillemets, vous pouvez leur insérer un caractère d'échappement ou utiliser d'autres guillemets ouvrants. Les deux exemples ci-dessous sont valides (utilisez la barre oblique inverse en guise de caractère d'échappement):
  - `username = "User’s"`
  - `username = 'User\'s'`
- Pour utiliser une barre oblique inverse dans une chaîne littérale, insérez une autre barre oblique inverse en guise de caractère d'échappement. `\\`
- Tous les types d'heures doivent utiliser des guillemets pour les dates au format suivant : `time = 'YYYY-MM-DD HH:MM:SS'`
- Tous les types d'heures exprimées en nombres de secondes depuis l'outil EPOCH (Jan 1, 1970), ne doivent pas être mis entre guillemets.
  Exemple : `time = 1448034064`
- TOUT LE RESTE ne doit pas être mis entre guillemets : Adresse IP, adresses Ethernet, chiffres, etc.
  Exemple : `service = 80 && ip.src = 192.168.1.1/16`

Exemples de syntaxe ambiguë en utilisant l'analyseur hérité

Voici un exemple de syntaxe ambiguë avec l'analyseur hérité obsolète :

select * where alias.host = server-xeon

Dans la requête ci-dessus, il semble évident que l'auteur de la requête souhaite renvoyer tous les méta dans lesquels alias.host est égal à `server-xeon`. Malheureusement, cela ne se produit pas avec l'analyseur hérité. Celui-ci analyse cette requête sous la forme `select * where alias.host = 'server'-'xeon'`. Il la convertit donc en une requête de plage (valeurs BETWEEN server et xeon, en utilisant l'opérateur dash -), et étant donné que cette plage renverra probablement des résultats incohérents avec `server-xeon`, les utilisateurs supposeront que le moteur de requêtes ne présente aucun problème. En mode strict 10.6, vous obtiendrez l'erreur suivante :

expecting <quoted_string> here: "server-xeon"

Ceci indique immédiatement à l'utilisateur la raison pour laquelle la requête d'analyse a échoué.

Voici un autre exemple de syntaxe ambiguë avec l'analyseur hérité obsolète :

```
select * where username=lastname,firstname
```

En langage Security Analytics, vous pouvez spécifier plusieurs valeurs en les séparant par des virgules (opérateur OR implicite). L'auteur de la requête voulait-il signifier `'lastname,firstname'` ou recherchait-il deux valeurs, `'lastname'` et `'firstname'` ? Là encore, la syntaxe est ambiguë, mais acceptée par l'analyseur hérité (qui l'interprète comme `'lastname' OR 'firstname'`). Avec l'analyseur moderne, vous devez être totalement clair (e) dans vos intentions, soit `'lastname,firstname'` ou `'lastname','firstname'`.

Dans l'exemple suivant, l'analyse ne s'effectue pas correctement :

```
select * where username = lastname, firstname
```

À première vue, vous pouvez ne pas remarquer qu'il y a un espace entre la virgule et le prénom. En l'absence de guillemets, l'analyse ne s'effectue pas correctement avec l'analyseur hérité et aucun message d'erreur ne s'affiche pour indiquer que l'analyse a échoué. Au lieu de cela, l'analyse s'exécute (en ignorant complètement le prénom du fait de l'espace existant). Le pire est que rien ne vous indique que la requête exécutée ne correspond pas à ce que vous avez soumis, sauf si vous parvenez à déterminer d'une certaine manière que le jeu de résultats est incomplet. Avec l'analyse stricte activée, une erreur d'analyse est renvoyée, chose qui doit toujours se produire. Au moins dans les versions antérieures (et le mode obsolète), les logs affichent immédiatement un message après le log d'audit pour la requête : **Rule '<rule name>' in deprecated format. Please make sure all text values are surrounded with quotes.**

