RSA NETWITNESS® SUITE

Guide de gestion des services Live

pour la version 11.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

février 2018

Sommaire

Gestion des services Live

RSA NetWitness Suite Live constitue la passerelle à un environnement riche offrant un accès aux feeds, outils et autres ressources.

NetWitness Suite Live

Live est le composant de NetWitness Suite qui gère la communication et la synchronisation entre les services NetWitness Suite et une bibliothèque de contenu Live disponible pour les clients RSA NetWitness Suite. Live offre une interface simple pour parcourir, sélectionner et déployer le contenu à partir du système de gestion de contenu NetWitness Suite Live vers des logiciels et des services de NetWitness Suite. En plus de gérer les flux provenant de la bibliothèque CMS, Live permet aux utilisateurs de déployer des flux et packages personnalisés.

La bibliothèque CMS

La bibliothèque du système de gestion de contenu (CMS) (appelée *Live*) est une source précieuse de ressources de sécurité Internet récentes pour les clients NetWitness Suite. Elle donne une vision des compétences de recherche et d'analyse collectives de la communauté de sécurité internationale afin de garantir que les utilisateurs ont une visibilité vraiment actuelle des secteurs d'attaque.

Live collecte les meilleurs renseignements et contenus avancés relatifs aux menaces dans la communauté de sécurité internationale, soit les idées, la recherche, le suivi continu et l'analyse, et les intègre directement dans le centre des opérations de sécurité des utilisateurs pour classifier définitivement les ordinateurs exposés aux botnets, aux logiciels malveillants et à d'autres exploits pernicieux. Live agrège, consolide et met en évidence uniquement les informations les plus pertinentes relatives à une organisation en temps réel.

NetWitness Suite Feedback et Data Sharing

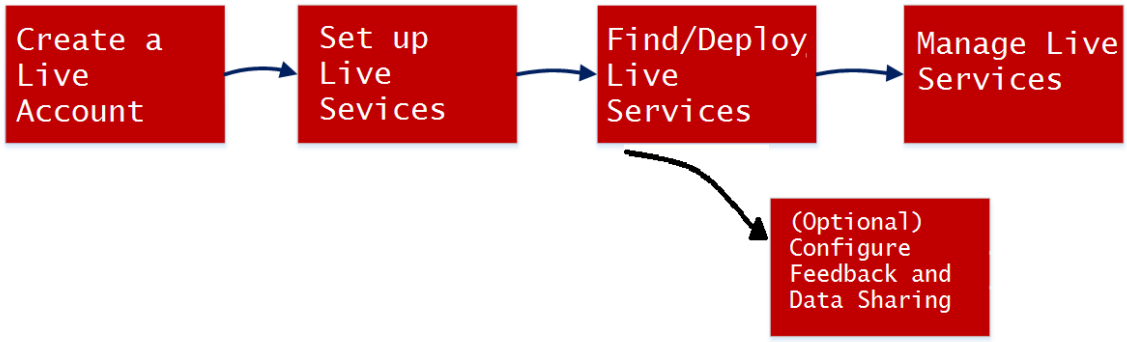
Live Feedback a été conçu pour améliorer RSA NetWitness Suite. Dès qu'un compte Live est configuré, les données d'utilisation sont partagées avec RSA.

RSA Live Connect est un service de renseignements sur les menaces basé sur le Cloud. Ce service collecte, analyse et évalue les renseignements sur les menaces (adresses IP, domaines, fichiers,etc.) qui sont collectés à partir de différentes sources. Il propose le service **Threat Insights** qui permet aux analystes d'extraire des données de renseignements sur les menaces provenant du service Live Connect. Il comprend également **Analyst Behaviors**, service automatisé de collecte de données dans le but de partager des renseignements potentiels sur les menaces en vue de leur analyse.

Pour plus d'informations, reportez-vous à la section Commentaires et Partage de données NetWitness Suite.

Procédures requises pour les services Live

Le workflow suivant décompose la configuration de base en quatre étapes, que vous pouvez compléter individuellement. Le moyen le plus simple de configurer le Decoder consiste à suivre la procédure de bout en bout dans cette section, Procédures requises pour les services Live, qui inclut toutes les étapes.

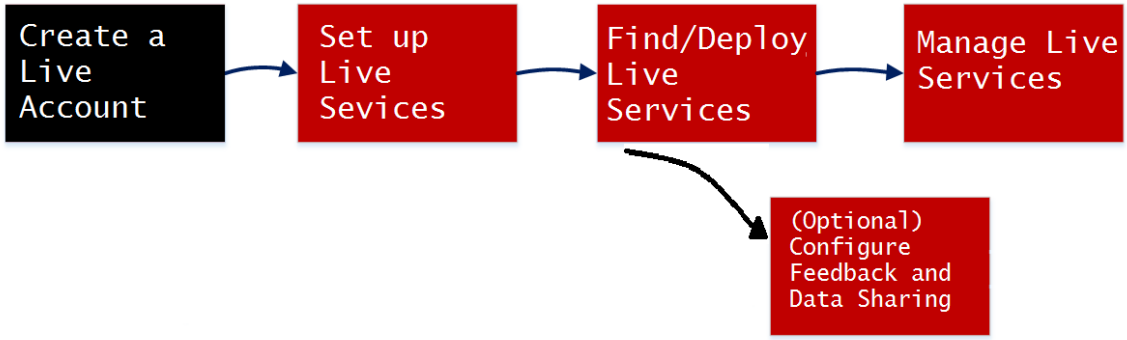


Étape de configuration	Description
Créer un compte Live	Créer un compte Live via l'URL du Portail d'inscription RSA Live :https://CMS.netwitness.com/registration/. Si vous avez déjà un compte, vous pouvez le gérer à l'aide de ce portail.
Configurer les services Live dans NetWitness Suite	Configurer les services Live dans NetWitness Suite en configurant une connexion avec le serveur CMS.
Trouver et déployer des ressources Live	Rechercher et parcourir des ressources dans la vue Live Search, puis déployer les ressources sélectionnées.
Gérer les ressources Live	Cette procédure est requise lorsque les administrateurs souhaitent effectuer une recherche, s'abonner et déployer des ressources à partir de Live.

Étape de configuration	Description
Commentaires et Partage de données NetWitness Suite	Décrit les fonctions de feedback et de partage de données dans RSA NetWitness® Suite , à partir des services Live. La participation est facultative mais elle peut contribuer à fournir des renseignements utiles pour la communauté.

Créer un compte Live

Vous devez créer un compte Live à l'aide du portail d'inscription RSA Live sur le serveur CMS. La bibliothèque CMS fournit l'accès à tout le contenu RSA à un endroit où vous pouvez afficher, rechercher, déployer le contenu RSA et vous y inscrire. Vous devez vous inscrire sur le portail d'inscription RSA Live et sélectionner un niveau d'inscription.



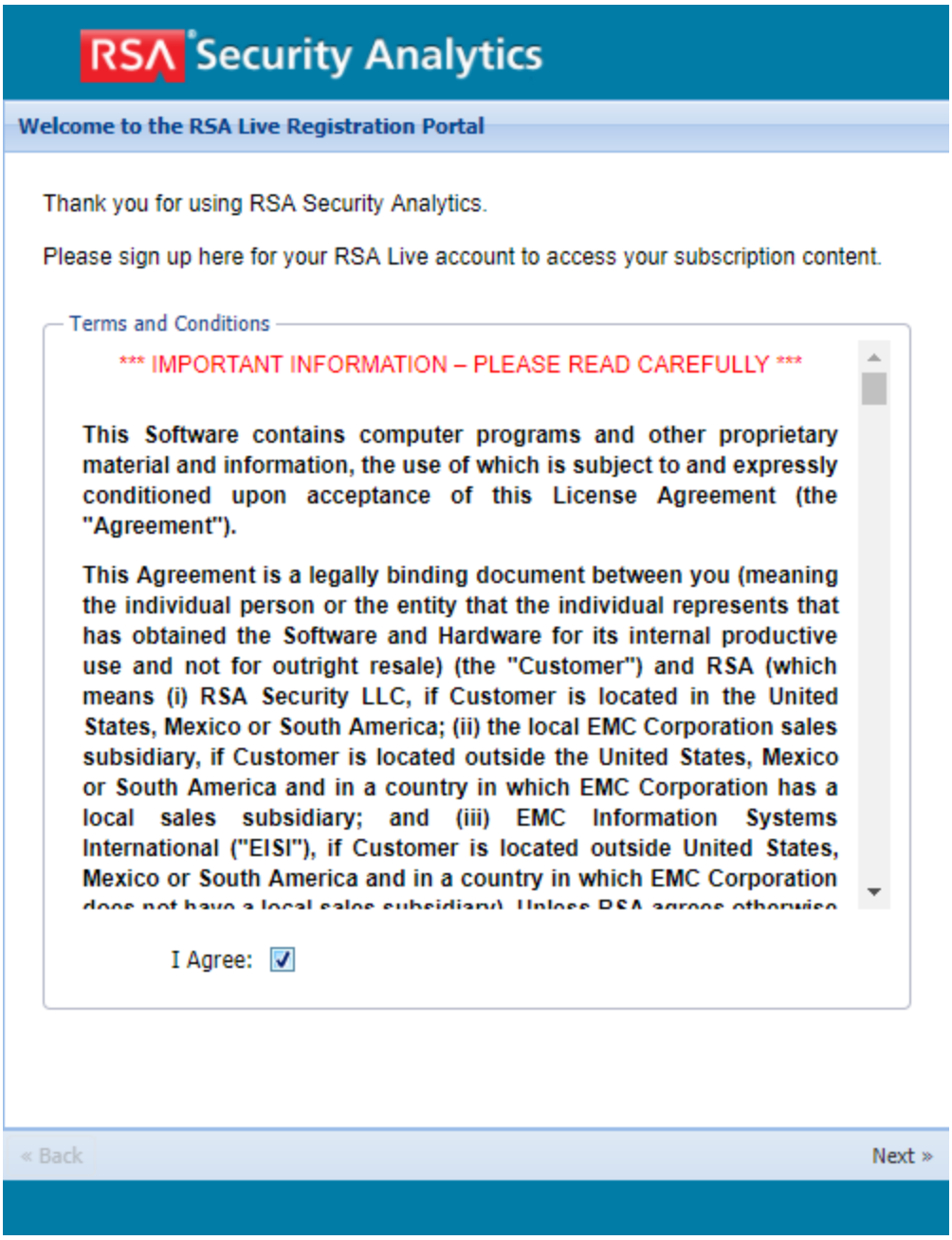
Vérifiez que les éléments suivants sont disponibles pour la configuration d'un compte RSA Live :

- Connexion à Internet active pour l'accès au portail.
- Un serveur de licence NetWitness Suite valide et enregistré sur le serveur Flexera, avant que vous ne puissiez vous inscrire sur un compte Live. Vous pouvez afficher l'ID de licence sur le panneau **ADMIN > Système > Informations**.

Remarque : Si le serveur de licence n'est pas configuré, contactez le service client RSA.

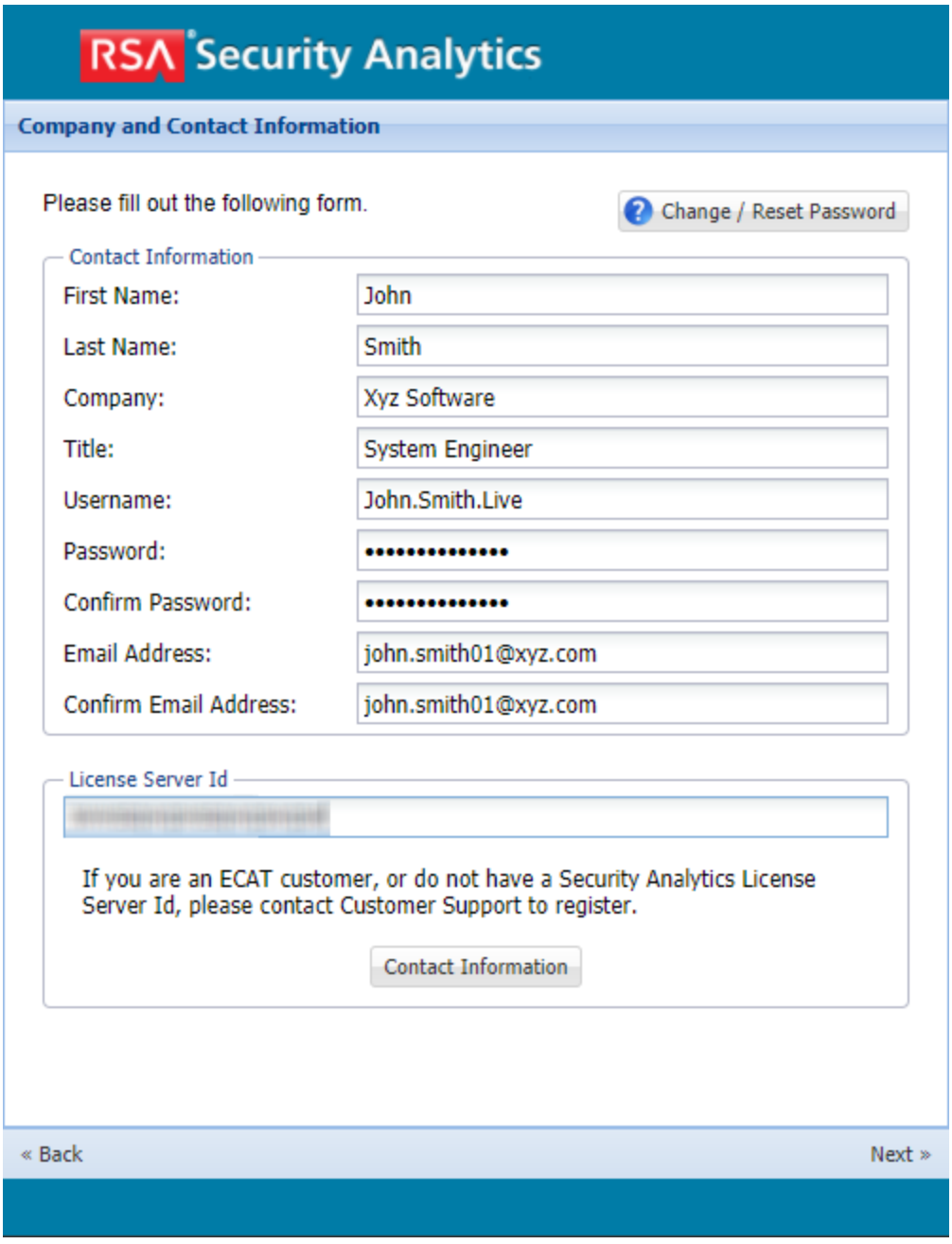
Pour créer un compte Live :

1. Accédez au portail RSA Live Registration à l'aide de l'URL :https://cms.netwitness.com/registration/.
   La page Bienvenue s'affiche.
2. Lisez soigneusement les conditions générales et cochez la case **J'accepte**, comme indiqué ci-dessous :



3. Cliquez sur **Suivant**.
4. Dans la section **Informations de contact**, saisissez tous les champs, comme indiqué ci-dessous :
   - Le **nom d'utilisateur** doit contenir un minimum de 9 caractères et un maximum de 60 caractères.

- Le **mot de passe** doit contenir un minimum de neuf caractères et un maximum de 60 caractères, avec au moins une majuscule, une minuscule, un chiffre et un caractère spécial.
- L'**adresse e-mail** que vous saisissez permet d'envoyer des notifications relatives à votre compte Live.



5. Dans la section **Niveau d'inscription**, sélectionnez l'un des niveaux d'inscription suivants :

- **Basic** : fournit un accès au contenu Live qui est balisé pour des groupes comme Basic, Panorama for Log Decoder, et Spectrum for Malware Analysis.
- **Amélioré** - Fournit un accès au contenu Live qui est balisé pour des groupes comme Enhanced, Basic, Panorama for Log Decoder, et Spectrum for Malware Analysis.
- **Premium** - Fournit un accès au contenu Live qui est balisé pour des groupes comme Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder et Spectrum for Malware Analysis.

6. Dans la section **Confirmer le niveau d'inscription**, sélectionnez à nouveau le niveau d'inscription pour confirmer.
7. Saisissez l'**ID de serveur de licence**. Vous pouvez afficher l'ID de licence sur la page **ADMIN > Système > Informations**.

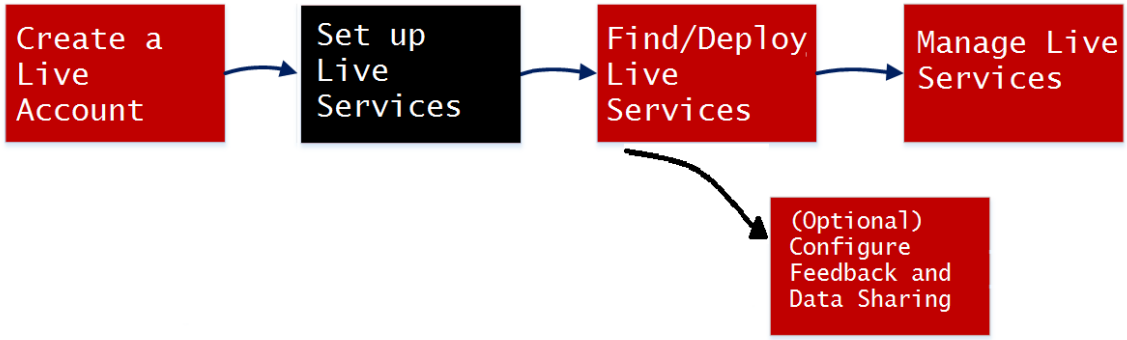
   Attention : Assurez-vous que l'ID de serveur de licence sur NetWitness Suite est valide et enregistré sur le serveur Flexera. Si ce n'est pas le cas, contactez le Support Clients de RSA.

8. Cliquez sur **Suivant**.

Si l'enregistrement réussit, vous recevrez l'e-mail de confirmation de compte RSA Live avec votre nom d'utilisateur. Vous avez désormais accès au contenu auquel vous vous êtes inscrit.

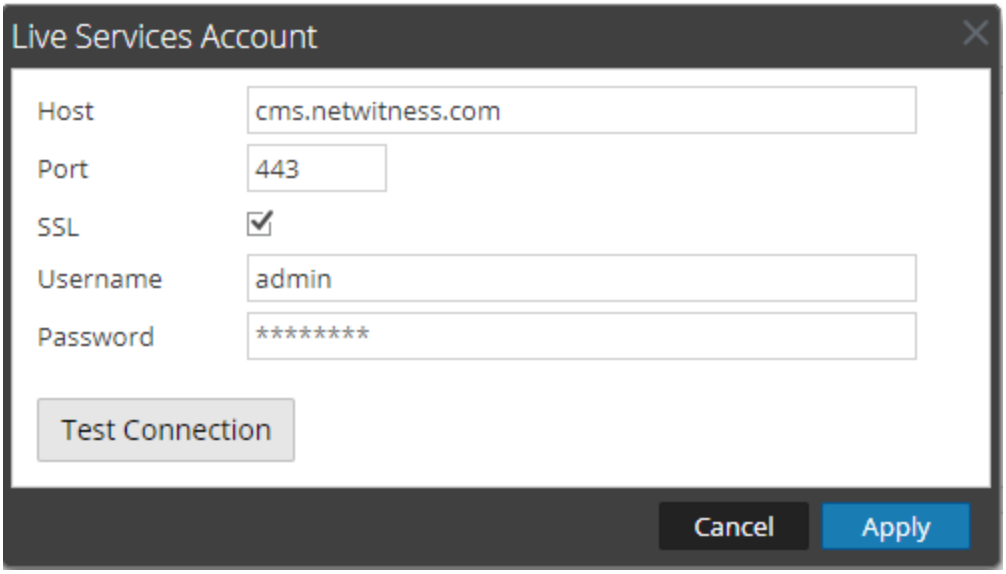
Configurer les services Live dans NetWitness Suite

Pour configurer Live sur NetWitness Suite, vous configurez la connexion et la synchronisation entre le serveur CMS et NetWitness Suite. L'interface utilisateur pour cette configuration est ADMIN > Système > Panneau de configuration des services Live.



Pour configurer la connexion au serveur CMS :

1. Configurez la connexion au serveur CMS et le compte Live.

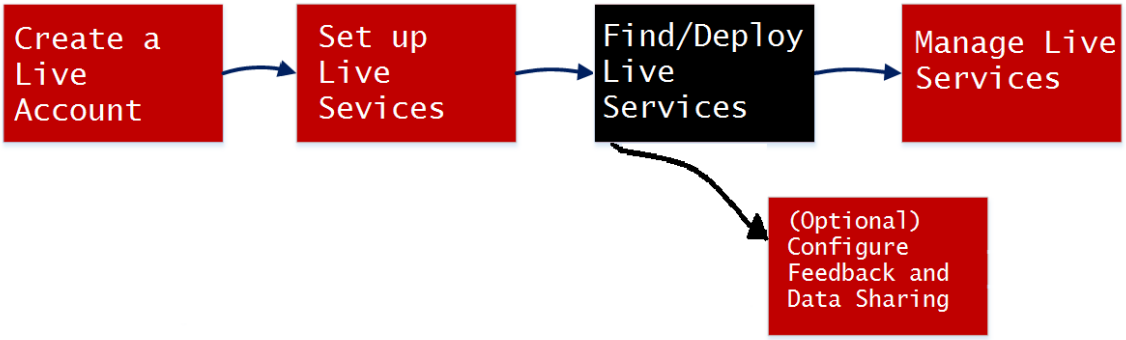


2. Configurez la période de synchronisation de NetWitness Suite avec les mises à jour provenant de Live.

Pour plus d'informations, consultez la section Configurer les paramètres des services Live dans le *Guide de configuration système*.

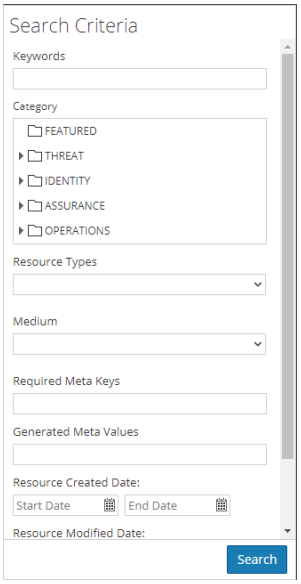
Trouver et déployer des ressources Live

Les administrateurs peuvent rechercher des ressources dans la vue Live Search, qui est identique à la procédure d'accès aux ressources CMS Live à l'aide du panneau Critères de recherche de la Vue Live Search.



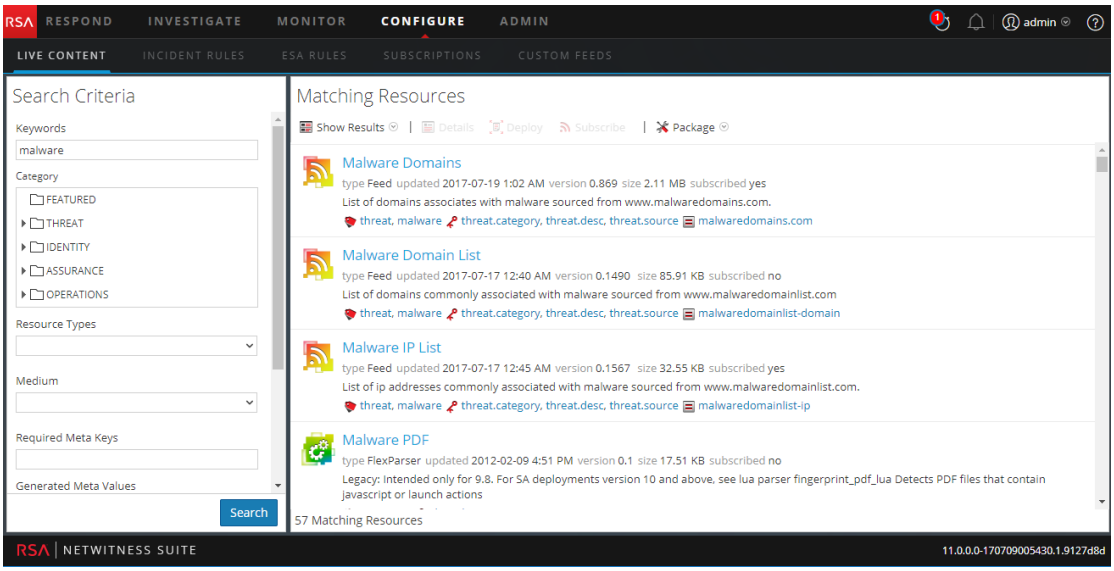
Rechercher des ressources

1. Dans le panneau **Critères de recherche**, spécifiez des critères de recherche. Saisissez tout ou partie de ces éléments : mot clé, catégorie, type de ressource, moyen, clés méta, valeurs de métadonnées, date de création de la ressource et date de modification de la ressource.



2. Cliquez sur **Rechercher**.

   Les résultats détaillés s'affichent dans le panneau Ressources correspondantes.



3. (Facultatif) Pour limiter les résultats dans le panneau Ressources correspondantes, cliquez sur une balise, une métaclé, un moyen ou une valeur méta de ressource dans un résultat.

Déployer des ressources dans Live

Dans RSA NetWitness Suite, vous pouvez déployer des ressources sélectionnées manuellement à l'aide de l'assistant Déploiement, ou vous pouvez vous abonner à un groupe de ressources.

- Lorsque vous obtenez des résultats après avoir parcouru des ressources dans NetWitness Suite Live, vous pouvez déployer les ressources manuellement vers un service ou un groupe de services sans souscrire à ces ressources.
- Le déploiement manuel des ressources effectue le déploiement sur les services sans tirer parti des puissantes fonctionnalités de gestion de ressource de NetWitness Suite. Si vous souhaitez recevoir des notifications et mises à jour pour les ressources mises à jour et pouvoir facilement supprimer les ressources d'un service, vous devez vous abonner aux ressources dans la vue Live Search et les déployer dans la Vue Configuration Live.

Pour le déploiement manuel, il s'agit de la procédure de base :

1. Sélectionnez une ressource ou un groupe de ressources, ou sélectionnez un package de ressources précédemment créé.
2. Cliquez sur Déployer, qui lance l'Assistant de déploiement.
3. Passez en revue la liste des ressources sélectionnées.
4. Sélectionnez les services ou les groupes de services vers lesquels vous voulez déployer les ressources sélectionnées.

5. Revoir vos sélections précédentes
6. Déploiement

La procédure suivante explique comment déployer un groupe de ressources ou un package de ressources :

- Vous pouvez sélectionner une ou plusieurs ressources dans la Vue Ressources Live, puis les déployer vers les services.
- Ou, si vous avez précédemment créé et enregistré un package de ressources, vous pouvez déployer le package vers les services. Pour connaître la procédure de création d'un package, reportez-vous à la rubrique Assistant Déploiement du package de la ressource.

Pour déployer des ressources manuellement :

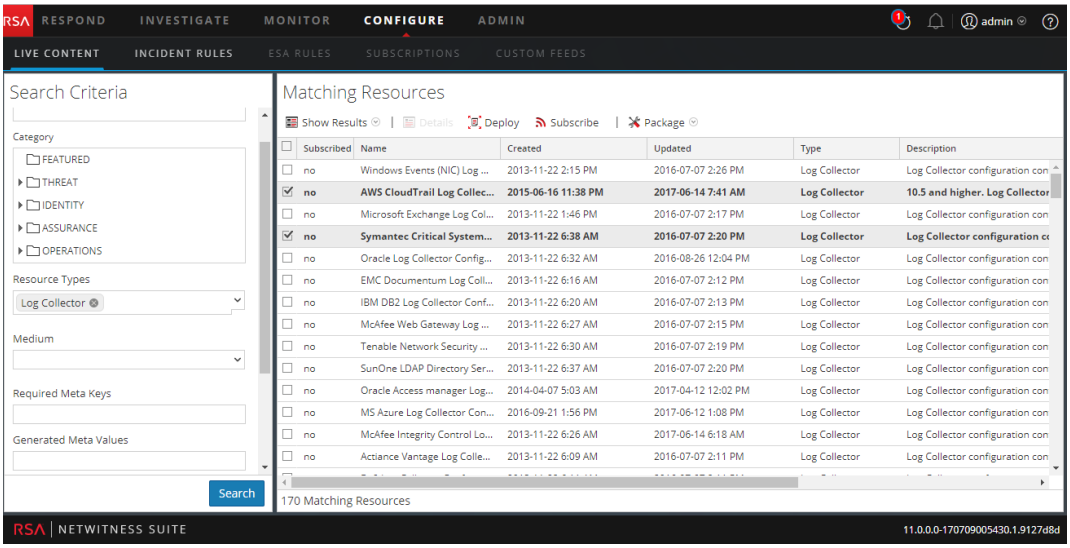
1. Accédez à **CONFIGURER > Contenu Live**.
2. Sélectionnez un groupe de ressources ou un package de ressources précédemment créé.

   Pour sélectionner une ressource ou un groupe de ressources :

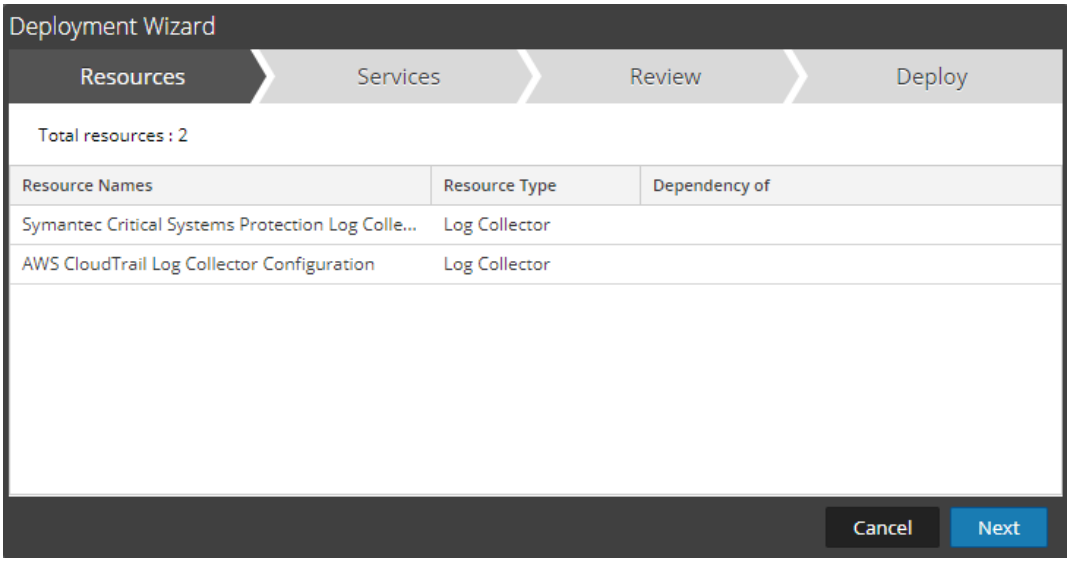
   a. Dans la **vue Live Search**, parcourez les ressources Live (par exemple, recherchez le type de ressource **Log Collector**).

   b. Dans le panneau **Ressources correspondantes**, sélectionnez **Afficher les résultats > Grille**.

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



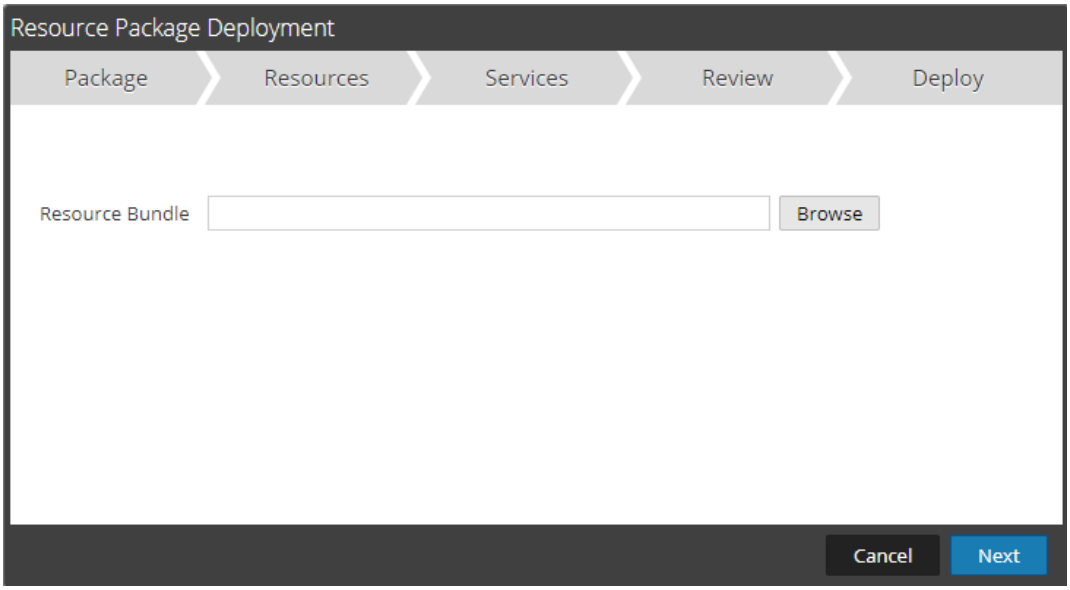
d. Dans la barre d'outils Ressources correspondantes, cliquez sur Deploy.



3. Pour sélectionner un package de ressources à déployer :

a. Dans la vue **Live Search**, dans la barre d'outils **Ressources correspondantes**, sélectionnez **Package** > **Déployer** :

La page Package de l'Assistant Déploiement du package de la ressource s'affiche.



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

c. Cliquez sur **Ouvrir**.

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

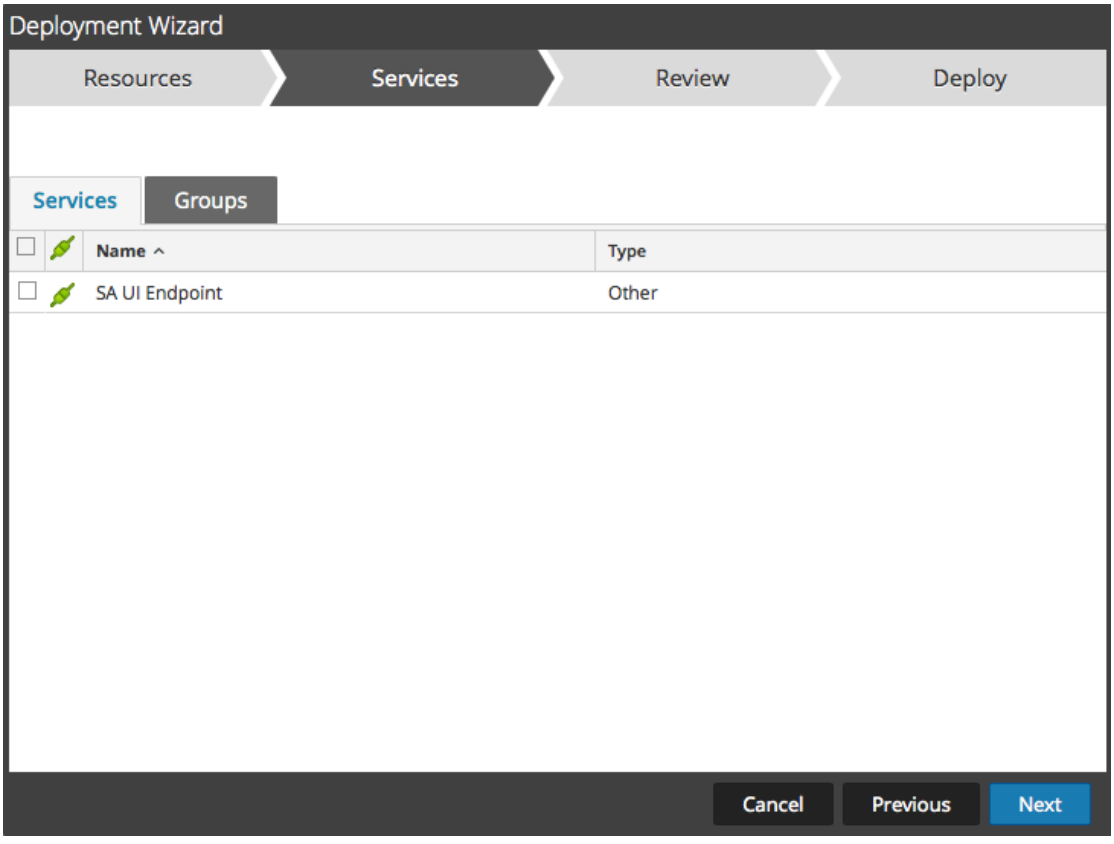
4. Cliquez sur **Suivant**.

