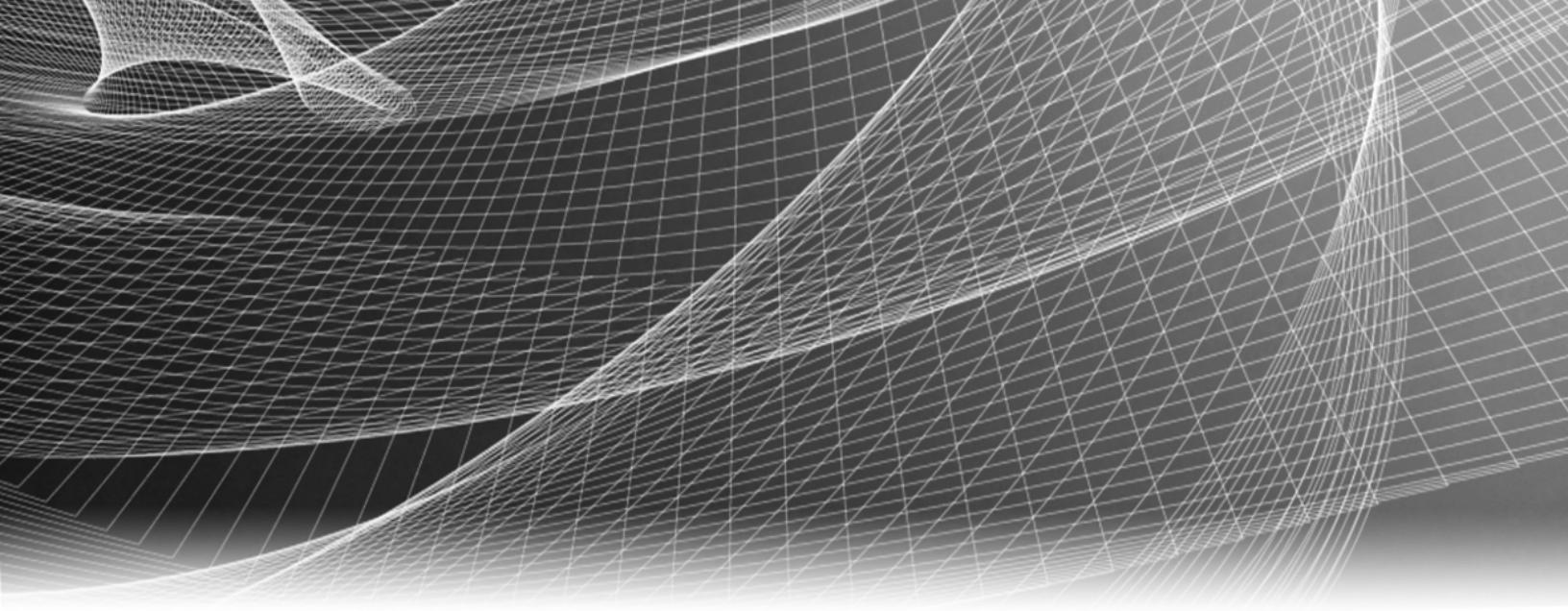


RSA Security Analytics

Gestion des services en direct pour la Version 10.6

RSA

EMC²

Trademarks

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Gestion des services en direct

Gestion des services en direct

Ce guide présente l'accès Security Analytics à Security Analytics Live. RSA Security Analytics Live constitue la passerelle à un environnement riche offrant un accès aux feeds, outils et autres ressources.

Last Modified: August 10 2016, 9:33AM

Contenu Live dans Security Analytics

Cette rubrique fournit une présentation de l'outil de gestion de contenu Live.

Security Analytics Live

Live est le composant de Security Analytics qui gère la communication et la synchronisation entre les services Security Analytics et une librairie de contenu Live disponibles pour les clients RSA Security Analytics. Live constitue une interface simple qui permet de parcourir, sélectionner et déployer du contenu entre le système de gestion de contenu Live de Security Analytics et les services et logiciels Security Analytics. En plus de gérer les flux provenant de la librairie CMS, Live permet aux utilisateurs de déployer des flux et packages personnalisés.

La librairie CMS

La librairie du système de gestion de contenu (CMS) (appelée *Live*) est une source précieuse de ressources de sécurité Internet récentes pour les clients Security Analytics. 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.

Avant d'accéder à CMS, vous devez configurer et initier la synchronisation entre le serveur CMS et Security Analytics.

Last Modified: August 10 2016, 9:33AM

Procédures requises

Cette rubrique explique comment configurer Live dans Security Analytics.

Liste de contrôle Gestion des ressources Live

Après avoir étudié cette rubrique, l'administrateur aura une pleine compréhension de la configuration de Live dans Security Analytics, de la recherche de ressources dans Live et de leur gestion.

Étape	Description
1	Configurer votre 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.
2	Configurer Live dans Security Analytics en configurant une connexion avec le serveur CMS
3	Utiliser la vue recherche Live pour rechercher des ressources Live
4	Gérer les ressources Live

Last Modified: August 10 2016, 9:33AM

RSA

Étape 1. Créer un compte Live

Cette rubrique décrit comment créer un compte Live à l'aide du portail RSA Live Registration Portal sur le serveur CMS.

Introduction

La librairie 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.

Conditions préalables

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

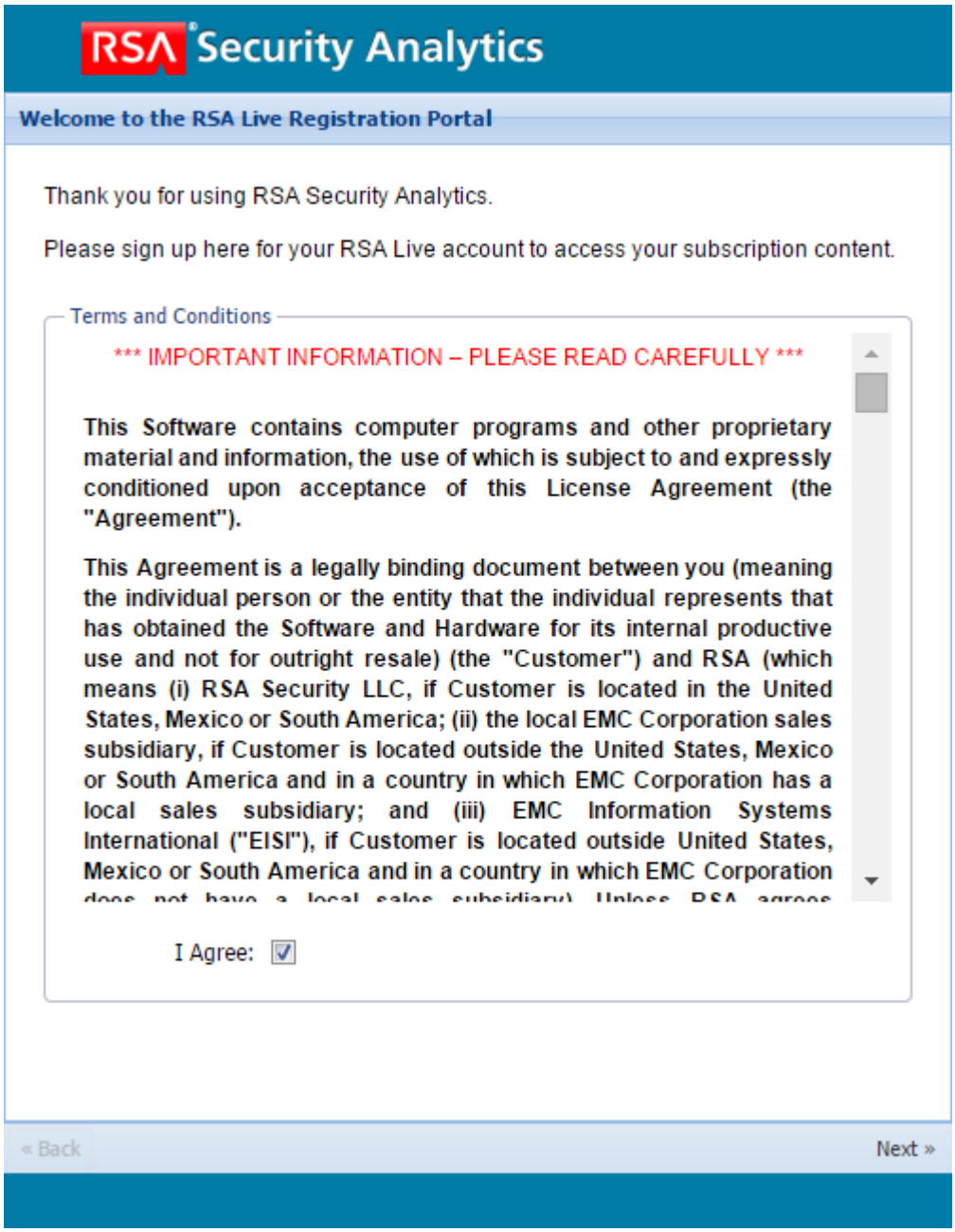
- Connexion à Internet active pour l'accès au portail.
- Un serveur de licence Security Analytics valide et enregistré sur le serveur Flexera, avant que vous ne puissiez vous inscrire sur un compte Live. Vous pouvez afficher l'ID de licence sur le panneau **Administration > Système > Informations**.

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

Procédure

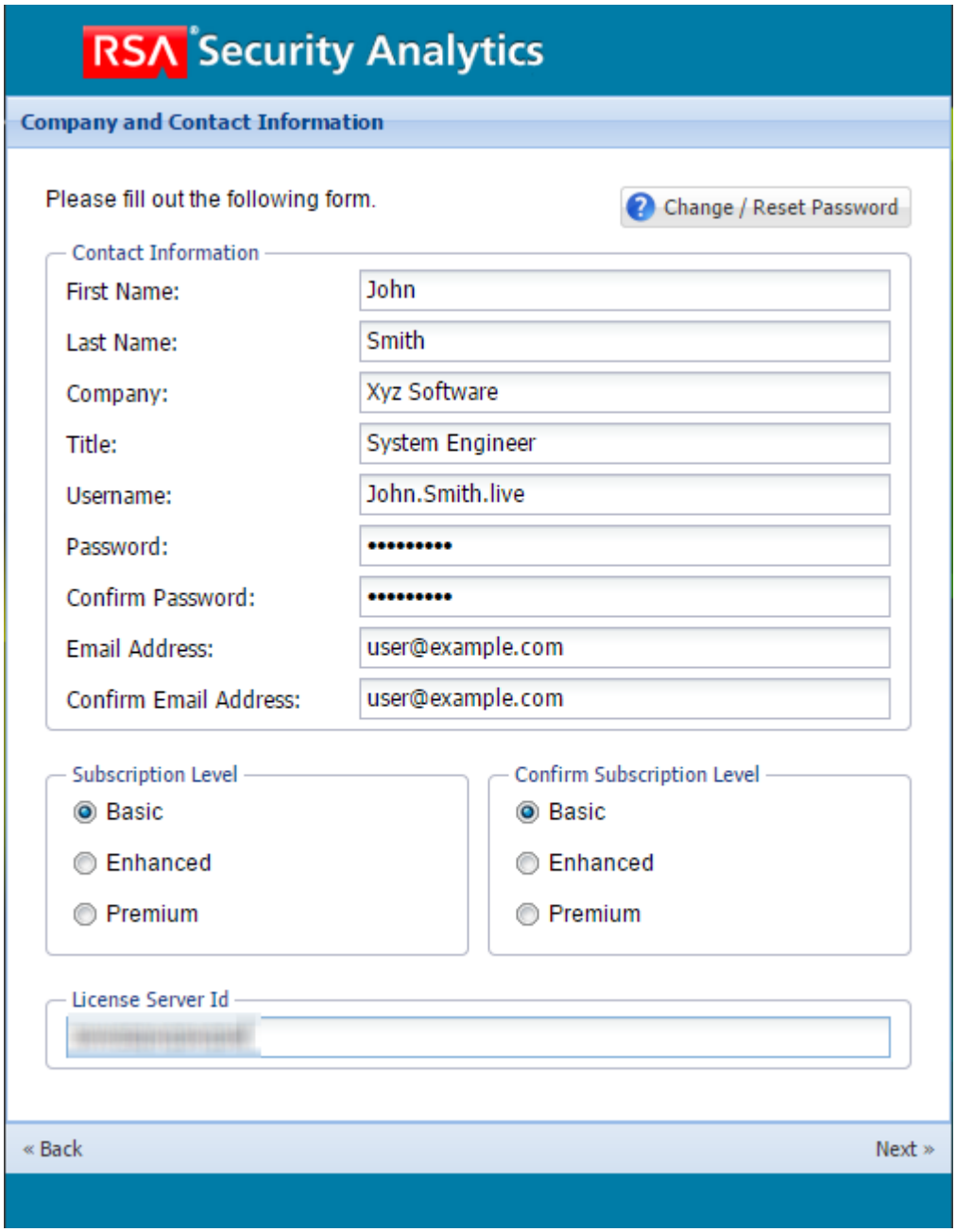
1. Accédez au portail d'inscription RSA Live grâce à l'URL : https://cms.netwitness.com/registration/.
   La page Bienvenue s’affiche.

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 tableau ci-dessous répertorie les informations que vous devez saisir dans la section des informations de contact :

Champ	Description
Prénom	Saisissez votre prénom.
Nom	Saisissez votre nom.
Entreprise	Saisissez le nom de votre entreprise.

Intitulé	Saisissez votre titre ou fonction dans l'entreprise.
Nom d'utilisateur	Saisissez un nom d'utilisateur pour la connexion à votre compte RSA Live. Le nom d'utilisateur doit contenir un minimum de 9 caractères et un maximum de 60 caractères.
Mot de passe	Saisissez le mot de passe pour la connexion à votre compte RSA Live. 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.
Confirmer le mot de passe	Saisissez à nouveau le mot de passe pour confirmer.
Adresse e-mail	Saisissez l'adresse e-mail à laquelle vous souhaitez recevoir des notifications liées au compte Live.
Confirmer l'adresse e-mail	Saisissez à nouveau l'adresse e-mail pour confirmer.

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 **Administration > Système > Informations**.

> ⚠ **Caution:** Assurez-vous que l'ID de serveur de licence sur Security Analytics soit 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.

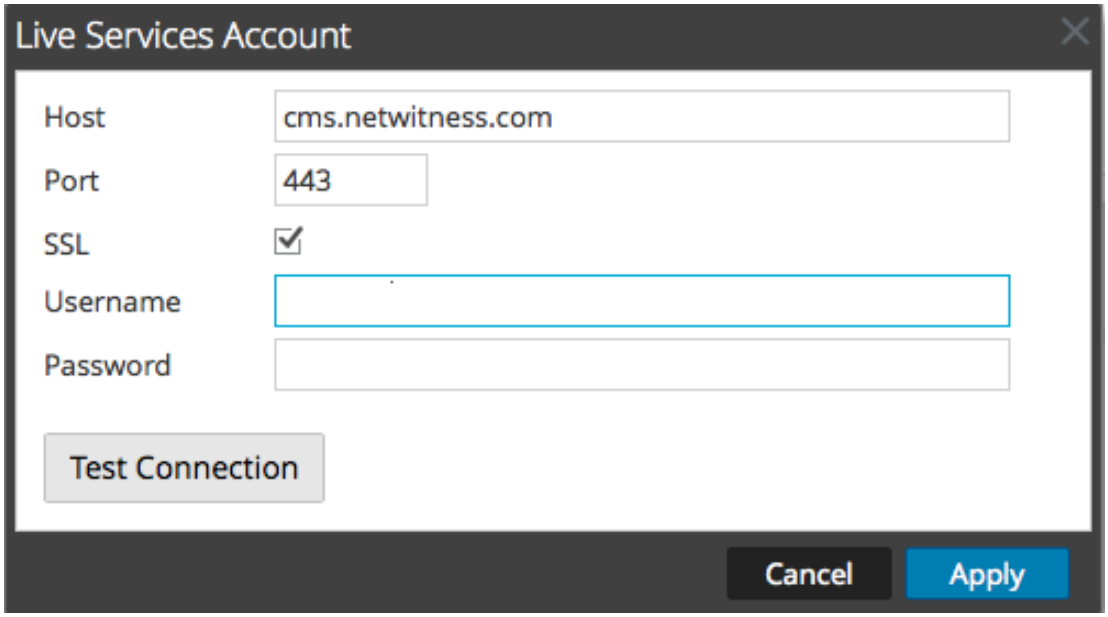
Étape 2. Configurer les services en direct dans Security Analytics

Cette rubrique indique aux administrateurs comment configurer Live sur Security Analytics en configurant la connexion et la synchronisation entre le serveur CMS et Security Analytics.

Pour configurer Live sur Security Analytics, vous configurez la connexion et la synchronisation entre le serveur CMS et Security Analytics. L'interface utilisateur pour cette configuration est Administration > Système > panneau Configuration des Services en direct.

Procédure

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



2. Configurez la période de synchronisation de Security Analytics avec les mises à jour de Live.

Étape 3. Trouver et déployer des ressources Live

Cette rubrique présente aux administrateurs la procédure de recherche 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.

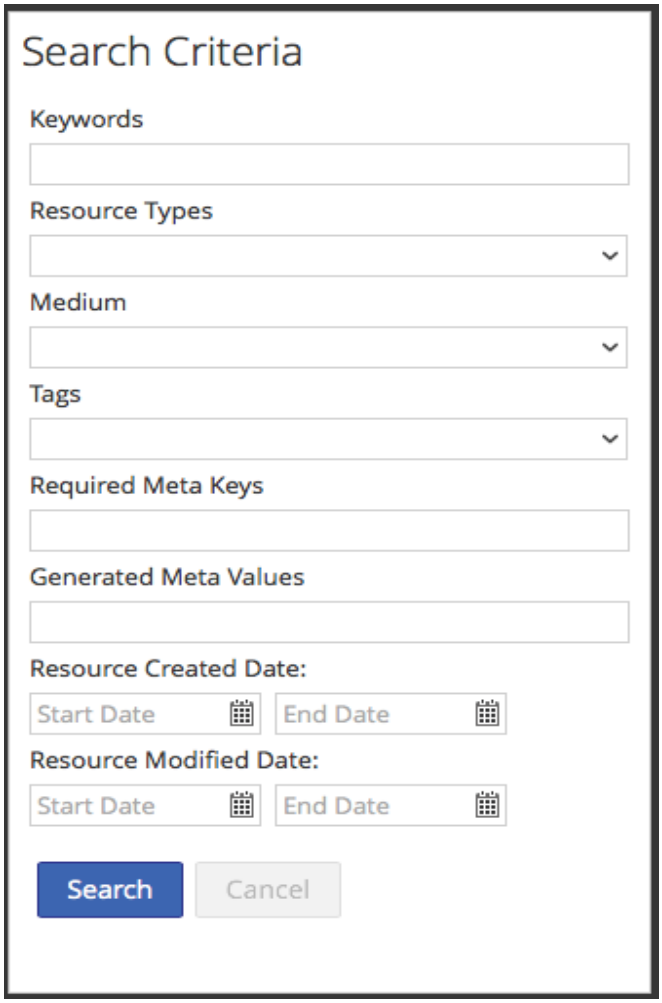
Conditions préalables

Une des conditions préalables de la recherche de ressources Live est de configurer une connexion et une synchronisation entre le serveur CMS et Security Analytics.

Last Modified: August 10 2016, 9:33AM

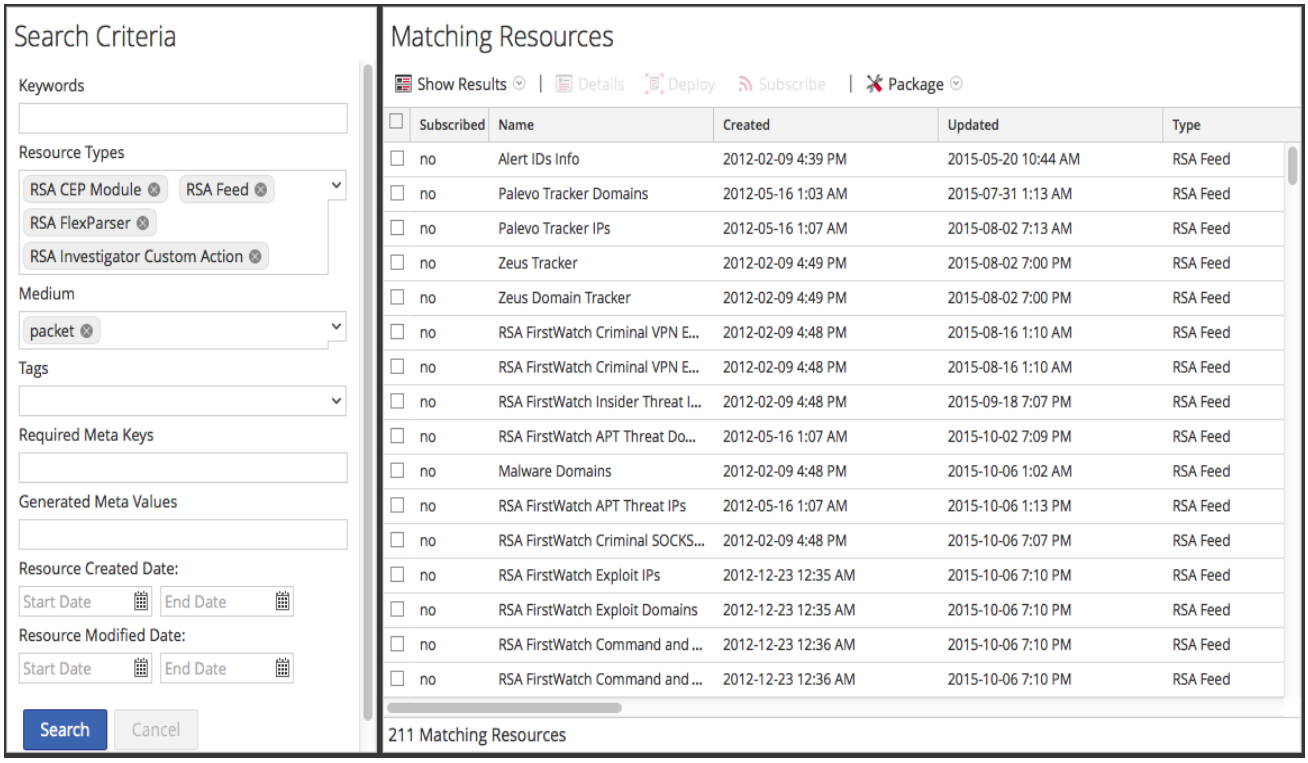
Procédure

1. Dans le panneau **Critères de recherche**, spécifiez des critères de recherche. Entrez un ou plusieurs des éléments suivants :mot-clé, type de ressource, balises, métaclés et métavaleurs.



Last Modified: August 10 2016, 9:33AM

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 métavaleur de ressource dans un résultat.

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.

Last Modified: August 10 2016, 9:33AM

RSA

Étape 4. Gérer les ressources Live

Cette rubrique indique aux administrateurs comment gérer des ressources dans Live.

Introduction

Cette procédure est requise 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.

Conditions préalables

Les conditions préalables pour effectuer cette tâche sont les suivantes :

- Accès Internet
- Compte RSA Live
- Synchronisation du serveur CMS avec Security Analytics

Procédures

Il existe plusieurs workflows possibles pour déployer les ressources dans les services et pour gérer ces déploiements. Il s'agit des workflows suivants :

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

Déploiement manuel

Le worklfow le plus simple pour déployer les ressources sur les services est la méthode manuelle, qui déploie instantanément les ressources au niveau des services. Parce que cette méthode ne nécessite pas d'abonnement aux

ressources, Security Analytics n'effectue pas de synchronisation avec Live lorsque les ressources déployées sont mises à jour dans Live.

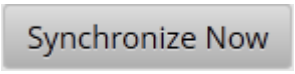
- La vue Live Search vous permet de rechercher des ressources Live, de sélectionner des ressources dans le panneau Résultats concordants, et de les déployer manuellement.
- Dans la vue Ressources Live, vous pouvez déployer la ressource active manuellement à l'aide de l'Assistant Déploiement.

Abonnement et déploiement

Les workflows d'abonnement et de déploiement tirent parti des outils de gestion des ressources disponibles dans Live. En s'abonnant aux ressources, vous acceptez de recevoir des ressources mises à jour conformément à la synchronisation configurée dans le panneau Live de la vue Administration > Système. En ajoutant les ressources souscrites à la liste des déploiements, vous configurez Security Analytics 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 Déploiements.
- Vous pouvez vous désabonner d'une ressource sous l'onglet Inscriptions et la vue Ressources Live.

Pour gérer les abonnements et le déploiement :

1. Dans le panneau **Administration > Système** > **Live** , spécifiez un intervalle auquel Security Analytics 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.

Suppression des ressources déployées

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

Dans la vue Ressources Live boîte de dialogue Déploiement d'un bundle de ressources, vous pouvez déployer un package de contenu créé dans Live sur un ou plusieurs services. Security Analytics accepte les packages au format **.nwp** ou **.zip**.

Last Modified: August 10 2016, 9:33AM

Télécharger les ressources

Dans la vue Ressources Live, vous pouvez télécharger des ressources Live sur votre système de fichiers local à l'aide du bouton **Télécharger**.

Configurer des sources de données

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

Last Modified: August 10 2016, 9:33AM

Procédures supplémentaires

Cette rubrique permet de trouver des informations supplémentaires sur les services en direct dans Security Analytics.

Last Modified: August 10 2016, 9:33AM

Ajouter des ressources souscrites à déployer au niveau des services

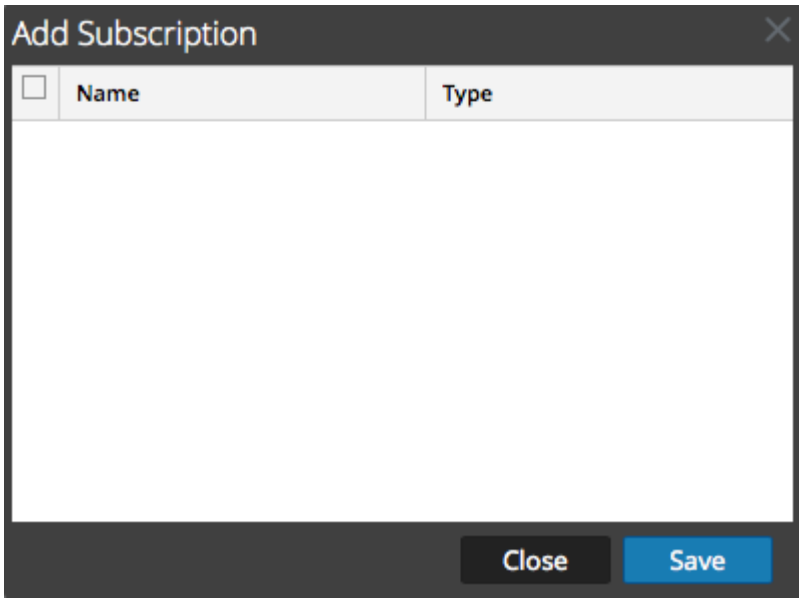
Cette rubrique vous indique comment ajouter des ressources souscrites pour un déploiement au niveau des services.

À la fin de cette procédure, vous aurez ajouté des ressources souscrites à déployer au niveau des services.

Ajouter des ressources souscrites à déployer au niveau des services

Pour ajouter des ressources souscrites à déployer au niveau des services :

1. Accédez à la vue Configurer Live > 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.

Last Modified: August 10 2016, 9:33AM

RSA

Créer un package de ressources

Cette rubrique vous indique comment créer un package de ressources que vous pouvez enregistrer dans un fichier .zip et partager avec d'autres utilisateurs. Pour obtenir plus d'instructions sur la procédure à suivre pour déployer des ressources à partir d'un package, reportez-vous à la rubrique Déployer des ressources à partir d'un package de ressources.

À la fin de cette procédure, vous aurez créé un package de ressources et l'aurez enregistré sur un disque réseau.

Conditions préalables

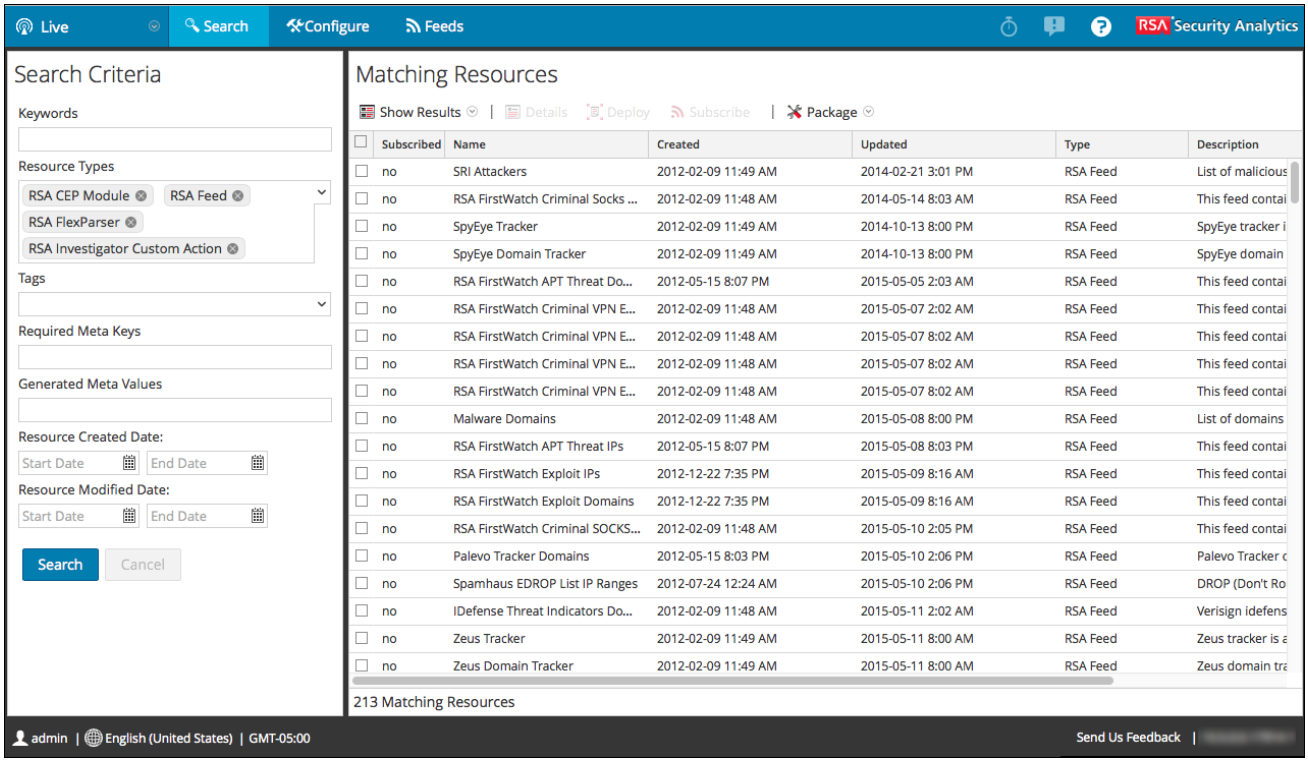
Une condition préalable pour créer des packages de ressources est de configurer la connexion et la synchronisation entre le serveur CMS et Security Analytics et d'avoir la possibilité de rechercher des ressources dans l'interface utilisateur.

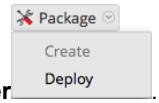
Procédure

Pour créer un package de ressources :

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

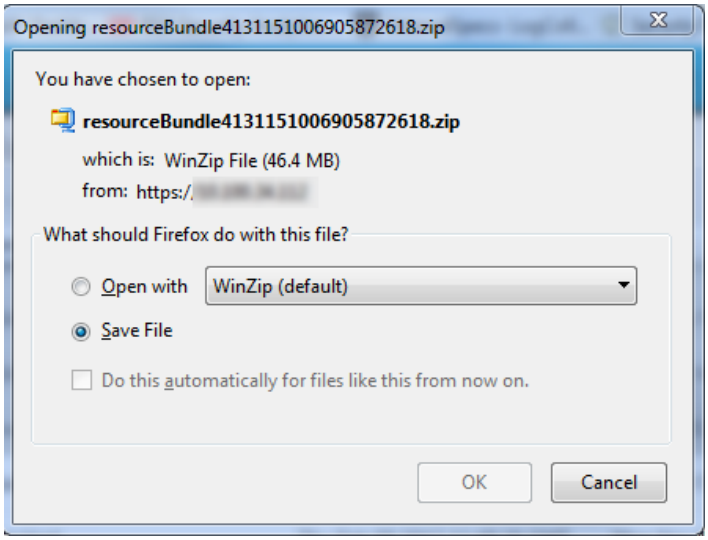
Last Modified: August 10 2016, 9:33AM



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

   Security Analytics 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.

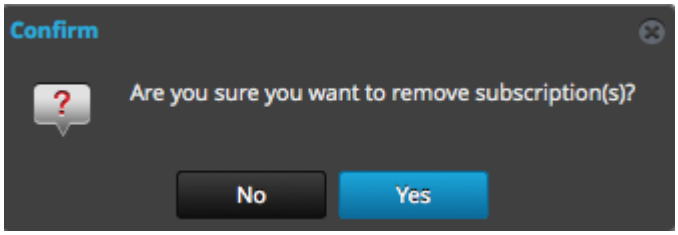
Security Analytics attribue un nom générique au package. Vous devez le renommer lorsque vous l'enregistrez afin qu'il identifie les ressources contenues dans le package.



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 Live Security Analytics. 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.

Déployer des ressources dans Live

Il existe plusieurs méthodes pour déployer des ressources RSA dans Security Analytics Live.

Last Modified: August 10 2016, 9:33AM

RSA

Déployer des ressources manuellement

Cette rubrique décrit la procédure de déploiement des ressources que vous avez actuellement sélectionnées dans la grille Ressources correspondantes de la vue Live Search à l'aide de l'assistant Déploiement.

Introduction

Lorsque vous possédez des résultats suite à l'exploration des ressources dans Security Analytics Live, vous pouvez déployer les ressources manuellement sur un service ou un groupe de services sans vous abonner aux ressources.

Le déploiement manuel des ressources effectue le déploiement sur les services sans tirer parti des puissantes fonctionnalités de gestion de ressource de Security Analytics. 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 Live Configurer.

À la fin de cette procédure, vous aurez :

- Déployé des ressources actuellement sélectionnées dans la grille Ressources correspondantes de la vue Live Search.
- Déployé des ressources à partir d'un package de la ressource précédemment créé sur votre réseau.

Procédure

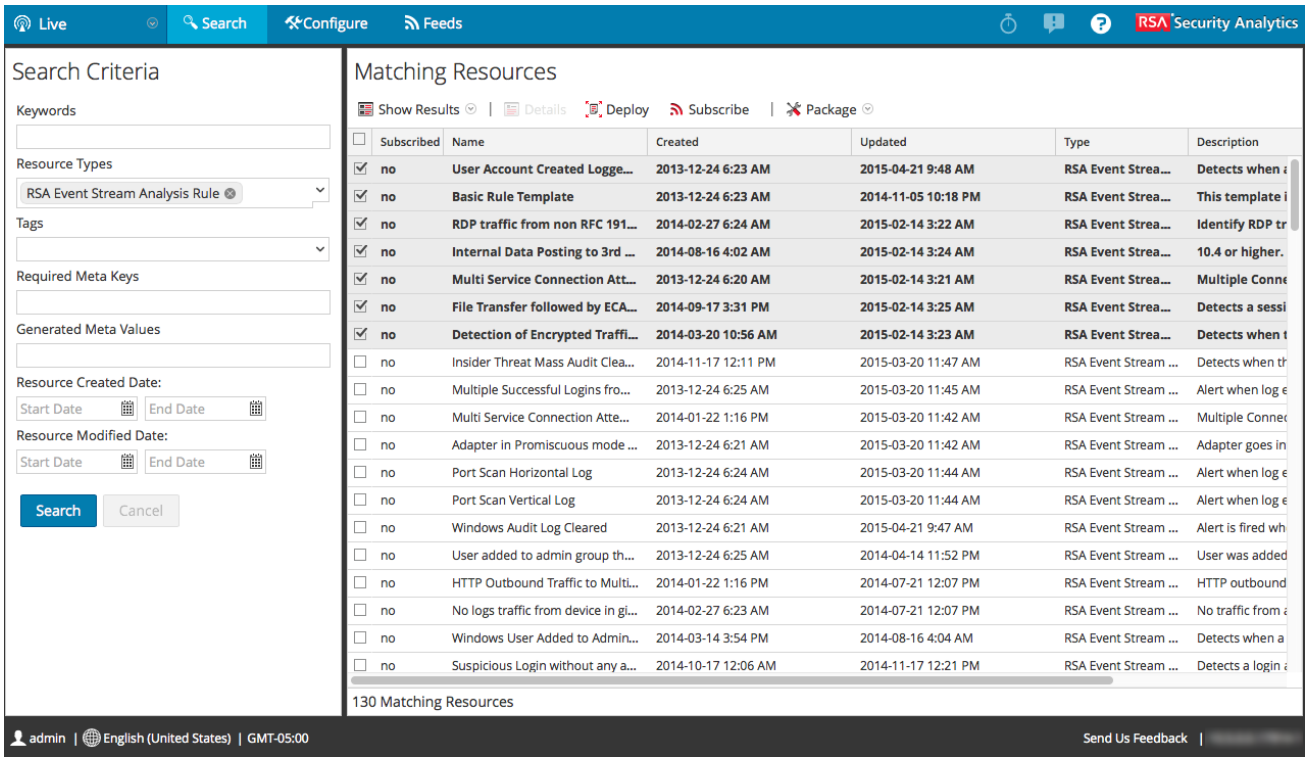
Pour déployer des ressources manuellement, suivez ces étapes :

1. Dans la **Vue Live Search,** parcourez la ressource Live (par exemple, recherchez le type de ressource **RSA Content**).
2. Dans le panneau **Ressources correspondantes**, sélectionnez **Afficher les résultats > Grille**.

