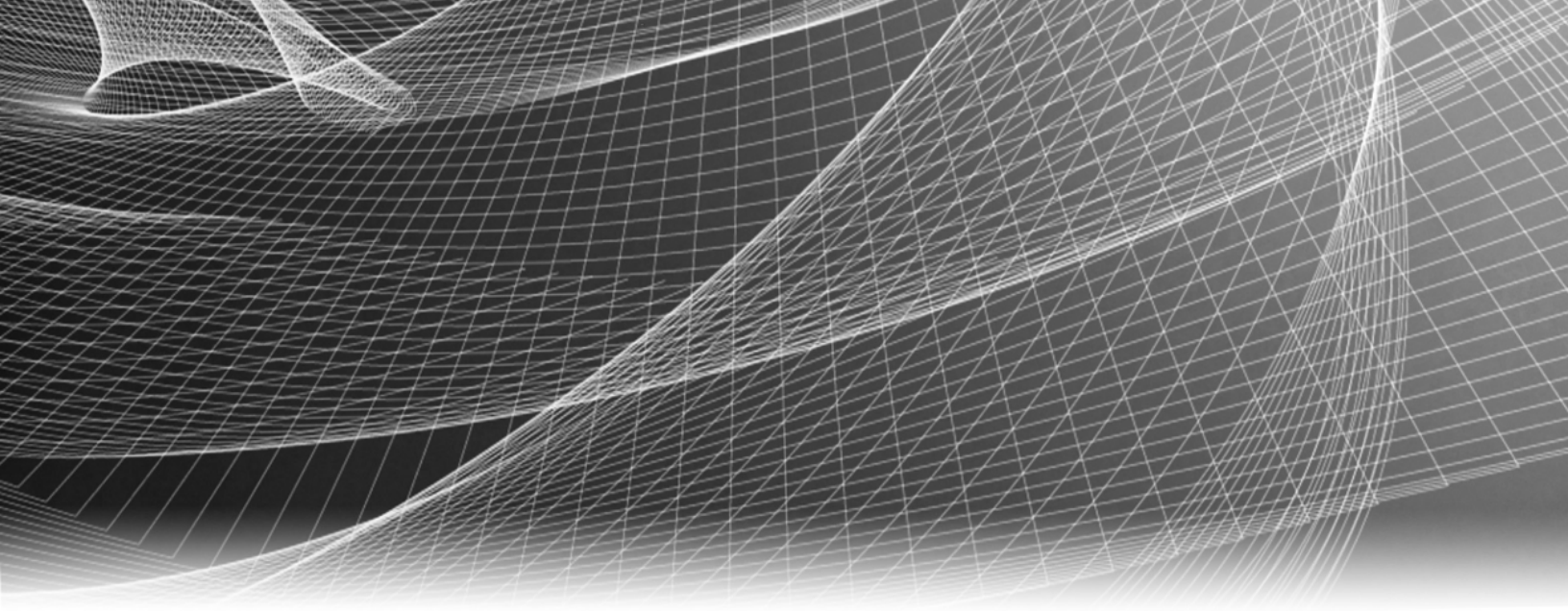


RSA Security Analytics

Guide de mise en route des hôtes et des services 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.

Guide de mise en route des hôtes et des services

RSA

Guide de mise en route des hôtes et des services

Ce guide indique aux administrateurs les procédures standard d'ajout et de configuration d'hôtes (appliances) et de services dans Security Analytics. Après une présentation de l'objectif de base des hôtes et services et de leur fonctionnement dans le réseau Security Analytics, ce guide décrit :

- Tâches minimales que vous devez effectuer pour configurer les hôtes et services dans votre réseau.
- Procédures supplémentaires que vous devez exécuter en fonction des besoins opérationnels quotidiens et à long termes de votre entreprise
- Rubriques de référence décrivant l'interface utilisateur.

Last Modified: August 10 2016, 9:33AM

Les bases

L'hôte est la machine sur laquelle un service s'exécute. Ce peut être une machine physique ou virtuelle.

Un service exécute une fonction spécifique, par exemple la collecte des logs ou l'archivage des données. Chaque service s'exécute sur un port dédié et se présente comme un plug-in à activer ou désactiver selon la fonction de l'hôte.

Vous devez commencer par configurer les services de base suivants :

- Decoder
- Concentrator
- Broker
- Log Decoder

Tous les services sont répertoriés ci-dessous et chaque service, excepté le Log Collector, a son propre guide ou partage un des Guides de configuration de l'hôte et des services. Le Log Collector a son propre ensemble de guides de configuration pour gérer la configuration de tous les protocoles de collecte d'événements pris en charge.

- Archiver
- Broker
- Concentrator
- Decoder
- Event Stream Analysis
- Context Hub
- Incident Management
- IPDB Extractor
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Warehouse Connector
- Workbench

Vous devez configurer les hôtes et les services pour qu'ils communiquent avec le réseau et entre eux afin d'exécuter leurs fonctions, par exemple le stockage ou la capture des données.

Last Modified: August 10 2016, 9:33AM

Maintenance des hôtes

Utilisez la vue Hôtes pour effectuer des ajouts, des modifications, des suppressions et d'autres tâches de maintenance pour les hôtes présents dans votre déploiement. Reportez-vous à la section :

- Procédures de configuration des hôtes - tâches minimales à effectuer pour configurer un hôte dans Security Analytics.
- Procédures de maintenance des hôtes - tâches de maintenance des hôtes à effectuer dans la vue Hôtes.
- Procédures relatives aux hôtes dans la boîte de dialogue Liste des tâches - tâches relatives aux hôtes et à leurs communications avec le réseau que vous effectuez dans la boîte de dialogue Liste des tâches.

Après avoir exécuté l'implémentation initiale de Security Analytics, la tâche principale à effectuer dans la vue Hôtes est la mise à jour de votre déploiement Security Analytics vers une nouvelle version.

Mettre à jour la convention de dénomination des versions

Utilisez la vue Hôtes pour appliquer les dernières mises à jour de la version depuis votre référentiel de mise à jour local (reportez-vous à la rubrique Gérer les mises à jour Security Analytics pour plus d'informations sur votre référentiel de mises à jour local). Vous devez comprendre la convention de dénomination des versions de mise à jour pour savoir quelle version appliquer à l'hôte. La convention de dénomination à appliquer est ***version-majeure.version-mineure.pack-service.correctif***. Par exemple, si vous choisissez la version 10.6.1.2, vous appliquerez la version suivante à l'hôte.

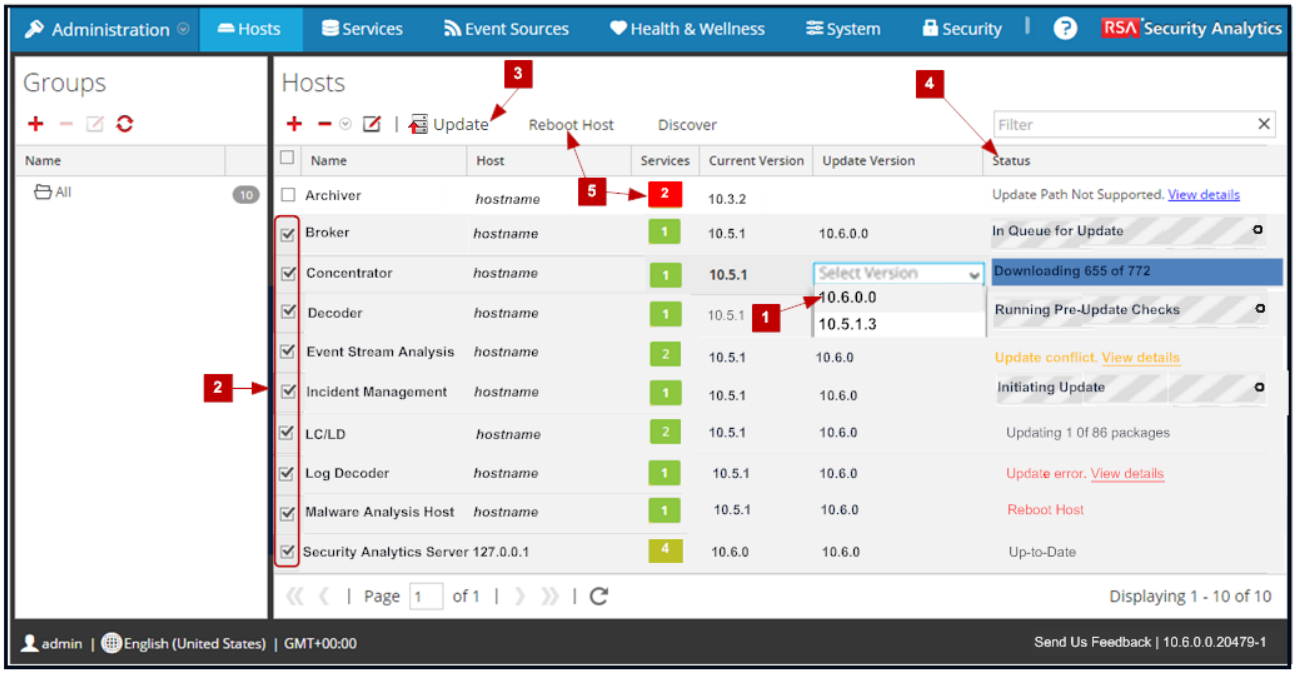
- 10 = version majeure
- 6 = version mineure
- 1 = pack service
- 2 = correctif

Mise à jour de la version d'un hôte

Pour mettre à jour un hôte vers une nouvelle version, utilisez la vue Hôtes. L'exemple ci-dessous illustre la procédure à suivre. Lorsque des mises à jour de version sont disponibles pour un hôte, Mise à jour disponible s'affiche dans la colonne **État** et vous pouvez choisir la mise à jour dans la colonne **Sélectionner la version**. Pour obtenir d'autres instructions sur la procédure à suivre pour appliquer une nouvelle mise à jour de version à un hôte, reportez-vous à Appliquer les mises à jour.

Note: Si vous ne trouvez pas une version, vous devrez peut-être renseigner votre référentiel de mises à jour local.

Last Modified: August 10 2016, 9:33AM



1	Sélectionnez la version dans la colonne **Mettre à jour la version**. • Si vous ne disposez pas d'un espace disque suffisant dans votre référentiel de mises à jour local pour télécharger une mise à jour de version, la boîte de dialogue **Gestion de l'espace du référentiel** s'affiche et indique le contenu et l'état de l'espace disque du référentiel (reportez-vous à la rubrique Libérer de l'espace disque dans le référentiel de mises à jour local pour obtenir plus d'instructions sur la manière de libérer de l'espace disque). Vous pouvez supprimer une ou plusieurs versions inutiles pour libérer suffisamment d'espace disque pour pouvoir télécharger la version voulue. (Reportez-vous à Résolution des avertissements, conflits et erreurs de mise à jour et pré-mise à jour). **Note:** Vous pouvez aussi mettre à jour vers la dernière version mineure ou un correctif.
2	Sélectionnez l'hôte ou les hôtes que vous souhaitez mettre à jour. • L'hôte du serveur Security Analytics (SA) doit être mis à jour vers la dernière version dans votre déploiement pour que vous puissiez appliquer cette version à un autre hôte. • Si vous sélectionnez plusieurs hôtes à mettre à jour, Security Analytics commence par mettre à jour l'hôte du serveur SA. • Dans votre déploiement, si vous tentez de mettre à jour un ou plusieurs hôtes autres que l'hôte du serveur SA vers la dernière version avant l'hôte du serveur SA, SA ne vous y autorise pas. • Si un hôte a actuellement une version qui n'est pas un chemin de mise à jour valide, Security Analytics vous indique de contacter le Support Clients pour plus d'instructions sur la manière de mettre à jour l'hôte vers un chemin valide. **Note:** Si vous rencontrez des conflits lors de la mise à jour des hôtes de serveur non SA, l'hôte du serveur SA demeure grisé jusqu'à ce que les autres conflits d'hôte soient résolus.
3	Cliquez sur **Mettre à jour** pour démarrer le processus de mise à jour.

Last Modified: August 10 2016, 9:33AM

4	Surveillez la progression de la mise à jour dans la colonne **État**. Lors du processus de mise à jour, Security Analytics : 1. Télécharge le package de mise à jour pour la version sélectionnée si ce package n'existe pas dans votre référentiel de mises à jour local. 2. Si vous sélectionnez plusieurs hôtes à mettre à jour, affiche **Dans la file d'attente pour la mise à jour** lorsqu'il applique la version à chaque hôte. 3. Affiche **Exécution des vérifications pré-mise à jour** lorsqu'il valide la configuration de votre version actuelle. • Affiche **Avertissement de mise à jour. Afficher les détails** en cas de problème dans votre configuration existante qui ne vous empêche pas d'effectuer la mise à jour vers la nouvelle version. • Affiche **Conflit de mise à jour. Afficher les détails** en cas de conflit dans votre configuration existante qui vous empêche d'effectuer la mise à jour vers la nouvelle version. Reportez-vous à Résolution des avertissements, conflits et erreurs de mise à jour et pré-mise à jour pour plus d'instructions sur la manière de résoudre ces avertissements et conflits de configuration. 4. Lance la mise à jour en l'absence de conflit. 5. Applique chaque package pour la version de mise à jour sélectionnée. 6. Surveille la mise à jour. Si une erreur se produit et bloque la mise à jour, Security Analytics affiche **Erreur de mise à jour. Afficher les détails.** Reportez-vous à Résolution des avertissements, conflits et erreurs de mise à jour et pré-mise à jour pour plus d'instructions sur la manière de résoudre ces erreurs. 7. Vous invite à **redémarrer l'hôte** après la mise à jour de l'hôte.
5	Cliquez sur **Redémarrer l'hôte**. • Lorsque vous mettez à jour plusieurs hôtes et que chaque hôte a été mis à jour et s'exécute, Security Analytics affiche **À jour**. • Si l'hôte est mis à jour, mais que tous les services ne sont pas redémarrés après le redémarrage, Security Analytics affiche les services en rouge. La mise en ligne des services peut prendre plusieurs minutes. Contactez le support Clients si l'hôte ne revient pas en ligne.

Déploiement de plusieurs versions

Security Analytics prend en charge plusieurs versions dans votre déploiement. L'hôte du serveur Security Analytics (SA) est mis à jour en premier et tous les autres hôtes doivent avoir une version identique ou antérieure à celle du serveur SA.

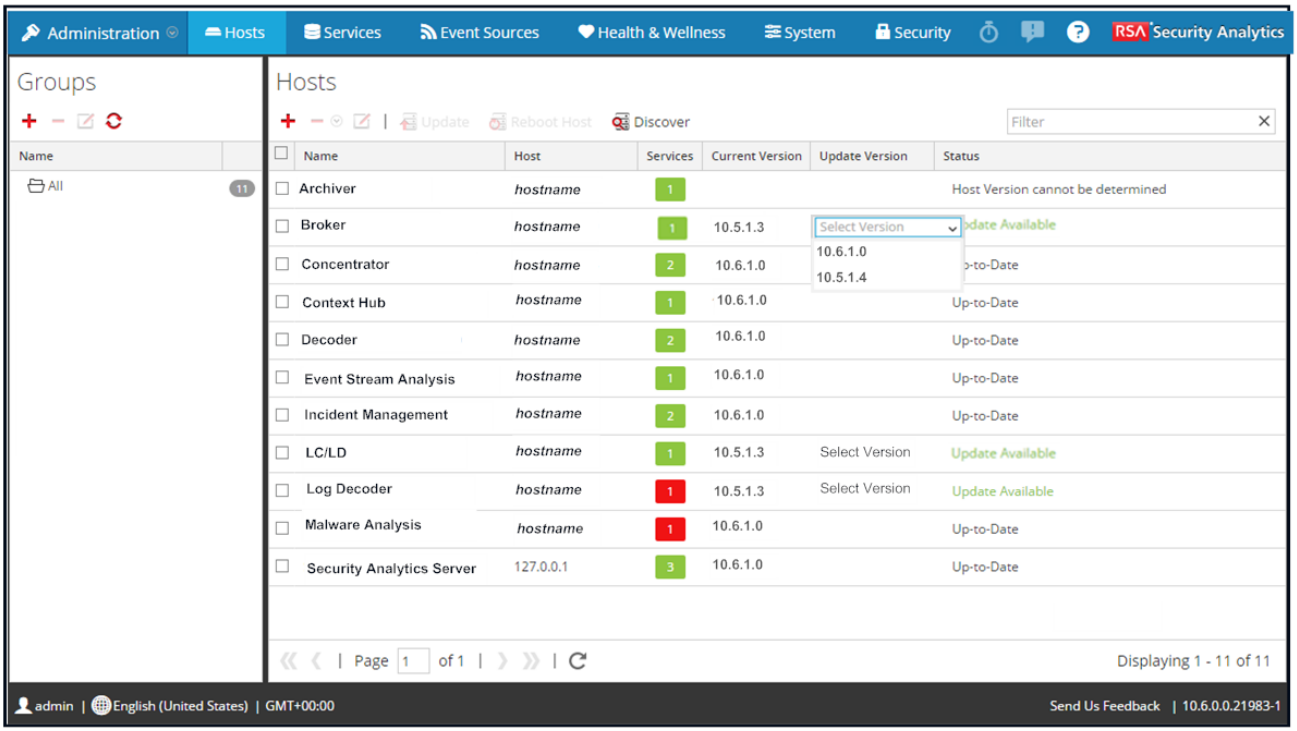
Note: La vue Hôtes permet de s'assurer que l'hôte du serveur SA est mis à jour en premier et que tous les autres hôtes ont une version identique ou antérieure à celle de l'hôte du serveur SA.

Dans l'exemple suivant de déploiement contenant plusieurs versions.

- Les mises à jour de version actuellement disponibles dans votre référentiel de mises à jour local sont les versions 10.6.1.0 et 10.5.1.4 pour les hôtes Broker, LC/LD et Log Decoder.
- L'hôte du serveur SA et tous les autres hôtes sont actuellement mis à jour vers la version 10.6.1.

Last Modified: August 10 2016, 9:33AM

Cela signifie que vous pouvez mettre à jour les hôtes Broker, LC/LD et Log Decoder vers la version 10.6.1.0 ou 10.5.1.4.



Maintenance des services

La vue Services permet d'ajouter, de modifier, de supprimer, de surveiller et d'effectuer d'autres tâches de maintenance des services dans votre déploiement. Pour obtenir des instructions détaillées sur les tâches que vous effectuez dans la vue Hôtes, reportez-vous à Procédures relatives aux services.

Last Modified: August 10 2016, 9:33AM

Procédures de configuration des hôtes

Les rubriques suivantes décrivent les tâches minimales que vous devez effectuer pour configurer un hôte dans Security Analytics.

Last Modified: August 10 2016, 9:33AM

Étape 1. Ajouter ou mettre à jour un hôte

Votre environnement Security Analytics détermine la façon dont vous ajoutez un hôte.

Environnement Security Analytics	Tâches générales
Mise à jour 10.6	1. Téléchargez la documentation sur RSA Security Analytics v10.6 à partir de SCOL (https://knowledge.rsasecurity.com/). 2. Suivez les instructions de mise à jour de RSA Security Analytics v10.6.
Hôte de serveur Security Analytics 10.6	1. Cliquez sur + pour ouvrir la boîte de dialogue Ajouter un hôte. 2. Dans le champ **Nom**, saisissez un nom pour l'hôte et dans le champ **Nom d'hôte**, saisissez 127.0.0 pour l'adresse IP de l'hôte. 3. Cliquez sur **Enregistrer**.

Il existe une procédure détaillée, étape par étape pour chaque type d'environnement.

Mettre à jour un hôte après une mise à jour

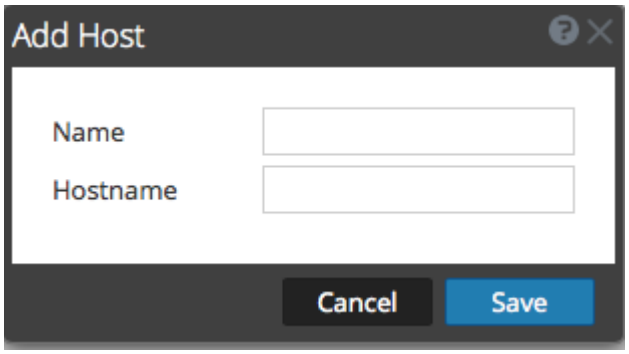
Caution: Avant d'essayer de mettre à jour un hôte vers la version 10.6, suivez la procédure suivante :
1. Téléchargez la documentation sur RSA Security Analytics v10.6 à partir de SCOL (https://knowledge.rsasecurity.com/).
2. Suivez les instructions de mise à jour de RSA Security Analytics v10.6.

1. Effectuez les tâches applicables à tous les services en cours d'exécution sur cet hôte comme décrit dans les sections suivantes des instructions de mise à jour de RSA Security Analytics v10.6.x.x :
   - Mettre à jour des tâches de préparation
   - Mettre une tâche à jour
   - Tâches consécutives à la mise à jour

Ajouter un hôte manuellement

1. Dans le menu Security Analytics, cliquez sur **Administration > Hôtes**.
   La vue Hôtes s'affiche.

2. Dans la barre d'outils du panneau Hôtes, sélectionnez +. La boîte de dialogue **Ajouter un hôte** s'affiche.



3. Dans le champ **Nom**, saisissez un nom pour l'hôte.
4. Dans le champ **Nom d'hôte**, saisissez l'**adresse IP** ou le **nom d'hôte** de l'hôte.
5. Cliquez sur **Enregistrer**.

RSA

Étape 2. Ajouter un service à un hôte

Chaque service se présente comme un plug-in à activer ou désactiver selon la fonction de l'hôte.

Conditions préalables

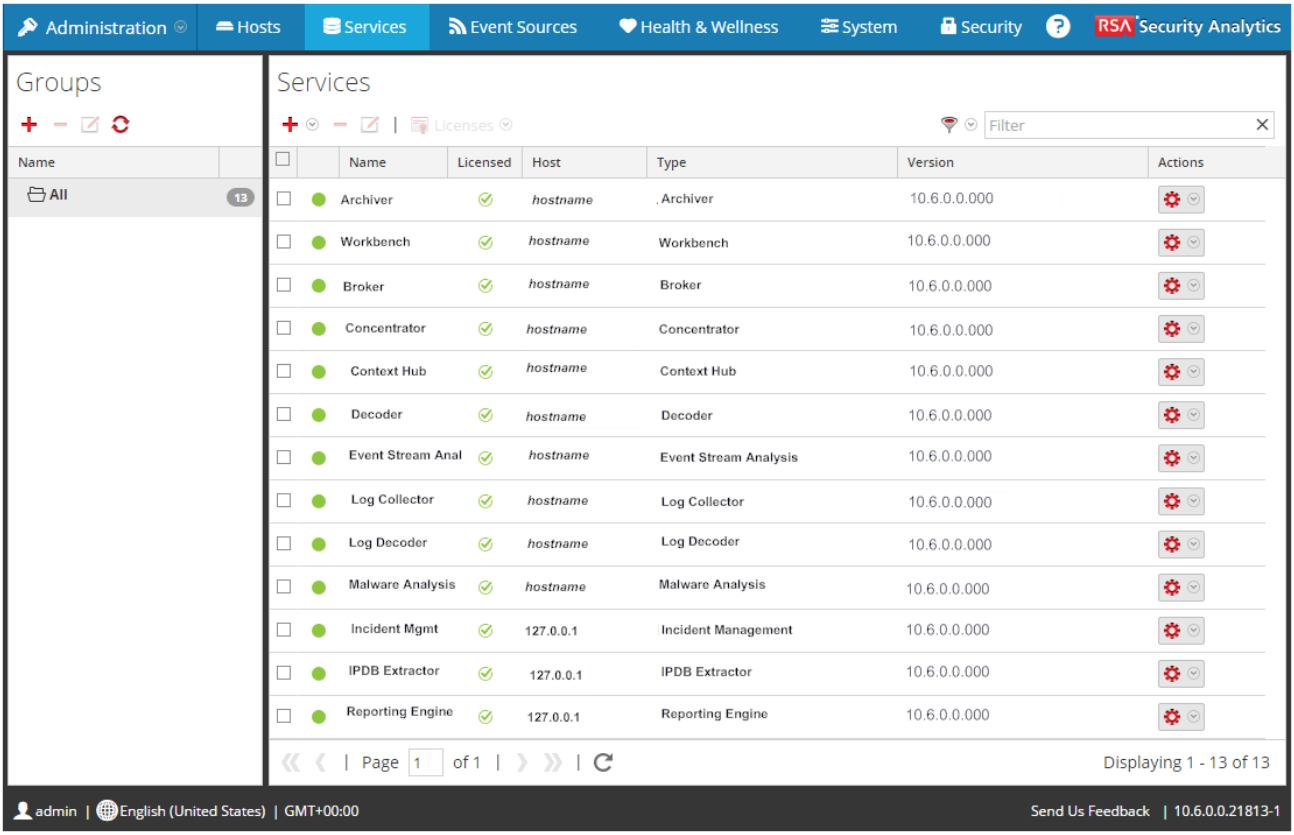
L'équipement, qui peut être de nature physique ou virtuel, doit être installé : Serveur Security Analytics, Broker, Concentrator, Decoder, Log Decoder, Archiver, Warehouse, serveur Malware Analysis ou serveur Event Stream Analysis.

Procédure

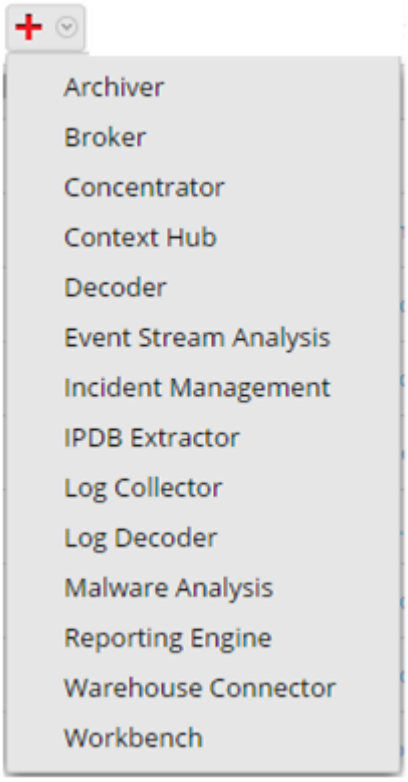
Pour ajouter un service à un hôte, effectuez les étapes suivantes :

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

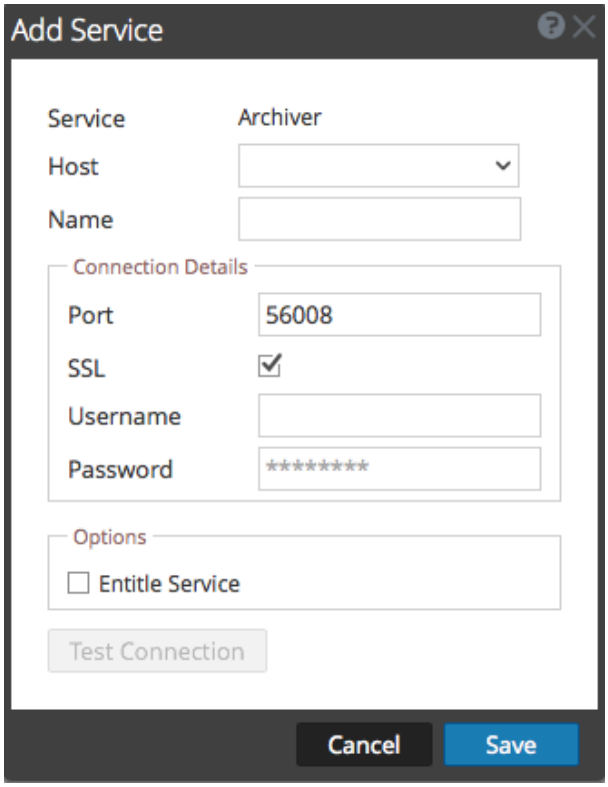
Last Modified: August 10 2016, 9:33AM



2. Dans la vue Services Administration, sélectionnez + dans la **barre d'outils du panneau Services**.



La boîte de dialogue Ajouter un service s'affiche.



Last Modified: August 10 2016, 9:33AM

3. Dans la liste déroulante, sélectionnez l'hôte sur lequel le serveur fonctionne.
4. Saisissez le nom du service.

> **Note:** Utilisez une convention de dénomination facile à comprendre pour faciliter les tâches administratives. Certains administrateurs préfèrent utiliser le nom d'hôte ou l'adresse IP (spécifiée dans le champ Hôte) pour le Nom également.

5. (Facultatif) Dans la section **Détails de connexion** :
   - **Port** - Si vous souhaitez utiliser un port autre que le port par défaut, saisissez son numéro dans le champ **Port**. Reportez-vous à l'Étape 3 : Passer en revue les ports SSL pour les connexions approuvées.
   - **SSL** - Si vous utilisez une connexion approuvée, sélectionnez **SSL**.
   - **Nom d'utilisateur** et **Mot de passe** - Saisissez les informations d'identification assignées à l'utilisateur sur le serveur Security Analytics.
6. (Facultatif) Dans la section **Options**, pour activer et appliquer une licence, sélectionnez **Autoriser le service**. Cette option apparaît uniquement pour les services qui nécessitent une licence.
7. Cliquez sur **Enregistrer**. Le service est ajouté et la boîte de dialogue se ferme.

RSA

Étape 3. Passer en revue les ports SSL pour les connexions approuvées

Pour prendre en charge les connexions approuvées, chaque service principal possède deux ports : un port non SSL non chiffré et un port SSL chiffré. Les connexions approuvées exigent le port SSL chiffré.

Condition préalable

Pour établir une connexion approuvée, chaque service Security Analytics Core doit être mis à niveau vers la version 10.4 ou ultérieure. Les connexions approuvées ne sont pas rétrocompatibles avec Security Analytics Core 10.3.x ou version antérieure.

Ports SSL chiffrés

Lorsque vous installez la version 10.4 ou supérieure ou mettez à niveau vers cette version, les connexions approuvées sont établies par défaut avec deux paramètres :

1. SSL est activé.
2. Le service Core est connecté à un port SSL chiffré.

Chaque service principal Security Analytics a deux ports :

- **Port non SSL** non chiffré
  Exemple : Archiver 50008
- **Port SSL** non chiffré
  Exemple : Archiver 56008

Le port SSL est le port non SSL + 6000.

Le tableau suivant répertorie tous les services Security Analytics avec leurs ports respectifs et indique que chaque service principal a deux ports. Tous les numéros de port répertoriés sont des ports TCP.

Service	Port non SSL non chiffré	Port SSL chiffré
Archiver	50008	56008
Broker	50003	56003
Concentrator	50005	56005

Last Modified: August 10 2016, 9:33AM

Service	Port non SSL non chiffré	Port SSL chiffré
Context Hub	S.O.	50022
Decoder	50004	56004
Event Stream Analysis	S.O.	50030
Gestion des incidents	S.O.	50040
IPDB Extractor	50025	56025
Log Collector	50001	56001
Log Decoder	50002	56002
Malware Analysis	S.O.	60007
Reporting Engine	S.O.	51113
Warehouse Connector	50020	56020
Workbench	50007	56007

Last Modified: August 10 2016, 9:33AM

RSA

Étape 4. Gérer l'accès à un service

Dans une connexion approuvée, un service fait explicitement confiance à Security Analytics Server pour gérer et authentifier les utilisateurs. Avec cette confiance, les services dans Administration > Services n'exigent plus la définition d'informations d'identification pour chaque service Core Security Analytics. Au lieu de cela, les utilisateurs qui ont été authentifiés par le serveur peuvent accéder au service sans entrer d'autre mot de passe.