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

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

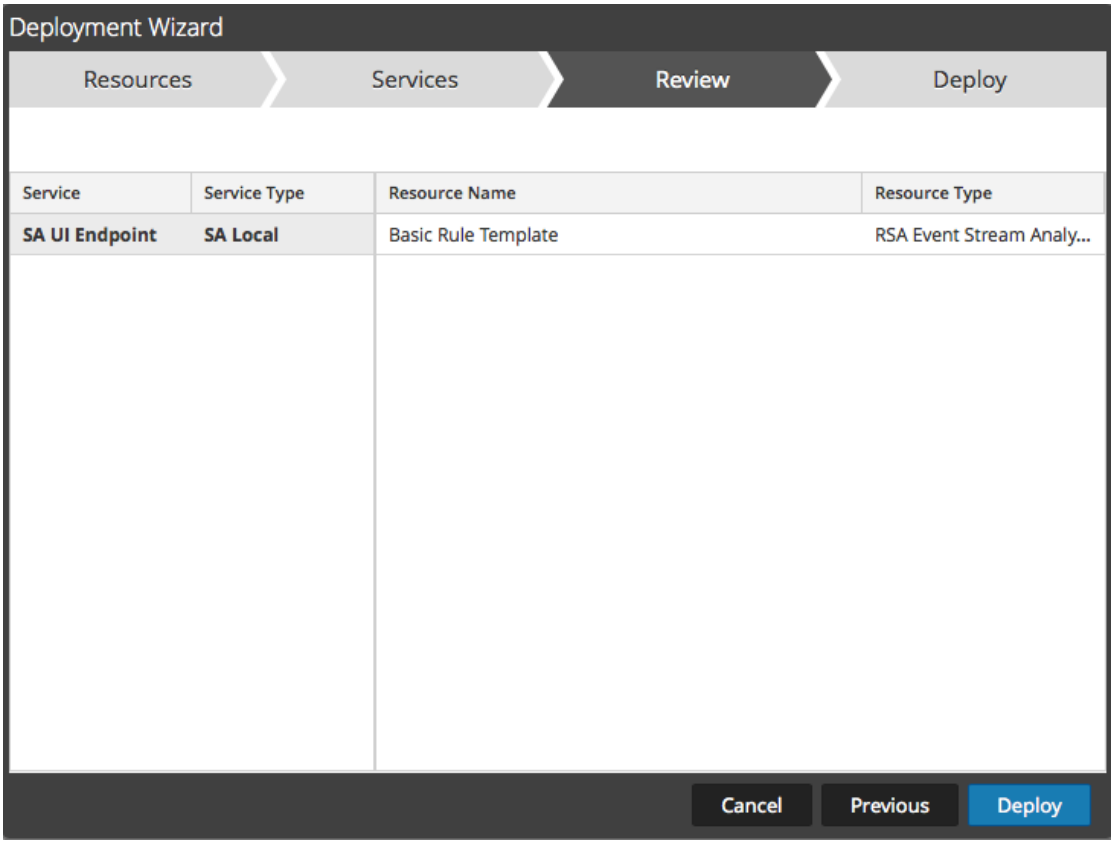
5. Sélectionnez les services au niveau desquels vous souhaitez déployer le contenu. Vous pouvez sélectionner une combinaison de services et de groupes de services.

   - Utilisez l'onglet **Services** pour sélectionner un seul service, une liste des services et des groupes de services qui sont configurés dans la vue Administration - Services.
   - Utilisez l'onglet **Groupes** pour sélectionner des groupes de services



6. Cliquez sur **Suivant**.

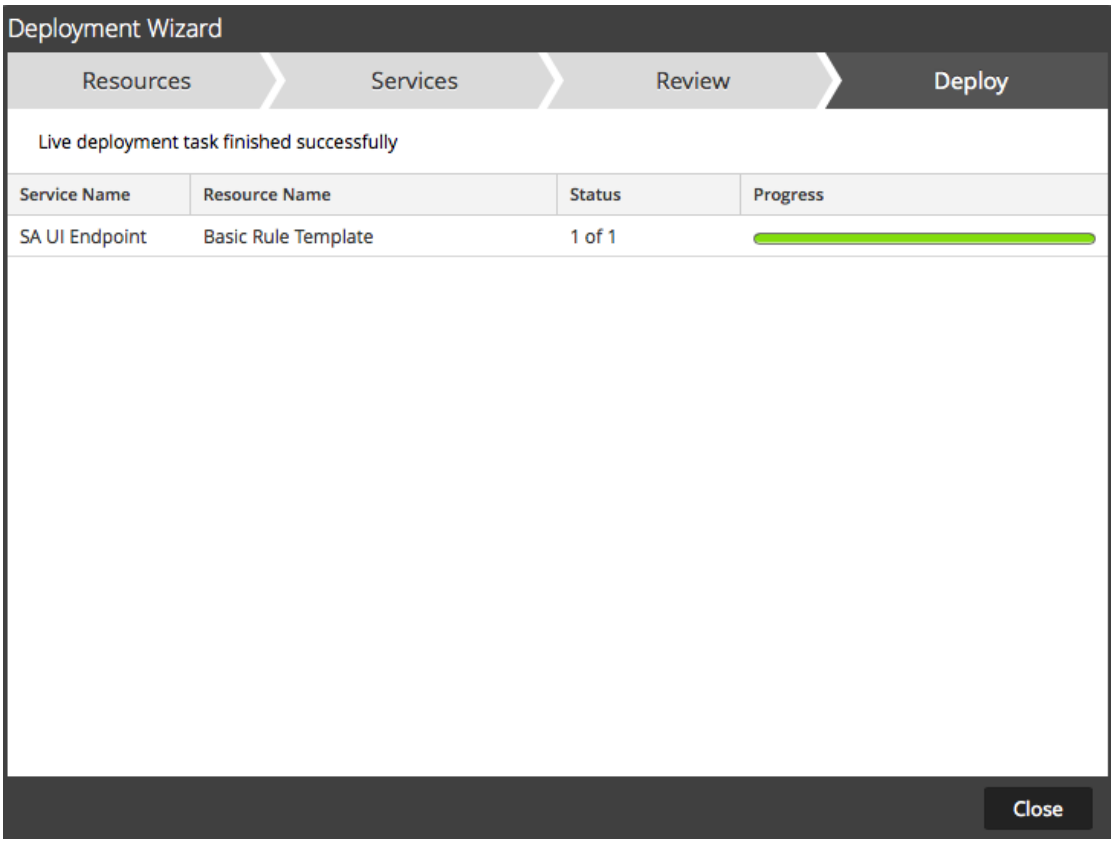
La page **Révision** s'affiche.



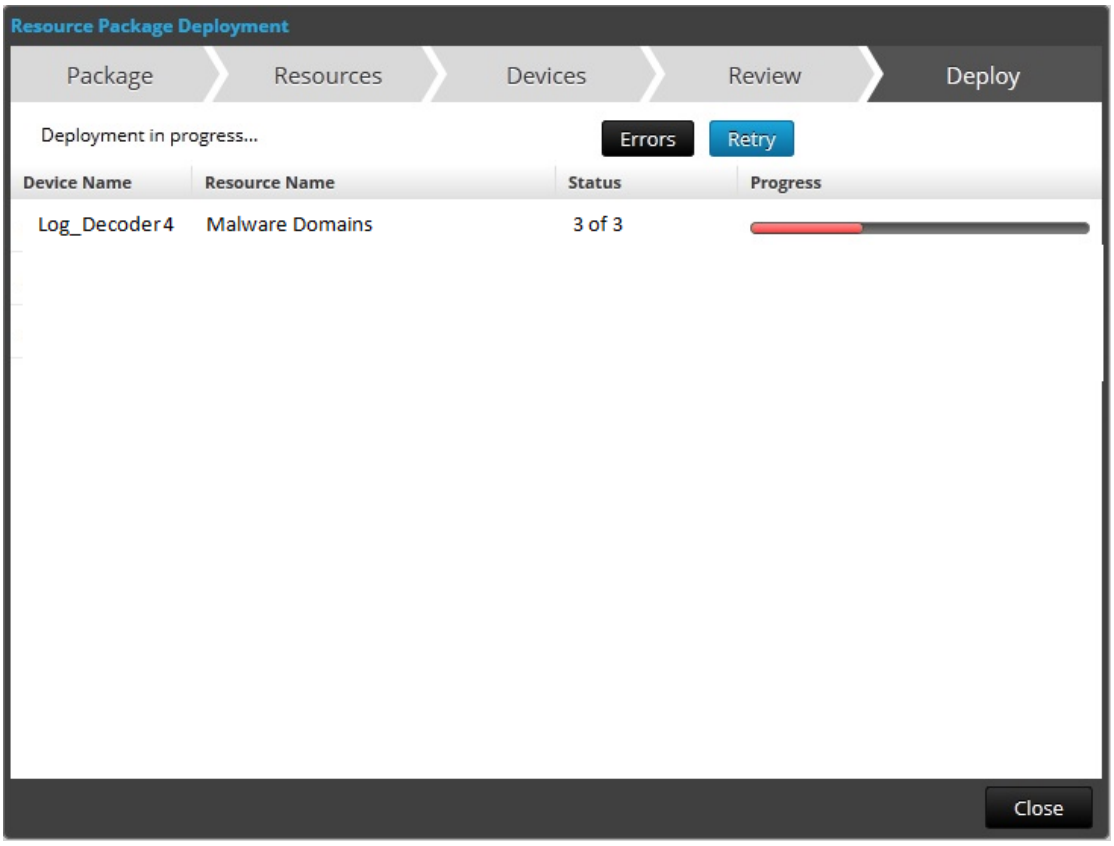
Veillez à sélectionner les ressources appropriées et les services au niveau desquels vous souhaitez effectuer le déploiement.

7. Cliquez sur **Déployer**.

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



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



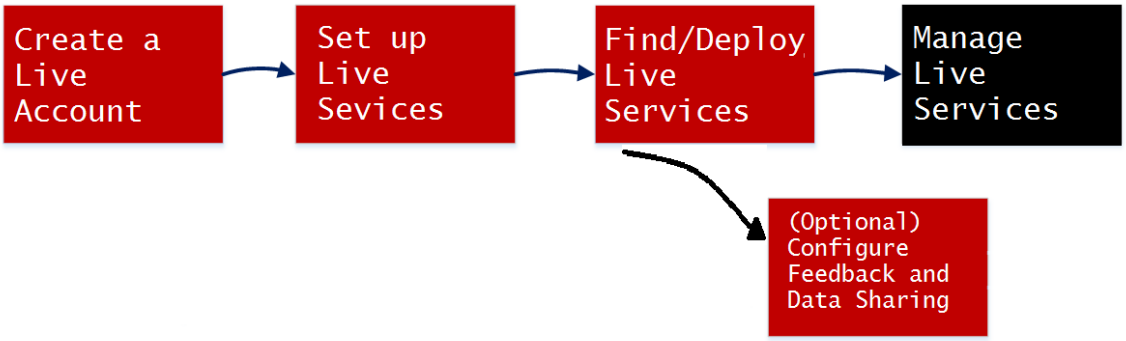
8. Cliquez sur **Fermer**.

Étapes suivantes

Après avoir déployé les parsers dans les Decoders et les Log Decoders, vous devez activer les parsers sur les différents services, comme il est décrit dans le *Guide de configuration de Decoder et Log Decoder*.

Gérer les ressources Live

Ces procédures sont requises lorsque les administrateurs souhaitent effectuer une recherche, s'abonner et/ou déployer des ressources de Live. Avec une connexion au serveur CMS, vous pouvez effectuer des recherches, vous abonner et déployer des ressources à partir de Live en fonction de votre niveau d'abonnement. Une fois que vous avez trouvé les ressources, déployez-les sur les services et les groupes de services qui ont été configurés dans la vue Administration - Services.



Procédures

Il existe plusieurs workflows possibles pour déployer les ressources dans les services et pour gérer ces déploiements. Ces composants sont les suivants :

- S'abonner et déployer les ressources.
- Déployer un bundle de ressources.
- Supprimer les déploiements de ressources.
- Télécharger les ressources.
- Configurer les sources de données.

Gérer l'abonnement et le déploiement

Les workflows d'abonnement et de déploiement tirent parti des outils de gestion des ressources disponibles dans Live. En vous abonnant aux ressources, vous acceptez de recevoir des ressources mises à jour conformément à la synchronisation configurée dans le panneau **Administration > Configuration de Live**.

En ajoutant les ressources souscrites à la liste des déploiements, vous configurez NetWitness Suite pour transmettre automatiquement ces ressources aux services sélectionnés dans les intervalles de synchronisation configurés. Cette méthode nécessite une certaine planification des groupes de services et des services où les ressources sont déployées. En outre :

- Vous pouvez supprimer une ressource de la liste des déploiements sous l'onglet Onglet Déploiements.
- Vous pouvez vous désabonner d'une ressource sous l'onglet Onglet Abonnements et la vue Vue Ressources Live.

Pour gérer les abonnements et le déploiement :

1. Dans le panneau **Administration > Système > Live** , spécifiez un intervalle auquel NetWitness Suite vérifie les mises à jour des ressources souscrites dans Live et spécifiez les adresses e-mail des personnes devant recevoir un e-mail contenant la liste des ressources souscrites qui ont été mises à jour.
2. Dans la vue **Live** > **Search** , recherchez des ressources Live pour vous y abonner.
3. Dans la vue **Live** > **Configurer** > **onglet Déploiements**, sélectionnez des ressources souscrites et ajoutez-les à la liste des déploiements des groupes de services.
4. (Facultatif) Dans le panneau **Administration** > **Système** > **Live** , cliquez sur 

pour déployer immédiatement les ressources affichées sous l'onglet Déploiements.
5. Dans la vue **Live** > **Configurer** > **onglet Déploiements**, sélectionnez les ressources déployées et supprimez-les des groupes de services.
6. Dans la vue **Live** > **Configurer** > **onglet Abonnements**, désabonnez-vous des ressources.

Supprimer une ressource déployée

Une fois déployées sur un service, les ressources Live restent sur le service jusqu'à leur suppression. Il est recommandé de supprimer les ressources inutilisées des services sur lesquels elles sont déployées.

Pour supprimer une ressource, accédez à la Vue Ressources Live, désabonnez-vous d'une ressource, puis supprimez la ressource des services sur lesquels elle est déployée.

Déployer un bundle de ressources

Pour déployer un package de contenu, utilisez l'Assistant Déploiement du package de la ressource. Vous pouvez déployer un package de contenu créé dans Live vers un ou plusieurs services. NetWitness Suite accepte les packages au format de fichiers **.nwp** ou **.zip**.

Télécharger les ressources

Pour télécharger des ressources Live sur votre système de fichiers local, utilisez le bouton **Télécharger** dans la vue Ressources Live.

Configurer les sources de données

Dans la vue **Live** > **Feeds** , vous pouvez configurer et gérer les feeds personnalisés et les feeds d'identité.

Procédures supplémentaires

Cette rubrique explique les procédures supplémentaires qu'un administrateur peut choisir de suivre, et qui ne sont pas indispensables à la configuration ou à l'utilisation des services Live.

- Exporter des données vers RSA
- Gérer les feeds personnalisés
  - Créer un Feed personnalisé
  - Créer un Feed STIX personnalisé
  - Créer et gérer un feed d'identité
  - Modifier un feed
  - Supprimer un feed
- Différentes procédures pour les services Live

Exporter des données vers RSA

Un administrateur NetWitness Suite peut exporter les metrics dans NetWitness Suite pour Live Feedback.

À propos de Live Feedback

Si le compte Live n'est pas configuré, vous pouvez manuellement télécharger les données d'utilisation de RSA. Pour plus d'informations, consultez la rubrique Panneau de configuration des Services Live dans le *Guide de configuration système*.

Le Panneau de configuration des services Live contient un log d'activité Live Feedback qui vous permet de télécharger les données d'utilisation requises pour Live Feedback. Il reste toujours actif quelle que soit la configuration du compte Live.

Vous pouvez télécharger en aval au préalable l'historique des données Live Feedback, puis le télécharger en amont pour effectuer un partage avec RSA

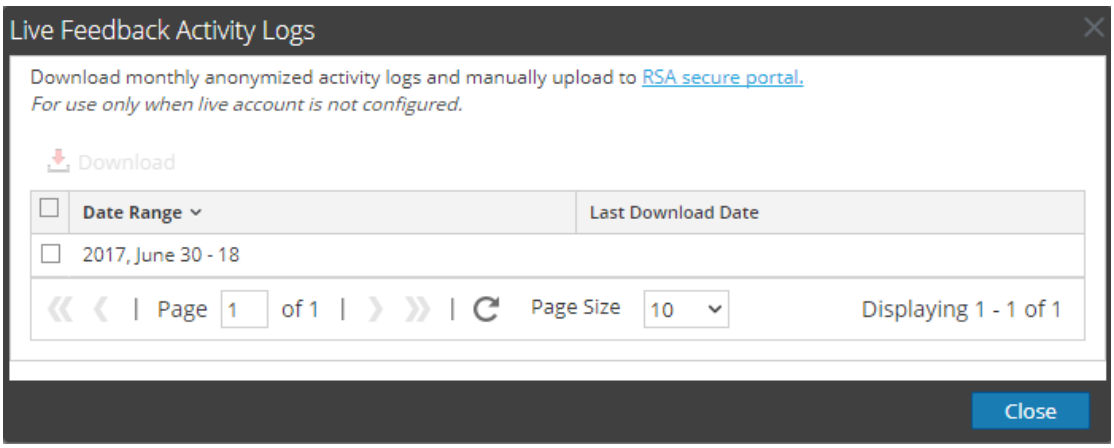
Télécharger l'historique des données Live Feedback

Pour télécharger l'historique des données Live Feedback :

1. Accédez à **ADMIN** > **System**.
2. Dans le panneau des options, sélectionnez **Services Live**.

   L'écran **Compte Live** composé des affichages **État Live RSA** et **Télécharger le log d'activité Live Feedback** apparaît.
3. Cliquez sur **Télécharger le log d'activité Live Feedback**.

   La fenêtre **Télécharger les logs d'activité Live Feedback** s'ouvre pour vous permettre de télécharger l'historique des données Live Feedback requis.



4. Sélectionnez une ou plusieurs entrées en sélectionnant les cases à cocher, puis cliquez

sur **Télécharger**.

Remarque : Si vous sélectionnez plusieurs entrées dans l'historique, le fichier zip téléchargé se compose d'un fichier JSON individuel par mois.

Les données Live Feedback téléchargées sont au formatJSON et sont compressées en fichier .zip. Pour plus d'informations, consultez la rubrique Présentation de Live Feedback dans le *Guide de configuration système*.

Partager des données dans RSA

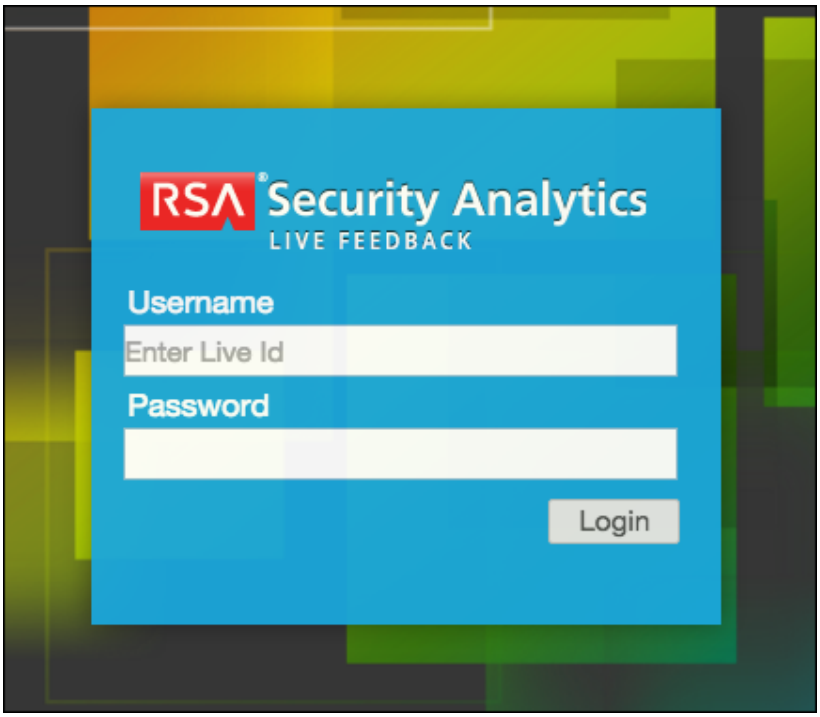
Après avoir téléchargé en aval les données Live Feedback, vous pouvez ensuite les télécharger en amont à l'aide de la procédure suivante.

Pour partager les données dans RSA :

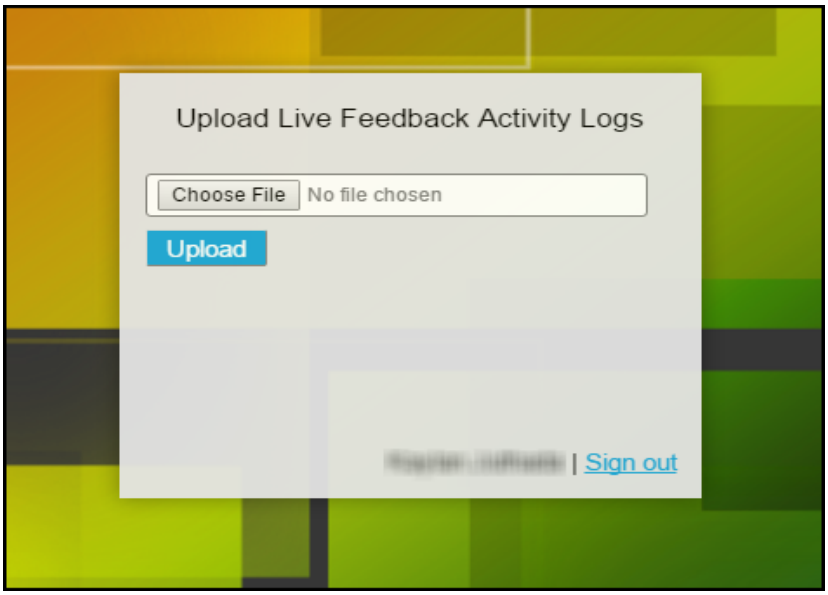
1. Cliquez sur le **portail sécurisé RSA** disponible dans la fenêtre **Logs d'activité Live Feedback**.

   L'écran de connexion RSA NetWitness Suite Live Feedback s'affiche.

2. Connectez-vous au portail Télécharger en amont les logs d'activité Live Feedback à l'aide de vos informations d'identification Live.



3. Cliquez sur **Télécharger le log d'activité Live Feedback**.



4. Cliquez sur **Télécharger**.

Gérer les feeds personnalisés

Cette rubrique présente la fonction de feed personnalisé qui est implémentée à l'aide de l'assistant Feed personnalisé, dans RSA NetWitness Suite, pour renseigner rapidement les Decoders grâce aux feeds personnalisés et aux feeds d'identité.

Création d'un feed personnalisé

Utilisez **Live** > **Feeds** > **Configurer le feed** > **Configurer un feed personnalisé** pour créer et déployer rapidement des feeds de Decoder en fonction d'une logique déterministe qui offre les clés métas spécifiques aux Decoders et Log Decoders sélectionnés. Bien que l'Assistant vous guide tout au long du processus pour créer des feeds à la demande et périodiques, vous devez comprendre la forme et le contenu d'un fichier de feed lorsque vous créez un feed.