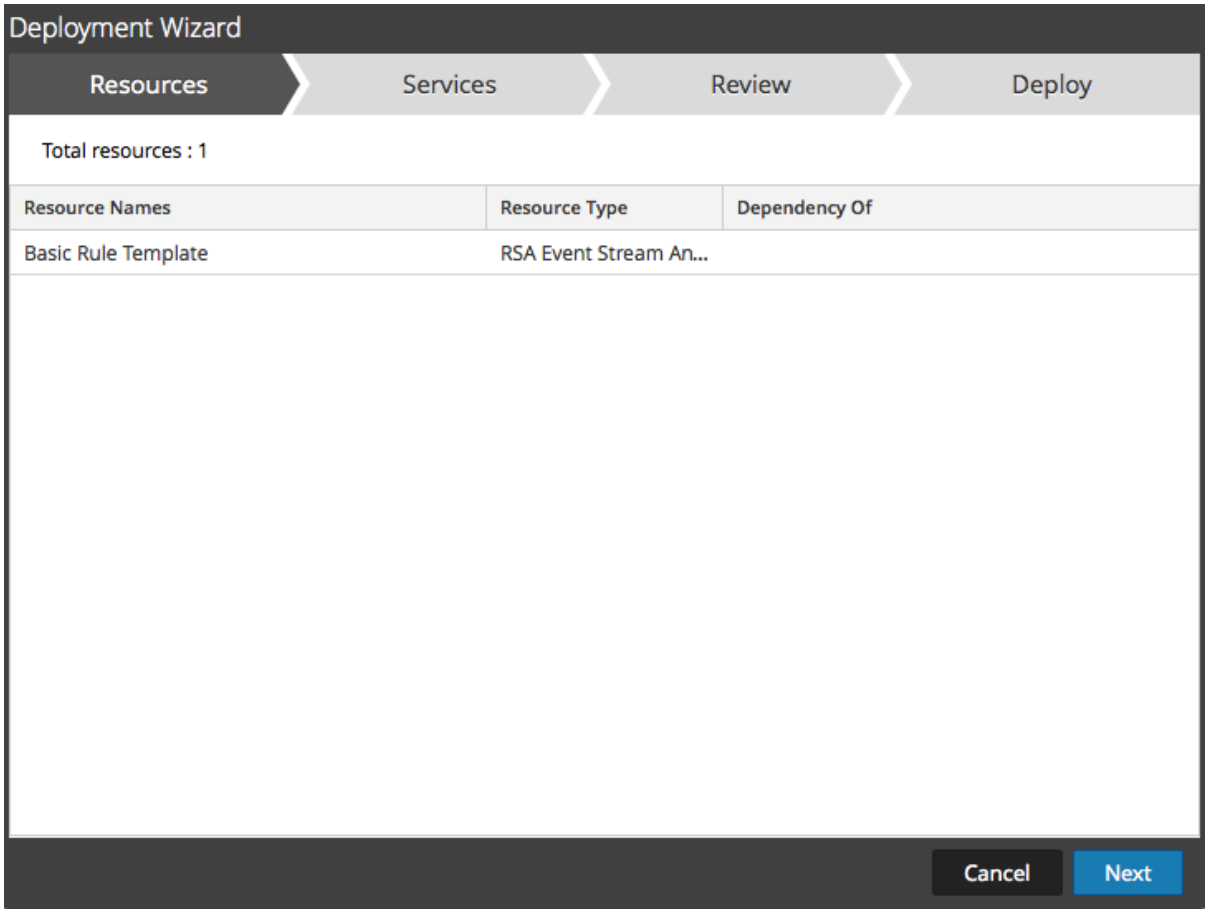
> **Note:** L'autorisation requise pour accéder à cette vue est **Déployer les ressources Live**.

Last Modified: August 10 2016, 9:33AM

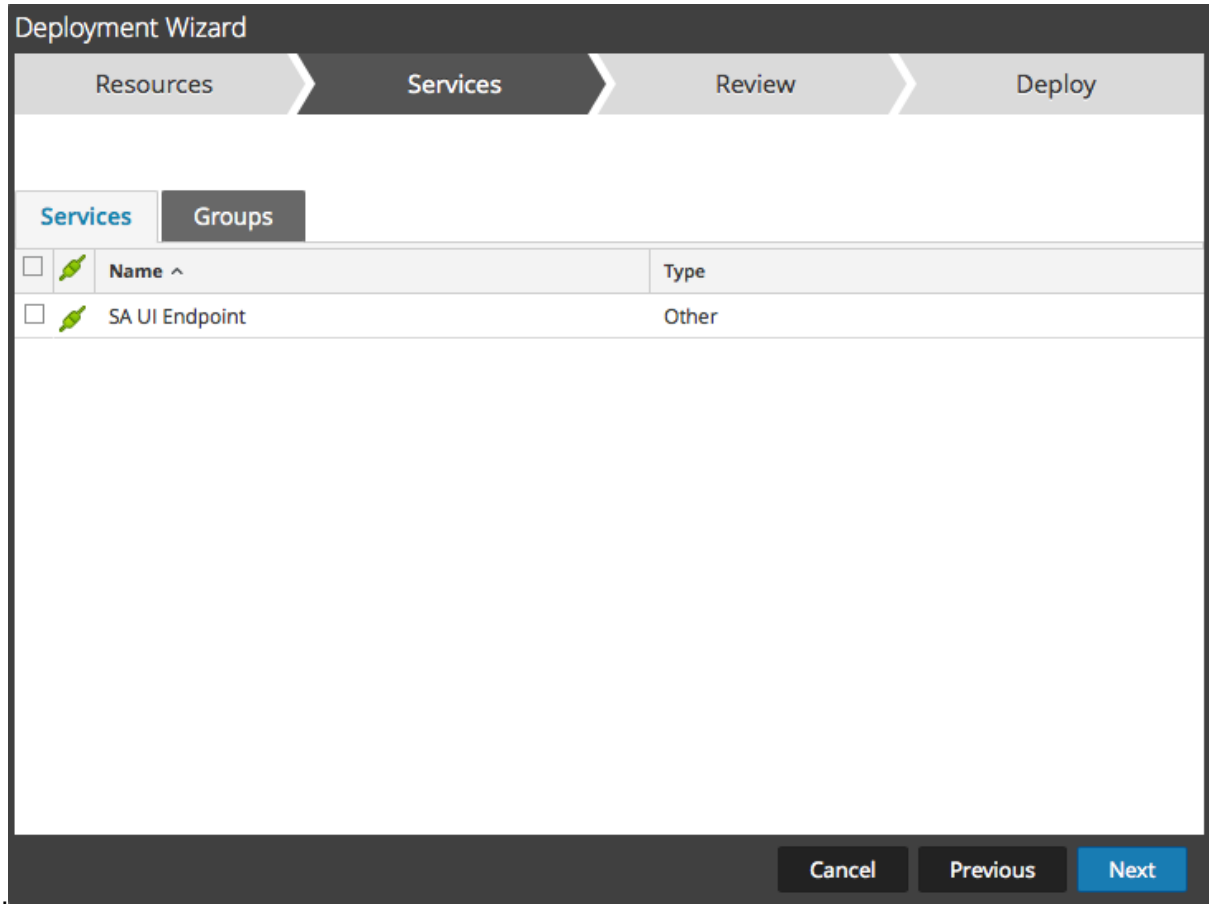
3. Cochez la case à gauche ou les ressources que vous souhaitez déployer.



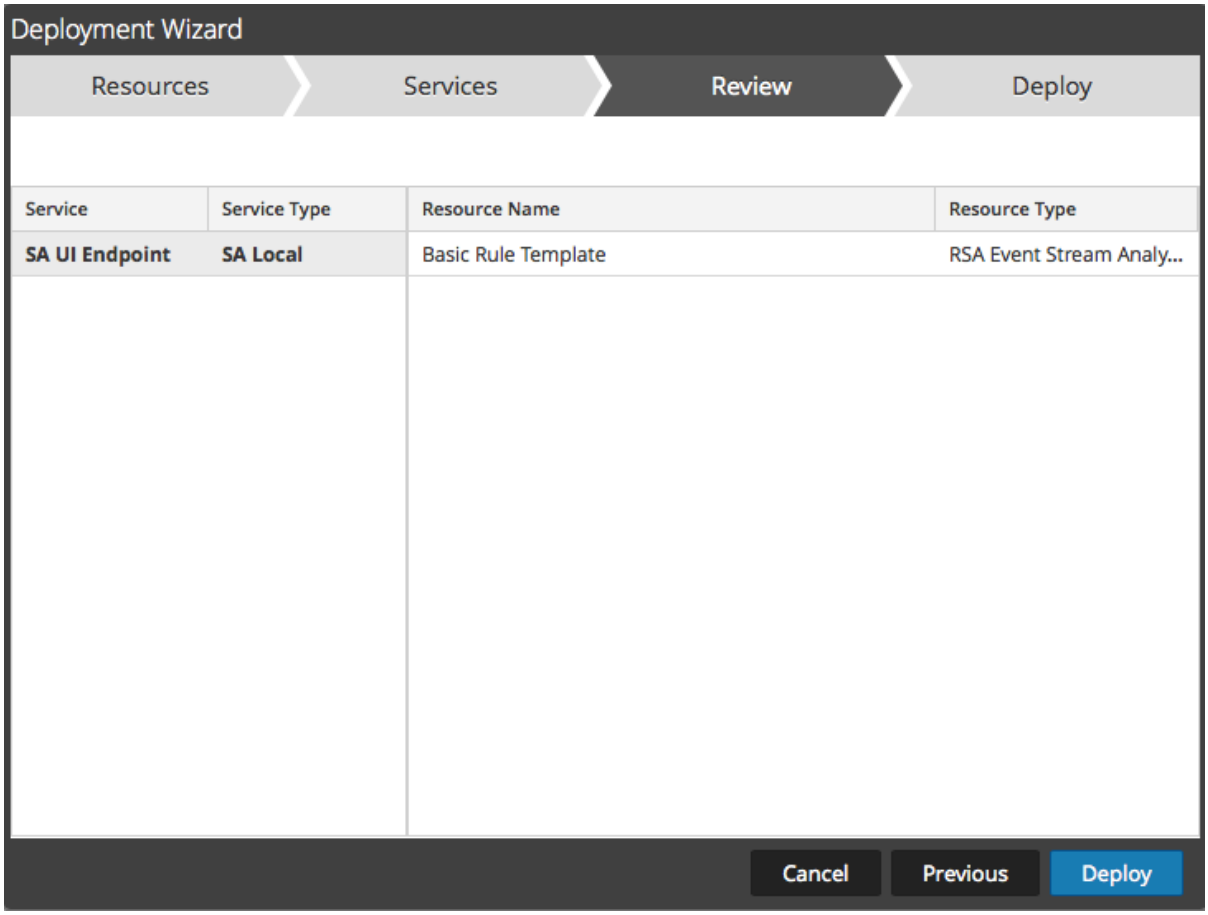
4. Dans la barre d'outils Ressources correspondantes, cliquez sur Deploy .
   L'**Assistant Déploiement** s'ouvre, et la page **Ressources** s'affiche.



5. 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.
6. Sélectionnez les services au niveau desquels vous souhaitez déployer le contenu. Vous pouvez sélectionner une combinaison de services et de groupes de services.
   - Utilisez l'onglet **Services** pour sélectionner chaque service, la liste des services et des groupes de services qui sont configurés dans la vue Administration - Services.
   - Utilisez l'onglet **Groupes** pour sélectionner des groupes de services



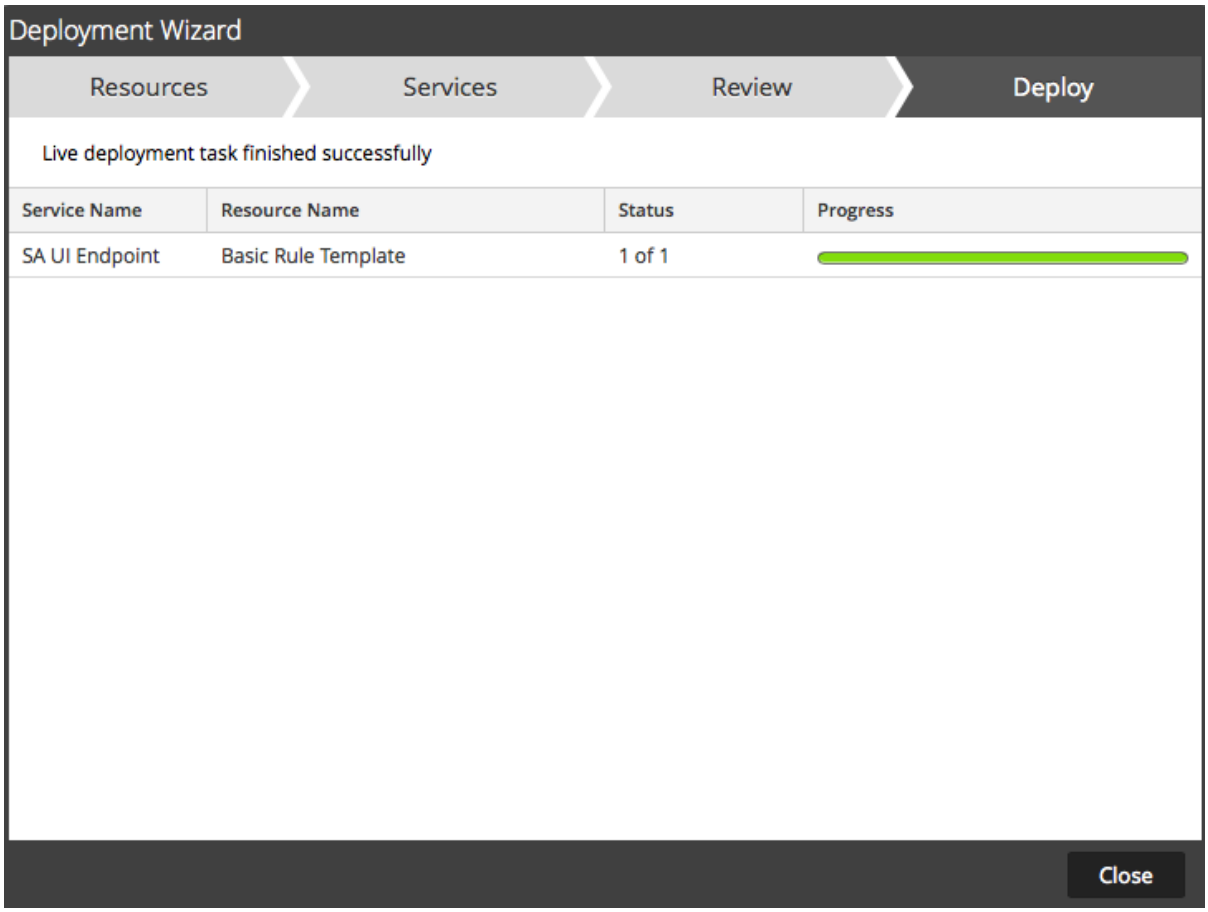
7. Cliquez sur **Suivant**.
   La page **Révision** s'affiche.



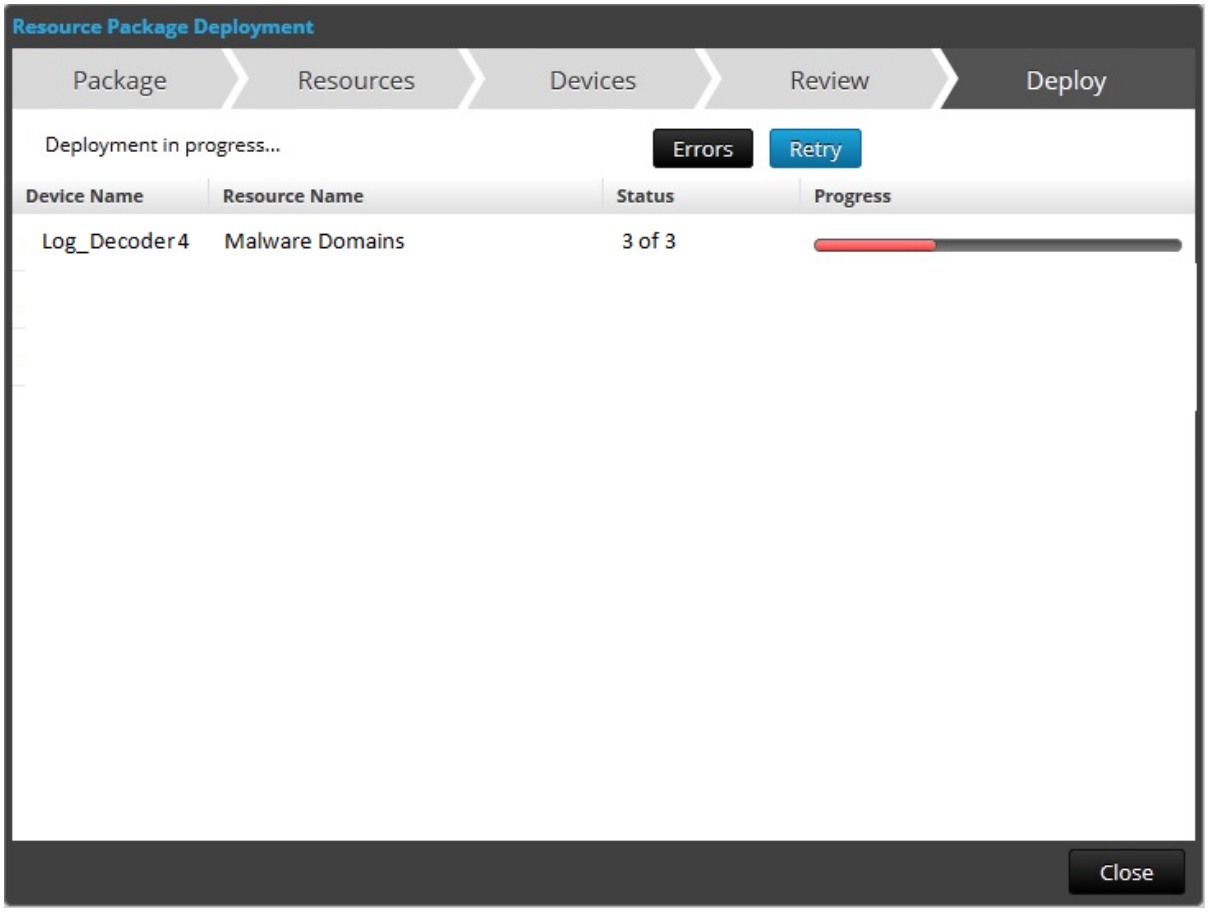
   Veillez à sélectionner les ressources appropriées et les services au niveau desquels vous souhaitez effectuer le déploiement.

8. 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, Security Analytics affiche les boutons Retry et Errors que vous pouvez sélectionner pour consulter les erreurs et essayer à nouveau d'effectuer le déploiement.



9. Cliquez sur **Fermer**.

Déployer des ressources à partir d'un package de ressources

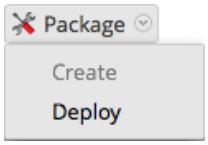
Cette rubrique vous indique comment déployer des ressources à partir d'un package à l'aide de l'Assistant Déploiement du package de la ressource.

Une fois cette procédure terminée, vous aurez déployé les ressources d'un package de ressources préalablement créé et enregistré sur votre réseau. Pour connaître la procédure de création d'un package, reportez-vous à la rubrique Créer un package de ressources.

Procédure

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

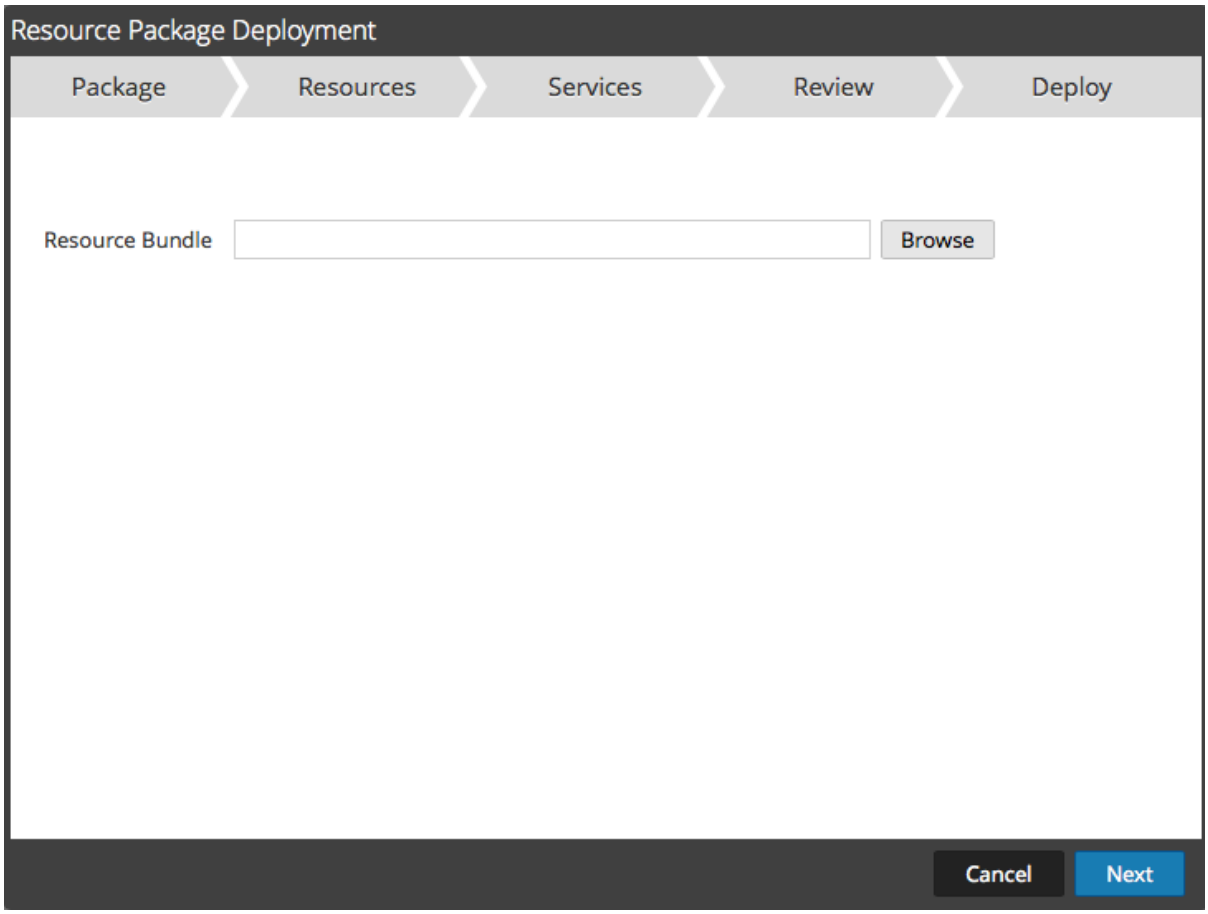
Pour déployer les ressources d'un package de ressources :

1. Dans la vue **Live Search**, sélectionnez **Package** > **Déployer** 

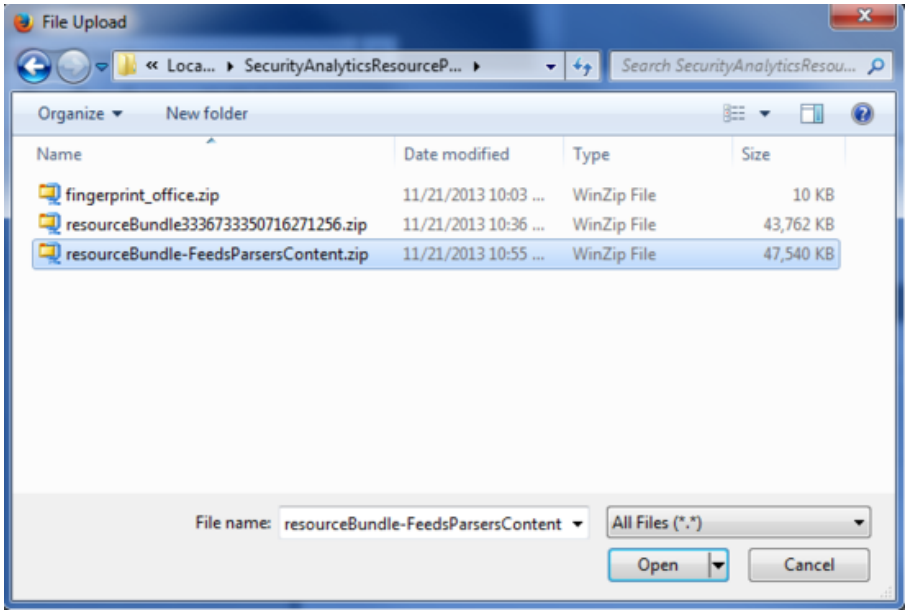
dans la barre d'outils **Ressources correspondantes**.

Last Modified: August 10 2016, 9:33AM

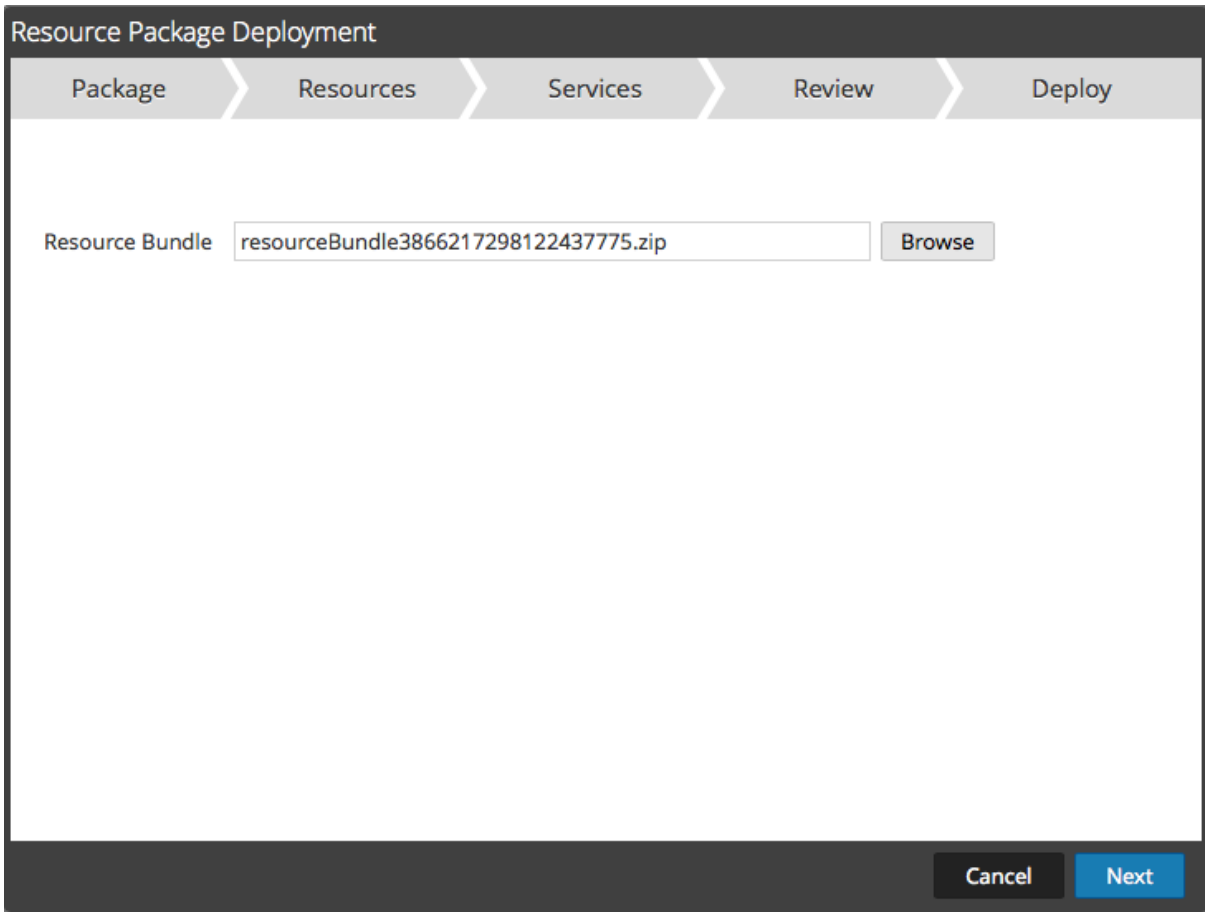
La page Package de l'Assistant Déploiement du package de la ressource s'affiche.



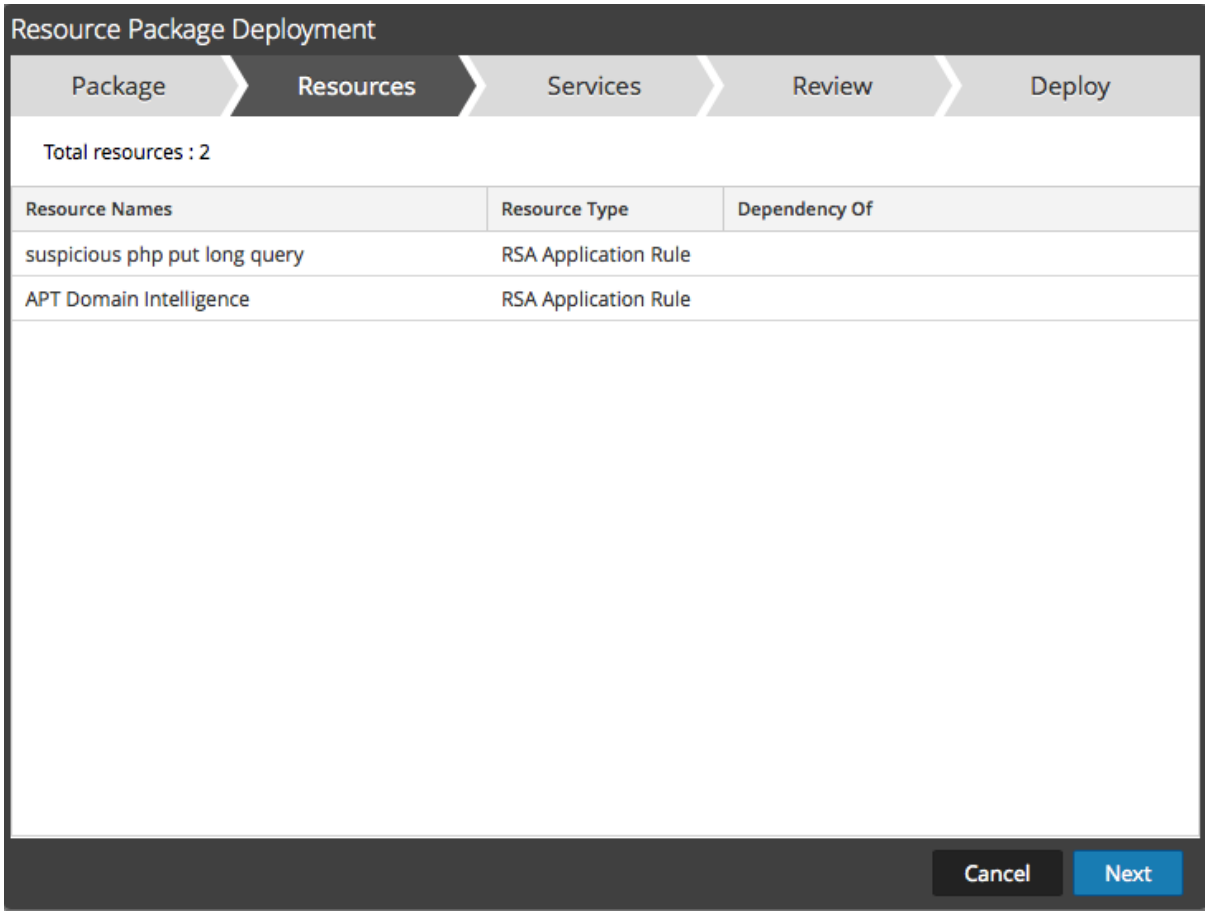
2. Cliquez sur Browse et sélectionnez un package sur votre réseau (par exemple, **resourceBundle-FeedsParsersContent.zip**).



3. Cliquez sur **Ouvrir**.
   Le package sélectionné s'affiche sur la page Package de l'assistant Déploiement du package de la ressource.

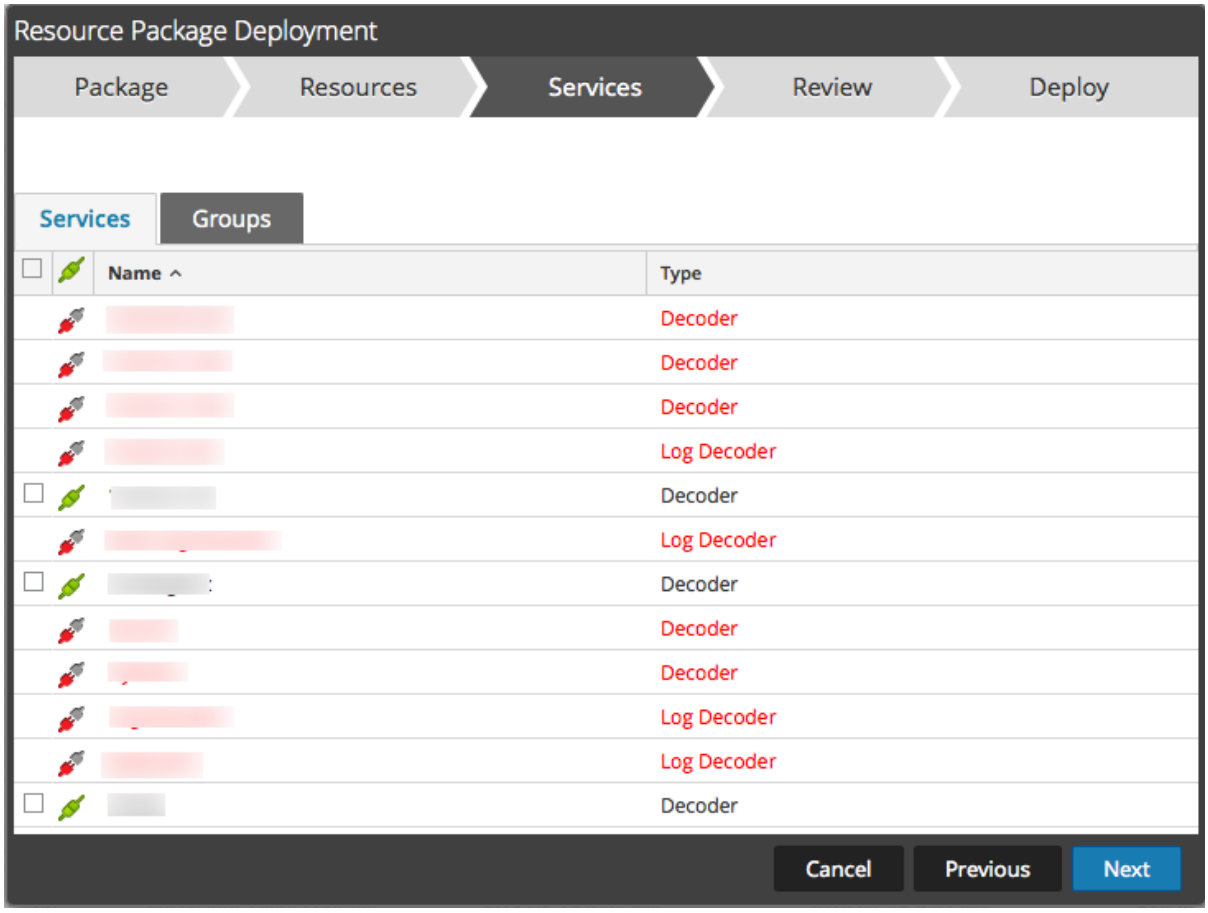


4. Cliquez sur **Suivant**.
   La page **Ressources** s'affiche.

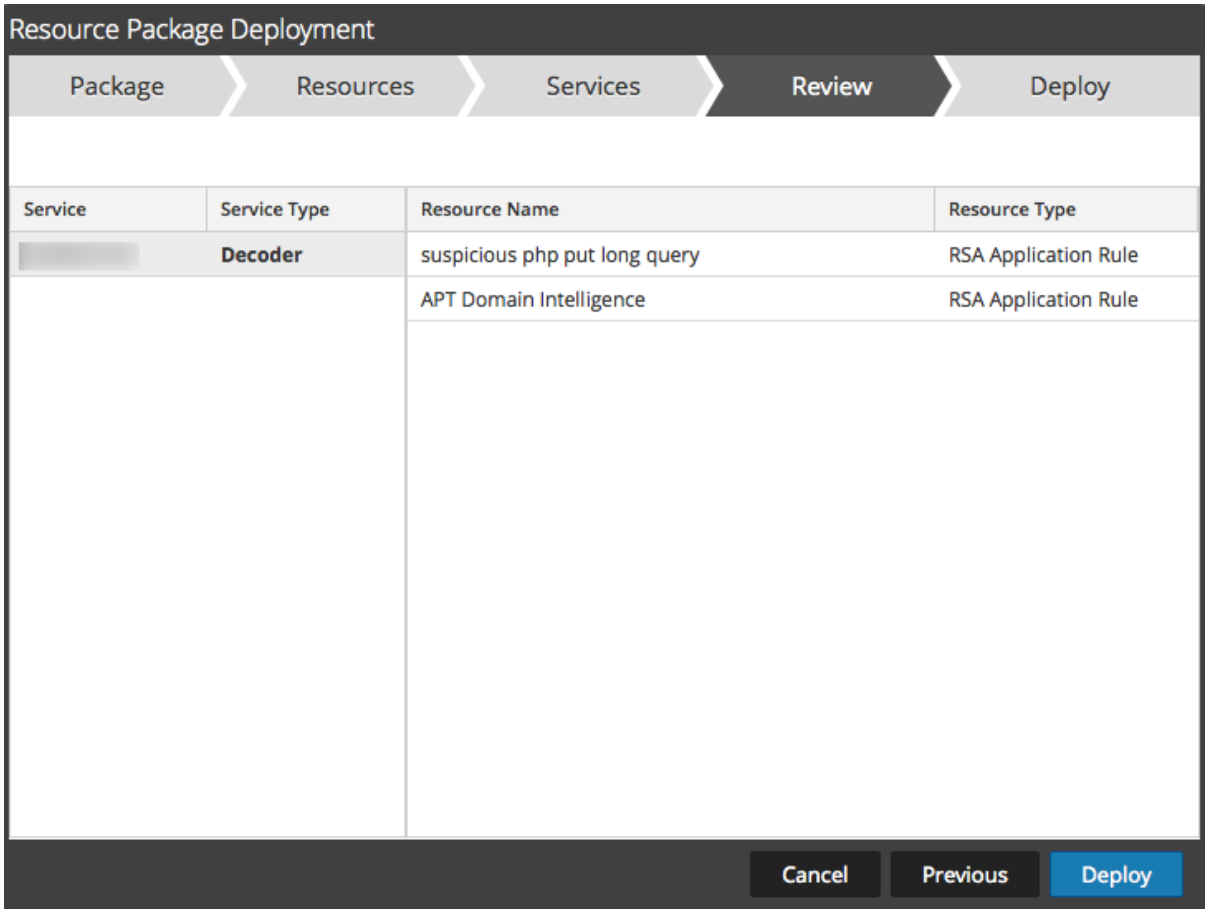


5. Cliquez sur Suivant
   , la page **Services** s'affiche.

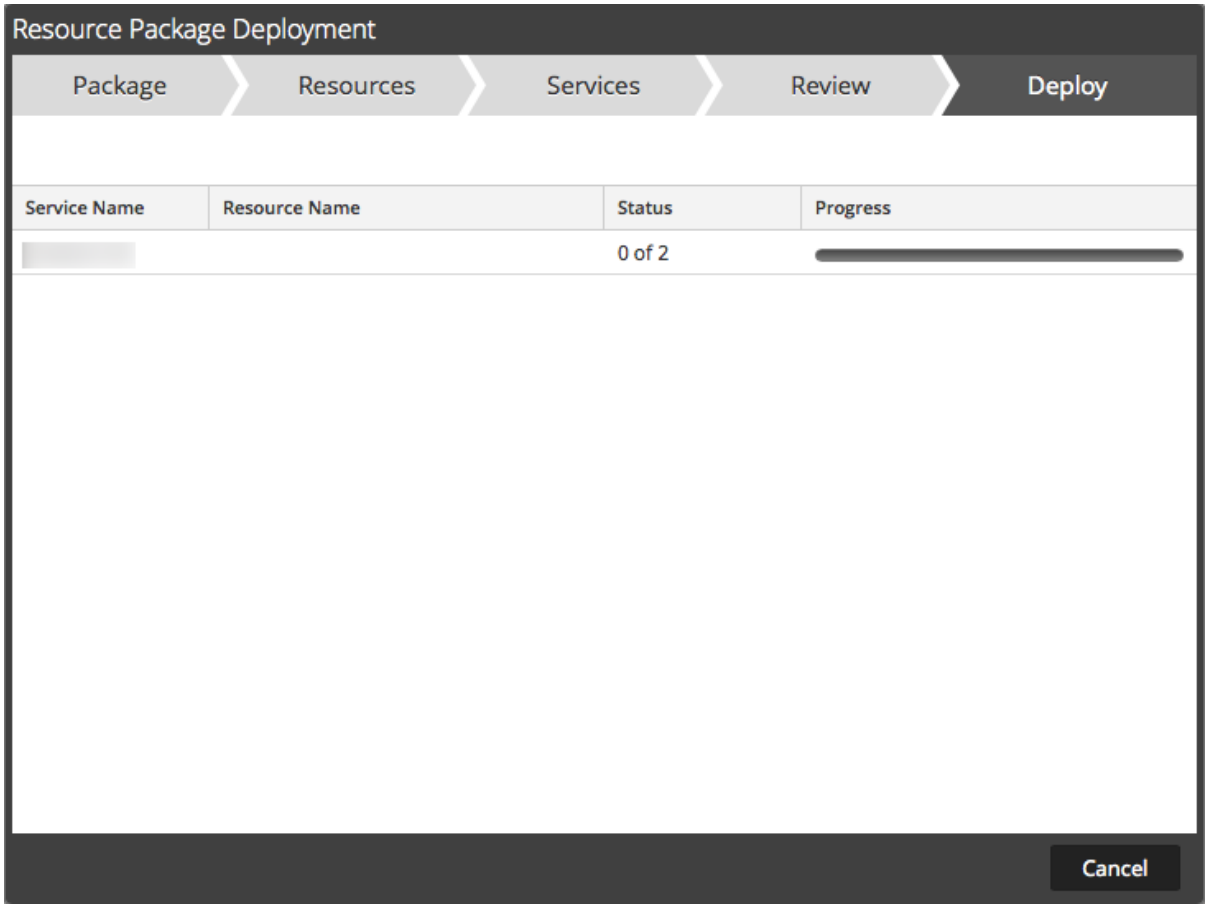
   La page **Services** contient deux onglets, **Services** et **Groupes**, qui fournissent la liste des services et des groupes de services configurés dans la vue **Administration** > Services.
6. Sélectionnez les services au niveau desquels vous souhaitez déployer le contenu. Vous pouvez sélectionner une combinaison de services et de groupes de services.
   - Utilisez l'onglet **Services** pour sélectionner chaque service, la liste des services et des groupes de services qui sont configurés dans la vue Administration - Services.
   - Utilisez l'onglet **Groupes** pour sélectionner des groupes de services.