Tester une connexion approuvée

Conditions préalables

1. Un rôle doit être attribué à l'utilisateur.
   Pour plus de détails, consultez la section Ajouter un utilisateur et attribuer un rôle dans le guide de gestion des utilisateurs et de la sécurité du système.
2. L'utilisateur doit :

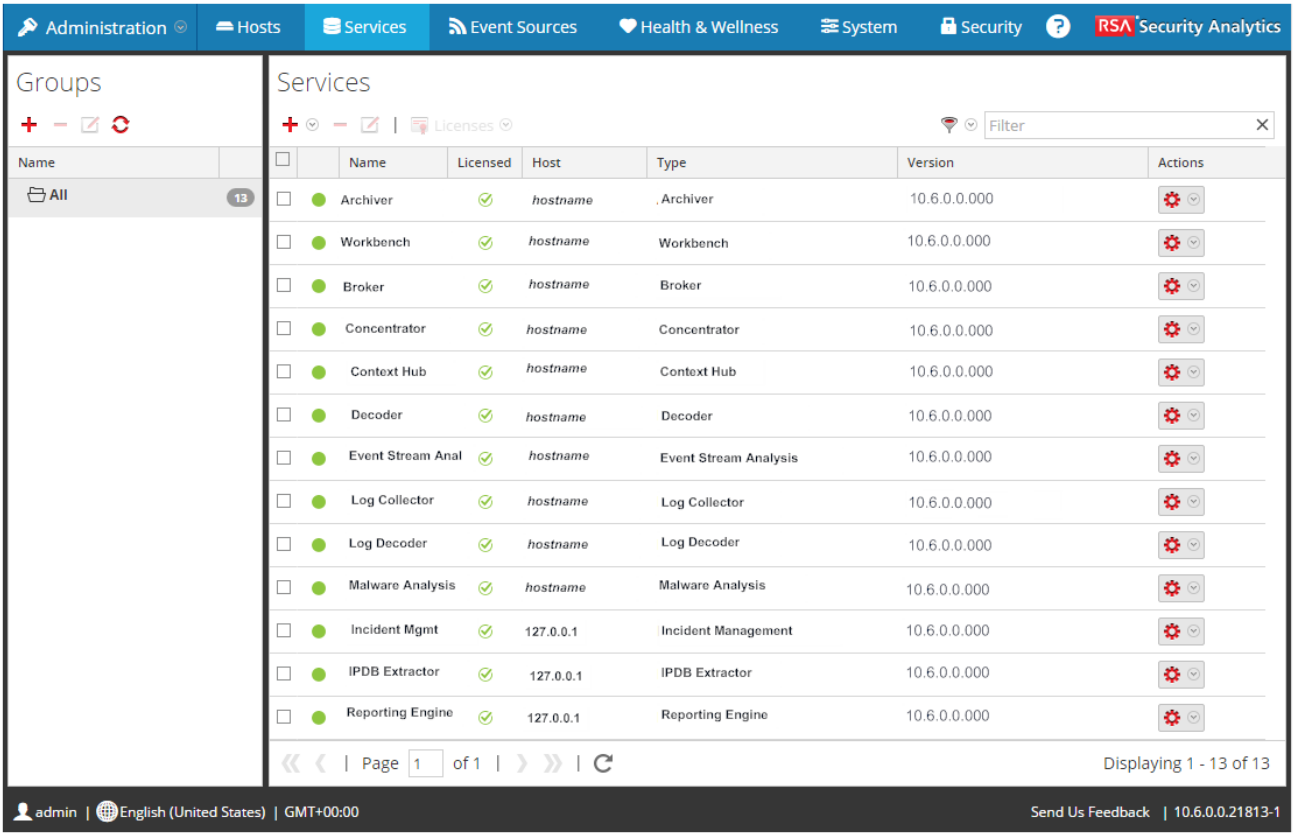
- Se connecter à Security Analytics pour être authentifié par le serveur
- Avoir accès au service

Procédure

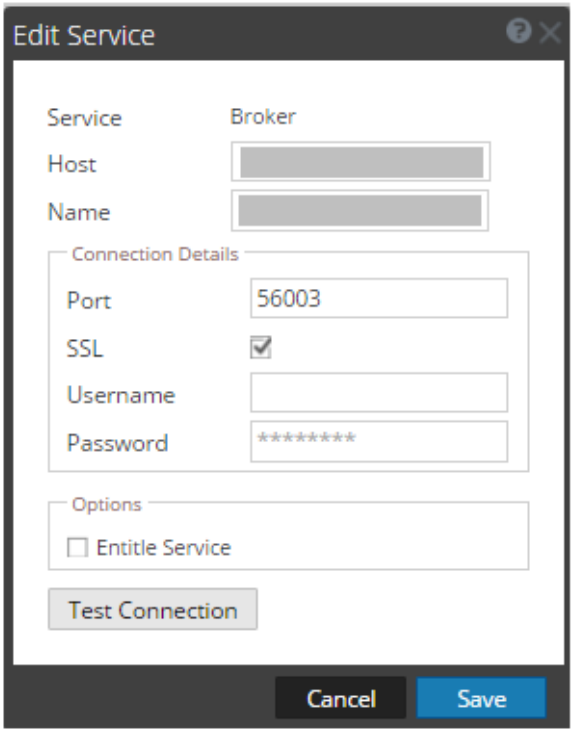
1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.

Last Modified: August 10 2016, 9:33AM

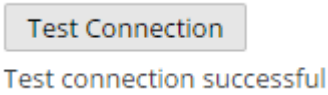
2. La vue Services s'affiche.



3. Sélectionnez le service à tester, puis cliquez sur .
   La boîte de dialogue **Modifier le service** s'affiche.



4. Si vous avez fait une nouvelle installation 10.6, le port est correct. Aucune action n'est requise dans le champ **Port**. Passez à l'étape suivante.
   Si vous avez effectué une mise à niveau vers la version 10.6 ou si vous possédez un environnement mixte de serveur 10.6 et d'hôtes 10.3, vous devez mettre à jour le **Port** en désactivant et en activant à nouveau **SSL**. Ensuite, le numéro de **Port** passe au port SSL crypté du service.
5. Supprimez le **Nom d'utilisateur** pour tester la connexion sans informations d'identification.
6. Cliquez sur **Tester la connexion**.



   Le message **Connexion testée avec succès** confirme que la connexion fiable est établie.
   Le précédent utilisateur authentifié peut accéder au service sans avoir à taper un nom d'utilisateur et un mot de passe sur le service.
7. Cliquez sur **Enregistrer**.

Procédures de maintenance des hôtes

Les rubriques suivantes décrivent les tâches de maintenance de base des hôtes que vous pouvez effectuer dans la vue Hôtes.

Last Modified: August 10 2016, 9:33AM

Appliquer les mises à jour

La vue Hôtes affiche les mises à jour de version logicielle disponibles dans votre référentiel de mises à jour local. Vous pouvez choisir d'appliquer les mises à jour que vous souhaitez à partir de cette vue. Reportez-vous à la rubrique Renseigner le référentiel de mises à jour local pour plus d'informations sur le mode de renseignement du référentiel de mises à jour local.

Procédure

Cette procédure vous indique comment mettre à jour un hôte vers une nouvelle version de Security Analytics.

Note: Lorsque vous mettez à jour l'hôte de serveur Security Analytics (SA), Security Analytics sauvegarde les fichiers de configuration System Management Service (SMS) (à l'exception du fichier `wrapper.conf`) du répertoire `/opt/rsa/sms/conf` vers le répertoire `/opt/rsa/sms/conf_%timestamp%`. Il s'agit d'une mesure de précaution pour les rares occasions où vous pourriez avoir besoin de restaurer la configuration de SMS à partir de la sauvegarde. Pour cela, remplacez les fichiers présents dans le répertoire `/opt/rsa/sms/conf` par les fichiers sauvegardés dans le répertoire `/opt/rsa/sms/conf_%timestamp%` après la mise à jour.

1. **(Conditionnel) Pour les déploiements sur plusieurs serveurs Security Analytics uniquement**, ouvrez une session SSH sur chaque hôte de serveur SA et vérifiez que le puppetmaster est activé à l'aide des commandes suivantes :
   ```
   chkconfig --add puppetmaster
   chkconfig --level 3 puppetmaster /etc/init.d/puppetmaster start
   ```
2. Connectez-vous à Security Analytics.
3. Dans le menu Security Analytics, sélectionnez **Administration** > **Hôtes**.

Note: Si vous disposez d'un hôte de serveur autre que Security Analytics exécutant une version qui est antérieure au chemin de mise à jour 10.6.0 (autrement dit, antérieure à la version 10.4.1), et que vous avez mis à jour votre hôte de serveur Security Analytics vers la version 10.6.0, l'hôte de serveur autre que Security Analytics affichera le “**chemin de mise à jour non pris en charge**” dans la colonne **État** de la vue Hôtes. La mise à jour ne peut pas être effectuée depuis cette vue. Contactez le Support Clients pour mettre l'hôte de serveur autre que Security Analytics sur le chemin non pris en charge.

4. Mettez à jour les hôtes de la séquence recommandée dans la rubrique Mettre à jour les hôtes dans la séquence appropriée.
   a. Sélectionnez la version que vous souhaitez appliquer à partir de la colonne **Mettre à jour la version**. Si vous souhaitez mettre à jour plusieurs hôtes vers cette version, activez la case à cocher située à gauche des hôtes.
   Mise à jour disponible apparaît dans la colonne **État** si vous disposez d'une mise à jour de version dans votre référentiel de mises à jour local pour les hôtes sélectionnés.
   Si :

- Vous ne pouvez pas trouver la version souhaitée, renseignez le référentiel de mises à jour local.
- Vous n'avez pas suffisamment d'espace disque dans votre référentiel de mises à jour local pour télécharger une version mise à jour, la boîte de dialogue **Gestion de l'espace du référentiel** s'affiche avec l'état du contenu et de l'espace disque du référentiel. Vous pouvez supprimer les versions dont vous n'avez pas besoin afin de libérer suffisamment d'espace disque pour télécharger la version que vous voulez. Voir la rubrique Libérer de l'espace disque dans le référentiel de mises à jour pour obtenir des instructions.

b. Cliquez sur **Mettre à jour** dans la barre d'outils. La colonne **État** vous indique ce qui se passe dans chacune des étapes suivantes de la mise à jour :
   - Téléchargement des packages de mises à jour.
   - Vérification de la configuration de votre version actuelle pour s'assurer qu'il n'y a pas de conflit. Indique :
     - Avertissement de mise à jour. Voir les détails en cas de conflit potentiel.
     - Conflit de mise à jour. Voir les détails en cas de conflit.
       Reportez-vous à la rubrique Dépannage suite aux avertissements, conflits et erreurs liés à la pré-mise à jour et mise à jour vers la version 10.6 pour obtenir des instructions sur la manière de régler ces avertissements et conflits de configuration.
   - Lancement de la mise à jour s'il n'y a pas de conflit.
   - Mise à jour des packages de mises à jour.
     Indique Erreur de mise à jour. Voir les détails si une erreur concerne un package qui bloque la mise à jour. Reportez-vous à la rubrique Dépannage suite aux avertissements, conflits et erreurs liés à la pré-mise à jour et la mise à jour vers la version 10.6 pour obtenir des instructions sur le mode de résolution de ces erreurs.

c. Après la mise à jour de l'hôte, Security Analytics vous invite à **redémarrer l'hôte**.

d. Cliquez sur **Redémarrer l'hôte** à partir de la barre d'outils.
   Security Analytics affiche l'état **Redémarrage en cours** jusqu'à ce que l'hôte soit à nouveau en ligne. Une fois que la connexion de l'hôte est rétablie, l'**état** indique **À jour**. Contactez le support Clients si l'hôte ne revient pas en ligne.

Note: Si la fonctionnalité DISA STIG est activée, l'ouverture des services de base peut prendre environ 5 à 10 minutes. Ce délai est dû à la génération des nouveaux certificats.

Modifier le nom ou le nom d'hôte d'un hôte

La vue Hôtes d'administration permet de modifier le nom et le nom d'hôte de l'hôte de l'interface utilisateur Security Analytics. Pour obtenir des informations sur la mise à jour d'un hôte, reportez-vous à l'étape 1 : Ajouter ou mettre à jour un hôte.

Modifier l'hôte

1. Dans le menu Security Analytics, sélectionnez **Administration > Hôtes**.
2. Dans la vue **Hôtes**, sélectionnez un hôte à modifier, puis dans la barre d'outils, sélectionnez  .
3. Dans la boîte de dialogue **Modifier l'hôte**, vous pouvez mettre à jour le **Nom** à tout moment.
4. Si le nom d'hôte réel change, mettez à jour le champ **Nom d'hôte**.
   Utilisez le script Python `changePuppetMaster.py`pour modifier l'adresse IP ou le nom d'hôte de l'hôte du serveur Security Analytics ou de tout autre hôte de votre déploiement Security Analytics. Exécutez ce script à partir de la ligne de commande de l'hôte du serveur Security Analytics. Reportez-vous à la section Modifier l'adresse IP ou le nom d'hôte d'un hôte pour obtenir des instructions sur la façon d'utiliser ce script.
5. Cliquez sur **Enregistrer**.

Last Modified: August 10 2016, 9:33AM

Créer et gérer des groupes d'hôtes

La vue Administration - Hôtes fournit les options permettant de créer et de gérer les groupes d'hôtes. La barre d'outils du panneau Groupes inclut les options de création, de modification et de suppression des groupes d'hôtes. Lorsque les groupes sont créés, vous pouvez faire glisser des hôtes individuels du panneau Hôtes vers un groupe.

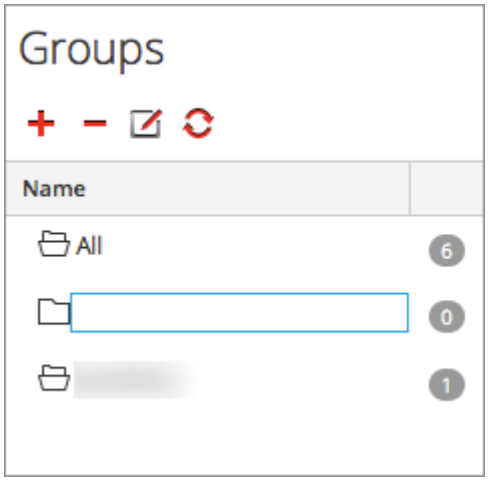
Les groupes peuvent refléter de manière utile une logique de fonctions, de géographie, de projets ou d'organisation. Un hôte peut appartenir à plusieurs groupes. Voici quelques exemples de regroupements possibles.

- Regroupement des différents types d'hôtes pour faciliter la configuration et la surveillance de tous les services Broker, Decoder ou Concentrator.
- Regroupement des hôtes faisant partie du même flux de données ; par exemple, un service Broker et tous les services Concentrator et Decoder associés.
- Regroupement des hôtes en fonction de leur région géographique et de leur emplacement au sein de la région. Si une importante panne d'alimentation se produit à un emplacement, les hôtes susceptibles d'être touchés sont facilement identifiables.

Créer un groupe

1. Dans **Security Analytics menu**, sélectionnez **Administration** > **Hôtes**.
   La vue Administration > Hôtes s'affiche.

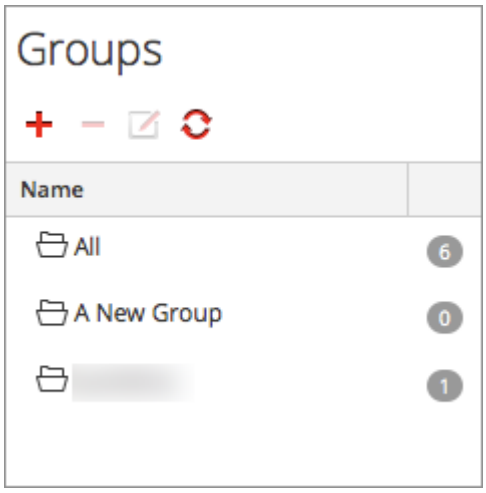
2. Dans la barre d'outils du panneau **Groupes**, cliquez sur +.
   Le curseur clignote dans le champ du nouveau groupe qui s'ouvre.



3. Saisissez le nom du nouveau groupe dans le champ (par exemple, **Nouveau groupe**) et appuyez sur **Entrée**.
   Le groupe est créé sous forme de dossier dans l'arborescence. Le nombre en regard du groupe indique le nombre d'hôtes

Last Modified: August 10 2016, 9:33AM

contenus dans ce groupe.



Modifier le nom d'un groupe

1. Dans la vue Hôtes **panneau Groupes**, double-cliquez sur le nom du groupe ou sélectionnez le groupe, puis cliquez sur .
   Le curseur clignote dans le champ du nom qui s'ouvre.
2. Saisissez le nouveau nom du groupe et appuyez sur **Entrée**.
   Le champ du nom se ferme et le nouveau nom de groupe s'affiche dans l'arborescence.

Ajouter un hôte à un groupe

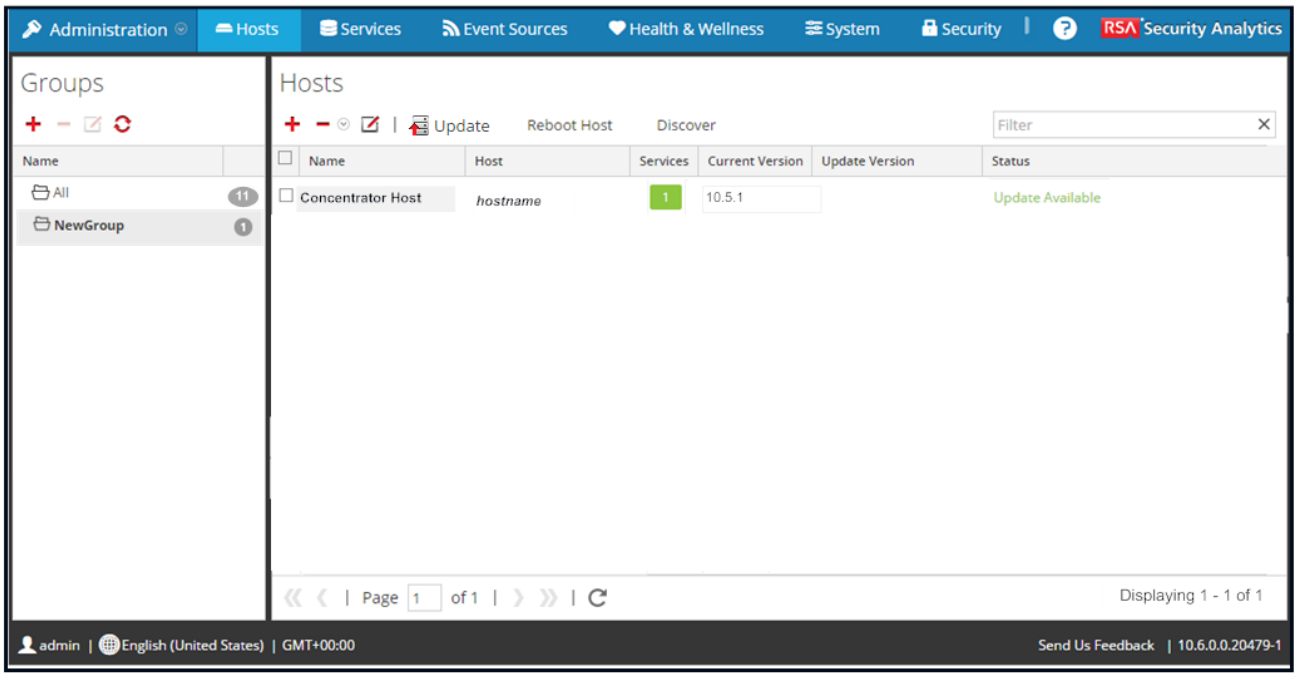
Dans la vue Hôtes **panneau Hôtes**, sélectionnez un hôte et faitesle glisser vers un dossier de groupe dans le panneau Groupes, par exemple **NouveauGroupe**.

AddHostToGrp.png

L'hôte est ajouté au groupe.

Afficher les hôtes dans un groupe

Pour afficher les hôtes dans un groupe, cliquez sur le groupe sous le **panneau Groupes**.
Le **panneau Hôtes** affiche les hôtes contenus dans ce groupe.



Supprimer un hôte d'un groupe

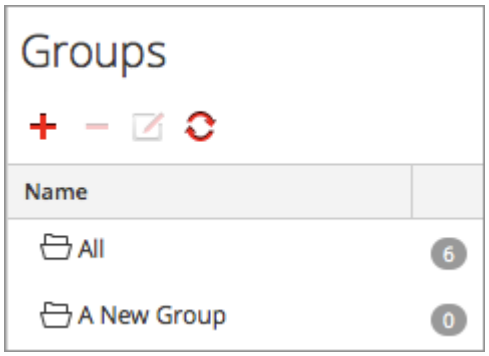
1. Dans la vue Hôtes **panneau Groupe**, sélectionnez le groupe qui contient l'hôte que vous souhaitez supprimer. Les hôtes de ce groupe s'affichent dans le panneau Hôtes.
2. Dans le **panneau Hôtes**, sélectionnez un ou plusieurs hôtes que vous souhaitez supprimer du groupe, et dans la barre

   d'outils, sélectionnez **> Supprimer du groupe**.
   Les hôtes sélectionnés sont supprimés du groupe, mais ne sont pas retirés de l'interface utilisateur Security Analytics. Le nombre d'hôtes dans le groupe, qui apparaît dans le nom du groupe, diminue en fonction des hôtes retirés du groupe. Le groupe **Tous** contient les hôtes qui ont été supprimés du groupe.

   Dans l'exemple suivant, le groupe d'hôtes nommé **Nouveau groupe** ne contient plus d'hôtes, puisque le service figurant dans

Last Modified: August 10 2016, 9:33AM

ce groupe a été supprimé.



Supprimer un groupe

1. Dans la vue Hôtes **panneau Groupes**, sélectionnez le groupe que vous souhaitez supprimer.
2. Cliquez sur −.
   Le groupe sélectionné est supprimé du panneau Groupes. Les hôtes qui figuraient dans le groupe ne sont pas retirés de l'interface utilisateur Security Analytics. Le groupe **Tous** contient les hôtes du groupe supprimé.

Libérer de l'espace disque dans le référentiel local des mises à jour

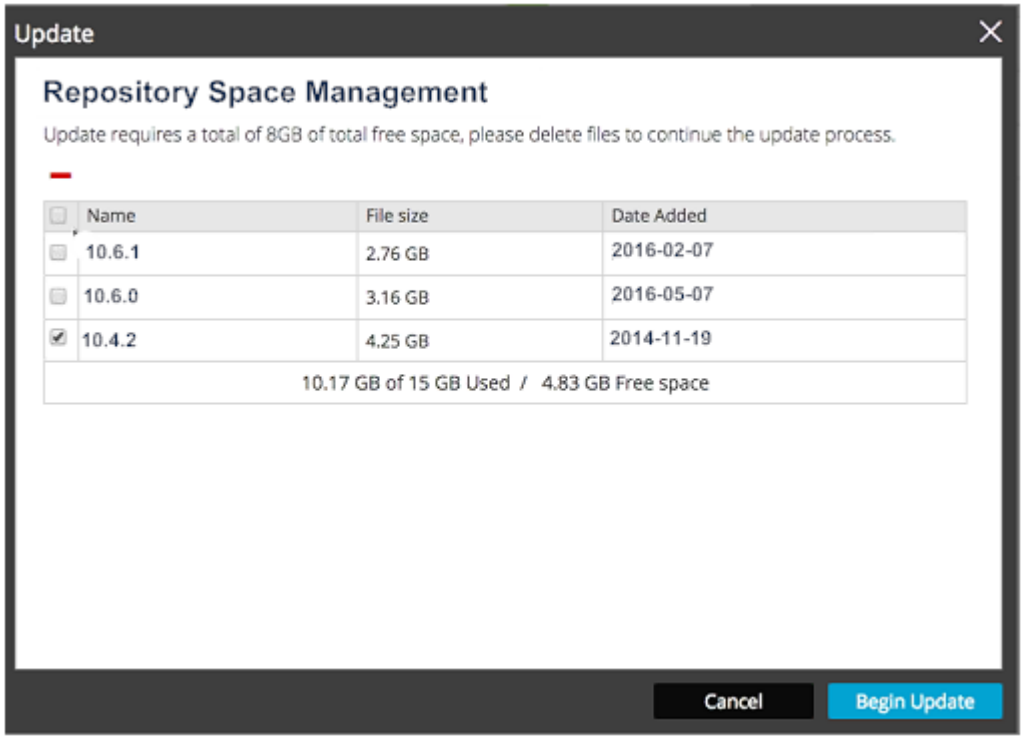
Si l'espace disque de votre référentiel local des mises à jour est insuffisant pour télécharger une mise à jour logicielle, la boîte de dialogue Référentiel des mises à jour de Security Analytics affiche le contenu et l'état de l'espace disque du référentiel. Vous pouvez supprimer une ou des versions inutiles pour libérer suffisamment d'espace disque pour télécharger la version souhaitée.

Procédure

Pour libérer de l'espace disque dans votre référentiel local des mises à jour :

1. Sélectionnez la version souhaitée dans la vue Hôtes.
   Si l'espace disque de votre référentiel local des mises à jour est insuffisant pour télécharger la version, la boîte de dialogue Gestion de l'espace du référentiel s'affiche.

2. Sélectionnez une ou des versions à supprimer.



Last Modified: August 10 2016, 9:33AM

3. Cliquez sur .
4. Cliquez sur **Commencer la mise à jour**.

Last Modified: August 10 2016, 9:33AM

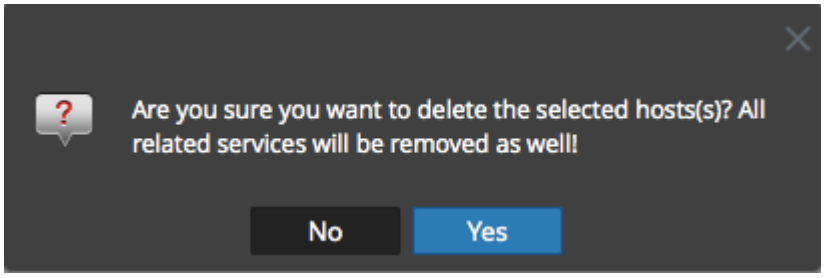
Supprimer un hôte

La suppression d'un hôte est une tâche de gestion d'hôte que vous pouvez réaliser dans la vue Hôtes d'administration. La vue Hôtes donne des informations supplémentaires sur les fonctions de gestion de l'hôte disponibles dans la vue Hôtes.

Supprimer un hôte

Suivez cette procédure pour supprimer un hôte qui n'est plus nécessaire de l'interface utilisateur Security Analytics et de ses services associés. Si vous supprimez un hôte, vous ne pourrez plus voir l'hôte et ses services associés dans Security Analytics.

1. Dans le menu Security Analytics, sélectionnez **Administration > Hôtes**.
2. Dans la vue **Hôtes**, sélectionnez un hôte que vous souhaitez supprimer, puis, dans la barre d'outils, sélectionnez > **Supprimer l'hôte**.
3. Une boîte de dialogue d'avertissement s'affiche.



4. Pour supprimer l'hôte, cliquez sur **Oui**.
   L'hôte sélectionné et ses services associés sont supprimés et vous ne pouvez plus les voir dans Security Analytics.

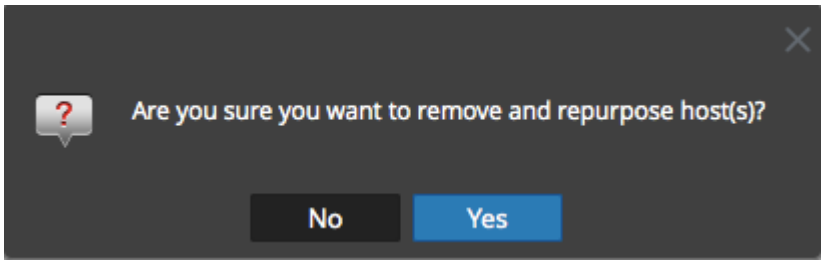
Supprimer et réaffecter un hôte

Suivez cette procédure lorsque vous voulez reconstruire complètement un hôte. Cette option est disponible uniquement sur le serveur primaire Security Analytics de l'hôte.

1. Dans le menu Security Analytics, sélectionnez **Administration > Hôtes**.
2. Dans la vue **Hôtes**, sélectionnez un hôte que vous souhaitez supprimer et réaffecter, puis, dans la barre d'outils, sélectionnez > **Supprimer et réaffecter l'hôte**.

Last Modified: August 10 2016, 9:33AM

3. Une boîte de dialogue d'avertissement s'affiche.



4. Pour supprimer et réaffecter l'hôte, cliquez sur **Oui**.

Rechercher des hôtes

Vous pouvez rechercher des hôtes dans une liste d'hôtes dans la vue Hôtes d'administration. La vue Hôtes permet de filtrer rapidement la liste des hôtes par Nom et Hôte. Il est possible d'avoir un grand nombre d'hôtes Security Analytics en cours d'utilisation pour différents objectifs. Au lieu de faire défiler la liste d'hôtes, vous pouvez filtrer rapidement la liste d'hôtes pour rechercher les hôtes à administrer.

Dans la vue Services d'administration, vous pouvez rechercher un service et trouver rapidement l'hôte qui exécute ce service.

Rechercher un hôte

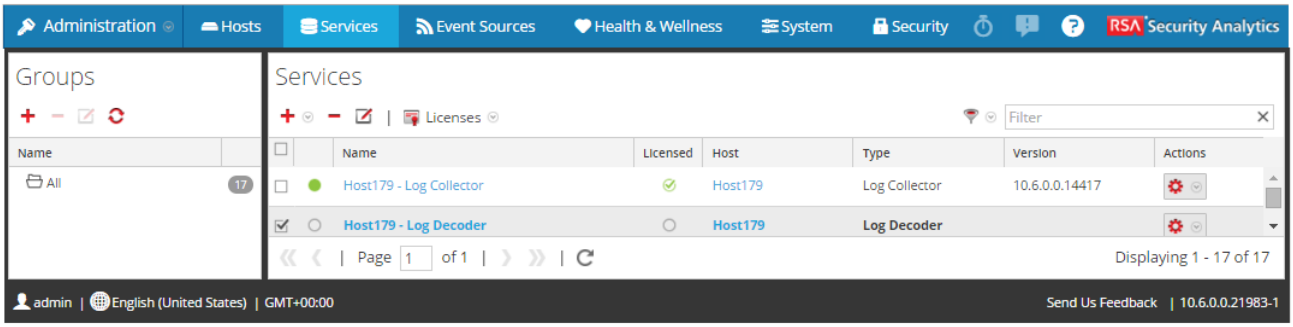
1. Dans le menu Security Analytics, sélectionnez **Administration > Hôtes**.
2. Dans la barre d'outils du panneau **Hôtes**, saisissez un **Nom** d'hôte ou **Nom d'hôte** dans le champ **Filtre**.

   Le panneau Hôtes répertorie les hôtes correspondant aux noms saisis dans le champ Filtre.

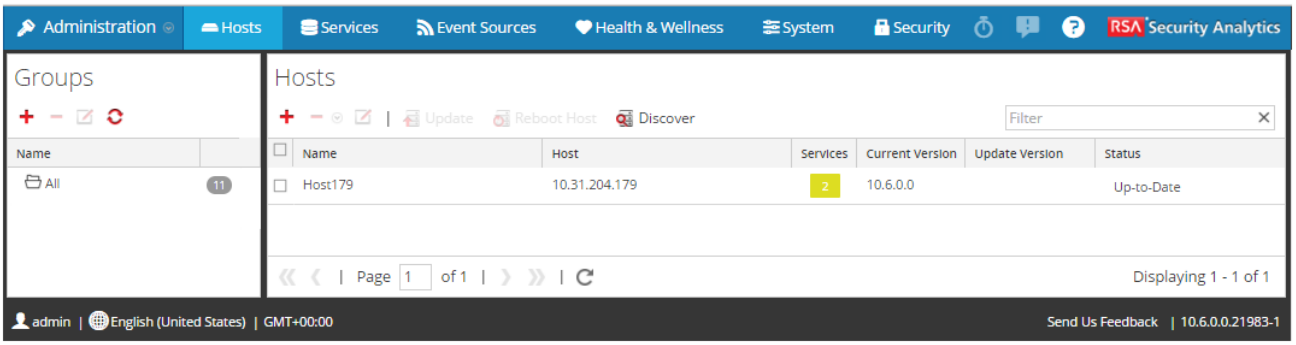
Rechercher l'hôte qui exécute un service

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Dans la vue Services, sélectionnez un service. L'hôte associé est répertorié dans la colonne **Hôte** pour ce service.



Last Modified: August 10 2016, 9:33AM

3. Pour administrer l'hôte dans la vue Hôtes, cliquez sur le lien dans la colonne **Hôte** correspondant à ce service. L'hôte associé au service sélectionné est affiché dans la vue Hôtes.



RSA

Mettre à jour les hôtes dans la séquence appropriée

Vous devez suivre une séquence spécifique lorsque vous effectuez la mise à jour des hôtes vers une nouvelle version. RSA recommande de suivre les instructions fournies dans cette rubrique.

Séquence de mise à jour de base

RSA recommande vivement que les clients :

- mettent à jour tous les hôtes au même moment (au cours de la même session).

  Note: Si vous échelonnez la mise à jour sur plusieurs sessions :
  - Vous ne perdrez pas les données.
  - Il se peut que toutes les fonctionnalités de la version ne soient pas opérationnelles si vous ne mettez pas à jour l'intégralité de votre déploiement.

- Effectuez la mise à jour des hôtes dans l'ordre suivant :
  1. Serveur Security Analytics

     Note: Le serveur Security Analytics est l'hôte sur lequel le serveur Security Analytics réside.
  2. Event Stream Analysis (ESA), Malware
  3. Services Decoder
  4. Services Concentrator
  5. Services Archiver
  6. Services Broker
- Évitez de mixer les modes (par exemple, un hôte en version 10.4.x, un hôte en version 10.5.x et un autre hôte en version 10.6.x dans le même déploiement de Security Analytics).

  Caution: Si vous déployez plusieurs serveurs Security Analytics, vous devez déterminer l'hôte qui fait office de serveur Security Analytics primaire et les hôtes qui font office de serveurs Security Analytics secondaires.

Mettre à jour Security Analytics dans un environnement avec plusieurs serveurs Security Analytics

La section suivante décrit comment mettre à jour un déploiement sur plusieurs serveurs Security Analytics.

Last Modified: August 10 2016, 9:33AM

Serveur primaire Security Analytics

Après avoir appliqué les mises à jour de sécurité sur un serveur Security Analytics, ce serveur devient le serveur Security Analytics primaire dans le cadre de votre déploiement. Tous les autres serveurs Security Analytics sont les serveurs Security Analytics secondaires. Le serveur Security Analytics primaire offre toutes les fonctionnalités d'un serveur Security Analytics comprenant fonctionnellement ce qui suit :

1. Vue **Hôtes** totalement fonctionnelle incluant la colonne **Mises à jour**.
2. Accès aux vues Intégrité.
3. Utilisation complète de la fonction de connexions approuvées.

Serveur Security Analytics secondaire

Un serveur Security Analytics secondaire présente les limitations suivantes :

1. Les colonnes **Mettre à jour la version** et **État** de la vue **Hôtes** sont valides pour le serveur Security Analytics primaire exclusivement. Elles reflètent l'état incorrect d'un serveur Security Analytics secondaire pour éviter les **interactions**.
2. Vous ne pouvez pas utiliser les vues Intégrité.
3. Vous ne pouvez pas utiliser la fonction de connexions approuvées.