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

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

Échantillon de fichier de définition de feed

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

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

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

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

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

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

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

 </FDF>
```

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

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

Paramètre NetWitness Suite	Équivalent du fichier de définition de feed
Onglet **Définir le feed**	

Paramètre NetWitness Suite	Équivalent du fichier de définition de feed
Type de feed	Sélectionnez : **Par défaut** - pour définir un feed basé sur un fichier de données de feed au format `.csv` . **STIX** - pour définir un feed basé sur un fichier STIX au format `.xml` .
Type de tâche par défaut	Selectionnez : **Adhoc** - pour créer un feed à la demande. **Récurrent** - pour créer un feed qui se répète automatiquement.
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.
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.
(STIX, récurrent) **Approuver tous les certificats**	Sélectionnez **Approuver tous les certificats** si vous ne souhaitez pas valider le certificat du serveur REST. Cette option est activée par défaut (cochée).
(STIX, récurrent) **Certificat/Naviguer**	Pour une authentification client avec l'URL REST, dans le champ **Certificat**, cliquez sur **Parcourir** et sélectionnez le certificat auto-signé. Les formats de certificat pris en charge sont .cer, .crt, avec des fichiers codés Base64 et DER.
Onglet **Définir le feed** - Options avancées	
Fichier de feed XML	Nom du fichier de définition de feed, par exemple, `dynamic_dns.xml`.
Separateur	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.

Paramètre NetWitness Suite	Équivalent du fichier de définition de feed
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, #.
Supprimer les données STIX antérieures à	Nombre de jours pour lesquels les packages STIX téléchargés à partir du serveur TAXII doivent être stockés. Les packages STIX antérieurs au nombre de jours spécifiés sont supprimés automatiquement. La valeur par défaut est 180 jours. C'est aussi la valeur maximale.
Onglet Sélectionner des services	Sélectionnez les services auxquels vous souhaitez envoyer le feed de données.
(onglet Définir des colonnes, Définir l'index) **Type**	Type de valeur de recherche dans la position d'index du fichier de données de feed. **IP** indique que chaque ligne du fichier de données de feed contient une adresse IP dans la position de valeur de recherche. La valeur IP est au format décimal à points (par exemple, 10.5.187.42). **Plage IP** indique que chaque ligne du fichier de données de feed contient une plage d'adresses IP dans la position de valeur de recherche. La plage IP est au format CIDR (par exemple, 192.168.2.0/24). **Non IP** indique que chaque ligne du fichier de données de feed contient une valeur de métadonnées autre que l'adresse IP dans la position de valeur de recherche. Les champs Type de service, Tronquer le domaine et Clé de retour deviennent actifs dans le cas d'un index Non IP.
(onglet Définir des colonnes, Définir l'index) **CIDR**	Spécifie que la valeur IP dans la position de recherche est au format CIDR. L'attribut **CIDR** définit le format de l'adresse IP dans le champ sur la notation Classless Inter-Domain Routing (CIDR).

Paramètre NetWitness Suite	Équivalent du fichier de définition de feed
(Onglet Définir des colonnes, Définir l'index) **Type de service**	Pour un index Non IP, type de service en nombre entier permettant de filtrer les recherches méta. Il correspond à l'attribut **MetaCallback apptype** dans le fichier de définition de feed. Une valeur de **0** indique qu'il n'y a aucun filtrage par type de service.
(Onglet Définir des colonnes, Définir l'index) **Tronquer le domaine**	Pour un index Non IP, le système peut extraire des données l'élément spécifique à l'hôte pour les métavaleurs qui contiennent les noms de domaine (par exemple, les noms d'hôtes). Tronquer le domaine correspond à l'attribut **MetaCallback truncdomain**. Si la valeur est www.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, Définir l'index) **Clés de rappel**	Pour un index Non IP, les métaclés disponibles à mettre en correspondance à la place de ip.src/ip.dst (les valeurs par défaut pour le type d'index IP) peuvent être sélectionnées dans la liste déroulante. La Clé de rappel correspond à l'attribut MetaCallback name, et la colonne index du fichier csv doit contenir des données pouvant correspondre à la clé méta choisie. Par exemple, si la clé méta du nom d'utilisateur est choisie, la colonne index du fichier csv doit être renseignée avec les utilisateurs à associer.

Paramètre NetWitness Suite	Équivalent du fichier de définition de feed
(Onglet Définir des colonnes, Définir l'index) **Colonne index**	Identifie la colonne du fichier de données de feed qui donne la valeur de recherche pour la ligne. Chaque position de chaque ligne du fichier de données de champ est identifiée par l'attribut **Index de champ** dans le fichier de définition de feed. Un champ dont l'index est **1** indique la première entrée de la ligne. Le second champ représente l'index **2**, le troisième champ l'index **3**, etc. Vous pouvez sélectionner plusieurs colonnes d'index, si le **Type de feed** est **STIX** et le **Type d'Index** est **Non IP**. Lorsque vous sélectionnez plusieurs colonnes d'index, les valeurs à partir de toutes les colonnes sélectionnées sont fusionnées dans la première colonne d'index que vous avez sélectionnée.
(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 **reputation.src** et **reputation.dst**). Cette valeur est référencée par l'attribut Clé de champ.

Étapes suivantes

- Créer un Feed personnalisé
- Créer et gérer un feed d'identité
- Modifier un feed
- Supprimer un feed

Créer un Feed personnalisé

Cette rubrique fournit des instructions pour créer un feed personnalisé à l'aide d'un fichier de données de feed au format .csv ou STIX dans RSA NetWitness Suite.

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

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` ou `.xml`. Si vous avez également un fichier de définition de feed associé au format `.xml`, qui décrit la structure du fichier de données de feed, vous pourrez utiliser le fichier de définition de feed pour créer un feed. L'assistant Feed personnalisé peut créer le feed en se basant sur un fichier de données de feed, ou en se basant sur un fichier de données de feed et le fichier de définition de feed correspondant.

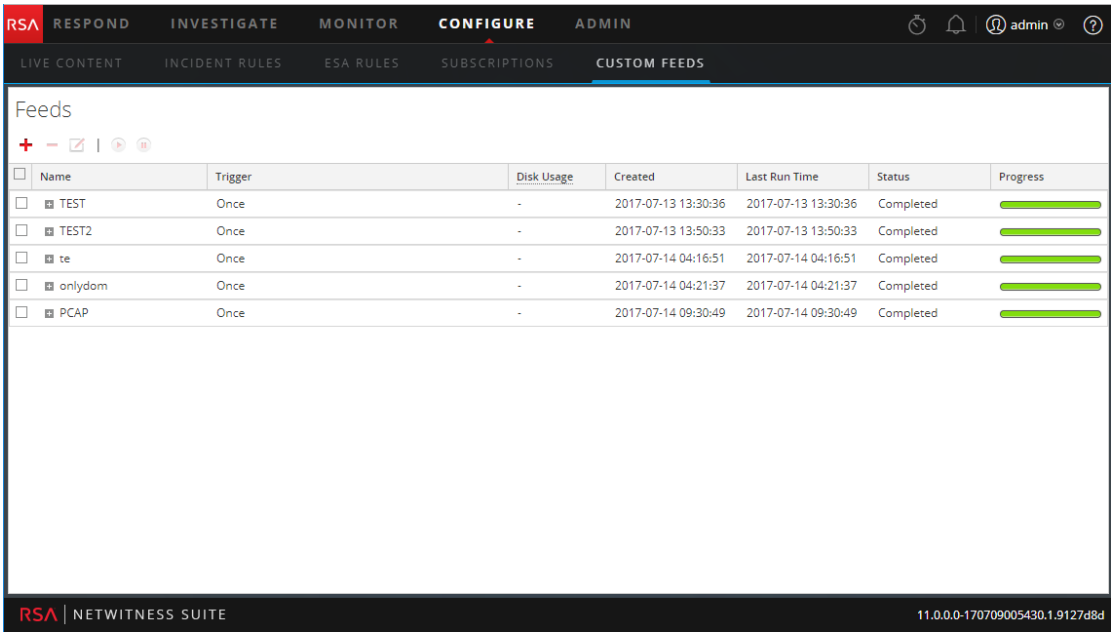
À la fin de cette procédure, vous aurez créé un feed personnalisé.

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

Pour créer un feed personnalisé :

1. Accédez à **CONFIGURER > FEEDS PERSONNALISÉS**.

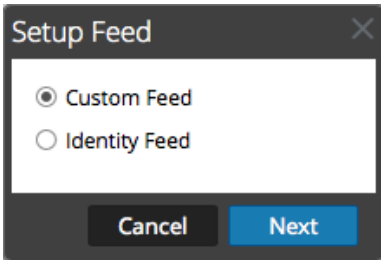
   La vue Feeds personnalisés s'affiche.



2. Dans la barre d'outils, cliquez sur

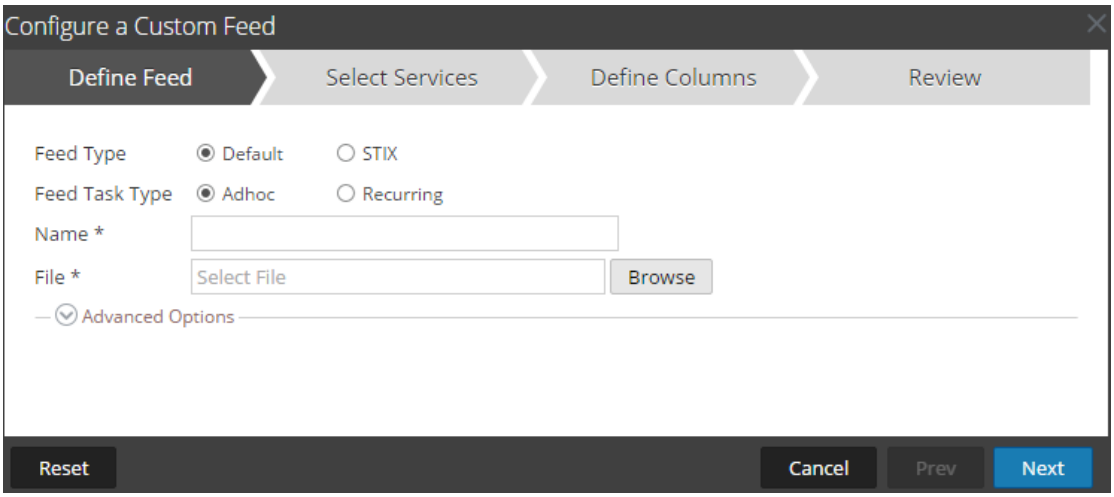
+.

La boîte de dialogue Configurer le feed s'affiche.



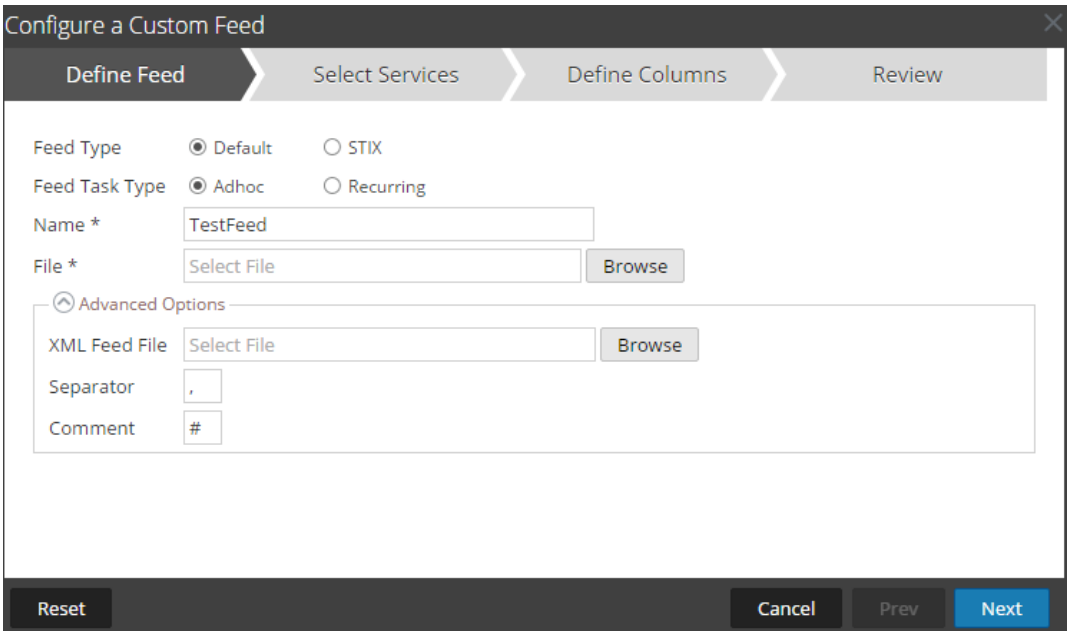
3. Pour sélectionner le type de feed, cliquez sur **Feed personnalisé**, puis sur **Suivant**.

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



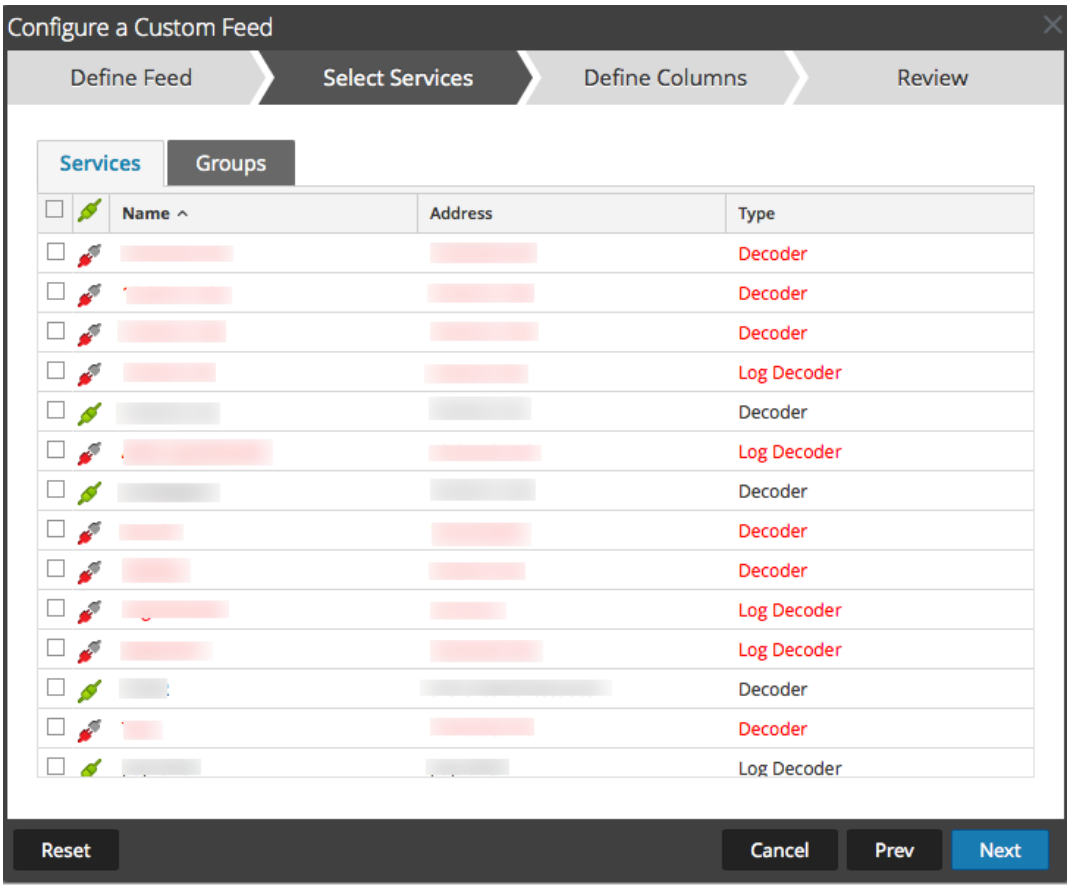
4. Pour définir un feed basé sur un fichier de données de feed au format `.csv`, sélectionnez **Par défaut** dans le champ **Type de feed**.
5. Pour définir une tâche de feed à la demande qui s'exécute une fois, sélectionnez **Ad hoc** dans le champ **Type de tâche par défaut** et procédez d'une des manières suivantes :
   a. (Conditionnel) Pour définir un feed basé sur un fichier 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**.

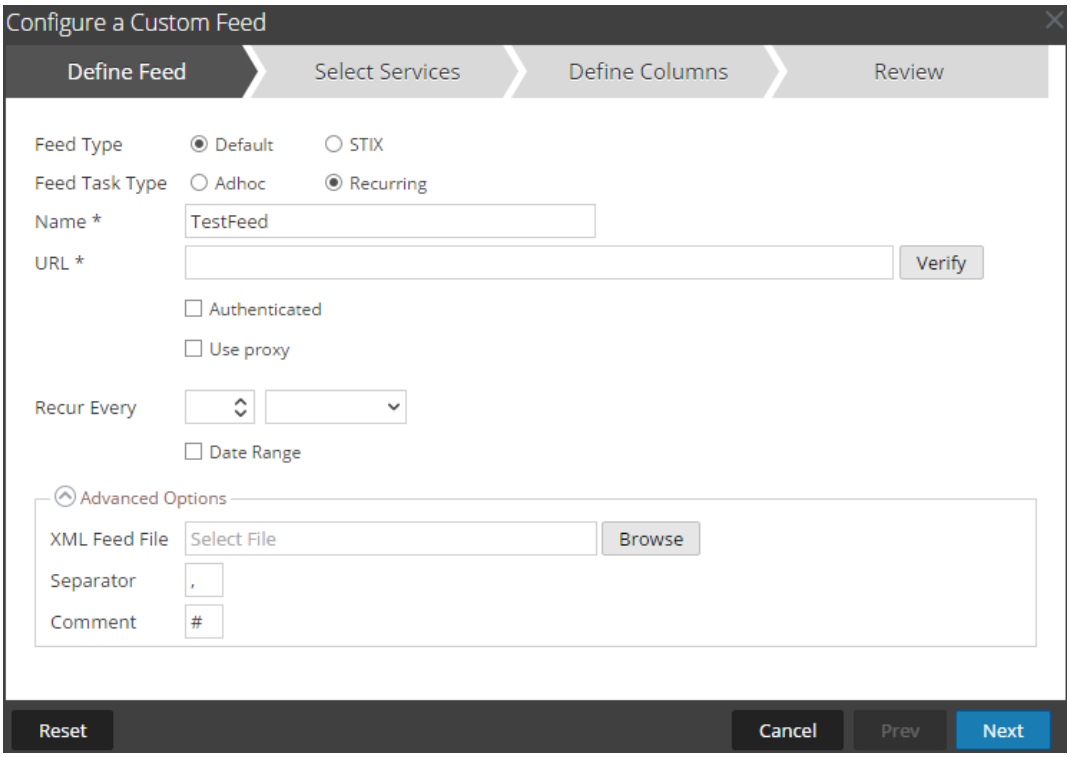
d. Le formulaire Sélectionner des services s'affiche. Voici un exemple de formulaire pour un feed basé sur un fichier de données de feed, sans fichier de définition de feed. Si vous définissez un feed basé sur un fichier de définition de feed, l'onglet Définir des colonnes n'est pas nécessaire.



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

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

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



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

   NetWitness Suite vérifie l'emplacement de stockage du fichier, de façon à ce que NetWitness Suite 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**.

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

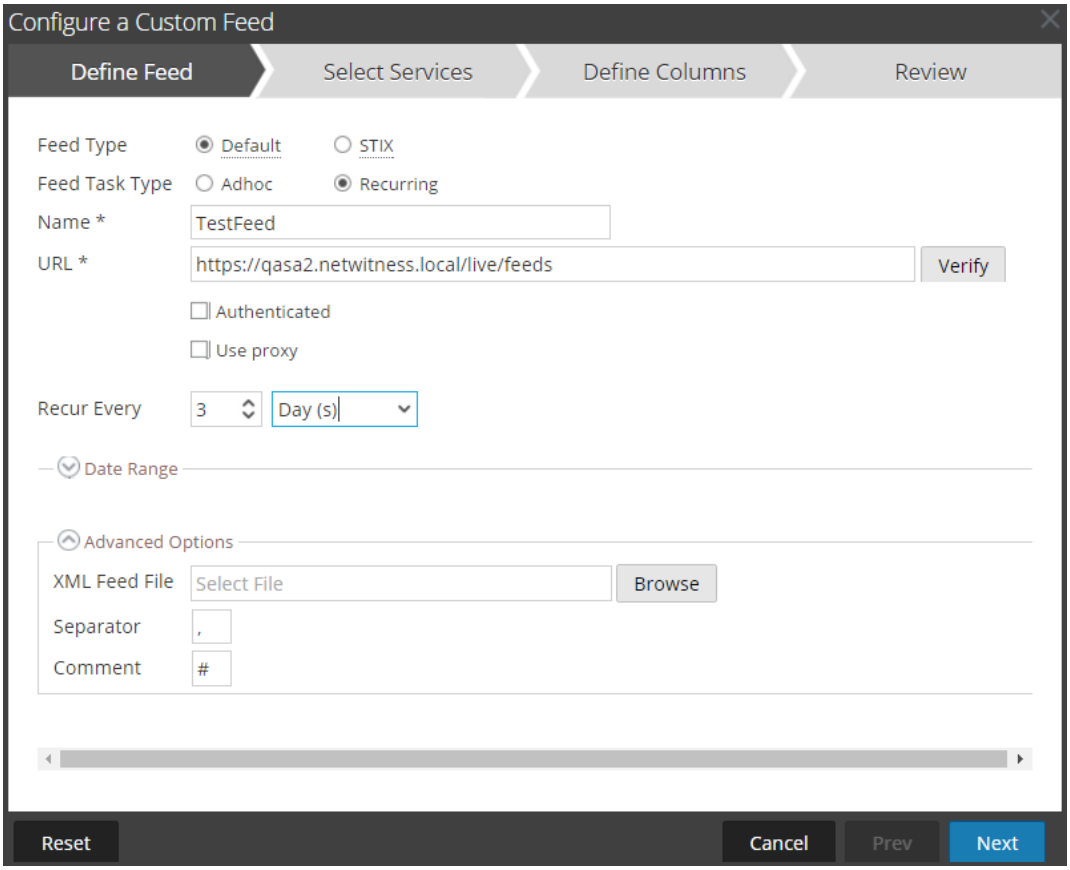
d. Si vous souhaitez que le serveur NetWitness Suite accède à l'URL du feed via un proxy, sélectionnez **Utiliser le proxy**. Pour plus d'informations sur la configuration d'un proxy, reportez-vous à la rubrique **Configurer un serveur proxy pour NetWitness Suite** dans le *Guide de configuration du 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.



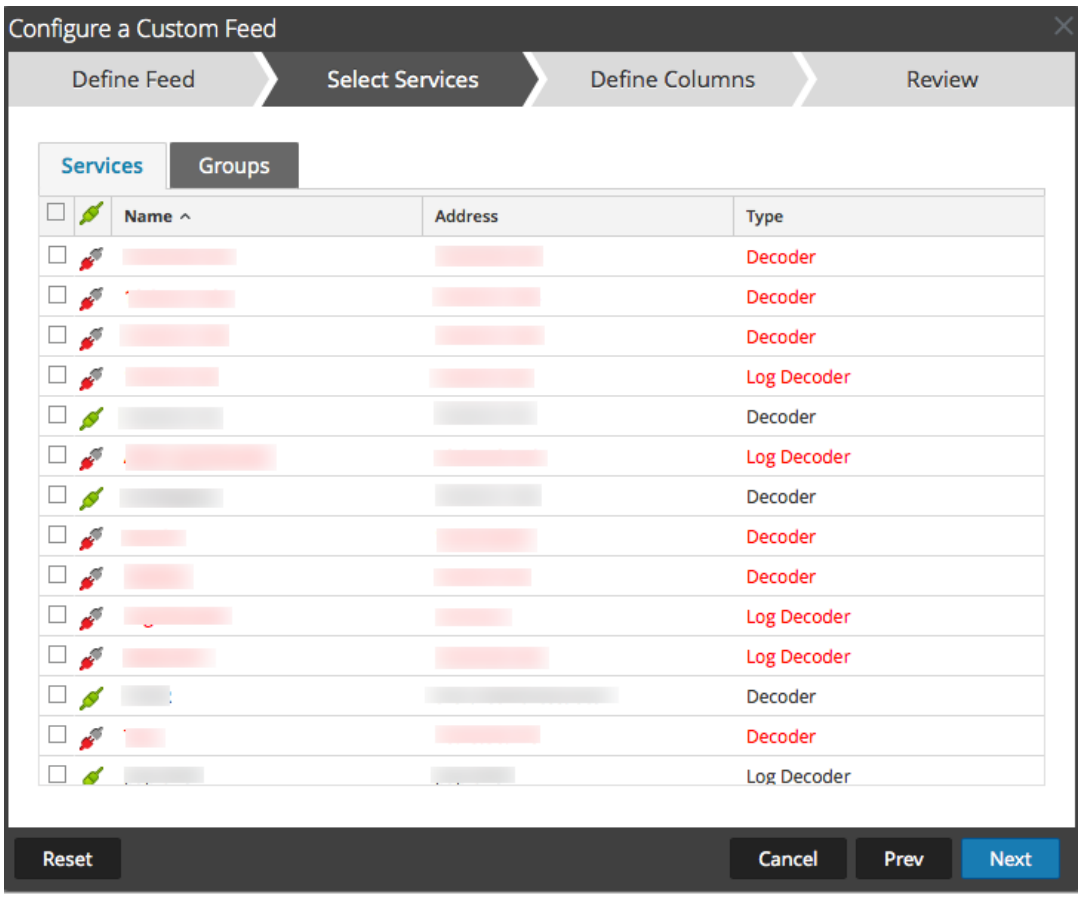
7. (Conditionnel) Si vous souhaitez définir un feed basé sur un fichier de feed XML :

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

     Les champs des Options avancées s'affichent.

   - Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le **Séparateur** (par défaut, il s'agit de la virgule), spécifiez les caractères du **Commentaire** utilisés dans le fichier de données de feed (la valeur par défaut est #) et cliquez sur **Suivant**.

Le formulaire Sélectionner des services s'affiche.



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

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

   b. Cliquez sur l'onglet **Groupes** et sélectionnez un groupe. Cliquez sur **Suivant**.

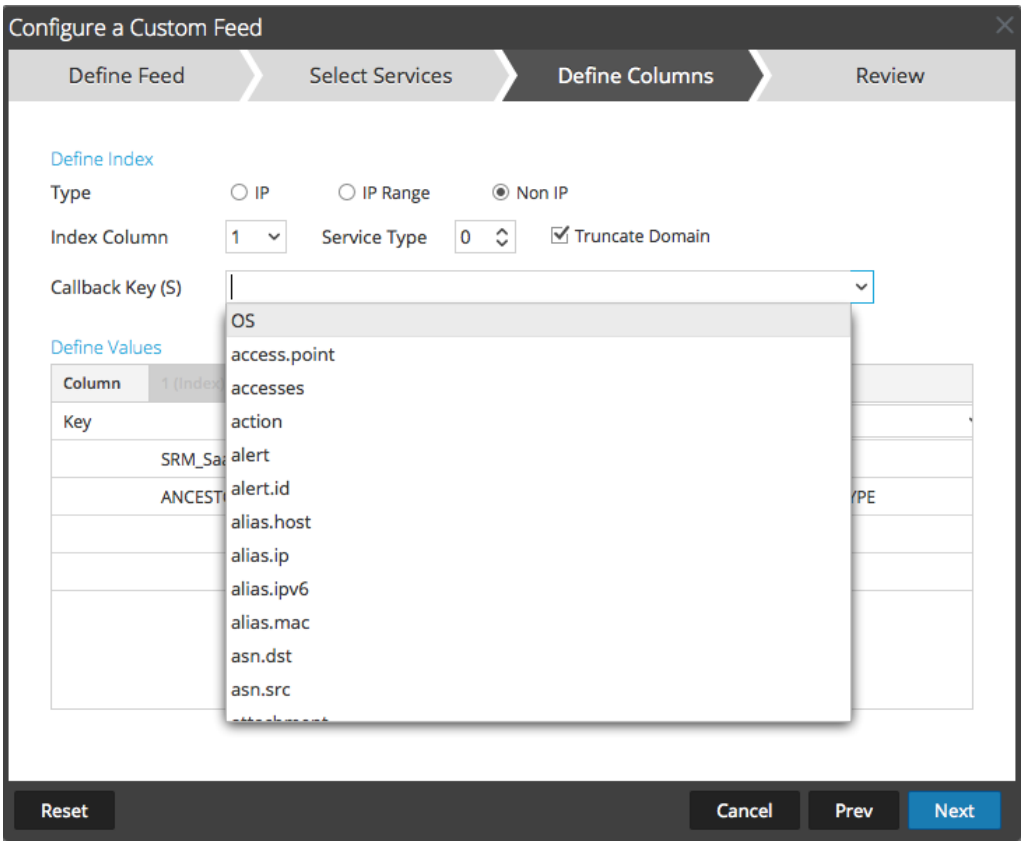
      Le formulaire Définir des colonnes s'affiche.

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

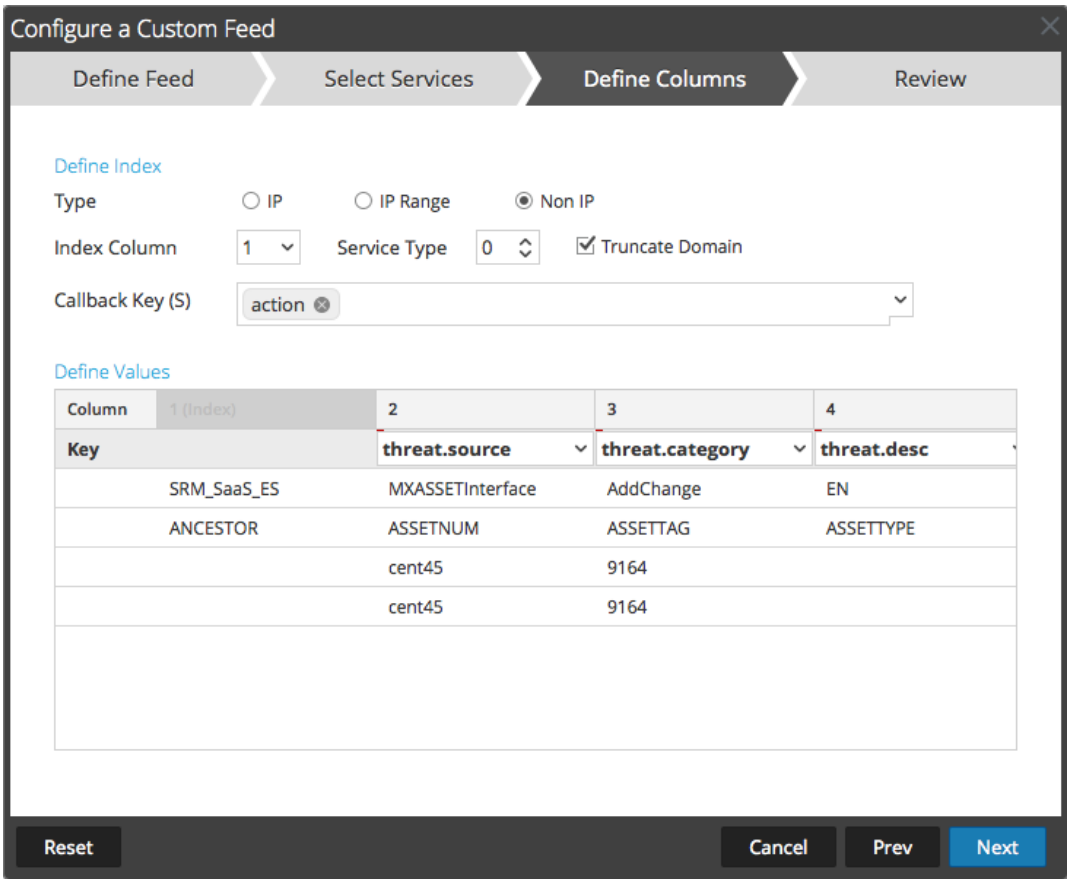
   a. Définir le type d'index : **IP**, **Plage IP** ou **Non IP**, et sélectionnez la colonne index.

   b. (Conditionnel) Si le type d'index est **IP** ou **Plage IP** et l'adresse IP est au format de notation CIDR, sélectionnez **CIDR**.

   c. (Conditionnel) Si le type d'index est **Non IP**, des paramètres supplémentaires s'affichent. Sélectionnez le type de service et **Clés de rappel**, et éventuellement, sélectionnez l'option **Tronquer le domaine**.

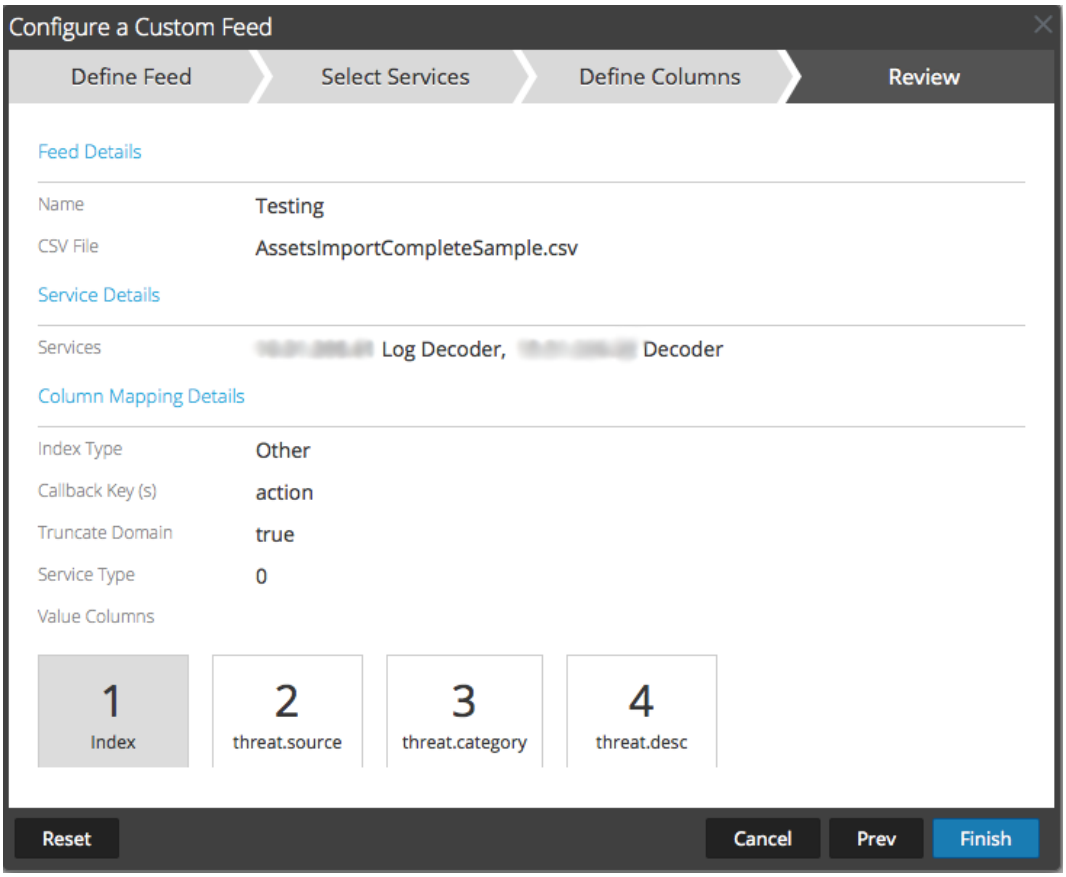


d. Sélectionnez la clé de langue à appliquer aux données de chaque colonne à partir de la liste déroulante. Le méta affiché dans la liste déroulante est basé sur les valeurs définies par le service. Si vous avez des compétences solides, vous pouvez également ajouter d'autres méta.



e. Cliquez sur **Suivant**.

   Le formulaire Révision s'affiche.



10. À tout moment avant de cliquer sur **Terminer**, vous pouvez :
    - Cliquez sur **Annuler** pour fermer l'assistant sans enregistrer votre définition de feed.
    - Cliquez sur **Réinitialiser** pour effacer les données de l'assistant.
    - Cliquez sur **Suivant** pour afficher le formulaire suivant (si ce n'est pas le dernier formulaire).
    - Cliquez sur **Précédent** pour afficher le formulaire précédent (si ce n'est pas le premier formulaire).

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

Feeds MetaCallback utilisant la plage d'index CIDR pour IPv4 et IPv6

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

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

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

.csv file:

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

.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator=","
comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0"
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

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

Créer un Feed STIX personnalisé