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



8. Veillez à sélectionner les ressources appropriées et les services au niveau desquels vous souhaitez effectuer le déploiement.
9. 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, Security Analytics affiche les boutons Retry et Errors que vous pouvez sélectionner pour consulter les erreurs et essayer à nouveau d'effectuer le déploiement.

10. Cliquez sur **Fermer**.

Déployer des ressources au niveau des services

Cette rubrique indique comment déployer une ressource sélectionnée dans la vue Ressources Live au niveau des services à l'aide de l'assistant Déploiement.

À la fin de cette procédure, vous aurez déployé une ressource sélectionnée dans la vue Ressources Live au niveau des services à l'aide de l'assistant Déploiement.

Procédure

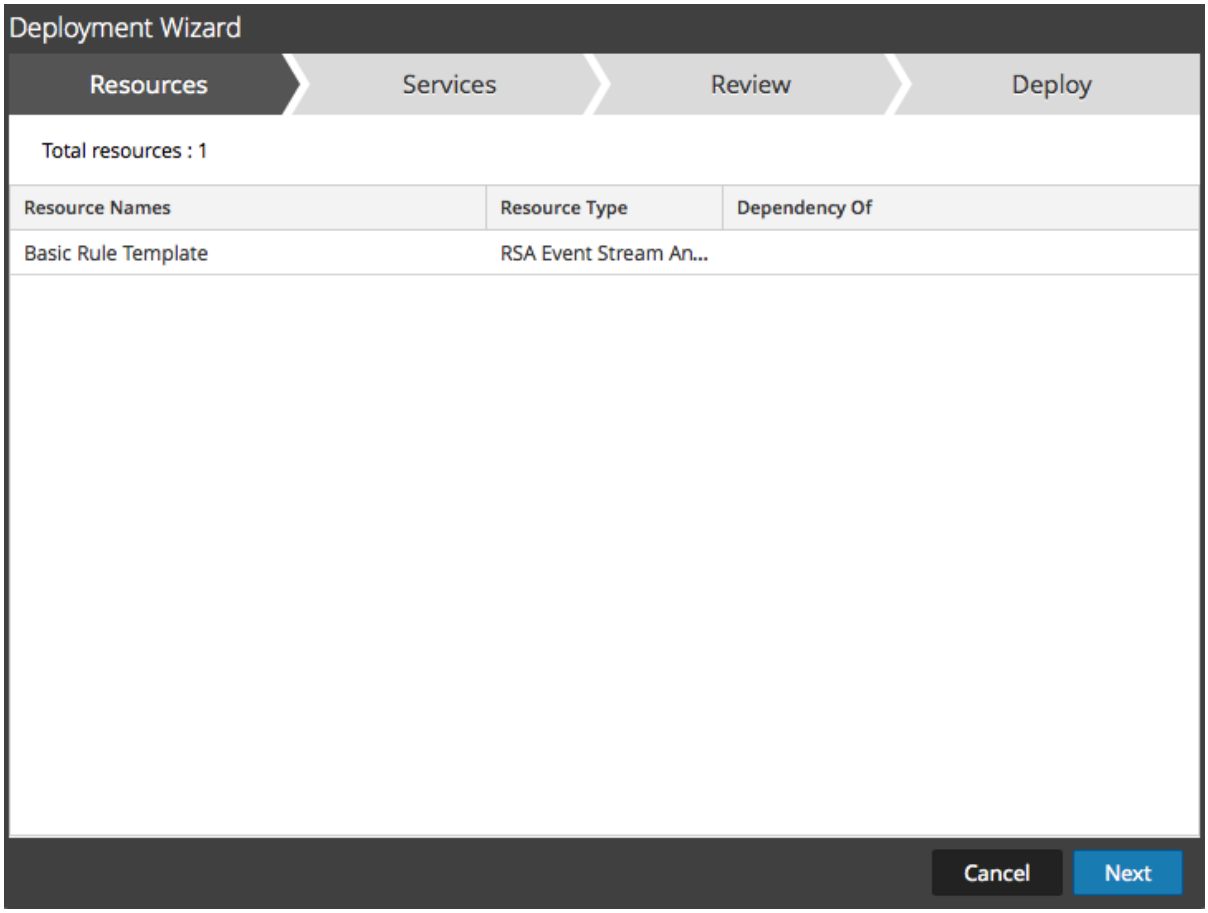
Note: L'autorisation requise pour accéder à cette vue est **Déployer les ressources Live**.

Pour déployer des ressources manuellement :

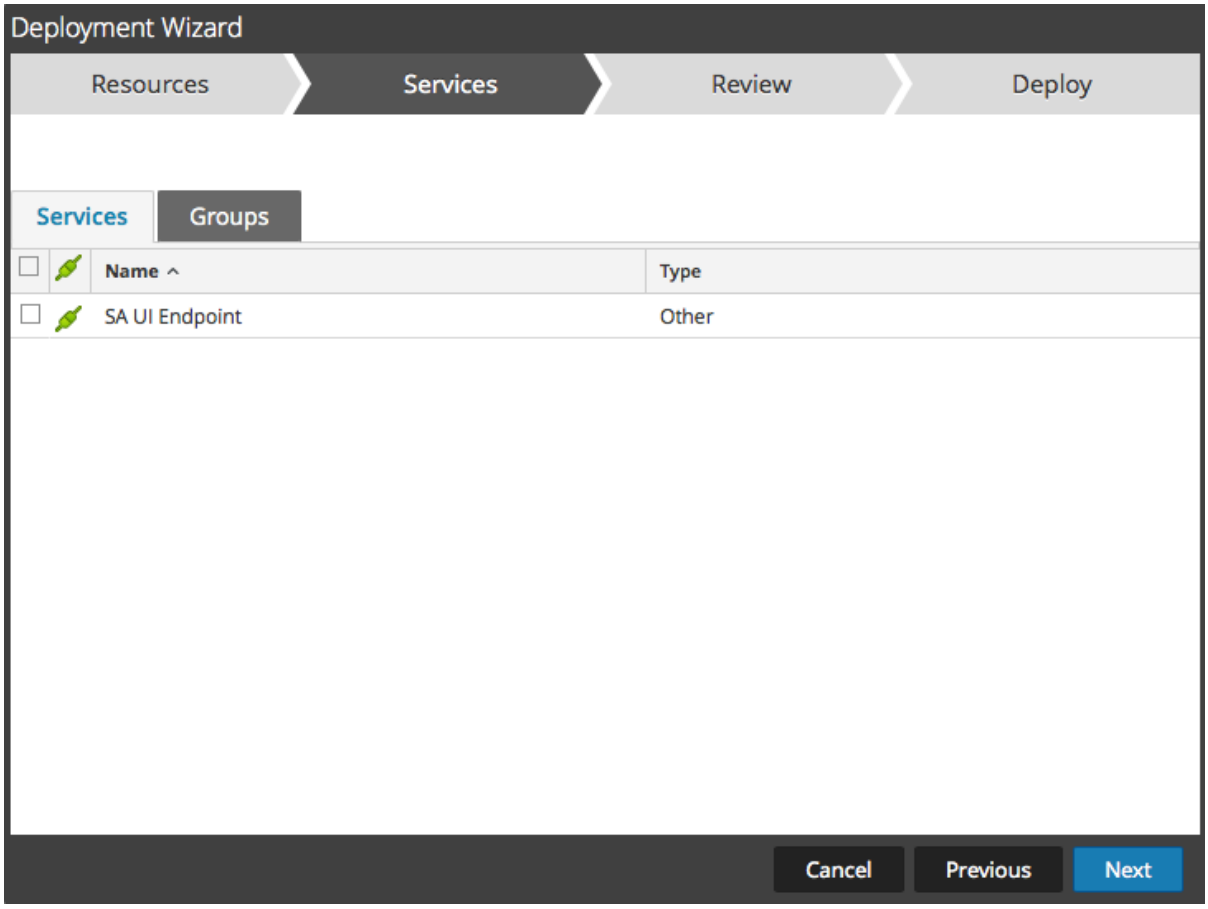
1. Dans le menu **Security Analytics**, sélectionnez **Live > Rechercher > Types de ressources**.
2. Saisissez vos critères de recherche et cliquez sur **Rechercher**.
3. Dans le panneau **Ressources correspondantes**, sélectionnez une ressource.

Last Modified: August 10 2016, 9:33AM

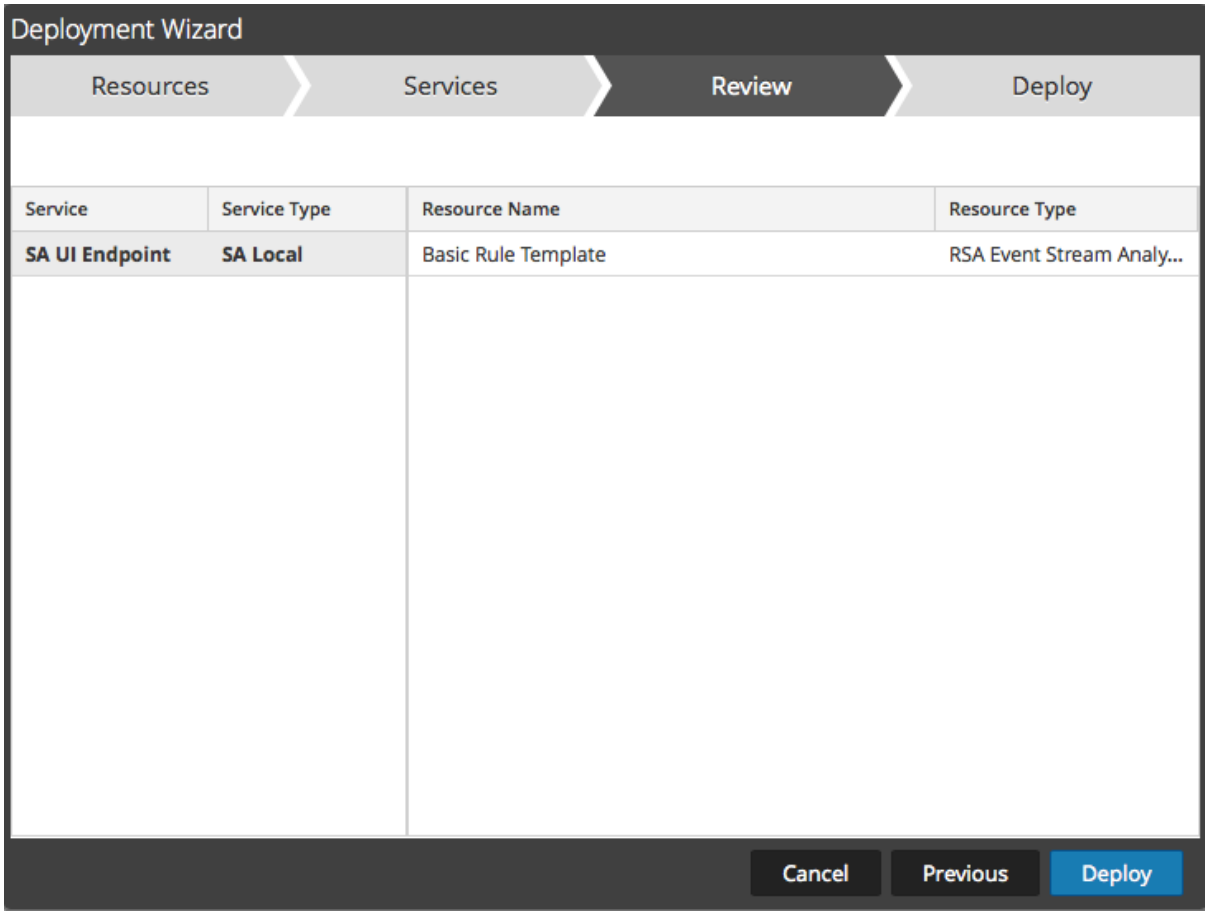
4. Dans la barre d'outils Ressources correspondantes, cliquez sur Deploy .
   L'**assistant Déploiement** s'ouvre et affiche la page **Ressources**.



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

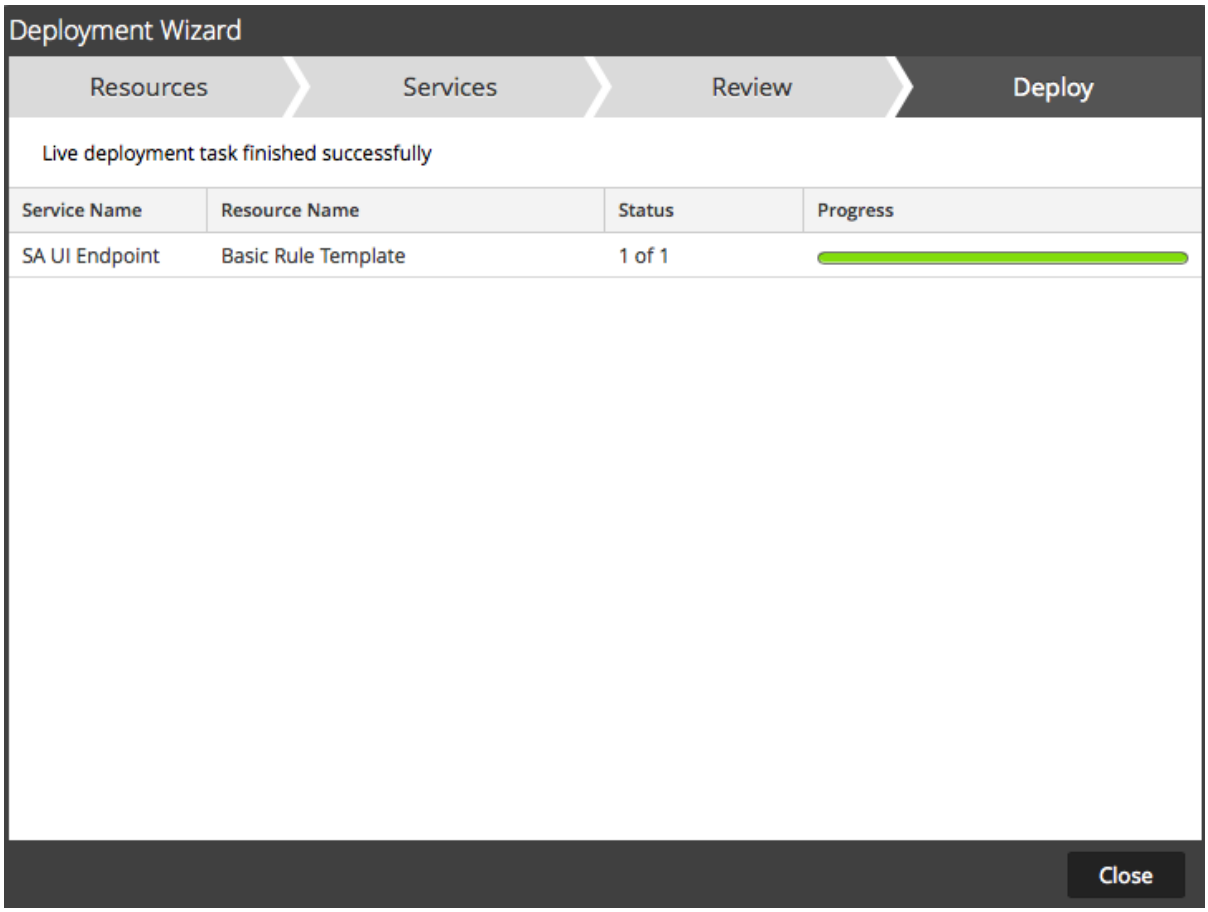


6. Cliquez sur **Suivant**.
   La page **Vérification** s'affiche.



7. Veillez à sélectionner la ressource appropriée et les services au niveau desquels vous souhaitez effectuer le déploiement.
8. Cliquez sur **Déployer**.
   La page Déployer s'affiche. La barre de progression devient verte lorsque vous avez réussi à déployer la ressource au niveau

des services sélectionnés.



9. Cliquez sur **Fermer**.

RSA

Déployer les ressources Live à l'aide de l'assistant Déploiement

Cette rubrique indique aux administrateurs comment déployer des ressources Live à l'aide de l'assistant Déploiement

Conditions préalables

Préalablement à cette tâche, il faut configurer et synchroniser le serveur CMS avec Security Analytics ainsi que la fonction de recherche de ressources Live.

Procédure

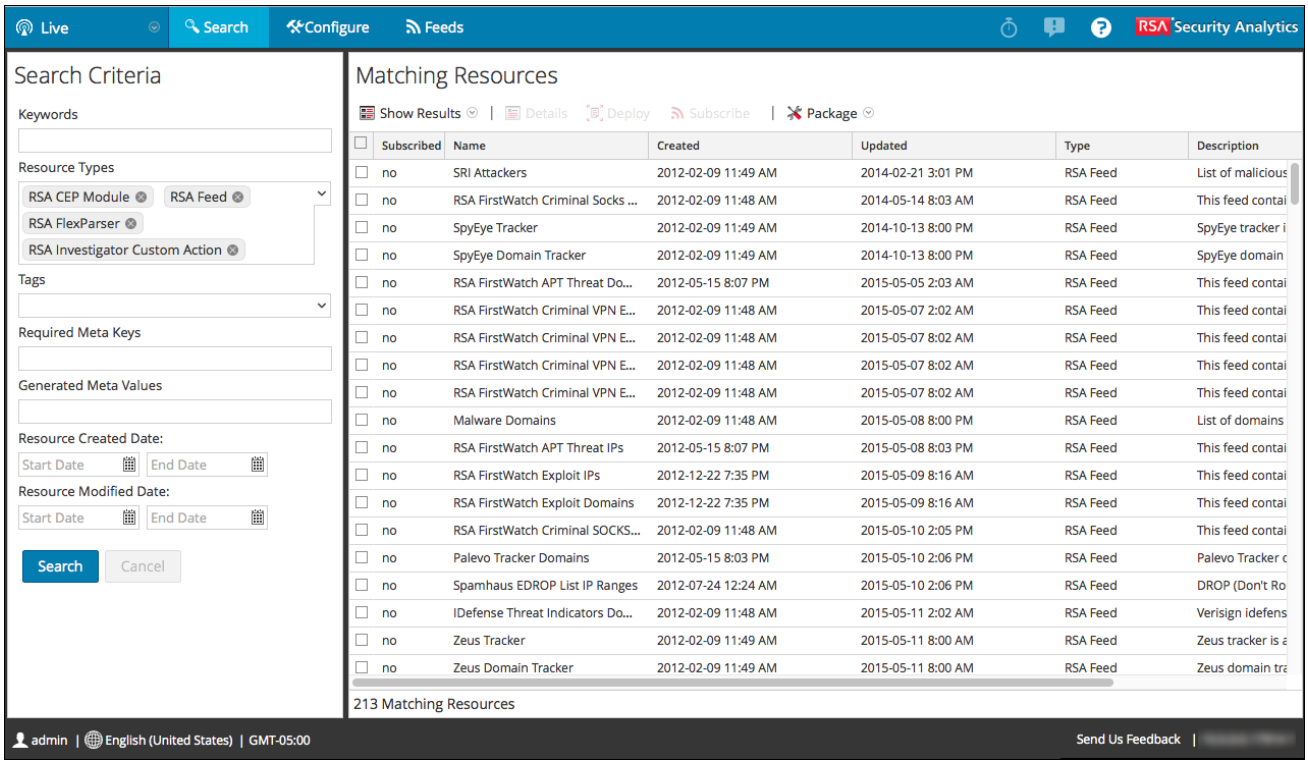
L'autorisation requise pour accéder à cette vue est **Déployer les ressources Live**.

Pour accéder à l'Assistant Déploiement :

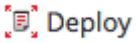
1. Dans la **vue Recherche Live**, accédez aux ressources Live.

Last Modified: August 10 2016, 9:33AM

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



3. Sélectionnez les ressources à déployer.

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

.

Last Modified: August 10 2016, 9:33AM

Afficher les détails des ressources dans la vue Ressource Live

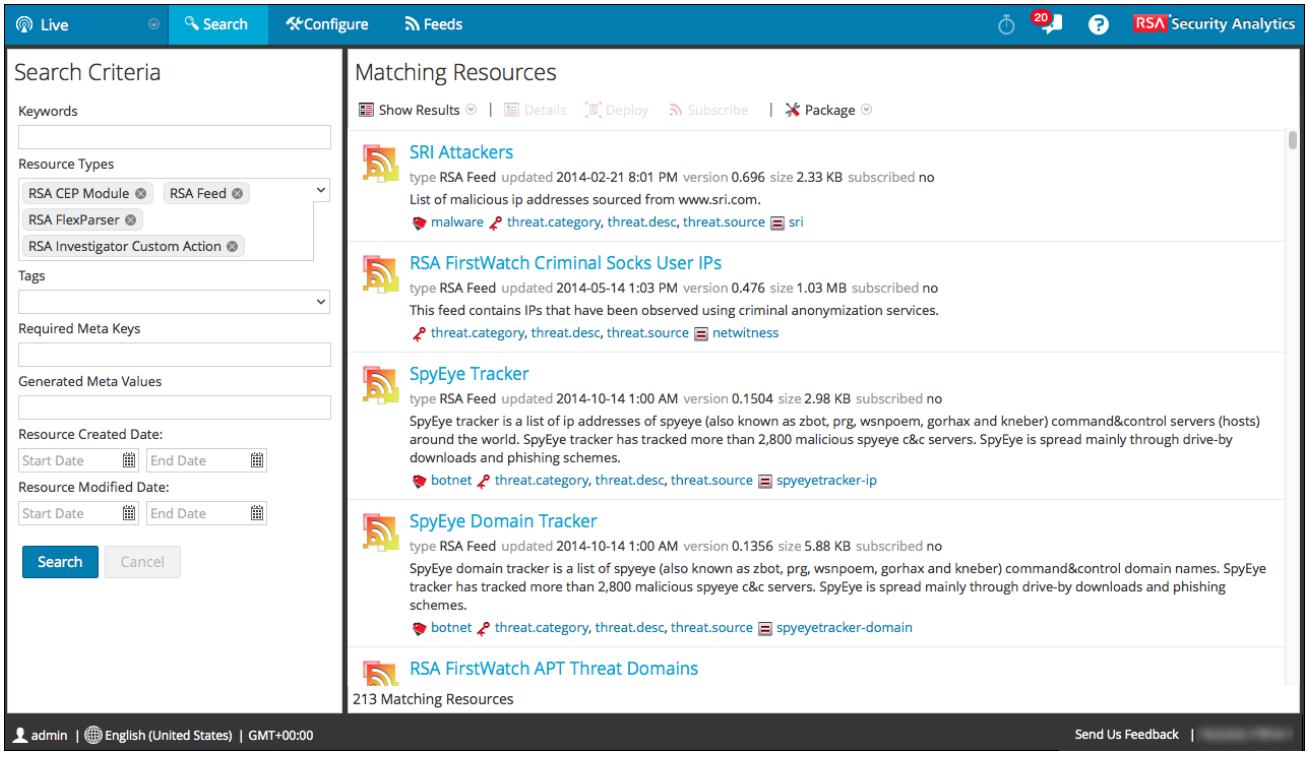
Cette rubrique vous indique comment sélectionner une ressource et afficher des informations détaillées à son sujet dans la vue Ressources Live.

Une fois cette procédure terminée, les informations détaillées d'une seule ressource sont affichées dans la vue Ressources Live.

Afficher les détails des ressources dans la vue Ressources Live

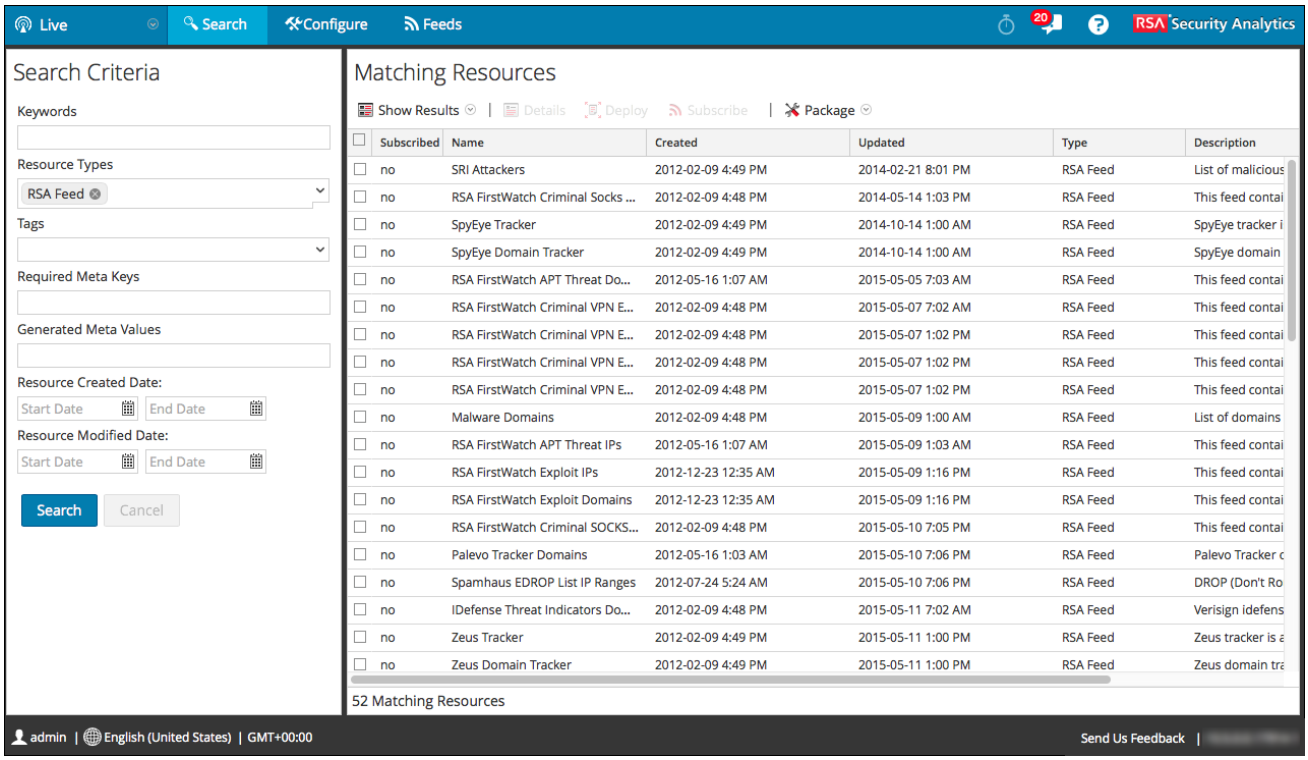
Pour ouvrir un onglet séparé dans la vue Ressources Live avec les informations détaillées de la ressource sélectionnée, choisissez l'une des méthodes suivantes :

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



Last Modified: August 10 2016, 9:33AM

- Dans **Résultats en grille**, double-cliquez sur une ressource ou sélectionnez une ressource et cliquez sur **Détails**.



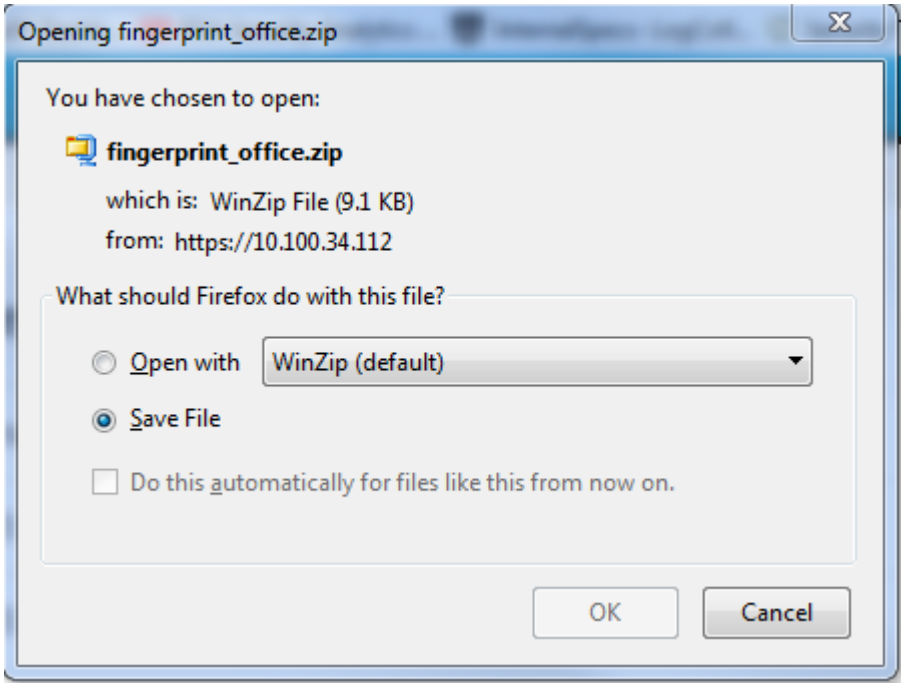
Télécharger une ressource

Cette rubrique indique comment télécharger une ressource depuis la vue Ressources Live.

Procédure

Pour télécharger une ressource :

1. Avec une ressource affichée dans la vue Ressources, cliquez sur Download.
   Une boîte de dialogue propose deux options : ouvrir le fichier ou l'enregistrer.



2. Sélectionnez **Enregistrer le fichier** et cliquez sur **OK**.
   Le fichier de ressource est ajouté au répertoire local de téléchargement.

Rechercher et supprimer une ressource déployée à partir des services

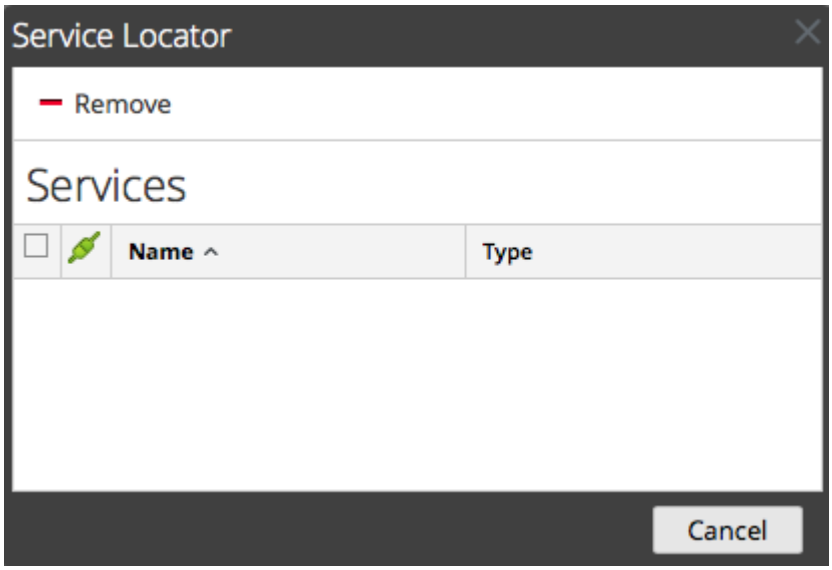
Cette rubrique explique comment localiser et supprimer une ressource déployée dans des services à partir de la vue Ressources Live.

Une fois la procédure terminée, vous aurez localisé et supprimé une ressource déployée dans des services à partir de la vue Ressources Live.

Procédure

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 grille **Services**.
3. Cliquez sur Remove .
   La ressource est supprimée des services sélectionnés.

Exporter des données vers RSA

Cette rubrique fournit les instructions permettant à un administrateur Security Analytics d'exporter les metrics dans Security Analytics pour Live Feedback.

Présentation

Si le compte Live n'est pas configuré, vous pouvez télécharger manuellement les données d'utilisation vers RSA. Pour plus d'informations, reportez-vous à la rubrique Panneau de configuration des Services en direct.

La section Compte 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.

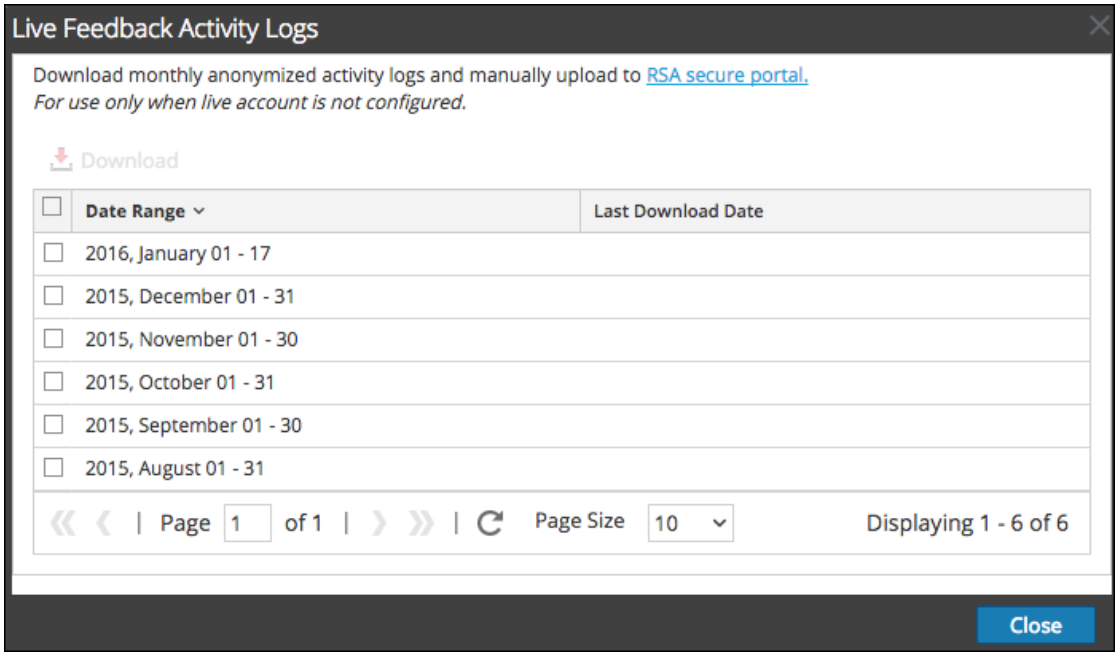
Télécharger l'historique des données Live Feedback

Pour télécharger l'historique des données Live Feedback :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Système**.
2. Dans le panneau des options, sélectionnez **Services Live**.
   L'écran **Compte Live** composé des affichages **État Live RSA** et **Télécharger les logs d'activité Live Feedback** apparaît.
3. Cliquez sur **Télécharger les logs d'activité Live Feedback**.

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

Last Modified: August 16 2016, 1:59PM



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

> **Note:** 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, reportez-vous à la rubrique Présentation de Live Feedback.