Scénario 1. Mise à jour intégrale, Ordre des mises à jour (fortement recommandé)

Déploiement du client v10.x – 1 serveur Security Analytics, 2 Decoders, 2 Concentrators, 1 Archiver, 1 Broker, 1 ESA, 1 Malware Analysis

1. Mettre à jour le serveur Security Analytics.
2. Mettre à jour les services ESA et Malware Analysis.
3. Mettre à jour les 2 Decoders.
4. Mettre à jour les 2 Concentrators et l'Archiver.
5. Mettre à jour le Broker.

Scénario 2. Mise à jour partielle

Déploiement du client v10.x – 1 serveur Security Analytics, 2 Decoders, 2 Concentrators, 1 Broker, 1 ESA, 1 Malware Analysis

1. Mettre à jour le serveur Security Analytics.
2. Mettre à jour les services ESA et Malware Analysis.
3. Mettre à jour 1 Decoder et 1 Concentrator.
   Temps écoulé au cours duquel Security Analytics traite une quantité importante de données.
4. Mettre à jour 1 Decoder, 1 Concentrator et 1 Broker.

Last Modified: August 10 2016, 9:33AM

Scénario 3. Mise à jour des paramètres régionaux avec plusieurs services Broker

Déploiement du client v10.x – 4 Decoders, 4 Concentrators, 2 Brokers, 1 serveur Security Analytics, 1 ESA, 1 Malware Analysis (2 sites, chacun doté de 2 Decoders, 2 Concentrators et 1 Broker)

Première session de mise à jour sur le Site 1

1. Mettre à jour le serveur Security Analytics.
2. Mettre à jour les services ESA et Malware Analysis.
3. Mettre à jour 2 Decoders, 2 Concentrators et 1 Broker sur le site 1.

Deuxième session de mise à jour sur le Site 2

Mettre à jour 2 Decoders, 2 Concentrators et 1 Broker sur le site 2.

Scénario 4. Mise à jour des paramètres régionaux avec plusieurs serveurs Security Analytics

Déploiement du client v10.x – 2 serveurs Security Analytics, 4 Decoders, 4 Concentrators, 2 Brokers, 1 ESA, 1 Malware Analysis (2 sites, chacun doté d'1 serveur Security Analytics, de 2 Decoders, de 2 Concentrators et d'1 Broker)

Première session de mise à jour sur le Site 1

1. Mettre à jour le serveur Security Analytics primaire.
2. Mettre à jour les services ESA et Malware Analysis.
3. Mettre à jour 2 Decoders, 2 Concentrators et 1 Broker sur le site 1.

Deuxième session de mise à jour sur le Site 2

1. Mettre à jour le serveur Security Analytics secondaire.
2. Mettre à jour 2 Decoders, 2 Concentrators et 1 Broker sur le site 2.

Last Modified: August 10 2016, 9:33AM

Procédures relatives à l'hôte dans la boîte de dialogue Liste des tâches

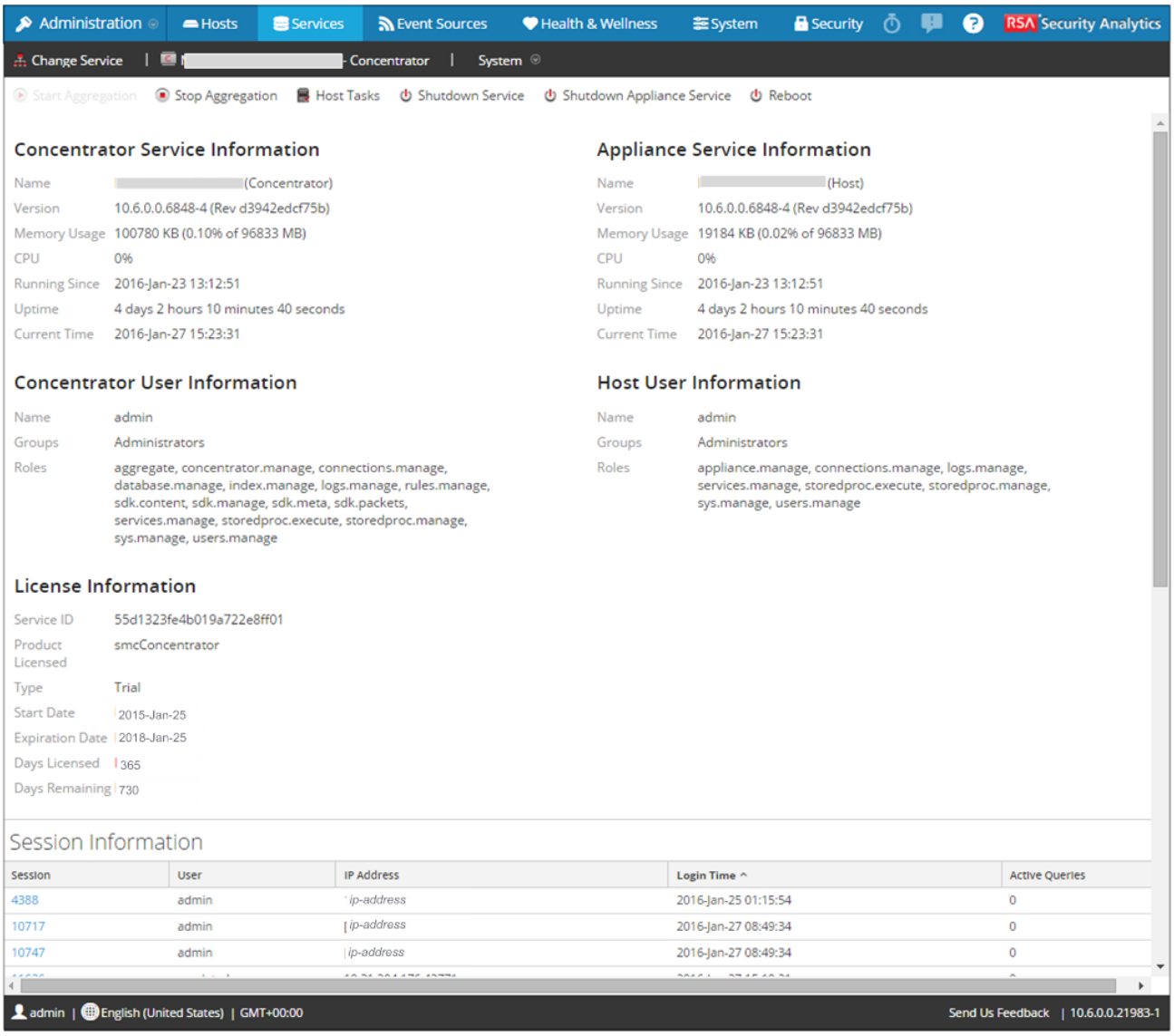
Utilisez la boîte de dialogue Liste des tâches de l'hôte pour gérer les tâches liées à un hôte et ses communications avec le réseau. Plusieurs options de configuration de service et d'hôte sont disponibles pour les hôtes Core. Les rubriques suivantes décrivent :

- Utilisation de la boîte de dialogue Liste des tâches de l'hôte.
- Tâches que vous pouvez effectuer dans la boîte de dialogue Liste des tâches de l'hôte.

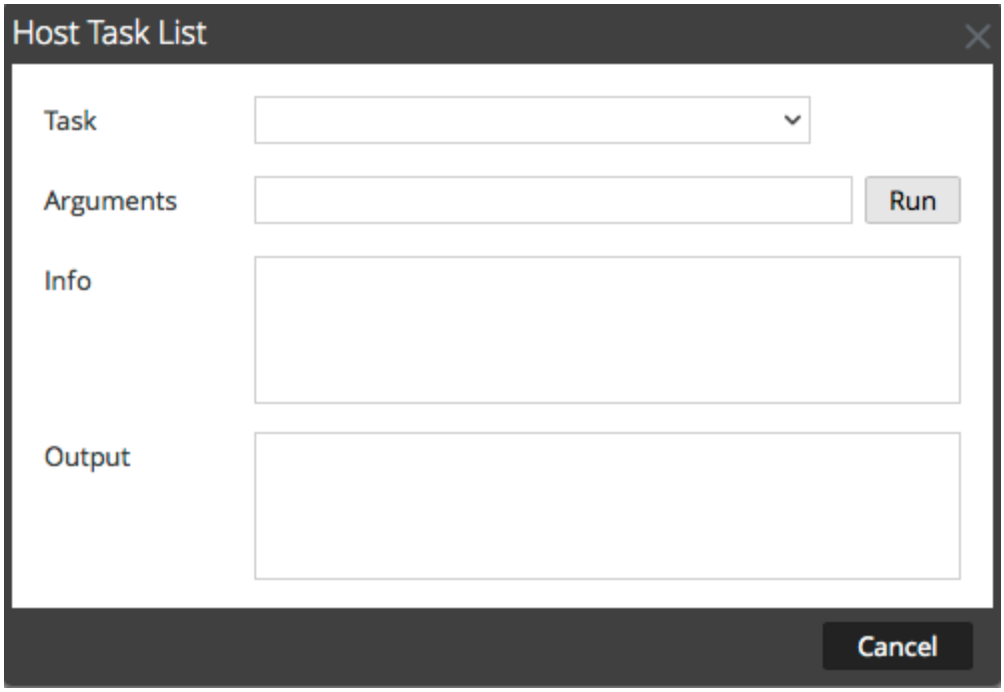
Last Modified: August 10 2016, 9:33AM

Exécuter une tâche à partir de la Liste des tâches de l'hôte

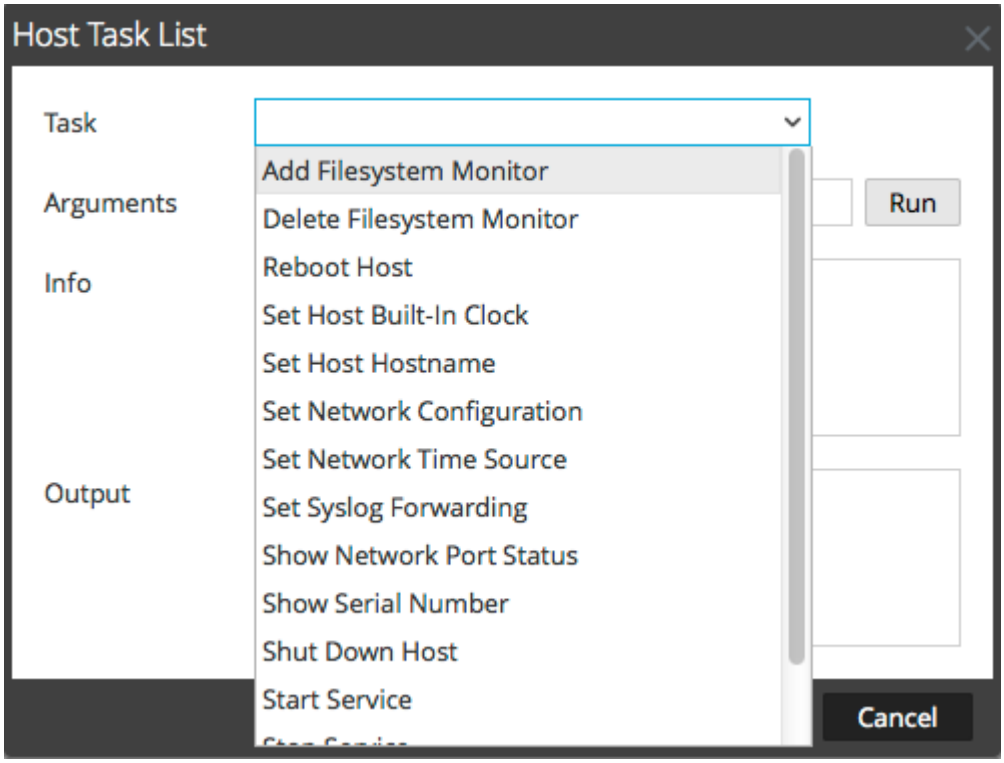
1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.



3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.

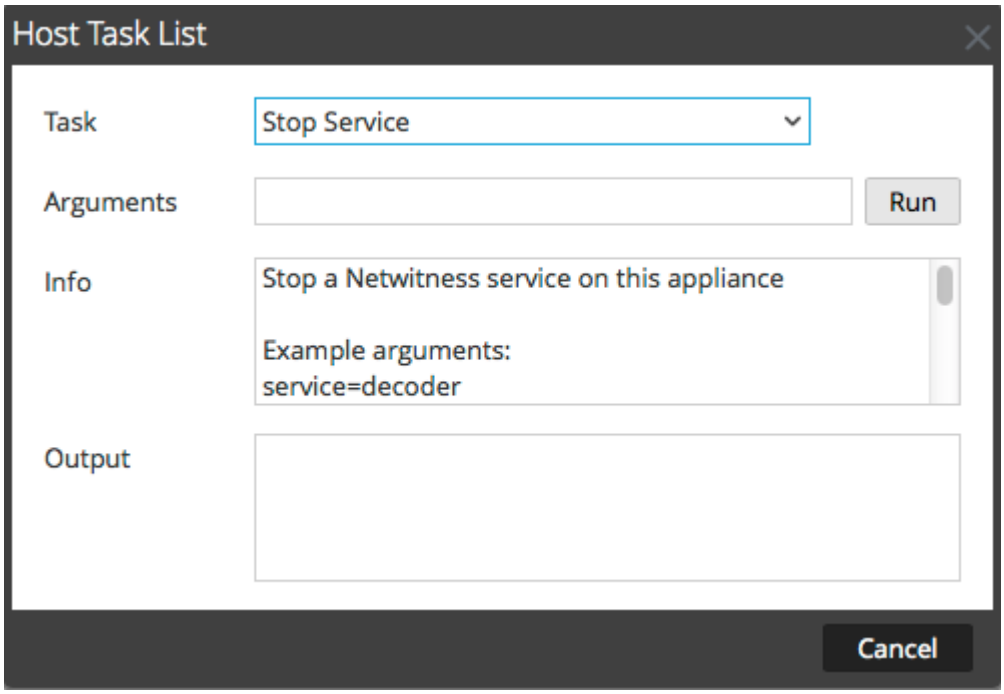


4. Dans la **Liste des tâches de l'hôte,** cliquez dans le champ **Tâche** pour afficher la liste déroulante des tâches qui s'exécutent sur un hôte.



5. Sélectionnez une tâche. Par exemple, cliquez sur **Arrêter le service**.
La tâche s'affiche dans le champ **Tâche**. La description des tâches, les exemples d'arguments, les rôles de sécurité et les

paramètres s'affichent dans la zone **Info**.



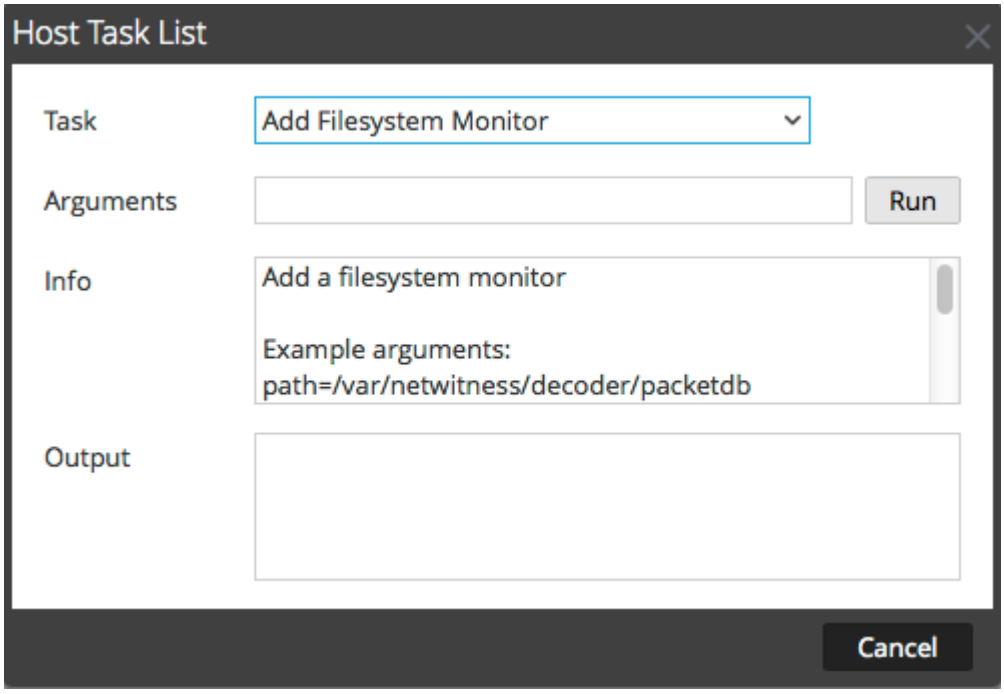
6. Saisissez des arguments si nécessaire, puis cliquez sur **Exécuter**.
La commande s'exécute et le résultat s'affiche dans la zone **Sortie**.

Ajouter et supprimer la surveillance d'un système de fichiers

Lorsque vous souhaitez qu'un service surveille le trafic sur un système de fichiers spécifique, vous pouvez sélectionner le service, puis spécifier le chemin. Security Analytics ajoute une surveillance du système de fichiers. Une fois qu'une surveillance du système de fichiers est ajoutée à un service, le service continue à surveiller le trafic sur ce chemin jusqu'à ce que la surveillance du système de fichier soit supprimée.

Configurer la surveillance d'un système de fichiers

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.
4. Dans la **Liste des tâches de l'hôte**, sélectionnez **Ajouter le moniteur du système de fichiers**.
   Dans la zone **Info**, une brève explication de la tâche et des arguments de la tâche s'affiche.



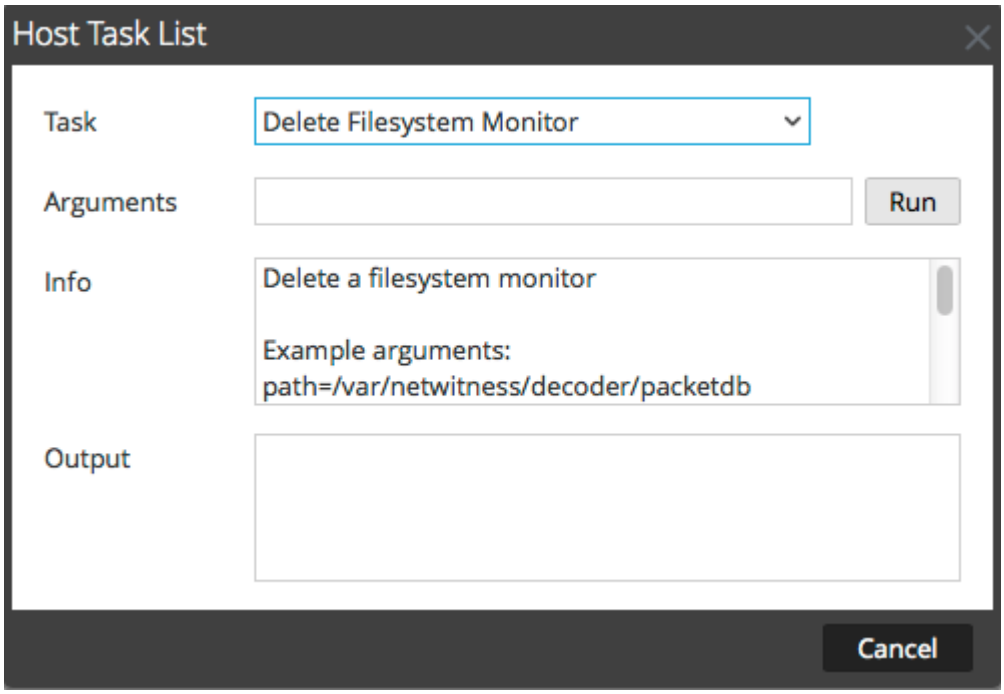
5. Pour identifier le système de fichiers à surveiller, tapez le chemin dans le champ **Arguments**. Par exemple : **path=/var/netwitness/decoder/packetdb**

Last Modified: August 10 2016, 9:33AM

6. Cliquez sur **Exécuter**.
   Le résultat s'affiche dans la zone **Sortie**. Le service commence à surveiller le système de fichiers et continue à le faire jusqu'à ce que vous supprimiez la surveillance du système de fichiers.

Supprimer la surveillance d'un système de fichiers

1. Accédez à la boîte de dialogue **Liste des tâches de l'hôte**.
2. Dans la **Liste des tâches de l'hôte**, sélectionnez **Supprimer le moniteur du système de fichiers**.
   Dans la zone **Info**, une brève explication de la tâche et des arguments de la tâche s'affiche.



3. Pour cesser de surveiller le système de fichiers, tapez le chemin dans le champ **Arguments**. Par exemple : **path=/var/netwitness/decoder/packetdb**
4. Cliquez sur **Exécuter**.
   Le résultat s'affiche dans la zone **Sortie**. Le service cesse de surveiller le système de fichiers.

Last Modified: August 10 2016, 9:33AM

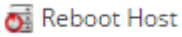
Redémarrer un hôte

Sous certaines conditions, il est nécessaire de redémarrer un hôte ; par exemple, après l'installation d'une mise à niveau logicielle. Cette procédure utilise un message de la liste des tâches de l'hôte pour arrêter et redémarrer un hôte.

Security Analytics offre également d'autres options pour arrêter un hôte :

- Pour arrêter et redémarrer un hôte via un service rattaché, accédez à la vue Hôtes à partir d'un service dans la vue Services (consultez Recherche d'un hôte), puis suivez la procédure *Arrêter et redémarrer un hôte à partir de la vue Hôtes* ci-dessous.
- Pour arrêter l'hôte physique sans redémarrer, consultez Arrêter l'hôte.

Arrêter et redémarrer un hôte à partir de la vue Hôtes

1. Dans **Security Analytics menu**, sélectionnez **Administration >Hôtes**.
2. Dans le panneau **Hôtes**, sélectionnez un hôte.
3. Sélectionnez 

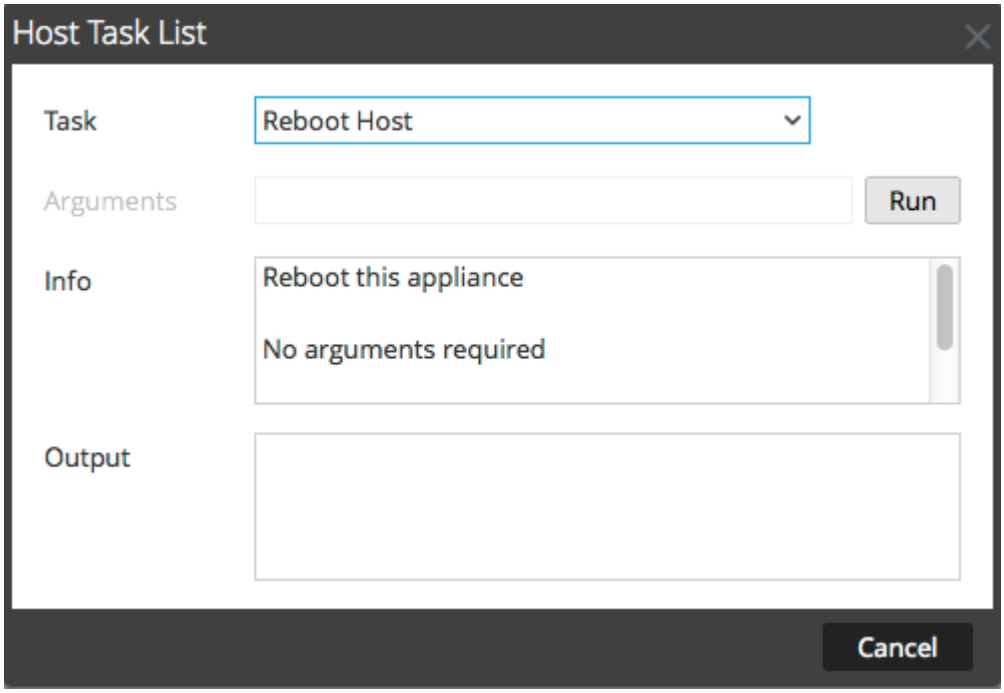
dans la barre d'outils.

Arrêter et redémarrer un Hôte à partir de la Liste des tâches de l'hôte

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans le panneau **Services**, sélectionnez un service et  **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.

Last Modified: August 10 2016, 9:33AM

4. Dans la **Liste des tâches de l'hôte**, sélectionnez **Redémarrer l'hôte** dans le champ **Tâche** .
   Aucun argument n'est requis.



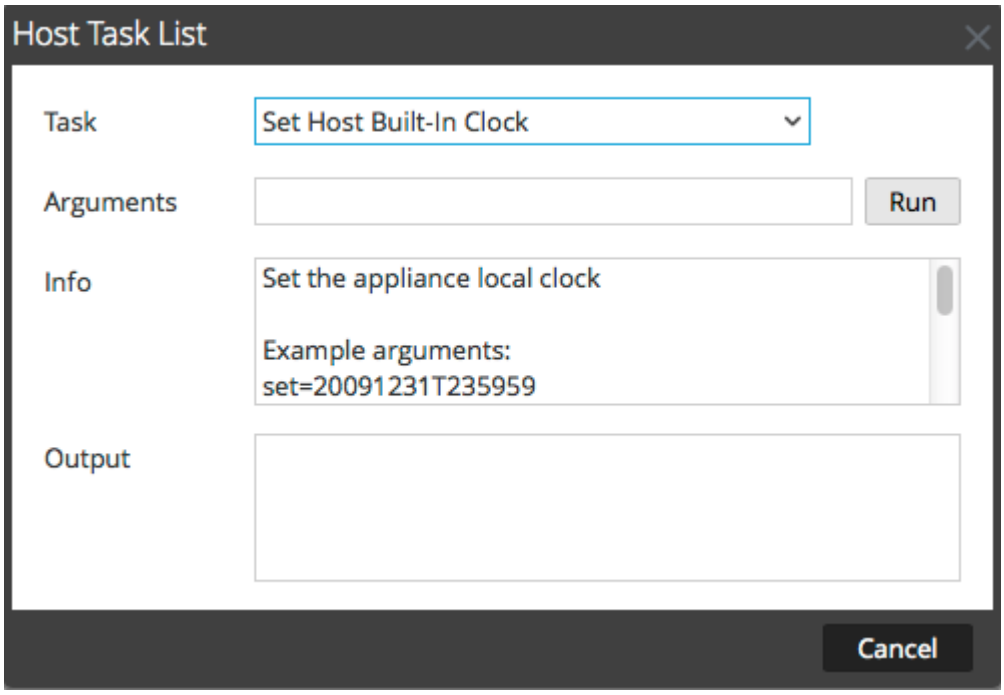
5. Cliquez sur **Exécuter**.
   L'hôte est redémarré et le résultat s'affiche dans la zone **Sortie**.

Paramétrer l'heure prédéfinie de l'hôte

Après un arrêt ou une panne de batterie, il peut être nécessaire de régler l'horloge locale d'un hôte. La tâche Paramétrer l'heure prédéfinie de l'hôte réinitialise l'heure de l'horloge.

Définir l'heure sur l'horloge locale

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services**, cliquez sur **Tâches de l'hôte**.
4. Dans la **Liste des tâches de l'hôte**, sélectionnez **Paramétrer l'heure prédéfinie de l'hôte**.
   L'aide associée à la tâche est affichée dans la zone **Infos**.



5. Entrez les arguments de date et d'heure dans le champ **Arguments**. Par exemple, pour spécifier 7 octobre 2014 à 23:59:59, saisissez :
   set=20141007T235959
6. Cliquez sur **Exécuter**.
   L'horloge est définie sur l'heure spécifiée et un message s'affiche dans la zone **Sortie**.

Last Modified: August 10 2016, 9:33AM

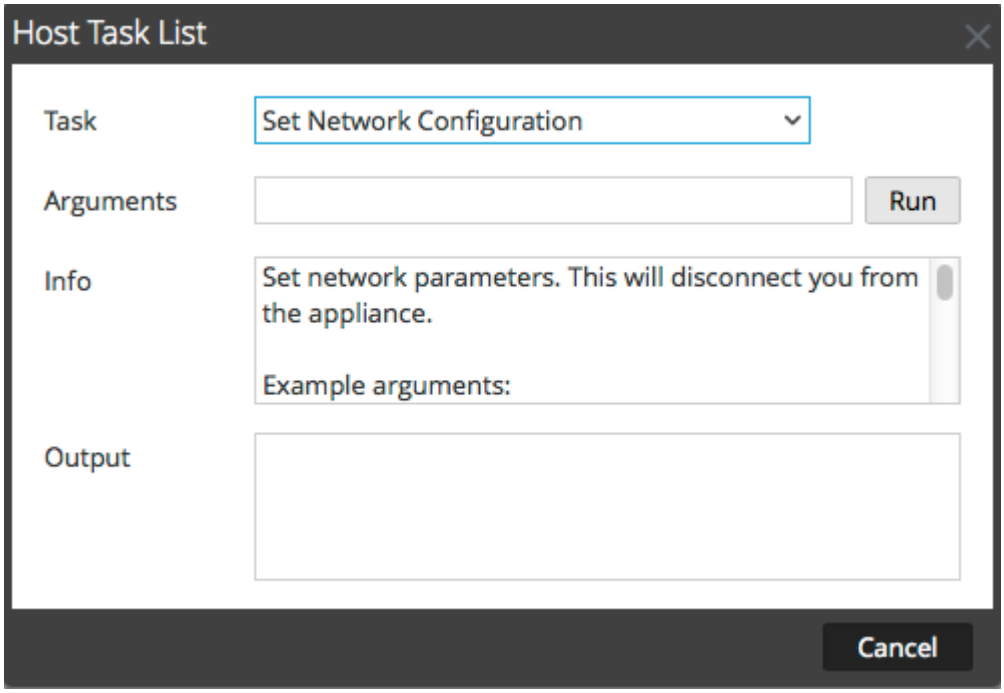
Définir la configuration réseau

Lorsqu'un hôte Core configuré doit changer d'adresse, vous pouvez définir une nouvelle adresse réseau, le masque de sous-réseau et la passerelle de l'hôte en utilisant le message **Définir la configuration réseau** dans la **Liste des tâches de l'hôte**.

⚠ **Caution:** Le changement prend effet immédiatement, et l'hôte est déconnecté de Security Analytics. Vous devez ensuite ajouter l'hôte à Security Analytics à nouveau à l'aide de la nouvelle adresse réseau.

Indiquer l'adresse réseau d'un hôte

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.
4. Dans la **Liste des tâches de l'hôte**, cliquez sur **Définir la configuration réseau**.
   Cette tâche s'affiche dans le champ **Tâche**, et l'aide s'affiche dans la zone **Info**.



Last Modified: August 10 2016, 9:33AM

5. Saisissez les arguments dans le champ **Arguments**. Par exemple :
   mode=static address=192.168.0.20 netmask=255.255.255.0 gateway=192.168.0.1
6. Cliquez sur **Exécuter.**
   La tâche s'exécute et le résultat s'affiche dans la zone **Sortie**. L'hôte est déconnecté de Security Analytics. Vous devez ajouter à nouveau l'hôte avec la nouvelle adresse.

Note: Si vous choisissez le mode DHCP, il sera impossible de déterminer la nouvelle adresse. Il peut être nécessaire de se connecter à l'hôte directement pour déterminer la nouvelle adresse.

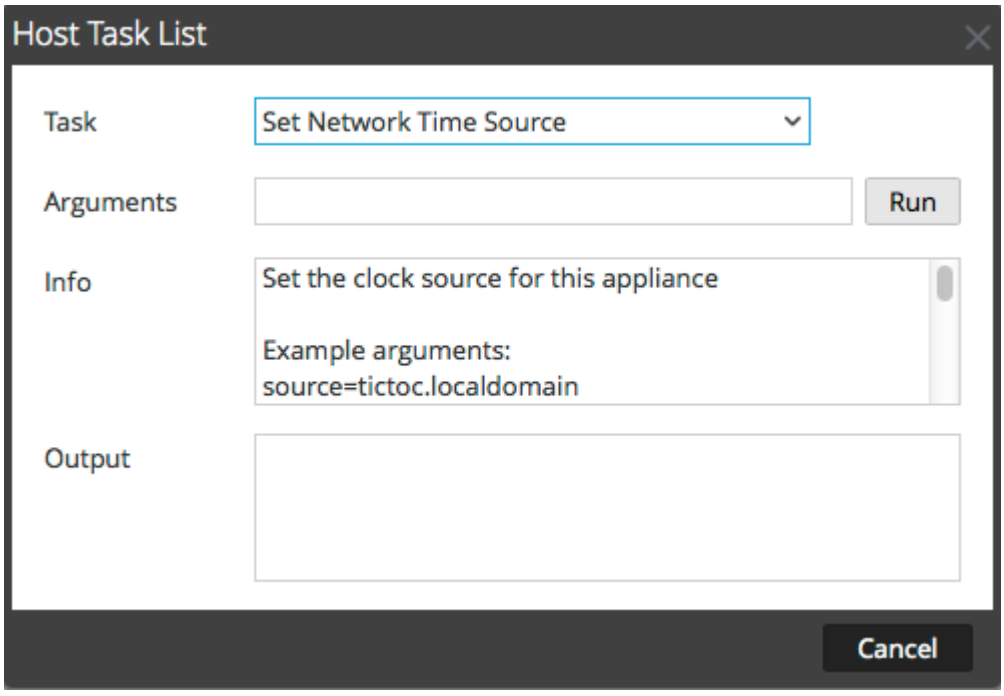
Last Modified: August 10 2016, 9:33AM

Définir la source de l'heure sur le réseau

Lorsque vous définissez la source d'horloge d'un hôte, définissez le nom d'hôte ou l'adresse d'un serveur NTP comme la source d'horloge réseau de l'hôte. Si l'hôte utilise une source d'horloge locale, vous devez spécifier **locale** ici pour que l'option **Définir la source d'horloge locale** devienne effective.