Vous pouvez créer un feed personnalisé à l'aide d'un fichier de données au format STIX ou .csv dans RSA NetWitness Suite.

Remarque : NetWitness Suite prend uniquement en charge les versions STIX (Structured Threat Information Expression) 1.0, 1.1 et 1.2.

Remarque : À partir de la version 10.6.1 ou d'une version supérieure, Security Analytics prend en charge le langage STIX (Structured Threat Information Expression).

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

Attention : Si un feed récurrent STIX est configuré et que vous mettez à jour Security Analytics de la version 10.6.x vers NetWitness Suite 11.0, vous devez reconfigurer le feed récurrent STIX.

Dans NetWitness Suite, le feed STIX (`.xml`) de type Indicateur ou Observable contenant des propriétés, telles que les adresses IP, les hachages de fichiers, les noms de domaine, les URI et les adresses électroniques sont pris en charge. Seules les valeurs de propriétés de l'opérateur Égal sont prises en charge. Les attributs tels que le type et le titre sont également lus à partir de STIX (`.xml`). Seul STIX (`.xml`) avec un seul STIX_Package est pris en charge.

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

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

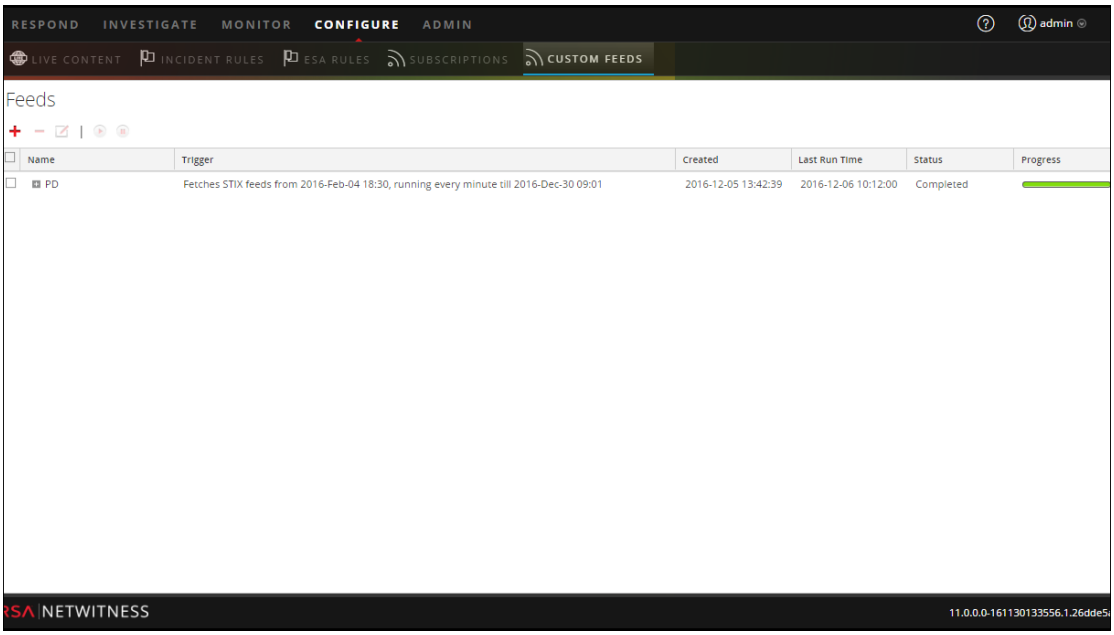
À l'exception du serveur TAXII, les données STIX peuvent également résider sur un serveur REST et vous pouvez extraire le fichier STIX depuis le serveur REST en fournissant l'URL du serveur REST. Par exemple, http://stixrestserver.internal.com.

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

Pour créer un feed STIX personnalisé :

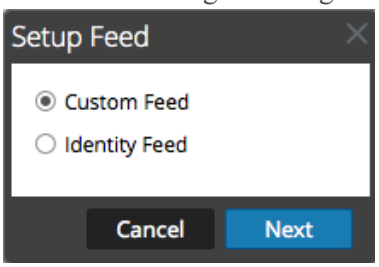
1. Accédez à **Configurer > Feeds personnalisés**.

   La vue Feeds s'affiche.



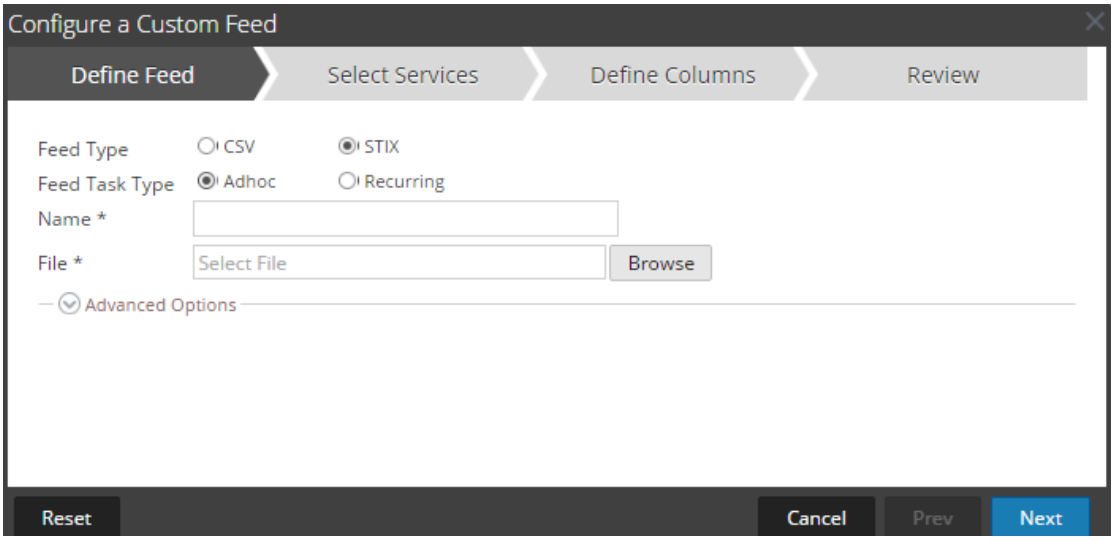
2. Dans la barre d'outils, cliquez sur +.

   La boîte de dialogue Configurer le feed s'affiche.



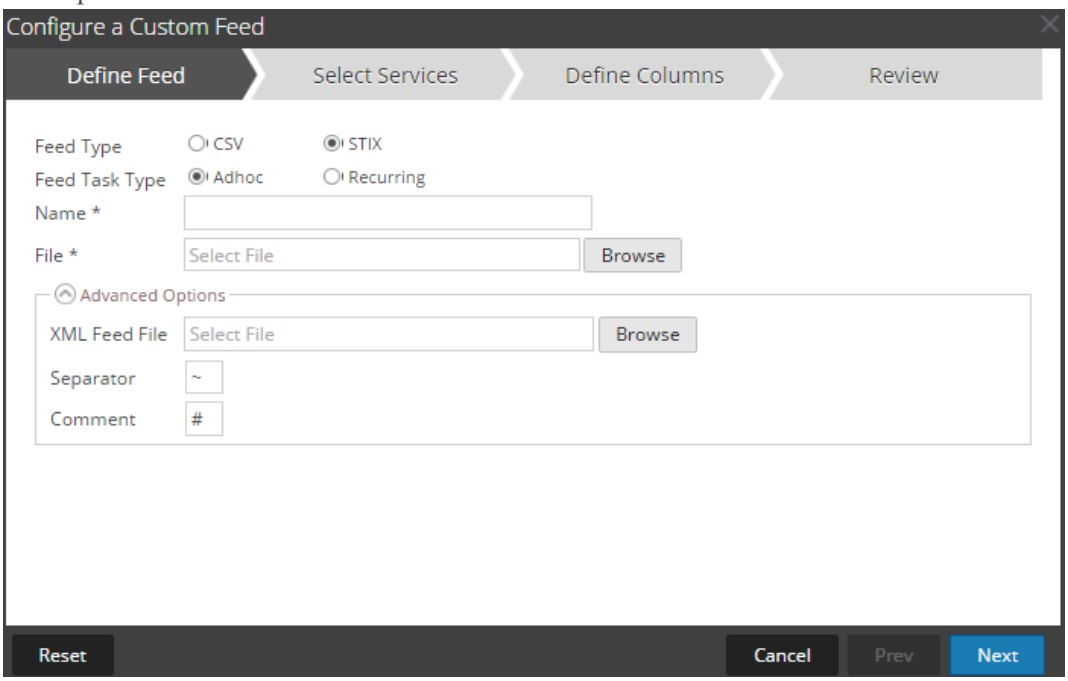
3. Pour sélectionner le type de feed, cliquez sur **Feed personnalisé**, puis sur **Suivant**.

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



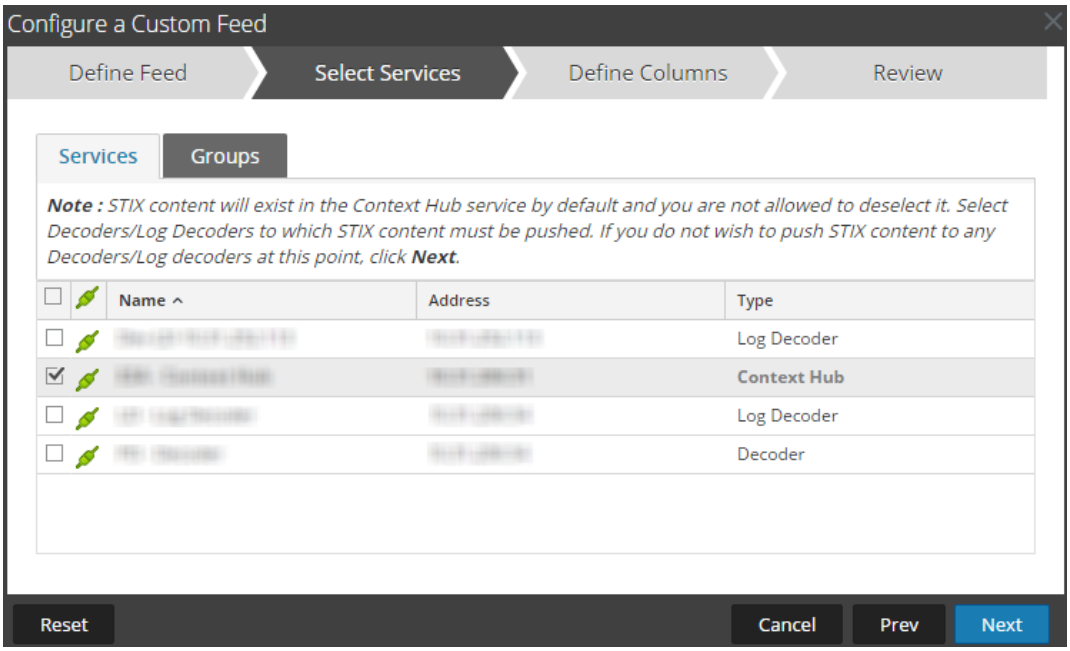
4. Pour définir un feed basé sur un fichier `.xml` au format STIX, sélectionnez **STIX** dans le champ **Type de feed**.
5. Pour définir une tâche de feed à la demande qui s'exécute une fois, sélectionnez **Ad hoc** dans le champ **Type de tâche par défaut** et procédez d'une des manières suivantes :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

Les Options avancées s'affichent.



c. Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le **Séparateur** (par défaut, il s'agit de la virgule) et spécifiez les caractères du **Commentaire** utilisés dans le fichier de données de feed (la valeur par défaut est #) et cliquez sur **Suivant**.

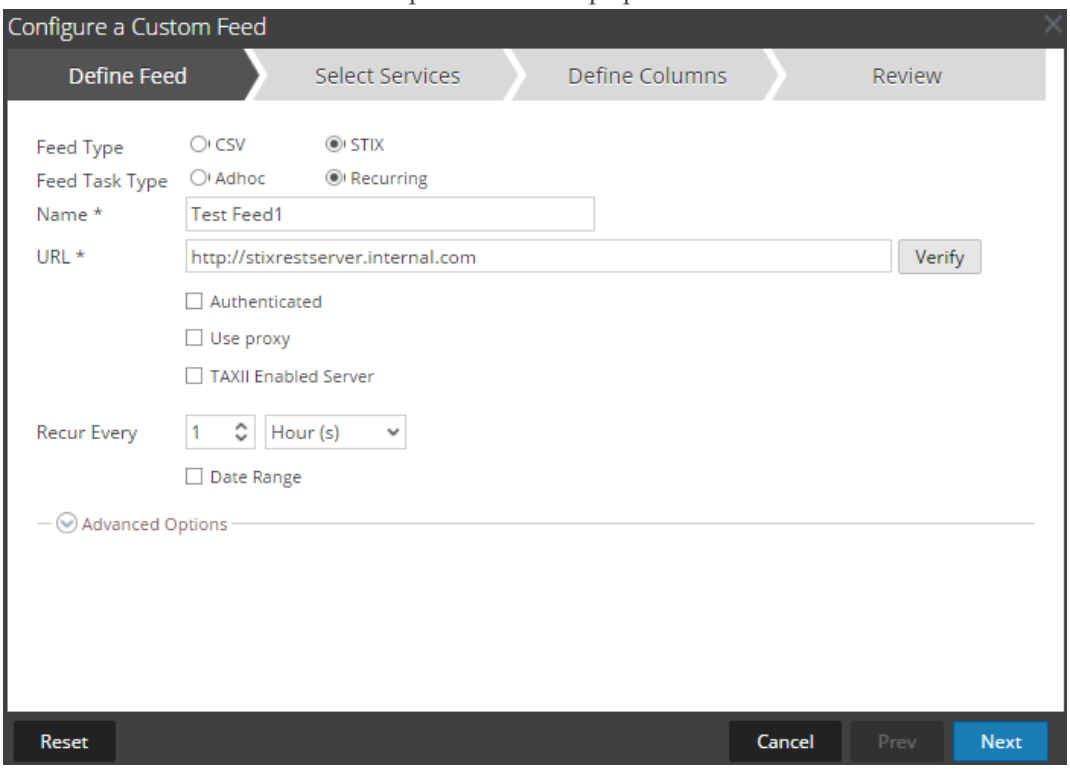
d. Le formulaire Sélectionner des services s'affiche. Voici un exemple de formulaire pour un feed basé sur un fichier de données de feed, sans fichier de définition de feed. Si vous définissez un feed basé sur un fichier de définition de feed, l'onglet Définir des colonnes n'est pas nécessaire.



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

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

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

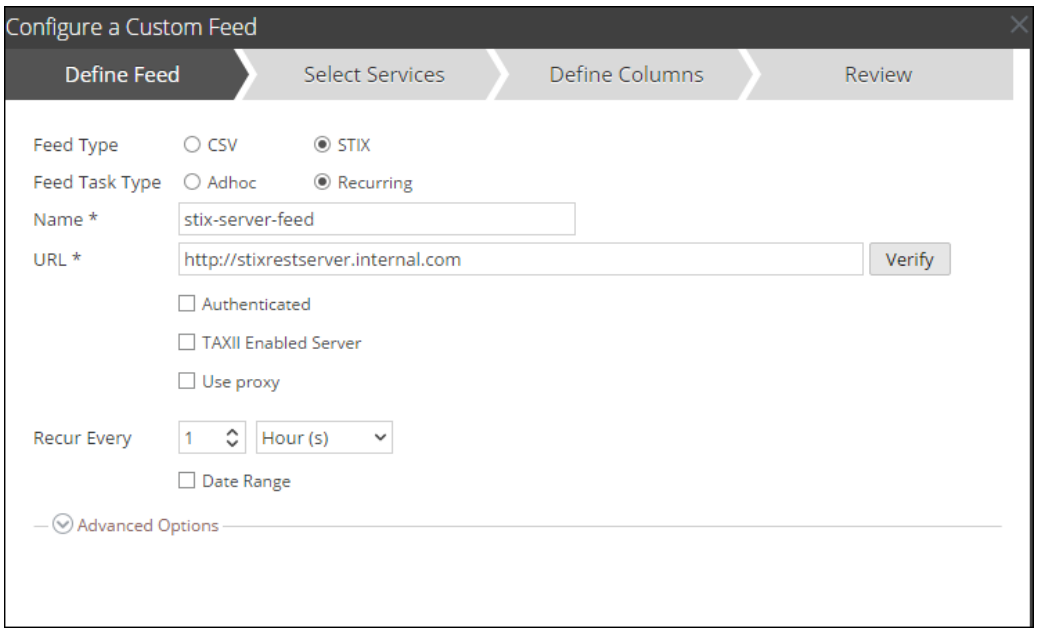


b. Dans le champ **URL**, saisissez l'un des éléments suivants :

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

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

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



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

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

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

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

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

f. Sélectionnez **Serveur TAXII activé**, si vous souhaitez sélectionner une collecte TAXII dans la liste.
Pour une adresse URL valide, une ou plusieurs collectes TAXII contenant le fichier de données STIX s'affiche en fonction de vos informations d'identification. Sélectionnez la collecte TAXII requise dans la liste. Une seule collecte peut être ajoutée à partir d'un serveur TAXII pour un feed.

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

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

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

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

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

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

j. Pour définir la période pour l'exécution récurrente du feed, spécifiez la **Date de début** et l'heure, ainsi que la **Date de fin** et l'heure. La date de début doit être définie à partir du moment où vous souhaitez extraire les données. Assurez-vous que la **Date de début** n'est pas antérieure à 180 jours à partir d'aujourd'hui.

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

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

  Les champs des Options avancées s'affichent.

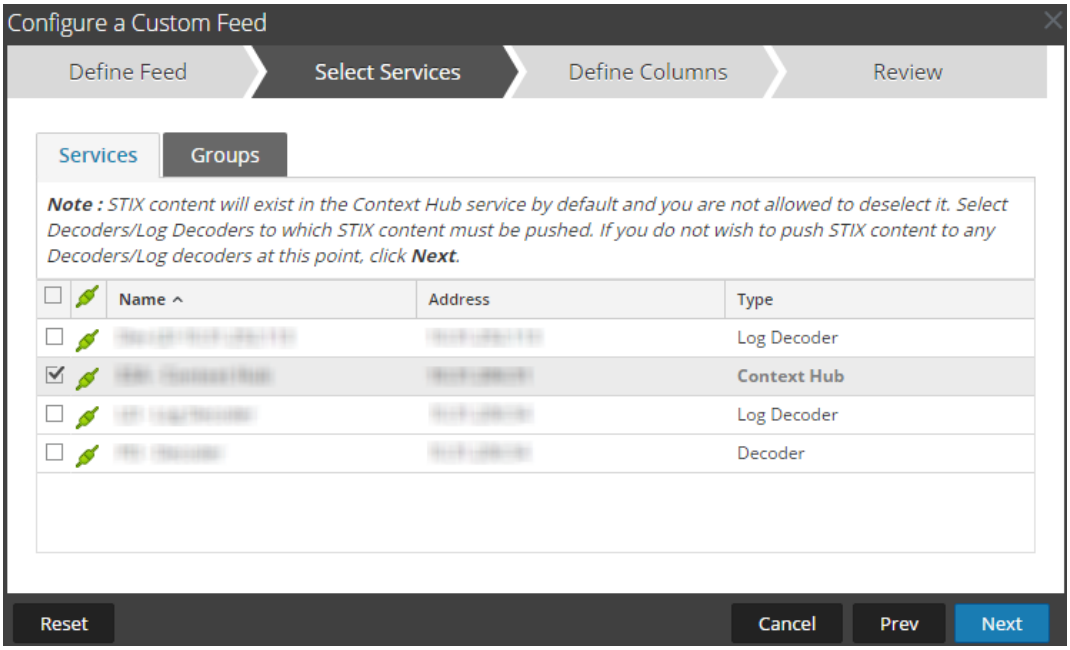
- Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez le **Séparateur** (par défaut, il s'agit de la virgule), spécifiez les caractères du **Commentaire** utilisés dans le fichier de données de feed (la valeur par défaut est #).

- Dans le champ **Supprimer les données STIX antérieures à**, indiquez le nombre de jours durant lesquels les packages STIX extraits du serveur TAXII doivent être stockés. Les packages STIX antérieurs au nombre de jours spécifiés sont supprimés automatiquement.
- Cliquez sur **Suivant**.
  Le formulaire Sélectionner des services s'affiche.

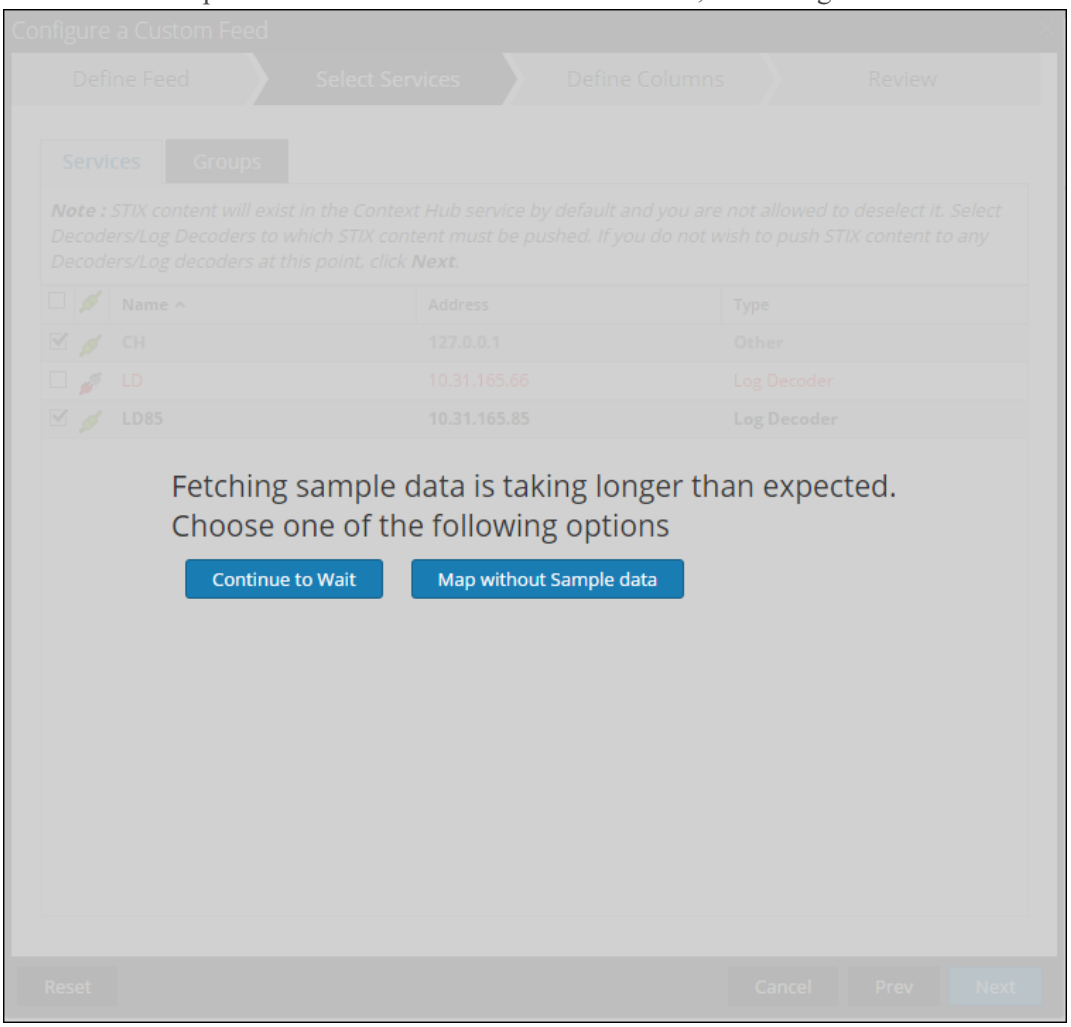
8. Pour identifier les services sur lesquels déployer le feed, effectuez l'une des opérations suivantes :

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

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



Si les données à partir du serveur STIX sont volumineuses, le message suivant s'affiche :

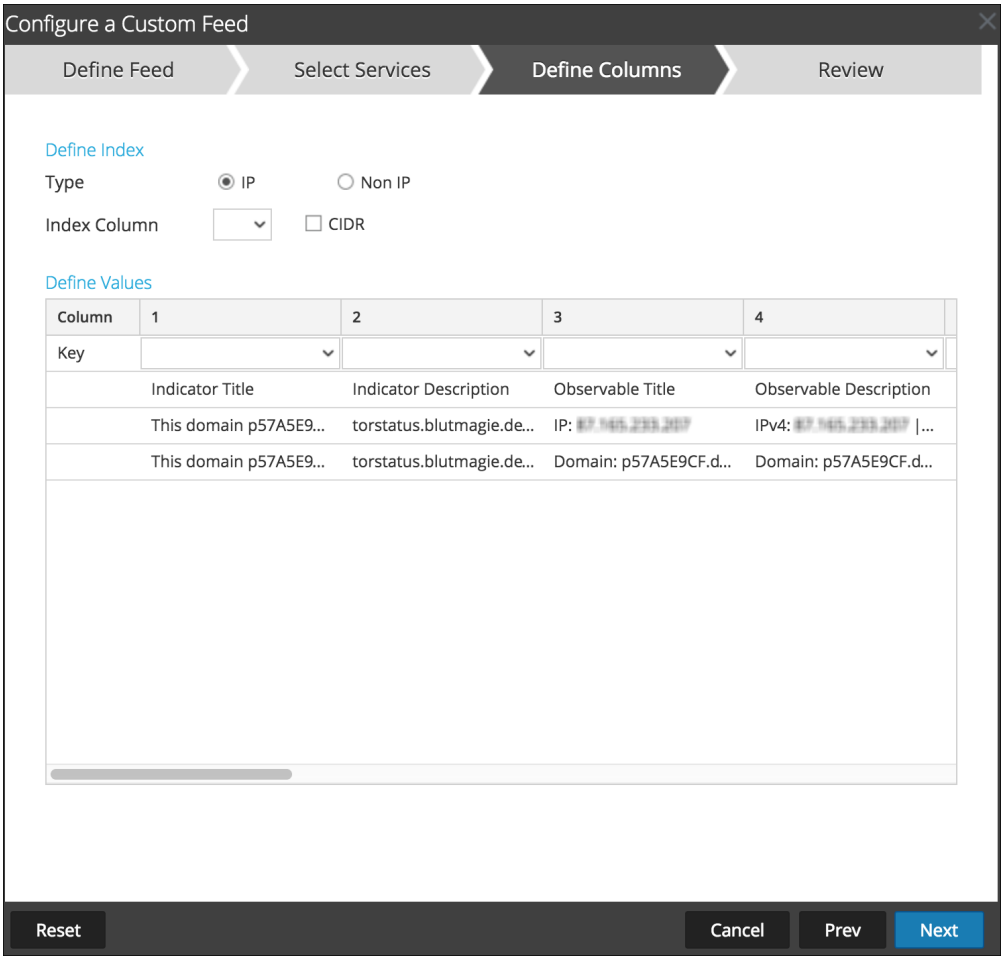


- Si vous cliquez sur **Continuer à attendre**, il continue à attendre jusqu'à ce que l'échantillon de données soit extrait ou que le délai expire (10 minutes), selon la première éventualité. Dans le cas d'expiration du délai, aucune donnée d'échantillon n'est récupérée même après 10 minutes.
- Si vous cliquez sur **Mapper sans les échantillons de données**, la colonne de mappage s'affiche sans les échantillons de données.

Le formulaire Définir des colonnes s'affiche.

9. Pour mapper les colonnes dans le formulaire Définir des colonnes :
   a. Définir le type d'index : **IP**, **Plage IP** ou **Non IP**, et sélectionnez la colonne index.
   b. (Conditionnel) Si le type d'index est **IP** ou **Plage IP** et l'adresse IP est au format de notation CIDR, sélectionnez **CIDR**.

c. (Conditionnel) Si le type d'index est **Non IP**, des paramètres supplémentaires s'affichent. Sélectionnez le type de service et **Clés de rappel**, et éventuellement, sélectionnez l'option **Tronquer le domaine**.



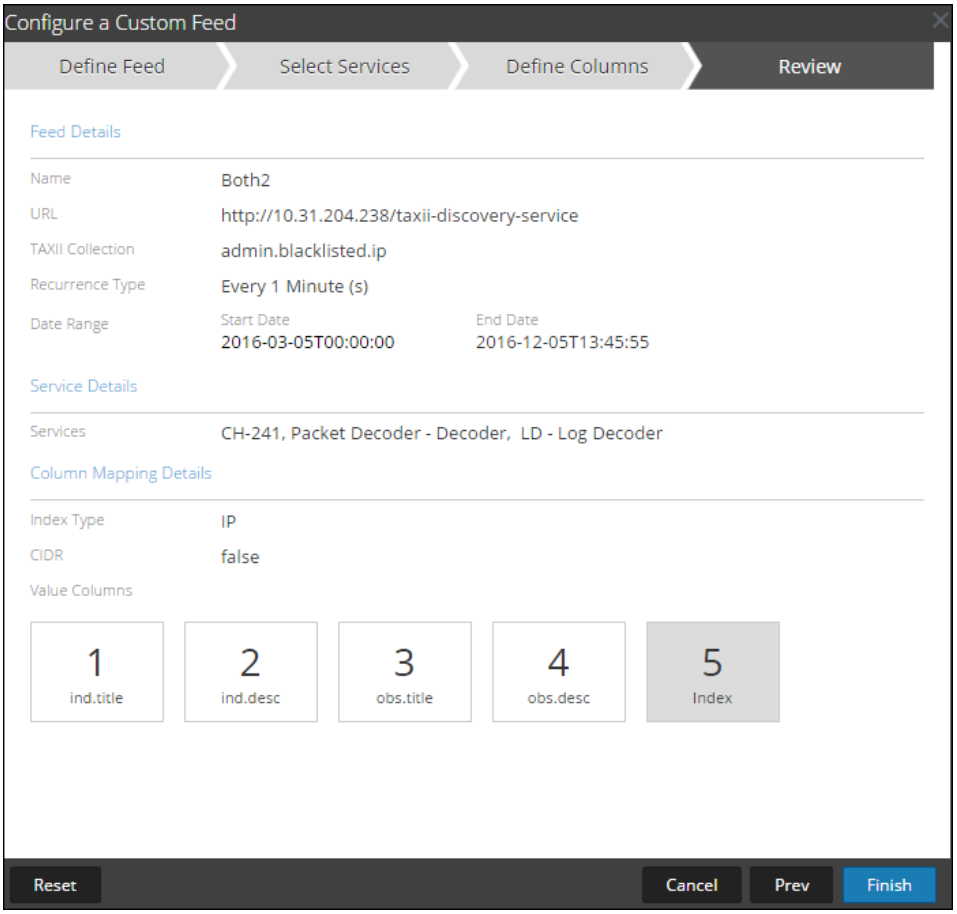
Remarque :
- Si le **type d'Index** est Non IP, vous pouvez sélectionner plusieurs colonnes d'index dans les **colonnes d'Index**. Les valeurs de toutes les colonnes sélectionnées sont fusionnées dans la première colonne d'index que vous avez sélectionnée et les valeurs fusionnées sont transférées vers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

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

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

e. Cliquez sur **Suivant**.

Le formulaire Révision s'affiche.

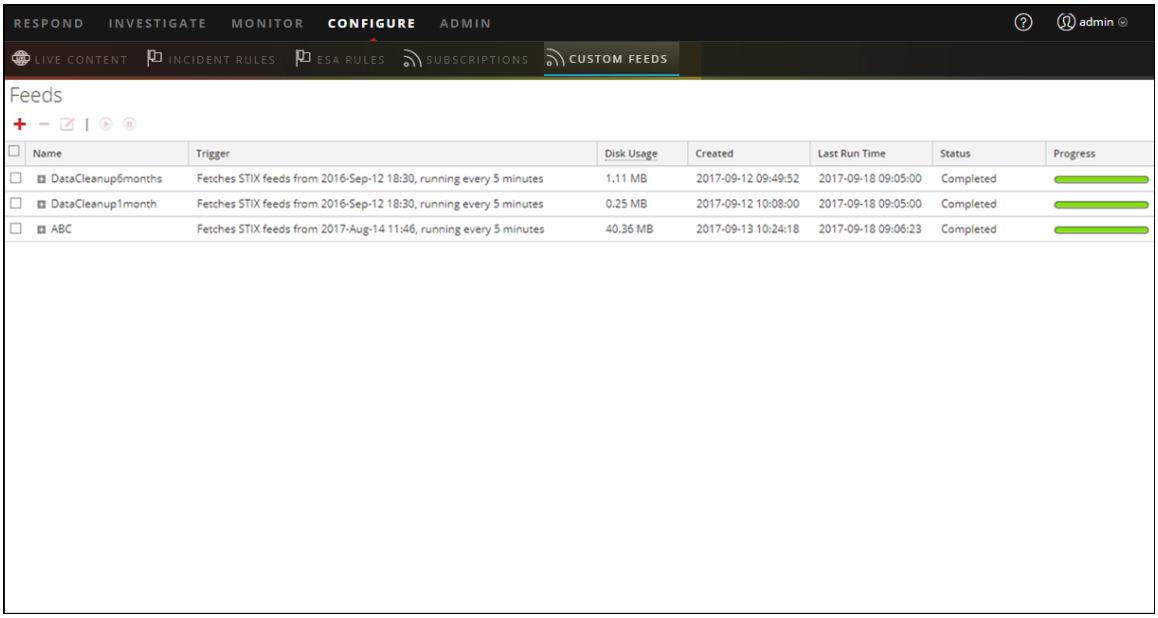


10. À tout moment avant de cliquer sur **Terminer**, vous pouvez :

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

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

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



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

Feeds MetaCallback utilisant la plage d'index CIDR pour IPv4 et IPv6

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

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

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

`.csv file:`

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

`.xml file:`

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," 
comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0" 
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

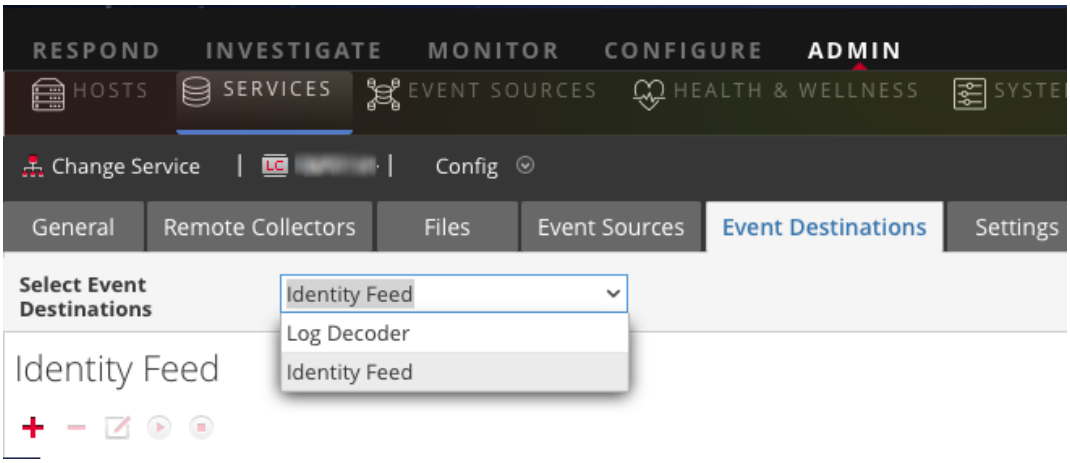
Remarque : Pour configurer une plage d'index CIDR pour les feeds avec un ou plusieurs MetaCallbacks de type de valeur IPv4 ou IPv6, le champ du type d'index DOIT contenir un attribut de plage avec range="cidr". En outre, la configuration des plages d'index « cidr » pour les feeds avec MetaCallbacks de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

Créer et gérer 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.

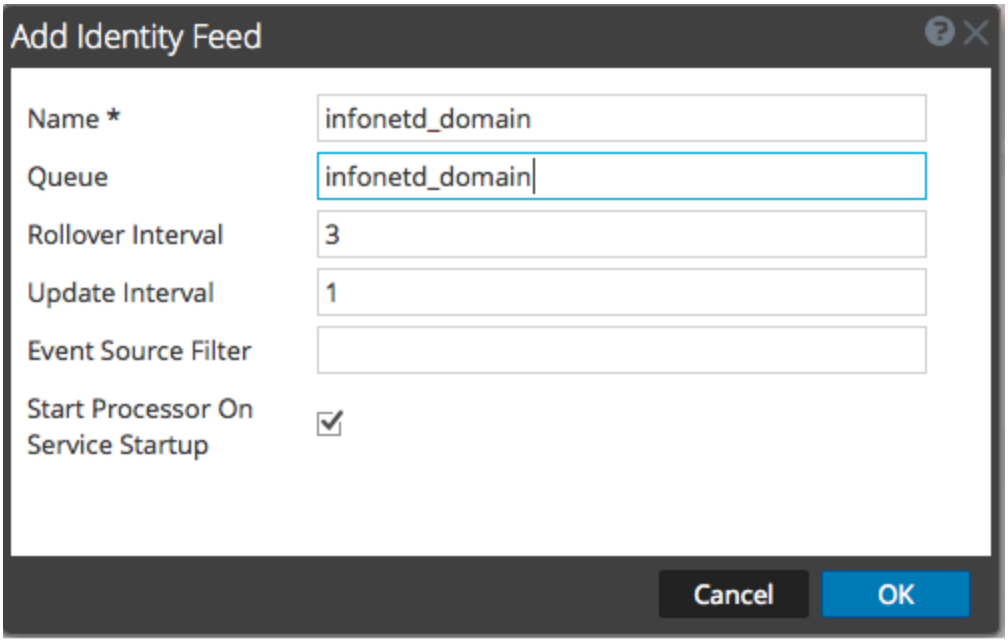
Pour créer un feed d'identité :

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



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

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



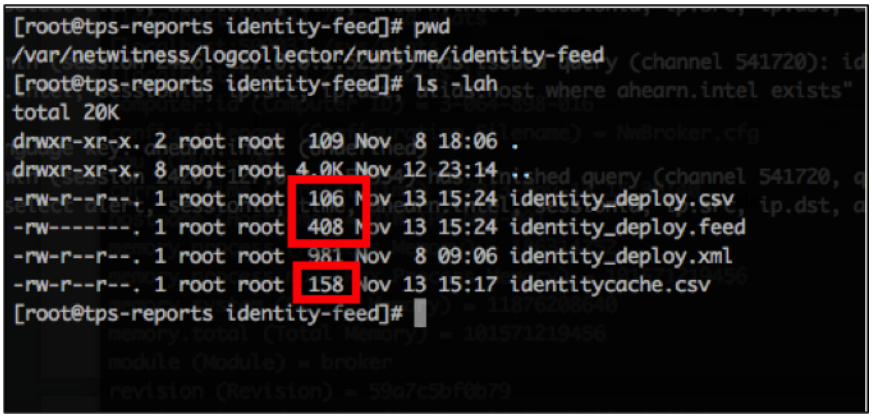
e. Cliquez sur **OK**.

2. Testez la génération de messages.

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

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

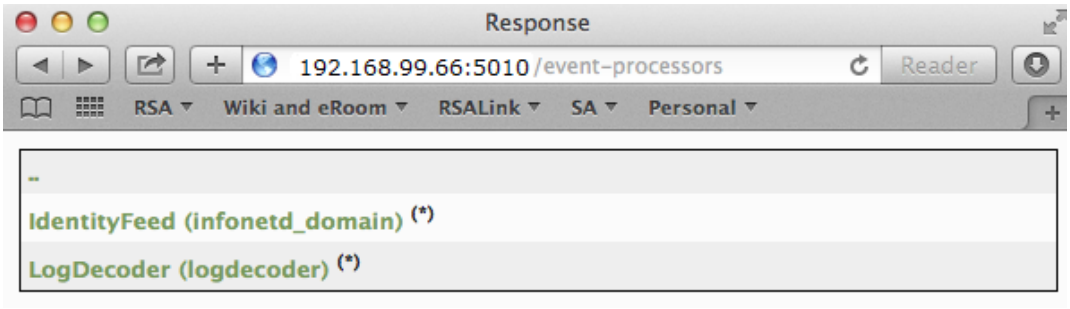
et vérifiez que les fichiers `Identity_deploy` se remplissent de données.



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

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

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

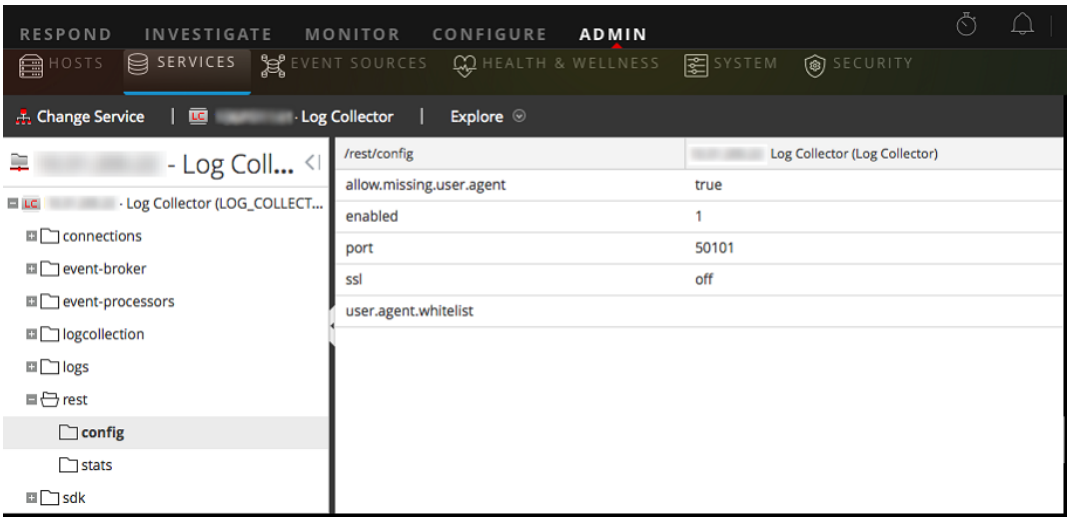


Notez que l'écran affiche le nom de l'identité du feed que vous avez créé précédemment (`infonetd_domain`, dans cet exemple).

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

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

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



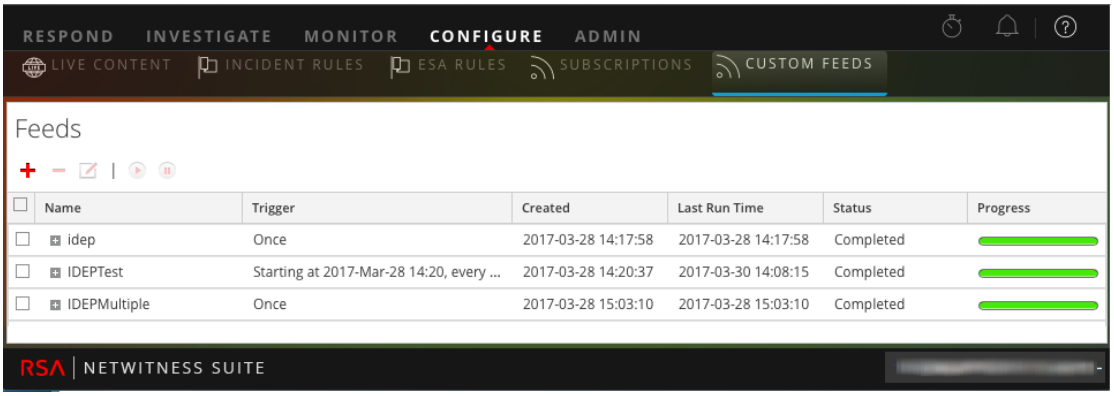
Pour que REST soit actif, **activé** doit être défini sur **1**.

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

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

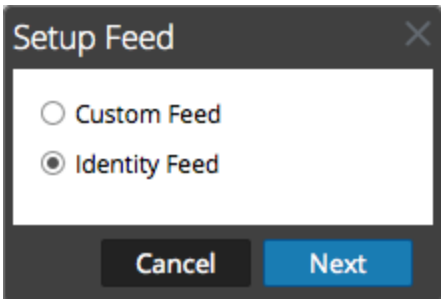
3. Accédez à **CONFIGURER > Live Content > Feeds personnalisés**.

La grille Feeds s'affiche.



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

La boîte de dialogue Configurer le feed s'affiche.



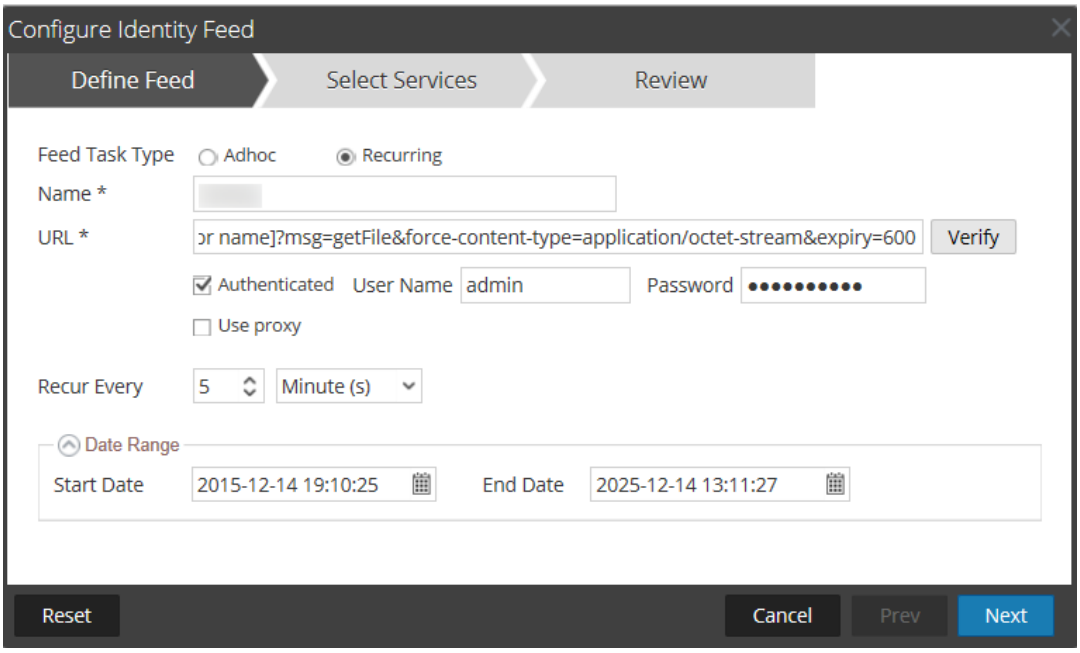
5. Assurez-vous que **Identity Feed** est sélectionné, puis cliquez sur **suivant**.

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

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

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

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



Remarque : RSA NetWitness Suite vérifie l'emplacement de stockage du fichier afin que Security Analytics puisse rechercher automatiquement le dernier fichier avant chaque récurrence.

7. Renseignez et vérifiez le champ URL.

a. Dans le champ **URL**, saisissez l'URL de l'emplacement du fichier de données de feed. Il s'agit de l'interface API REST qui a été configurée précédemment. Vous devez avoir connaissance des informations suivantes pour construire l'URL :

   - L'adresse IP du Log Collector utilisée pour créer le fichier Identity Feed.
   - Le nom d'identité de la file d'attente, tel que défini dans l'étape 2c.
   - Si SSL est activé ou non sur le port REST du Log Collector, tel que défini dans l'étape 2f.

   Vous créez cette valeur comme suit :

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

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

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

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

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

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

   Exemple de mauvaise connexion :

   ```
   * About to connect() to 192.168.99.66 port 50105 (#0)
   * Trying 192.168.99.66... No route to host
   * couldn't connect to host
   ```