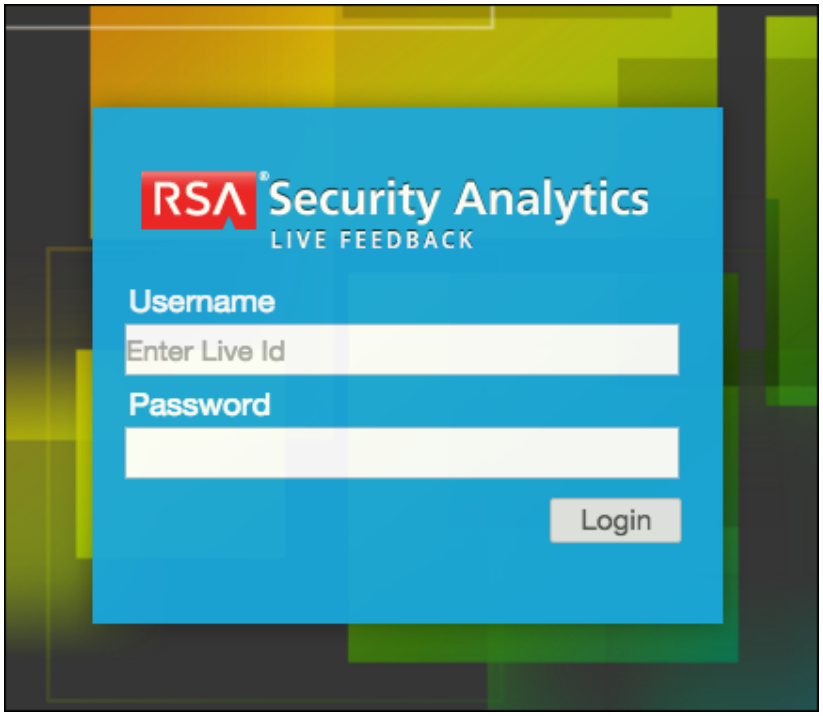
Partager des données dans RSA

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

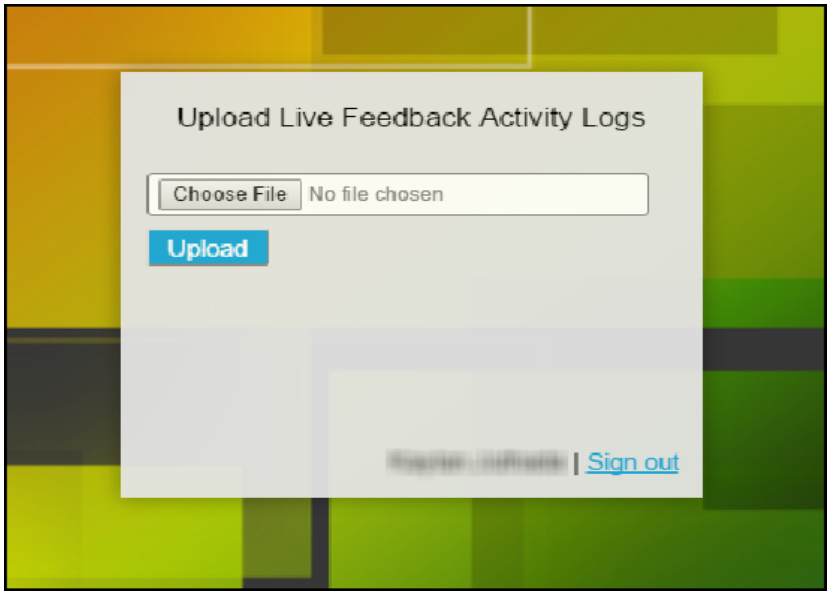
Pour partager les données dans RSA :

1. Cliquez sur le **portail sécurisé RSA** disponible dans la fenêtre **Logs d'activité Live Feedback**.
   L'écran de connexion RSA Security Analytics 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.

Last Modified: August 16 2016, 1:59PM



3. Cliquez sur **Choisir un fichier**, puis sélectionnez le fichier téléchargé en aval.



4. Cliquez sur **Télécharger**.

RSA

Gérer les feeds personnalisés

Présentation

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

Création d'un feed personnalisé

Utilisez l'assistant **Live** > **Feeds** > **Configurer le feed** > **Configurer un feed personnalisé** pour créer et déployer rapidement des feeds 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 à la fois 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.

Dans RSA Security Analytics, les noms des fichiers de feed sont au format `<nom de fichier>.feed`. Pour créer un feed, Security Analytics a besoin d'un fichier de données de feed au format `.csv` et un fichier de définition de feed au `.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 Security Analytics peut récupérer la dernière version du fichier pour chaque récurrence. Après la création d'un feed Security Analytics, vous pouvez télécharger le feed sur votre système de fichiers local, modifier les fichiers de feed, puis modifier le feed Security Analytics afin qu'il utilise les fichiers de feed mis à jour.

Échantillon de fichier de définition de feed

Voici un exemple de fichier de définition de feed nommé **dynamic_dns.xml**, que Security Analytics crée en se basant sur vos entrées dans les assistants Feed. Il définit la structure du fichier de données de feed intitulé **dynamic_dns.csv**.