Vue Système de services - Decoders

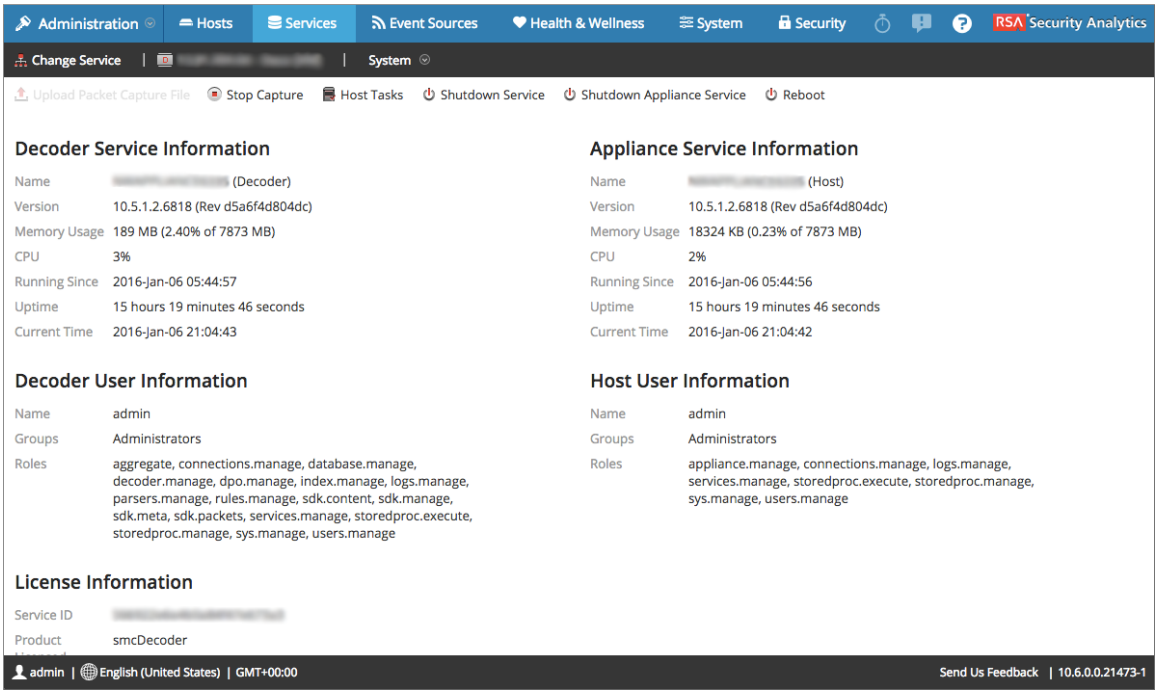
Cette rubrique présente les fonctions de la vue Système qui appartiennent spécifiquement aux Decoders et Log Decoders.

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.

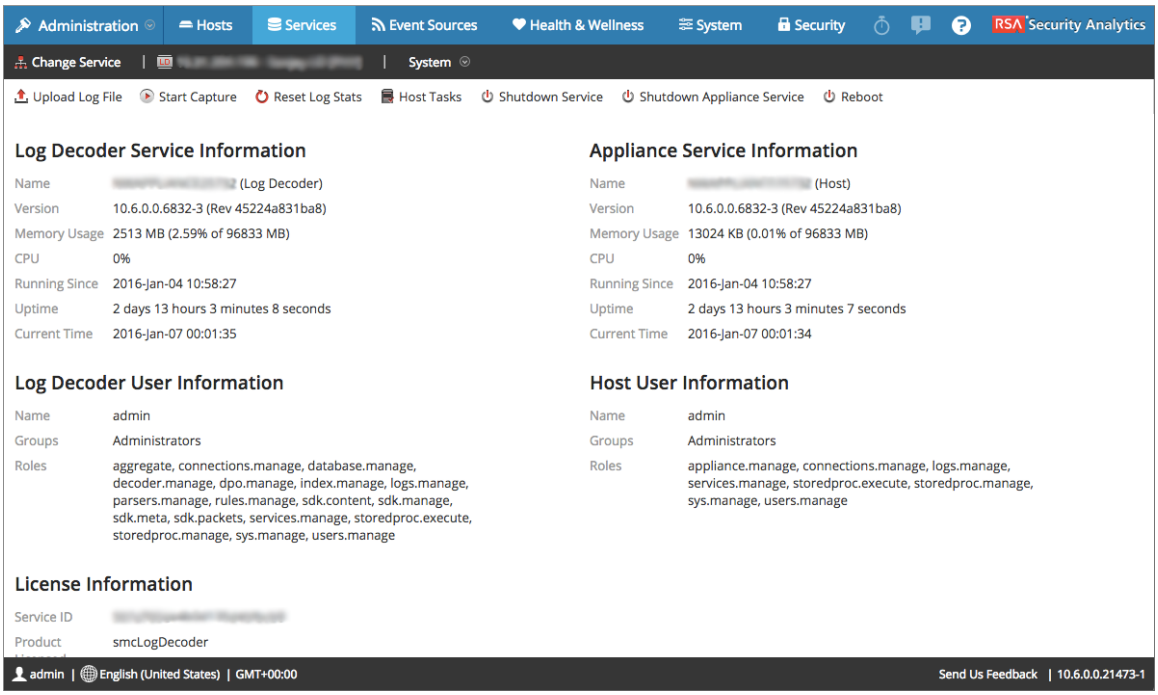
Pour accéder à la vue Système de services pour un Decoder :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services Administration s'affiche.
2. Sélectionnez un Decoder ou un Log Decoder, puis  **> Vue>Système**.

Exemple de vue Configuration des services pour un Decoder.



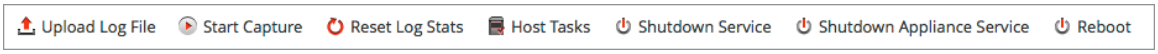
Exemple de vue Système de services pour un Log Decoder.



Fonctions

Barre d'outilsInfo 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 Télécharger le fichier de capture de paquets. **Remarque :** Cette option ne s'applique pas aux Log Decoders.

Action	Description :
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 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.

Rubriques connexes

- **Vue Système de services** dans le *Guide de mise en route des hôtes et des services*