```
* Closing connection #0

curl: (7) couldn't connect to host

Example of Good connection:

* About to connect() to 192.168.99.66 port 50105 (#0)

* Trying 192.168.99.66... connected

* Connected to 192.168.99.66 (192.168.99.66) port 50105
(#0)

> GET / HTTP/1.1

> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2

> Host: 192.168.99.66:50105

> Accept: */*

>

< HTTP/1.1 401 Unauthorized

< Content-Length: 71

< Connection: Keep-Alive

< Pragma: no-cache

< Expires: -1

< Cache-Control: no-cache, no-store, must-revalidate

< WWW-Authenticate: Basic realm="NetWitness"

< Content-Type: text/xml; charset=utf-8

<

<?xml version="1.0" encoding="utf-8"?>

<error>401 Unauthorized</error>

* Connection #0 to host 192.168.99.66 left intact

* Closing connection #0
```

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

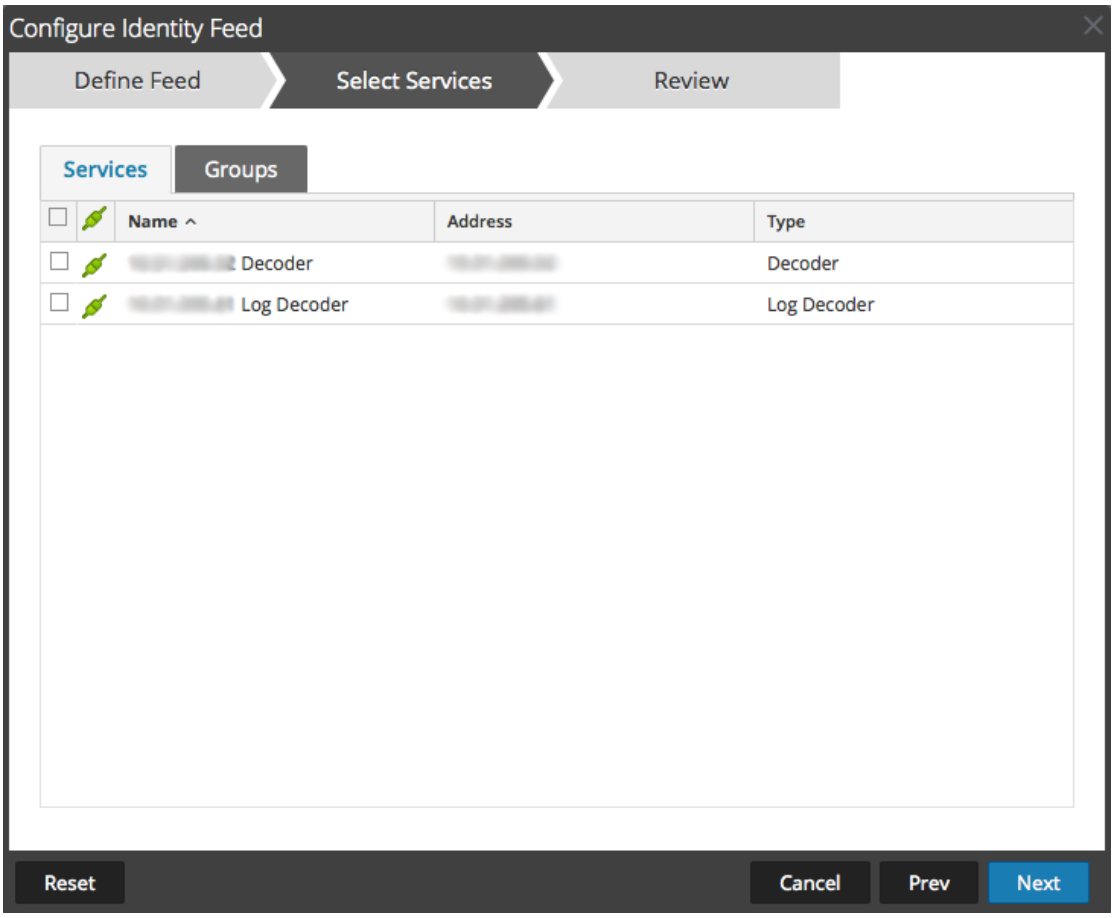
Pour afficher les comptes disponibles, accédez à **ADMIN > Services > <Log Collector en cours de configuration> > Actions > Vue > Sécurité**.

Sous le tableau des utilisateurs, tous les utilisateurs qui peuvent être utilisés dans cette étape s'affichent. Pour une sécurité renforcée, il est recommandé de créer un compte utilisateur spécifiquement pour cette configuration et a n'utiliser nulle part ailleurs dans l'environnement. Pour plus de détails, consultez la section « Ajouter un utilisateur et attribuer un rôle » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*. (Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.)

9. Pour définir l'intervalle de récurrence, effectuez l'une des opérations suivantes :
   - Spécifiez le nombre de minutes, d'heures ou de jours entre les récurrences du champ.
   - Pour définir la période pour l'exécution récurrente du feed, spécifiez la **Date de début** et l'heure, ainsi que la **Date de fin** et l'heure.
10. Si vous utilisez le chiffrement SSL, vous devez installer le certificat SSL de l'API REST pour le Log Collector dans l'interface utilisateur du serveur Security Analytics. Pour plus d'informations, reportez-vous à la rubrique Importer le certificat SSL.

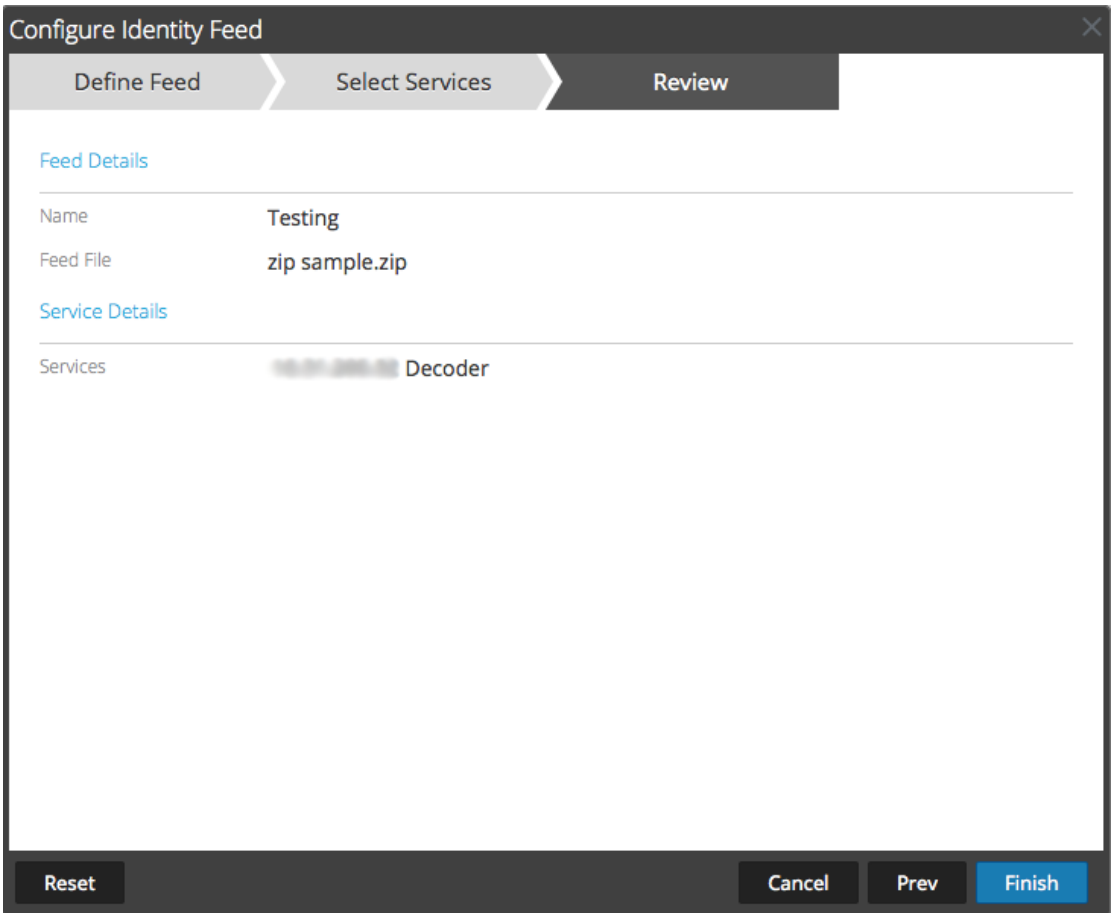
    Si, après l'importation du certificat SSL, la vérification de l'URL échoue à nouveau, consultez la section Impossible de vérifier l'URL du feed d'identité.
11. Cliquez sur **Vérifier** pour vérifier votre configuration du feed identité avant de procéder au formulaire Sélectionner des services.
12. Cliquez sur **Suivant**.

    Le formulaire Sélectionner des services s'affiche.



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

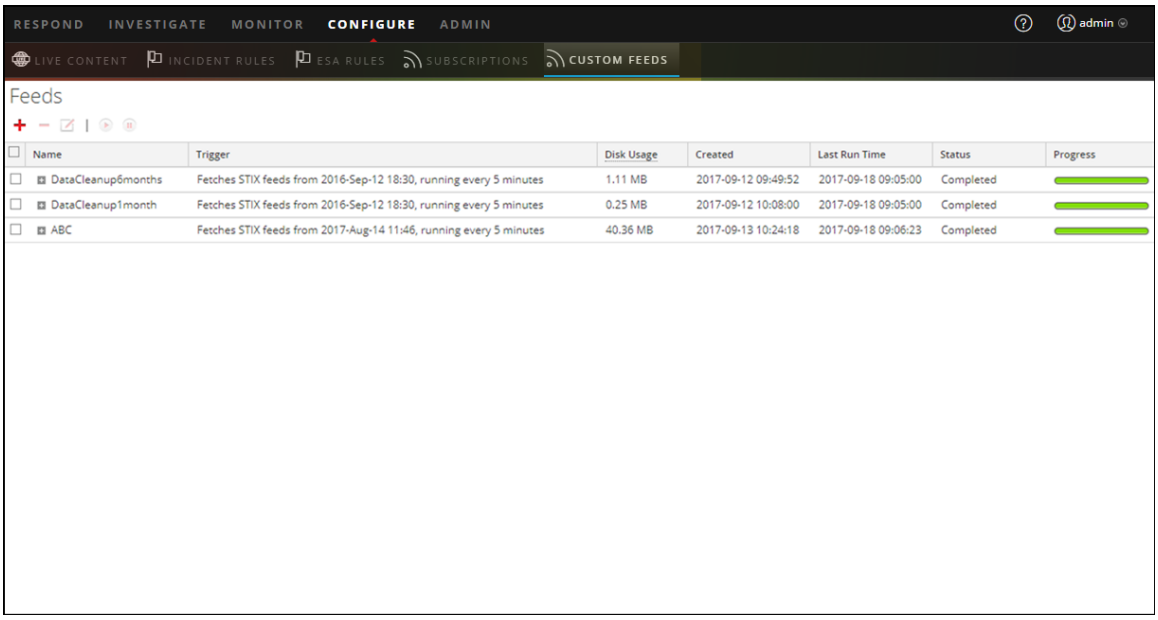
    Le formulaire Révision s'affiche.



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.

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

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



Importer le certificat SSL

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

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

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

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

   Par exemple :

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

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

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

   Par exemple :

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

3. Le système demande un mot de passe. Saisissez le mot de passe du magasin de clés sur l'interface utilisateur du serveur Security Analytics, et non celui du magasin de clés jetty. Le mot de passe par défaut est **changeit**.
4. Redémarrez **jettysrv** pour autoriser jetty à lire le nouveau certificat dans la zone de stockage.

Impossible de vérifier l'URL du feed d'identité

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

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

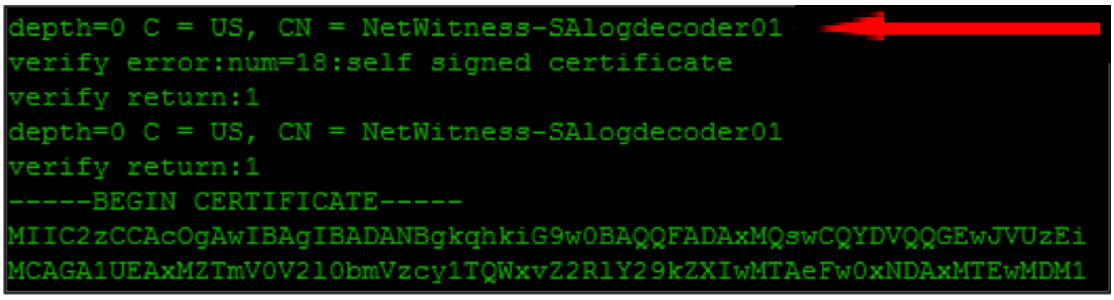
1. Ouvrez une session SSH sur l'interface utilisateur du serveur Security Analytics.
2. Exécutez la commande suivante pour sortir le nom CN du certificat SSL :

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

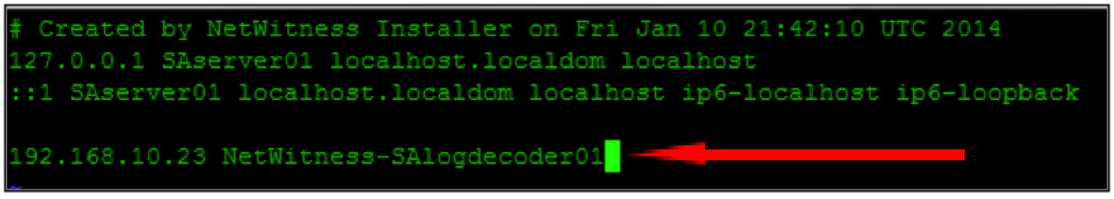
   Exemple :

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

3. Récupérer le nom CN du certificat SSL.



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



5. Redémarrez les services de réseau sur l'appliance.
6. Confirmez que le nom placé dans le fichier **/etc/hosts** est utilisé au lieu du nom de domaine

complet ou l'adresse IP de l'URL du feed d'identité.

7. Vérifiez à nouveau l'URL du feed d'identité.

Examiner un feed d'identité

Un feed d'identité effectue le suivi des événements de connexion interactive à partir d'un système d'exploitation Windows. Les feeds d'identité n'effectuent pas le suivi des événements de déconnexion interactifs.

Pour qu'un feed d'identité traite des événements et y appose des balises, les événements doivent être collectés à l'aide d'un module Windows Log Collection où un Contrôleur de domaine actif/Contrôleur de nondomaine est configuré. Remarquez que les feeds d'identité ne peuvent être traités que via un Processeur d'événements Identity Feed.

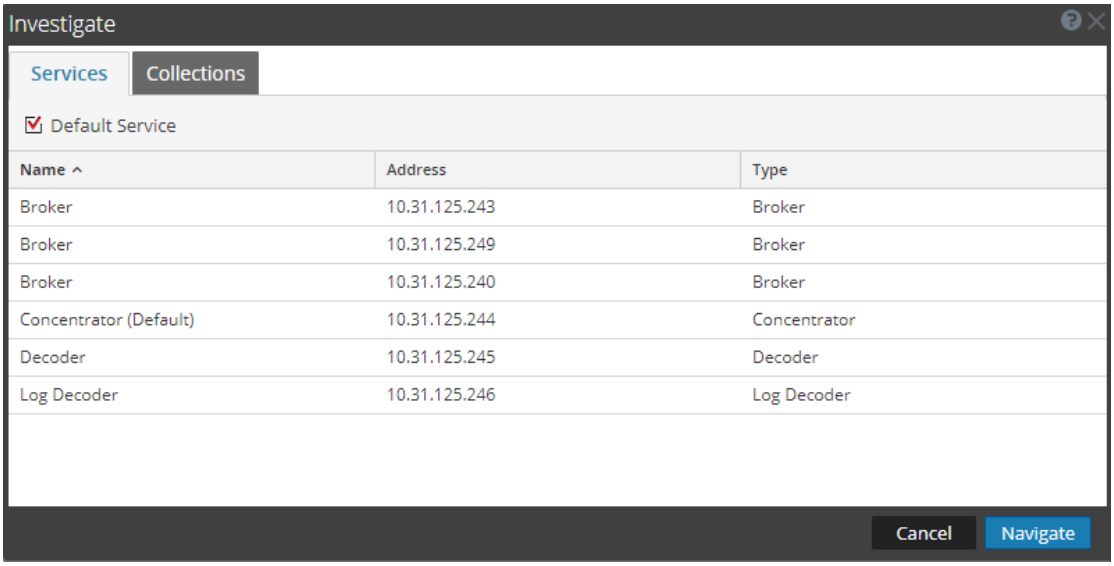
Remarque : Un feed d'identité n'effectue le suivi que d'un fichier log à la fois. Si deux utilisateurs se connectent à un système en même temps, les données du second utilisateur remplacent celles du premier dans le feed d'identité.

Lorsque vous avez créé un feed d'identité, vous pouvez afficher les résultats en examinant le feed.

Pour examiner un feed d'identité configuré :

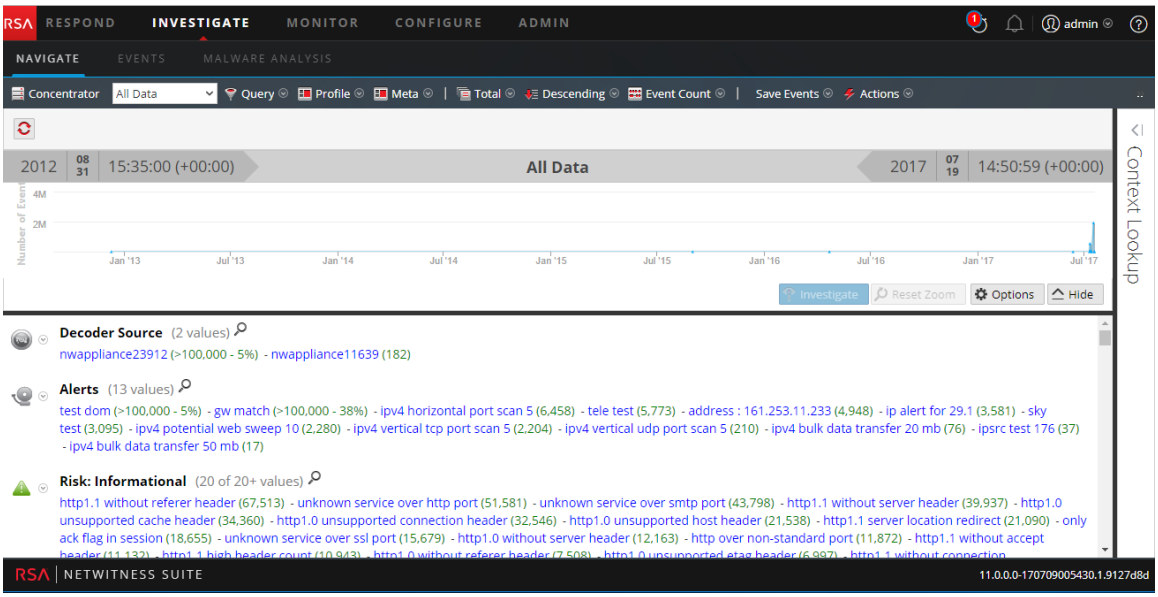
1. Accédez à **Enquêter > Naviguer.**

   Si aucun service par défaut n'est sélectionné, la boîte de dialogue Enquêter s'affiche.



2. Sélectionnez un service, généralement un Concentrator, puis cliquez sur **Naviguer**.
3. Sélectionnez **Charger les valeurs** pour récupérer les métadonnées.

Dans le panneau Valeurs, faites défiler pour trouver les clés méta indiquées dans l'illustration suivante.



Le feed d'identité donne des informations sur les Decoders et Log Decoders sélectionnés. Il associe les données IP de l'hôte entre le système d'exploitation Windows et l'utilisateur qui se connecte à cet hôte afin de baliser tous les logs associés à cette adresse IP et de procéder à l'enquête.

Modifier un feed

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

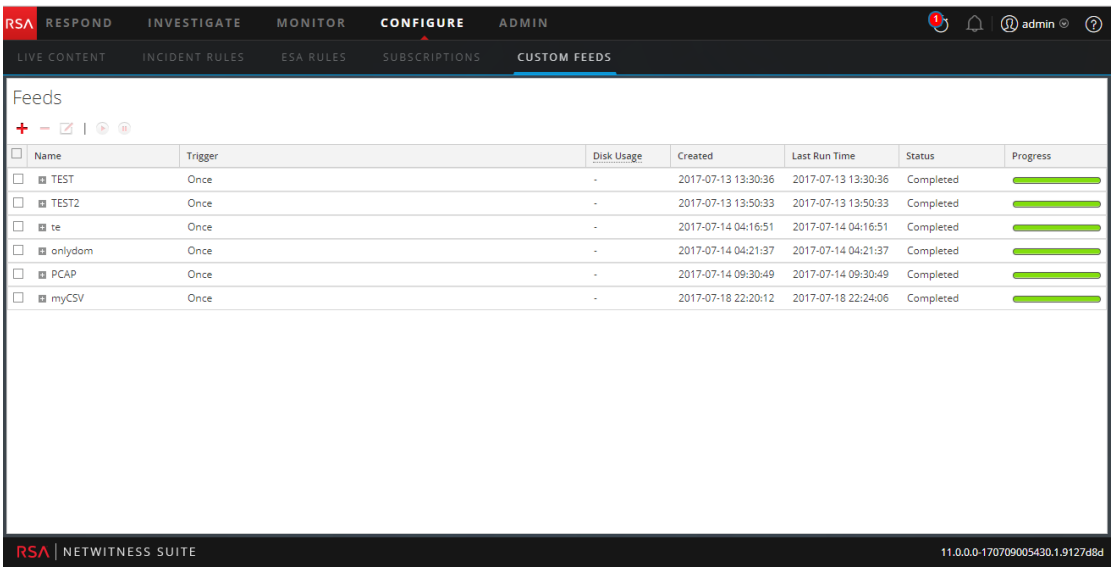
L'exécution de cette procédure aura pour résultat :

- 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 :

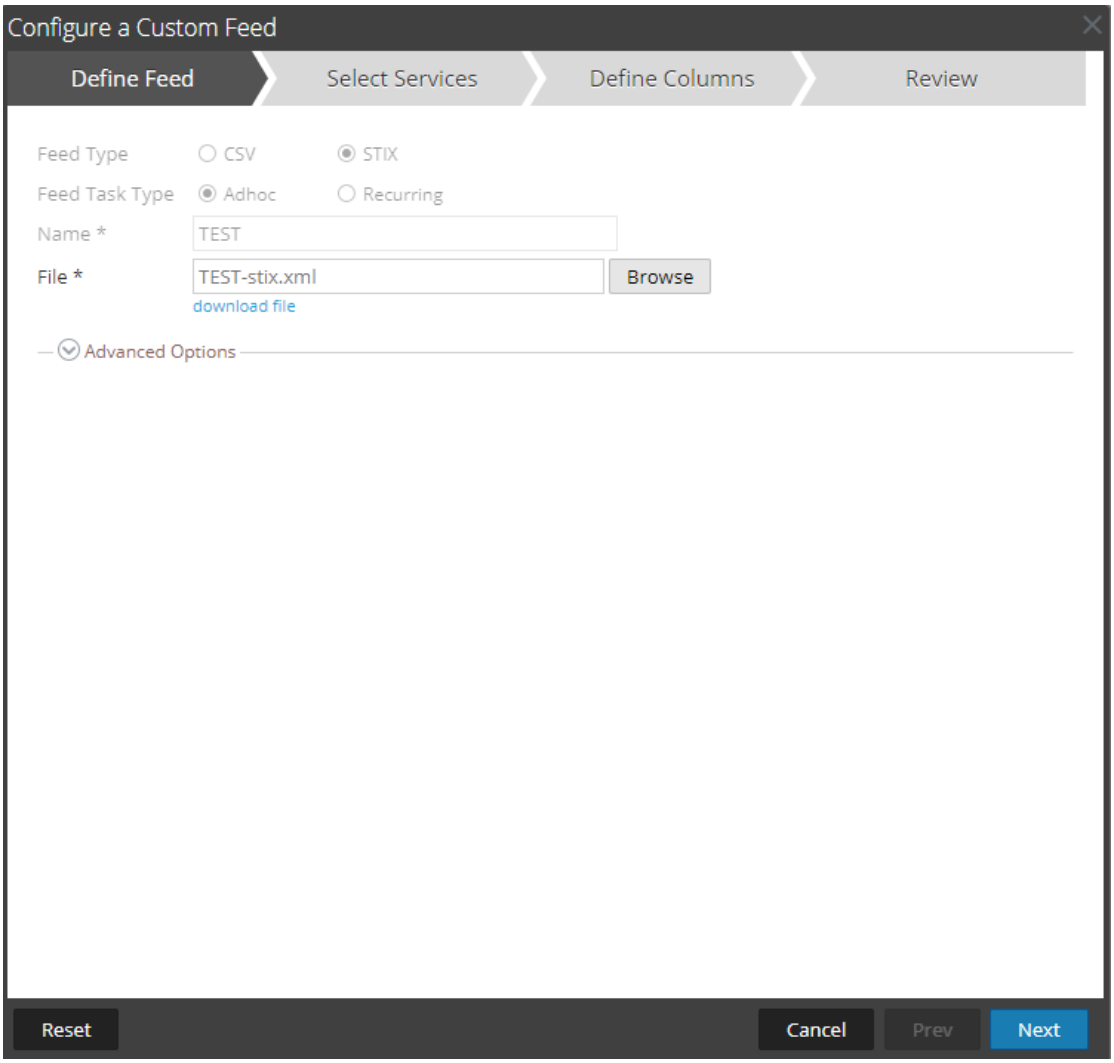
1. Accédez à **Configurer > Feeds personnalisés**.

   La vue Feeds personnalisés 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 feed est créé avec succès, l'assistant Créer un feed se ferme, et le feed et le fichier de token correspondant sont répertoriés dans la liste Feeds. Vous pouvez développer ou réduire l'entrée pour voir combien de services sont inclus, et quels services ont abouti.

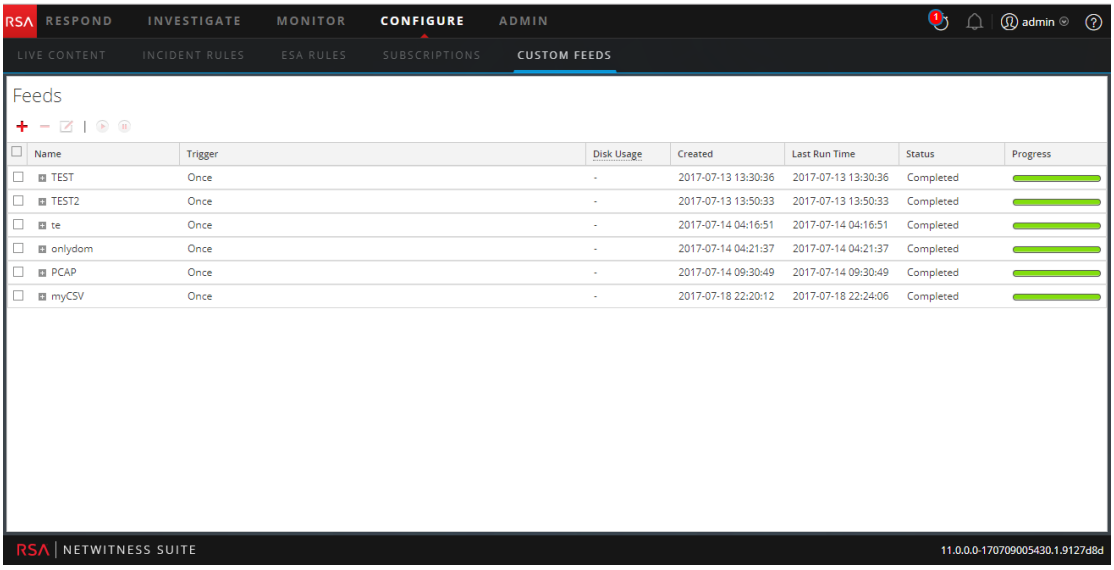
Supprimer un feed

Cette rubrique fournit des instructions pour la suppression d'un feed.

Pour supprimer un feed :

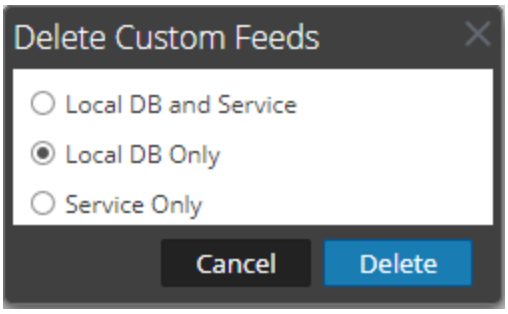
1. Accédez à **CONFIGURER > Feeds personnalisés**.

   La vue Feeds personnalisés s'affiche.



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

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



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

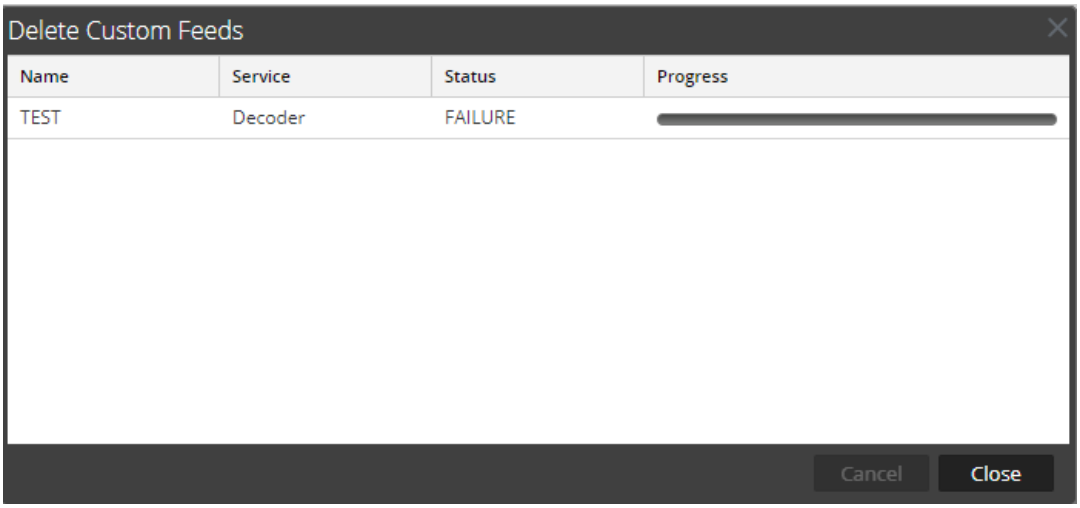
- Si vous choisissez de supprimer le feed dans **BD locale et Service**, le feed sera supprimé à la fois dans la zone des services et de la zone NetWitness Suite locale. Le feed supprimé n'apparaîtra plus dans l'interface utilisateur NetWitness Suite.
- Si vous choisissez de supprimer le feed depuis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

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

   Une boîte de dialogue d'avertissement s'affiche.

4. Cliquez sur **oui** pour confirmer la suppression du feed des zones sélectionnées.
   - Si vous avez choisi de supprimer le feed dans **Base de données uniquement**, le feed est supprimé.
   - Si vous avez choisi de supprimer le feed dans **Base de données locale et service** ou **Service uniquement**, la vue Supprimer les feeds personnalisés s'affiche et indique la

progression de la suppression au niveau du service.



Différentes procédures pour les services Live

Cette section contient les rubriques suivantes :

Ajouter des ressources souscrites à déployer au niveau des services

1. Accédez à la **Configurer > Abonnements > Onglet Déploiements**.
2. Dans le panneau **Groupes**, sélectionnez un groupe.
   Les ressources souscrites éventuelles sont répertoriées dans le panneau Abonnements de l'onglet Déploiements.
3. Dans le panneau **Abonnements**, cliquez sur  .

   La boîte de dialogue Ajouter un abonnement s'affiche et contient les abonnements disponibles à déployer.
4. Sélectionnez les ressources souscrites à déployer dans le groupe de services.
5. Cliquez sur **Enregistrer**.

   La boîte de dialogue se ferme et les abonnements sont ajoutés à la liste dans le panneau Abonnements de l'onglet Déploiements. Les ressources à déployer sont alors stockées lors de la synchronisation suivante.

Créer un package de ressources

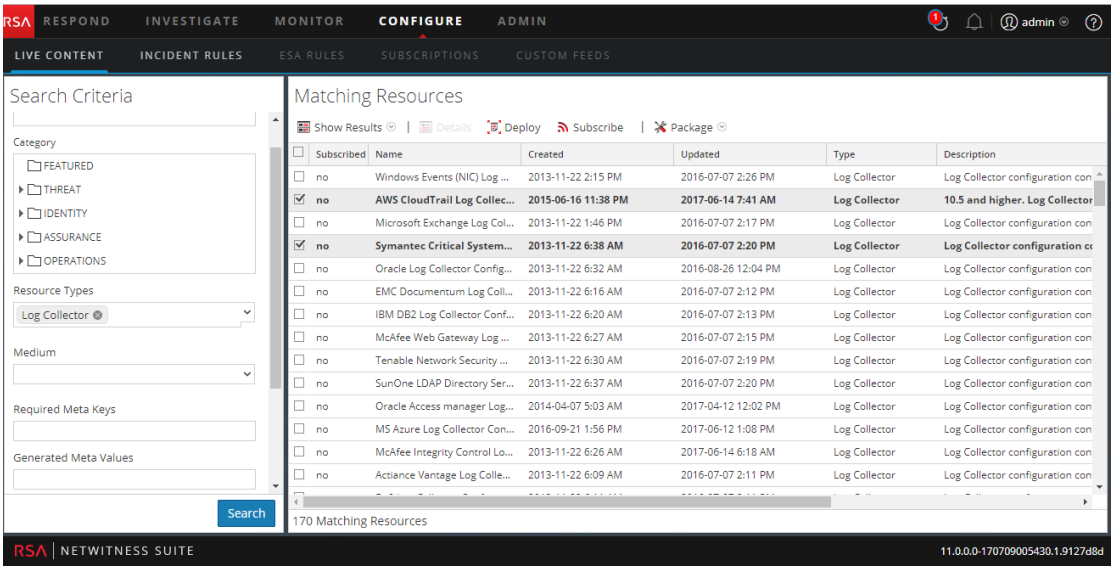
Vous pouvez créer un package de ressources pouvant être enregistré dans un fichier .zip et partagé avec d'autres utilisateurs.

Conditions préalables

Une condition préalable pour créer des packages de ressources est de configurer la connexion et la synchronisation entre le serveur CMS et NetWitness Suite et d'avoir la possibilité de rechercher des ressources dans l'interface utilisateur.

Pour créer un package de ressources :

1. Sélectionnez les ressources à inclure dans le package dans la grille Ressources correspondantes.



2. Sélectionnez **Package** > **Créer** :

   NetWitness Suite crée un fichier **.zip** qui contient les ressources sélectionnées et affiche la boîte de dialogue suivante dans laquelle vous pouvez ouvrir le fichier .zip ou l'enregistrer sur un disque réseau pour partager les ressources du package ou les déployer ultérieurement.

   NetWitness Suite attribue un nom générique au package. Vous devez le renommer lorsque vous l'enregistrez afin qu'il identifie les ressources contenues dans le package.

Supprimer un abonnement

Lorsque vous supprimez un abonnement à une ressource, les instances déployées de la ressource ne sont pas supprimées. La ressource déployée reste sur les services jusqu'à sa suppression explicite, mais la ressource n'est plus synchronisée avec la ressource dans NetWitness Suite Live.

Pour supprimer un abonnement :

1. Sous l'onglet **Abonnements**, sélectionnez les abonnements à supprimer.
2. Cliquez sur .

   Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer l'abonnement.
3. Pour confirmer la suppression, cliquez sur **Oui**.

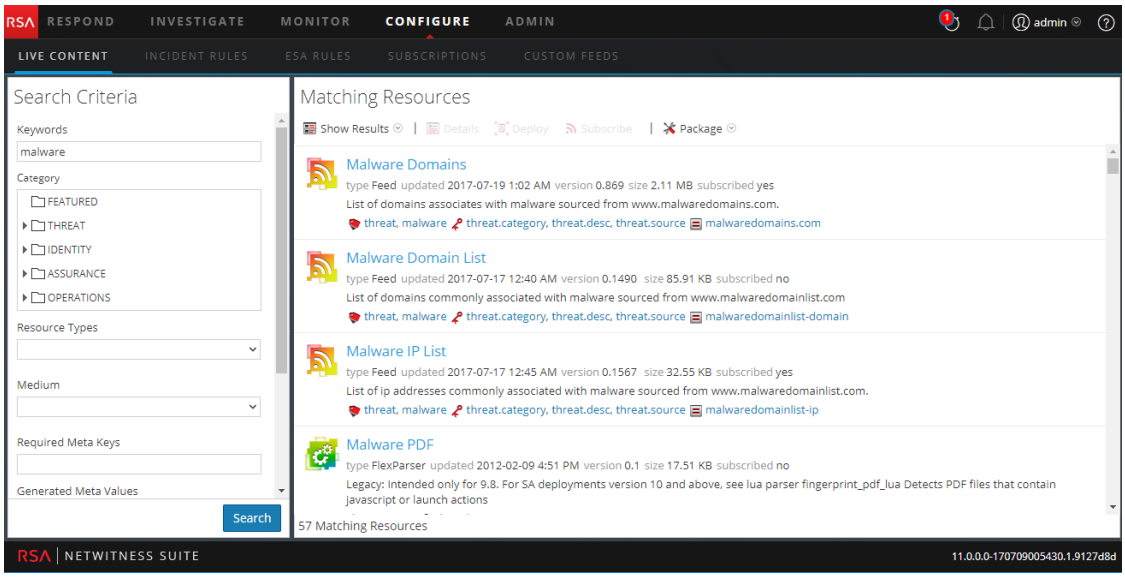
   L'abonnement est supprimé de la liste des abonnements, mais les instances déployées de la ressource souscrite demeurent sur les services.

Afficher les détails des ressources dans la vue Ressources Live

Lorsque vous sélectionnez une ressource (dans la vue Ressources Live), vous pouvez afficher ses informations détaillées.

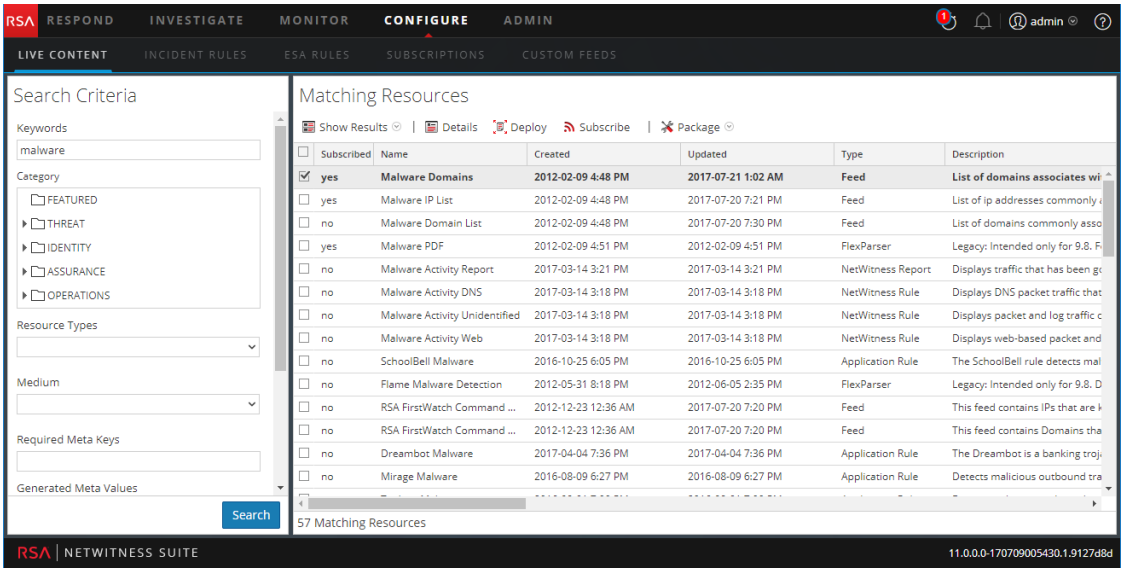
Pour ouvrir un onglet séparé dans la vue Ressources Live avec les informations détaillées de la ressource sélectionnée, choisissez l'une des méthodes suivantes :

- Dans la vue **Résultats détaillés**, cliquez sur l'icône du type de ressource ou sur le nom de la ressource.



- Dans la vue Résultats en grille, double-cliquez sur une ressource ou sélectionnez une

ressource et cliquez sur **Détails**.



Télécharger une ressource

Vous pouvez télécharger une seule ressource à partir de la Vue Ressources Live.

Pour télécharger une ressource :

1. Accédez à **Configurer > Contenu Live**.
2. Dans le panneau **Critères de recherche**, saisissez les critères nécessaires pour renvoyer la ressource que vous souhaitez télécharger.
3. Sélectionnez une seule ressource, puis cliquez sur Details.
4. Cliquez sur Download.

La ressource est enregistrée en tant qu'archive ZIP dans votre dossier local Téléchargements.

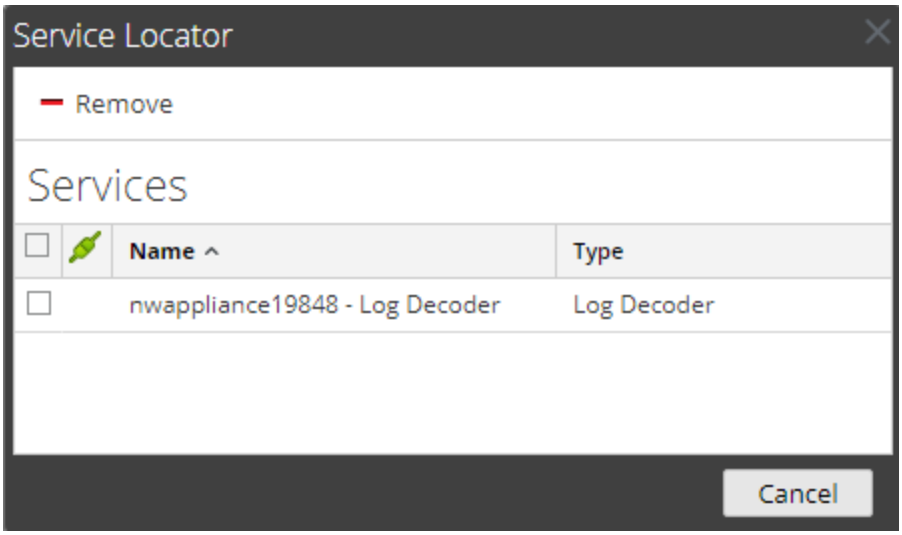
Rechercher et supprimer une ressource déployée à partir des services

Vous pouvez rechercher et supprimer une ressource déployée à partir de la Vue Ressources Live.

Pour afficher une liste des services dans lesquels une ressource est déployée :

1. Avec une ressource affichée dans la **vue Ressources**, cliquez sur Service Locator.

   La boîte de dialogue Localisateur de services s'affiche.



2. Sélectionnez un ou plusieurs services dans la liste **Services**.
3. Cliquez sur .

   La ressource est supprimée des services sélectionnés.

Supprimer les ressources souscrites de la grille Abonnements aux déploiements

Les abonnements sélectionnés pour être déployés sur un groupe de services sont déployés pendant la synchronisation. Vous pouvez supprimer des abonnements dans la vue Configurer Live > onglet Déploiements > panneau Abonnements, mais ceux qui ont été effectivement déployés sur les services demeurent déployés jusqu'à leur suppression.

Pour supprimer les ressources du panneau Abonnements de l'onglet Déploiements :

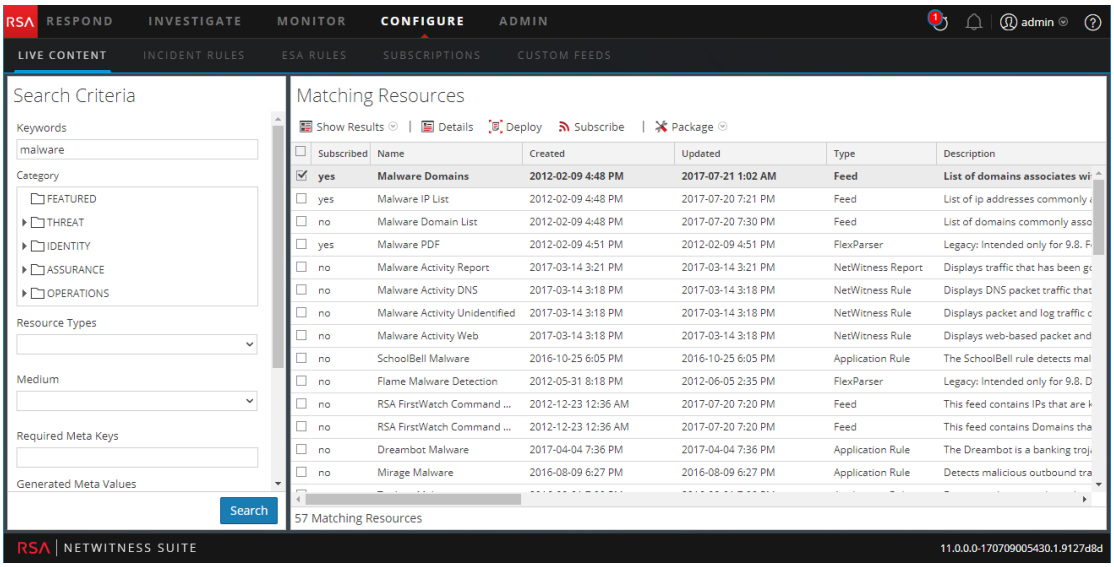
1. Dans le panneau **Groupes**, sélectionnez un groupe.

   Les ressources souscrites éventuelles sont répertoriées dans le panneau Abonnements.
2. Dans le panneau Abonnements, cliquez sur .

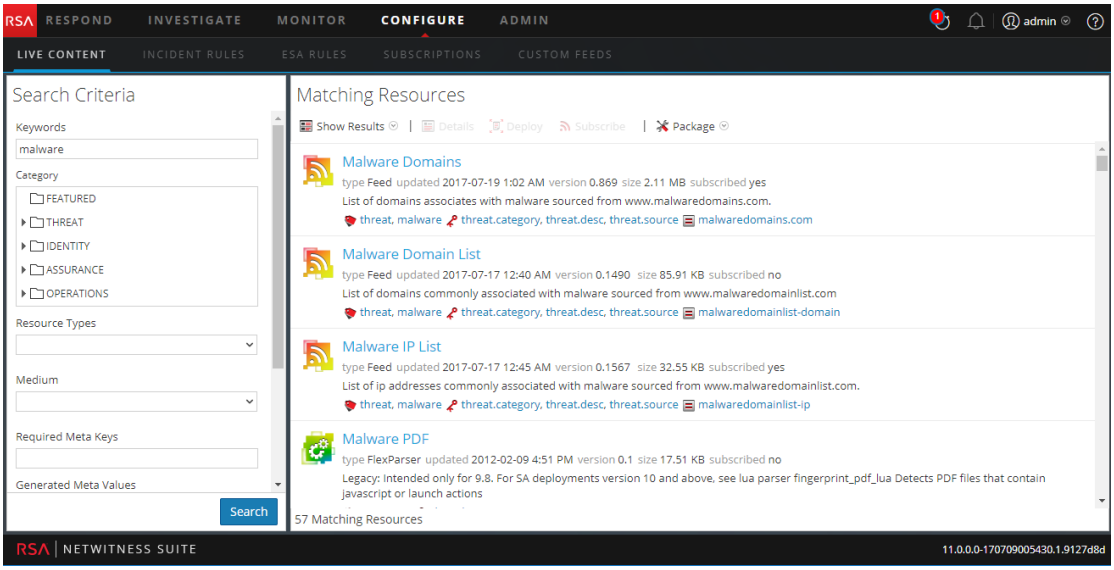
   Une boîte de dialogue vous invite à confirmer que vous voulez supprimer la ressource du groupe de services. La ressource est supprimée du panneau Abonnements de l'onglet Déploiements, mais elle n'est pas supprimée des services sur lesquels elle est déployée.

Afficher les résultats sous forme de liste ou de façon détaillée

1. Pour accéder aux résultats en grille à partir de l'affichage des résultats détaillés, cliquez sur **Afficher les résultats > Grille**.



2. Pour accéder aux résultats détaillés à partir de l'affichage sous forme de grille, cliquez sur **Afficher les résultats > Détaillés**.



S'abonner et se désabonner d'une ressource

S'abonner

Lorsque vous vous abonnez à des ressources, vous recevez une notification lorsque de nouvelles versions des ressources sont disponibles.

Pour s'abonner à une ressource :

1. Accédez à la vue Live > Rechercher.
2. Dans le panneau **Critères de recherche**, spécifiez des critères de recherche et cliquez sur **Rechercher**.
3. Sélectionnez une ou plusieurs ressources, puis cliquez sur Subscribe.

   Une boîte de dialogue de confirmation s'affiche : **En vous abonnant à ces ressources, vous indiquez que vous souhaitez recevoir une notification lorsque de nouvelles versions sont disponibles.**
4. Pour confirmer votre abonnement à la ressource, cliquez sur **OK**.

   La ressource est ajoutée aux abonnements gérés sous l'onglet Abonnements et peut être déployée sous l'onglet Déploiements.

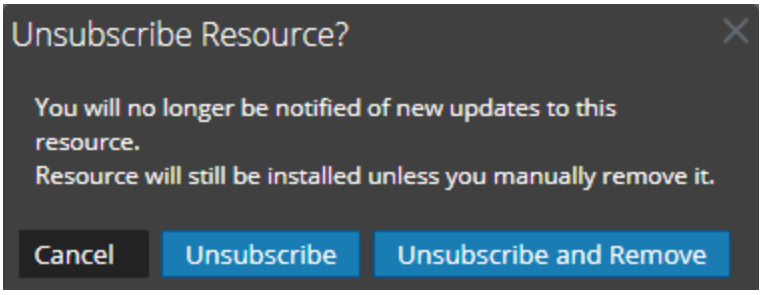
Se désabonner

Lorsque vous vous désabonnez d'une ressource, vous pouvez conserver la ressource dans les services de déploiement ou la supprimer des services.

Pour se désabonner d'une ressource :

1. Lorsqu'une ressource est affichée dans **Abonnements**, cliquez sur Unsubscribe.

   Une boîte de dialogue de confirmation s'affiche.



2. Exécutez l'une des opérations suivantes :
   - Pour confirmer votre désabonnement de la ressource et la conserver dans les services de déploiement, cliquez sur **Se désabonner**.
   - Pour confirmer votre désabonnement de la ressource et la supprimer des services de déploiement, cliquez sur **Annuler et supprimer un abonnement des services**.
   - Pour fermer la boîte de dialogue sans vous désabonner, cliquez sur **Annuler**.

   L'action sélectionnée est appliquée.

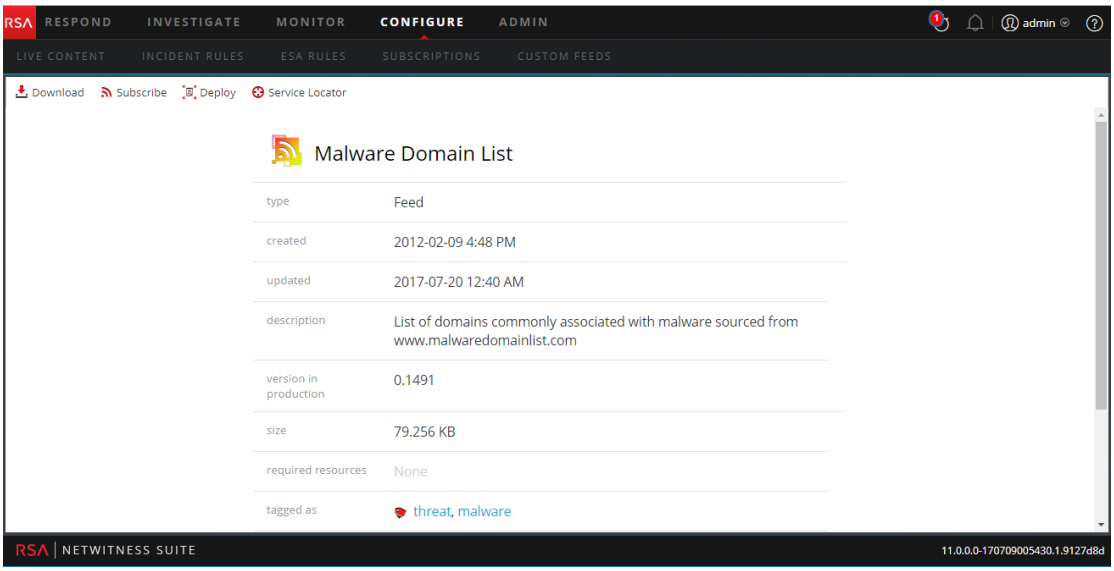
Afficher les détails des ressources

Vous pouvez afficher des informations détaillées sur une ressource souscrite dans la vue Ressource.

Pour afficher les détails :

1. Dans l'onglet **Inscriptions**, sélectionnez une seule inscription.
2. Cliquez sur Details .

   Les informations détaillées de la ressource s'affichent dans la vue Ressource.



Afficher les ressources souscrites sélectionnées pour un déploiement au niveau des services

Dans la vue Configurer Live > onglet Déploiements, vous pouvez visualiser les ressources souscrites sélectionnées pour être déployées dans des services.

Pour afficher les ressources souscrites qui ont été sélectionnées pour le déploiement au niveau des services :

Dans le panneau **Groupes**, sélectionnez un groupe et développez-le pour afficher ses services. Les inscriptions de ressource sélectionnées pour le déploiement sont répertoriées dans l'onglet Déploiements du panneau Inscriptions.

Résolution des problèmes

Cette rubrique donne des instructions de dépannage pour les problèmes rencontrés lors de l'utilisation du module Services Live dans NetWitness Suite.

Résolution des problèmes OutOfMemoryError sur le serveur Context Hub

Cette section fournit des instructions de dépannage du problème OutOfMemoryError sur le serveur Context Hub lorsque le service cesse de répondre.

Si des feeds TAXII sont configurés, Intégrité déclenche des alertes lorsque la mémoire disponible sur le serveur de Context Hub est extrêmement faible. Si l'état du serveur Context Hub est Mauvais en raison du manque de mémoire, procédez comme suit :

1. Assurez-vous que la **Date de début** des feeds ne dépasse pas les 180 derniers jours.
2. Vérifiez que le feed TAXII ne consomme pas trop d'espace disque. Le feed TAXII peut consommer jusqu'à 300 Mo. S'il consomme davantage d'espace disque, vous devez réduire la valeur du champ **Supprimer les données STIX antérieures à** sous **Options avancées** dans l'**Assistant de création du feed personnalisé** lorsque vous modifiez des feeds TAXII.

Remarque : Si le problème persiste, vous devez exécuter l'étape 3.

3. Pour réduire le nombre de threads parallèles disponibles pour le traitement STIX, procédez comme suit :
   a. Accédez à **ADMIN** > **Services** > **service Context Hub** > **Vue** > **Explorer**.
   b. Dans le volet d'arborescence, accédez à **enrichment/stix/ config**.
   c. Dans le volet de droite, définissez le champ **stix-query-scheduler-pool-size** sur la valeur 2. La valeur par défaut est 5. Ce paramètre contrôle le nombre de nombre de threads autorisées à traiter des requêtes pour les données STIX en même temps.
   d. Définissez le champ **taxii-poll-scheduler-pool-size** sur la valeur 2. La valeur par défaut est 5. Ce paramètre contrôle le nombre de threads autorisées à interroger les serveurs TAXII en même temps.
   e. Redémarrez le serveur Context Hub.

Références

Cette rubrique rassemble des références qui décrivent l'interface utilisateur et fournissent un complément d'informations sur le fonctionnement de Live dans NetWitness Suite. Ces rubriques sont présentées par ordre alphabétique.

- Onglet Déploiements
- Onglet Ressources interrompues
- Vue Configuration Live
- Vue Feeds Live
- Vue Ressources Live
- Vue Live Search
- Commentaires et Partage de données NetWitness Suite
- Assistant Déploiement du package de la ressource
- Portail d'inscription RSA Live
- Onglet Abonnements

Vue Configuration Live

Dans la vue Configuration Live, NetWitness Suite met à disposition des outils intégrés pour gérer les ressources Live. Vous pouvez gérer des abonnements à des ressources, des déploiements sur des services et des ressources interrompues. Le rôle requis pour accéder à cette vue est **Configurer des ressources Live**. Pour obtenir une description générale de l'utilisation des différentes vues dans NetWitness Suite Live, consultez la rubrique Gestion des services Live.

Pour accéder à cette vue, accédez à **CONFIGURER > Abonnements**. Cette vue propose les onglets suivants :

- Onglet Déploiements
- Onglet Abonnements
- Onglet Ressources interrompues

Onglet Déploiements

L'onglet Déploiements fournit une interface utilisateur dans la vue Live Configurer pour :