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


Last Modified: August 10 2016, 9:33AM

```
<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 Security Analytics fournit des options permettant de définir la structure du fichier de feed de données. Ils correspondent directement aux attributs du fichier de définition de feed (.xml).

Paramètre Security Analytics	Équivalent du fichier de définition de feed
Onglet **Définir le feed**	
Type de tâche par défaut	Sélectionnez : **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.

Last Modified: August 10 2016, 9:33AM

Paramètre Security Analytics	Équivalent du fichier de définition de feed
Fichier/ Parcourir	Il s'agit du nom du fichier de données du feed. Il correspond à l'attribut `flatfeedfile path` dans le fichier de définition de feed, par exemple, dynamic_dns.csv.
Onglet **Définir le feed** - Options avancées	
Fichier de feed XML	Nom du fichier de définition de feed, par exemple, `dynamic_dns.xml`.
Séparateur	Caractère de séparation utilisé pour séparer les attributs dans le fichier de données du feed. Il correspond à l'attribut `flatfeedfile separator` dans le fichier de définition de feed, par exemple, une virgule.
Comment	Caractère utilisé pour identifier un commentaire dans le fichier de données du feed. Il correspond à l'attribut `flatfeedfile comment` dans le fichier de définition de feed, par exemple, **#**.
Onglet **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).
(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

Paramètre Security Analytics	Équivalent du fichier de définition de feed
	de rappel correspond à l'attribut **MetaCallback name**, et la colonne index du fichier csv doit contenir des données pouvant correspondre à la clé méta choisie. Par exemple, si la clé méta du nom d'utilisateur est choisie, la colonne index du fichier csv doit être renseignée avec les utilisateurs à associer.
(Onglet Définir des colonnes, Définir l'index) **Colonne index**	Identifie la colonne du fichier de données de feed qui donne la valeur de recherche pour la ligne. Chaque position de chaque ligne du fichier de données de champ est identifiée par l'attribut **Index de champ** dans le fichier de définition de feed. Un champ dont l'index est **1** indique la première entrée de la ligne. Le second champ représente l'index **2**, le troisième champ l'index **3**, etc.
(DÉFINIR LES VALEURS) **Clé**	Nom de **LanguageKey**, tel qu'il est défini dans le fichier de définition de feed, pour lequel les méta sont créées à partir de cette ligne du fichier de données de feed. Il correspond à l'attribut **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.

Créer un Feed personnalisé

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

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

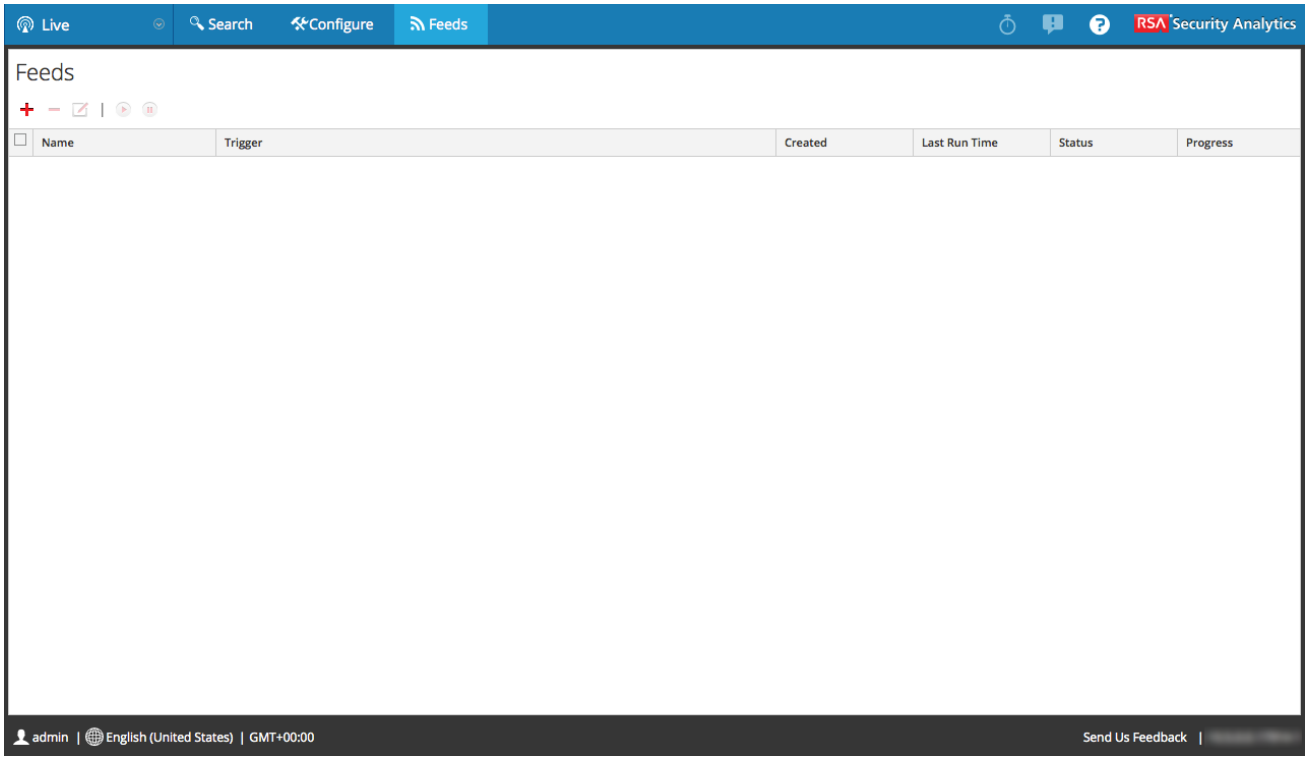
Créer un Feed personnalisé

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

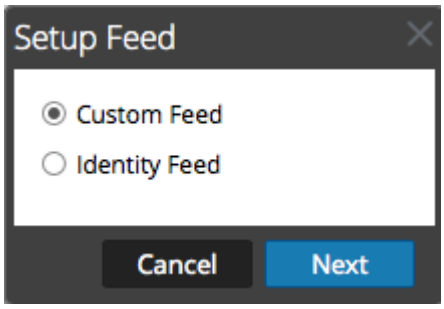
Pour créer un feed personnalisé :

Last Modified: August 10 2016, 9:33AM

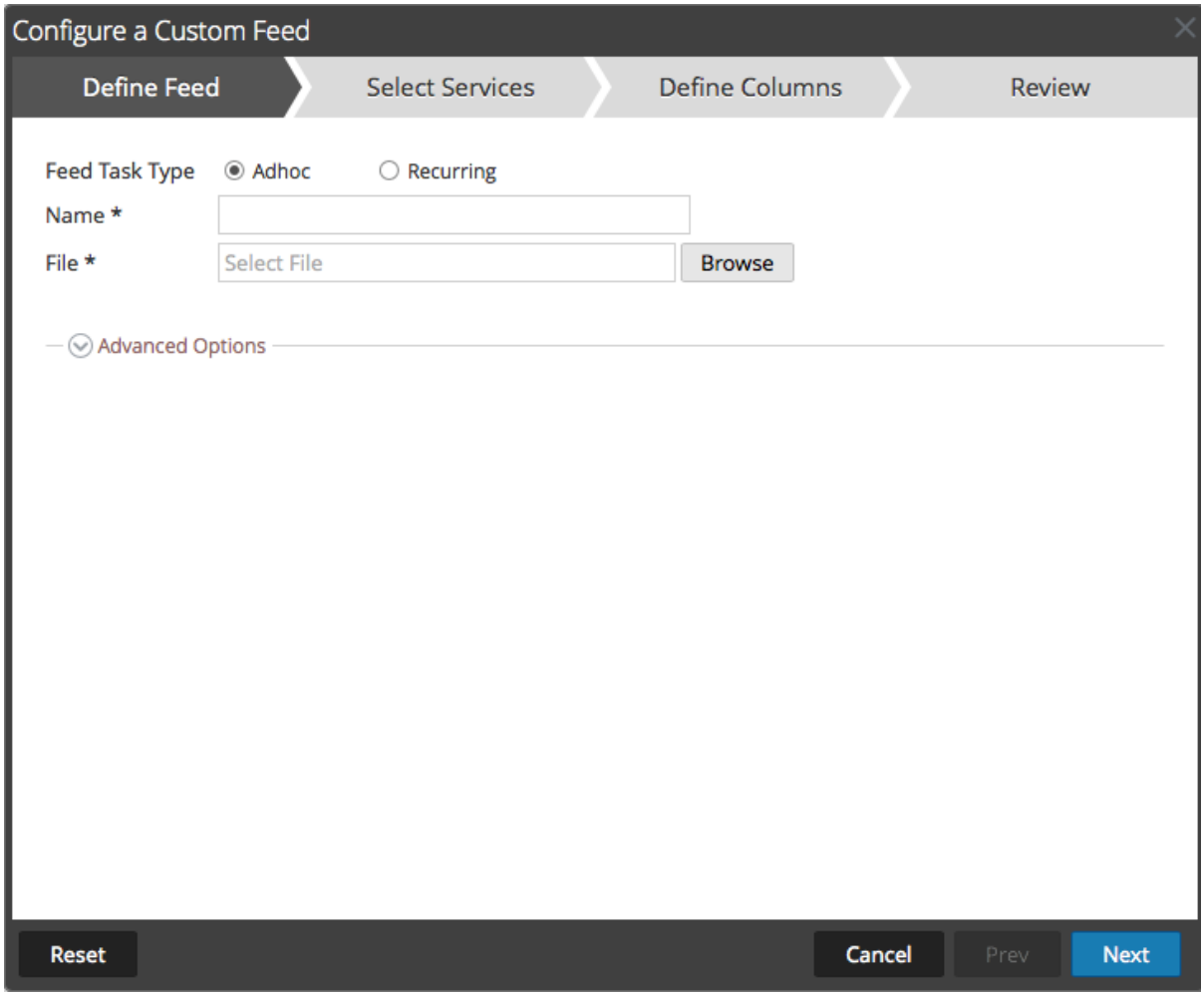
1. Dans le menu **Security Analytics**, sélectionnez **Live > Feeds.**
   La vue Feeds s'affiche.



2. Dans la barre d'outils, cliquez sur +.
   La boîte de dialogue Configurer le feed s'affiche.

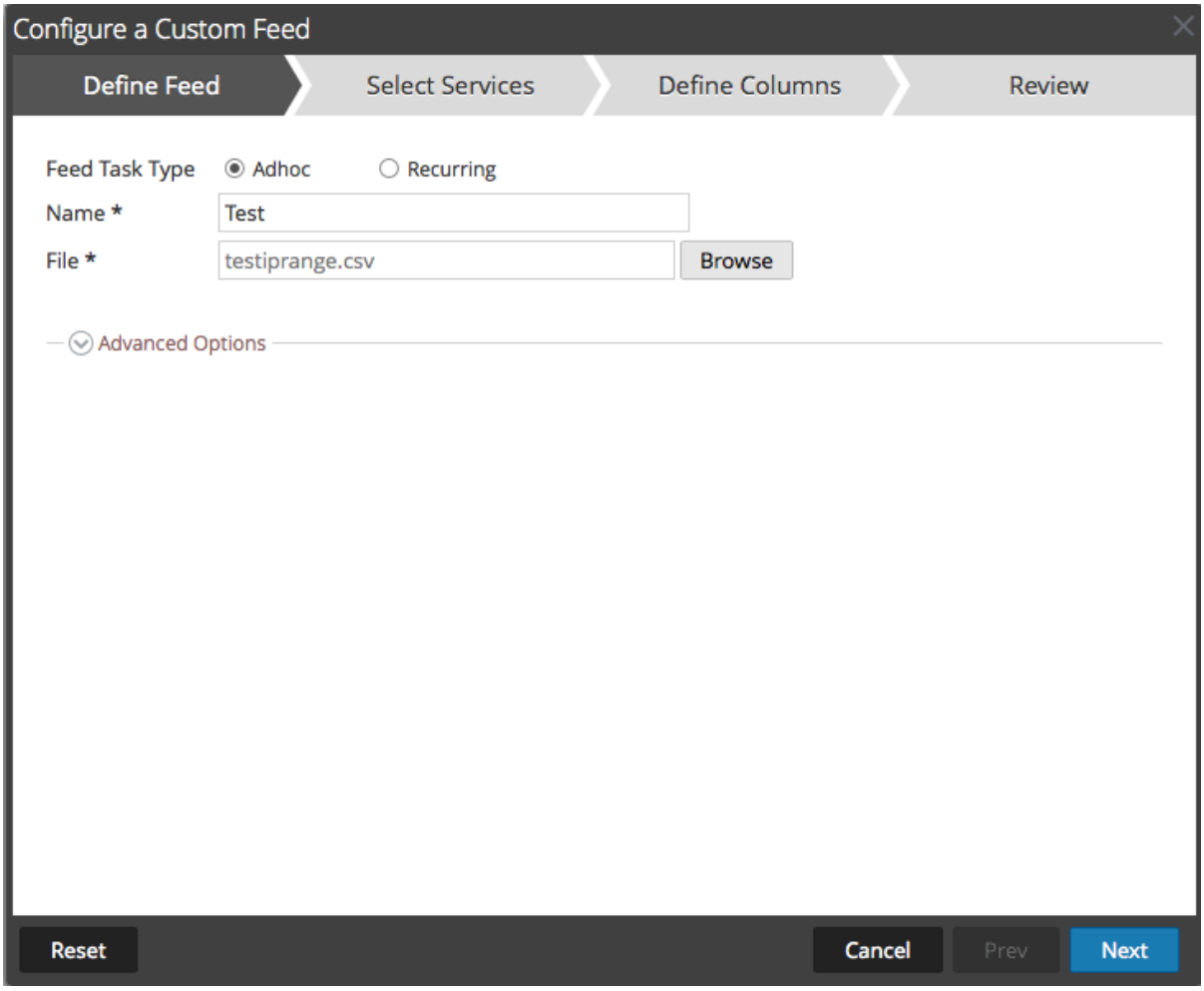


3. Pour sélectionner le type de feed, cliquez sur **Feed personnalisé,** puis sur **Suivant**.
   Le panneau Configurer un feed personnalisé s'affiche avec le formulaire Définir le feed ouvert.



4. Pour définir une tâche de feed à la demande qui s'exécute une fois, sélectionnez **Adhoc** dans le champ **Type de tâche par défaut** et procédez de l'une des façons 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 au format .csv dans le système de fichiers local, puis cliquez sur **Suivant**.
   b. (Conditionnel) Pour définir un feed basé sur un fichier de feed XML, sélectionnez **Options avancées** :

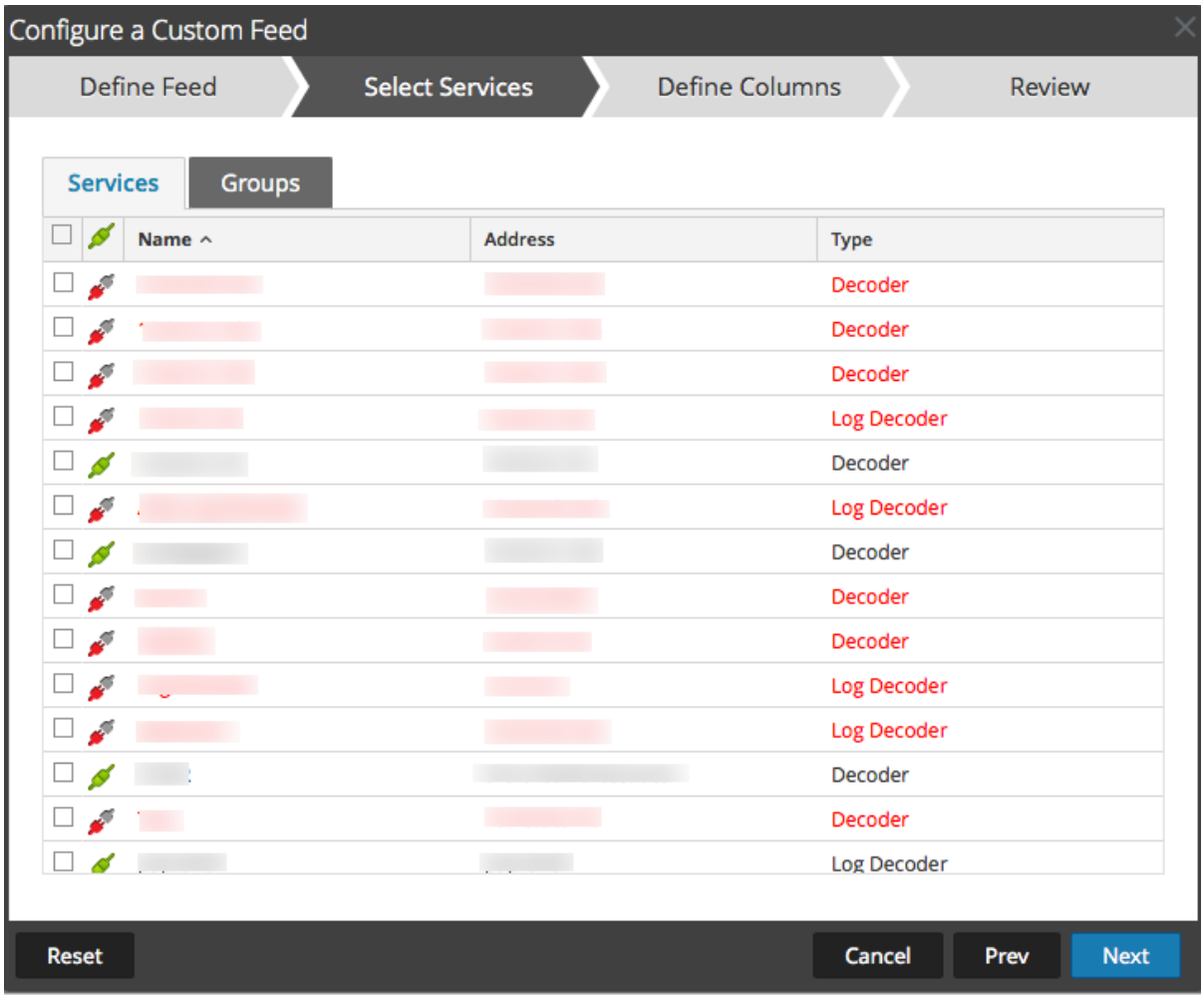
Les Options avancées s'affichent.



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

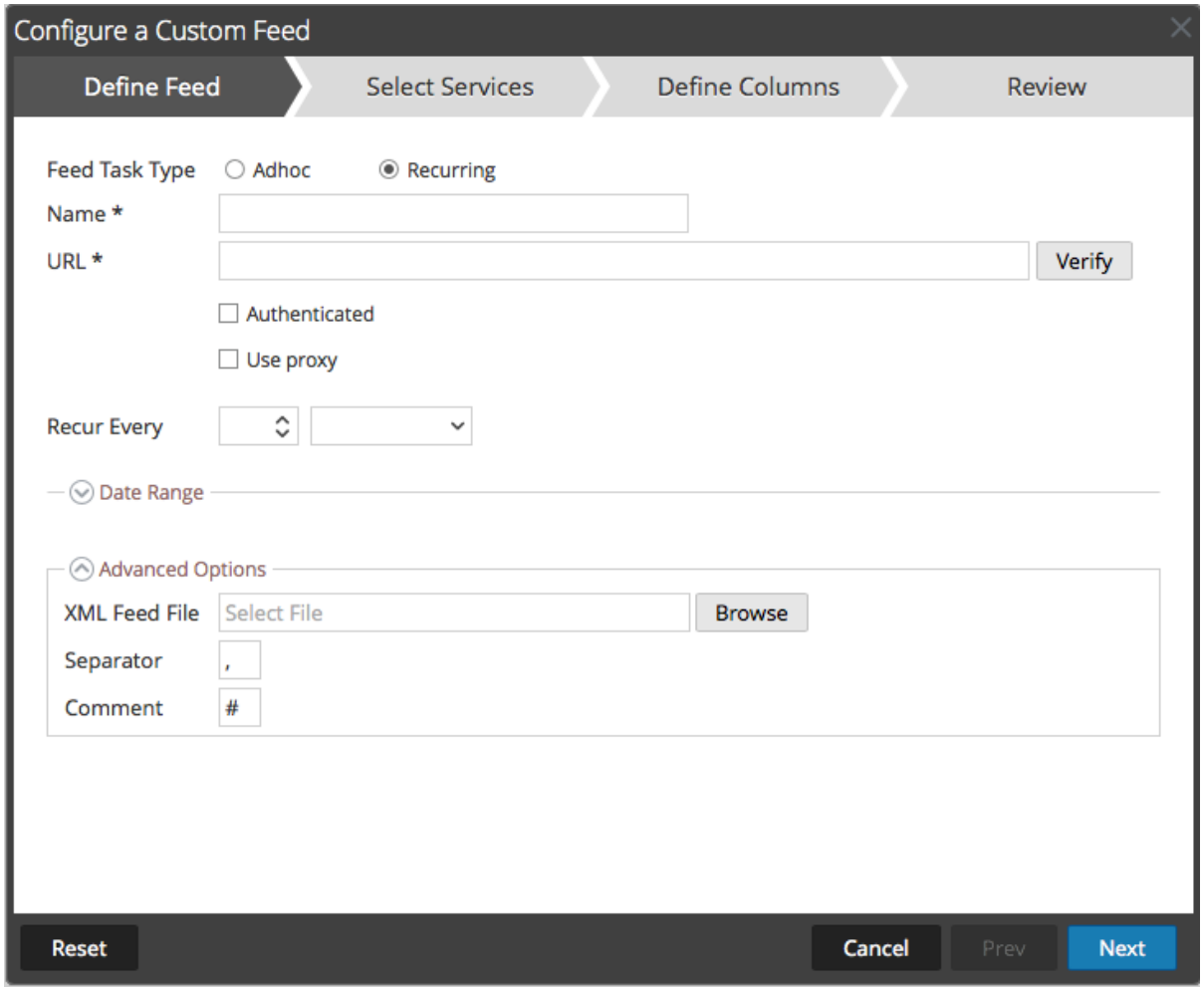
d. Le formulaire Sélectionner des services s'affiche. Voici un exemple de formulaire pour un feed basé sur un fichier de données de feed, sans fichier de définition de feed. Si vous définissez un feed basé sur un fichier de définition de feed,

l'onglet Définir des colonnes n'est pas nécessaire.



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

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



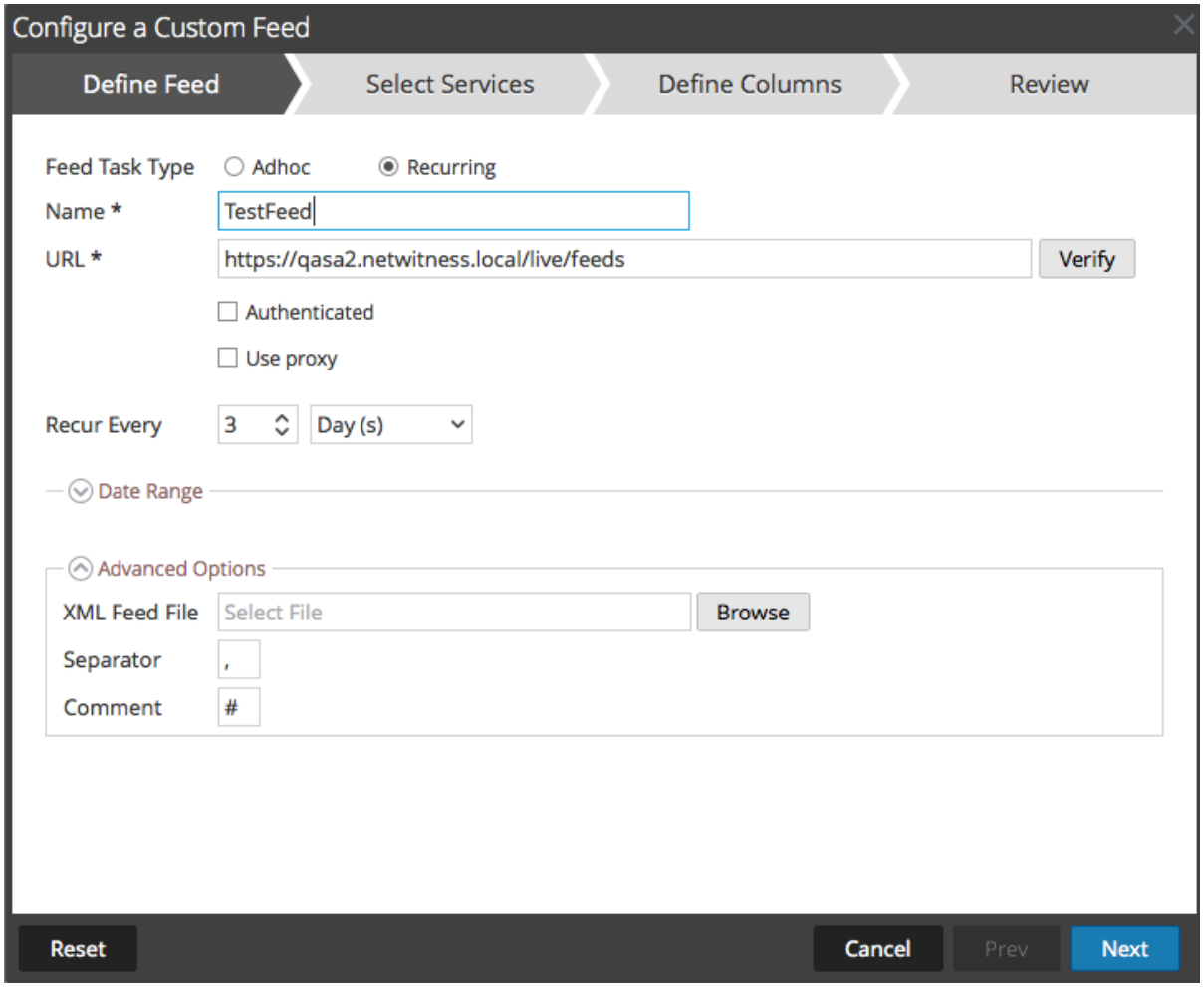
b. Dans le champ **URL**, saisissez l'URL de l'emplacement du fichier de données feed, par exemple, `http://<hostname>/<feeddatafile>.csv`, puis cliquez sur **Vérifier**.
Security Analytics vérifie l'emplacement de stockage du fichier, de façon à ce que Security Analytics puisse vérifier automatiquement le dernier fichier avant chaque récurrence.

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

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

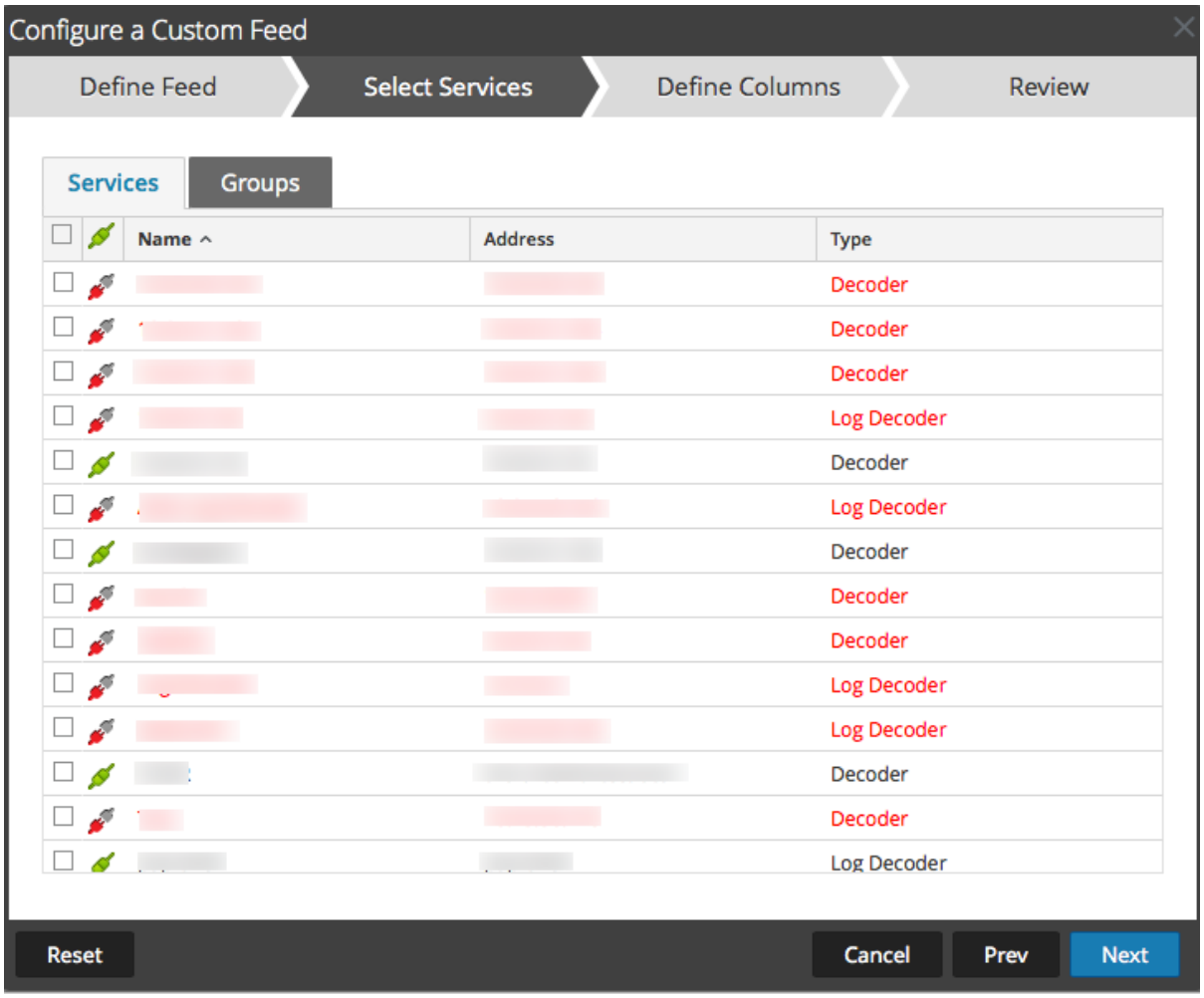
e. Pour définir l'intervalle de récurrence, effectuez l'une des opérations suivantes :
   1. Spécifiez le nombre de minutes, d'heures ou de jours entre les récurrences du champ.
   2. Spécifiez une récurrence hebdomadaire, puis sélectionnez les jours de la semaine.

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



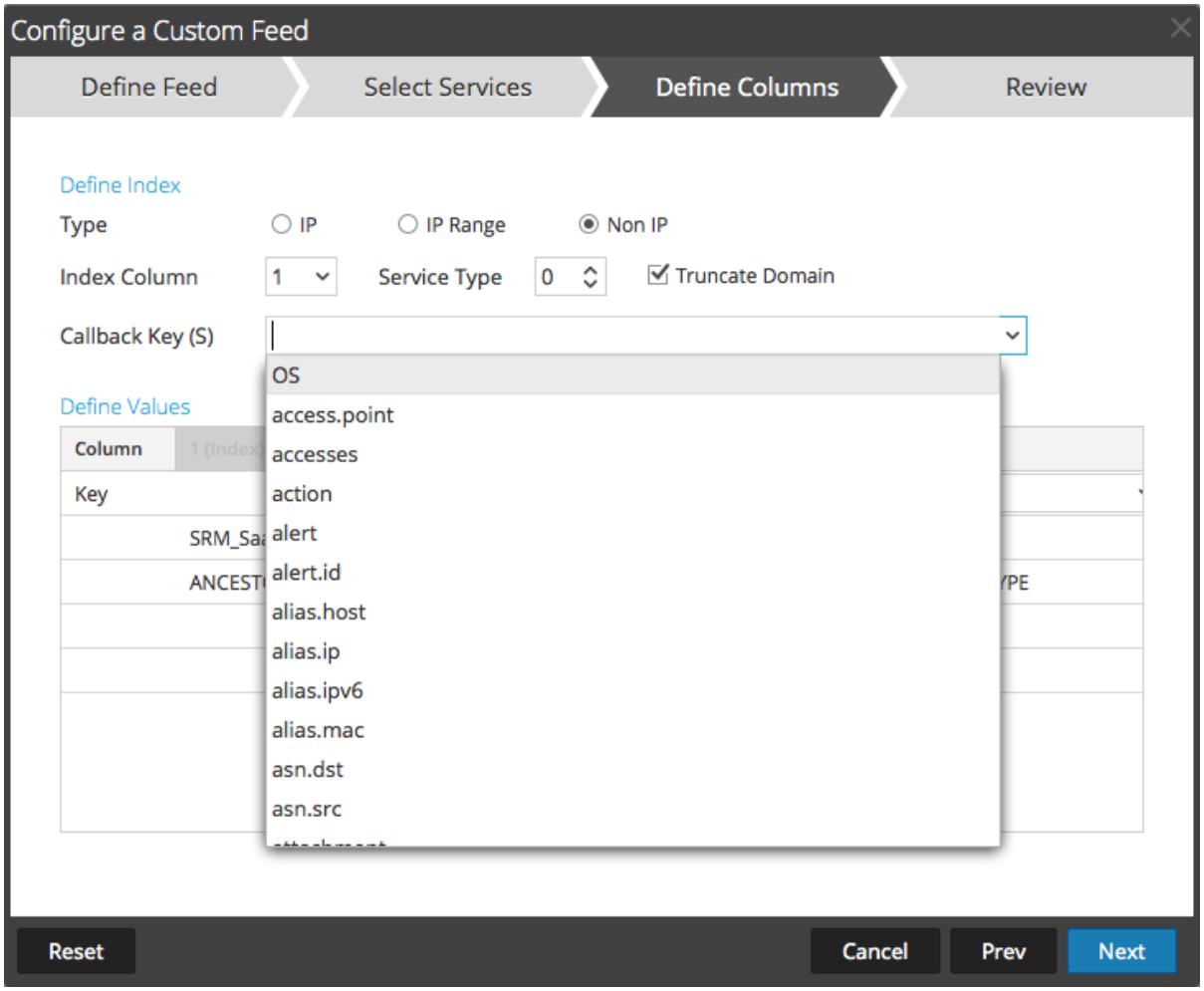
6. (Conditionnel) Si vous souhaitez définir un feed basé sur un fichier de feed XML :
   a. Saisissez le **nom** du feed, puis sélectionnez **Options avancées**.
   Les champs des Options avancées s'affichent.
   b. Sélectionnez un fichier de feed XML à partir du système de fichiers local, choisissez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

Le formulaire Sélectionner des services s'affiche.



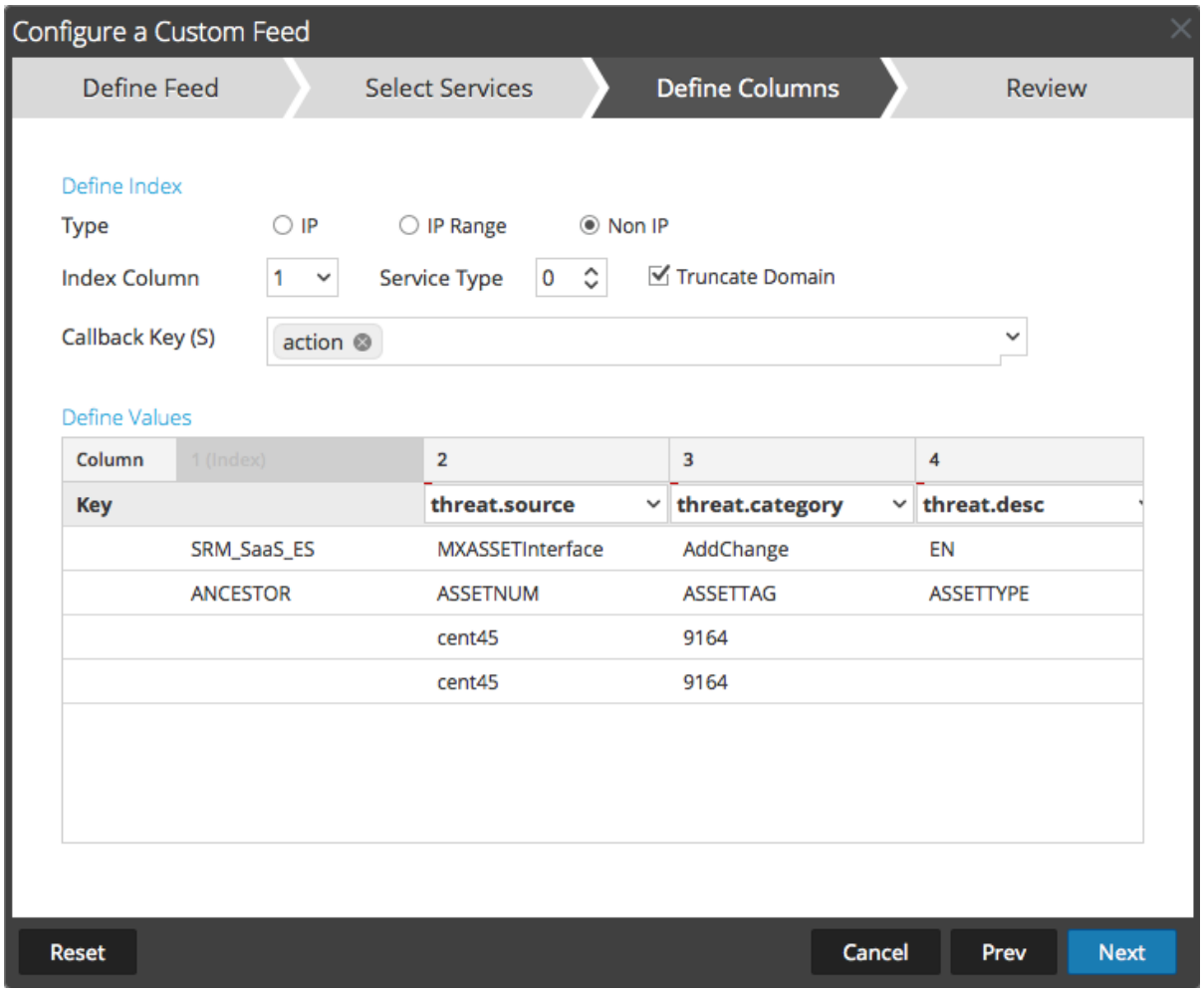
7. Pour identifier les services sur lesquels déployer le feed, effectuez l'une des opérations suivantes :
   a. Sélectionnez un ou plusieurs Decoders et Log Decoders, et cliquez sur **Suivant**.
   b. Cliquez sur l'onglet **Groupes** et sélectionnez un groupe. Cliquez sur **Suivant**.
   Le formulaire Définir des colonnes s'affiche.
8. Pour mapper les colonnes dans le formulaire Définir des colonnes :
   a. Définir le type d'index : **IP**, **Plage IP** ou **Non IP**, puis sélectionnez la colonne d'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**.

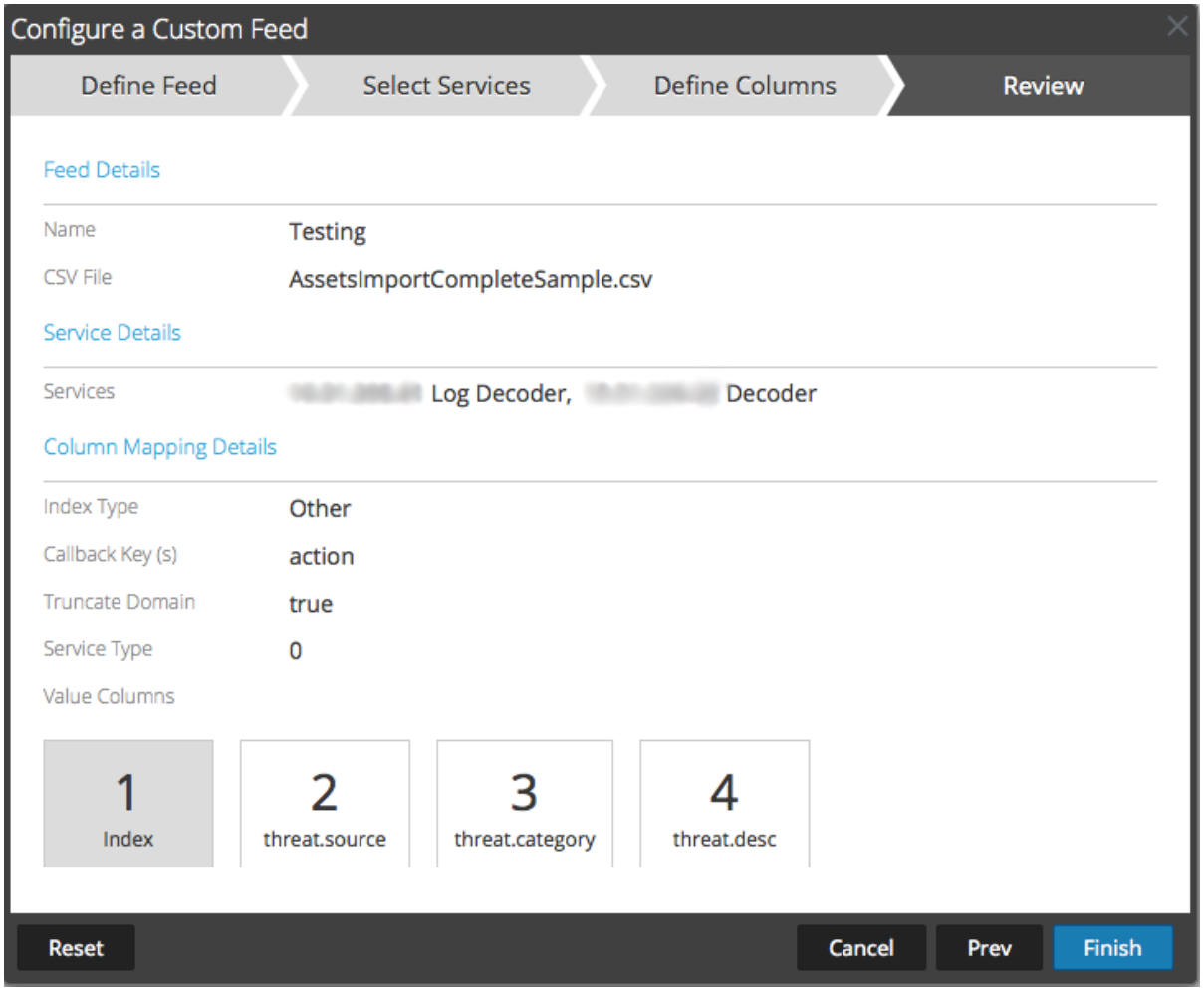


d. Sélectionnez la clé de langue à appliquer aux données de chaque colonne à partir de la liste déroulante. Le méta affiché dans la liste déroulante est basé sur les valeurs définies par le service. Sur la base de compétences solides, vous pouvez

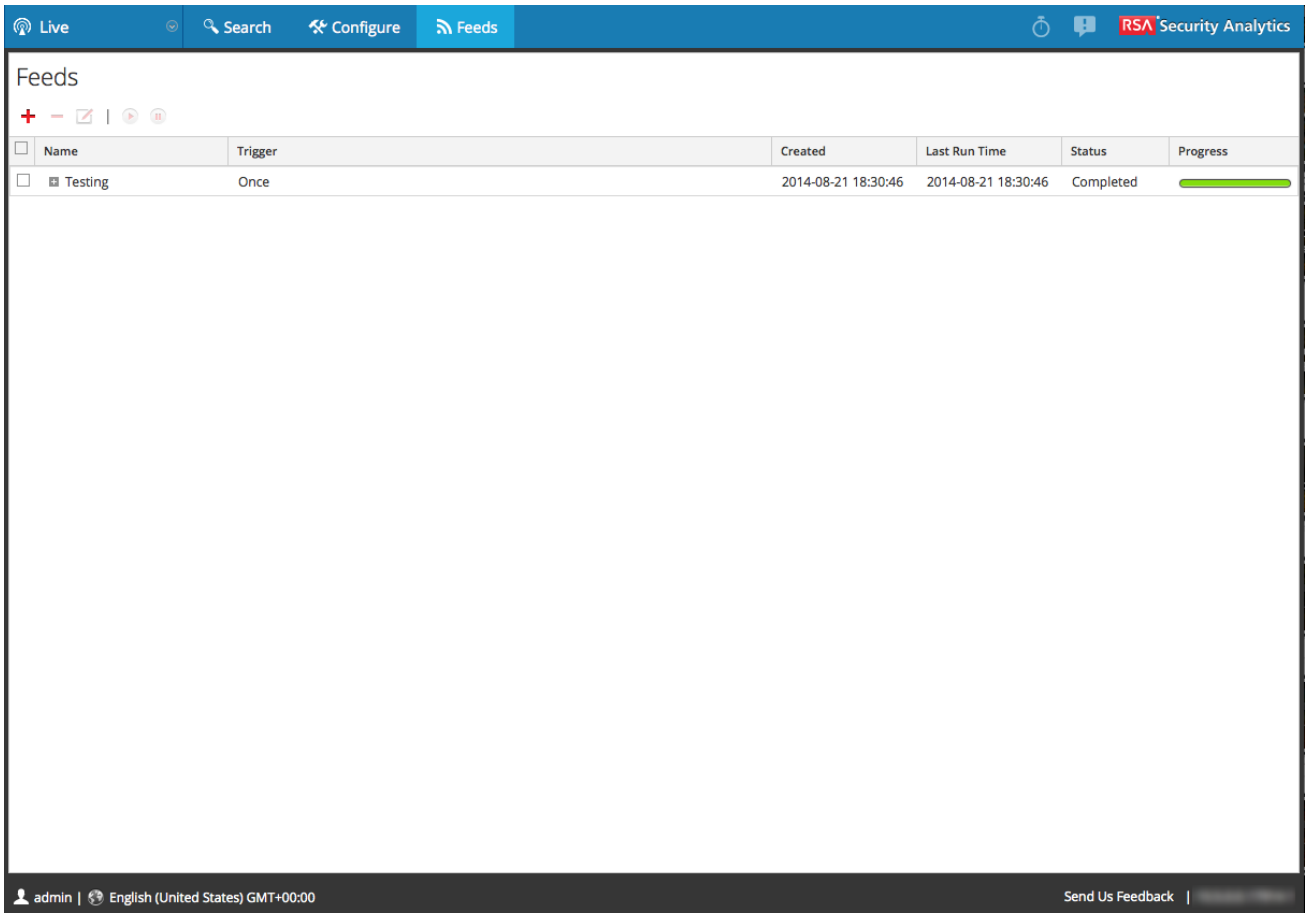
également ajouter d'autres méta.



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



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



Créer un feed d'identité

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

Conditions préalables

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

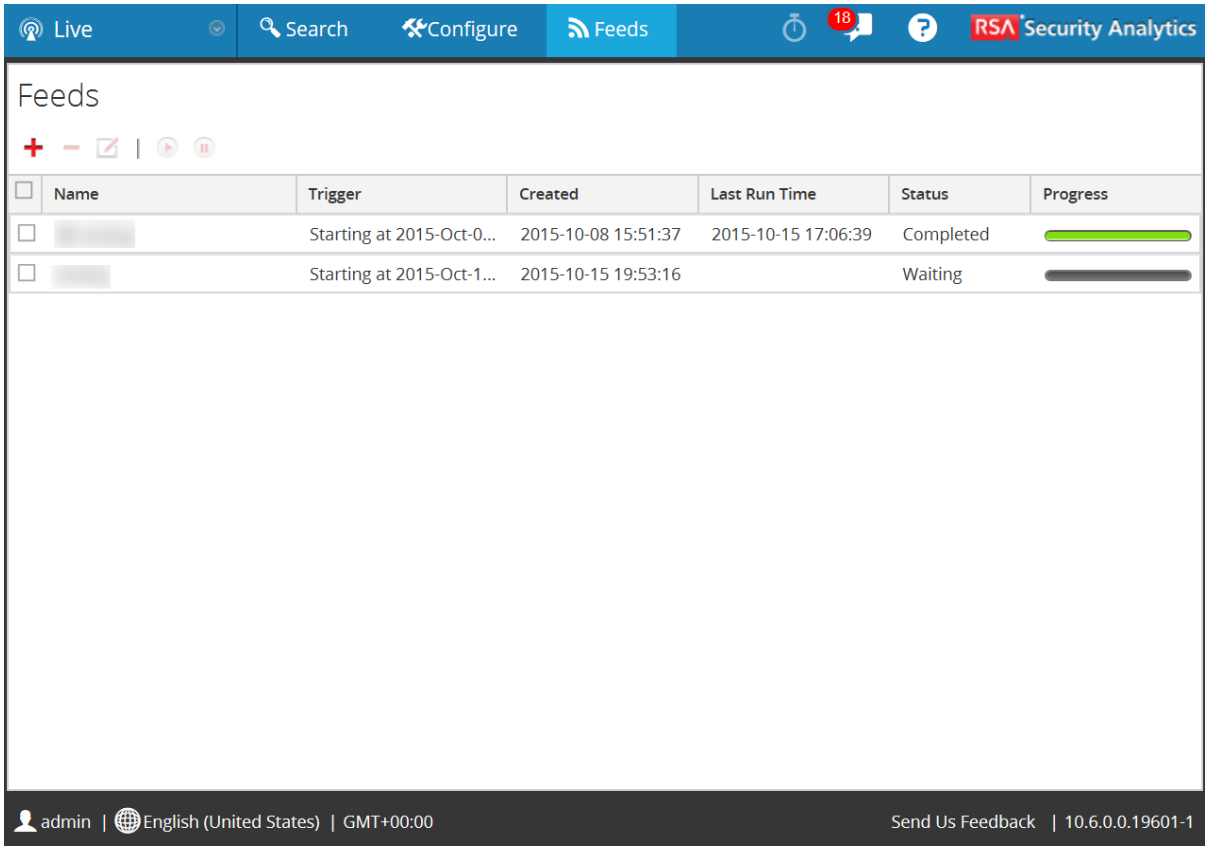
- Le service Log Collector avec le processeur d'événements Identity Feed
- Le service Log Collector avec la collection Windows configurée et activée

Créer un feed d'identité

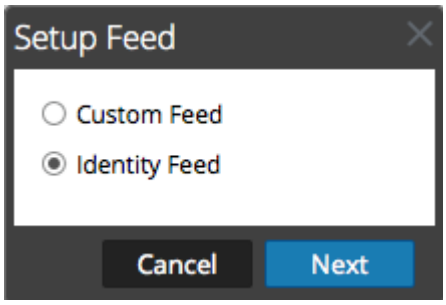
Pour créer un feed d'identité :

1. Dans le menu **Security Analytics**, sélectionnez **Live > Feeds.**
   La grille Feeds s'affiche.

Last Modified: August 10 2016, 9:33AM

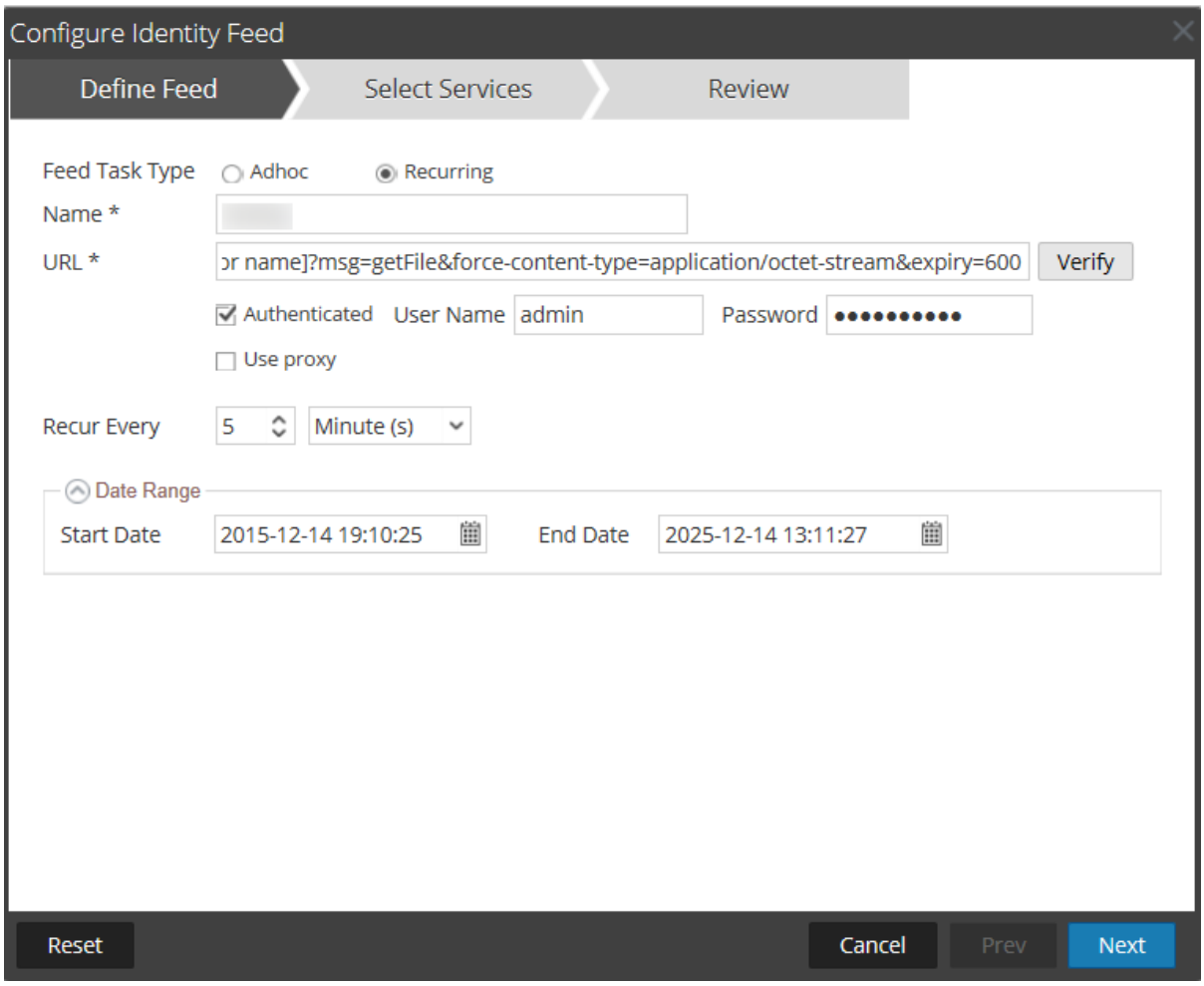


2. Dans la barre d'outils, cliquez sur + .
   La boîte de dialogue Configurer le feed s'affiche, avec Identity Feed sélectionné par défaut.



3. Sélectionnez **Feed d'identité**, puis cliquez sur **Suivant**.
   Le panneau Configurer Identity Feed s'ouvre avec l'onglet **Définir le feed** affiché.
4. (Conditionnel) 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.



Note: Security Analytics vérifie l'emplacement de stockage du fichier, de façon à ce que Security Analytics puisse vérifier automatiquement le dernier fichier avant chaque récurrence.

- Dans le champ **URL**, saisissez l'URL où le fichier de données de feed est placé, par exemple, `http://<LogCollector>:50101/event-processors/<ID de l'événement/ nom du processeur>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

Note: Vous devez fournir les informations pour le <LogCollector> et l'<ID de l'événement/nom du processeur> dans l'URL.

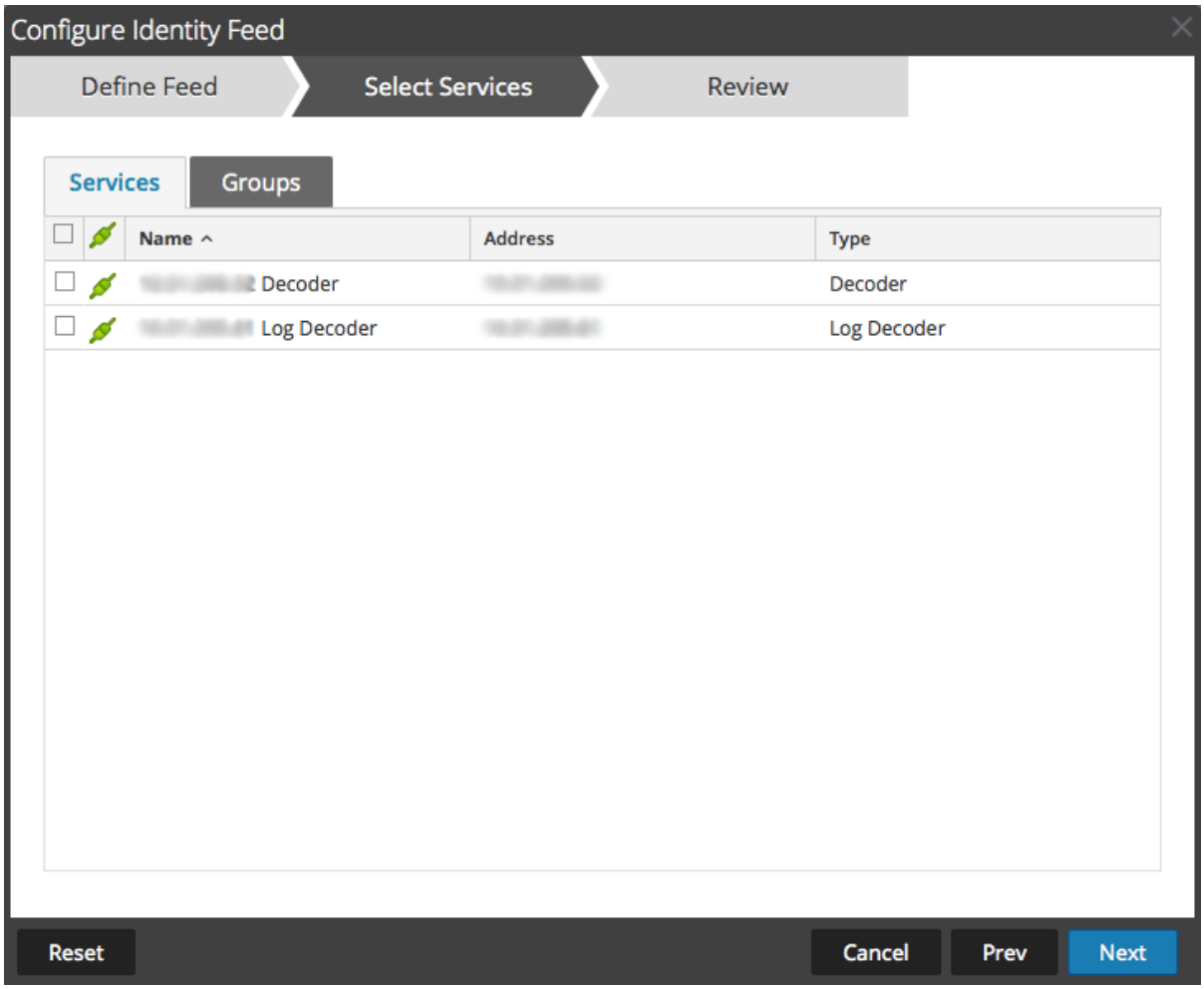
5. (Facultatif) Si l'URL présente un accès restreint et requiert une authentification à l'aide de votre nom d'utilisateur et mot de passe, sélectionnez **Authentifié**. Security Analytics fournit votre nom d'utilisateur et mot de passe pour l'authentification auprès de l'URL.
6. Pour définir l'intervalle de récurrence, effectuez l'une des opérations suivantes :

- Spécifiez le nombre de minutes, d'heures ou de jours entre les récurrences du champ.

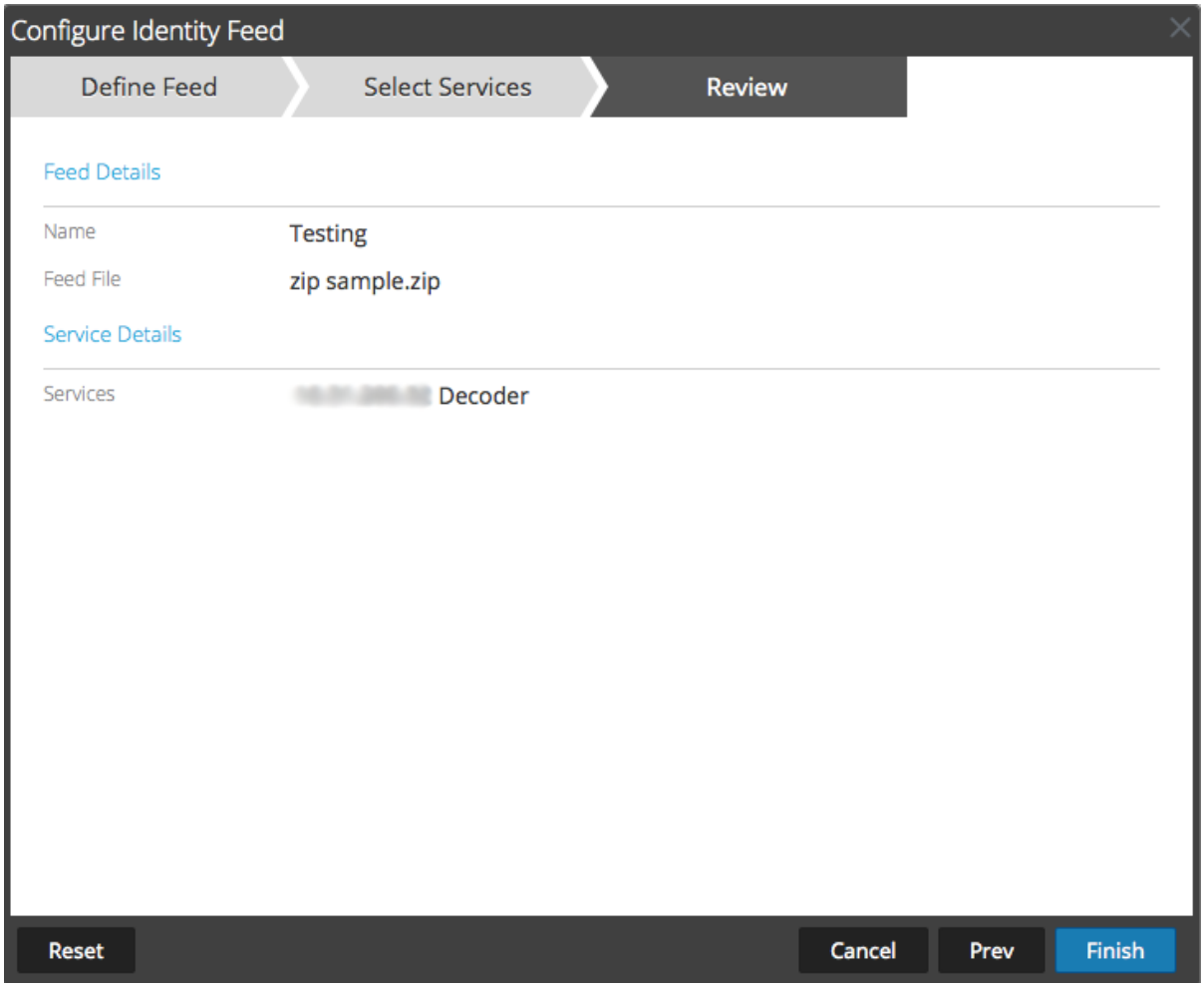
- Pour définir la période pour l'exécution récurrente du feed, spécifiez la **Date de début** et l'heure, ainsi que la **Date de fin** et l'heure.

8. Cliquez sur **Vérifier** pour vérifier votre configuration du feed identité avant de procéder au formulaire Sélectionner des services.
9. Cliquez sur **Suivant**.

Le formulaire Sélectionner des services s'affiche.



6. Pour identifier les services sur lesquels déployer le feed :
7. Sélectionnez un ou plusieurs Decoders et Log Decoders, et cliquez sur **Suivant**.
8. Cliquez sur l'onglet **Groupes** et sélectionnez un groupe. Cliquez sur **Suivant**.
   Le formulaire Révision s'affiche.