Spécifier la source d'horloge réseau

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et cliquez sur **Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches des hôtes**.
4. Dans la **Liste de tâches des hôtes**, sélectionnez **Définir la source d'horloge sur le réseau**.



5. Exécutez l'une des opérations suivantes :
   - Saisissez le nom d'hôte ou l'adresse du serveur NTP qui servira de source d'horloge à cet hôte, par exemple : **source=tictoc.localdomain**
   - Pour utiliser l'horloge hôte comme source d'horloge, saisissez : **source=local**

Last Modified: August 10 2016, 9:33AM

6. Cliquez sur **Exécuter**.
   La source d'horloge est définie et un message s'affiche dans la zone **Sortie**.

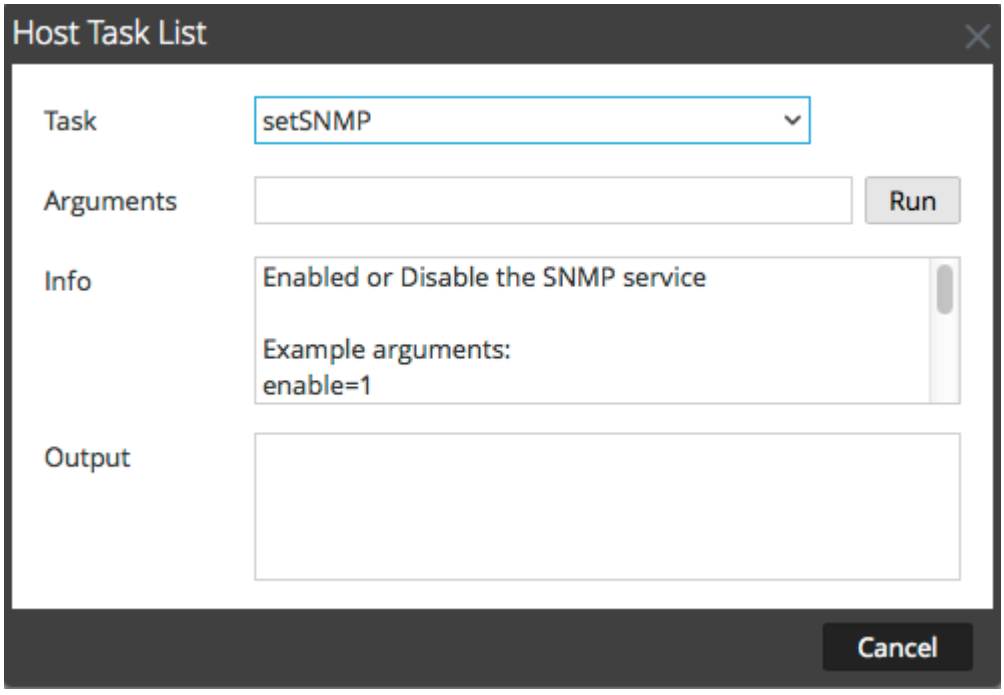
Note: Si vous avez spécifié une source d'horloge NTP **locale**, l'horloge hôte sert de source d'horloge et l'heure est configurée à l'aide de Régler l'horloge intégrée de l'hôte.

Configurer SNMP

Dans la liste de tâches des hôtes, l'option Configurer SNMP active ou désactive le service SNMP sur l'hôte. Pour qu'un hôte reçoive des notifications SNMP, le service SNMP doit être activé. Si vous n'utilisez pas SNMP pour les notifications Security Analytics, il n'est pas nécessaire d'activer le service.

Basculer le service SNMP sur l'hôte

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services**, cliquez sur **Tâches des hôtes**.
4. Dans la **Liste de tâches des hôtes**, sélectionnez **setSNMP**.
   Dans la zone **Info**, une brève explication de la tâche et des arguments de la tâche s'affiche.



5. Exécutez l'une des opérations suivantes :
   - Pour désactiver le service, saisissez **enable=0** dans le champ **Arguments**.
   - Pour activer le service, saisissez **enable=1** dans le champ **Arguments**.

Last Modified: August 10 2016, 9:33AM

6. Cliquez sur **Exécuter**.
   Le résultat s'affiche dans la zone **Sortie**.

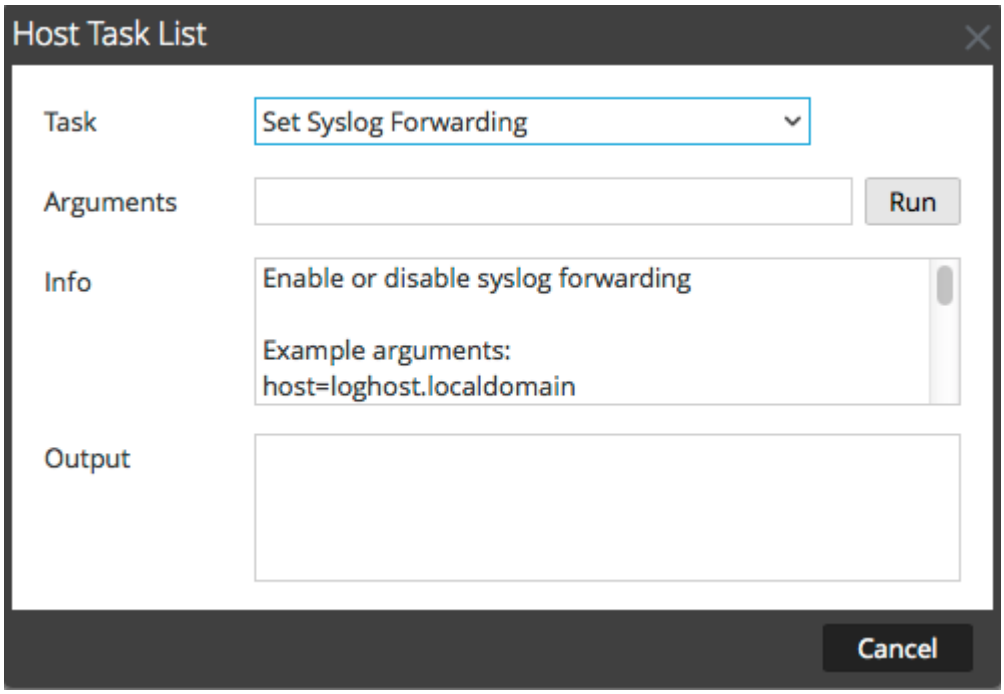
RSA

Définir le transfert Syslog

Vous pouvez configurer le transfert Syslog pour envoyer les logs du système d'exploitation de vos hôtes Security Analytics à un serveur syslog distant. Pour cela, vous pouvez utiliser la tâche Définir le transfert Syslog de la liste des tâches de l'hôte pour activer ou désactiver le transfert syslog.

Définir et lancer un transfert syslog

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et  **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.
4. Dans la **liste de tâches des hôtes**, sélectionnez **Définir le transfert Syslog**.
   Dans la zone **Info**, une brève explication de la tâche et des arguments de la tâche s'affiche.



5. Dans le champ **Arguments**, procédez de l'une des façons suivantes :
   - Pour activer le transfert syslog, utilisez l'un des formats suivants :
     - **host=<hôte log>.<domaine local>** (par exemple, host=syslogserver.local).

Last Modified: August 10 2016, 9:33AM

- **host=<hôte log>.<domaine local>:<port>** (par exemple, host=syslogserver.local:514).
- **host=<IP>** (par exemple, host=10.31.244.244).
- **host=<IP>:<port>** (par exemple, host=10.31.244.244:514).

Le tableau suivant répertorie les paramètres utilisés pour activer le transfert syslog et en fournit une description.

Paramètre	Description
hôte log	Nom d'hôte du serveur syslog distant.
domaine local	Domaine du serveur syslog distant.
port	Adresse IP du serveur syslog distant.
IP	Numéro de port sur lequel le serveur syslog reçoit les messages syslog.

- Pour désactiver le transfert syslog, saisissez **host=disable.**

6. Cliquez sur **Exécuter**.
   Le résultat s'affiche dans la zone **Sortie**.

   Une fois le transfert syslog activé ou désactivé, le fichier /etc/rsyslog.conf est automatiquement mis à jour de façon à activer ou désactiver un tel transfert vers la destination syslog distante, puis le service syslog est redémarré.

   Si vous activez le transfert syslog, les logs du service configuré sont transmis au serveur syslog défini et le transfert se poursuit jusqu'à ce qu'il soit désactivé.

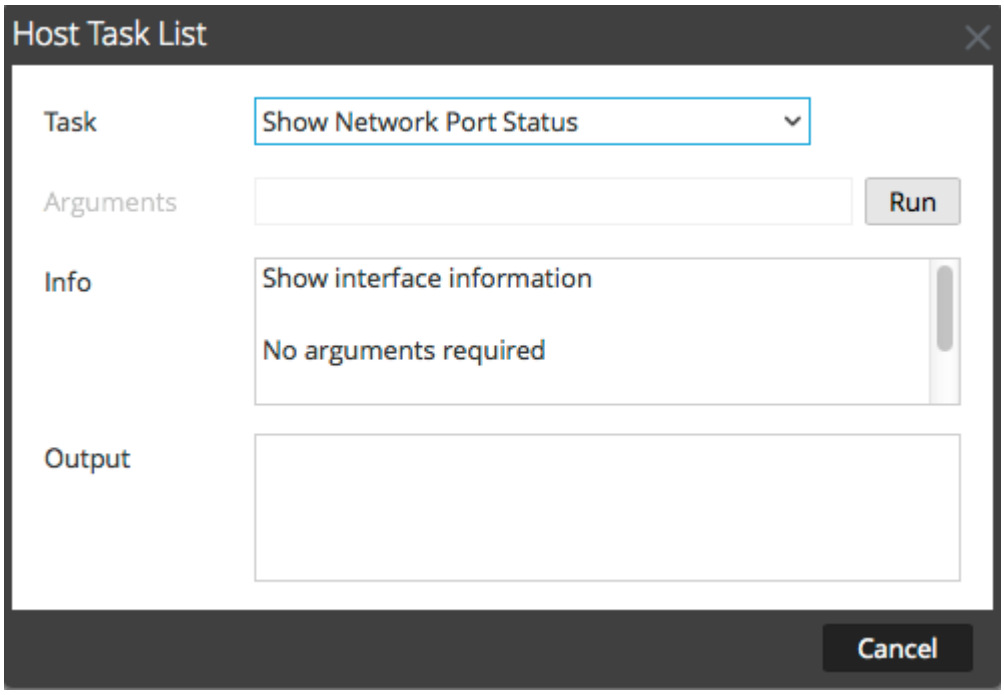
Note: Vous pouvez ensuite vous connecter au serveur syslog distant et vérifier si les messages reçus proviennent bien des
services Security Analytics configurés pour le transfert syslog.

Afficher l'état du port réseau

Dans la liste des tâches de l'hôte, la tâche Afficher l'état du port réseau indique l'état de tous les ports configurés sur l'hôte.

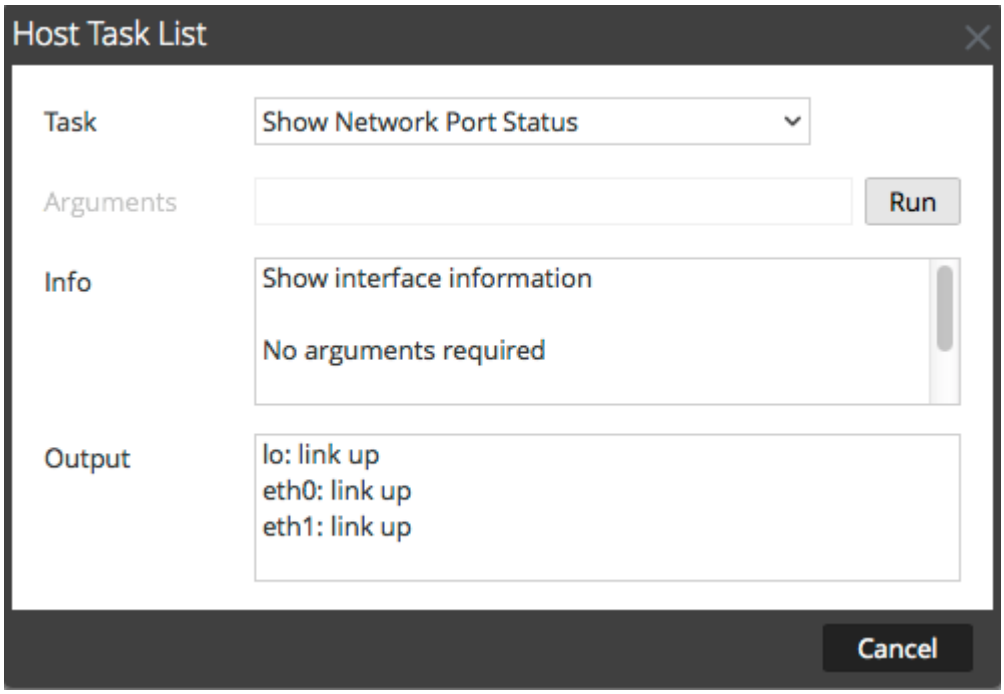
Afficher l'état du port réseau

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système pour le service sélectionné s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.
4. Dans la **Liste des tâches des hôtes**, cliquez sur **Afficher l'état du port réseau**.
   Cette tâche s'affiche dans le champ **Tâche**, et des informations sur la tâche s'affichent dans la zone **Info**.



5. Pour exécuter la tâche, cliquez sur **Exécuter**.
   L'état de chaque port sur l'hôte s'affiche dans la zone **Sortie**.

Last Modified: August 10 2016, 9:33AM

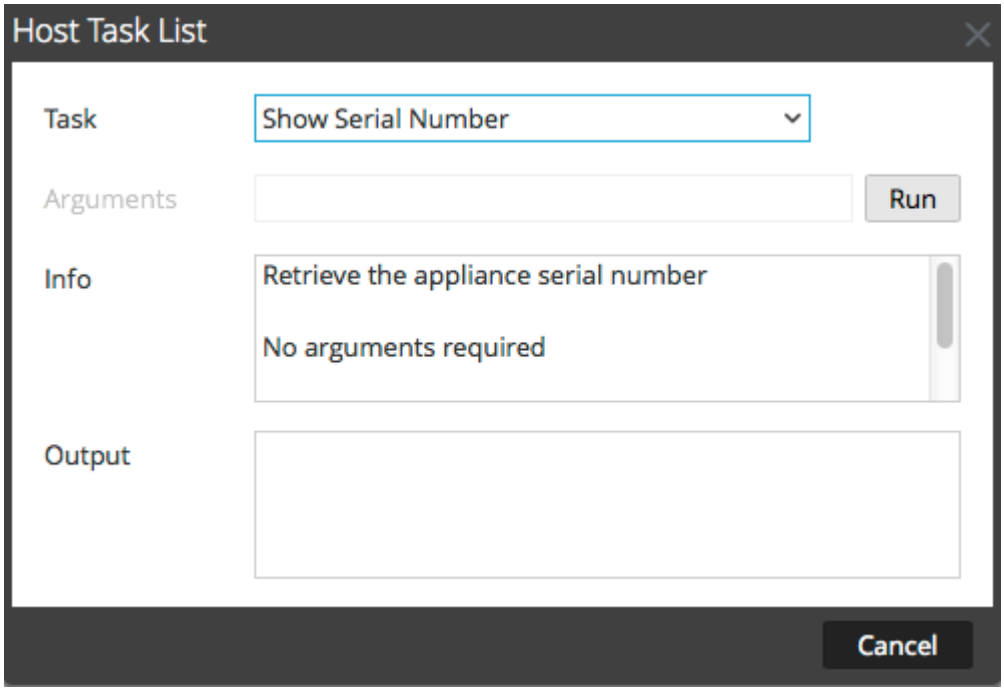


Afficher le numéro de série

La tâche Afficher le numéro de série de la Liste des tâches de l'hôte permet d'obtenir le numéro de série d'un hôte.

Afficher le numéro de série

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.
4. Dans la **Liste de tâches des hôtes**, sélectionnez **Afficher le numéro de série**.
5. Dans la zone **Info**, une brève explication de la tâche et des arguments de la tâche s'affiche.



6. Aucun argument n'est requis pour cette tâche. Cliquez sur **Exécuter**.
   Le numéro de série de l'hôte sélectionné s'affiche dans la zone **Sortie**.

Last Modified: August 10 2016, 9:33AM

Arrêter l'hôte

Dans certaines circonstances, par exemple lors d'une mise à niveau matérielle ou d'une coupure de courant prolongée dépassant la capacité électrique de secours, il peut être nécessaire d'arrêter un hôte physique. Lorsque vous arrêtez un hôte, tous les services exécutés sur cet hôte sont arrêtés et l'hôte physique s'éteint.

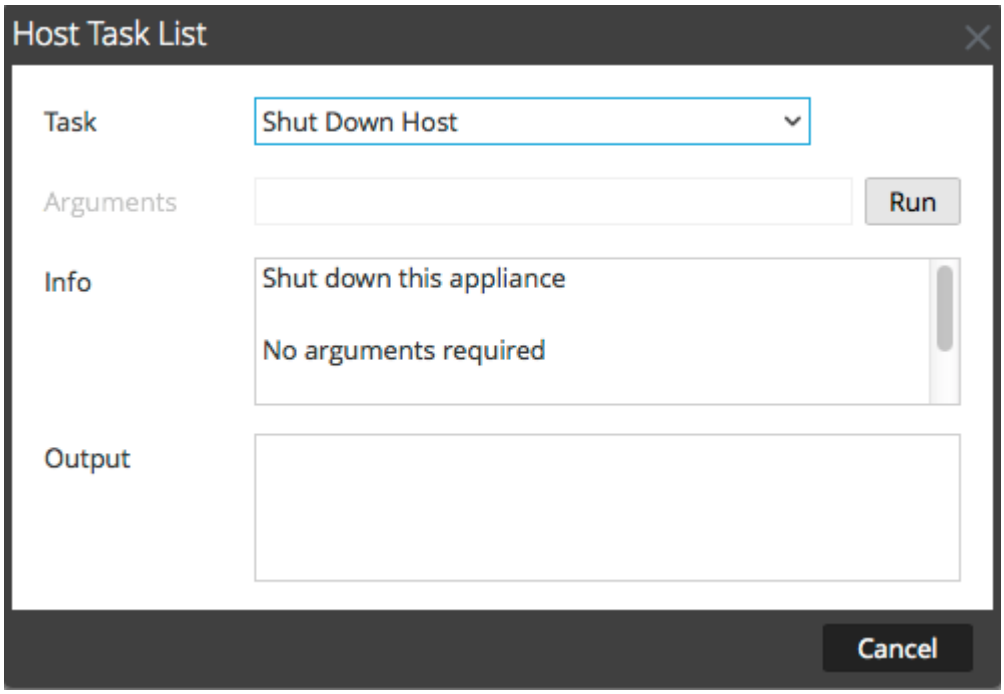
L'hôte physique ne redémarre pas automatiquement. et l'interrupteur électrique doit être utilisé pour le redémarrer. Une fois l'hôte physique redémarré, l'hôte et les services sont configurés pour redémarrer automatiquement.

Security Analytics propose d'autres options pour démarrer et arrêter un hôte sans arrêter l'hôte physique :

- Pour arrêter et redémarrer un hôte via un service rattaché, reportez-vous à Redémarrer un hôte.
- Pour arrêter et redémarrer un hôte à l'aide d'une tâche d'hôte, reportez-vous à Redémarrer un hôte.

Arrêter l'hôte physique

1. Dans la boîte de dialogue Liste de tâches des hôtes, sélectionnez **Arrêter l'hôte** dans le champ **Tâche**.



2. Pour exécuter la tâche, cliquez sur **Exécuter**.
   L'hôte s'arrête et l'hôte physique s'éteint.

Last Modified: August 10 2016, 9:33AM

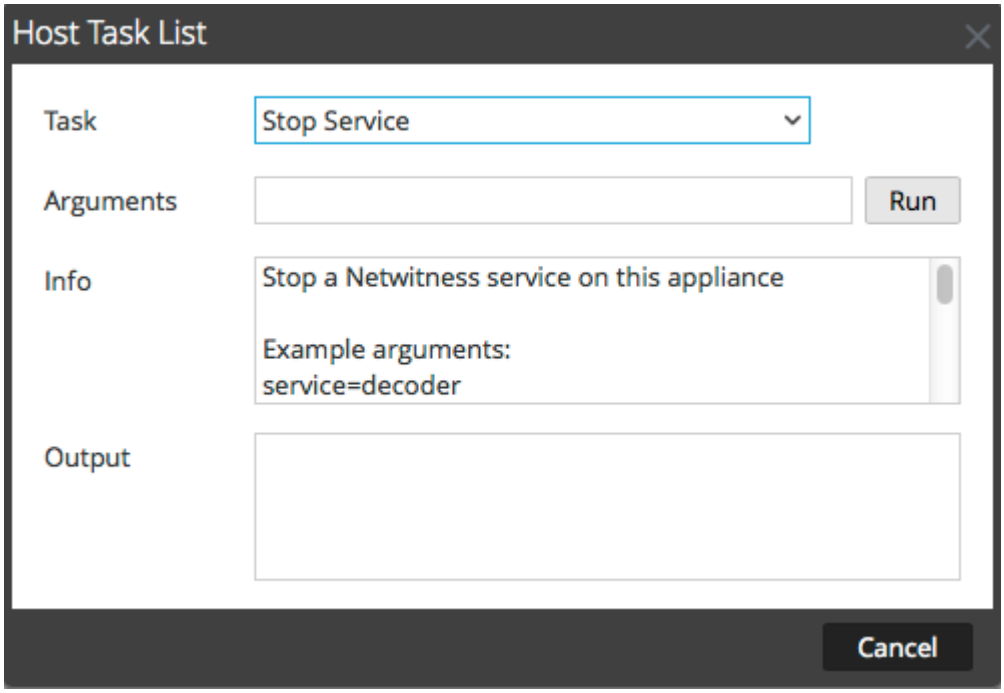
Arrêter et démarrer un service sur un hôte

La liste des tâches de l'hôte comporte deux options pour arrêter et démarrer un service sur un hôte. Lorsque vous arrêtez un service à l'aide du message **Arrêter le service**, tous les processus s'y rapportant sont arrêtés et les utilisateurs connectés au service sont déconnectés. À moins d'un problème avec le service, il redémarre automatiquement. Il en va de même avec l'option **Arrêter le service** de la vue Système de services.

Si un service ne redémarre pas automatiquement après son arrêt, vous pouvez le redémarrer manuellement à l'aide du message **Démarrer le service**.

Arrêter un service sur un hôte

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service et **> Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services**, cliquez sur **Tâches de l'hôte**.
4. Dans la **liste des tâches de l'hôte**, cliquez sur **Arrêter le service**.
   Cette tâche s'affiche dans le champ **Tâche**, et des informations sur la tâche s'affichent dans la zone **Info**.

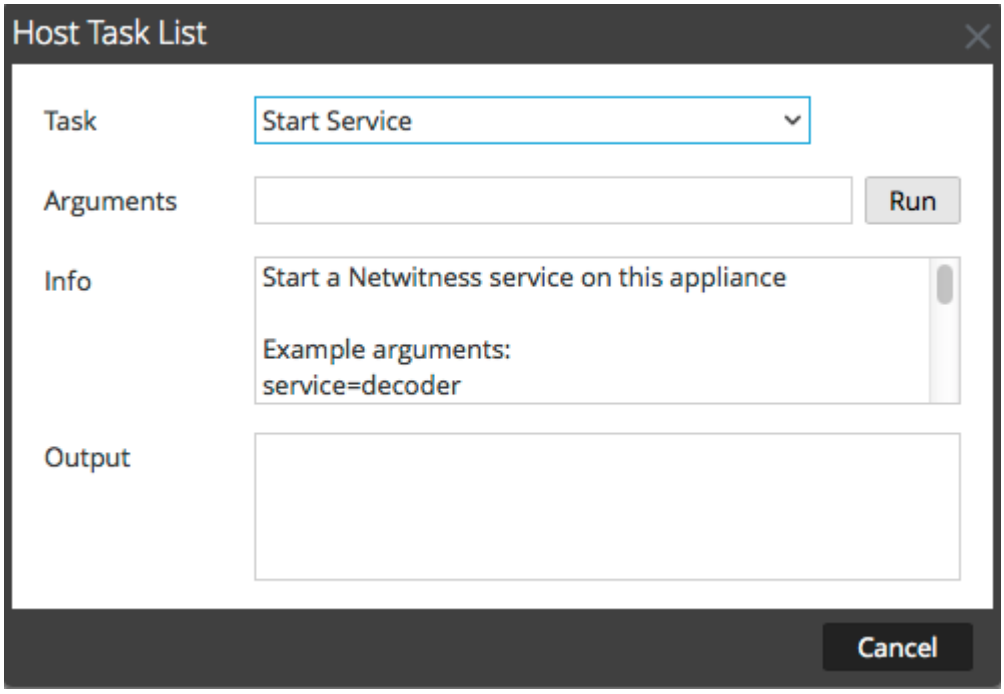


Last Modified: August 10 2016, 9:33AM

5. Dans le champ **Arguments**, spécifiez le service (decoder, concentrator, broker, logdecoder, logcollector) à arrêter. Par exemple,
service=decoder
6. Pour exécuter la tâche, cliquez sur **Exécuter**.
Le service s'arrête et son état s'affiche dans la zone **Sortie**. Tous les processus du service sont arrêtés et les utilisateurs connectés au service en sont déconnectés. À moins d'un problème avec le service, il redémarre automatiquement.

Démarrer un service sur un hôte

1. Dans la **liste des tâches de l'hôte**, cliquez sur **Démarrer le service**.
Cette tâche s'affiche dans le champ **Tâche**, et des informations sur la tâche s'affichent dans la zone **Info**.



2. Dans le champ **Arguments**, spécifiez le service (decoder, concentrator, broker, logdecoder, logcollector) à démarrer. Par exemple,
service=decoder
3. Pour exécuter la tâche, cliquez sur **Exécuter**.
Le service démarre et son état s'affiche dans la zone **Sortie**.

Procédures relatives aux services

Les procédures ci-dessous décrivent comment :

- Attribuer un accès et des autorisations à un service.
- Démarrer et arrêter un service.
- Examiner l'état de fonctionnement d'un service.

Last Modified: August 10 2016, 9:33AM

Ajouter, répliquer ou supprimer un utilisateur de service

Vous devez ajouter un utilisateur à un service pour :

- Agrégation
- Accéder au service avec le :
  - client Thick
  - API REST

Note: Cette rubrique ne s'applique pas aux utilisateurs qui accèdent aux services via l'interface utilisateur sur le serveur Security Analytics. Vous devez ajouter ces utilisateurs au système et non au service. Pour plus de détails, reportez-vous à la rubrique Configurer un utilisateur.

Pour chaque utilisateur du service, vous pouvez effectuer les opérations suivantes :

- Configurer les propriétés d'authentification utilisateur et les propriétés de gestion des requêtes pour le service.
- Attribuer un rôle de membre à l'utilisateur pour qu'il dispose des autorisations appropriées
- Répliquer le compte utilisateur sur d'autres services
- Changer le mot de passe utilisateur sur les services sélectionnés

La rubrique Modifier le mot de passe d'un utilisateur de service fournit les instructions permettant de modifier le mot de passe utilisateur dans les différents services.

Éléments à prendre en compte en matière de réplication et migration

Lors de la réplication d'un utilisateur à partir d'un service Security Analytics 10.5 ou version supérieure vers un service Security Analytics 10.4, Expiration du délai de la requête migre vers Niveau de requête selon le niveau le plus proche. Par exemple, si un utilisateur obtient un Délai d'expiration de la requête de 15 minutes, son Niveau de requête sera de 3 après la migration. Si un utilisateur obtient un Délai d'expiration de la requête de 35 minutes, son Niveau de requête sera de 2 après la migration. Si un utilisateur obtient un Délai d'expiration de la requête de 45 minutes, son Niveau de requête sera de 2 après la migration.

Lors de la migration ou réplication d'un utilisateur à partir d'un service Security Analytics 10.4 vers un service Security Analytics 10.5 ou version supérieure, le Niveau de requête migre vers le Délai d'expiration de la requête selon les définitions suivantes :

- Niveau de requête 1 = 60 minutes
- Niveau de requête 2 = 40 minutes
- Niveau de requête 3 = 20 minutes

Last Modified: August 10 2016, 9:33AM

Procédures

Accéder à la vue Sécurité

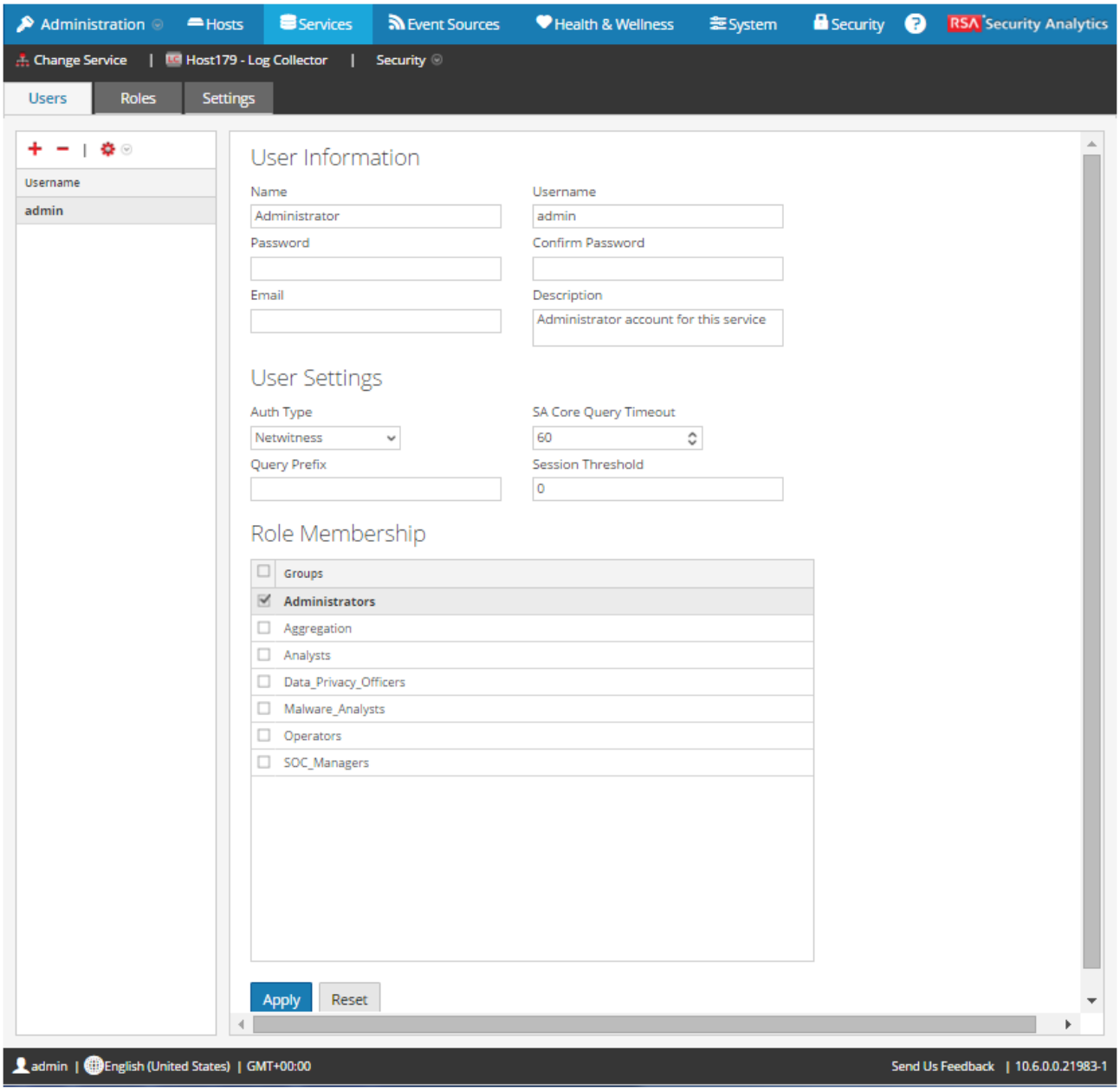
Chacune des procédures suivantes débute dans la vue Sécurité des services.

Pour accéder à la vue Sécurité des services :

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

Last Modified: August 10 2016, 9:33AM

2. Sélectionnez un service, puis **> Vue > Sécurité**.
   La vue Sécurité du service sélectionné s'affiche avec l'onglet Utilisateurs ouvert.



Note: Pour Security Analytics 10.4 et les versions de service antérieures, dans la section Paramètres utilisateur, le champ **Niveau de requête** s'affiche à la place de **Expiration du délai de requête de base QA**.

Ajouter un utilisateur de service

1. Dans l'onglet **Utilisateurs**, cliquez sur +.

2. Saisissez le nom d'utilisateur pour accéder au service, puis appuyez sur **Entrée**.
   La section Informations utilisateur affiche le nom d'utilisateur. Vous pouvez modifier le reste des champs.
3. Saisissez le mot de passe pour la connexion au service, dans les champs **Mot de passe** et **Confirmer le mot de passe**.
4. (Facultatif) Fournissez des informations complémentaires :
   - **Nom** pour la connexion à Security Analytics
   - **Adresse e-mail**
   - **Description** de l'utilisateur
5. Dans la section Paramètres utilisateur, procédez comme suit :
   - **Type d'authentification**
     - Si Security Analytics authentifie l'utilisateur, sélectionnez Netwitness.
     - Si Active Directory ou le module PAM est configuré sur le serveur Security Analytics pour authentifier l'utilisateur, sélectionnez Externe.