- Afficher les ressources souscrites sélectionnées pour le déploiement sur les services d'un groupe de services.
- Sélectionner les ressources souscrites pour le déploiement dans les services d'un groupe de services.
- Supprimer les ressources souscrites sélectionnées pour le déploiement sur les services d'un groupe de services.

Les ressources répertoriées ici ne sont pas déployées immédiatement après l'ajout à un groupe de services. Au lieu de cela, les ressources souscrites sont envoyées aux services lorsque NetWitness Suite se synchronise avec RSA NetWitness Suite Live. Le planning de synchronisation est configuré dans le panneau Configuration de Live. Si vous ne souhaitez pas attendre la synchronisation planifiée, vous pouvez également indiquer à NetWitness Suite d'effectuer la synchronisation dès à présent dans le panneau Configuration de Live.

De même, les ressources supprimées du panneau Déploiements ne sont pas supprimées du service sur lequel elles ont été déployées. Pour supprimer les ressources des services, supprimez-les de la vue Ressources Live.

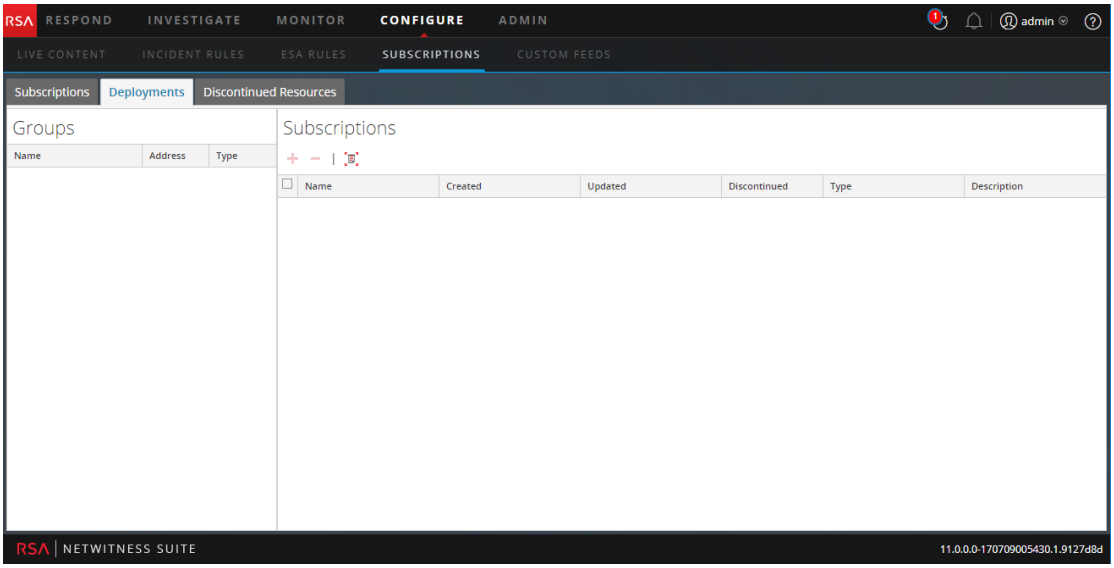
L'autorisation requise pour accéder à cette vue est **Gérer les ressources Live**.

Pour accéder à cette vue :

1. Allez à **CONFIGURER > Abonnements**.

   L'onglet **Abonnements** est ouvert par défaut.

2. Cliquez sur l'onglet **Déploiements**.



L'onglet Déploiements possède deux panneaux : **Groupes** et **Inscriptions**.

Panneau Groupes

Le panneau Groupes est un affichage statique des groupes de services configurés qui ont été créés dans la vue Services d'administration. La sélection d'un groupe dans le panneau Groupes remplit le panneau Inscriptions avec une liste d'inscriptions qui sont sélectionnées pour le déploiement sur les services dans le groupe de services.

Fonction	Description
Nom	Il s'agit du nom de groupe de services. Le fait de cliquer sur le signe Plus affiche une liste de services imbriquée dans le groupe.
Adresse	Il s'agit de l'adresse IP de chaque service dans le groupe.
Type	Il s'agit du type de service.

Panneau Inscriptions

Le tableau suivant décrit les fonctions du panneau Inscriptions.

Fonction	Description
	Cliquez sur pour ouvrir une boîte de dialogue qui répertorie les inscriptions qui ont été ajoutées dans la vue Ressources Live et sont disponibles pour le déploiement.
	Cliquez sur pour supprimer les inscriptions sélectionnées dans la liste de déploiement pour le groupe de services.
	Cliquez sur  pour synchroniser vos ressources avec les dernières versions disponibles sur Live.
Nom	Il s'agit du nom de la ressource.
Créé	Il s'agit de la date et de l'heure de création de la ressource.
Mise à jour	Il s'agit de la date et de l'heure de dernière mise à jour de la ressource.
Type	Il s'agit du type de ressource.
Description	Il s'agit d'une description de la ressource.

Onglet Abonnements

Les abonnements sont des ressources NetWitness Suite Live auxquelles vous vous abonnez dans la vue Live Search ou Ressources Live. Lorsque vous vous abonnez à une ressource, vous acceptez de recevoir régulièrement des mises à jour de la part de RSA NetWitness Suite Live. Les sélections effectuées dans le panneau Configuration de Live déterminent la fréquence de la synchronisation et si vous recevez des notifications par e-mail pour les mises à jour. Par ailleurs, si vous ne souhaitez pas attendre la prochaine mise à jour, vous pouvez effectuer de force une synchronisation immédiate.

L'onglet Abonnements permet de gérer les abonnements. Toutes les ressources auxquelles NetWitness Suite est abonné sont répertoriées dans cet onglet.

Dans le panneau Abonnements, vous pouvez :

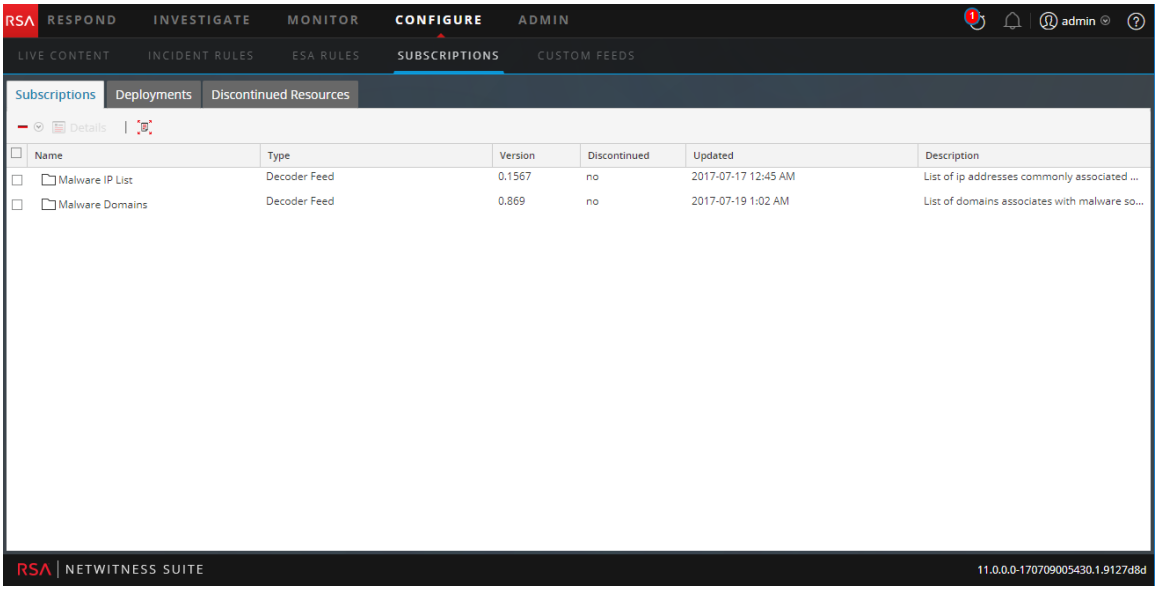
- Consulter toutes les ressources auxquelles cette instance NetWitness Suite est abonnée
- Ouvrir une vue détaillée d'un abonnement dans la vue Ressource Live
- Supprimer un abonnement

Remarque : l'abonnement à une ressource n'a pas pour effet de déployer cette ressource dans les services. Pour déployer une ou plusieurs ressources faisant l'objet d'un abonnement, accédez à l'onglet Déploiements. Pour déployer manuellement une ressource, utilisez l'option Déployer de la vue Ressource.

L'autorisation requise pour accéder à cette vue est **Gérer les ressources Live**.

Pour accéder à cette vue, dans le Menu principal, sélectionnez **CONFIGURER > Abonnements**.

L'onglet Abonnements est ouvert par défaut.



L'onglet **Abonnement** comporte une barre d'outils et une grille.

Barre d'outils

Ce tableau décrit les options disponibles dans la barre d'outils.

Fonction	Description
	Supprime les abonnements sélectionnés.
	Affiche dans la vue Ressource le détail d'une ressource faisant l'objet d'un abonnement.
	Vérifier Live Server pour détecter les dernières ressources interrompues.

Grille

Colonne	Description
	Sélectionnez les ressources auxquelles vous êtes abonné pour en consulter le détail ou pour les supprimer. Vous pouvez consulter les détails d'une ressource. Vous pouvez supprimer une ou plusieurs ressources parmi celles faisant l'objet d'un abonnement. Il vous suffit pour cela de vous désabonner.
Nom	Nom de la ressource à laquelle vous êtes abonné.
Type	Type de la ressource à laquelle vous êtes abonné.
Version	Version de la ressource à laquelle vous êtes abonné.
Interrompu	Indique l'état des ressources interrompues pour la ressource souscrite. **Oui** - la ressource est interrompue. **Non** - la ressource n'est pas interrompue. **--** - Live Server n'est pas sélectionné pour les ressources interrompues.
Mise à jour	Affiche la date et l'heure auxquelles la ressource faisant l'objet d'un abonnement a été mise à jour pour la dernière fois.
Description	Description de la ressource à laquelle vous êtes abonné.

Onglet Ressources interrompues

Cette rubrique présente les fonctions de la **vue Configuration Live > onglet Ressources interrompues**.

L'onglet Ressources interrompues fournit une interface utilisateur dans la vue Configuration Live pour :

- Analyser les services pour rechercher les ressources interrompues.
- Supprimer les ressources interrompues de tous les services ou groupes de services.

L'autorisation requise pour accéder à cette vue est **Gérer les ressources Live**.

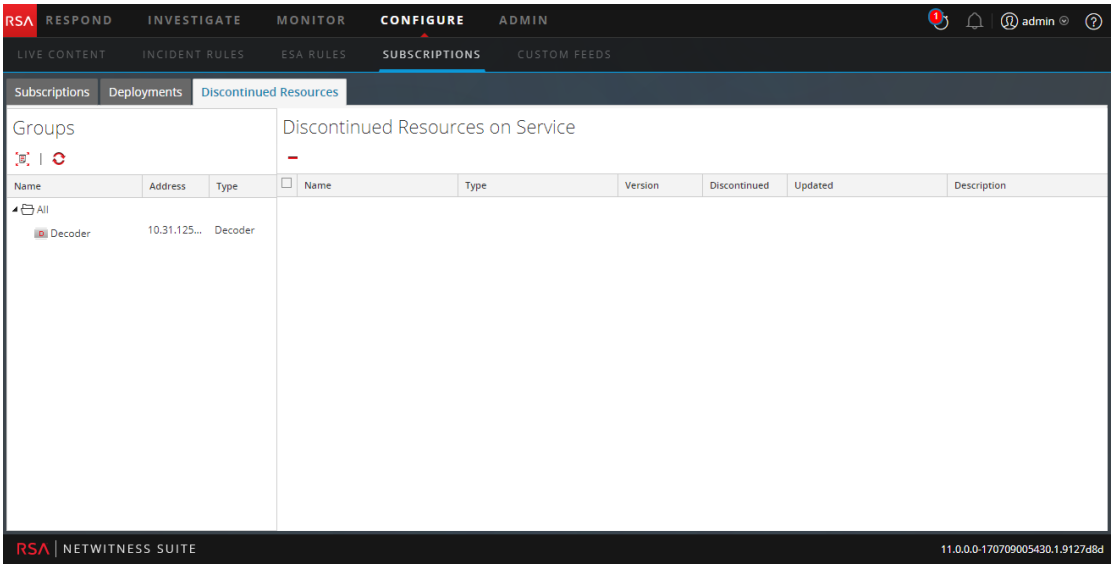
Pour accéder à cette vue :

1. Allez à **CONFIGURER > Abonnements**.

   L'onglet **Abonnements** est ouvert par défaut.

2. Cliquez sur l'onglet **Ressources interrompues**.

   Il s'agit d'un exemple de l'onglet Ressources interrompues.



Cet onglet comporte deux panneaux : Groupes et Ressources interrompues en service.

Panneau Groupes

Le panneau Groupes est un affichage statique des groupes de services configurés qui ont été créés dans la vue Services d'administration. La sélection d'un groupe dans le panneau Groupes remplit le panneau Ressources interrompues avec une liste de ressources interrompues déployées sur le service ou le groupe de services sélectionné.

Fonction	Description
	Cliquez sur  pour analyser les services afin de rechercher une ressource interrompue.
	Affiche l'état actuel des ressources interrompues d'un service. **Remarque :** l'état d'un peut changer pendant l'analyse des services.
Nom	Il s'agit du nom de groupe de services. Le fait de cliquer sur le signe Plus affiche une liste de services imbriquée dans le groupe.
Adresse	Il s'agit de l'adresse IP de chaque service dans le groupe.
Type	Il s'agit du type de service.

Panneau Ressources interrompues en service

Le tableau suivant décrit les fonctions du panneau Ressources interrompues en service.

Fonction	Description
	Cliquez sur pour supprimer les ressources sélectionnées du service ou du groupe de services.
Nom	Il s'agit du nom de la ressource.
Type	Il s'agit du type de ressource.
Version	Version de la ressource interrompue.
Interrompu	Indique l'état des ressources interrompues pour la ressource souscrite. **Oui** - la ressource est interrompue. **Non** - la ressource n'est pas interrompue. **--** - Live Server n'est pas sélectionné pour les ressources interrompues.
Mise à jour	Il s'agit de la date et de l'heure de dernière mise à jour de la ressource.
Description	Il s'agit d'une description de la ressource.

Vue Feeds Live

La vue Feeds Live permet de :

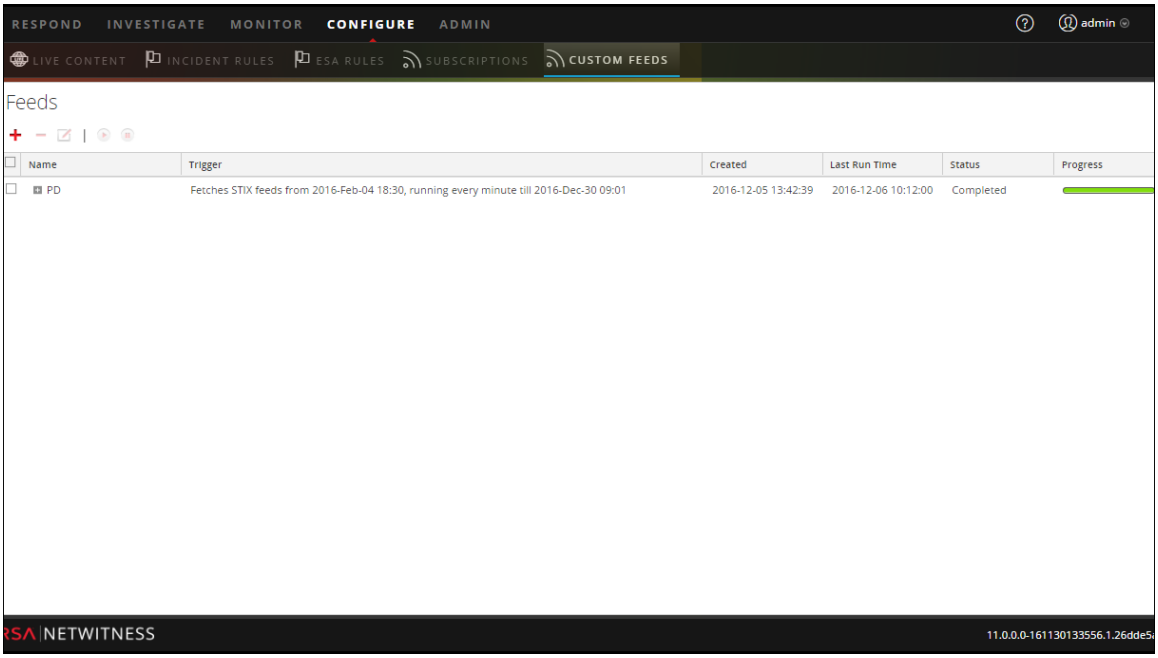
- Créer des feeds personnalisés.
- Créer des feeds d'identité.
- Modifier des feeds.

Le rôle requis pour accéder à cette vue est **Gérer les périphériques**.

Pour accéder à cette vue, procédez de l'une des façons suivantes :

- Dans le Menu principal, sélectionnez **Live > Feeds.**
- Dans une vue du module Live, sélectionnez **Feeds** dans le menu Menu principal.

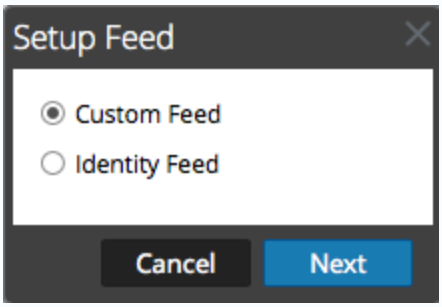
Il s’agit d’un exemple de la vue Feeds.



L'onglet **Feeds** contient une barre d'outils et une grille.

Barre d’outils

Ce tableau décrit les options de la grille.

Fonction	Description
	Lance la création d'un feed personnalisé ou d'un feed d'identité en affichant la boîte de dialogue **Configurer le feed**.  • Feed personnalisé ouvre l'assistant **Configurer un feed personnalisé**. • Identity Feed ouvre l'assistant **Configurer Identity Feed**.
	Supprime le feed que vous avez sélectionné.
	Ouvre l'assistant Configurer un feed personnalisé ou Configurer Identity Feed pour le feed sélectionné (reportez-vous à la rubrique Modifier un feed).
	Démarre ou reprend un feed de données.
	Arrête ou suspend un feed de données.

Grille Feeds

Ce tableau décrit les colonnes de la grille.

Colonne	Description
	Sélectionne un feed.
Nom	Nom du feed. **Remarque :** vous pouvez maintenant utiliser des caractères spéciaux pour définir le nom du feed personnalisé.
Déclencheur	Affiche la fréquence d'exécution du feed qui est déterminée par la valeur définie dans **Type de tâche par défaut** lors de la création du feed.
Créé	Date et heure de création du feed.

Colonne	Description
Utilisation des disques	Affiche la taille du stockage MongoDB utilisée par le feed TAXII.
Heure de la dernière exécution	Affiche la date et l'heure de la dernière exécution du feed.
État	État du feed.
Progression	Barre de progression.

Vue Ressources Live

La vue Ressources Live offre une vue détaillée d'une ressource sélectionnée, et contient les options qui permettent d'effectuer les opérations suivantes :

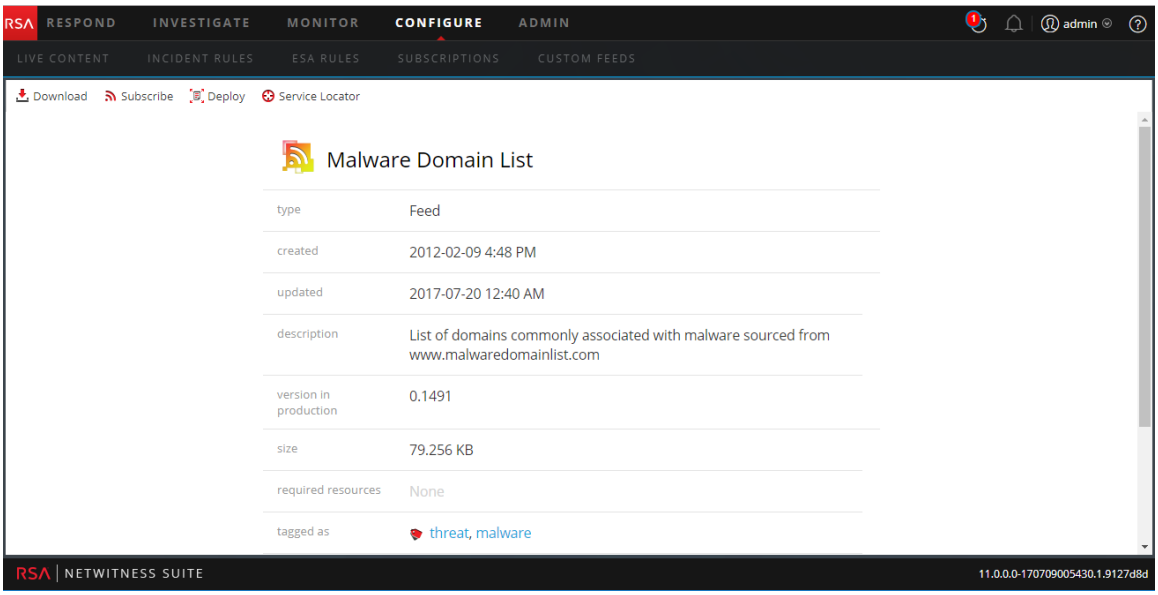
- Téléchargez la ressource.
- Abonnez-vous à la ressource ou désabonnez-vous.
- Déployer la ressource sur les services.
- Rechercher les services sur lesquels la ressource est déployée et supprimer la ressource des services.

L'autorisation requise pour accéder à cette vue est Afficher les détails des ressources Live.

Pour accéder à cette vue, procédez de l'une des façons suivantes :

1. Dans le Menu principal, sélectionnez **CONFIGURER > CONTENU LIVE > Critères de recherche**.
2. Dans la vue Live Search, **Résultats détaillés**, cliquez sur l'icône du type de ressource ou le nom de la ressource.
3. Dans la vue Live Search, **Résultats en grille**, double-cliquez sur une ressource ou sélectionnez une ressource, puis cliquez sur **Détails**.

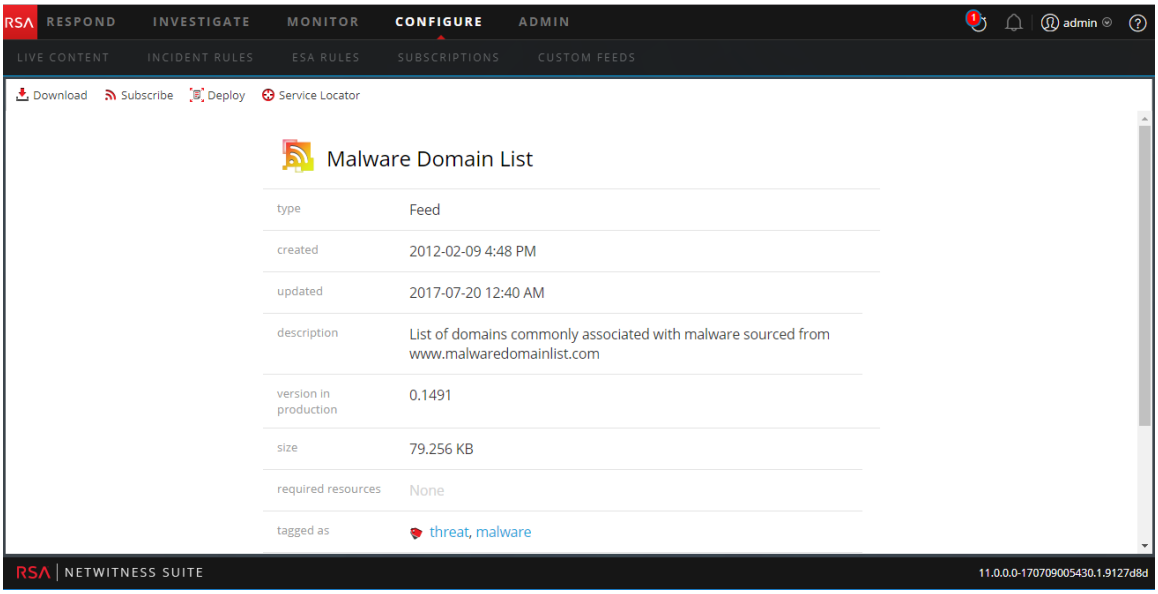
Il s'agit d'un exemple de la vue Ressource.



La vue Ressource Live offre une vue détaillée d'une seule ressource et d'une barre d'outils.

Détails de la ressource

Il s'agit d'un exemple de détails de la ressource s'affichant dans la vue Ressource.



Le tableau suivant décrit les éléments de la section Détails des ressources.

Fonction	Description
Icône Type de ressource	Représentation graphique du type de ressource, par exemple  .

Fonction	Description
Nom	Nom de la ressource, par exemple **fingerprint_office_lua**.
Type	Type de ressource, par exemple, **RSA Lua Parser**.
Créé	Date à laquelle la ressource a été créée, par exemple, **2013-09-15 02:16 PM**.
Mise à jour	Date à laquelle la ressource a été mise à jour pour la dernière fois, par exemple, **2013-09-15 02:16 PM**
Description	Description de la ressource, par exemple, **Identifie les documents Microsoft Office 95, Word 2007, Excel et PowerPoint**.
Version en production	Version de la ressource, par exemple **0.1**.
Taille	Taille de la ressource, par exemple **9,079 Ko**.
Ressources requises	Liste des ressources auxquelles dépend cette ressource, par exemple, **NetWitness Lua Library**. Cliquer sur une ressource permet de remplacer les détails actuellement affichés par les détails de la ressource que vous avez sélectionnée.
Étiquetées en tant que	Balises qui s'appliquent à la ressource. Dans l'exemple, l'étiquette est de type **featured, informational**. Cliquer sur une étiquette permet d'ouvrir la vue Live Search avec la recherche restreinte pour obtenir une correspondance avec les ressources dotées d'une étiquette.
Clés méta requises	Clés méta qui s'appliquent à la ressource. Dans l'exemple, il n'y a pas de clés méta requises. Cliquer sur une clé méta permet d'ouvrir la vue Live Search avec la recherche restreinte pour obtenir une correspondance avec les ressources dotées de cette clé méta.

Fonction	Description
Génère des valeurs méta	Métavaleurs  que la ressource génère. Dans l'exemple, il n'y a pas de métavaleurs requises. Cliquez sur une valeur méta ppour ouvrir la vue Live Search avec la recherche restreinte pour obtenir une correspondance avec les ressources dotées de cette clé méta.
Autorisations	Autorisations requises pour la ressource.

Barre d'outils de la vue Ressource

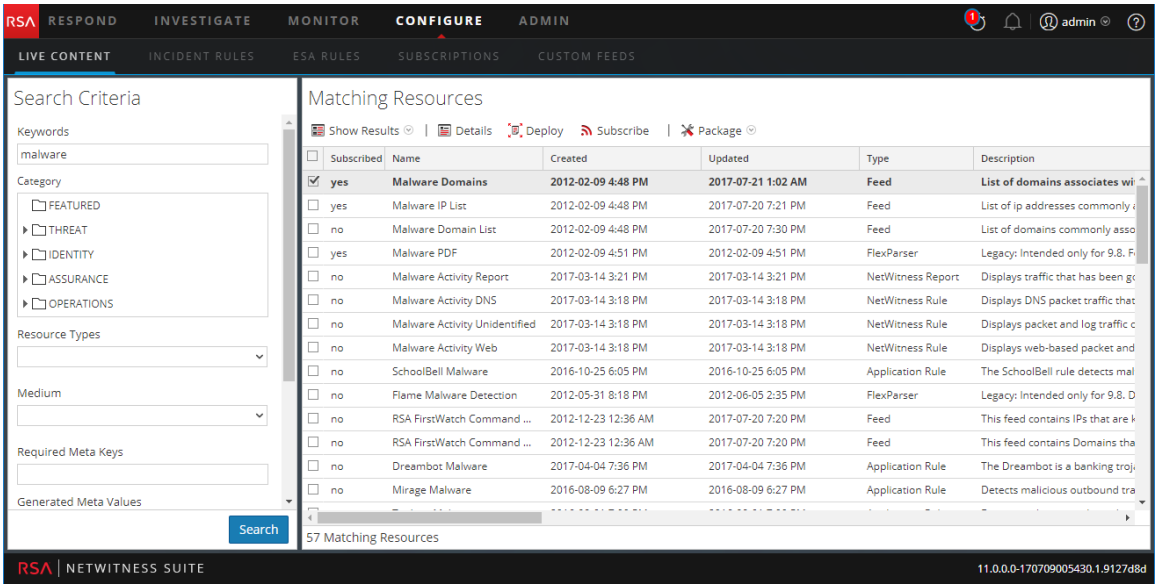
Ce tableau décrit les options de la barre d'outils Ressources Live.

Fonction	Icône	Description
Télécharger		Cette option télécharge la ressource actuellement affichée dans la vue Ressource.
Inscription ou annulation de l'inscription		Cet option permet de s'abonner ou de se désabonner de la ressource actuellement affichée dans la vue Ressource. • Cliquer sur **S'abonner** permet d'ouvrir une boîte de dialogue vous indiquant que vous acceptez de recevoir une notification lorsque les ressources sélectionnées sont mises à jour. Vous pouvez annuler l'opération ou cliquer sur **OK**. • En cliquant sur **Se désabonner**, vous devez confirmer que vous souhaitez arrêter de recevoir la notification lorsque les ressources sélectionnées sont mises à jour. Vous pouvez alors choisir d'annuler l'opération ou de cliquer sur **Se désabonner** ou encore **Se désabonner ou supprimer**, qui permet également de supprimer la ressource des services sur lesquels elle est déployée.
Déployer		Cette option permet de déployer la ressource actuellement affichée dans la vue Ressource. Cliquer sur **Déployer** permet d'ouvrir la boîte de dialogue Déploiement manuel de la ressource.
Localisateur de services		Cette option affiche la liste des services sur lesquels la ressource actuellement affichée est déployée. Vous pouvez supprimer la ressource de tous les services ou les services sélectionnés.

Vue Live Search

La vue Recherche Live offre la capacité à parcourir les ressources de Live CMS. Une fois que les ressources correspondantes sont trouvées, vous pouvez afficher les détails, vous abonner aux ressources et les déployer sur des services et des groupes de services.

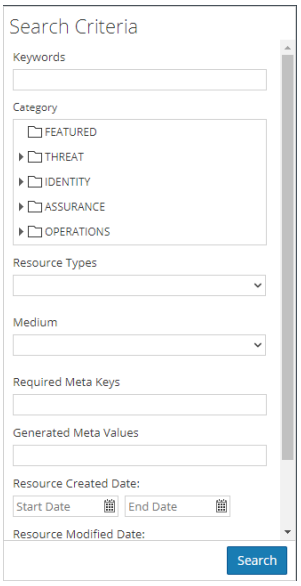
Voici un exemple de la vue de recherche.



La vue Recherche Live possède un panneau pour spécifier les critères de recherche et un panneau qui affiche les ressources correspondantes. Le panneau Critères de recherche peut être réduit pour augmenter la largeur d'affichage du panneau Ressources correspondantes.

Panneau Critères de recherche

Voici un exemple du panneau Critères de recherche.



Le tableau ci-dessous fournit des descriptions des fonctionnalités du panneau Critères de recherche.

Fonction	Description
Mots clés	Saisissez un ou des mots-clés pour rechercher des ressources comportant le mot-clé dans leur nom ou leur description. Vous pouvez utiliser des caractères génériques lorsque vous saisissez un mot-clé.
Catégorie	Les catégories reflètent le modèle hiérarchique de procédure d'enquête utilisé par RSA pour organiser les ressources. Le modèle de la procédure d'enquête vise à fournir un chemin d'accès précis à la réponse aux incidents de sécurité des informations. Pour plus d'informations, reportez-vous à la rubrique Modèle de procédure d'enquête.

Fonction	Description
Types de ressources	Sélectionnez des types de ressources dans la liste déroulante pour filtrer les ressources par type. Les valeurs possibles sont les suivantes : • Advanced Analytics (Warehouse) • Règle d'application • Offre groupée • Règle de corrélation • Règle Event Stream Analysis • Intégration • FlexParser • Log Collector • Log Device • Lua Parser • Règles de malware • Liste NetWitness • Rapport de NetWitness • Règle de NetWitness
Support	Sélectionnez un ou plusieurs supports de la liste déroulante pour rechercher du contenu en fonction de la source de données méta. Les valeurs disponibles pour les supports sont les suivantes: • **log** : appliqué au contenu qui utilise des méta dérivées des données du log • **paquet** : appliqué au contenu qui utilise des méta dérivés des paquets réseau • **log et paquet** : appliqué à un contenu qui corrèle les méta dérivés entre les données de logs et de paquets
Balises	Sélectionnez des balises méta dans la liste déroulante pour parcourir la liste selon la façon dont les métas sont balisés. Par exemple, par parcourir les ressource d'un Log Decoder, sélectionnez la balise **netwitness for logs**. Vous pouvez également cliquer sur une balise dans le panneau Ressources correspondantes pour insérer cette balise dans ce champ.

Fonction	Description
Clés méta requises	Saisissez une clé méta spécifique, par exemple, **threat.source**. Vous pouvez également cliquer sur une clé méta dans le panneau Ressources correspondantes pour insérer cette balise dans ce champ.
Valeurs méta générées	Saisissez une métavaleur générée, par exemple, **netwitness**. Vous pouvez également cliquer sur une clé méta générée dans le panneau Ressources correspondantes pour insérer cette balise dans ce champ.
Recherche par date de création	Spécifiez une plage de données pendant laquelle les ressources ont été modifiées. Par exemple, pour parcourir les ressources créées entre le 1er et le 4 janvier, vous devez sélectionner le 1er janvier en tant que date de départ et le 4 en tant que date de fin. Vous devez indiquer des dates au format jj/mm/aaaa ou bien cliquer sur  et choisir les dates à partir d'un calendrier.
Recherche par date de modification	Spécifiez une plage de données pendant laquelle les ressources ont été modifiées. Par exemple, pour parcourir les ressources modifiées entre le 1er et le 4 janvier, vous devez sélectionner le 1er janvier en tant que date de départ et le 4 en tant que date de fin. Vous devez indiquer des dates au format jj/mm/aaaa ou bien cliquer sur  et choisir les dates à partir d'un calendrier.
Rechercher	Cliquez sur **Rechercher** pour envoyer la requête de recherche au serveur Live. Davantage de critères de recherche plus précis retournent des correspondances de ressources plus rapidement.
Annuler	Cliquez sur **Annuler** pour annuler la recherche en cours.
Inclure les ressources interrompues	Cochez **Inclure les ressources interrompues** pour inclure les ressources interrompues dans les résultats de recherche. Pour obtenir une liste à jour des ressources qui ont été interrompues, reportez-vous à la rubrique Contenu interrompu.

Panneau Ressources correspondantes

Le panneau Ressources correspondantes présente les résultats de la recherche en fonction des sélections effectuées dans le panneau Critères de recherche. Les résultats sont d'abord affichés dans une grille, mais vous pouvez basculer entre deux options Afficher les résultats : Option Détails ou Grille.

Résultats détaillés

Dans les résultats détaillés, vous pouvez cliquer sur une balise, une clé méta, ou une ressource méta pour remplir automatiquement le panneau Critères de recherche et faire pivoter les résultats de la recherche.

Le tableau suivant décrit les éléments des résultats détaillés.

Fonction	Description
Icône Type de ressource	Représentation graphique du type de ressource. Par exemple,  .