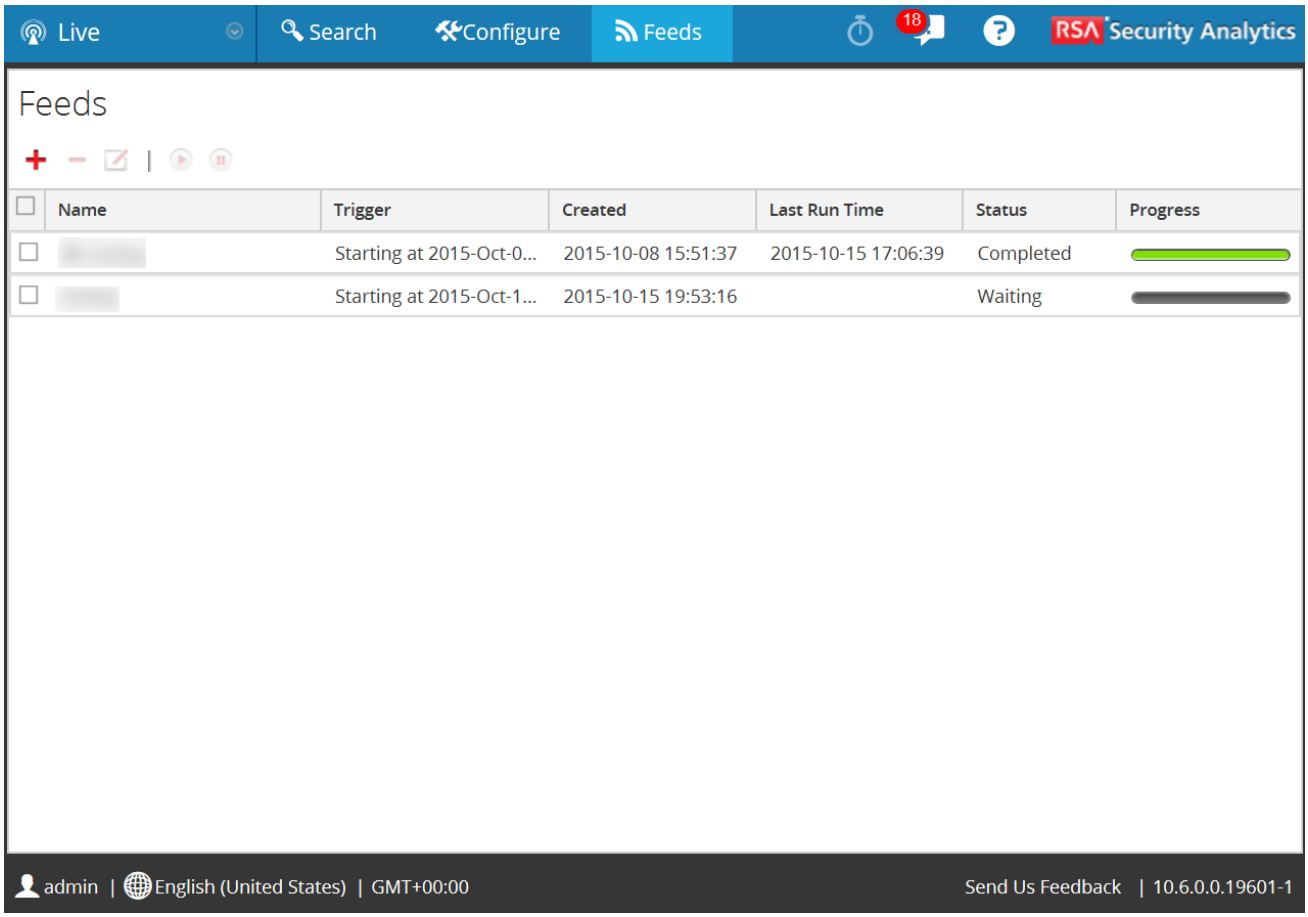


Note: Si un groupe de périphériques avec des Decoders et Log Decoders est utilisé pour créer des feeds récurrents ou personnalisés, vous pouvez modifier le feed et ajouter un nouveau groupe au feed.

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

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.

Last Modified: August 10 2016, 9:33AM



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.

Note: 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.

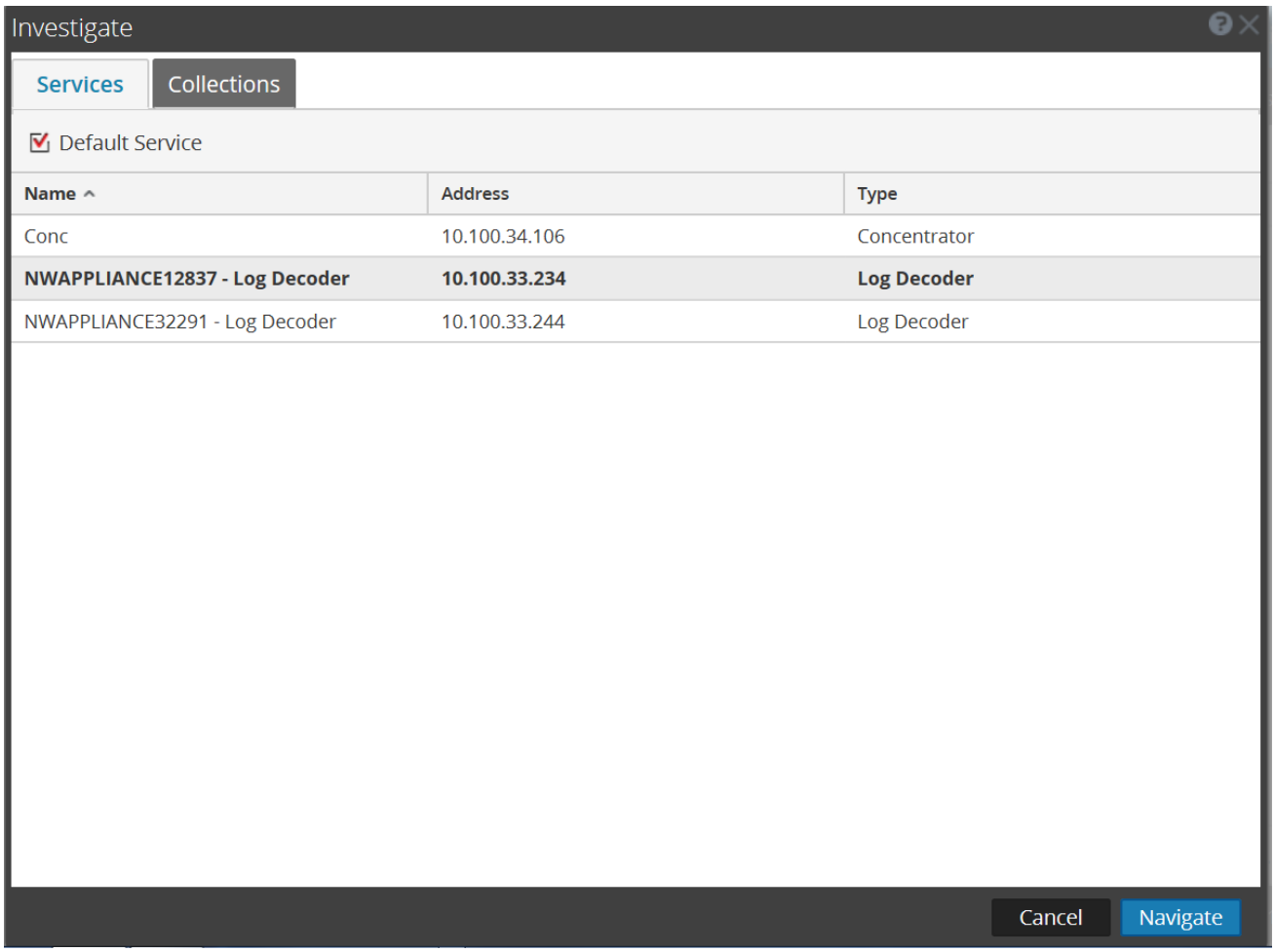
Lorsque vous avez créé un feed d'identité, vous pouvez afficher les résultats en examinant le feed.

Pour examiner un feed d'identité configuré :

1. Allez dans le menu Security Analytics.

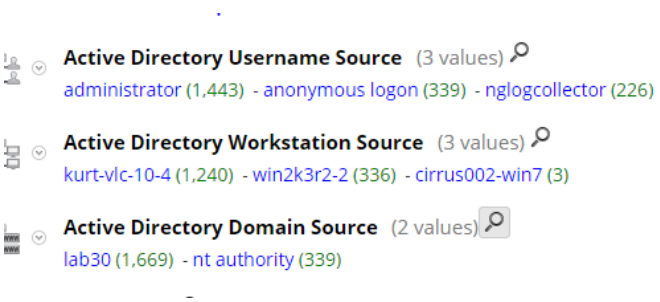
Last Modified: August 10 2016, 9:33AM

2. Sélectionnez **Examiner > Naviguer**.
   L'écran Procédure d'enquête s'affiche.



3. Sélectionnez **Conc** (Concentrator) et sélectionnez **Naviguer**.
4. Sélectionnez **Charger les valeurs** pour récupérer les clés méta.

Dans le panneau inférieur, 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.

Last Modified: August 10 2016, 9:33AM

Modifier un feed

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

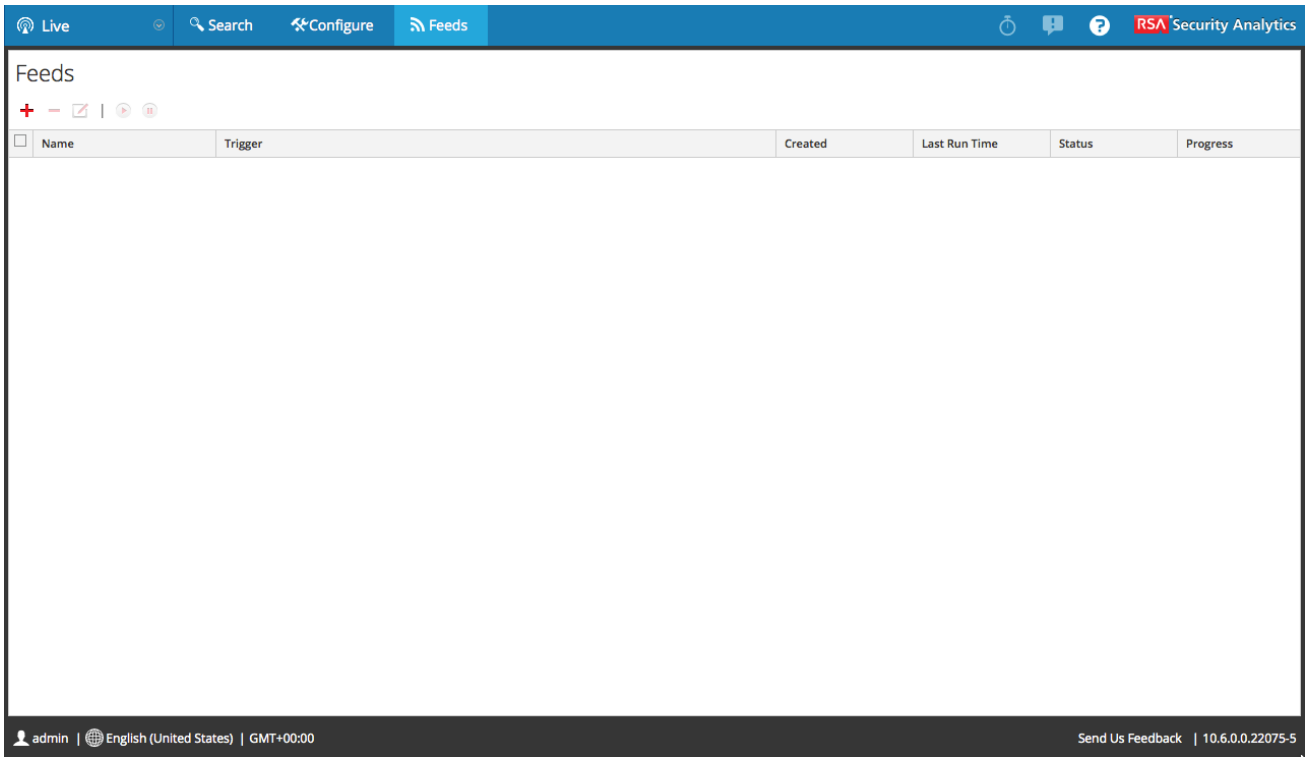
L'exécution de cette procédure aura pour résultat :

- 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.

Modifier un feed existant

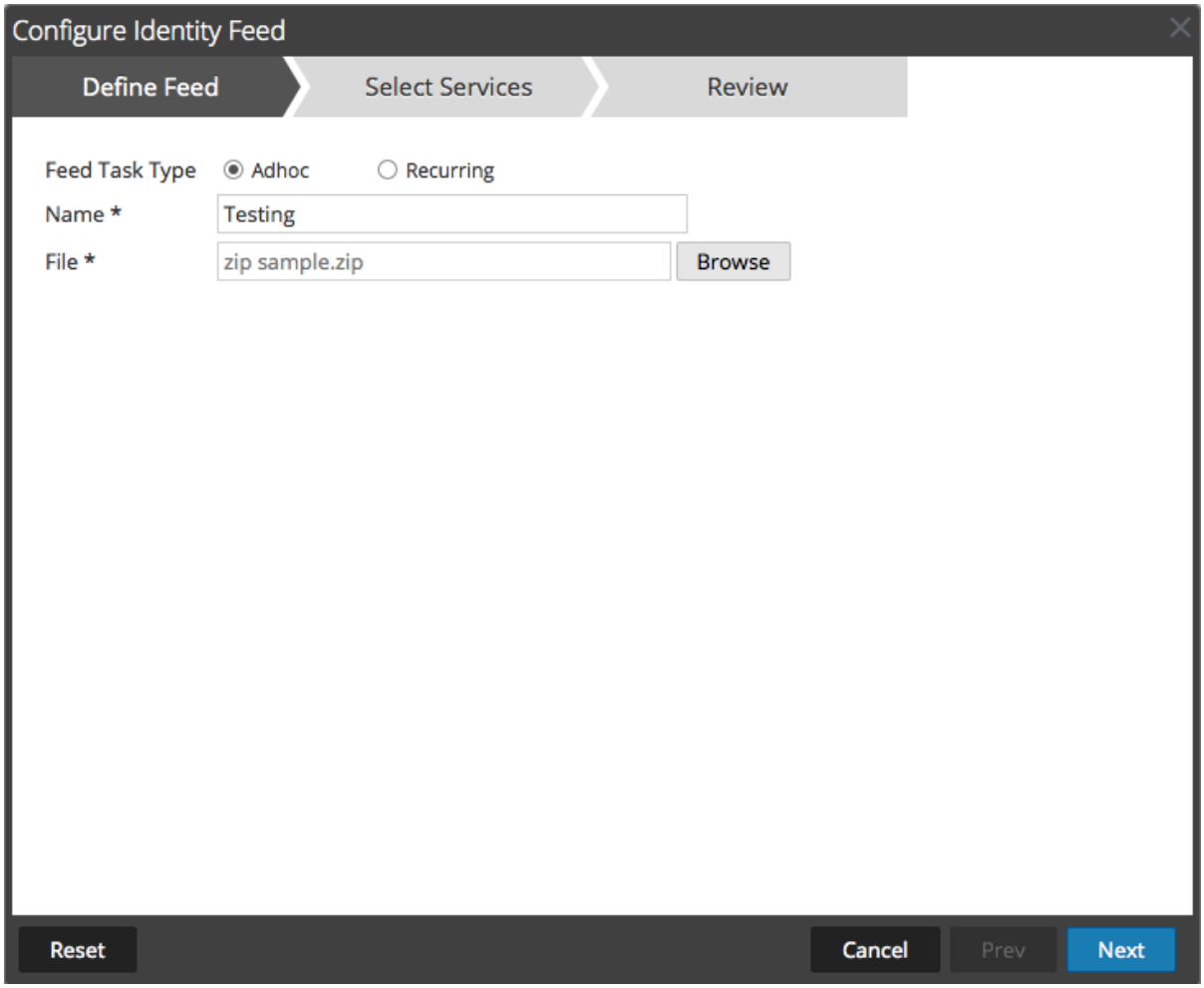
Pour modifier un feed existant :

1. Dans le **Security Analytics menu**, sélectionnez **Live > Feeds.**
   La vue Feeds s'affiche.



Last Modified: August 10 2016, 9:33AM

2. Dans la barre d'outils, sélectionnez un feed et 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 tout autre paramètre s'appliquant au type de feed dans les onglets Définir le feed, Sélectionner des services et Définir des colonnes.
5. À tout moment avant de cliquer sur **Terminer**, vous pouvez :
   - Cliquer sur **Annuler** pour fermer l'assistant sans enregistrer vos modifications.
   - Cliquez sur **Réinitialiser** pour effacer les données de l'assistant.
   - Cliquez sur **Suivant** pour afficher le formulaire suivant (si ce n'est pas le dernier formulaire).
   - Cliquez sur **Précédent** pour afficher le formulaire précédent (si ce n'est pas le premier formulaire).
6. Sous l'onglet **Révision**, passez en revue les informations du feed et, si elles sont correctes, cliquez sur **Terminer**.
   Le feed est ajouté à la liste de feeds et la barre de progression indique l'avancement. Lorsque le fichier de définition de fichier du feed est créé avec succès, l'assistant Créer un feed se ferme, et le feed et le fichier de token correspondant est répertorié

dans la grille de feed. Vous pouvez développer ou réduire l'entrée pour voir combien de services sont inclus, et quels services ont abouti.

Last Modified: August 10 2016, 9:33AM

Supprimer un feed

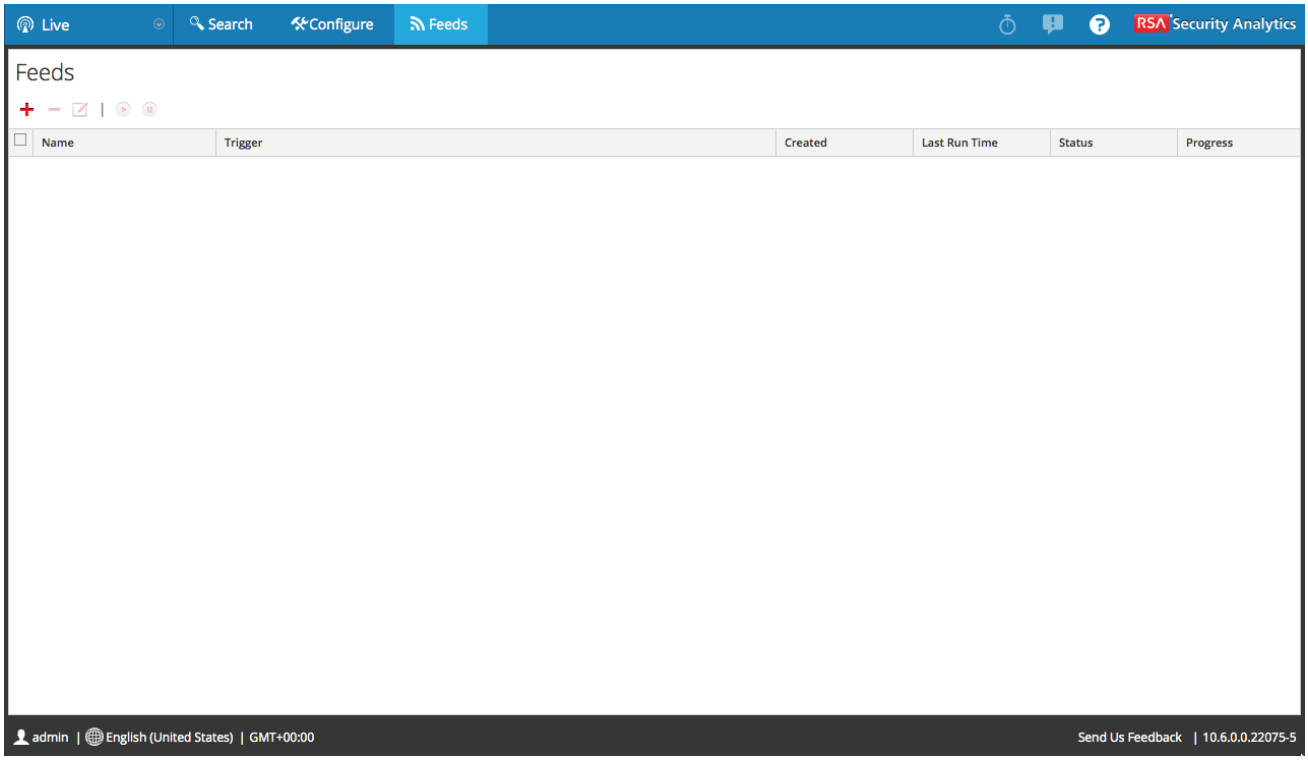
Présentation

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

Procédure

Pour supprimer un feed :

1. Dans le **Security Analytics menu**, sélectionnez **Live > Feeds.**
   La vue Feeds s'affiche.

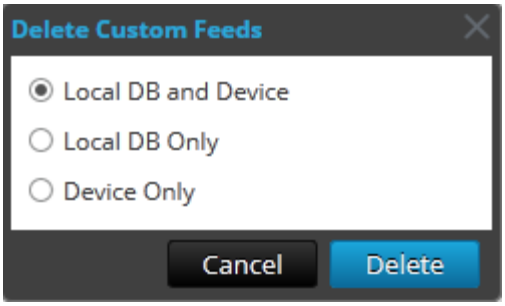


2. Dans la barre d'outils, sélectionnez un feed et cliquez sur — .
   La boîte de dialogue Supprimer les feeds personnalisés s'affiche. Vous pouvez sélectionner l'une des options suivantes pour supprimer le feed :

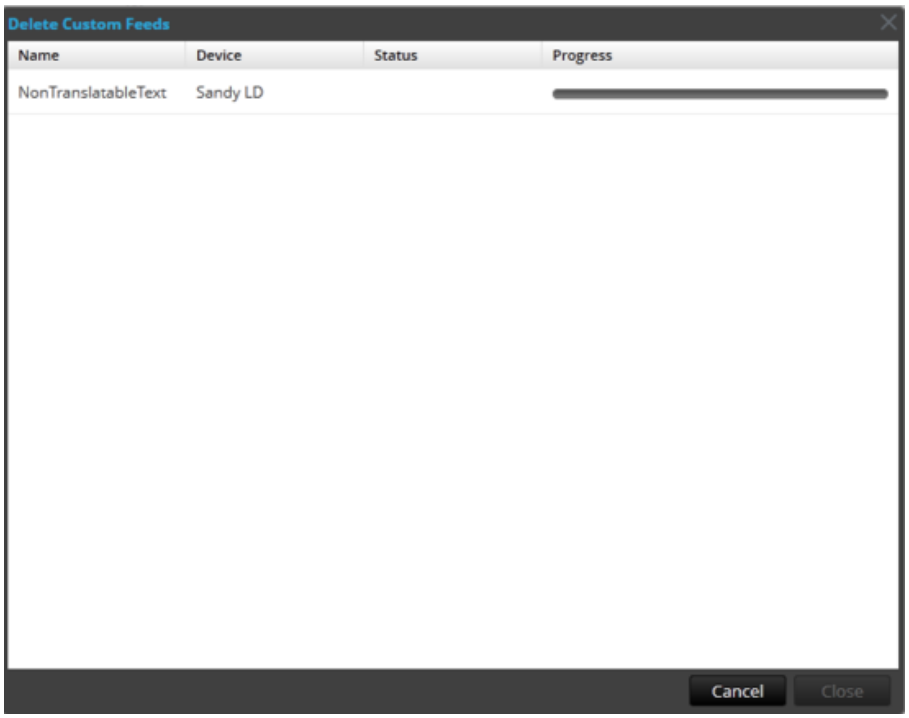
- Si vous choisissez de supprimer le feed dans **BD locale et Service**, le feed sera supprimé à la fois dans la zone des services et de l'instance locale de Security Analytics. Le feed supprimé n'apparaîtra plus dans l'interface utilisateur Security Analytics.

Last Modified: August 10 2016, 9:33AM

- Si vous choisissez de supprimer le feed depuis **BD locale uniquement**, le feed sera supprimé de la zone Security Analytics locale. Le feed supprimé n'apparaît plus dans l'interface utilisateur Security Analytics ; 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 Security Analytics 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.



Supprimer les ressources souscrites de la grille Abonnements aux déploiements

Cette rubrique vous indique comment supprimer des ressources à partir de la vue Configurer Live > onglet Déploiements > panneau Abonnements.

Cette procédure supprime les ressources du panneau Abonnements de l'onglet Déploiements.

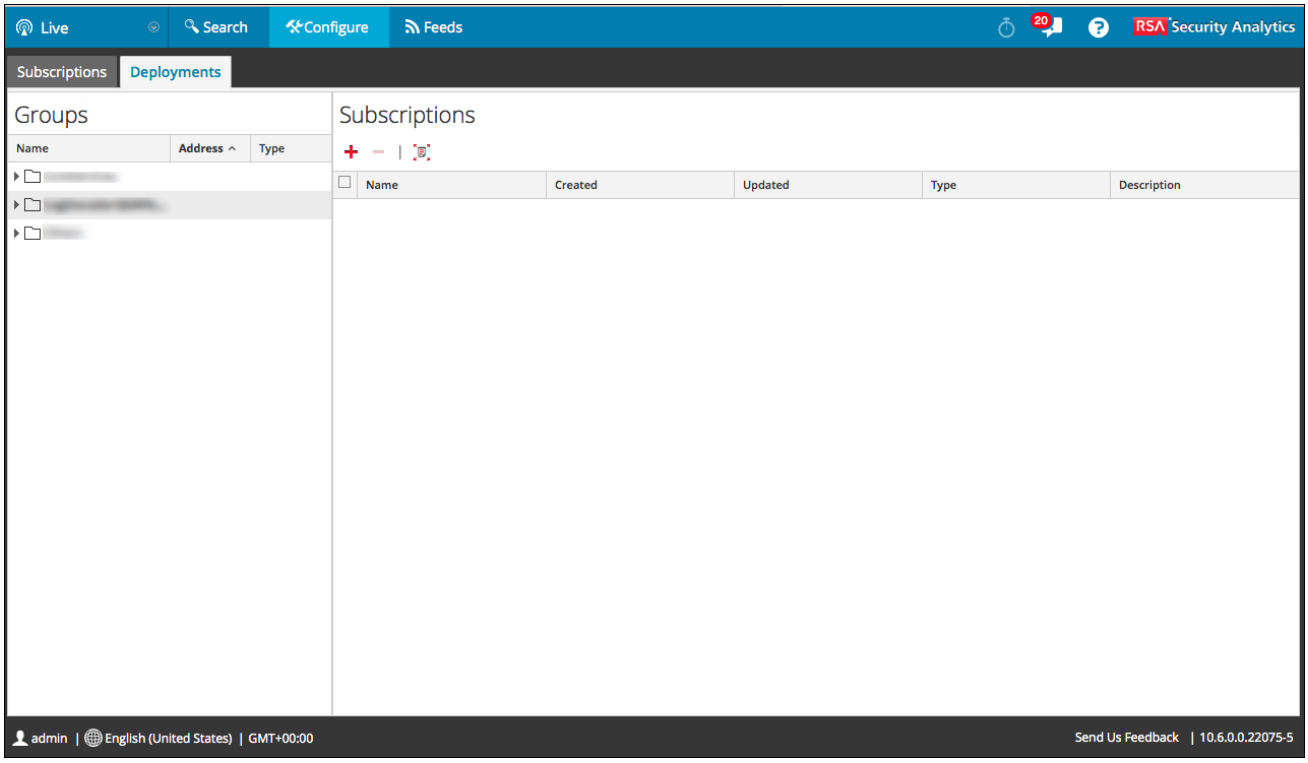
Supprimer les ressources souscrites de la grille Abonnements aux déploiements

Les abonnements sélectionnés pour être déployés sur un groupe de services sont déployés pendant la synchronisation. Vous pouvez supprimer des abonnements dans le panneau Abonnements de l'onglet Déploiements, 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.

Last Modified: August 10 2016, 9:33AM



S'abonner et se désabonner d'une ressource

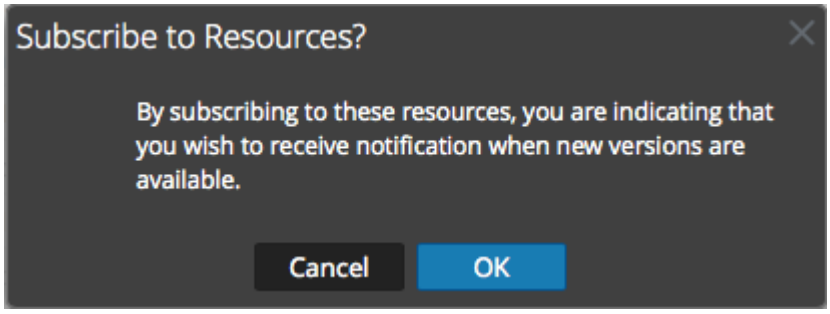
L'exécution de cette procédure aura pour résultat :

- Abonnement à une ressource de la vue Ressources Live.
- Désabonnement d'une ressource de la vue Ressources Live.

S'abonner à une ressource

Pour s'abonner à une ressource :

1. Dans le panneau **Critères de recherche**, spécifiez des critères de recherche et cliquez sur **Rechercher**.
2. Sélectionnez une ou plusieurs ressources, puis cliquez sur Subscribe.
   Une boîte de dialogue de confirmation s'affiche.



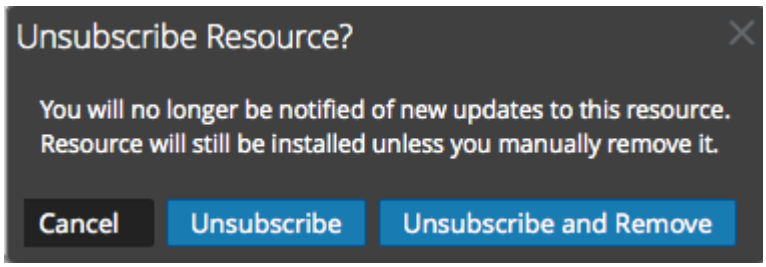
3. Pour confirmer votre abonnement à la ressource, cliquez sur **OK**.
   La ressource est ajoutée aux abonnements gérés sous l'onglet Abonnements et peut être déployée sous l'onglet Déploiements.

Se désabonner d'une ressource

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 :

Last Modified: August 10 2016, 9:33AM

1. Avec une ressource affichée dans la **vue Ressources**, 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 résultats sous forme de grille ou de façon détaillée

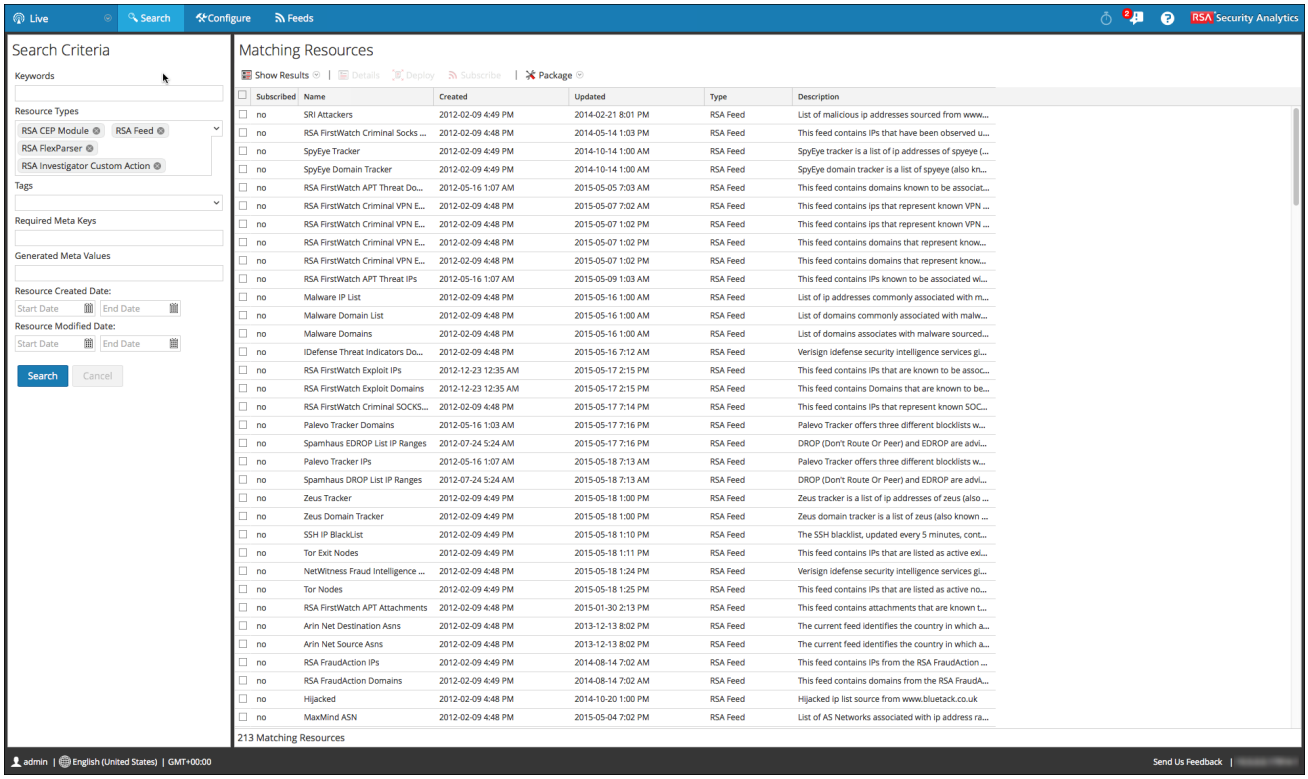
Cette rubrique vous indique comment basculer entre les vues Détails et Grille dans le panneau Ressources correspondant de la vue Live Search.

Une fois cette procédure terminée, les résultats de votre recherche s'afficheront dans une grille ou de façon détaillée.

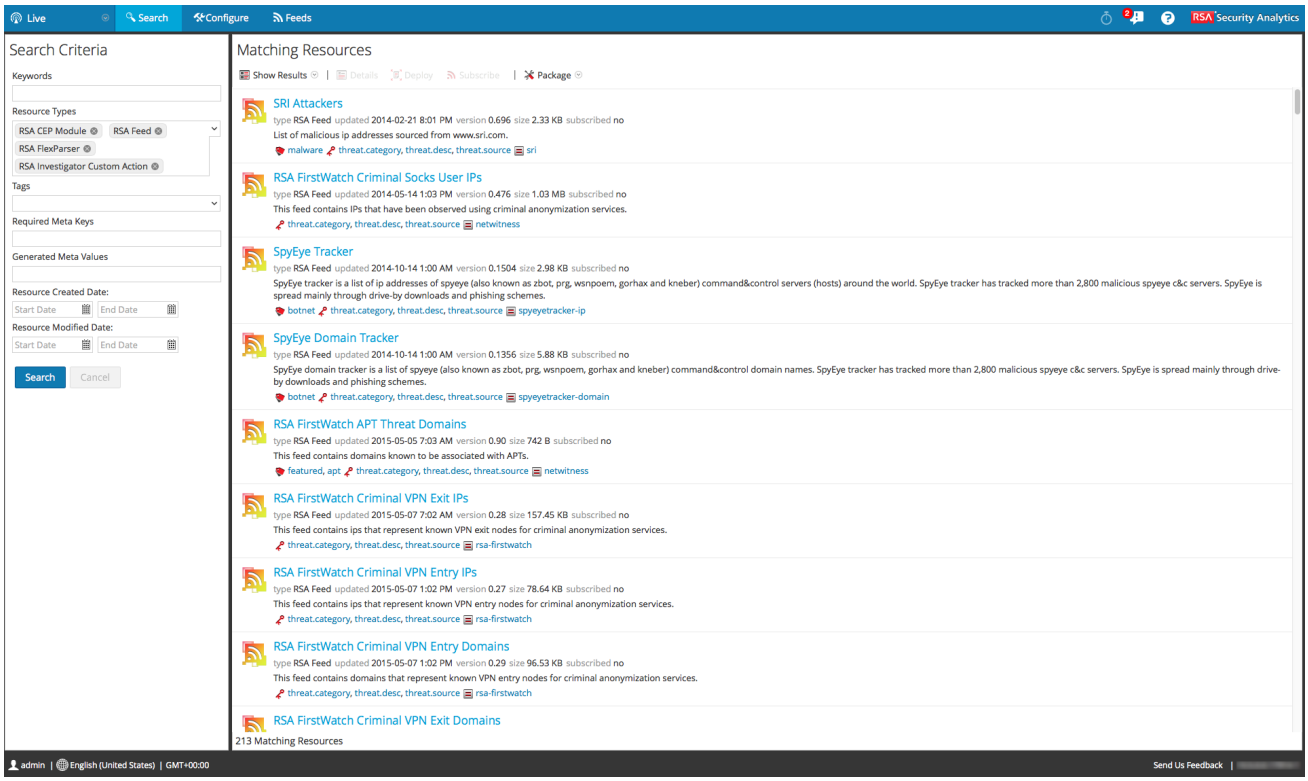
Afficher les résultats sous forme de grille ou de façon détaillée

Pour basculer d'une page d'affichage à une vue sous forme de grille :

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



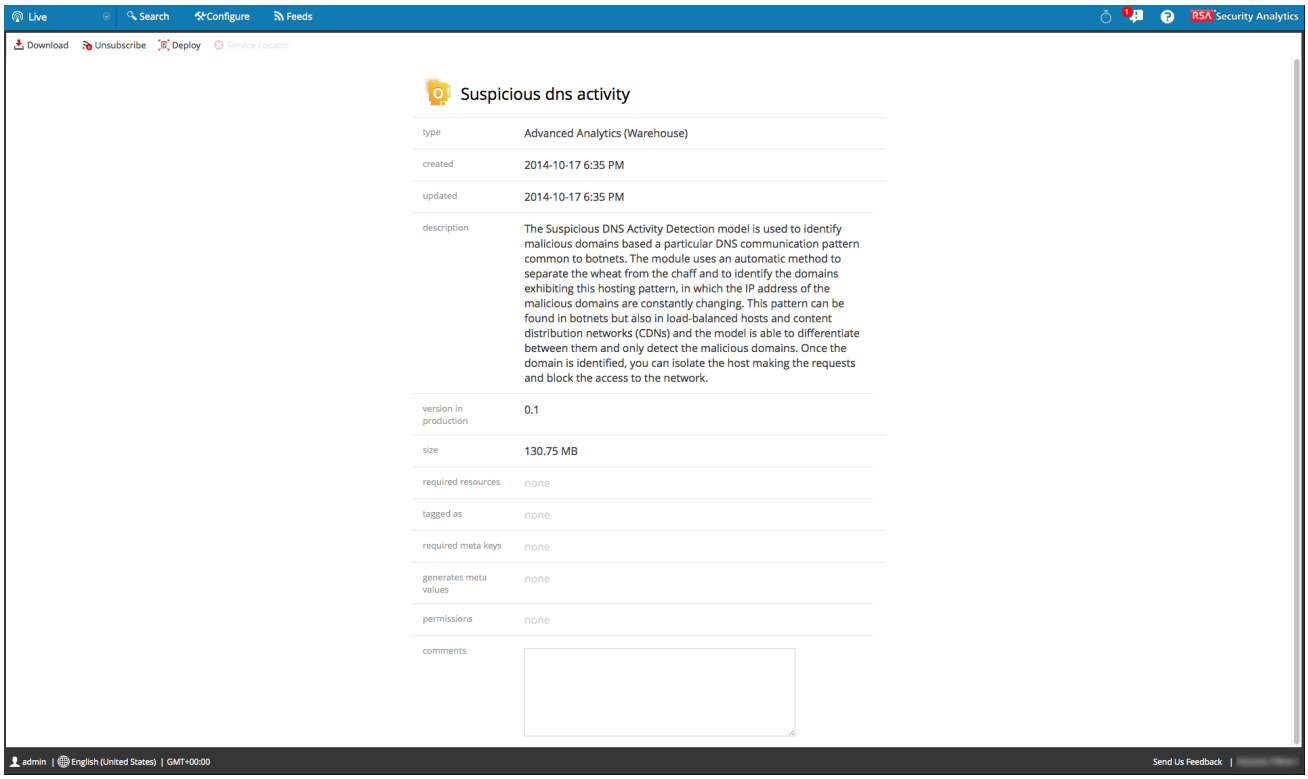
2. Pour accéder aux résultats détaillés à partir de l'affichage sous forme de grille, cliquez sur **Afficher les résultats > Détaillés**.



Afficher les détails d'une ressource souscrite dans la vue Ressource

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.

Procédure

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.

Last Modified: August 10 2016, 9:33AM

Références

Cette rubrique décrit les fonctionnalités et le fonctionnement de l'interface utilisateur de Live dans Security Analytics.

Le composant Live de Security Analytics doit être configuré afin de communiquer avec le CMS. Il dispose des vues suivantes : Rechercher, Configurer et Feeds.

Last Modified: August 10 2016, 9:33AM

Assistant de déploiement

Lorsque vous obtenez des résultats après avoir parcouru des ressources dans 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 fait qu'elles sont directement déployées vers les services sans tirer parti des puissantes fonctions de gestion des ressources de Security Analytics. 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**.

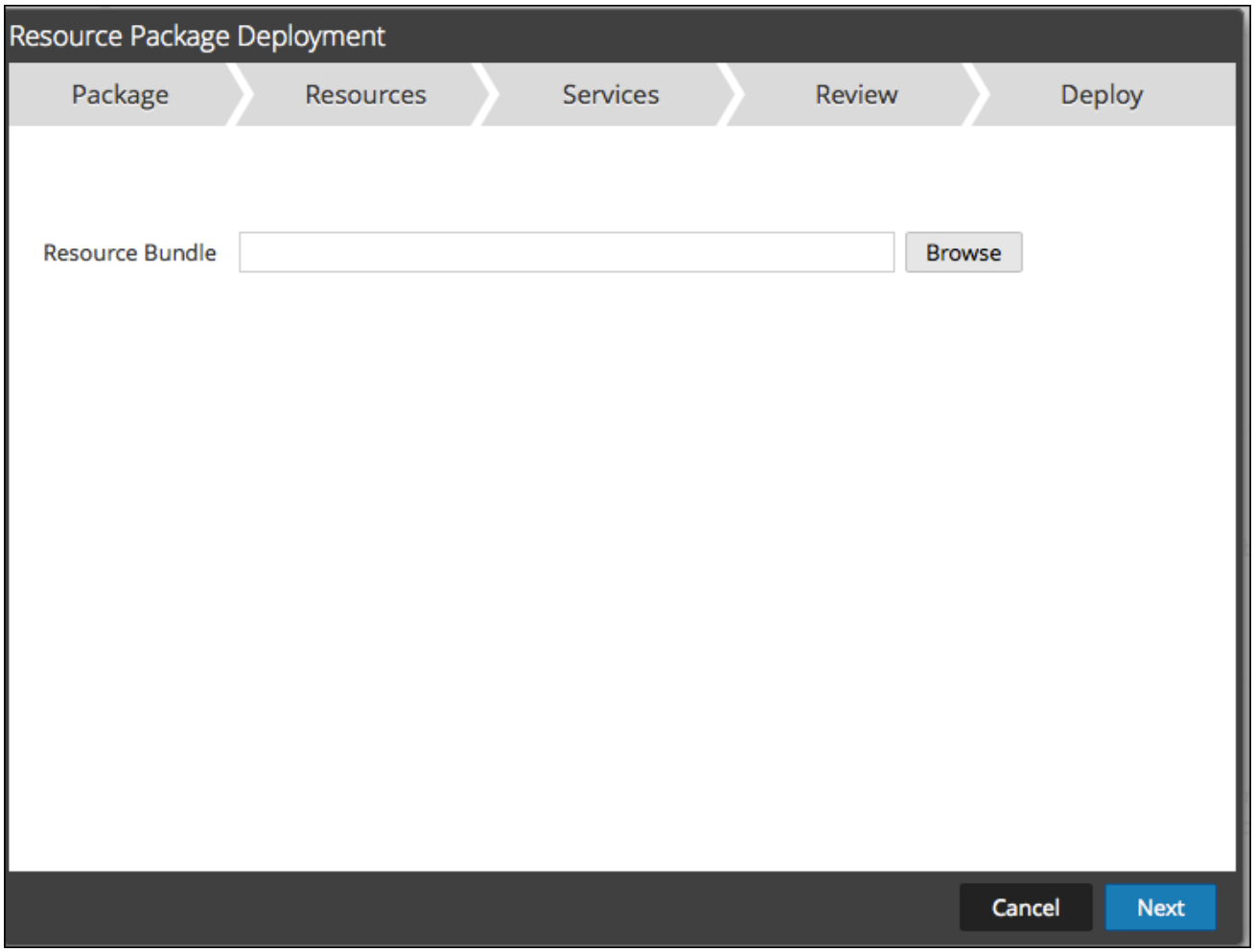
Caractéristiques

L'assistant Déploiement contient cinq onglets : **Package, Ressources**, **Services**, **Vérifier** et **Déployer**.
Fermer permet de quitter la boîte de dialogue et de revenir à la vue Live Search.

Onglet Package

Cet onglet est utilisé pour rechercher un package de ressources.

La figure suivante donne un exemple de l'onglet **Package**.



Onglet Ressources

Affiche les ressources sélectionnées dans les résultats en grille du panneau Ressources correspondantes.

Cet onglet est utilisé pour sélectionner les ressources à déployer. La figure suivante donne un exemple de l'onglet **Ressources**.

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

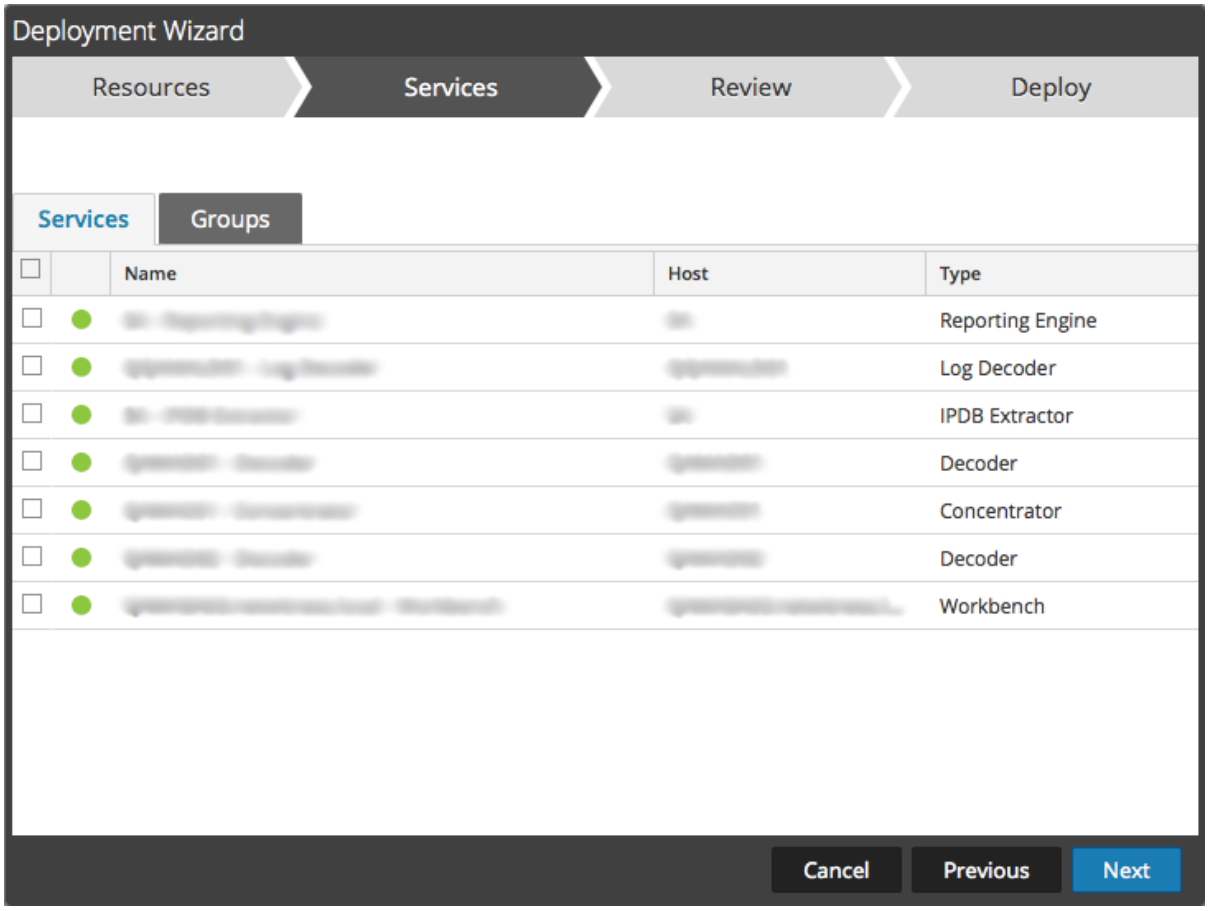
Élément	Description
Noms des ressources	Affiche le nom des ressources que vous avez sélectionnées (par exemple, **NetWitness Lua Library**).

Élément	Description
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**).
Boutons de commande	
Annuler	Annule le déploiement et quitte l'assistant.
Suivant	Affiche la page suivante de l'assistant.

Onglet Services

Affiche deux onglets, **Services** et **Groupes.** Ils fournissent une liste des services et des groupes de services configurés dans la vue **Administration** > **Services**. Les colonnes représentent un sous-ensemble des colonnes disponibles dans la vue Services.

Cet onglet est utilisé pour sélectionner les services ou les groupes de services vers lesquels vous voulez déployer les ressources sélectionnées. La figure suivante donne un exemple de l'onglet **Services**.



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

Élément	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.
Hôte	Affiche le nom de l'hôte de ressource.
Type	Affiche le type de service Security Analytics (type d'hôte/de service).
Groupes	

Élément	Description
	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.
Boutons de commande	
Annuler	Annule le déploiement et quitte l'assistant.
Précédent	Affiche l'onglet précédent de l'assistant.
Suivant	Affiche l'onglet suivant de l'assistant.