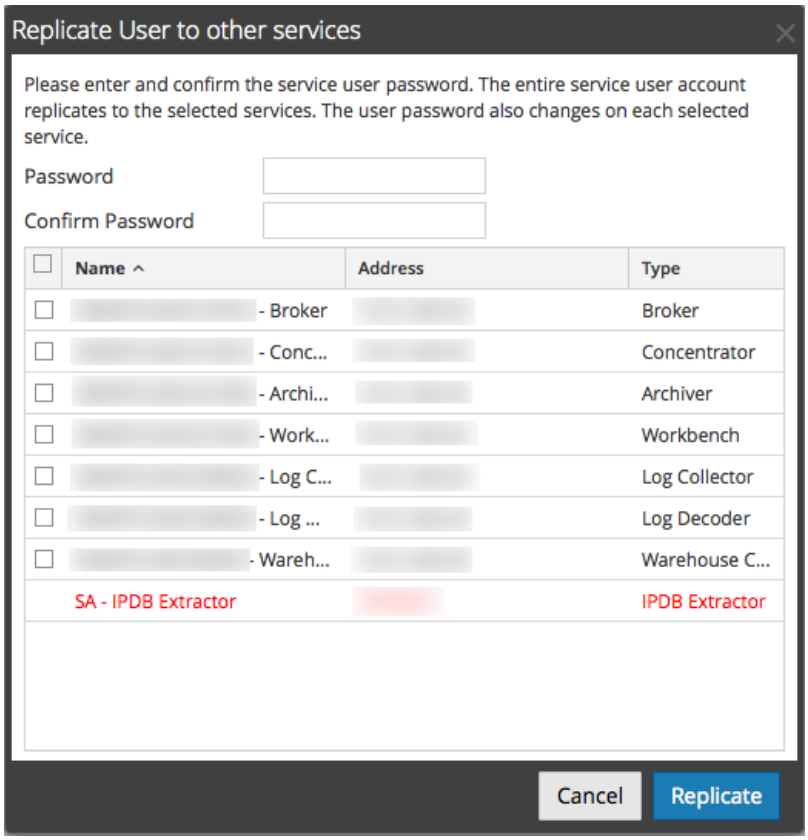
Note: Dans les versions 10.4 et ultérieures, les connexions fiables rendent inutile la configuration des comptes utilisateur externes sur le service. Toute la configuration externe est centralisée sur le serveur Security Analytics.

   - **Expiration du délai de requête de base QA** est le nombre maximal de minutes qu'un utilisateur peut utiliser pour exécuter une requête sur le service. Ce champ s'applique à Security Analytics 10.5 et versions de service supérieures et il ne s'affiche pas pour 10.4 et versions antérieures.
   - **Niveau de requête** est le nombre maximal de minutes autorisé à un utilisateur pour réaliser une requête sur un service. Il existe trois niveaux de requête : 1, 2 et 3. Ce champ s'applique à Security Analytics 10.4 et aux versions de service antérieures. Il ne s'affiche pas pour la version 10.5 et toute version ultérieure du service.
6. (Facultatif) Spécifier des critères de requête :
   - Le **Préfixe de requête** permet de filtrer les requêtes. Saisissez un préfixe pour restreindre les résultats visibles par l'utilisateur.
   - Le **Seuil de sessions** contrôle la façon dont le service analyse les métavaleurs pour déterminer le décompte des sessions. Toute métavaleur avec un nombre de sessions supérieur au seuil établi arrête sa détermination du véritable nombre de sessions.
7. Dans la section **Adhésion aux rôles**, sélectionnez chaque rôle à attribuer à l'utilisateur. Si un utilisateur est membre d'un rôle sur un service, il bénéficiera des autorisations attribuées au rôle.
8. Pour activer le nouvel utilisateur du service, cliquez sur **Appliquer**.

L'utilisateur est ajouté au service immédiatement.

Répliquer un utilisateur à d'autres services

1. Sous l'onglet Utilisateurs, sélectionnez un utilisateur, puis **> Répliquer**.
   La boîte de dialogue Répliquer l'utilisateur sur les autres services s'affiche.



2. Saisissez le **mot de passe** de l'utilisateur, puis confirmez-le.
3. Sélectionnez chaque service auquel vous répliquez l'utilisateur.
4. Cliquez sur **Répliquer**.

Le compte utilisateur est ajouté à chaque service sélectionné.

Supprimer un utilisateur de service

1. Sous l'onglet **Utilisateurs**, sélectionnez le **nom d'utilisateur**, puis cliquez sur .
   Security Analytics vous demande de confirmer que vous souhaitez supprimer l'utilisateur sélectionné.
2. Pour confirmer, cliquez sur **Oui**.

L'utilisateur est supprimé du service immédiatement.

Last Modified: August 10 2016, 9:33AM

Ajouter un Rôle d'utilisateur de service

Dans Security Analytics, des rôles préconfigurés sont installés sur le serveur et sur chaque service. Vous pouvez également ajouter des rôles personnalisés. Le tableau suivant répertorie les rôles système préconfigurés ainsi que les autorisations qui leur sont associées.

Rôle	Autorisation
Administrateurs	Accès complet au système
Opérateurs	Accès aux configurations mais pas au contenu méta et de session
Analystes	Accès au contenu méta et de session mais pas aux configurations
Responsables du SOC	Même accès que les Analystes avec des autorisations supplémentaires pour gérer les incidents
Analystes du malware	Accès aux événements de malware et au contenu méta et de session
Spécialistes de la confidentialité des données	Accès au contenu méta et de session ainsi qu'aux options de configuration qui gèrent l'obscurcissement et l'affichage des données sensibles dans le système (voir Gestion de la confidentialité des données).

Vous devez ajouter un rôle de service si vous avez ajouté l'un des éléments suivants :

- Utilisateurs ou utilisateur du **Service** qui requièrent un nouvel ensemble d'autorisations.
- **Rôle personnalisé sur le serveur Security Analytics** car les connexions approuvées requièrent que le même rôle personnalisé existe à la fois sur le serveur et sur chaque service auquel aura accès le rôle personnalisé. Les noms doivent être identiques. Par exemple, si vous ajoutez un rôle Analystesjuniors sur le serveur, vous devez également ajouter ce rôle sur chacun des services auxquels le rôle accédera. Pour plus d'informations, reportez-vous à la rubrique Ajouter un rôle et attribuer des autorisations.

Il existe également un rôle de service préconfiguré intitulé **Agrégation**. Le rôle Agrégation et les rôles et autorisations d'utilisateurs de service fournissent des informations complémentaires.

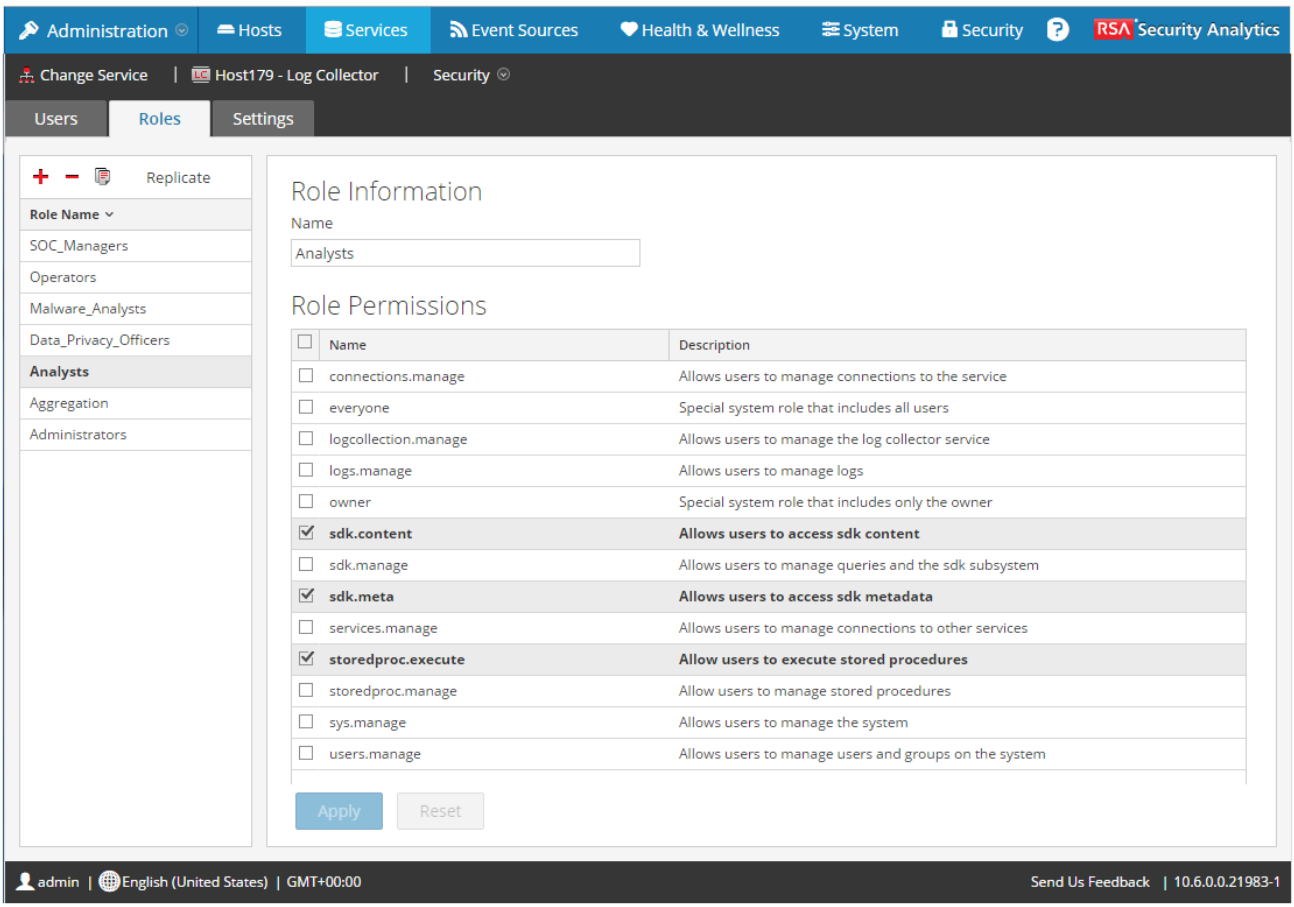
Procédure

Pour ajouter un rôle d'utilisateur de service et y associer des autorisations :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis  **> Vue > Sécurité**.
   La vue Sécurité du service sélectionné s'affiche avec l'onglet Utilisateurs ouvert.

Last Modified: August 10 2016, 9:33AM

3. Sélectionnez l'onglet **Rôles**, puis cliquez sur +.
   La vue Sécurité des services qui s'affiche indique les cinq rôles préconfigurés.



4. Cliquez sur +, saisissez le **nom du rôle** et appuyez sur la touche **Entrée**.
   Le nom du rôle s'affiche au-dessus de la liste des **autorisations de rôle**.
5. Sélectionnez chacune des autorisations dont disposera le rôle sur le service.
6. Cliquez sur **Appliquer**.

Le rôle est ajouté au service immédiatement. Vous pouvez y ajouter des utilisateurs de services sous l'onglet **Utilisateurs**.

Modifier le mot de passe d'un utilisateur de service

Cette procédure permet aux administrateurs de modifier le mot de passe d'un utilisateur de service et de répliquer le nouveau mot de passe sur tous les services principaux pour lesquels ce compte utilisateur est défini. Seule la modification du mot de passe est répliquée sur les services principaux sélectionnés. Le compte utilisateur intégral n'est pas répliqué. Les administrateurs peuvent également modifier le mot de passe du compte **admin** sur les services principaux.

Note: L'option Modifier le mot de passe ne s'applique pas aux utilisateurs externes.

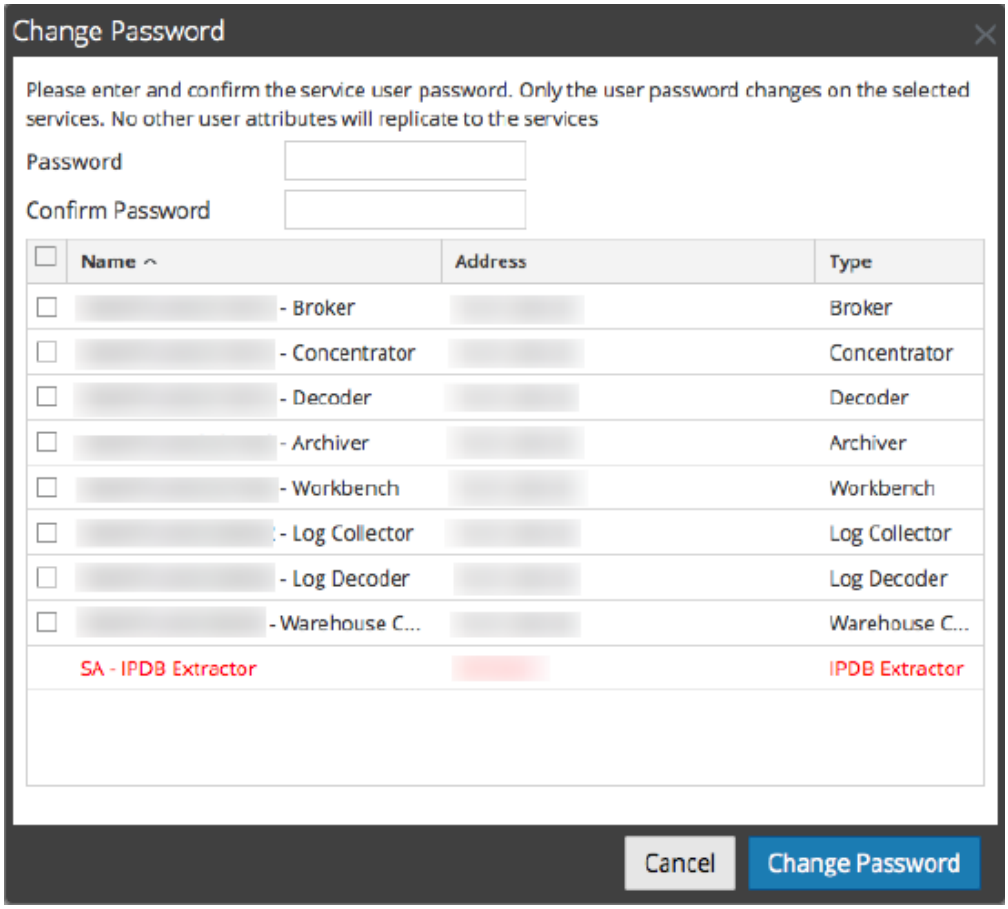
Procédure

Pour modifier le mot de passe d'un utilisateur de service :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services d'administration s'affiche.
2. Sélectionnez un service, puis cliquez sur  **> Vue > Sécurité**.
   La vue Sécurité s'affiche pour les services sélectionnés.

Last Modified: August 10 2016, 9:33AM

3. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur et cliquez sur  **> Modifier le mot de passe**.
   La boîte de dialogue **Modifier le mot de passe** s'affiche.



4. Saisissez un nouveau mot de passe pour l'utilisateur et confirmez ce mot de passe.
5. Sélectionnez les services pour lesquels vous souhaitez modifier le mot de passe.
6. Cliquez sur **Modifier le mot de passe**.
   L'état de modification du mot de passe sur les services sélectionnés s'affiche.

RSA

Créer et gérer des groupes de services

La vue Administration - Services fournit les options permettant de créer et de gérer les groupes de services. Le panneau Services inclut les options de création, de modification et de suppression des groupes de services. Lorsque les groupes sont créés, vous pouvez faire glisser des services individuels du panneau Services vers un groupe.

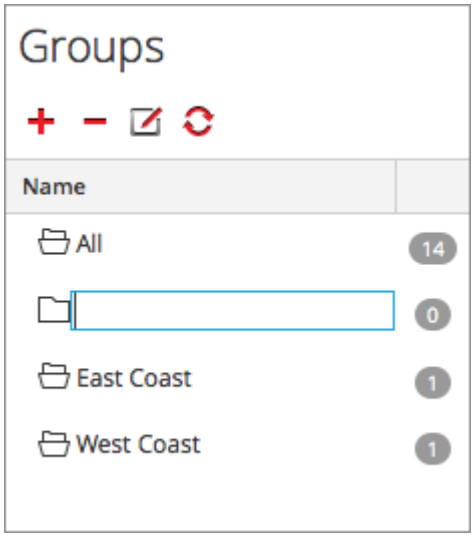
Les groupes peuvent refléter de manière utile une logique de fonctions, de géographie, de projets ou d'organisation. Un service peut appartenir à plusieurs groupes. Voici quelques exemples de regroupements possibles.

- Regroupement des différents types de services pour faciliter la configuration et la surveillance de tous les services Broker, Decoder ou Concentrator.
- Regroupement des services faisant partie du même flux de données ; par exemple, un service Broker et tous les services Concentrator et Decoder associés.
- Regroupement des services en fonction de leur région géographique et de leur emplacement au sein de la région. Si une importante panne d'alimentation se produit à un emplacement, les services susceptibles d'être touchés sont facilement identifiables.

Créer un groupe

1. Dans **Security Analytics menu**, sélectionnez **Administration >Services**.
   La vue Services d'administration s'affiche.

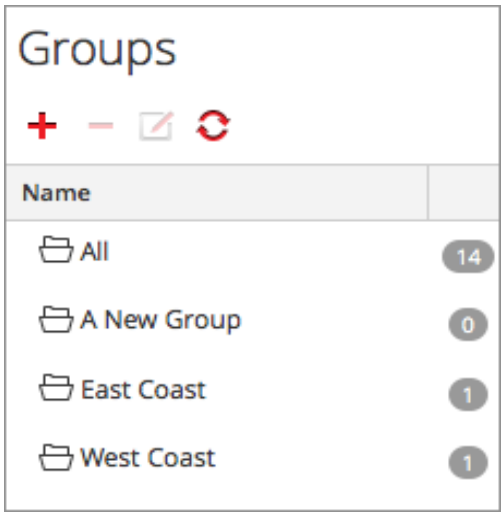
2. Dans la barre d'outils du panneau **Groupes**, cliquez sur +.
   Le curseur clignote dans le champ du nouveau groupe qui s'ouvre.



3. Saisissez le nom du nouveau groupe dans le champ (par exemple, **Nouveau groupe**) et appuyez sur **Entrée**.
   Le groupe est créé sous forme de dossier dans l'arborescence. Le nombre en regard du groupe indique le nombre de services

Last Modified: August 10 2016, 9:33AM

contenus dans ce groupe.



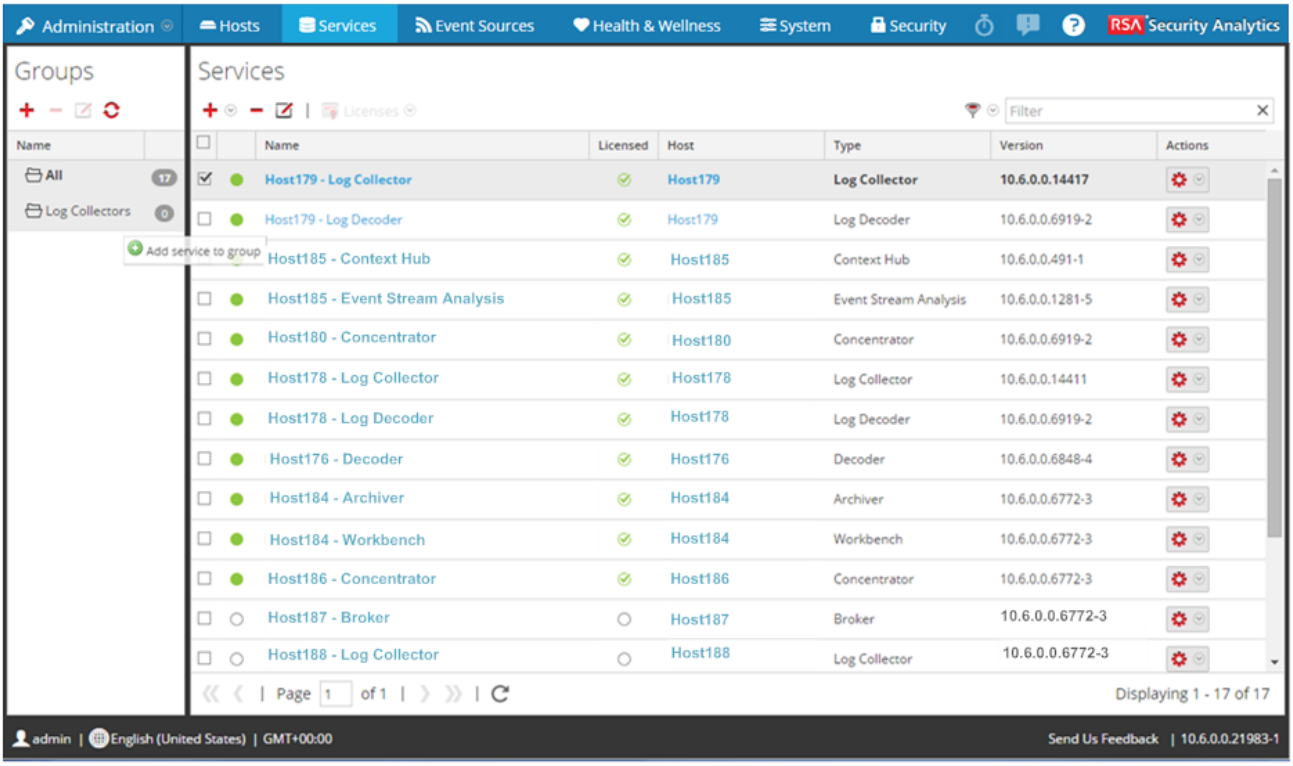
Modifier le nom d'un groupe

1. Dans la vue Services **panneau Groupes**, double-cliquez sur le nom du groupe ou sélectionnez le groupe, puis cliquez sur .
   Le curseur clignote dans le champ du nom qui s'ouvre.
2. Saisissez le nouveau nom du groupe et appuyez sur **Entrée**.
   Le champ du nom se ferme et le nouveau nom de groupe s'affiche dans l'arborescence.

Ajouter un service à un groupe

Dans la vue Services **panneau Services**, sélectionnez un service et faitesle glisser vers un dossier de groupe dans le panneau Groupes, par exemple **Log Collectors**.

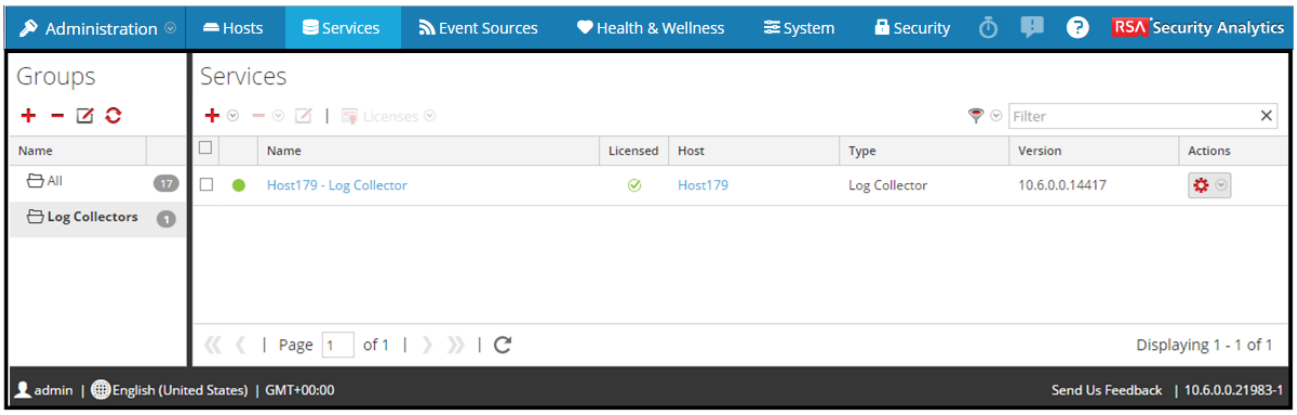
Last Modified: August 10 2016, 9:33AM



Le service est ajouté au groupe.

Afficher les services dans un groupe

Pour afficher les services dans un groupe, cliquez sur le groupe sous le panneau **Groupes**.
Le panneau **Services** affiche les services contenus dans ce groupe.



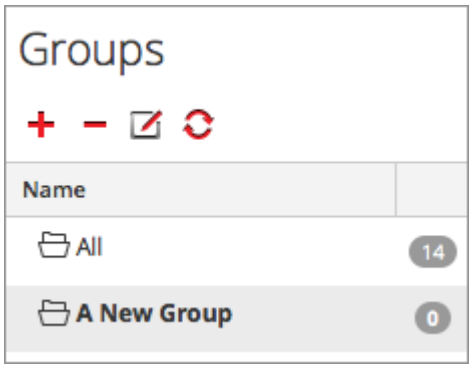
Supprimer un service d'un groupe

1. Dans la vue Services **panneau Groupe**, sélectionnez le groupe qui contient le service que vous souhaitez supprimer. Les services de ce groupe s'affichent dans le panneau Services.

Last Modified: August 10 2016, 9:33AM

2. Dans le **panneau Services**, sélectionnez un ou plusieurs services que vous souhaitez supprimer du groupe, et dans la barre d'outils, sélectionnez **> Supprimer du groupe**.
   Les services sélectionnés sont supprimés du groupe, mais ne sont pas retirés de l'interface utilisateur Security Analytics. Le nombre de services dans le groupe, qui apparaît dans le nom du groupe, se réduit en fonction des services retirés du groupe. Le groupe **Tous** contient les services qui ont été supprimés du groupe.

   Dans l'exemple suivant, le groupe de services nommé **Nouveau groupe** ne contient plus de services, puisque le service figurant dans ce groupe a été supprimé.



Supprimer un groupe

1. Dans la vue Services **panneau Groupes**, sélectionnez le groupe que vous souhaitez supprimer.

2. Cliquez sur .
   Le groupe sélectionné est supprimé du panneau Groupes. Les services qui figuraient dans le groupe ne sont pas retirés de l'interface utilisateur Security Analytics. Le groupe **Tous** contient les services du groupe supprimé.

Dupliquer ou répliquer un rôle de service

Un moyen efficace d'ajouter un nouveau rôle de service est de dupliquer un rôle similaire, de l'enregistrer sous un nouveau nom et de réviser les autorisations qui sont déjà attribuées. Par exemple, vous pouvez dupliquer le rôle des analystes. Puis l'enregistrer comme JuniorAnalysts et modifier les autorisations.

Répliquer un rôle est un moyen rapide d'ajouter un rôle existant à d'autres services. Par exemple, vous pouvez répliquer le rôle des JuniorAnalysts qui existe sur un broker vers un concentrator et un log decoder.

Chacune des procédures suivantes débute dans la vue Sécurité des services.

Pour accéder à la vue Sécurité des services :

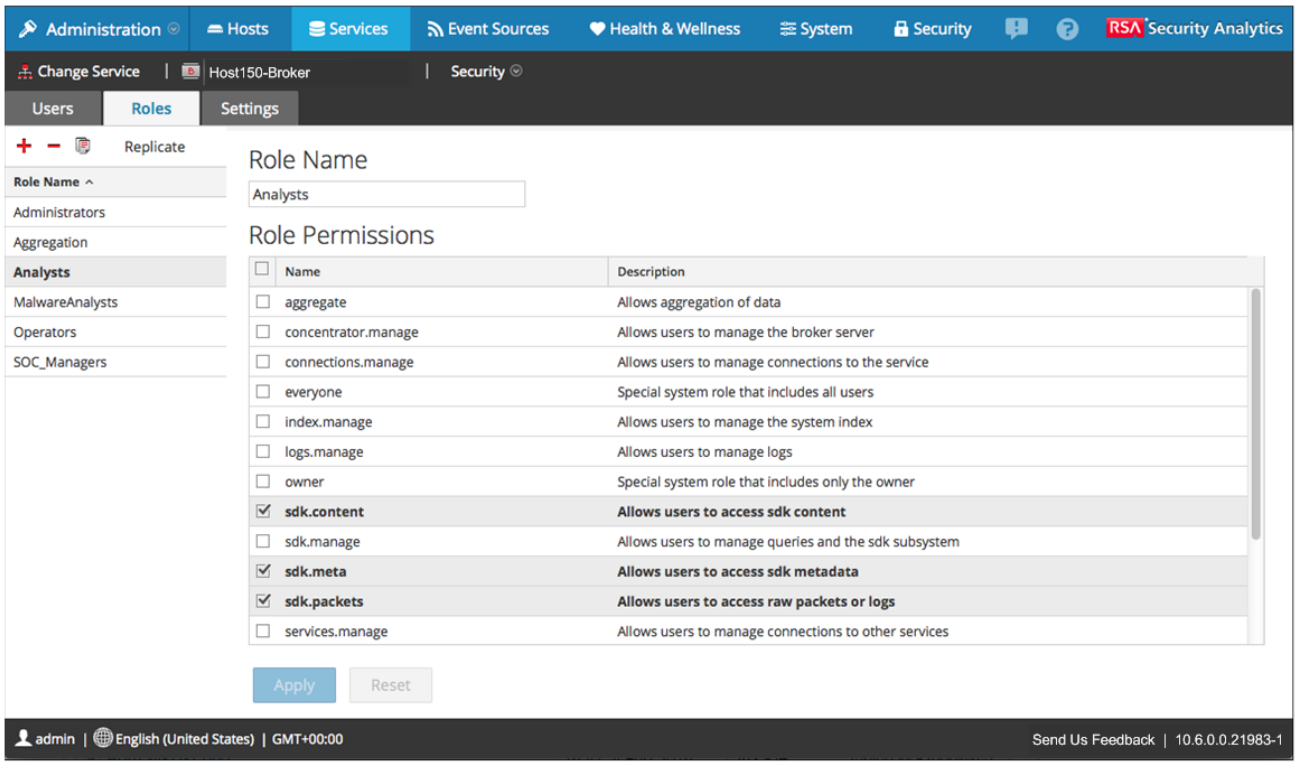
1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis  **> Vue > Sécurité**.
   La vue Sécurité du service sélectionné s'affiche avec l'onglet Utilisateurs ouvert.
3. Sélectionnez l'onglet **Rôles**.

Procédures

Last Modified: August 10 2016, 9:33AM

Dupliquer un rôle de service

1. Sous l'onglet Rôles, sélectionnez le rôle que vous voulez dupliquer.



2. Cliquez sur **Dupliquer le rôle.**
3. Saisissez un nom et cliquez sur **Enregistrer**.
4. Sélectionnez le nouveau rôle.
5. Dans la section **Autorisations du rôle**, sélectionnez ou désélectionnez des autorisations pour modifier ce que le nouveau rôle peut faire.

Le rôle dupliqué est ajouté au service immédiatement.

Répliquer un rôle

1. Sous l'onglet Rôles, sélectionnez le rôle que vous voulez répliquer et cliquez sur **Répliquer**.
2. Dans la boîte de dialogue **Répliquer le rôle sur les autres services**, sélectionnez chaque service sur lequel vous souhaitez ajouter le rôle.
3. Cliquez sur **Répliquer**.

Le rôle répliqué est ajouté à chaque service sélectionné immédiatement.

Modifier les fichiers de configuration de service Core

Les fichiers de configuration des services --Decoder, Log Decoder, Broker, Concentrator, Archiver et Workbench-- sont modifiables au format de fichier texte. La vue Configuration des services > onglet Fichiers vous permet d'effectuer les opérations suivantes :

- Afficher et modifier un fichier de configuration de service en cours d'utilisation par le système Security Analytics.
- Récupérer et restaurer la dernière sauvegarde du fichier que vous modifiez.
- Transmettre le fichier ouvert aux autres services.
- Enregistrer les modifications effectuées dans un fichier.

Les fichiers qu'il est possible de modifier dépendent du type de service en cours de configuration. Les fichiers communs à tous les services Core sont :

- le fichier d'index du service ;
- le fichier Netwitness ;
- le fichier du rapporteur d'incidents ;
- le fichier du planificateur.

De plus, le Decoder dispose de fichiers qui permettent de configurer les parsers et les définitions de feed. Il dispose également d'un adaptateur de réseau local sans fil.

Note: Les valeurs par défaut de ces fichiers de configuration sont généralement adaptées aux situations les plus courantes. Toutefois, il est nécessaire de les modifier en partie pour les services facultatifs, comme le rapporteur d'incidents ou le planificateur. Seuls les administrateurs disposant d'une bonne compréhension des réseaux et des facteurs qui affectent la façon dont les services collectent et analysent les données devraient apporter des modifications à ces fichiers sous l'onglet Fichiers.

Pour plus de détails sur les paramètres de configuration des services, reportez-vous à la rubrique Paramètres de configuration des services.