Nom	Nom de la ressource, par exemple **Gestion des groupes**. **Remarque :** (Interrompu) s'affiche en regard du nom de ressource si une ressource est interrompue.
Type	Type de ressource, par exemple **Règle**.
Mise à jour	Date à laquelle la ressource a été mise à jour pour la dernière fois, par exemple, **2015-09-15 4:27 PM**.
Version	Version de la ressource, par exemple **0.1**.
Taille	Taille de la ressource, par exemple **153 Ko**.
Abonné	État de l'abonnement : • **oui** : Cette instance NetWitness Suite est abonnée à cette ressource de contenu. • **non** : cette instance NetWitness Suite n'est pas abonnée à cette ressource de contenu.
Description	Description de la ressource, par exemple **Gestion des groupes de règles**.

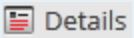
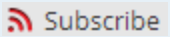
Fonction	Description
Balises	Balises qui s'appliquent à la ressource. Cliquer sur une balise permet de restreindre la recherche aux ressources avec balise. Par exemple,  .
Clés méta	Clés méta qui s'appliquent à la ressource. Cliquer sur une clé méta permet de restreindre la recherche à cette clé méta. Par exemple,  .
Valeurs méta de ressource	Valeurs méta générées par la ressource. Cliquer sur une métavaleur permet de restreindre la recherche aux ressources qui ont généré la métavaleur. Par exemple,  .

Résultats en grille

Dans la vue en grille, vous pouvez sélectionner une ou plusieurs ressources et utiliser des options supplémentaires dans la barre d'outils pour afficher les détails d'une seule ressource, vous abonner aux ressources et les déployer.

Le tableau suivant décrit les éléments des résultats de la grille.

Fonction	Description
Abonné	État de l'abonnement : • **oui** : Cette instance NetWitness Suite est abonnée à cette ressource de contenu. • **non** : cette instance NetWitness Suite n'est pas abonnée à cette ressource de contenu.
Nom	Nom de la ressource, par exemple **Gestion des groupes**. **Remarque :** le nom de la ressource s'affiche en rouge si elle est interrompue.
Créé	Date à laquelle la ressource a été créée, par exemple, **2015-08-12 3:11 PM**.

Fonction	Description
Mise à jour	Date à laquelle la ressource a été mise à jour pour la dernière fois, par exemple, **2015-09-15 4:27 PM**.
Type	Type de ressource, par exemple **Règle**.
Interrompu	État des ressources interrompues : **oui** - la ressource qui correspond aux critères de recherche est interrompue. **non** - la ressource n'est pas interrompue. **--** - Live Server n'est pas sélectionné pour les ressources interrompues.
Description	Description de la ressource, par exemple **Gestion des groupes de règles**.
	Barre d'outils
	Ce menu offre deux méthodes d'affichage des résultats de la recherche : **Détails** et **Grille**.
	Cette option s'applique à une seule ressource sélectionnée. Cliquer sur **Détails** permet d'ouvrir la ressource sélectionnée dans la vue Ressources Live.
	Cette option s'applique à une ou plusieurs ressources sélectionnées.
	Cette option s'applique à une ou plusieurs ressources sélectionnées. Cliquer sur **S'abonner** permet d'ouvrir une fenêtre de confirmation vous demandant si vous souhaitez recevoir une notification lorsque les ressources sélectionnées sont mises à jour.

Fonction	Description

Package	Ce menu offre deux fonctions de mise en package pour les ressources sélectionnées :
	• **Créer** : crée un fichier **resourceBundle.zip** qui contient les ressources sélectionnées et ouvre une boîte de dialogue dans laquelle vous pouvez :
	  • ouvrir le fichier, ou
	  • enregistrer le fichier pour le déploiement suivant.
	• **Déployer** : permet d'ouvrir l'assistant Déploiement du package de la ressource où vous pouvez choisir un fichier **resourceBundle.zip** pour le déployer.

Voir aussi

- Pour de plus amples informations sur le déploiement (Deploy), consultez la rubrique Trouver et déployer des ressources Live.
- Pour plus d'informations sur le déploiement d'un Package (Package), consultez la rubrique Assistant Déploiement du package de la ressource.

Assistant Déploiement du package de la ressource

Si vous avez créé un package de ressources et que vous l'avez enregistré sur un lecteur réseau, vous pouvez utiliser l'Assistant Déploiement du package de la ressource pour déployer les ressources manuellement vers un service ou un groupe de services, sans souscrire à ces ressources. NetWitness Suite accepte les packages dans les fichiers **.nwp** ou **.zip**.

Le déploiement manuel des ressources fait qu'elles sont directement déployées vers les services sans tirer parti des puissantes fonctions de gestion des ressources de NetWitness Suite.

Si vous souhaitez recevoir une notification et des mises à jour pour les ressources mises à jour et si vous souhaitez pouvoir retirer facilement des ressources d'un service, vous devez souscrire aux ressources dans la vue Recherche Live et les déployer dans la vue **Configuration Live**.

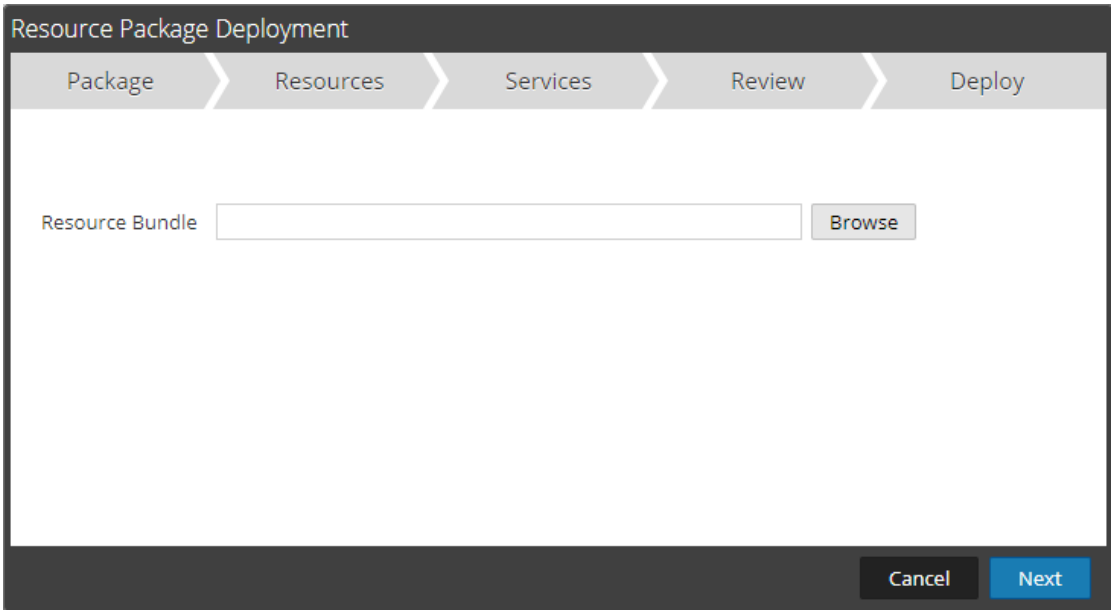
Remarque : utilisez NetWitness Suite Live pour créer des packages de ressources ; il s'agit d'une application distincte qui ne fait pas partie de NetWitness Suite. Lorsque vous sélectionnez **Package** > **Créer** dans la barre d'outils **Recherche Live - Ressources correspondantes**, la fenêtre Outil de package de contenu s'affiche. Vous pouvez y choisir des ressources à inclure à un package, puis enregistrer ce dernier en tant que fichier de package NetWitness Suite.

L'autorisation requise pour accéder à cette vue est **Déployer les ressources Live**.

Pour accéder à cette vue :

1. Dans le Menu principal, sélectionnez **CONFIGURER > CONTENU LIVE**.
2. Dans la barre d'outils **Recherche Live - Ressources correspondantes**, sélectionnez **Package** > **Déploiement.**

   L'assistant Déploiement du package de la ressource s'affiche.



Fonctions

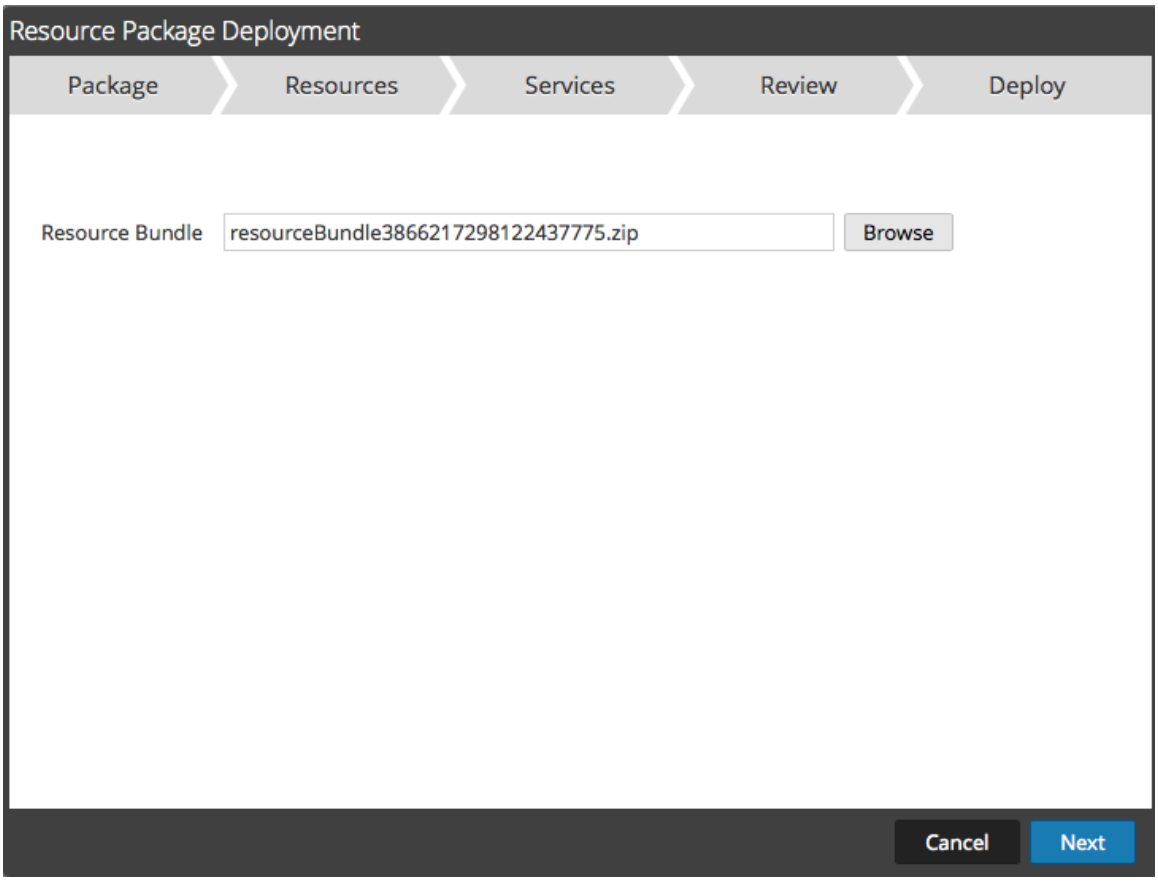
L'assistant Déploiement contient cinq onglets : **Package, Ressources**, **Services**, **Vérifier** et **Déployer**.
Utilisez **Fermer** pour quitter avant d'exécuter l'assistant.

Lorsque vous avez fini de suivre les étapes de l'assistant, NetWitness Suite retourne à la vue Ressources Live.

Onglet Package

Cet onglet permet de sélectionner un package de ressources à partir de votre réseau.

C'est un exemple d'onglet Package, avec un bundle de ressources déjà sélectionné.



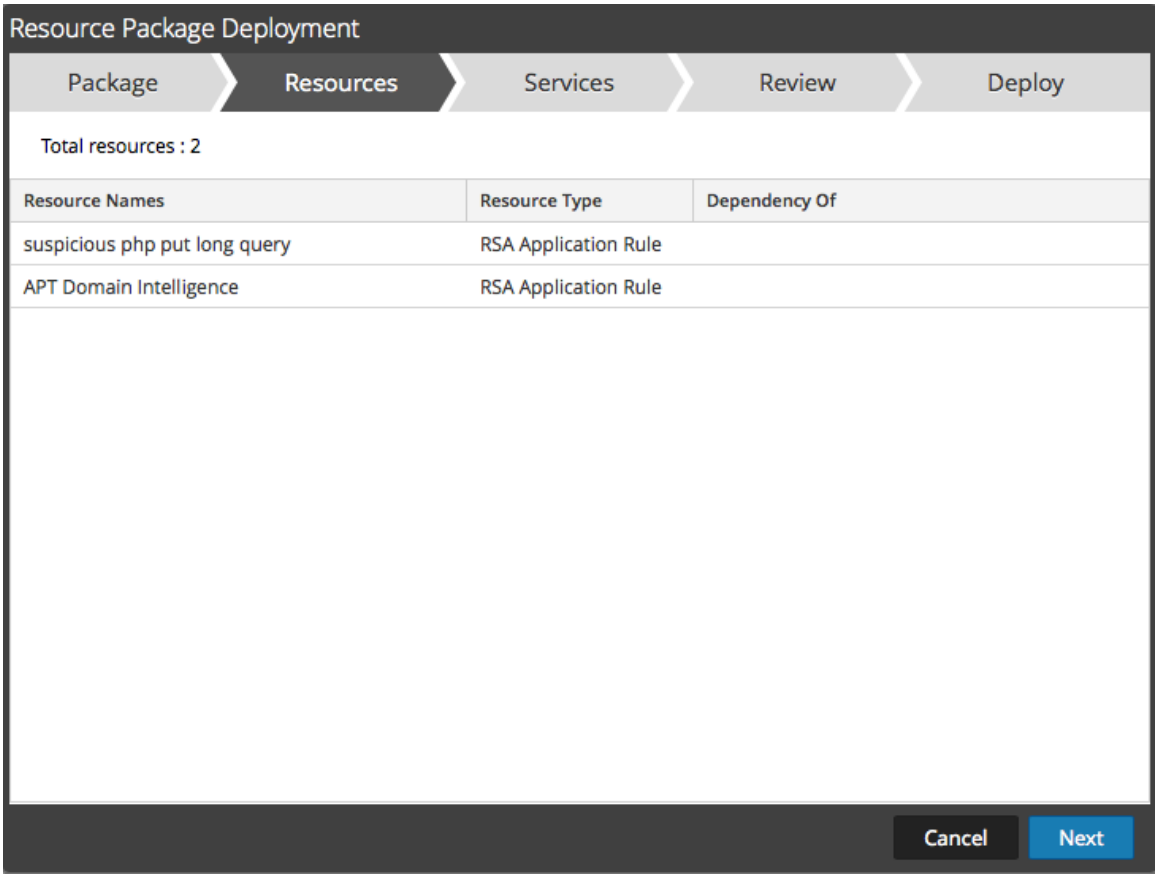
Le tableau suivant décrit les éléments de l'onglet Package.

Colonne	Description
Package de ressources	Le champ de saisie pour indiquer un package de ressources. Vous pouvez saisir un chemin dans ce champ ou rechercher le package en utilisant le bouton Browse.
Boutons de commande	
Parcourir	Ce bouton ouvre une boîte de dialogue Téléchargement de fichier dans laquelle vous pouvez parcourir le système de fichiers local et sélectionner un package.
Annuler	Annule le déploiement et ferme l'assistant.
Suivant	Affiche l'onglet suivant de l'assistant.

Onglet Ressources

Cet onglet affiche les ressources du package.

La figure suivante donne un exemple de l'onglet Ressources.



Le tableau suivant décrit les éléments de l'onglet Ressources.

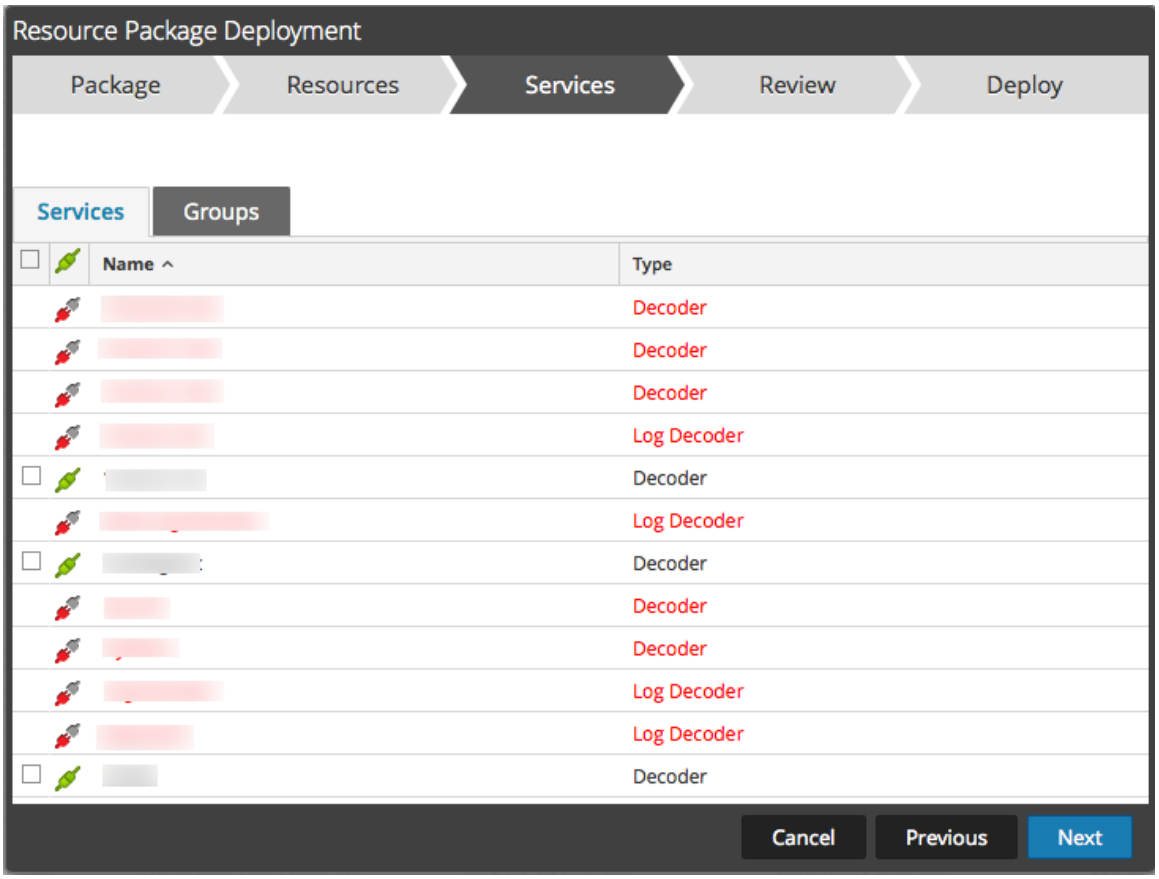
Colonne	Description
Nom de ressource	Affiche le nom des ressources que vous avez sélectionnées (par exemple **NetWitness Lua Library**).
Type de ressource	Affiche les types de ressources que vous avez sélectionnées (par exemple **RSA Lua Parser**)
Dépendance de	Affiche la ou les ressources desquelles dépend la ressource sélectionnée (par exemple **AIM lua**).

Onglet Services

Sélectionnez les services vers lesquels vous souhaitez déployer les ressources de ce package.

L'onglet Services contient deux onglets : **Services** et **Groupes**. Ils fournissent une liste des services et des groupes de services configurés dans ADMIN > vue Services. Les colonnes représentent un sous-ensemble des colonnes disponibles dans la vue Services. Vous pouvez sélectionner les services ou les groupes de services vers lesquels vous souhaitez déployer les ressources de ce package.

Il s'agit d'un exemple de l'onglet Services.



Le tableau suivant décrit les éléments de l'onglet Services.

Colonne	Description
Services	
☐	Permet de sélectionner les services au niveau desquels vous souhaitez déployer le contenu. Vous pouvez sélectionner une combinaison de services et de groupes de services.
Nom	Affiche les services de votre environnement au niveau desquels vous pouvez déployer le contenu.

Colonne	Description
Hôte	Affiche le nom de l'hôte de ressource.
Type	Affiche le type de service NetWitness Suite.
Groupes	
	Permet de sélectionner les groupes de services (si vous avez des groupes de services définis dans votre environnement).
Nom	Affiche les noms des groupes de services.

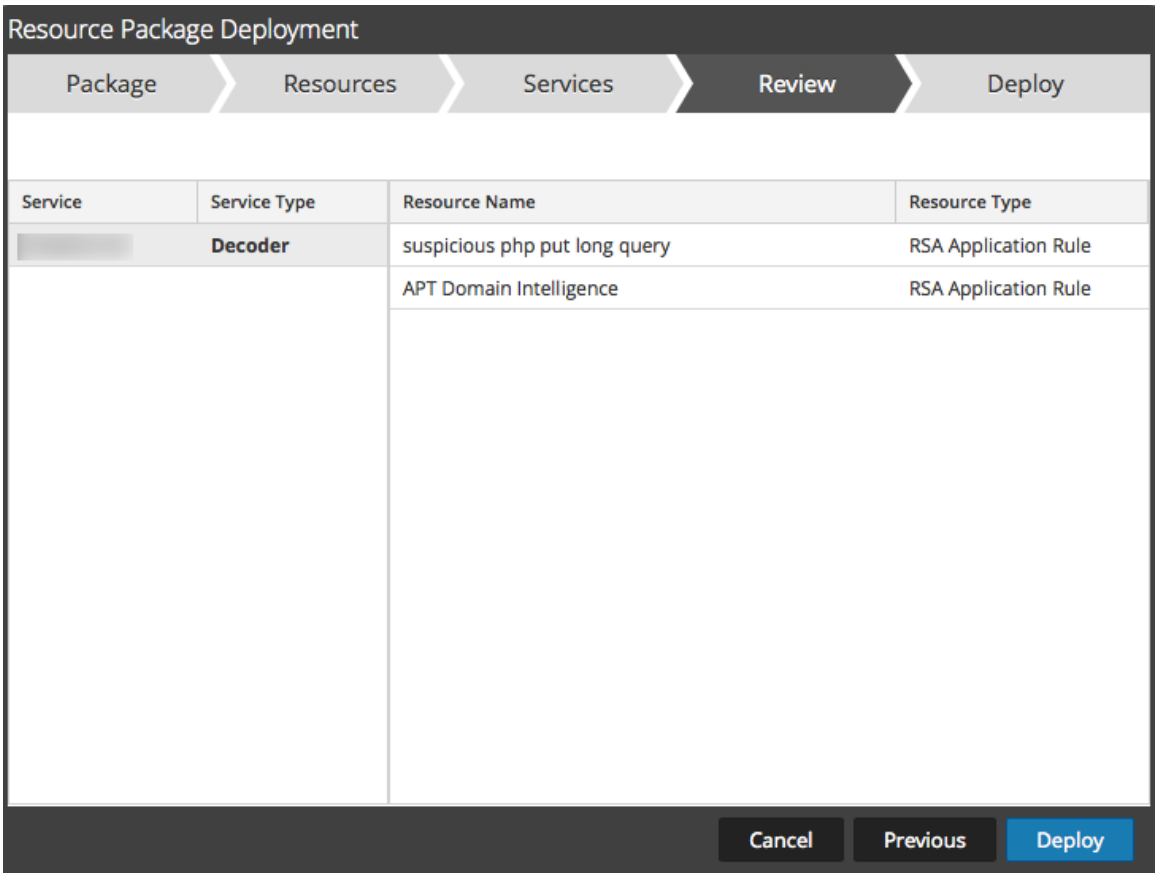
Onglet Révision

Affiche les ressources et les services sur lesquels les ressources seront déployées.

Sous cet onglet, vous pouvez :

- Passer en revue le contenu et les services avant de les déployer.
- Lancez le déploiement des ressources.

La figure suivante donne un exemple de l'onglet Révision.



Le tableau suivant décrit les éléments de l'onglet Révision.

Colonne	Description
Informations de service	
Service	Affiche les services de votre environnement au niveau desquels vous pouvez déployer le contenu.
Type de service	Affiche le type de chaque service NetWitness Suite (type d'hôte/de service).
Informations relatives aux ressources	
Nom de ressource	Affiche le nom des ressources que vous avez sélectionnées (par exemple, **NetWitness Lua Library**).
Type de ressource	Affiche les types de ressources que vous avez sélectionnées (par exemple **RSA Lua Parser**).

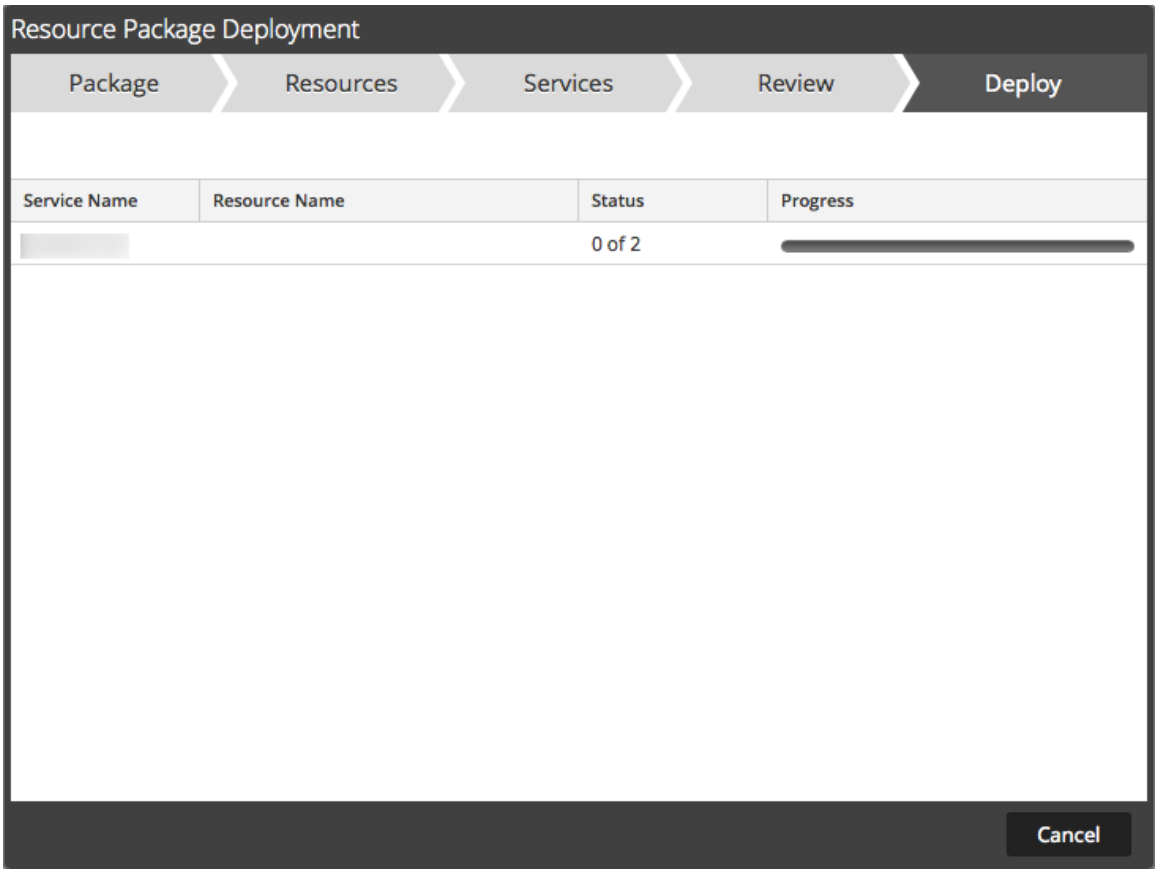
Colonne	Description
Déployer	Lance le déploiement des ressources et affiche la page **Déploiement** (la dernière de l'assistant).

Onglet Déploiement

Sous cet onglet, vous pouvez :

- Afficher la progression de la tâche.
- Annuler la tâche

Il s'agit d'un exemple de l'onglet Déploiement.



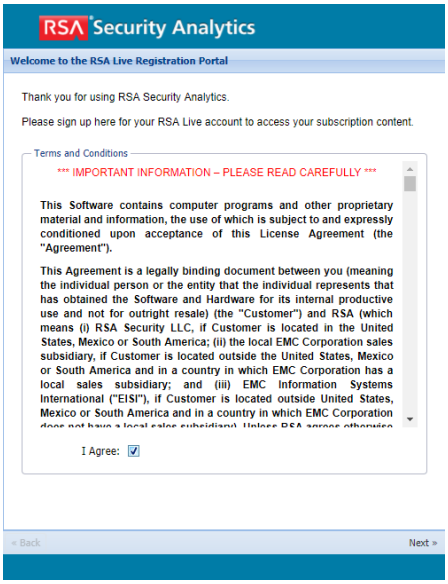
Le tableau suivant décrit les éléments de l'onglet Déploiement.

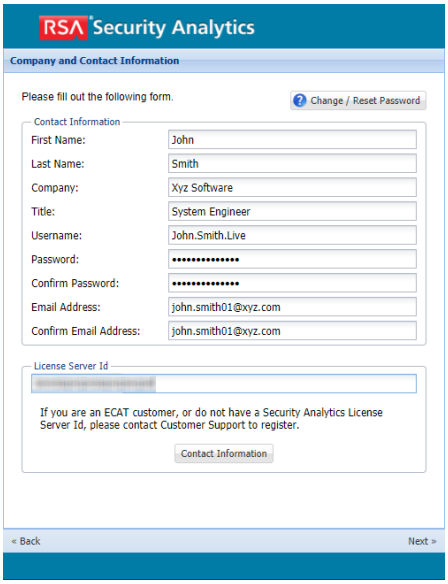
Fonction	Description
Nom du service	Nom des services sur lesquels les ressources sont déployées.

Fonction	Description
Nom de ressource	Nom de ressource.
État	État du déploiement manuel.
Progression	Progression du déploiement manuel dans une barre de progression. Lorsque l'action est terminée, la barre est verte et pleine.
Boutons de commande	
Fermer	Ferme l'assistant.
Erreurs	Ne s'affiche que si NetWitness Suite a rencontré des erreurs. Cliquez pour afficher les erreurs.
Réessayer	Ne s'affiche que si NetWitness Suite a rencontré des erreurs. Cliquez sur ce bouton pour essayer de déployer les ressources à nouveau à l'aide de l'assistant.

Portail d'inscription RSA Live

Le portail d'inscription RSA Live est un assistant en libre-service dans lequel les clients peuvent configurer un compte Live et modifier ou réinitialiser leur mot de passe. Un compte Live est nécessaire pour accéder aux flux, parsers, règles et autres contenus de la bibliothèque RSA Live. Pour accéder au portail, accédez à l'URL suivante : https://cms.netwitness.com/registration/.





Acceptez les conditions générales et cliquez sur **Suivant** : pour accéder aux champs de configuration d'un compte. Les champs affichés sont les suivants : Informations sur le contact, Niveau d'abonnement et ID de serveur de licences.

Le tableau suivant répertorie les champs de la section Informations sur le contact et leur description :

Paramètre	Description
Modifier/Réinitialiser le mot de passe	Permet aux utilisateurs de modifier ou de réinitialiser leur mot de passe RSA Live.
Prénom	Votre prénom.
Nom	Votre nom de famille.
Entreprise	Nom de votre entreprise.
Titre	Votre fonction ou poste dans l'entreprise.
Nom d'utilisateur	Nom d'utilisateur employé pour la connexion au compte RSA Live. Le nom d'utilisateur doit contenir un minimum de 9 caractères et un maximum de 60 caractères.

Paramètre	Description
Mot de passe	Mot de passe du compte RSA Live. Ce mot de passe doit contenir entre 9 et 60 caractères, dont au moins un en majuscules, un en minuscules, un nombre et un caractère spécial.
Confirmer le mot de passe	Confirmation de votre mot de passe.
Adresse e-mail	Adresse e-mail à laquelle vous souhaitez recevoir les notifications relatives au compte Live.
Confirmer l'adresse e-mail	Confirmation de l'adresse e-mail.
Niveau d'abonnement/Confirmer le niveau d'abonnement	• **De base** : fournit un accès au contenu Live qui est balisé pour des groupes comme Basic, Panorama for Log Decoder et Spectrum for Malware Analysis. • **Amélioré** : fournit un accès au contenu Live qui est balisé pour des groupes comme Enhanced, Basic, Panorama for Log Decoder et Spectrum for Malware Analysis. • **Premium** : fournit un accès au contenu Live qui est balisé pour des groupes comme Premium, Verisign Premium, Enhanced, Basic, Panorama for Log Decoder et Spectrum for Malware Analysis.
ID de serveur de licences	ID de licence figurant sur la page **ADMIN > SYSTÈME > Info**. **Attention :** dans NetWitness Suite, l'ID de serveur de licences doit être valide et être enregistré sur le serveur Flexera. Si tel n'est pas le cas, contactez le Support Clients de RSA.

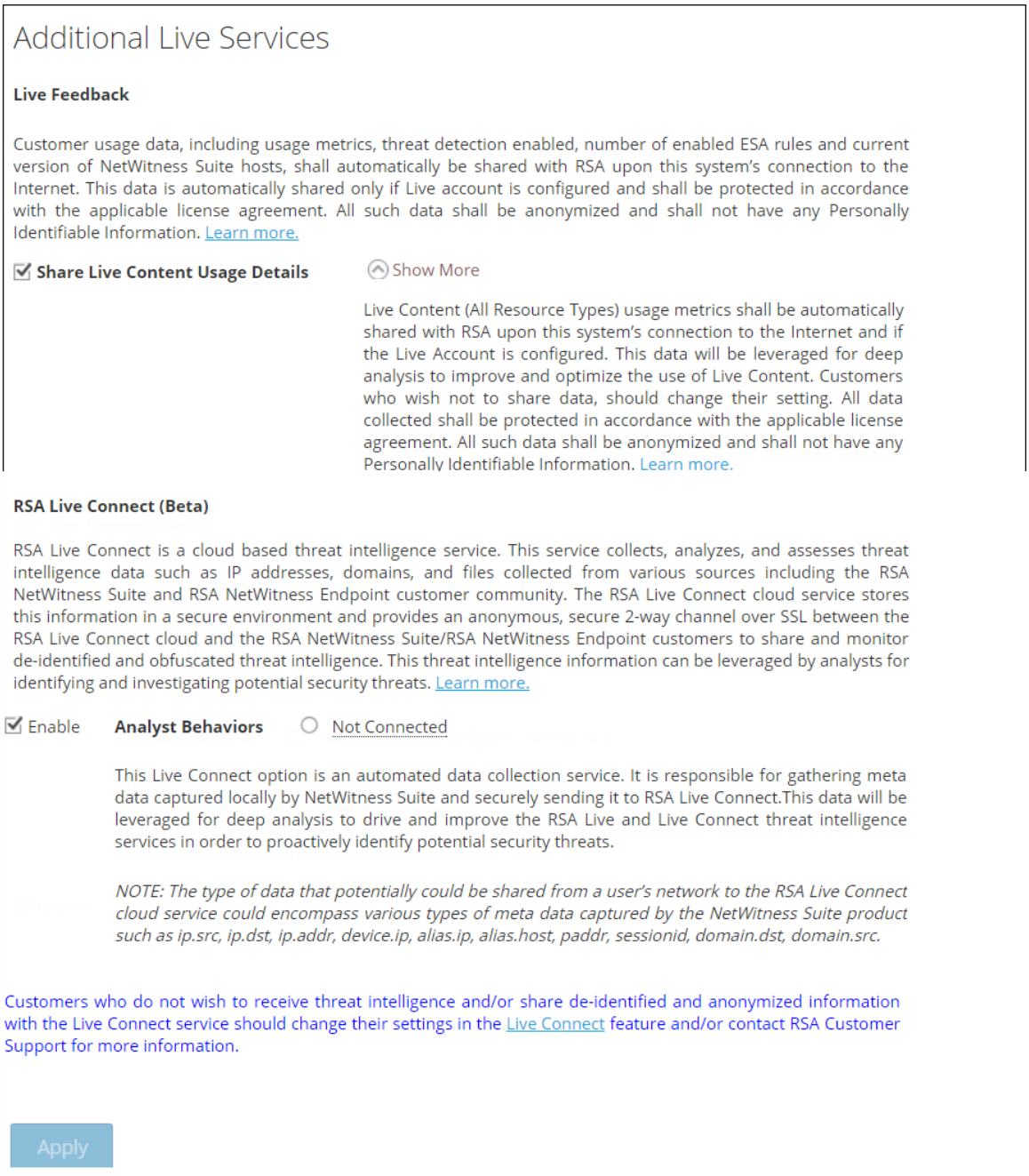
Commentaires et Partage de données NetWitness Suite

Cette rubrique présente les fonctions Commentaires et Partage de données de NetWitness Suite.

Les paramètres de ces fonctions sont disponibles dans **ADMIN** > **SYSTÈME** > vue **Services Live**, dans la section Services Live supplémentaires.

Services Live supplémentaires

La participation aux Services Live supplémentaires est configurée dans **ADMIN > SYSTÈME > Services Live**.



Live Feedback

Live Feedback a été conçu pour améliorer RSA NetWitness Suite.

Dès qu'un compte Live est configuré, les données d'utilisation sont partagées avec RSA. Les données sont protégées conformément au contrat de licence applicable. Les données d'utilisation client, notamment les metrics d'utilisation et la version actuelle des hôtes NetWitness Suite, sont automatiquement partagées avec RSA lors de la connexion du système à Internet.

Avant que les données soient envoyées à RSA, toutes les informations personnellement identifiables sont supprimées. De ce fait, seules les données d'utilisation anonymes sont transférées à RSA.

Pour plus d'informations, consultez la rubrique **Présentation de Live Feedback** dans le*Guide de Configuration système*.

RSA Live Connect

RSA Live Connect est un service de renseignements sur les menaces basé sur le Cloud. Ce service collecte, analyse et évalue les renseignements sur les menaces (adresses IP, domaines, fichiers,etc.) qui sont collectés à partir de différentes sources, y compris la communauté de clients RSA NetWitness Suite et RSA ECAT. RSA Live Connect se compose des fonctions suivantes :

- Threat Insights
- Comportements d'analyste

Threat Insights

Threat Insights fournit aux analystes la possibilité d'extraire des données de renseignement sur les menaces, telles que des informations liées à la propriété intellectuelle, du service Live Connect, qui seront exploitées par les analystes pendant la procédure d'enquête.

Par défaut, **Threat Insights** est activé dans la section **Services Live supplémentaires**. Si le service Context Hub est configuré, Live Connect est ajouté automatiquement comme source de données pour Context Hub. Pour plus d'informations, consultez la rubrique **Configurer une source de données Live Connect pour Context Hub** dans le *Guide de configuration de Context Hub*.

Avec Live Connect en tant que source de données pour Context Hub, vous pouvez utiliser l'option Recherche contextuelle dans Procédure d'enquête > vue Naviguer ou Procédure d'enquête > vue Événements pour extraire des informations contextuelles. Pour obtenir des instructions, reportez-vous à Afficher le contexte supplémentaire pour un point de données.

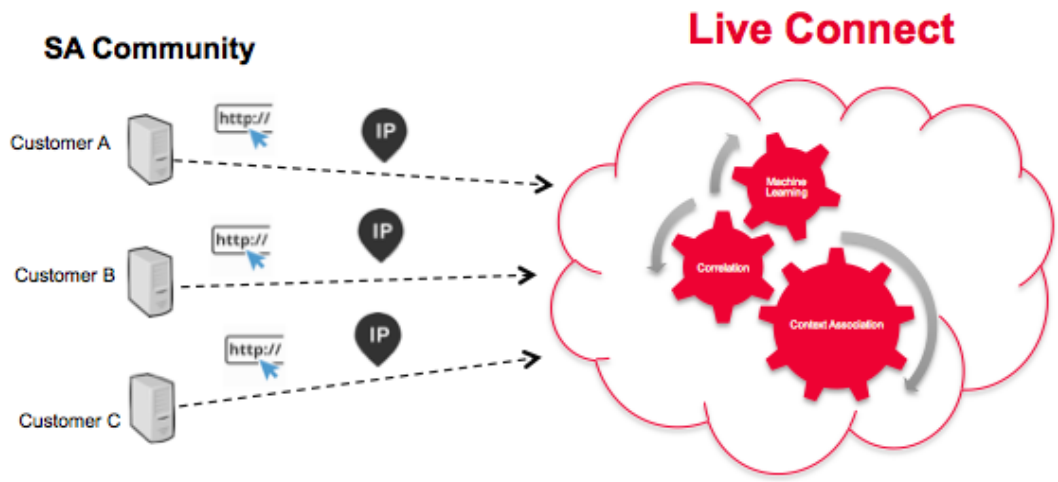
Comportements d'analyste

Comportements d'analyste est une fonction dans laquelle les analystes participent au partage de données avec la communauté RSA. Il s'agit d'un service de collecte de données automatisée. Son objectif est de partager des données de renseignements sur les menaces potentielles sur le service de Cloud RSA Live Connect à des fins d'analyse. Le type de données pouvant être partagé depuis votre réseau d'un utilisateur vers RSA Live Connect peut inclure différents types de métadonnées capturées par NetWitness Suite, telles que ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src.

Remarque : Toutes les données collectées localement sont désidentifiées et obfusquées, puis envoyées de manière sécurisée et anonyme au service de Cloud RSA Live Connect où elles sont stockées dans un environnement sécurisé.

Description

Live Connect Threat Data Sharing a été développé sous forme d'une plate-forme de renseignements sur les menaces communautaires liées à Live Connect.



Ce service présente les caractéristiques et objectifs suivants :

- Crowdsourcing : la Communauté RSA contribue à la collecte intégrale des renseignements
- Collecter et analyser les données de façon centralisée depuis la communauté RSA
- Réduire la durée de cycle des renseignements de plusieurs jours à quelques minutes

Voici certains détails à prendre en compte :

- Nous tirons profit de l'activité de procédure d'enquête des analystes
- Nous collectons les métadonnées telles que les adresses IP et les noms de domaine
- Nous effectuons une analyse approfondie des données : tendances, corrélation, détection des anomalies
- N'oubliez pas que cette fonctionnalité est actuellement en version bêta.

Participation

La participation du client est facultative. Lors de la première installation ou de la mise à niveau vers NetWitness Suite 11.0, un écran de confirmation s'affiche. Le programme s'ouvre par défaut, mais vous pouvez refuser son ouverture.

Authentification du Cloud

L'authentification d'accès au programme est effectuée dans l'interface utilisateur NetWitness Suite dans laquelle vous configurez le compte Live dans la section Services Live.

Configuration

Pour afficher ou modifier les paramètres de Live Connect Threat Data Sharing, ouvrez le menu Menu principal, sélectionnez **ADMIN > SYSTÈME > Services Live**. Activez ou désactivez la case à cocher **Activer** pour participer ou arrêter de participer au programme.

Collecte des données

Les données sont collectées comme suit :

- Attribution de données Anonyme
- Source de données Sous-ensemble de clés méta et de métavaleurs des vues de la page d'un analyste NetWitness Suite à partir des logs de requêtes NetWitness Suite Core.
- Processus de récolte des logs de requêtes :
  - Calendrier : Mode de traitement par lots toutes les 24 heures (de 4:00 à 6:00 UTC)
  - Collecte des logs : le serveur NetWitness Suite collecte les entrées de log des périphériques NetWitness Suite Core pour les 24 heures précédentes
  - Entrées de log : Seuls les appels d'API de requête SDK qui contiennent une clause where sont collectés
  - Analyse des attributs de log : Chaque entrée doit contenir l'un des indicateurs de clés méta suivants : **ip.src**, **ip.dst**, **ip.addr**, **device.ip**, **alias.ip**, **alias.host**, **paddr**, **sessionid**, **domain.dst** ou **domain.src**. Si tel est le cas, les clés méta et les valeurs méta issues de l'entrée seront collectées.

Remarque : lorsque les critères ci-dessus sont remplis, NetWitness Suite n'envoie pas seulement les indicateurs des clés méta, mais toutes les clés méta et les métavaleurs de la requête au Cloud.

Le rapport de log est envoyé au format JSON via le protocole SSL. Il contient :

- Horodatages
- Nom d'utilisateur Live CMS (sha256)
- NetWitness SuiteID de serveur de licences (sha256)
- Liste des ID de point de terminaison SA (sha256)
- Valeurs méta collectées (MD5 et SHA256 hachés)

Exemple

Cette section répertorie les entrées d'un log, puis la section correspondante des données extrapolées.

Section d'un fichier log :