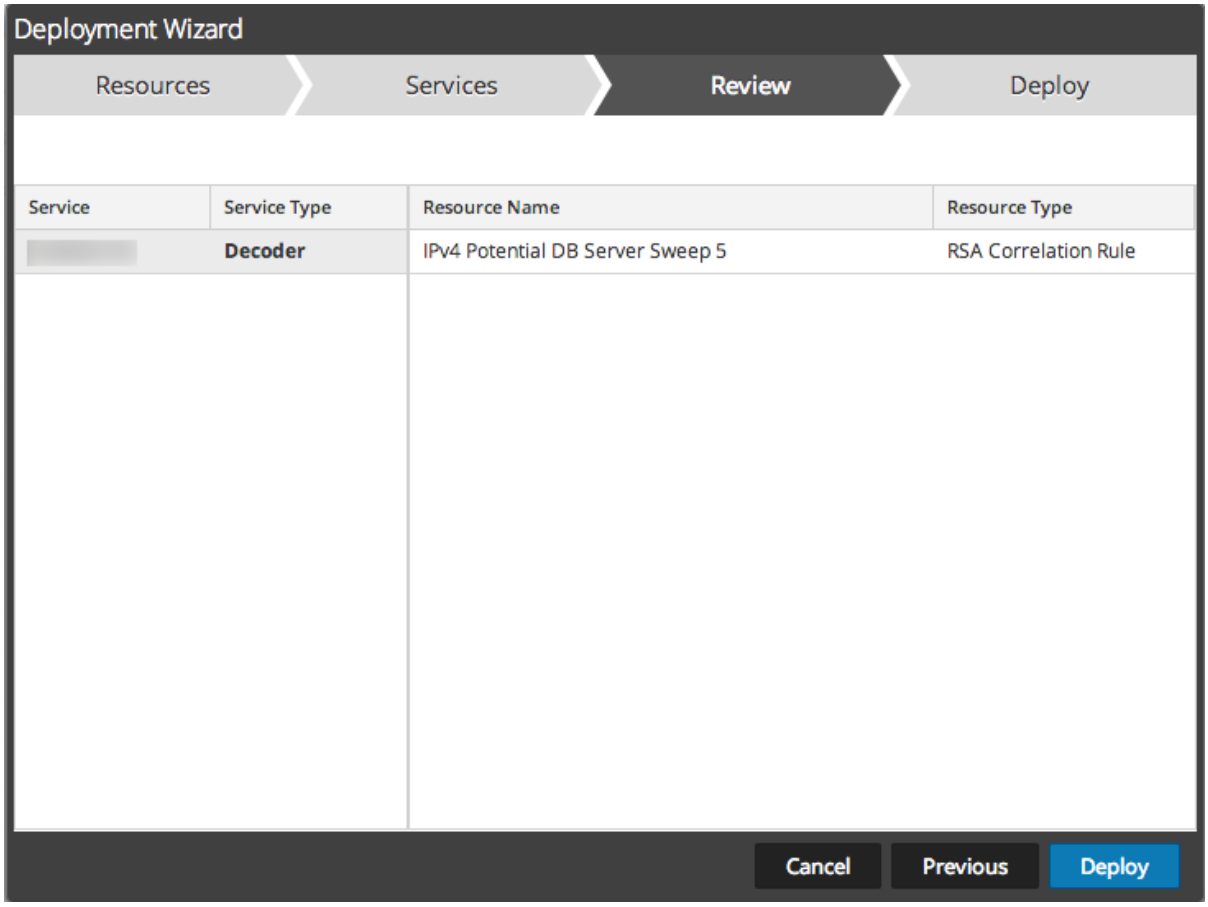
Onglet Révision

Affiche les ressources et les services sur lesquels les ressources sont 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**.

Élément	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 Security Analytics (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**).

Last Modified: August 10 2016, 9:33AM

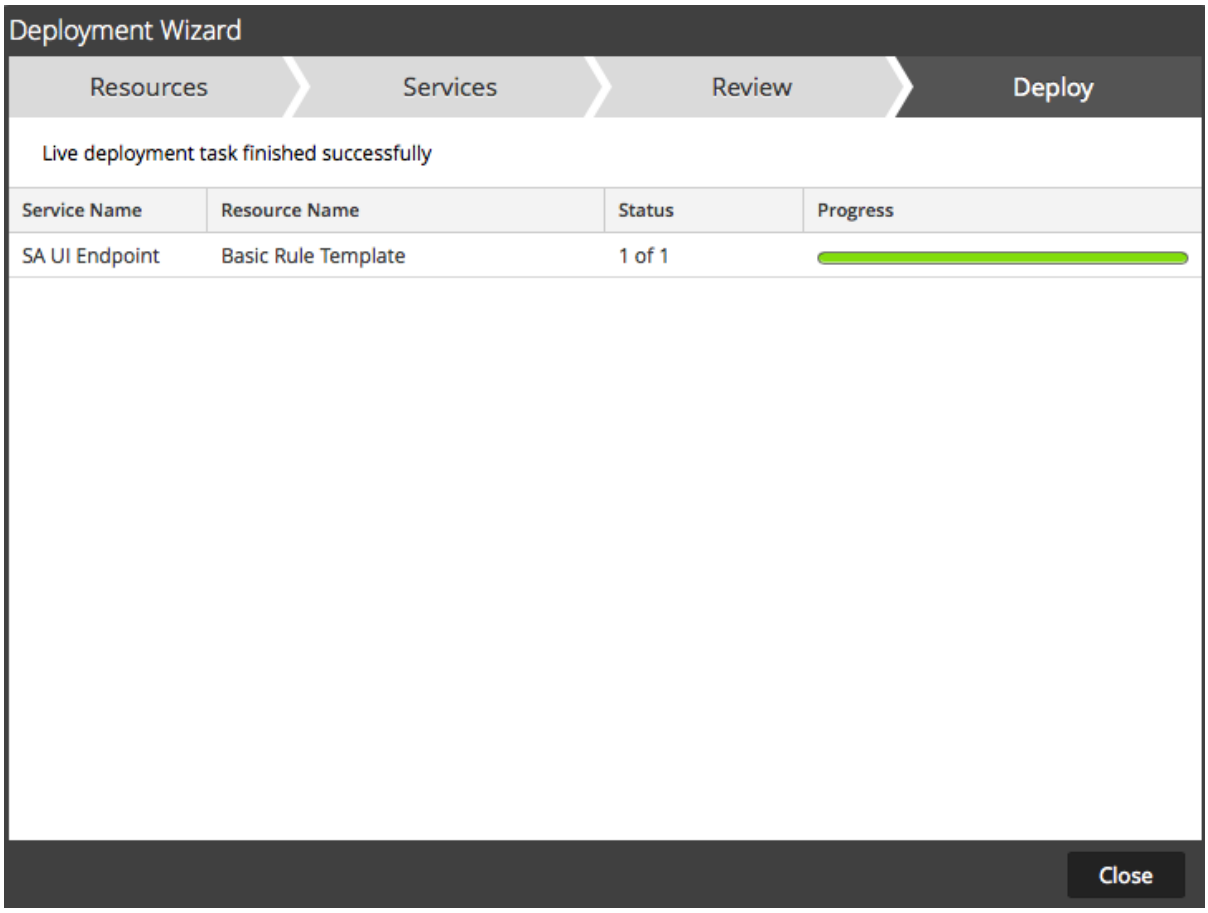
Élément	Description
Type de ressource	Affiche les types de ressources que vous avez sélectionnées (par exemple, **RSA Lua Parser**)
Boutons de commande	
Annuler	Annule le déploiement et quitte l'assistant.
Précédent	Affiche l'onglet précédent de l'assistant.
Déploiement	Lance le déploiement des ressources 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.

La figure suivante donne 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.
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	

Last Modified: August 10 2016, 9:33AM

Fermer	Quitte l'assistant.
Erreurs	Ne s'affiche que si Security Analytics a rencontré des erreurs. Cliquez pour afficher les erreurs.
Réessayer	Ne s'affiche que si Security Analytics a rencontré des erreurs. Cliquez sur ce bouton pour essayer de déployer les ressources à nouveau à l'aide de l'assistant.

Last Modified: August 10 2016, 9:33AM

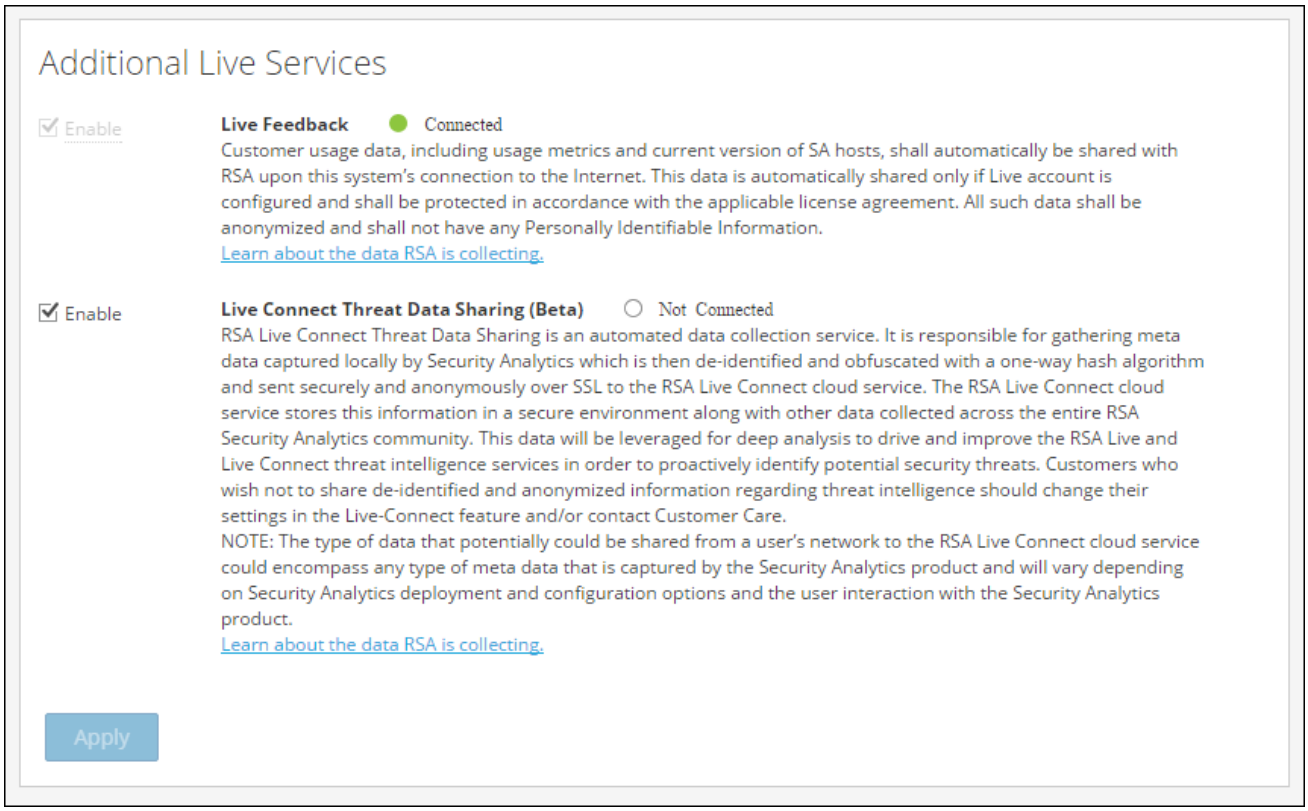
Security Analytics Feedback et Data Sharing

Cette rubrique présente les fonctionnalités Feedback et Data Sharing de Security Analytics.

Les paramètres de ces fonctionnalités sont disponibles sous Administration > Système > vue Services Live, dans la section Services Live supplémentaires.

Services Live supplémentaires

La participation aux Services Live supplémentaires est configurée sous Administration > Système > vue Services Live.



Live Feedback

Live Feedback a été conçu pour améliorer RSA Security Analytics.

Last Modified: August 10 2016, 9:33AM

Dès qu'un compte Live est configuré, les données d'utilisation sont partagées avec RSA. Ces données sont partagées conformément au contrat de licence applicable. Les données d'utilisation client, comprenant les metrics d'utilisation et la version actuelle des hôtes Security Analytics, sont automatiquement partagées avec RSA via la connexion de ce 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.

Live Connect Threat Data Sharing (bêta)

RSA LiveThreat Data Sharing RSA est un service de collecte de données automatisé. Son objectif est de partager, à des fins d'analyse, les données de renseignement sur les menaces pouvant toucher le service de Cloud RSA Live Connect. Toutes les métadonnées peuvent être collectées en fonction du déploiement, de la configuration, de l'activité réseau et de l'interaction des analystes avec Security Analytics.

Par défaut, le paramétrage de ce service est activé. Pour modifier le paramètre, accédez à Administration > Système > vue Services Live (ou contactez le Support Clients pour le désactiver).

Les métadonnées sont capturées localement par Security Analytics pour être envoyées de manière sécurisée et anonyme au service de Cloud RSA Live. Ce service stocke ces informations avec les données collectées auprès de toute la communauté RSA Security Analytics afin d'améliorer les services de renseignement sur les menaces RSA Live.

Note: 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.

Vue Configuration Live

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

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

- Dans le menu **Security Analytics**, sélectionnez **Live > Configurer.**
- À partir de n'importe quelle vue du module Live, sélectionnez **Configurer** dans la barre d'outils de Security Analytics.

Caractéristiques

La vue Configurer est dotée de fonctions réparties dans deux onglets :

- Onglet Déploiements
- Onglet Abonnements

Last Modified: August 10 2016, 9:33AM

Onglet Déploiements

Cette rubrique présente les fonctions de la vue Configuration Live > 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 Security Analytics se synchronise avec RSA Security Analytics 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 Security Analytics 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.

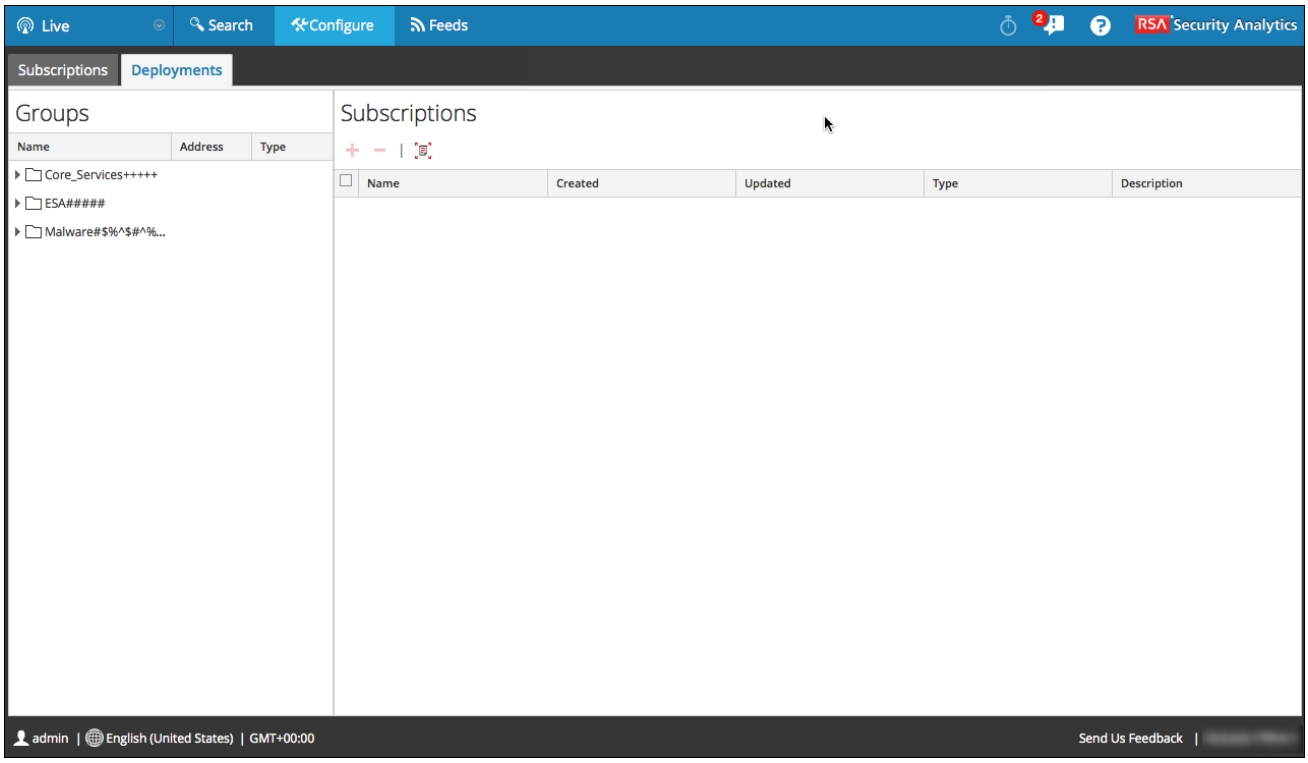
L'autorisation requise pour accéder à cette vue est **Gérer les ressources Live**.

Pour accéder à cette vue :

1. Dans le menu **Security Analytics**, sélectionnez **Live > Configurer**.
   L'onglet **Abonnements** est ouvert par défaut.
2. Cliquez sur l'onglet **Déploiements**.

Voici un exemple de l'onglet Déploiements.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

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.

Last Modified: August 10 2016, 9:33AM

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.
Créée	Il s'agit de la date et de l'heure de création de la ressource.
Updated	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 Security Analytics 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 Security Analytics 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 Security Analytics est abonné sont répertoriées dans cet onglet. Dans le panneau Abonnements, vous pouvez :

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

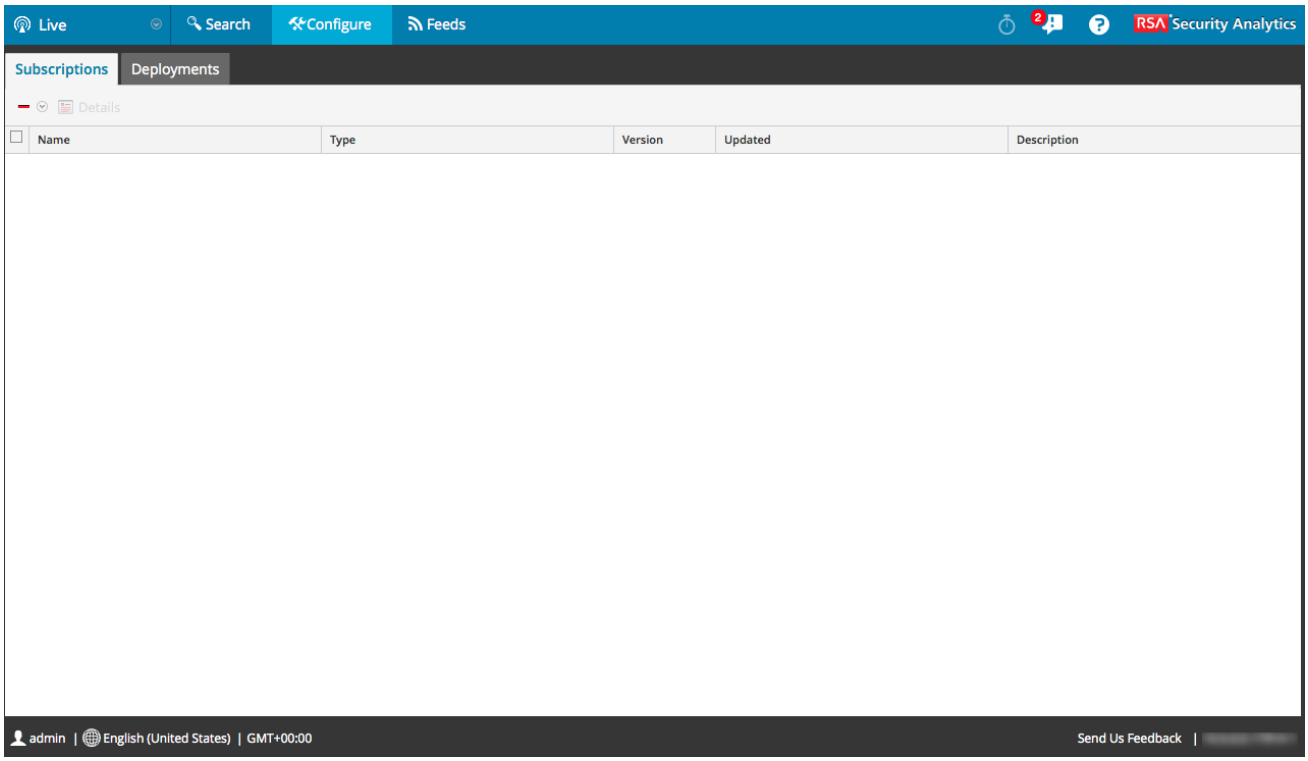
Note: L'abonnement à une ressource n'a pas pour effet de déployer cette ressource dans les services. Pour déployer une ou plusieurs ressources faisant l'objet d'un abonnement, accédez à l'onglet Déploiements. Pour déployer manuellement une ressource, utilisez l'option Déployer de la vue Ressource.

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

Pour accéder à cette vue :

- Dans le menu **Security Analytics**, sélectionnez **Live > Configurer.**
  L'onglet **Abonnements** est ouvert par défaut.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

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

Toolbar

Ce tableau décrit les options de la grille.

Fonction	Description
—	Supprime les abonnements sélectionnés.
Details	Affiche dans la vue Ressource le détail d'une ressource faisant l'objet d'un abonnement.

Grille

Ce tableau décrit les colonnes de la 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.
Updated	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.

Vue Feeds Live

La vue Feeds Live permet de :

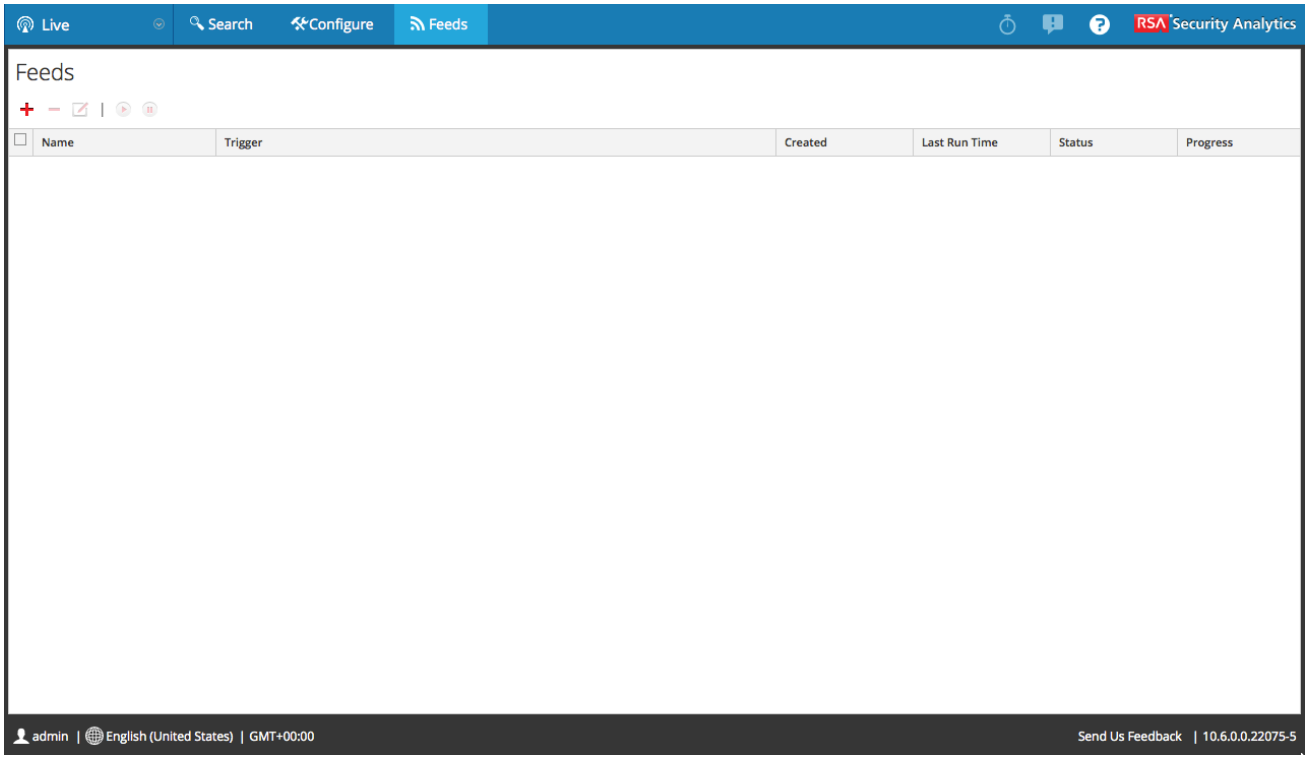
- Créer des feeds personnalisés.
- Créer des feeds d'identité.
- Modifier des feeds.

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

Voici un exemple de la vue Feeds.



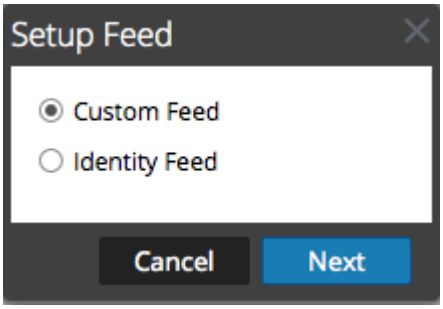
Last Modified: August 10 2016, 9:33AM

Caractéristiques

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

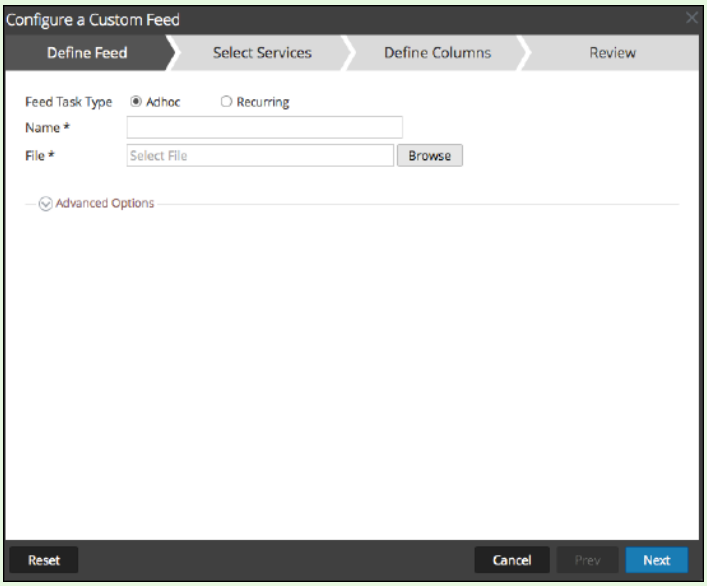
Toolbar

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

Fonction	Description
+	Lance la création d'un feed personnalisé ou d'un feed d'identité en affichant la boîte de dialogue **Configurer le feed**.  • Le feed personnalisé ouvre l'assistant **Configurer un feed personnalisé** (reportez-vous à la rubrique Créer un feed personnalisé). • Le feed d'identité ouvre l'assistant **Configurer Identity Feed** (reportez-vous à la rubrique Créer un feed d'identité).
−	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/reprend un feed de données.
	Arrête/suspend un feed de données.

Grille Feeds

Ce tableau décrit les colonnes de la grille.

Colonne	Description
	Sélectionne un feed.
Nom	Nom du feed. **Note:** Vous pouvez 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.
Créée	Date et heure de création du feed.
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.

Last Modified: August 10 2016, 9:33AM

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.

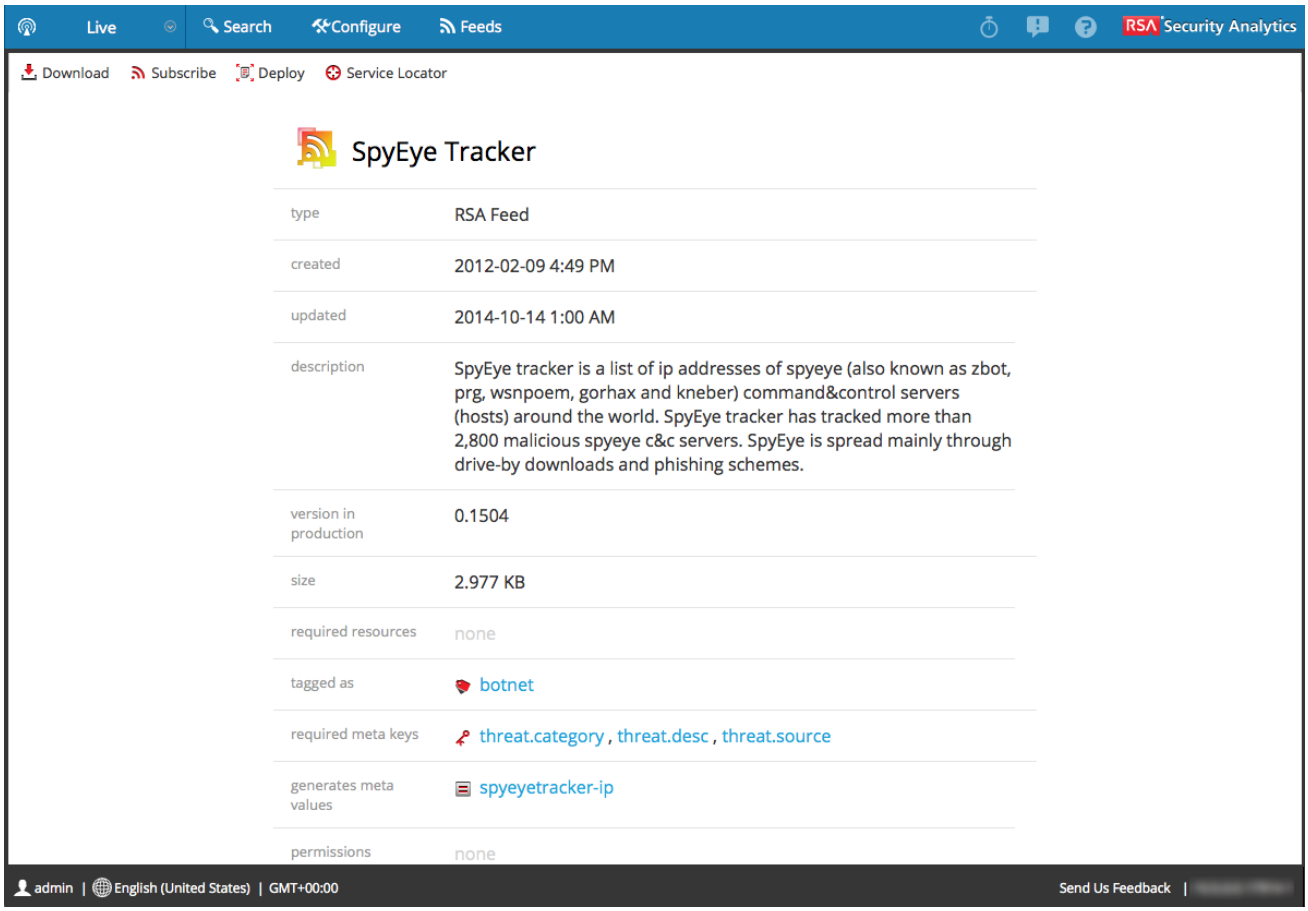
L'autorisation requise pour accéder à cette vue est Afficher les détails des ressources Live.

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

1. Dans le menu **Security Analytics**, sélectionnez **Live > Search > Types de ressourcess.**
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**.

Voici un exemple de la vue Ressource.

Last Modified: August 10 2016, 9:33AM



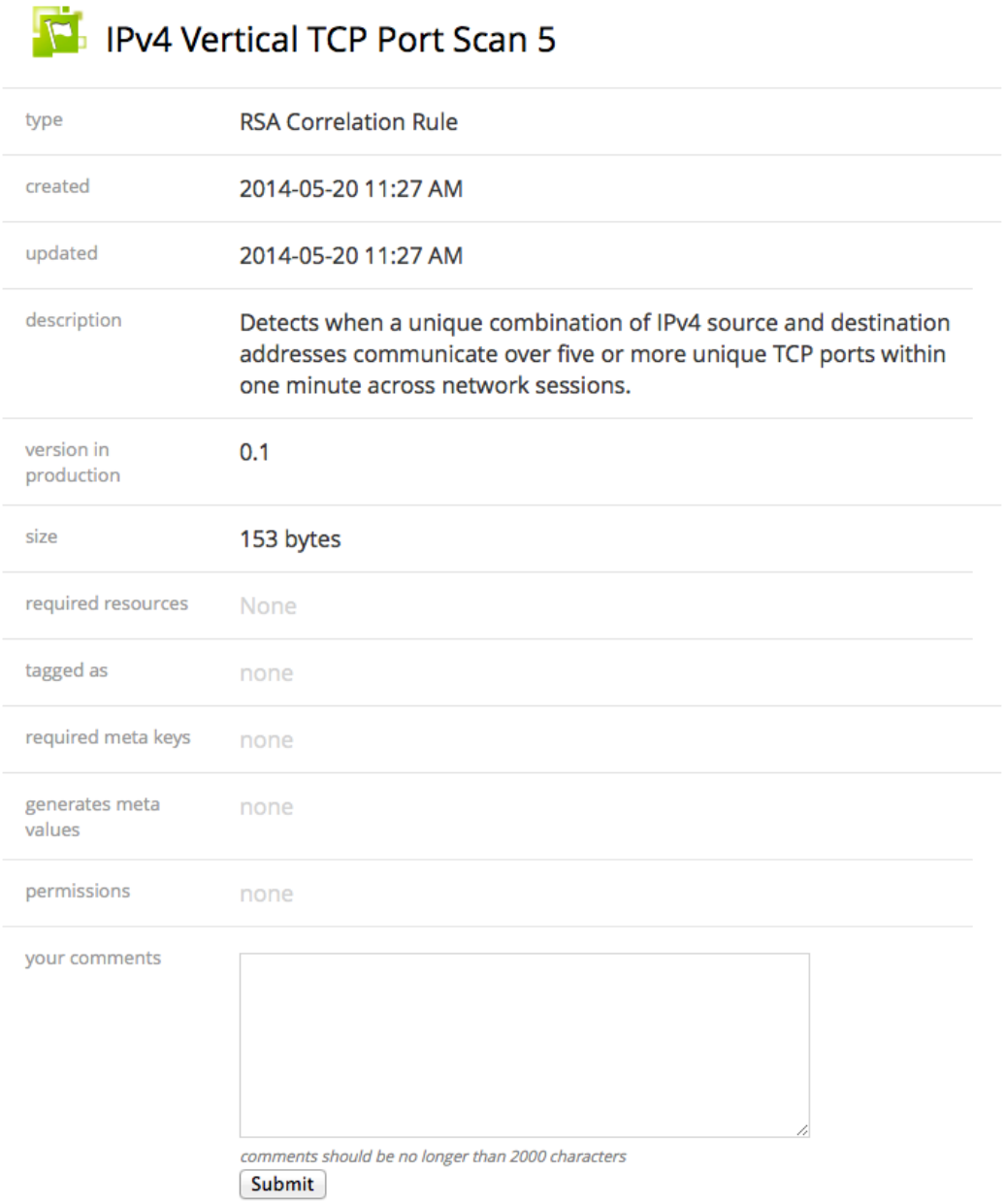
Caractéristiques

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

Détails de la ressource

Voici un exemple de détails de la ressource s'affichant dans la vue Ressource.

Last Modified: August 10 2016, 9:33AM



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

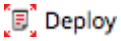
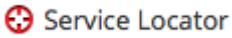
Fonction	Description
Icône Type de ressource	Représentation graphique du type de ressource, par exemple  .
Nom	Nom de la ressource, par exemple **fingerprint_office_lua**.

Fonction	Description
Type	Type de ressource, par exemple, **RSA Lua Parser**.
Créée	Date à laquelle la ressource a été créée, par exemple, **2013-09-15 02:16 PM**.
Updated	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, 2007 Word, 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	Étiquettes 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.
Génère des valeurs méta	Métavaleurs que la ressource génère. Dans l'exemple, il n'y a pas de métavaleurs générées. Cliquer sur une métavaleur permet d'ouvrir la vue Live Search avec la recherche restreinte pour obtenir une correspondance avec les ressources dotées de cette métavaleur.
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.

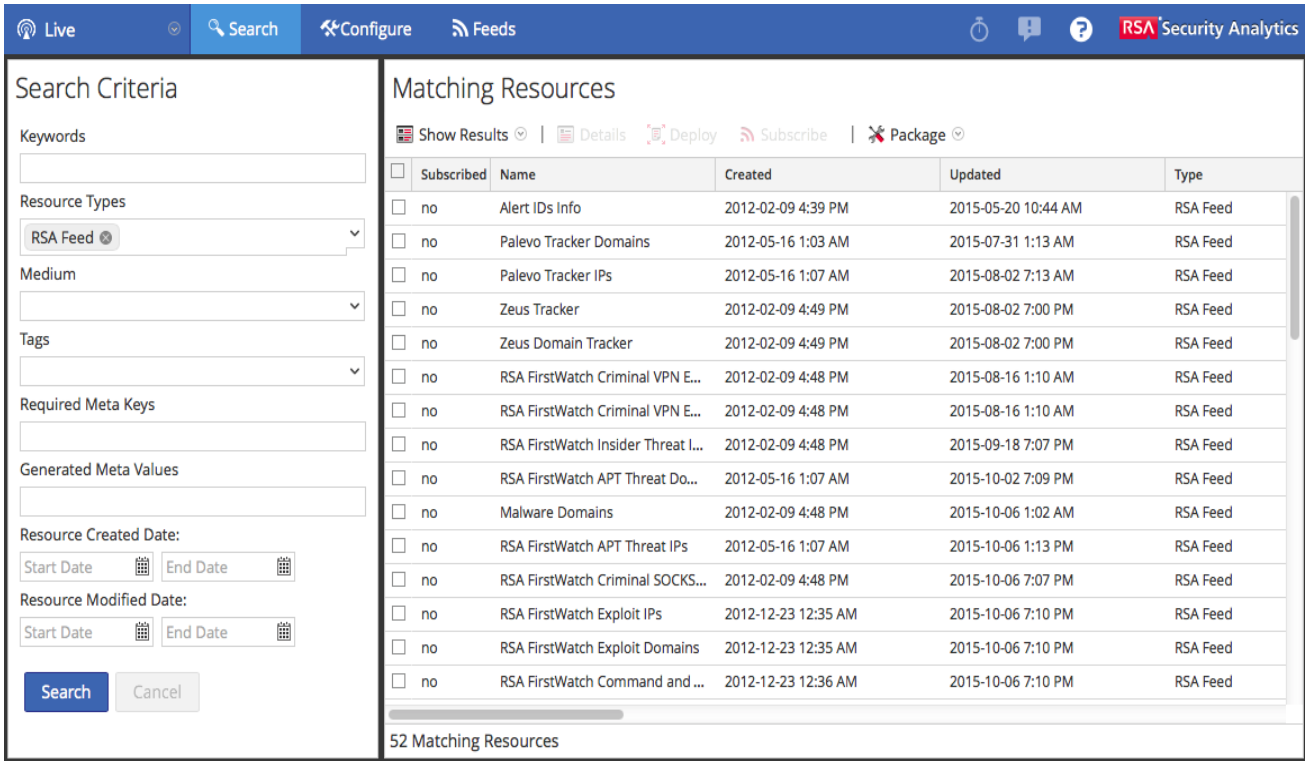
Fonction	Description
Download	Cette option télécharge la ressource actuellement affichée dans la vue Ressource.
Subscribe ou Unsubscribe	Cet option permet de s'abonner ou de se désabonner de la ressource actuellement affichée dans la vue Ressource.