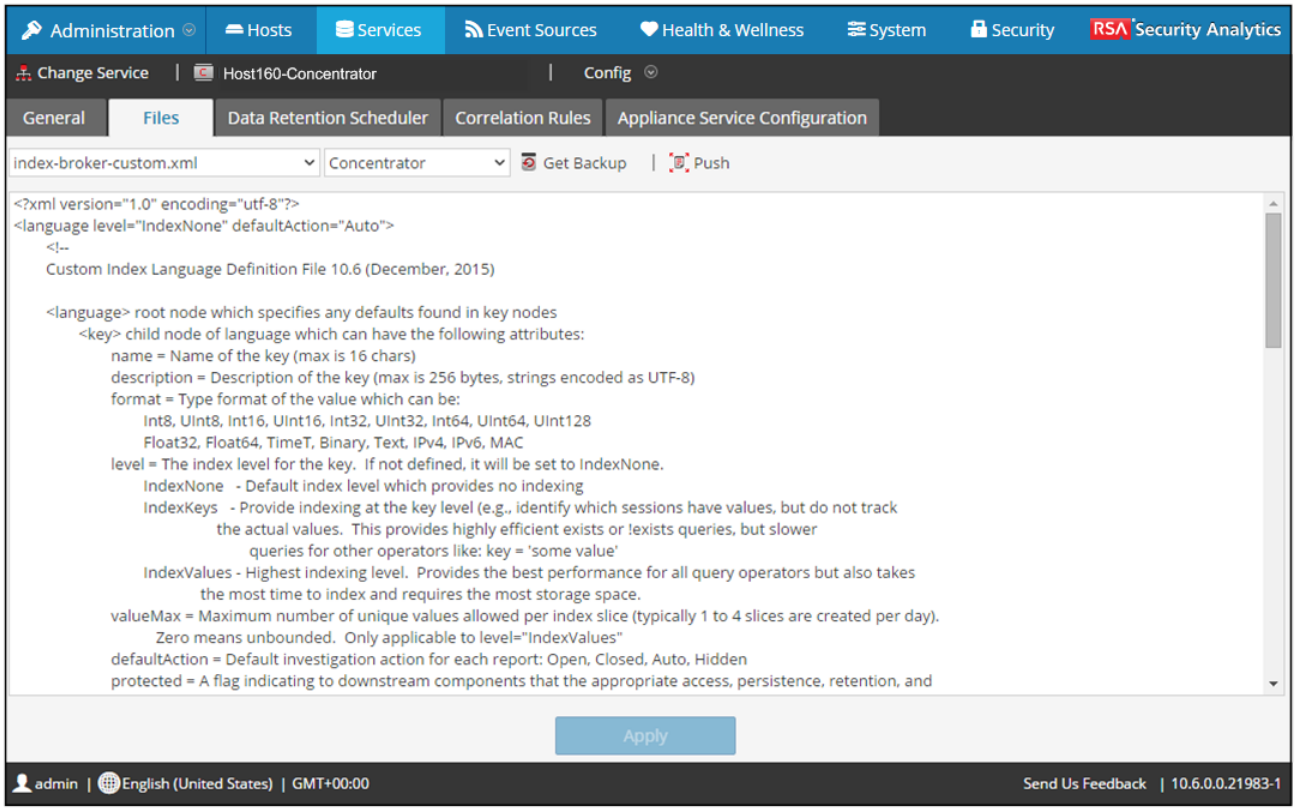
Modifier un fichier de configuration de service

Pour modifier un fichier :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la Grille des services, sélectionnez un service.
3. Sélectionnez  **> Vue > Config**.
   La vue Configuration des services s'ouvre sur l'onglet Général.

Last Modified: August 10 2016, 9:33AM

4. Cliquez sur l'onglet **Fichiers**.
   Le service sélectionné tel que Concentrator apparaît dans la liste déroulante à droite de l'écran.
5. (Facultatif) Pour modifier un fichier relatif à l'hôte au lieu du service, sélectionnez **Hôte** dans la liste déroulante.
6. Choisissez un fichier dans la liste déroulante **Sélectionnez un fichier à modifier**.
   Le contenu du fichier s'affiche en mode modification.



7. Modifiez le fichier et cliquez sur **Enregistrer**.

Le fichier actuel est remplacé et un fichier de sauvegarde est créé. Les modifications prennent effet après le redémarrage du service.

Restaurer la version de sauvegarde d'un fichier de configuration de service

Après avoir effectué les modifications dans un fichier de configuration, enregistrez-le, puis redémarrez le service. Un fichier de sauvegarde devient alors disponible. Pour restaurer la sauvegarde d'un fichier de configuration :

1. Pour sélectionner un fichier de configuration, suivez les étapes 1 à 6 de la procédure précédente.
2. Cliquez sur Get Backup.
   Le fichier de sauvegarde s'ouvre dans l'éditeur de texte.
3. Pour restaurer la version de sauvegarde, cliquez sur **Enregistrer**.

Les modifications prennent effet après le redémarrage du service.

Last Modified: August 10 2016, 9:33AM

Transmettre un fichier de configuration à d'autres services.

Une fois que vous avez modifié un fichier de configuration de service, vous pouvez transmettre la même configuration à d'autres services du même type.

1. Pour sélectionner un fichier de configuration, suivez les étapes 1 à 6 de la première procédure.
2. Cliquez sur 

. La boîte de dialogue Sélectionner des services s'affiche.
3. Sélectionnez les services pour lesquels le fichier de configuration doit être appliqué.
   Chaque service doit être du même type que celui sélectionné dans la vue Services.

> ⚠ **Caution:** Si vous décidez de ne pas transmettre le fichier de configuration, cliquez sur **Annuler**.

4. Pour appliquer le fichier de configuration à tous les services, cliquez sur **OK**.

Le fichier de configuration est transmis à tous les services sélectionnés.

Last Modified: August 10 2016, 9:33AM

RSA

Configurer le Planificateur de tâches

Le fichier du planificateur

L'un des fichiers disponibles pour modification dans la vue Configuration des services > onglet Fichiers est **le planificateur.** Ce fichier configure le planificateur de tâche intégré pour un service. Le planificateur de tâche peut automatiquement envoyer des messages à des intervalles prédéfinis ou à des heures spécifiques de la journée.

Syntaxe de tâche du planificateur

Une ligne de tâche dans le fichier du planificateur se compose de la syntaxe suivante, où **<Value>** ne comporte pas d'espace :

```
<ParamName>=<Value>
```

si **<Value>** comporte des espaces, la syntaxe est la suivante :

```
<ParamName>="<Value>"
```

Dans chaque ligne de tâche, ces instructions s'appliquent :

- Le paramètre **time** ou l'un des paramètres d'intervalle (**seconds**, **minutes** ou **hours**) est atteint.
- Insérez un caractère d'échappement devant les caractères spéciaux à l'aide de **** (slash inversé).

Paramètres de ligne de tâche

Les paramètres de ligne de tâche suivants sont acceptés par le planificateur.

Syntaxe	Description
daysOfWeek : <string, optional, {enum-any:sun|mon|tue|wed|thu|fri|sat|all}>	Jours de la semaine pour exécuter une tâche. La valeur par défaut est **all**.
deleteOnFinish : <bool, optional>	Supprimez la tâche une fois qu'elle est bien terminée.
hours : <uint32, optional, {range:1 to 8760}>	Nombre d'heures entre les exécutions.
logOutput : <chaîne, facultatif>	Sort la réponse à consigner avec le nom de module spécifié.
minutes : <uint32, optional, {range:1 to 525948}>	Nombre de minutes entre les exécutions.

Last Modified: August 10 2016, 9:33AM

Syntaxe	Description
msg : <chaîne>	Message pour envoyer le nœud.
params : <chaîne, facultatif>	Paramètres du message.
pathname : <chaîne>	Chemin du nœud qui reçoit le message.
seconds : <uint32, optional, {range:1 to 31556926}>	Nombre de secondes entre les exécutions.
time : <chaîne>	Heure de l'exécution au format HH::MM:SS (heure locale de ce serveur).
timesToRun : <uint32, optional>	Nombre d'exécutions depuis le début du service, **0** = illimité (par défaut).

Messages

Les éléments ci-dessous sont les chaînes de message à utiliser dans le paramètre **msg** du planificateur de tâche.

Message	Description
addInter	Ajoutez une tâche à exécuter à intervalles réguliers. Par exemple, ce message exécute la commande **/index save** toutes les 6 heures : addInter hours=6 pathname=/index msg=save
addMil	Ajoutez une tâche à exécuter à une heure spécifique de la journée ou des journées de la semaine. Par exemple, ce message exécute la commande **/index save** à 13 h 00 tous les jours ouvrés : addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri
delSched	Supprime une tâche planifiée existante. Le paramètre **id** de la tâche doit être récupéré à partir du message d'impression.
print	Imprime toutes les tâches planifiées.
replace	Attribuez toutes les tâches planifiées dans un message, en supprimant toutes les tâches existantes.
save	Indiquer un nœud à enregistrer

Ligne de tâche d'échantillon

L'exemple de ligne de tâche suivant dans le fichier du planificateur télécharge le fichier du package feeds (**feeds.zip**) sur le Decoder sélectionné toutes les 120 minutes à partir du serveur hôte feeds :

```
minutes=120 pathname=/parsers msg=feed params="type\=wget file\=http://feedshost/nwlive/feeds.zip"
```


Last Modified: August 10 2016, 9:33AM

RSA

Modifier un fichier d'index de service

Cette rubrique fournit des informations et des instructions importantes pour la configuration des fichiers d'index personnalisés relatifs aux services, qui sont modifiables dans la vue Configuration des services > onglet Fichiers.

Le fichier d'index, associé aux autres fichiers de configuration, contrôle le fonctionnement de chaque service de base. L'accès au fichier d'index dans la vue Configuration des services dans Security Analytics ouvre le fichier dans un éditeur de texte, où vous pouvez modifier le fichier.

Note: Seuls les administrateurs avec une compréhension approfondie et complète de la configuration des services Core sont qualifiés pour modifier un fichier d'index, qui est l'un des fichiers de configuration de base pour le service Appliance. Les modifications apportées doivent être cohérentes dans tous les services de base. Des entrées non valides ou un fichier mal configuré peuvent empêcher le démarrage du système et nécessiter l'assistance du Support RSA pour rétablir l'état de fonctionnement du système.

Voici les fichiers d'index :

- **index-broker.xml**, **index-broker-custom.xml**
- **index-concentrator.xml**, **index-concentrator-custom.xml**
- **index-decoder.xml**, **index-decoder-custom.xml**
- **index-logdecoder.xml**, **index-logdecoder-custom.xml**
- **index-archiver.xml**, **index-archiver-custom.xml**
- **index-workbench.xml**, et **index-workbench-custom.xml**

Fichiers d'index et fichiers d'index personnalisés

Toutes les modifications concernant un index spécifique à un client sont effectuées dans le fichier **index-<service>-custom.xml**. Ce fichier remplace les paramètres contenus dans le fichier **index-<service>.xml**, qui est exclusivement contrôlé par RSA.

Note: Les clients utilisant les versions antérieures à la version 10.1 de Security Analytics devaient personnaliser les fichiers d'index en modifiant et enregistrant le fichier d'index. Cette méthode reposait sur Security Analytics pour la création d'une sauvegarde du fichier d'index en cours lors du redémarrage du service. Grâce à ce processus, le fichier en cours est remplacé et un fichier de sauvegarde est créé. L'option de barre d'outils fournit un moyen de revenir à une version de sauvegarde du fichier d'index.
Lors des mises à niveau logicielles, le fichier **index-<service>.xml** n'est pas conservé, car il est remplacé par les modifications apportées par l'équipe chargée de la gestion du contenu RSA. Toutefois, une sauvegarde

Last Modified: August 10 2016, 9:33AM

est faite dans le même répertoire et nommée **index-<service>.xml.rpm_pre_save**. Le fichier **index-<service>.xml.rpm_pre_save** peut être référencé si nécessaire pour créer le fichier **index-<service>-custom.xml** spécifique au client, qui ne doit être effectué qu'une seule fois. Par la suite, le nouveau système a permis à RSA d'effectuer des changements d'index sans modifier les changements personnalisés existants.

Le fichier d'index personnalisé, **index-<service>-custom.xml**, permet de créer des définitions ou remplacements personnalisés de vos propres clés de langue qui ne sont pas écrasées lors du processus de mise à niveau.

- Les clés qui sont définies dans le fichier **index-<service>-custom.xml** remplacent les définitions trouvées dans le fichier **index--<service>.xml**.
- Les clés qui sont ajoutées au fichier **index-<service>-custom.xml** et qui ne figurent pas dans le fichier **index-<service>.xml** sont ajoutées à la langue comme une nouvelle clé.

Voici les quelques applications communes pour la modification du fichier d'index :

- Ajouter de nouvelles clés méta personnalisées pour ajouter de nouveaux champs à l'interface utilisateur Security Analytics
- Configurer les clés méta protégées dans le cadre d'une solution de protection des données comme décrit dans le guide Gestion de la confidentialité des données.
- Ajuster les performances des requêtes de la base de données Security Analytics Core comme décrit dans le Guide d'optimisation de la base de données principale de Security Analytics.

Note: Pour les versions Security Analytics 10.1 et supérieures, il n'est pas nécessaire de modifier le fichier d'index personnalisé du Broker, sauf pour les rôles système ou scénarios de déploiement pour la confidentialité des données. Le Broker fusionne automatiquement les clés de tous les services agrégés pour créer une langue détaillée. La langue de base définie dans les fichiers **index-broker.xml** et **index-broker-custom.xml** est utilisée s'il n'y a aucun service ou si tous les services sont hors ligne.

Caution: Ne définissez jamais le niveau d'index dans IndexKeys ou IndexValues pour un Decoder si vous avez un Concentrator ou un Archiver qui effectue une agrégation à partir du Decoder. La taille de partition de l'index est trop petite pour prendre en charge l'indexation au-delà de la clé méta `time`.

Activer le service de rapport sur les incidents

Le service de rapport sur les incidents est un service facultatif pour les services Security Analytics. Lorsqu'il est activé pour un des services de base, le service de rapport sur les incidents génère automatiquement un package d'informations à utiliser pour le diagnostic et la résolution du problème à l'origine de la défaillance du service. Le package est automatiquement envoyé à RSA pour analyse. Les résultats sont transférés au Support RSA pour toute autre action.

Le package d'informations envoyé à RSA ne contient pas de données capturées. Ce package d'informations se compose des informations suivantes :

- Trace de pile
- Logs
- Paramètres de configuration
- Version du logiciel
- Informations sur le CPU
- Fichiers RPM installés
- Géométrie du disque

L'analyse des incidents par le service de rapport sur les incidents peut être activée pour n'importe quel produit Core.

Fichier crashreporter.cfg

L'un des fichiers pouvant être modifiés dans la vue Configuration des services **>** onglet Fichiers est **crashreporter.cfg**, le fichier de configuration du serveur client pour le service de rapport sur les incidents.

Ce fichier est utilisé par le script qui vérifie, met à jour et crée des rapports d'incidents rencontrés sur l'hôte. Les services Decoder, Concentrator, hôtes et Broker peuvent être inclus dans la liste des produits à surveiller.

Ce tableau répertorie les paramètres du fichier **crashreporter.cfg**.

Paramètre	Description
applicationlist=decoder, concentrator, host	Définit la liste des produits à surveiller.
sitedir=/var/crashreporter	Emplacement du répertoire du site pour le rapport.
webdir=/usr/share/crashreporter/Web	Emplacement du répertoire Web.

Last Modified: August 10 2016, 9:33AM

Paramètre	Description
devdir=/var/crashreporter/Dev	Emplacement du répertoire de développement.
datadir=/var/crashreporter/data	Emplacement du répertoire de stockage des fichiers de données.
perldir=/usr/share/crashreporter/perl	Emplacement des fichiers perl.
bindir=/usr/share/crashreporter/bin	Emplacement des fichiers exécutables binaires.
libdir=/usr/share/crashreporter/lib	Emplacement des bibliothèques binaires.
cfgdir=/etc/crashreporter	Emplacement des fichiers de configuration.
logdir=/var/log/crashreporter	Emplacement des fichiers log.
scriptdir=/usr/share/crashreporter/scripts	Emplacement du répertoire contenant les scripts.
workdir=/var/crashreporter/work	Emplacement du répertoire de travail des processus.
sqldir=/var/crashreporter/sql	Emplacement des fichiers SQL créés.
reportdir=/var/crashreporter/reports	Emplacement des rapports temporaires créés.
packagedir=/var/crashreporter/packages	Emplacement des fichiers de package créés.
gdbconfig=/etc/crashreporter/crashreporter.gdb	Emplacement du fichier de configuration gdb.
corewaittime=30	Définit le nombre de secondes d'attente après avoir trouvé un fichier mémoire afin de déterminer si le fichier mémoire est toujours accessible en écriture.
cyclewaittime=10	Définit le nombre de minutes d'attente entre les cycles de recherche.
deletecores=1	Indique si les fichiers mémoire doivent être supprimés après le rapport. 0 = Non 1 = Oui **REMARQUE :** Jusqu'à la suppression du fichier mémoire, chaque redémarrage du service de rapport sur les incidents est signalé.
deletereportdir=1	Indique si le répertoire des rapports doit être supprimé après le rapport. Utile pour afficher les rapports sur les fichiers mémoire. 0 = Non 1 = Oui **REMARQUE :** S'il n'est pas supprimé, le répertoire sera inclus dans chaque package ultérieur.
debug=1	Indique si les messages de débogage sont activés ou désactivés dans la sortie de consignation **crashreporter**.

Paramètre	Description
	0 = Non 1 = Oui
posturl=https://www.netwitnesslive.com/crash...ter/submit.php	Définit l'URL de publication sur le serveur Web.
postpackages=0	Indique si les packages doivent être publiés sur le serveur Web. 0 = Non 1 = Oui
deletepackages=1	Indique si les packages doivent être supprimés après avoir été publiés sur le serveur Web. 0 = Non 1 = Oui

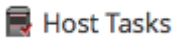
Configurer le service de rapport sur les incidents

Pour configurer le service de rapport sur les incidents :

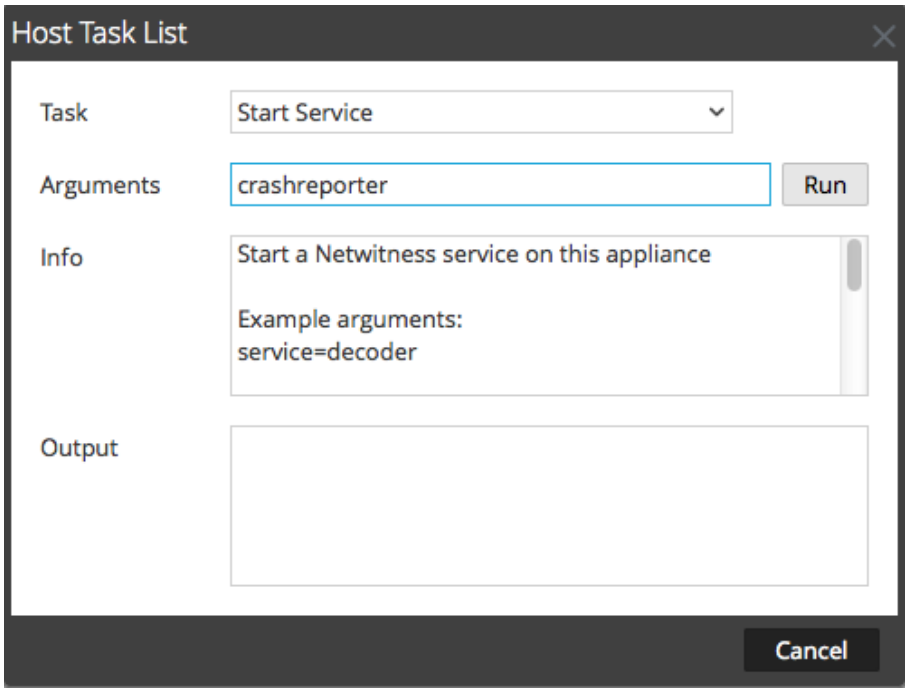
1. Dans la vue Services, sélectionnez un service, puis cliquez sur  **> Vue > Config**.
2. Sélectionnez l'onglet **Fichiers**.
3. Modifiez le fichier **crashreporter.cfg**.
4. Cliquez sur **Enregistrer**.
5. Pour afficher la vue Système de services, sélectionnez **Config > Système**.
6. Pour redémarrer le service, cliquez sur  .
   Le service s'arrête, puis redémarre.

Démarrage et arrêt du service de rapport sur les incidents

Pour démarrer le service de rapport sur les incidents :

1. Dans la vue Services, sélectionnez le service, puis cliquez sur  **> Vue > Système**.
2. Dans la barre d'outils, cliquez sur  .
   La liste Tâches de l'hôte s'affiche.
3. Dans la liste déroulante Tâche, sélectionnez **Démarrer le service**.

4. Dans le champ Arguments, saisissez **crashreporter**, puis cliquez sur **Exécuter**.



Le service de rapport sur les incidents est activé et reste actif jusqu'à ce que vous l'arrêtiez.

Pour arrêter le service de rapport sur les incidents, sélectionnez **Arrêter le service** dans la liste déroulante Tâche.

Maintenir les fichiers de mappage des tables

Le fichier de mappage de tables fourni par RSA, **table-map.xml**, est une composante importante du Log Decoder. Il s'agit d'un fichier de définition de métadonnées qui mappe également les clés utilisées dans un analyseur de log aux clés de la base de métadonnées.

Ne modifiez pas le fichier **table-map.xml**. Si vous souhaitez apporter des modifications à ce fichier, faites-les dans le fichier **table-map-custom.xml**. La dernière version du fichier table-map.xml est disponible sur Live pour que RSA en effectue la mise à jour si nécessaire. Si vous modifiez le fichier table-map.xml, les modifications peuvent être écrasées lors d'une mise à niveau du service ou du contenu.

Dans le fichier **table-map.xml**, certaines clés méta sont définies sur `Transient` et d'autres sur `None`. Pour stocker et indexer une clé méta spécifique, la clé doit être définie sur `None`. Pour modifier le mappage, vous devez créer une copie du fichier nommé table-map-custom.xml dans le Log Decoder et définir les clés méta sur `None`.

Pour l'indexation des clés meta :

- Lorsqu'une clé est définie sur `None` au sein du fichier **tablemap.xml** dans le Decoder Log, elle est indexée.
- Lorsqu'une clé est définie sur `Transient` au sein du fichier **table-map.xml** dans le Decoder Log, elle n'est pas indexée. Pour indexer la clé, copiez l'entrée dans le fichier **table-map-custom.xml** et remplacez le mot clé `flags="Transient"` par `flags="None"`.
- Si le fichier **table-map.xml** ne comporte aucune clé, ajoutez une entrée dans le fichier **table-map-custom.xml** dans le Decoder Log.

> ⚠ **Caution:** Ne mettez pas le fichier **table-map.xml** à jour car une mise à niveau pourrait l'écraser. Ajoutez tous les changements que vous souhaitez apporter au fichier **table-map-custom.xml**.

Conditions préalables

Si le Log Decoder ne dispose pas du fichier **table-map-custom.xml**, créez une copie du fichier **table-map.xml** et renommez-la en **table-map-custom.xml**.

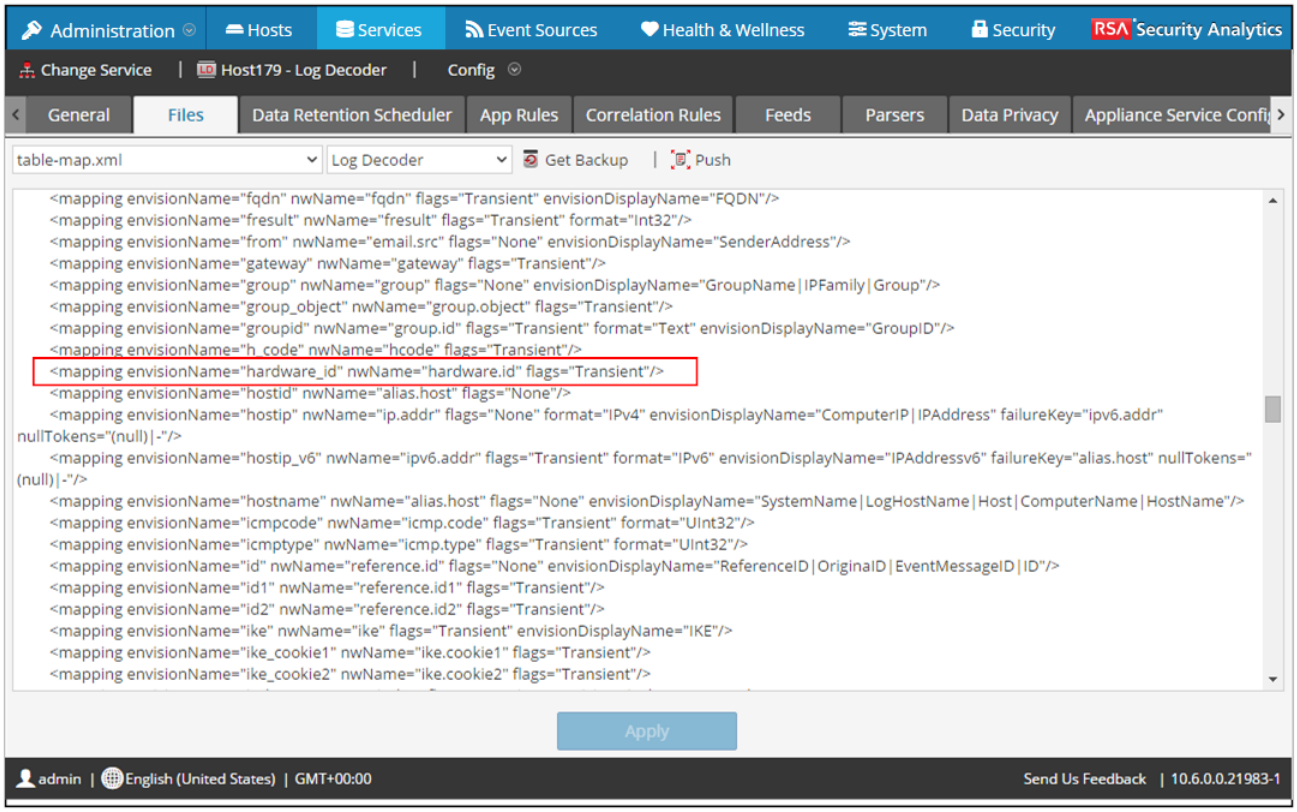
Procédure

Pour vérifier et mettre à jour le fichier de mappage de tables :

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

Last Modified: August 10 2016, 9:33AM

2. Dans la grille Services, sélectionnez un Log Decoder et **> Vue > Configuration**.
3. Cliquez sur l'onglet **Fichiers**, puis sélectionnez le fichier **table-map.xml**.



4. Vérifiez que les mots-clés des balises sont définis correctement sur `Transient` ou `None`.
5. Si vous devez modifier une entrée, ne modifiez pas le fichier **table-map.xml** car une mise à niveau pourrait l'écraser. À la place, copiez l'entrée, sélectionnez le fichier **table-map-custom.xml** et remplacez le mot-clé de balise `Transient` par `None`.

   Par exemple, l'entrée suivante pour la clé meta hardware.id dans le fichier **table-map.xml** n'est pas indexée et le mot-clé de balise est `Transient` :
   ```
   <mapping envisionName="hardware_id" nwName="hardware.id" flags="Transient"/>
   ```
   Pour indexer la clé méta hardware.id, remplacez le mot-clé de balise `Transient` par `None` dans le fichier **table-map-custom.xml** :
   ```
   <mapping envisionName="hardware_id" nwName="hardware.id" flags="None"/>
   ```
6. Si le fichier table-map.xml ne contient pas d'entrée, ajoutez-en une dans le fichier **table-map-custom.xml**.
7. Après avoir effectué vos modifications dans le fichier **table-map-custom.xml**, cliquez sur **Appliquer**.

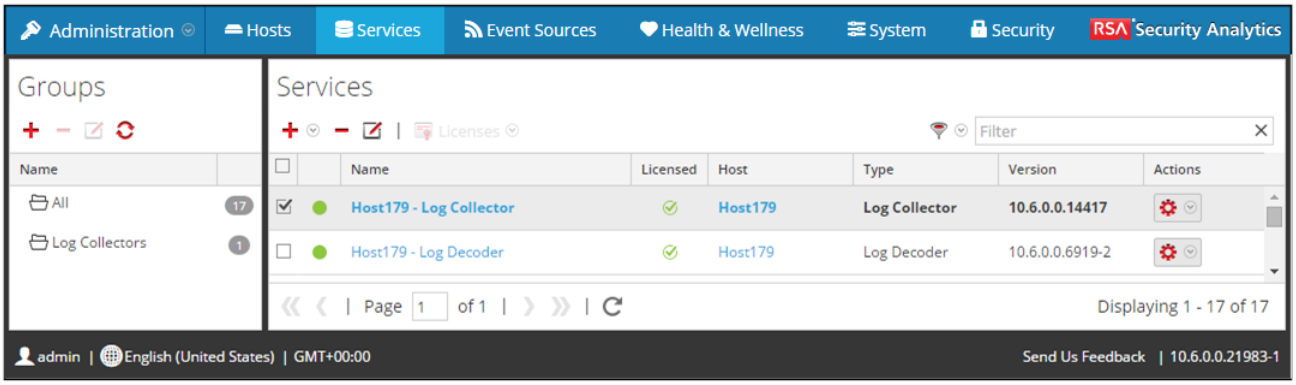
> ⚠ **Caution:** Avant de modifier les fichiers de mappage de tables, examinez attentivement l'effet de la modification de l'index suite au remplacement de `Transient` en `None`, car il peut y avoir un impact sur la capacité de stockage disponible et les performances du Log Decoder. C'est pour cette raison que seules certaines clés méta sont pré-indexées. Utilisez le fichier **table-map-custom.xml** pour d'autres usages.

Modifier ou supprimer un service

Vous pouvez modifier les paramètres d'un service, comme le changement de nom d'hôte ou de numéro de port, ou supprimer un service dont vous n'avez plus l'utilité.

Chacune des procédures suivantes démarre dans la vue Services.

Pour accéder à la vue Services, dans le menu Security Analytics, sélectionnez **Administration > Services**.

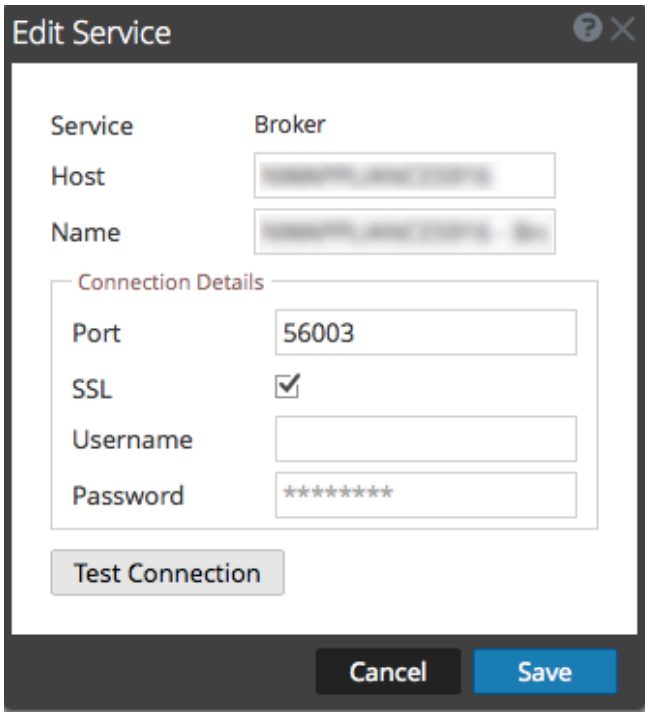


Procédures

Last Modified: August 10 2016, 9:33AM

Modifier le service

1. Dans la vue Services, sélectionnez un service et cliquez sur ou **> Modifier**.
   La boîte de dialogue **Modifier le service** s'affiche. Elle n'affiche que les champs applicables au service sélectionné.



2. Modifiez les détails du service en modifiant l'un des champs suivants :

- **Nom**
- **Port** - Chaque service principal dispose de deux ports, SSL et non SSL. Pour les connexions approuvées, vous devez utiliser le port SSL.
- **SSL** - Pour les connexions approuvées, vous devez utiliser SSL.
- **Nom d'utilisateur** et **Mot de passe** - Utilisez ces informations d'identification pour tester la connexion à un service.
  a. Si vous utilisez une connexion approuvée, supprimez le nom d'utilisateur.
     Si ce n'est pas le cas, saisissez un nom d'utilisateur et un mot de passe.
  b. Cliquez sur **Tester la connexion**.

3. (Facultatif) Si le service nécessite une licence, sélectionnez Activer un service. Cette option apparaît uniquement pour les services qui nécessitent une licence.
4. Cliquez sur Enregistrer.

Les modifications prennent effet immédiatement.

Supprimer un service

1. Dans la vue Services, sélectionnez un ou plusieurs services et cliquez sur ou **> Supprimer**.
2. Une boîte de dialogue demande confirmation. Pour supprimer le service, cliquez sur **Oui**.

Le service supprimé n'est plus disponible pour les modules Security Analytics.