```
User admin (session 204298, 10.4.50.60:57454) has issued values (channel 205237)
(thread 2332): fieldName=filter id1=1 id2=23138902 threshold=100000 size=20
flags=sessions,sort-total,order-descending,ignore-cache where="(alias.host =
'mail.google.com') && (ip.src = 161.253.31.130) && time=\"2015-12-07 18:08:00\"-
\"2015-12-07 21:07:59\""
```

Extrapolation des données avec hachage :


```
{
    timestamp: 1452282588000,
    session: 204298,
    id1: 1,
    id2: 23138902,
    userName: "8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918",
    loggerName: "SDK-Values",
    timeRange: "\"2015-12-07 18:08:00\"-\"2015-12-07 21:07:59\"",
  - metaList: [
      - {
            metaKey: "alias.host",
          - properties: {
                domain_hint: "mai*********.com",
                domain_tld: "com",
                md5_value: "be5cab0695415d9363d18ad1345c73eb",
                sha256_value: "3f2728499a4b29460f3e3150df508e06b19edf0f58efd051fac777844d28e452"
            }
        },
      - {
            metaKey: "ip.src",
          - properties: {
                md5_value: "03b81ffdff109a05a3dac88dbec10c59",
                sha256_value: "1d88c6893797c896070bd5470d0026e11b515d5dee97c6173771a43719fa7e78"
            }
        }
    ]
},
```


Résolution des problèmes

Cette section présente brièvement comment résoudre les problèmes liés à Live Connect Threat Data Sharing.

Exemple de récupération de log de requête

Pour récupérer un échantillon de données de renseignements sur les menaces envoyé à Live Connect, construisez une URL en définissant les paramètres suivants :

- **sendReport** : la valeur est **true** ou **false** : true pour envoyer ce rapport au serveur Live Connect. False pour se contenter de créer le rapport et de le consulter. La valeur par défaut est false.
- **hashValues** : la valeur est **true** ou **false** : true pour hacher les valeurs en md5/sha256. False pour afficher les valeurs en texte clair : n'utiliser que pour l'affichage manuel. La valeur par défaut est false.

- **startDate / endDate** : Dates des limites temporelles des entrées de log. Format : AAAA-MM-JJ HH:mm:ss

Voici un exemple de l'URL à utiliser pour récupérer les logs de requête :

```
https://<server>/admin/liveconnect/force_aggregation?startDate=2016-01-18%2000:00:00&endDate=2016-01-19%2010:10:00&sendReport=false&hashValues=true
```

Consignation système : Débogage

Vous pouvez accéder à certaines informations de débogage en procédant comme suit.

1. Sélectionnez **ADMIN > SYSTÈME > Consignation système**.
2. Cliquez sur l'onglet **Paramètres**.
3. Dans la section Configuration des packages, sélectionnez **com > netwitness > plateforme > serveur > liveconnect > service (DÉBOGAGE)**.