Fonction	Description
	• 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.
	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.
	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.



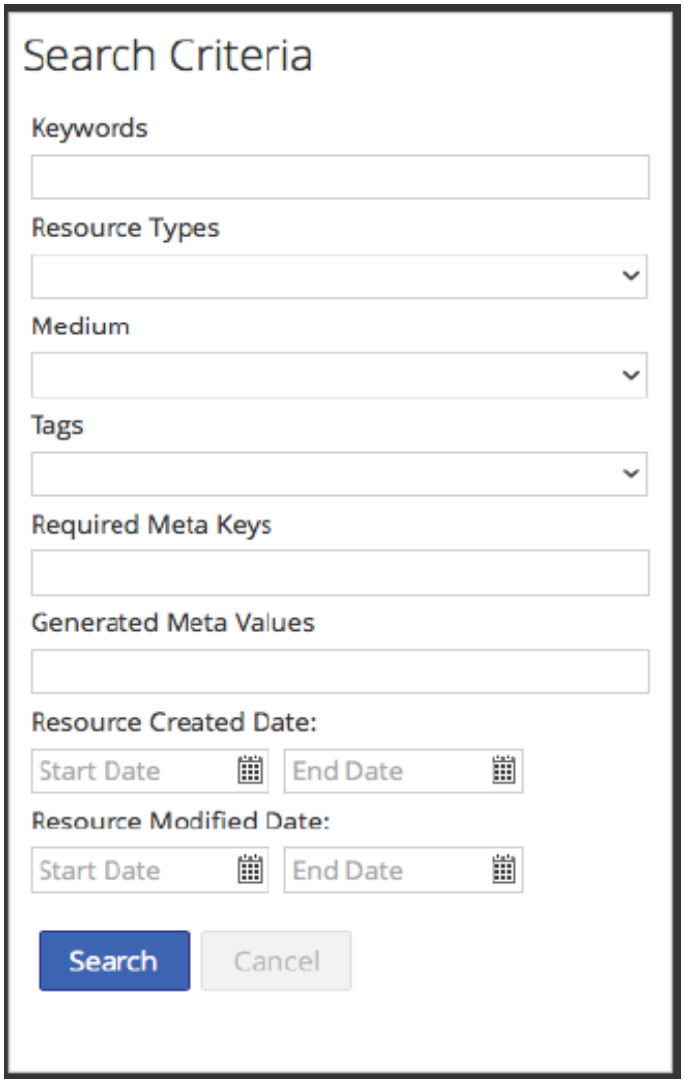
Caractéristiques

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.

Last Modified: August 10 2016, 9:33AM

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.
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)**

Last Modified: August 10 2016, 9:33AM

Fonction	Description
	• **Règle d'application RSA** • **Module CEP RSA** • **Contenu RSA** • **Règle de corrélation RSA** • **Règle RSA Event Stream Analysis** • **Feed RSA** • **RSA FlexParser** • **Action personnalisée RSA Investigator** • **RSA Log Collector** • **RSA Log Device** • **RSA Lua Parser** • **Règles RSA Malware** • **Clé méta RSA** • **Liste RSA Security Analytics** • **Rapport RSA Security Analytics** • **Règle RSA Security Analytics** • **Document source RSA**
(Pour version 10.5.1 ou ultérieure) **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
Mots clés	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.
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.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
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.

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.

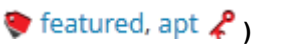
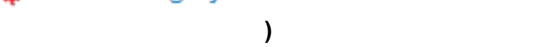
Résultats détaillés

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 **(par exemple**  **)**	Représentation graphique du type de ressource.

Last Modified: August 10 2016, 9:33AM

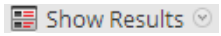
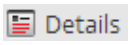
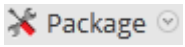
Fonction	Description
Nom	Nom de la ressource, par exemple **Gestion des groupes**.
Type	Type de ressource, par exemple, **Règle**.
Updated	Date à laquelle la ressource a été mise à jour pour la dernière fois, par exemple, **2013-09-15 4:27 PM**
Version	Version de la ressource, par exemple **0.1**.
Taille	Taille de la ressource, par exemple **135 Ko**.
Abonné	État de l'abonnement : **oui** = cette instance Security Analytics est abonnée à cette ressource de contenu. **non** = cette instance Security Analytics n'est pas abonnée à cette ressource de contenu.
Description	Description de la ressource, par exemple **Gestion des groupes de règles**.
Balises **(par exemple,**  **)**	Étiquettes qui s'appliquent à la ressource. Cliquer sur une balise permet de restreindre la recherche aux ressources avec balise.
Clés méta **(par exemple,**  **)**	Clés méta qui s'appliquent à la ressource. Cliquer sur une clé méta permet de restreindre la recherche à cette clé méta.
Valeurs méta de ressource **(par exemple,**  **)**	Valeurs méta générées par la ressource. Cliquer sur une métavaleur permet de restreindre la recherche aux ressources qui ont généré la métavaleur.

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.

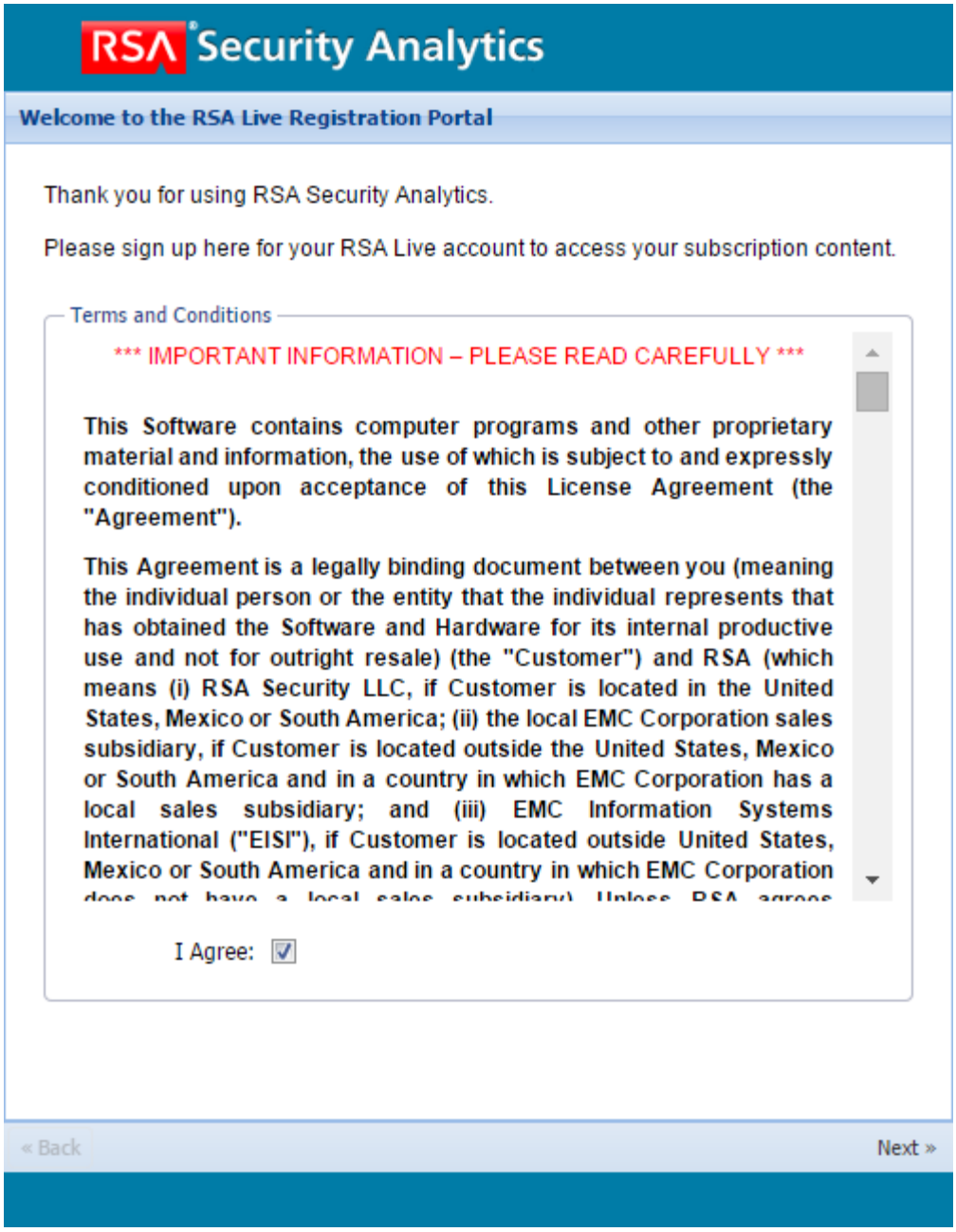
Fonction	Description
Abonné	État de l'abonnement : **oui** = cette instance Security Analytics est abonnée à cette ressource de contenu. **non** = cette instance Security Analytics n'est pas abonnée à cette ressource de contenu.
Nom	Nom de la ressource, par exemple, **Réputation adresse IP RSA FirstWatch**.

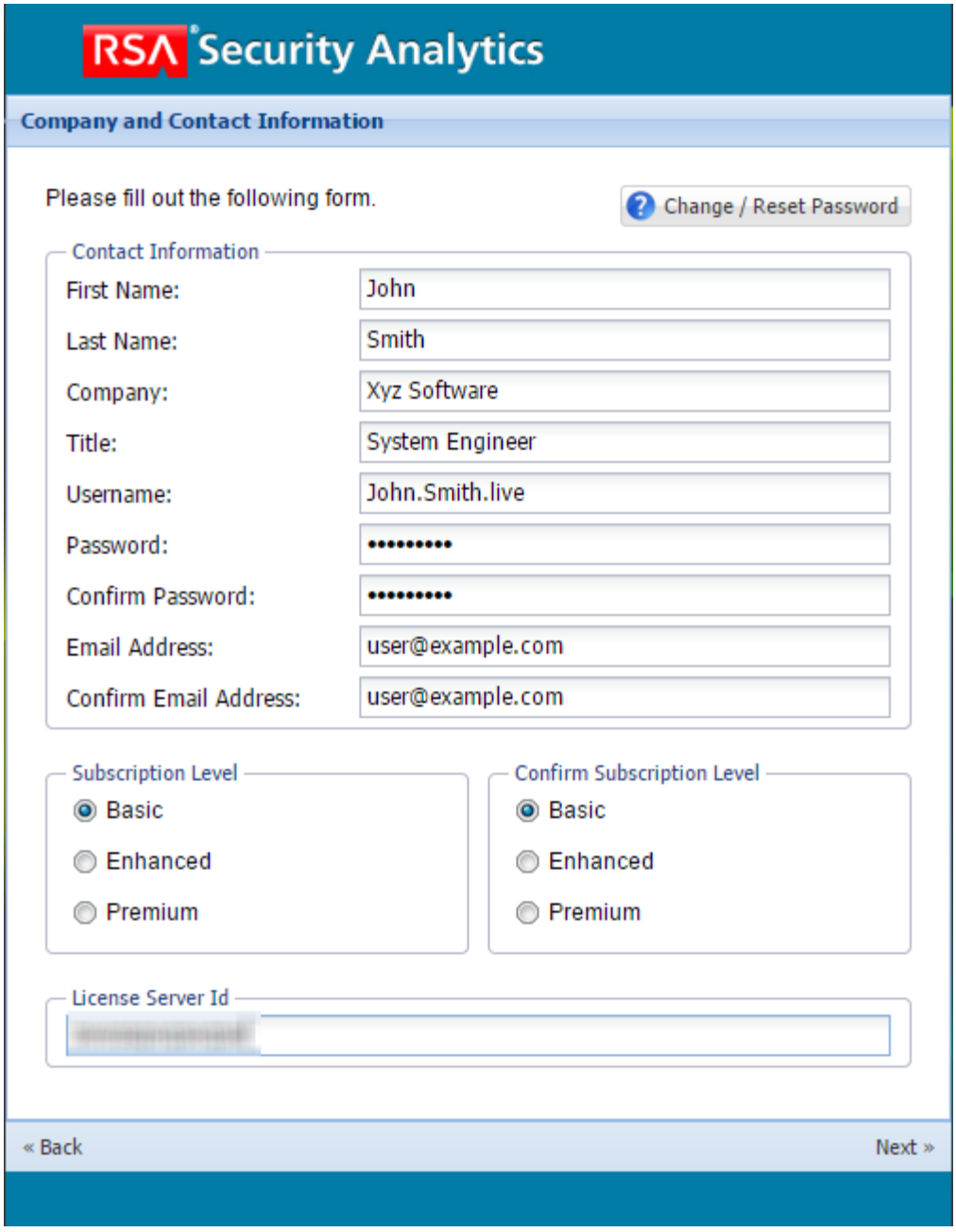
Fonction	Description
Créée	Date à laquelle la ressource a été créée, par exemple, **2013-09-15 4:27 PM**.
Updated	Date à laquelle la ressource a été mise à jour pour la dernière fois, par exemple, **2013-09-15 4:27 PM**
Type	Type de ressource, par exemple, **FEED**.
Description	Description de la ressource, par exemple, **Ce feed contient des adresses IP connues à associer aux APT.**
	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. Cliquer sur **Déployer** permet d'ouvrir l'assistant Déploiement.
	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.
	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.

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 librairie RSA Live. Pour accéder au portail, saisissez l'URL suivante : https://cms.netwitness.com/registration/.

Last Modified: August 10 2016, 9:33AM





Caractéristiques

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.
Intitulé	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.
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 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	• 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.
ID de serveur de licences	ID de licence figurant sur la page **Administration > Système > Informations**. **Caution:** Dans Security Analytics, l'ID de serveur de licences doit être valide et être enregistré sur le serveur Flexera. Si ce n'est pas le cas, contactez le Support Clients de RSA.

Assistant Déploiement du package de la ressource

Dans l'assistant Déploiement du package de la ressource, vous pouvez déployer un package de contenu créé dans Security Analytics Live vers un ou plusieurs services. Security Analytics accepte les packages au format **.nwp** ou **.zip**.

Note: Utilisez Security Analytics Live pour créer des packages de ressources ; il s'agit d'une application distincte qui ne fait pas partie de Security Analytics. 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 Security Analytics (.nwp).

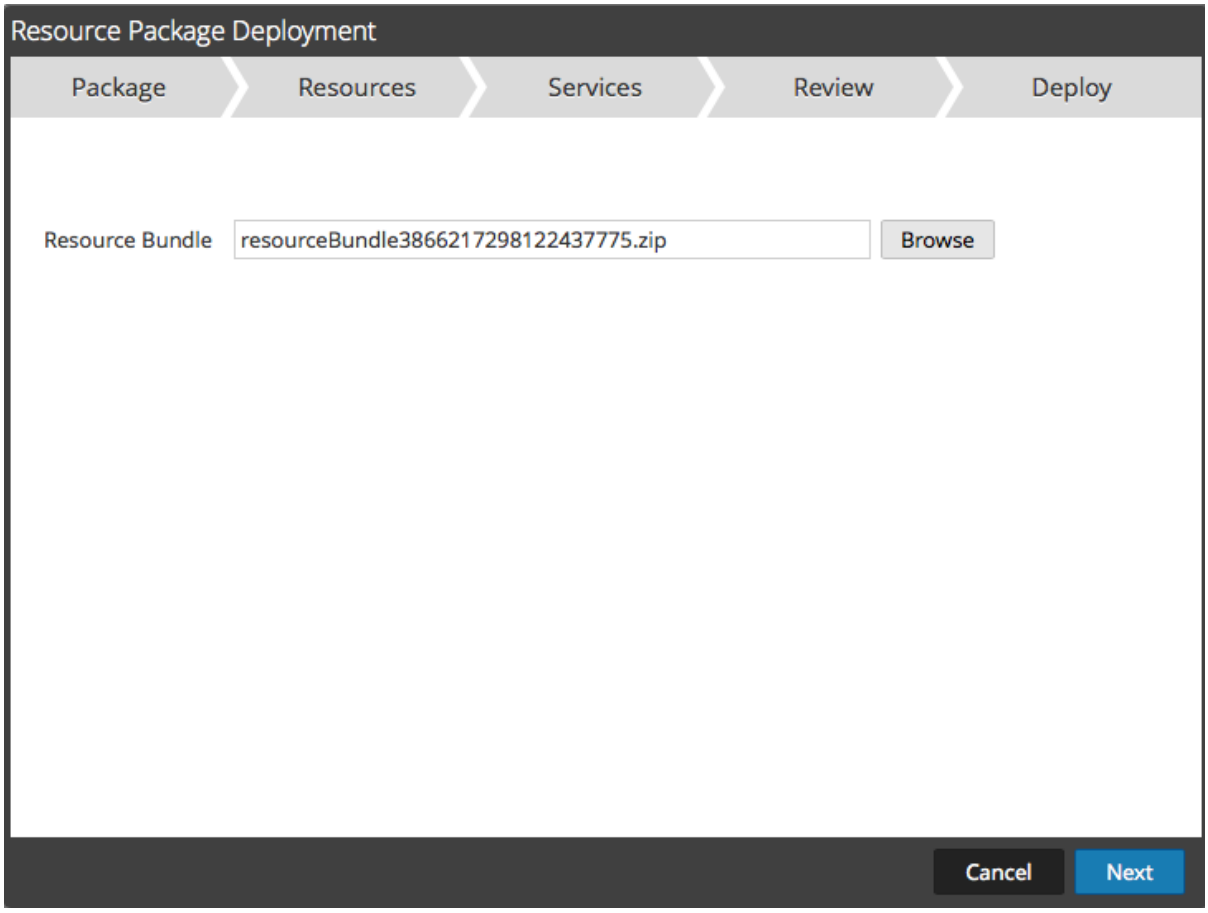
L'autorisation requise pour accéder à cette vue est **Déployer les ressources Live**.

Pour accéder à cette vue :

1. Dans le menu **Security Analytics**, sélectionnez **Live > Recherche.**
2. Dans la barre d'outils **Recherche Live - Ressources correspondantes**, sélectionnez **Package** > **Déploiement.**

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

Last Modified: August 10 2016, 9:33AM



Caractéristiques

L'assistant Déploiement de package de la ressource contient cinq onglets :

- Onglet Package
- Onglet Ressources
- Onglet Services
- Onglet Révision
- Onglet Déploiement

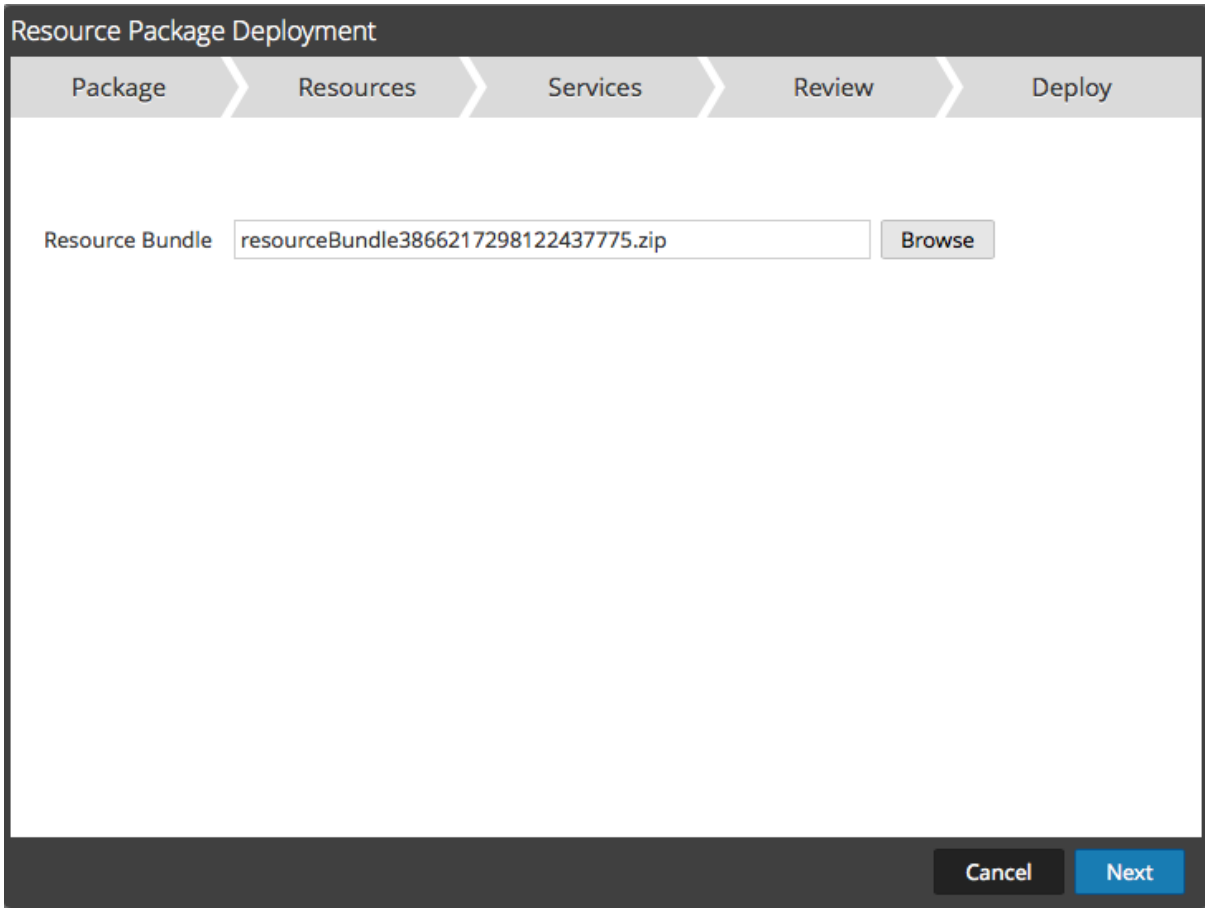
Lorsque vous avez fini de suivre les étapes de l'assistant, Security Analytics retourne à la vue Ressources Live.

Onglet Package

Sur cette page, vous sélectionnez un package de ressources de votre réseau.

Voici un exemple de l'onglet Package.

Last Modified: August 10 2016, 9:33AM



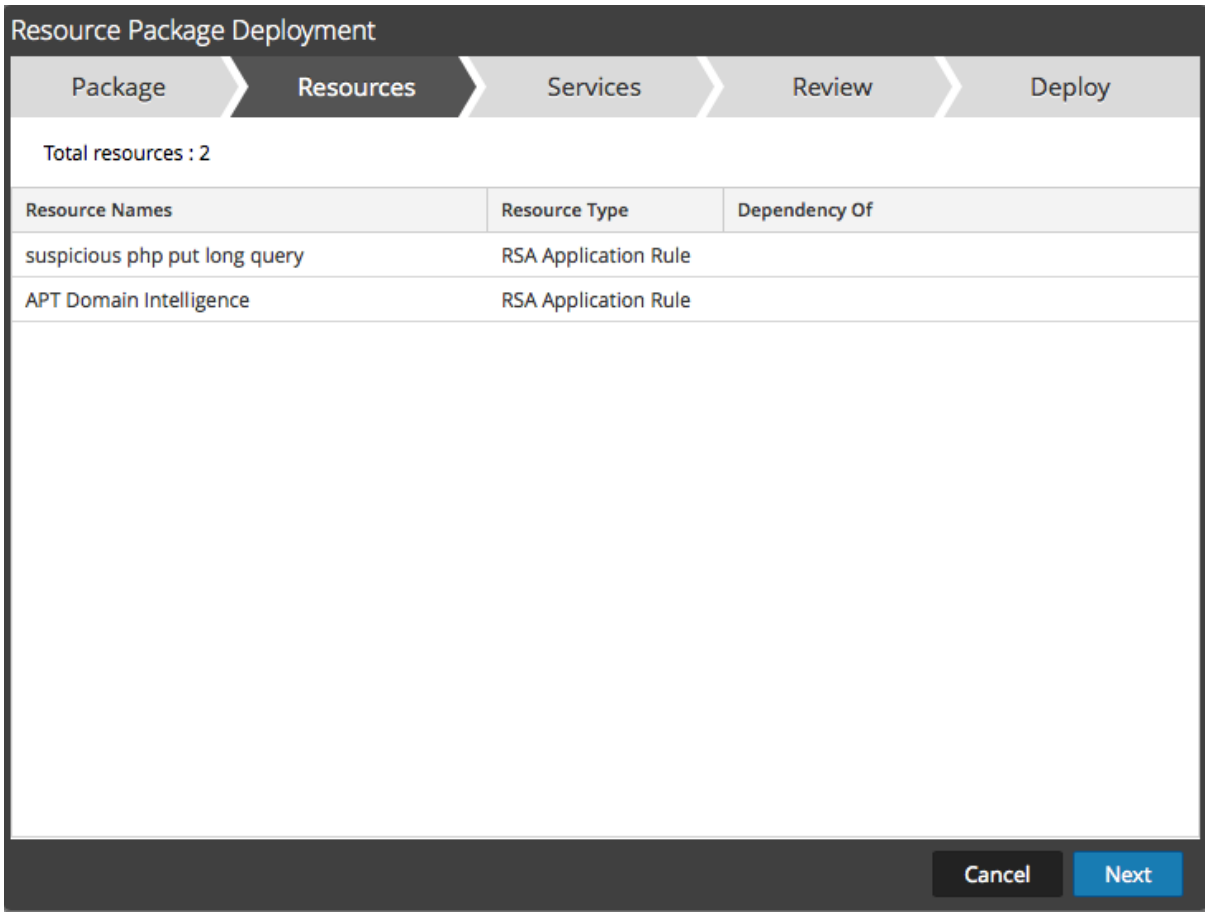
Le tableau suivant décrit les éléments de l'onglet Package.

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 répertorie les ressources du package.

Voici un exemple de l'onglet Ressources.



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

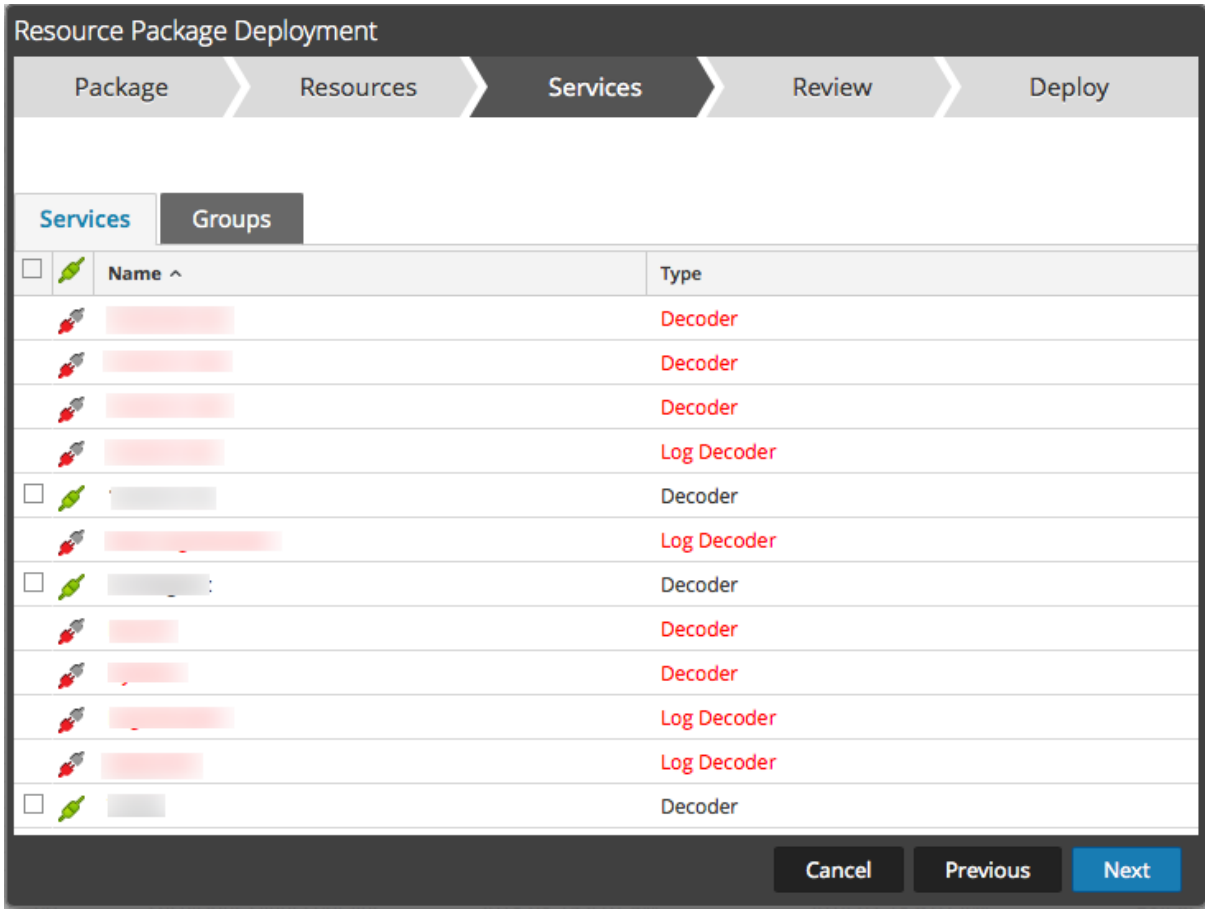
Colonne	Description
Nom de ressource	Affiche le nom des ressources du package.
Type de ressource	Affiche les types des ressources du package.
Dépendance de	Affiche les ressources desquelles dépendent les ressources du package.
Boutons de commande	
Annuler	Annule le déploiement et ferme l'assistant.
Précédent	Affiche l'onglet précédent de l'assistant.
Suivant	Affiche l'onglet suivant de l'assistant.

Onglet Services

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

L'onglet Services contient deux onglets, Services et Groupes, qui répertorient les services et groupes de services configurés dans la vue Administration > 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.

Voici un exemple de l'onglet Services.



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

Élément	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.

Last Modified: August 10 2016, 9:33AM

Élément	Description
Nom	Affiche les services de votre environnement au niveau desquels vous pouvez déployer le contenu.
Type	Affiche le type de service Security Analytics.
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.
Boutons de commande	
Annuler	Annule le déploiement et ferme l'assistant.
Précédent	Affiche l'onglet précédent de l'assistant.
Suivant	Affiche l'onglet suivant de l'assistant.

Onglet Révision

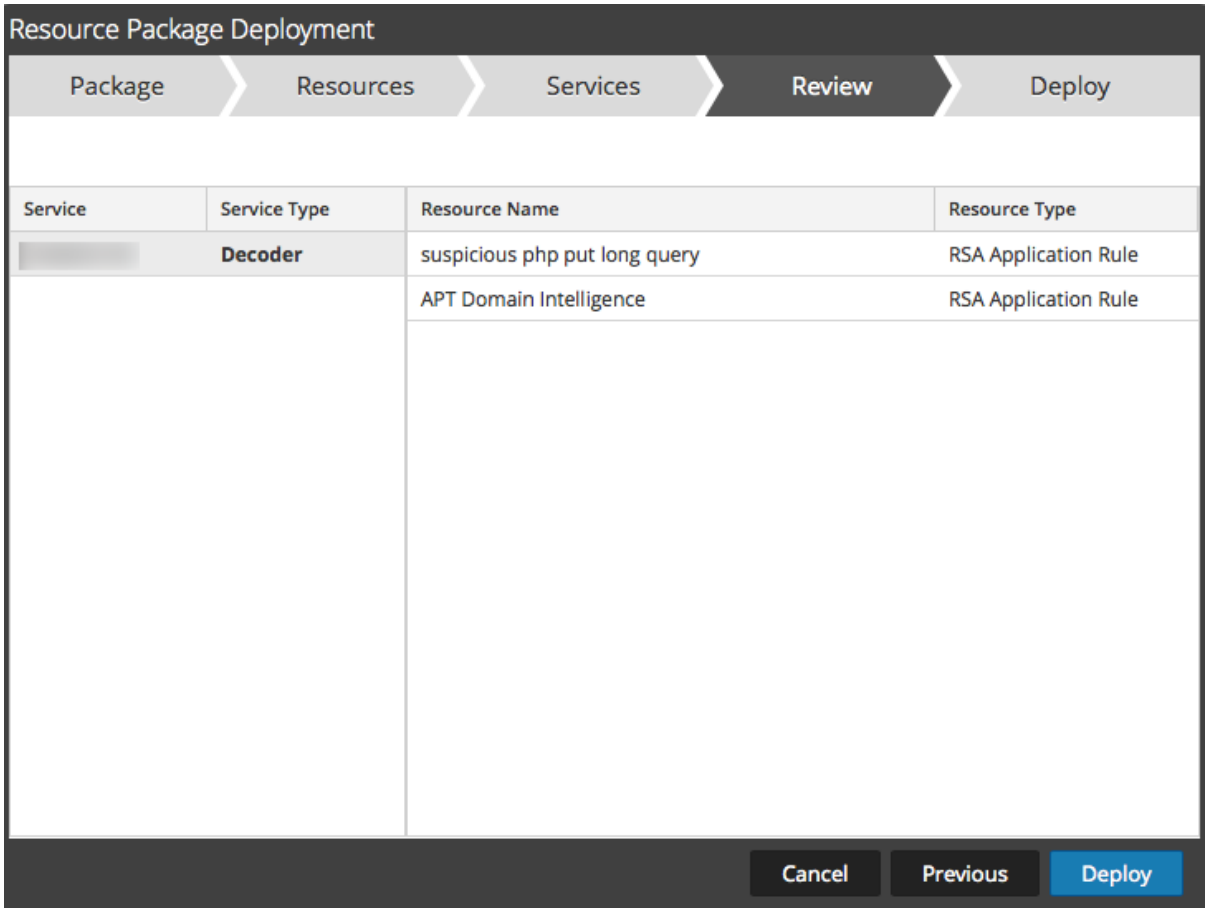
Affiche les ressources et les services sur lesquels les ressources seront déployées.

Sous cet onglet, vous pouvez :

1. Passer en revue le contenu et les services sur lesquels les ressources seront déployées.
2. Lancez le déploiement des ressources.

Voici un exemple de l'onglet Révision.

Last Modified: August 10 2016, 9:33AM



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

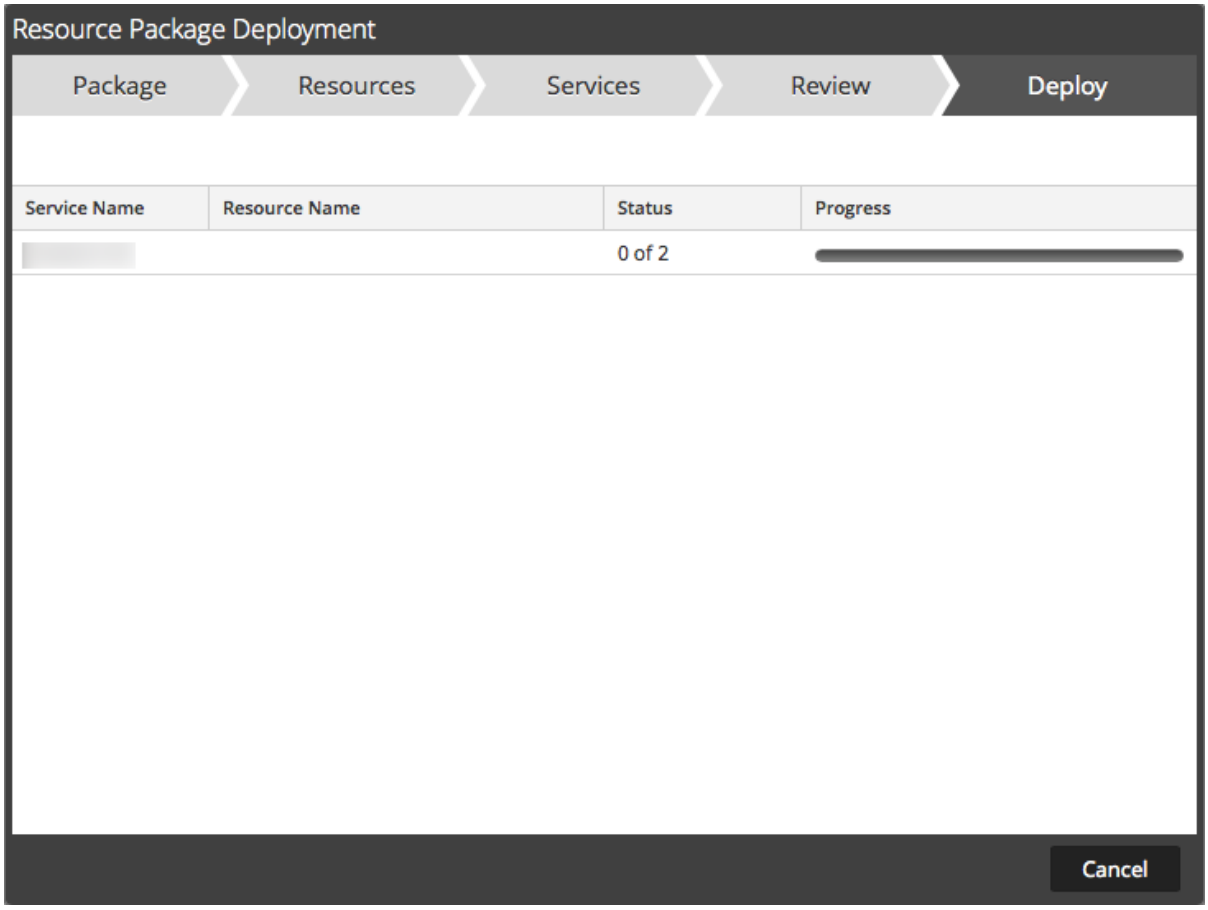
Élément	Description
Services	
	Permet de sélectionner les services au niveau desquels vous souhaitez déployer le contenu. Vous pouvez sélectionner une combinaison de services et de groupes de services.
Nom	Affiche les services de votre environnement au niveau desquels vous pouvez déployer le contenu.
Type	Affiche le type de service Security Analytics (type d'hôte/de service).
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.
Boutons de commande	

Élément	Description
Annuler	Annule le déploiement et ferme l'assistant.
Précédent	Affiche l'onglet précédent de l'assistant.
Suivant	Affiche l'onglet suivant de l'assistant.

Déploiement

Sous l'onglet Déploiement, vous pouvez déployer le package de ressources vers les services ou groupes de services sélectionnés, afficher la progression de la tâche et annuler la tâche.

Voici 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.

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 Security Analytics a rencontré des erreurs. Cliquez pour afficher les erreurs.
Réessayer	S'affiche uniquement si Security Analytics a rencontré des erreurs. Cliquez sur ce bouton pour essayer de déployer les ressources à nouveau à l'aide de l'assistant.

Last Modified: August 10 2016, 9:33AM