Last Modified: August 10 2016, 9:33AM

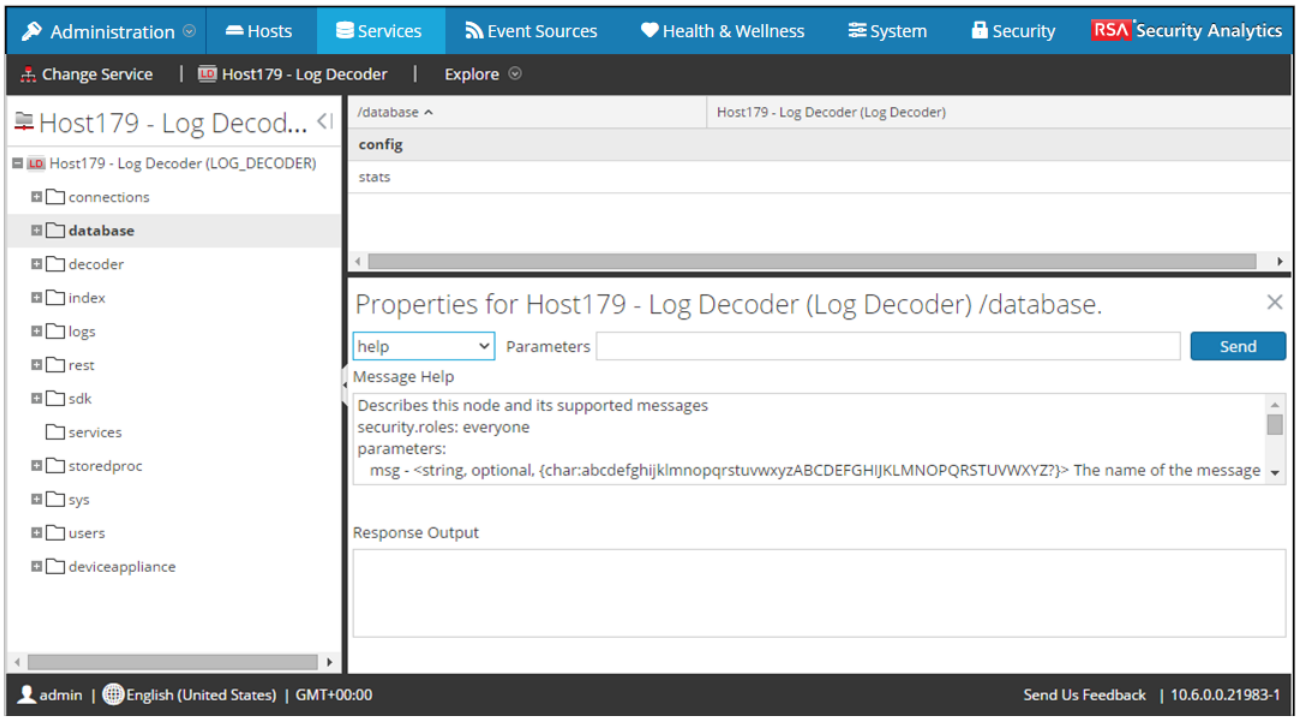
Explorer et modifier l'arborescence des propriétés du service

Vous disposez d'un accès avancé et du contrôle des fonctions du service dans la vue Explorer des services, qui se compose de deux parties. La liste de nœuds affiche la fonctionnalité du service dans une arborescence de dossiers. Le panneau Surveiller affiche les propriétés du dossier ou du fichier sélectionné dans la liste des nœuds.

Chacune des procédures suivantes démarre dans la vue Explorer.

Pour accéder à la vue Explorer :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis **> Vue > Explorer**.
   La vue Explorer s'affiche. La liste des nœuds se trouve sur la gauche et le panneau Surveiller sur la droite.



Procédures

Last Modified: August 10 2016, 9:33AM

Afficher ou modifier une propriété de service

Pour afficher une propriété de service :

1. Cliquez avec le bouton droit de la souris sur un fichier dans la liste de nœuds ou dans le panneau Surveiller.
2. Cliquez sur **Propriétés**.

Pour modifier la valeur d'une propriété de service :

1. Dans le **panneau Surveiller**, sélectionnez une valeur de propriété modifiable.
2. Saisissez une nouvelle valeur.

Envoyer un message à un nœud

1. Dans la boîte de dialogue Propriétés, PropDBsélectionnez un **type de message**. Les options varient selon le fichier sélectionné dans la liste des nœuds.
   Une description du type de message sélectionné s'affiche dans le champ **Aide relative aux messages**.
2. (Facultatif) Si le message l'indique, saisissez les **Paramètres**.
3. Cliquez sur **Envoyer**.
   La valeur ou le format s'affiche dans le champ **Sortie de réponse**.

RSA

Supprimer la connexion à un service

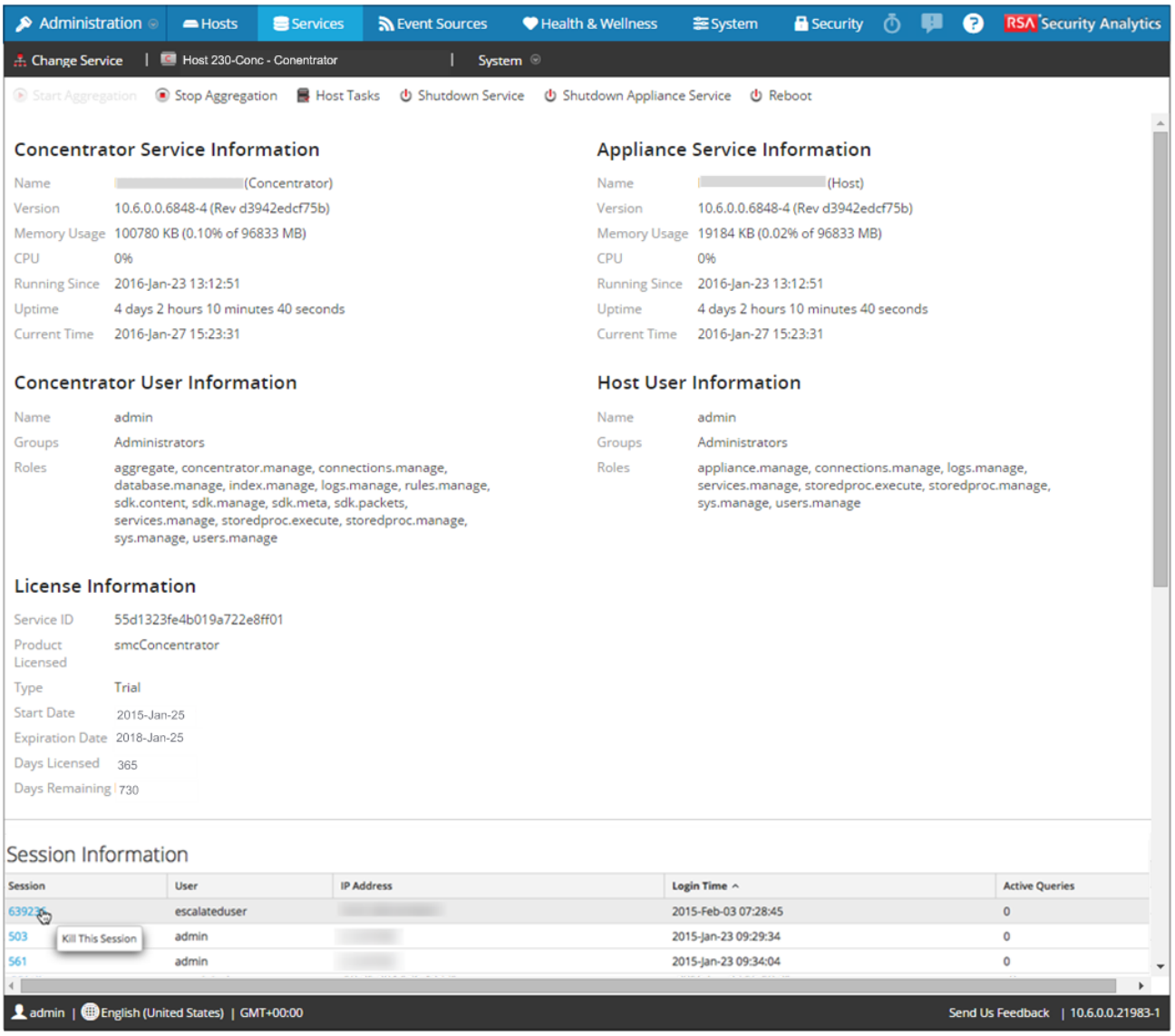
Dans la vue Système de services, vous pouvez afficher les sessions en cours d'exécution sur un service. Dans la liste des sessions, vous pouvez mettre fin à la session et aux requêtes actives d'une session.

Mettre fin à une session sur un service

1. Dans **Security Analytics menu**, sélectionnez **Administration >** Services.
   La vue Services d'administration s'affiche.

Last Modified: August 10 2016, 9:33AM

2. Sélectionnez un service et cliquez sur  **> Vue > Système**.
   La vue Système de services s'affiche.



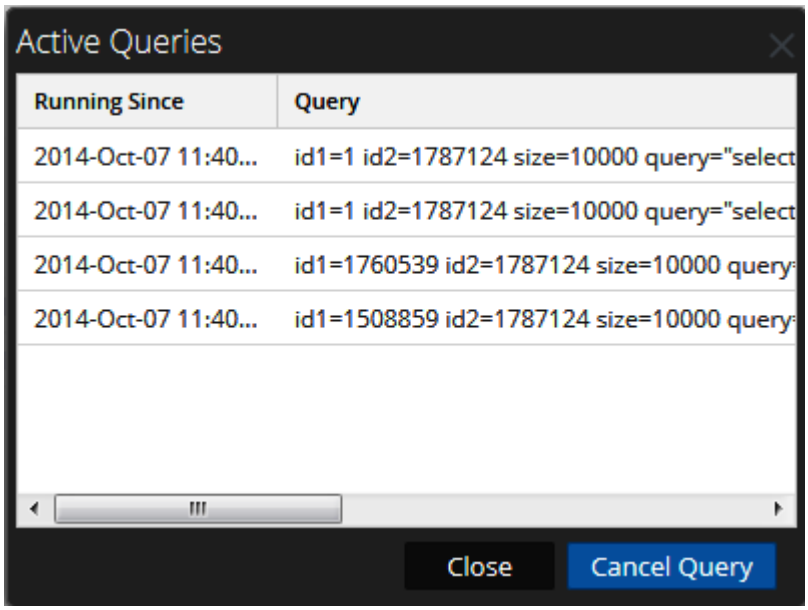
3. Dans la grille **Sessions** en bas, cliquez sur un **numéro de session > Supprimer cette session**.

La session se termine et est supprimée de la grille.

Mettre fin à une requête active dans une session

1. Faites défiler jusqu'à la grille **Sessions**.
2. Dans la colonne **Requêtes actives**, cliquez sur un nombre de requêtes actives différent de zéro pour une session. Vous ne pouvez pas cliquer sur un nombre de requêtes actives égal à 0.

La boîte de dialogue Requêtes actives s'affiche.



3. Sélectionnez une requête et cliquez sur **Annuler la requête**.
   La requête s'arrête et la colonne Requêtes actives est mise à jour.

Rechercher des services

Vous pouvez rechercher des services dans la liste des services de la vue Services d'administration. La vue Services permet de filtrer rapidement la liste des services par nom, hôte et type. Vous pouvez utiliser le menu déroulant Filtrer et le champ Filtre séparément ou simultanément pour filtrer la vue Services.

En plus de localiser les services d'un hôte dans la vue Services, vous pouvez aussi trouver rapidement les services qui s'exécutent sur un hôte dans la vue Hôtes.

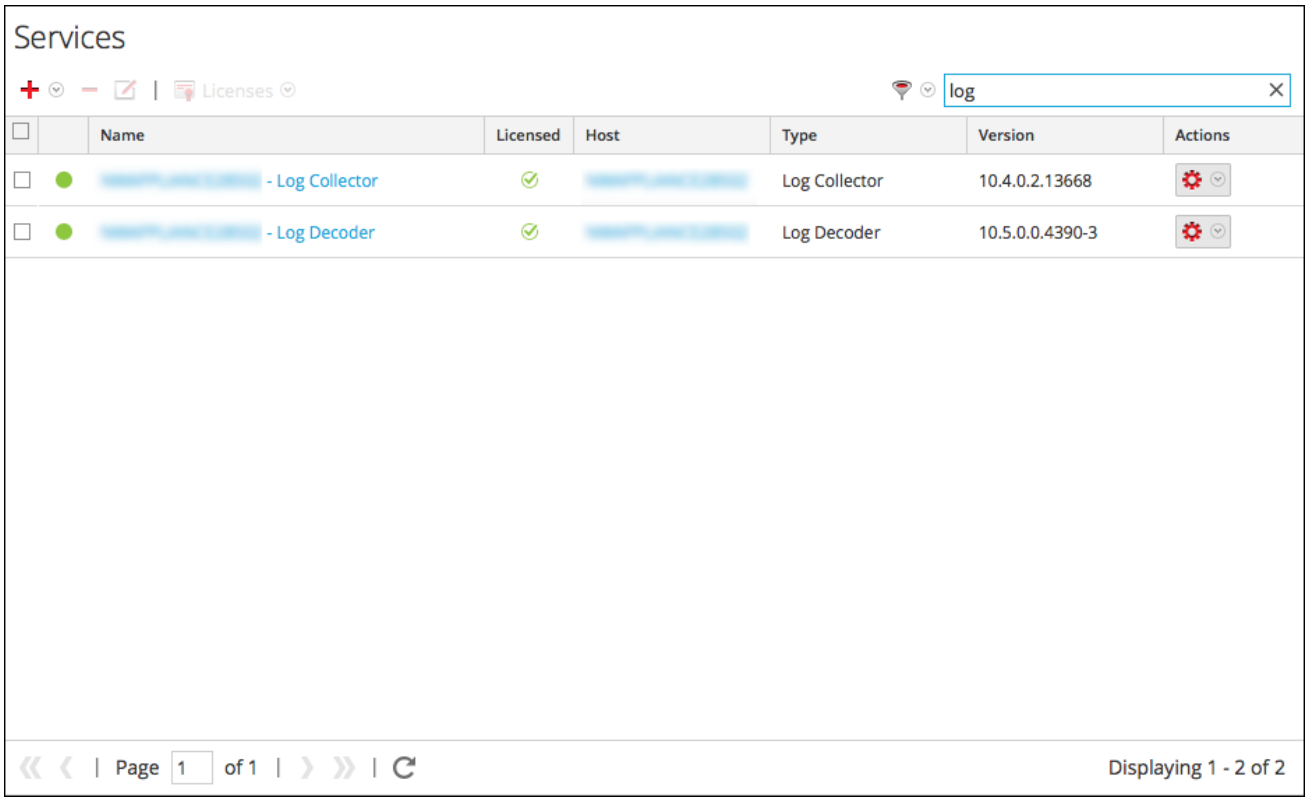
Rechercher un service

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Dans la barre d'outils du panneau **Services**, saisissez un **nom de service** ou un **nom d'hôte** dans le champ **Filtre**.

Le panneau Service répertorie les services correspondant aux noms entrés dans le champ Filtre.
L'exemple suivant illustre les résultats de recherche qui apparaissent lorsque vous commencez à saisir le mot **log** dans le

Last Modified: August 10 2016, 9:33AM

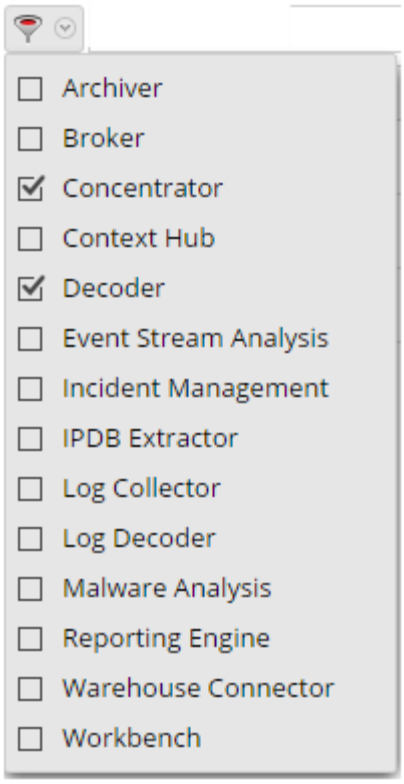
champ de filtre.



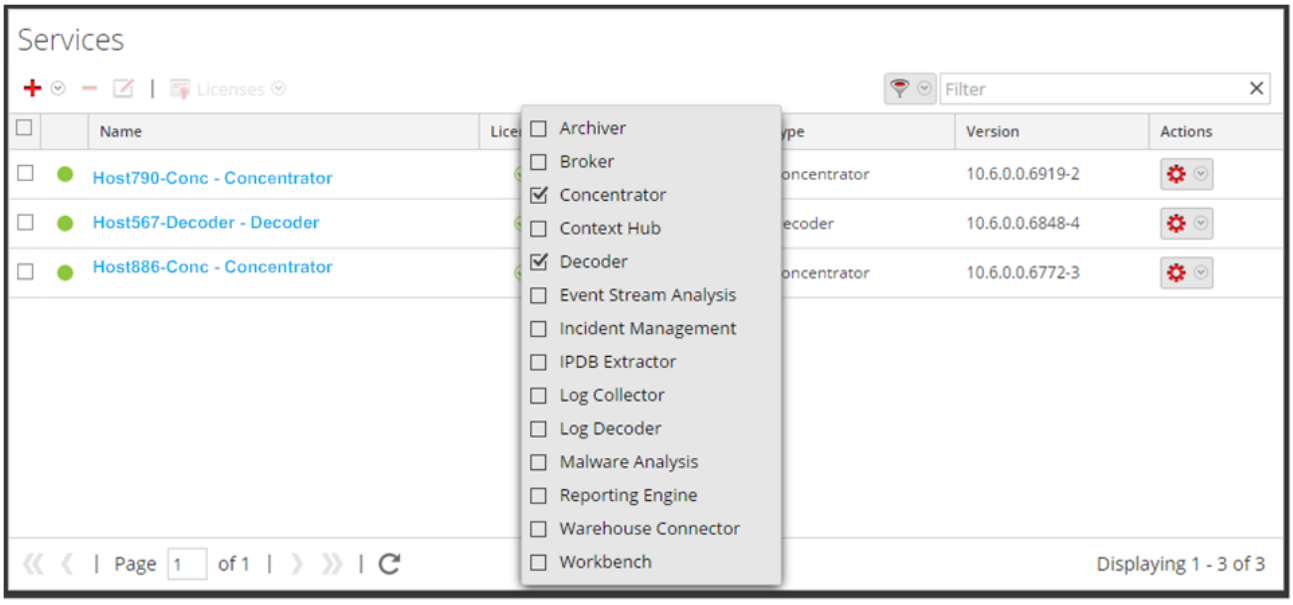
Filtrer les services par type

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Dans la vue Services, cliquez sur , puis sélectionnez le type de service que vous souhaitez faire apparaître dans cette vue.

Last Modified: August 10 2016, 9:33AM



Les types de services sélectionnés apparaissent alors dans la vue Services.
L'exemple suivant affiche la vue Services filtrée sur Concentrator et Decoder.

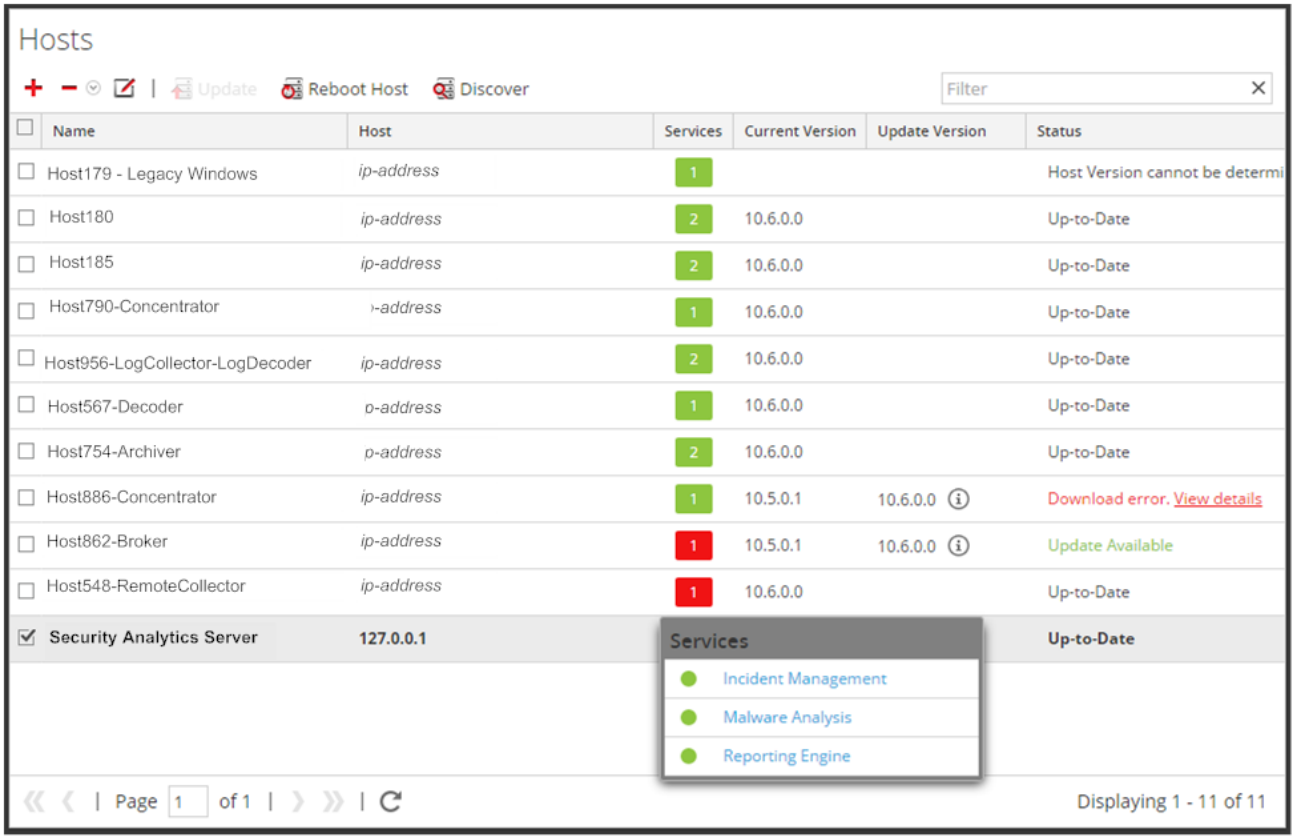


Last Modified: August 10 2016, 9:33AM

Trouver les services sur un hôte

En plus de localiser les services d'un hôte dans la vue Services, vous pouvez aussi trouver rapidement les services qui s'exécutent sur un hôte dans la vue Hôtes.

1. Dans le menu Security Analytics, sélectionnez **Administration > Hôtes**.
2. Dans la vue Hôtes, sélectionnez un hôte, puis cliquez sur la zone contenant un nombre (nombre de services) dans la colonne **Services**. La liste des services installés sur l'hôte sélectionné s'affiche.
   Dans l'exemple suivant, trois services sont répertoriés pour l'hôte sélectionné si vous cliquez sur la zone contenant le nombre 3.



Vous pouvez cliquer sur les liens associés aux services pour les consulter dans la vue Services.

Last Modified: August 10 2016, 9:33AM

Démarrer, arrêter ou redémarrer un service

Ces procédures s'appliquent uniquement aux services principaux.

Chacune des procédures suivantes démarre dans la vue Services. Dans le menu Security Analytics, sélectionnez **Administration > Services**.

Démarrer un service

Sélectionnez un service et cliquez sur  **> Démarrer**.

Arrêter un service

Lorsque vous arrêtez un service, tous ses processus s'arrêtent et les utilisateurs actifs sont déconnectés de ce service.

Pour arrêter un service :

1. Sélectionnez un service et cliquez sur  **> Arrêter**.
2. Une boîte de dialogue demande confirmation. Pour arrêter le service, cliquez sur **Oui**.

Redémarrer un service

Vous devez parfois redémarrer un service pour que les modifications soient appliquées. Lorsque vous modifiez un paramètre qui nécessite un redémarrage, Security Analytics affiche un message.

Pour redémarrer un service :

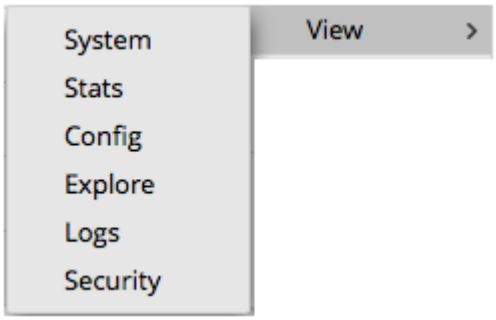
1. Sélectionnez un service et cliquez sur  **> Redémarrer**.
2. Une boîte de dialogue demande confirmation. Pour arrêter le service, cliquez sur **Oui**.

Le service s'arrête et redémarre ensuite automatiquement.

Last Modified: August 10 2016, 9:33AM

Afficher les détails d'un service

Vous pouvez afficher et modifier des informations sur les services à l'aide des options du menu Affichage d'un service.



Objectif de chaque vue Service

Chaque vue affiche une portion fonctionnelle d'un service et est décrite en détail dans sa propre section :

- La vue Système affiche un résumé du service, le service de l'appliance, l'utilisateur de l'hôte, la licence et les informations de session.
- La vue Statistiques donne un moyen de surveiller les opérations et l'état du service.
- La vue Configuration permet de configurer tous les aspects d'un service.
- La vue Explorer permet d'afficher et de modifier les configurations des hôtes et des services.
- La vue Logs affiche les logs du service dans lesquels vous pouvez effectuer une recherche.
- La vue Sécurité est un moyen d'ajouter des comptes utilisateur Core Security Analytics pour l'agrégation, les utilisateurs clients thick et les utilisateurs de l'API REST.

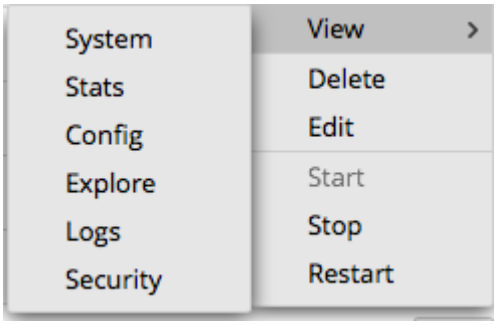
Accéder à la vue Service

Pour accéder à la vue d'un service :

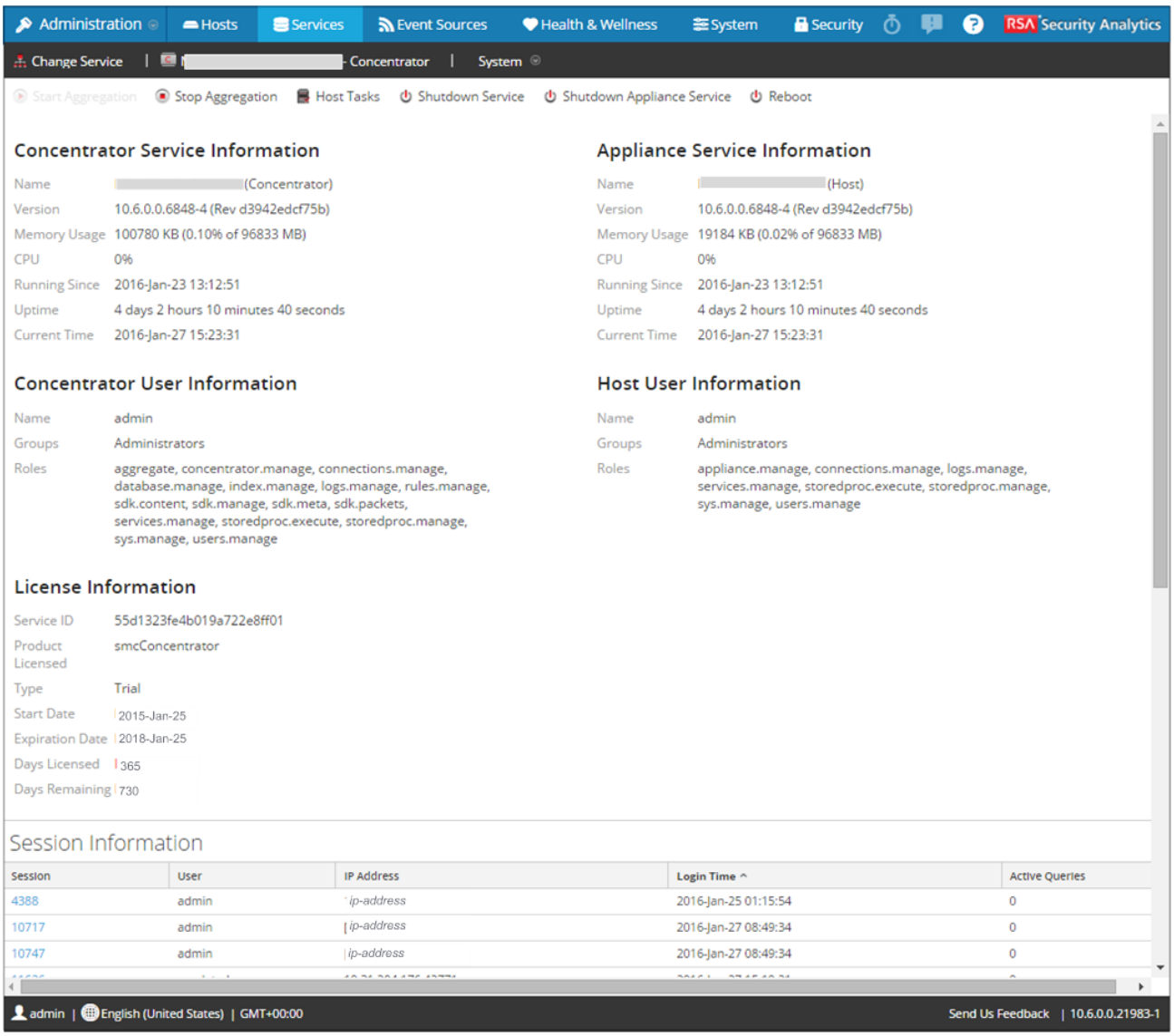
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.

Last Modified: August 10 2016, 9:33AM

2. Sélectionnez un service, puis cliquez sur  **> Affichage**.
   Le menu Affichage s'affiche.



3. Parmi les options situées sur la gauche, sélectionnez une vue.
   Il s'agit d'une vue du système de Concentrator



4. Utilisez la barre d'outils pour naviguer :

- Cliquez sur **Modifier le service** pour sélectionner un autre service.
- Cliquez sur le **nom du service en cours**, EL5EL6Conc dans l'exemple, pour afficher sa configuration.
  La lettre de l'icône à gauche du nom indique le type de service :
  - **B** pour Broker
  - **C** pour Concentrator
  - **D** pour Decoder et Log Decoder.
- Cliquez sur à la droite de la **vue en cours**, qui est Système dans l'exemple, pour sélectionner une vue différente.

Références

Cette rubrique constitue une référence concernant les fonctions de l'interface utilisateur d'administration de Security Analytics.

Cette rubrique décrit les fonctions disponibles dans l'interface utilisateur de Security Analytics Administration . Le module Administration regroupe les activités d'administration Security Analytics dans une seule vue afin de surveiller et de gérer les hôtes (appliances), services, tâches ainsi que la sécurité.

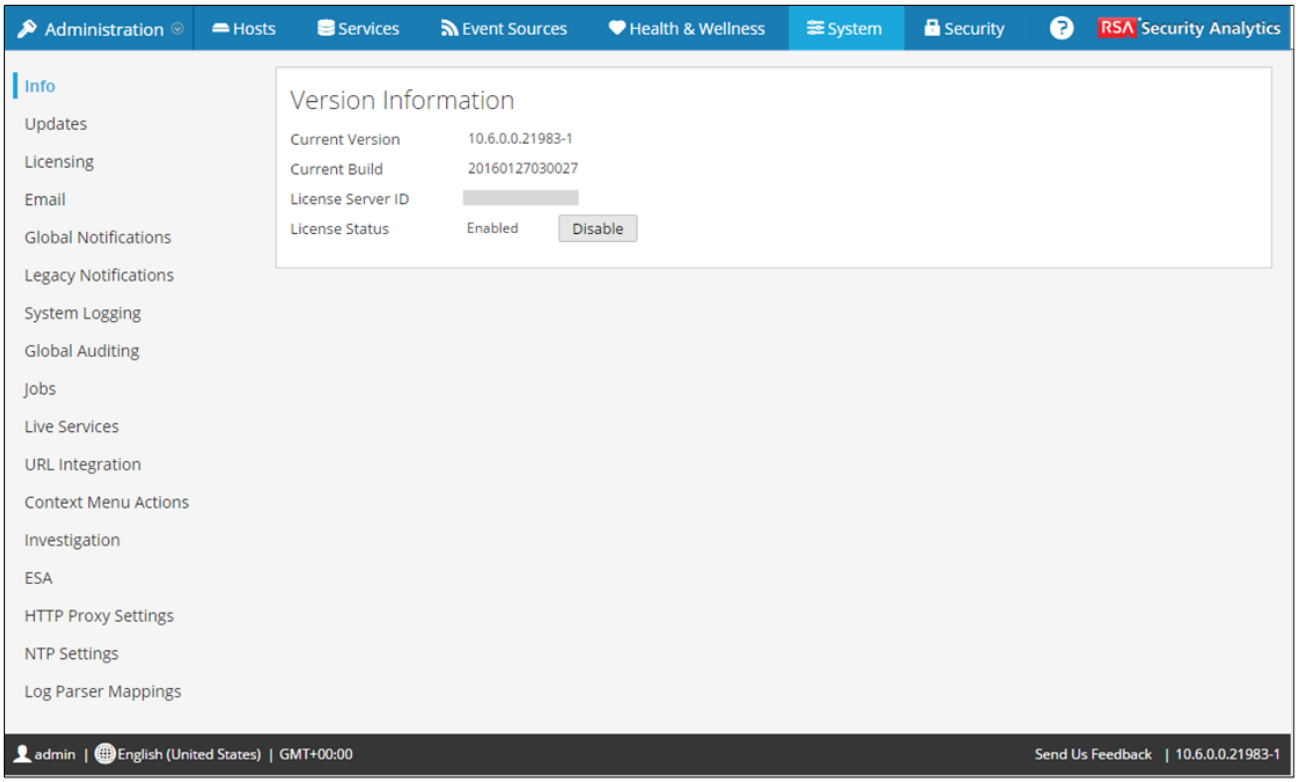
Last Modified: August 10 2016, 9:33AM

Vue Système d'administration

Cette rubrique présente les fonctions de la vue Système d'administration de Security Analytics.

La vue Système d'administration consolide la configuration de l'audit global, de l'e-mail, de la consignation, des tâches, de la connexion aux services RSA Live, de l'intégration d'URL, de la procédure d'enquête, de l'ESA (Event Stream Analysis) et des paramètres de performances avancés. En outre, vous pouvez gérer les versions Security Analytics, mettre à jour la version Security Analytics et configurer le serveur d'attribution de licence local.

Pour accéder à la vue Système, dans le menu **Security Analytics**, sélectionnez **Administration > Système**.



Caractéristiques

Sur le panneau de gauche de la vue Système d'administration se trouve le panneau d'options qui répertorie tous les nœuds système disponibles pour la configuration. Lorsque vous sélectionnez un nœud, le contenu associé s'affiche dans le panneau de droite.

Last Modified: August 10 2016, 9:33AM

Last Modified: August 10 2016, 9:33AM

Panneau de consignation système

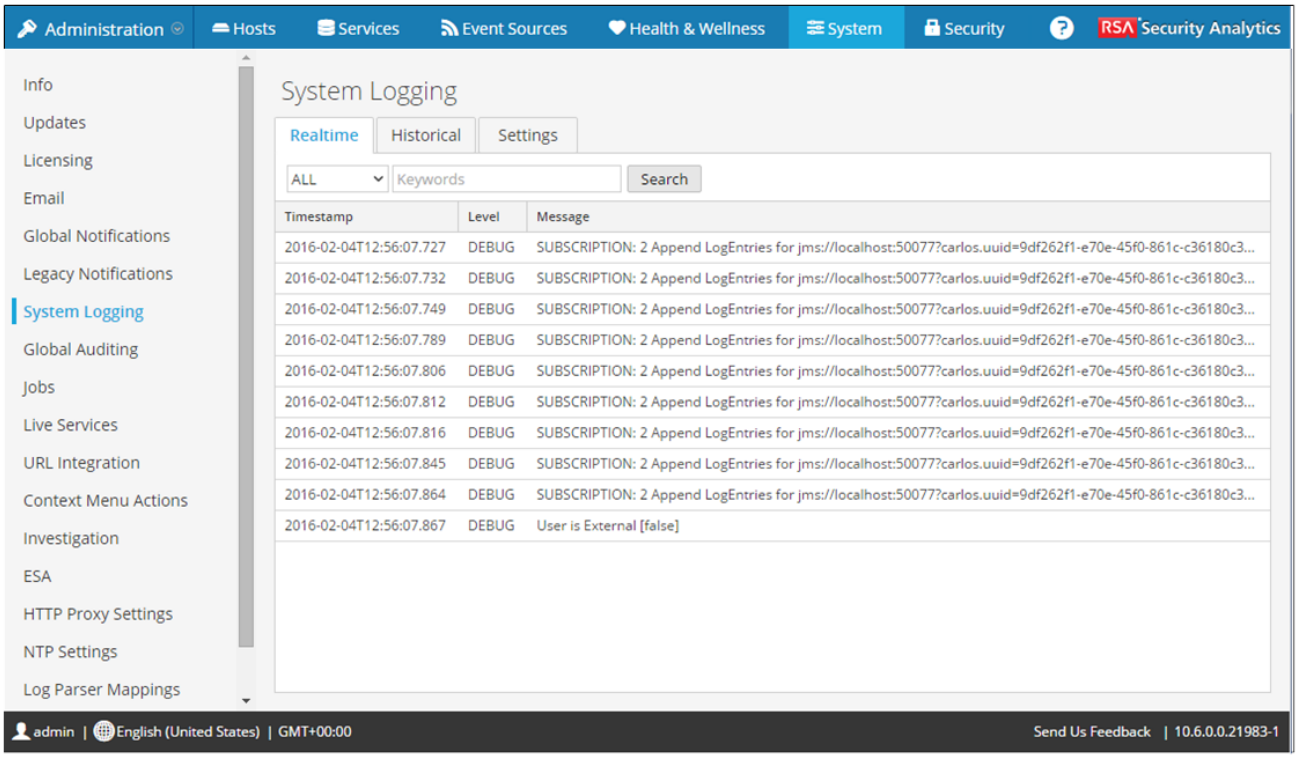
Cette rubrique présente les fonctionnalités du panneau de consignation système.

La vue Logs système permet d'afficher et d'explorer les logs système Security Analytics. La vue Logs système est similaire à la vue Logs de services à deux exceptions près :

- Les logs de services disposent d'un filtre supplémentaire pour sélectionner les messages pour le service ou l'hôte.
- Le panneau de consignation système contient des onglets supplémentaires pour Paramètres et Audit.

Pour accéder à la vue Logs système Security Analytics :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Système.**
2. Dans le panneau des options, cliquez sur **Consignation système**.



Caractéristiques

Le panneau Consignation système contient trois onglets : En temps réel, Historique et Paramètres.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
Onglet En temps réel	C'est le mode surveillance du log Security Analytics. Pour plus d'informations, reportez-vous à Onglet En temps réel.
Onglet Historique	C'est une vue du log Security Analytics dans laquelle une recherche peut être effectuée. Pour plus d'informations, reportez-vous à Onglet Historique.
Onglet Paramètres	Cet onglet permet de modifier la configuration de base de la consignation pour Security Analytics, ainsi que les packages à consigner. Pour plus d'informations, reportez-vous à Onglet Paramètres.

Last Modified: August 10 2016, 9:33AM

Onglet Historique

Cette rubrique décrit les fonctions de Système de services - Consignation > onglet Historique et de la vue Logs de services > onglet Historique.

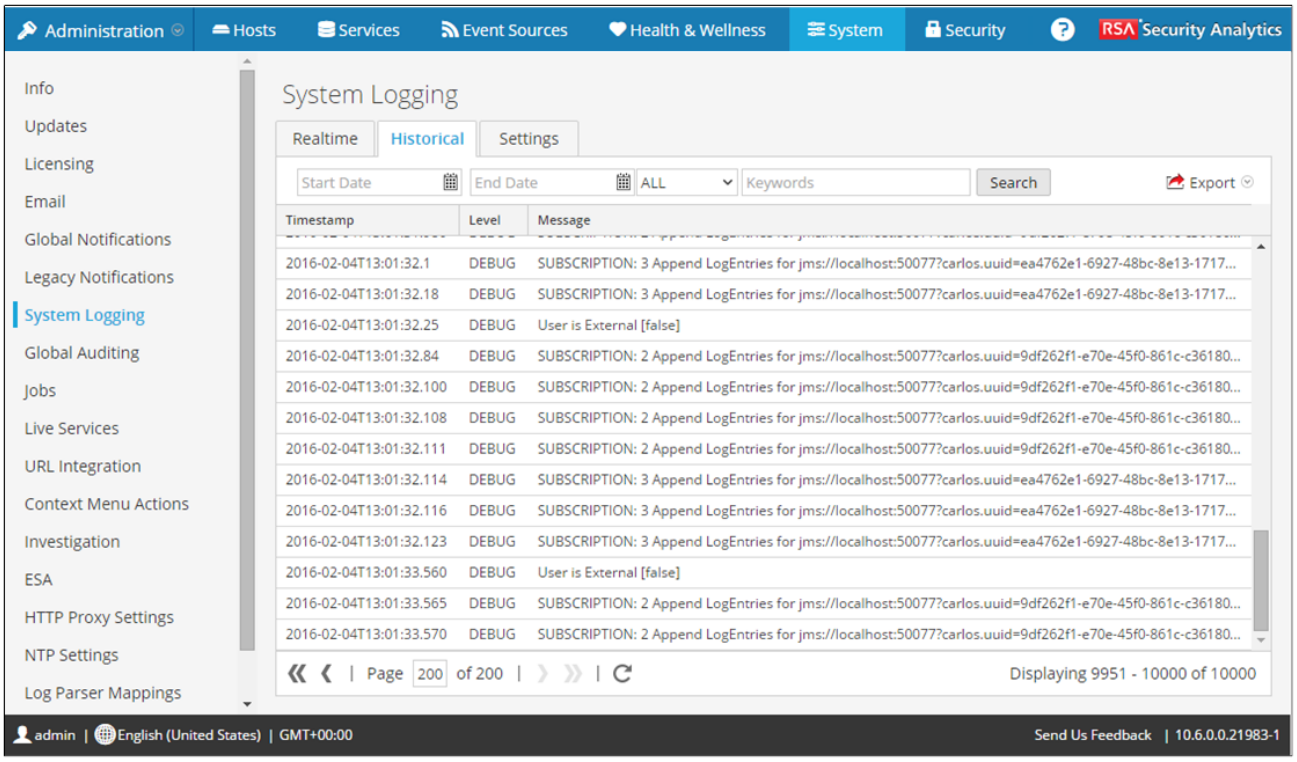
L'onglet Historique fournit une vue du log Security Analytics dans laquelle une recherche peut être effectuée, ou le log de service au format page. Lors du chargement initial, la grille affiche la dernière page des entrées de log pour le système.

Pour accéder à l'onglet Historique :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Système.**
2. Dans le panneau des options, cliquez sur **Consignation système**.
   Le panneau Consignation système s'ouvre sur l'onglet **En temps réel** par défaut.
3. Cliquez sur l'onglet **Historique**.

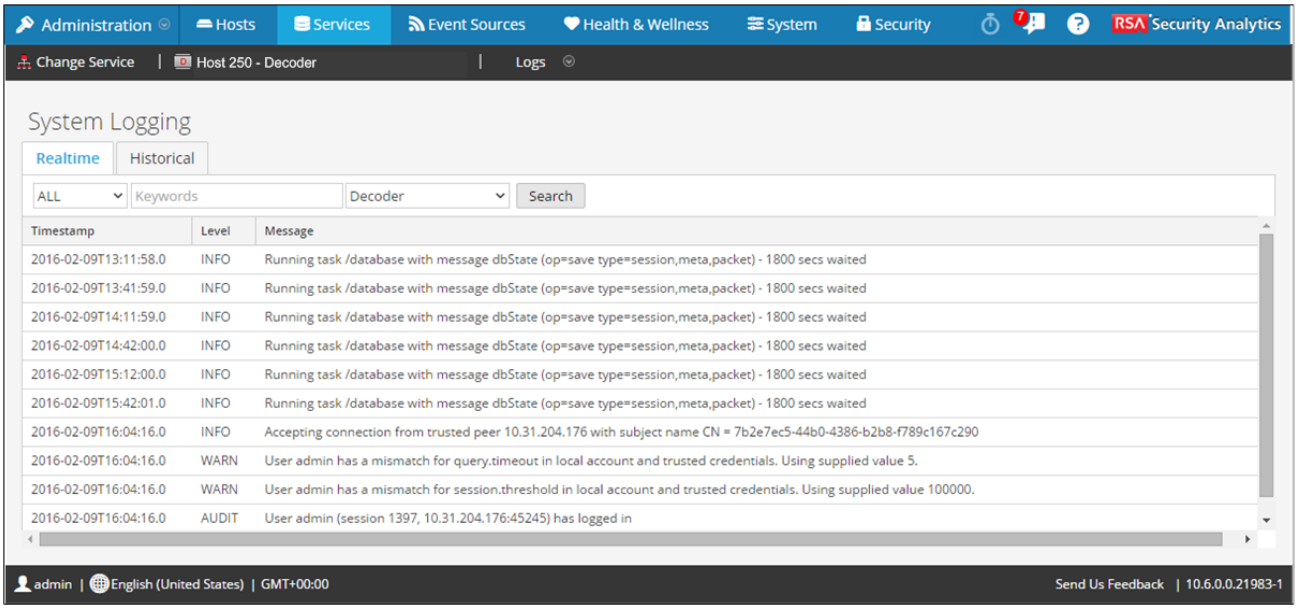
Pour obtenir des informations sur l'accès aux logs de service, reportez-vous à la rubrique Vue Logs de services.

Voici un exemple de l'onglet **Historique** dans le panneau Consignation système. Il affiche les logs Security Analytics.



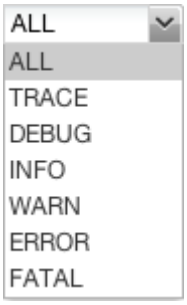
Last Modified: August 10 2016, 9:33AM

Voici un exemple de l'onglet **Historique** dans le panneau Logs de services. Il affiche les logs de services.



Caractéristiques

L'onglet **Historique** contient une barre d'outils avec des champs de saisie permettant le filtrage des entrées, ainsi qu'une grille contenant les entrées de log et les outils de pagination.

Fonction	Description
Date de début et **Date de fin**	Les options de recherche dans la plage **Date de début** et **Date de fin** limitent les entrées de log à un point dans le temps. En cas d'utilisation, vous devez fournir la date de début et la date de fin. Les heures sont facultatives. La période est validée pour vérifier que la date de fin n'est pas antérieure à la date de début.
Liste déroulante Niveau de consignation 	Sélectionne le niveau de consignation pour les entrées à afficher dans la grille. La liste déroulante **Niveau de consignation** affiche les niveaux de consignation disponibles pour le système ou le service. • Les logs système disposent de sept niveaux de consignation. • Les logs des services ne comptent que six niveaux de consignation car ils ne comprennent pas le niveau **SUIVRE**. • La valeur par défaut est **TOUTES** les entrées de log.
Champ Mot-clé	Spécifie un mot clé à utiliser lors du filtrage des entrées. Ce champ est le même pour le filtrage des logs de service et de système.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
Champ Service (Logs de service uniquement)	Spécifie le type de service à utiliser lors du filtrage des entrées de log de service. Les valeurs possibles sont l'hôte ou le service.
Bouton Rechercher	Cliquez pour activer une recherche basée sur les dates de début et de fin, le niveau de log, les mots-clés et les sélections de service.
Exporter	Cliquez pour exporter les entrées de la grille en cours d'affichage au format de fichier texte. Vous pouvez sélectionner un format texte séparé par des virgules ou des tabulations pour les entrées du fichier.

Colonne	Description
Horodatage	Il s'agit de l'horodatage de l'entrée.
Niveau	Il s'agit du niveau de consignation du message.
Message	Il s'agit du texte de l'entrée de log.

Les outils de pagination figurant sous la grille permettent de parcourir les pages du log.

Outil	Description
«	Première page
‹	Page précédente
Page 1 of 16	Numéro de page
›	Page suivante
»	Dernière page
↻	Bouton Actualiser

Rechercher les entrées de log

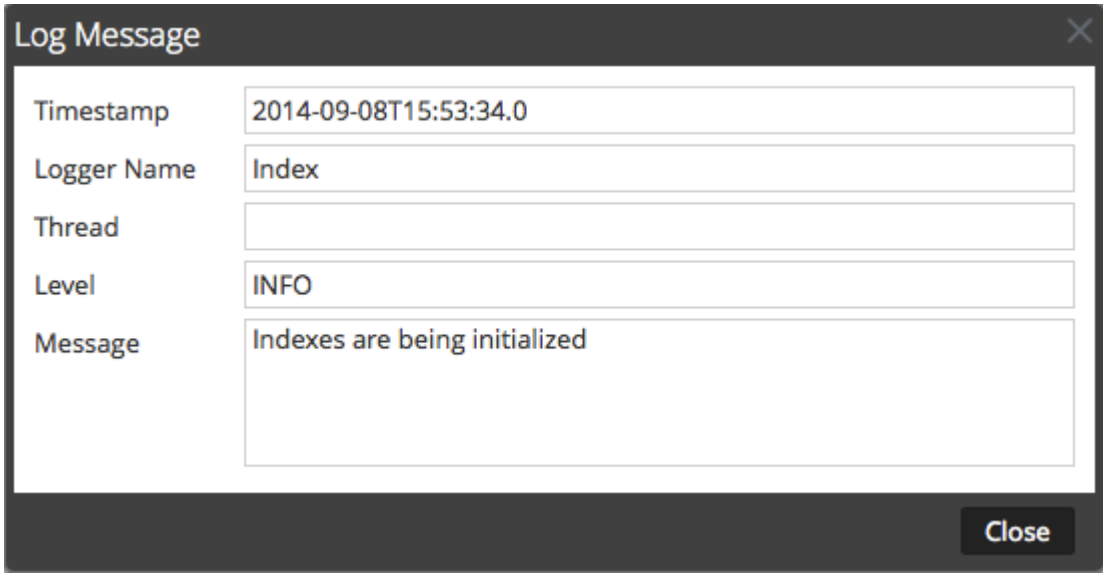
Pour rechercher les résultats affichés sous l'onglet **Historique** :

1. (Facultatif) Sélectionnez une **Date de début** et une **Date de fin**. Éventuellement, sélectionnez une **Heure de début** et une **Heure de fin**.
2. (Facultatif) Pour les logs de système et de service, sélectionnez un **Niveau de log** et un **Mot clé**, ou les deux.
3. (Facultatif) Pour les logs de service, sélectionnez le **Service** : hôte ou service.
4. Cliquez sur **Rechercher**.
   La vue est réinitialisée avec les 10 entrées les plus récentes qui correspondent à votre filtre. Alors que de nouvelles entrées de log correspondantes deviennent disponibles, la vue est mise à jour pour afficher ces entrées.

Afficher les détails d'une entrée de log

Chaque ligne de la grille de log sous l'onglet **Historique** propose des informations de synthèse sur l'entrée de log. Pour afficher les détails complets :

1. Cliquez deux fois sur une entrée de log.
   La boîte de dialogue Message log, qui contient l'horodatage, le nom de l'enregistreur, le thread, le niveau et le message, s'affiche.



2. Lorsque vous avez terminé de la consulter, cliquez sur **Fermer**.

Parcourir les entrées

Pour consulter les différentes pages de la grille, utilisez les commandes de pagination en bas de la grille, comme suit :

- Utilisez les boutons de navigation
- Saisissez manuellement le numéro de la page que vous souhaitez afficher, puis appuyez sur **ENTRÉE**.

Last Modified: August 10 2016, 9:33AM

Exporter

Pour exporter les logs dans la vue actuelle :

1. Cliquez sur **Exporter** et sélectionnez l'une des options de la liste déroulante, le **Format CSV** ou **Séparé par des tabulations**. Le fichier est téléchargé avec un nom de fichier qui identifie le type de log et le séparateur de champ. Par exemple, un log système Security Analytics exporté avec des valeurs séparées par des virgules est nommé **UAP_log_export_CSV.txt**, et un log d'appliance exporté avec des valeurs séparées par des tabulations est nommé **APPLIANCE_log_export_TAB.txt**.

Last Modified: August 10 2016, 9:33AM

Onglet En temps réel

Cette rubrique décrit les fonctions des onglets En temps réel accessibles dans Consignation système et Logs de services.

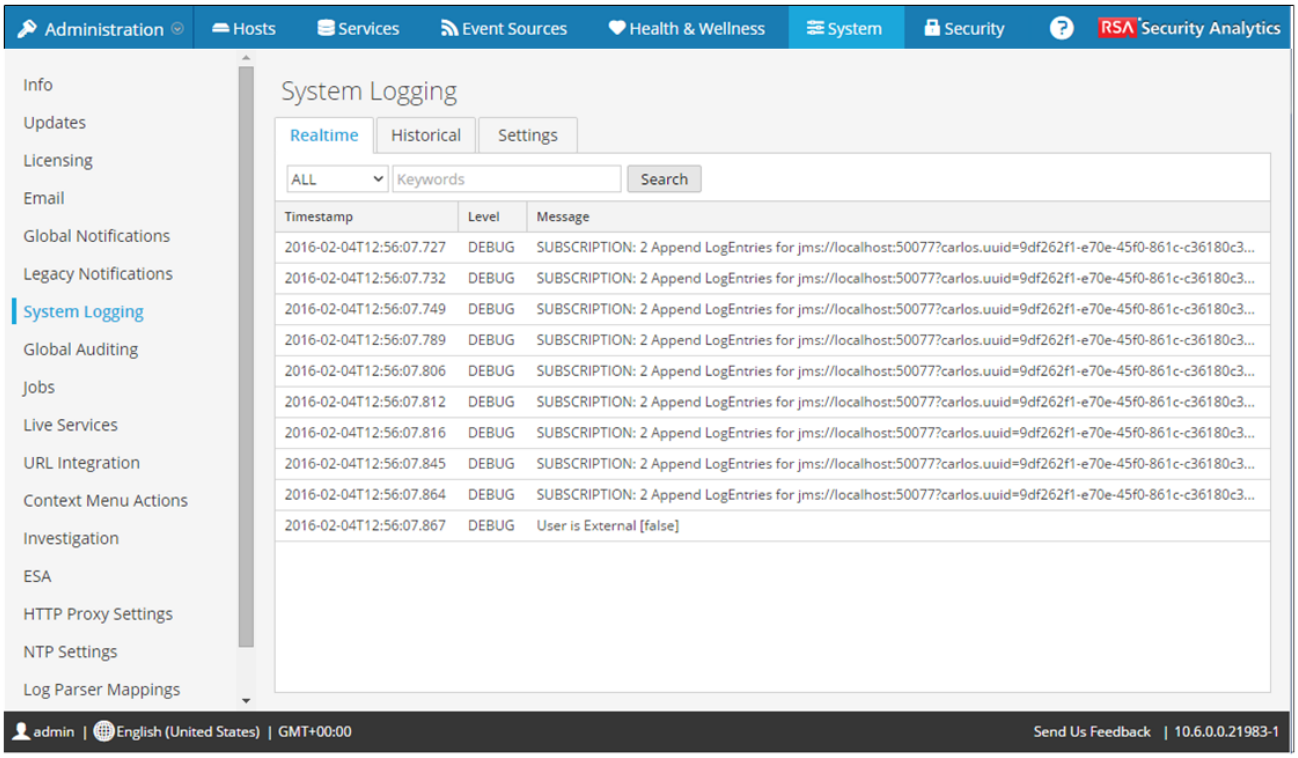
L'onglet **En temps réel** affiche une vue du log Security Analytics ou d'un service. Lors de son chargement initial, cette vue contient les 10 dernières entrées du log. Lorsque de nouvelles entrées deviennent disponibles, elles sont intégrées à la vue.

Pour accéder à l'onglet En temps réel :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Système.**
2. Dans le panneau des options, sélectionnez **Consignation système**.
   Le panneau Consignation système affiche par défaut l'onglet **En temps réel**.

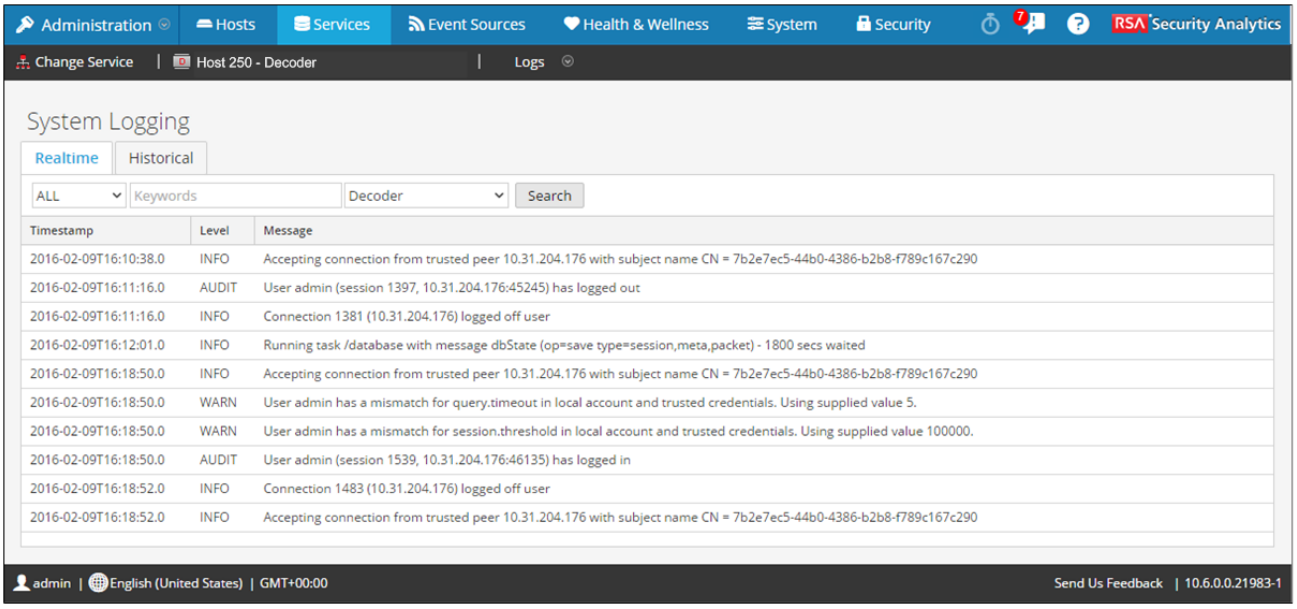
Pour obtenir des informations sur l'accès aux logs de service, reportez-vous à la rubrique Vue Logs de services.

Vous trouverez ci-dessous un exemple de l'onglet **En temps réel** dans le panneau Consignation système.



Last Modified: August 10 2016, 9:33AM

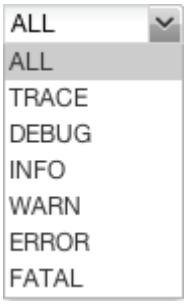
Vous trouverez ci-dessous un exemple de l'onglet **En temps réel** dans la vue Logs de services, qui est similaire.



Caractéristiques

L'onglet **En temps réel** comporte une barre d'outils dotée de champs de saisie qui permettent de filtrer les entrées. Sous cette barre d'outils se trouve une grille contenant les entrées du log.

Barre d'outils

Fonction	Description
Liste déroulante Niveau de consignation 	Sélectionne le niveau de consignation pour les entrées à afficher dans la grille. La liste déroulante **Niveau de consignation** affiche les niveaux de consignation disponibles pour le système ou le service. • Les logs système disposent de sept niveaux de consignation. • Les logs des services ne comptent que six niveaux de consignation car ils ne comprennent pas le niveau **SUIVRE**. • La valeur par défaut est **TOUTES** les entrées de log.
Champ Mot clés	Spécifie un mot clé à utiliser lors du filtrage des entrées. Ce champ est le même pour le filtrage des logs de service et de système.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
Champ Service (Logs de service uniquement)	Spécifie le type de service à utiliser lors du filtrage des entrées de log de service. Les valeurs possibles sont l'hôte ou le service.
Bouton Filtre	Cliquez sur ce bouton pour activer le filtre sur la base des niveaux de consignation, mots-clés et services sélectionnés.

Colonnes de la grille des logs

Colonne	Description
Horodatage	Il s'agit de l'horodatage de l'entrée.
Niveau	Il s'agit du niveau de consignation du message.
Message	Il s'agit du texte de l'entrée de log.

Onglet Paramètres

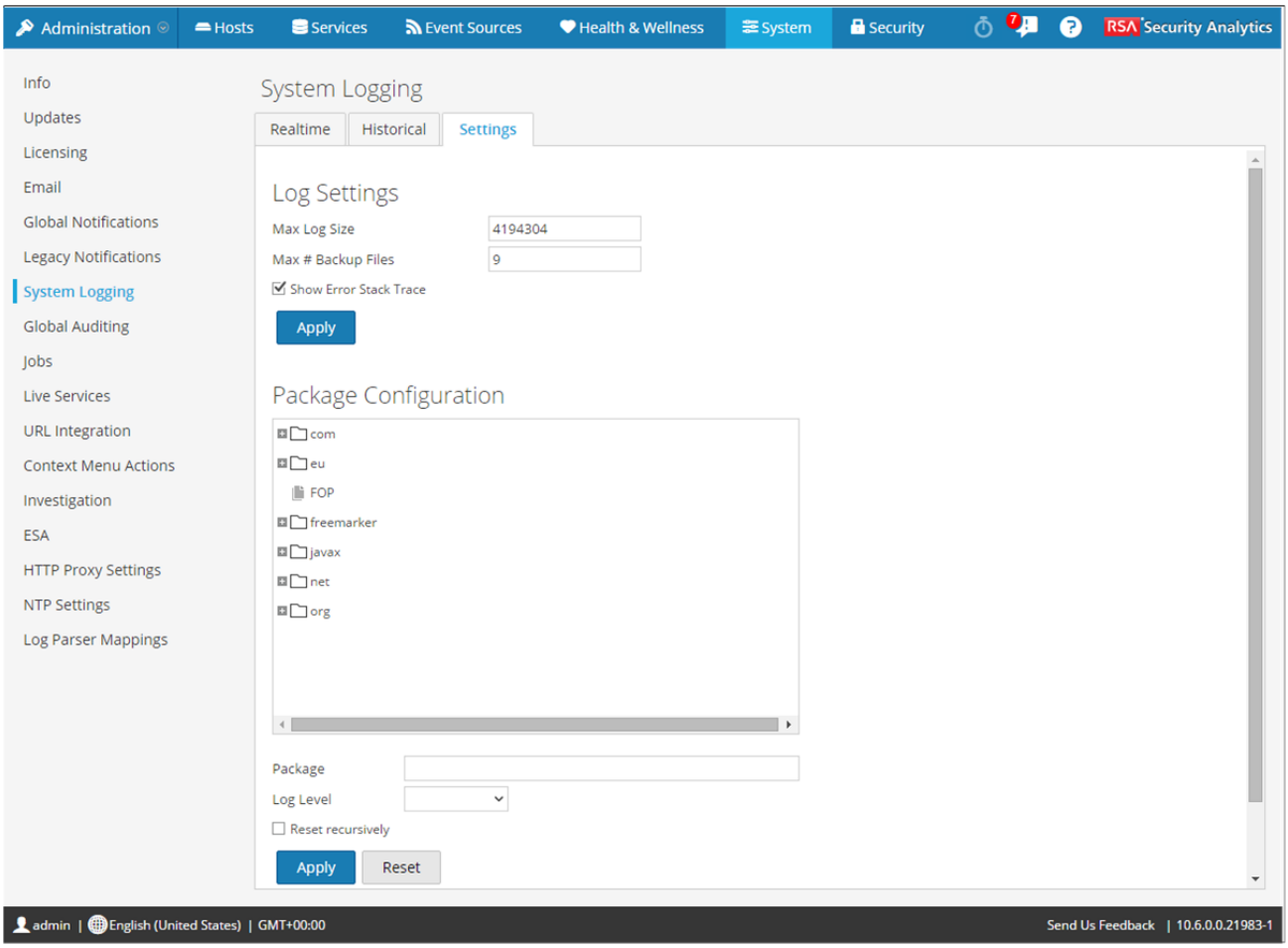
Cette rubrique présente les fonctions de l'onglet Paramètres du panneau Consignation système.

L'onglet Paramètres de RSA Security Analytics, accessible dans le panneau Consignation système, permet de configurer la taille des fichiers logs, le nombre de fichiers logs de sauvegarde gérés, ainsi que le niveau de consignation par défaut des packages dans Security Analytics. La rubrique Configurer les paramètres des fichiers logs propose des procédures détaillées.

Pour accéder à l'onglet Paramètres :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Système.**
2. Dans le panneau des options, sélectionnez **Consignation système**.
   Le panneau Consignation système qui s'ouvre affiche par défaut l'onglet En temps réel.
3. Cliquez sur l'onglet **Paramètres**.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

L'onglet **Paramètres** présente deux sections : Paramètres de log et Configuration des packages.

Paramètres de log

La section Paramètres de log permet de configurer la taille des fichiers logs Security Analytics et le nombre de logs de sauvegarde gérés par Security Analytics.

Fonction	Description
Taille de log max.	Configure la taille maximale (en octets) de chaque fichier log. La valeur minimale de ce paramètre est **4096**.
Nbre max. de fichiers de sauvegarde	Indique le nombre de fichiers logs de sauvegarde qui sont gérés. La valeur minimale de ce paramètre est **0**. Lorsque le nombre maximum de fichiers log est atteint et que le nouveau fichier de sauvegarde est élaboré, la sauvegarde la plus ancienne est ignorée.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
☐ Afficher la trace de pile d'erreurs	Activez la case à cocher pour afficher les messages log ERROR, STACK et TRACE.
Appliquer	Applique immédiatement les paramètres pour tous les futurs logs.

Configuration des packages

La section Configuration des packages affiche les packages Security Analytics sous forme d'arborescence.

Fonction	Description
Arborescence des packages	L'arborescence contient tous les packages utilisés dans Security Analytics. Vous pouvez descendre dans l'arborescence pour afficher les niveaux de consignation de chaque package. Le niveau **racine** correspond au niveau de consignation par défaut de tous les packages qui ne sont pas explicitement définis. Le niveau racine est paramétré sur **INFO**.
Champ Package	Ce champ contient le nom du package que vous sélectionnez dans l'arborescence **Package**.
Niveau de consignation	Si le package sélectionné est associé à un niveau de consignation explicite, sa valeur est affichée dans le champ **Niveau de consignation**.
☐ Réinitialiser de manière récursive	Activez la case à cocher pour réinitialiser le log de manière récursive.
Appliquer	Ce bouton permet d'appliquer immédiatement les paramètres pour tous les futurs logs.
Réinitialiser	Ce bouton permet de réinitialiser le package sélectionné sur le niveau de consignation **racine**.

Panneau Intégration d'URL

Cette rubrique présente les fonctions du panneau Intégration d'URL.

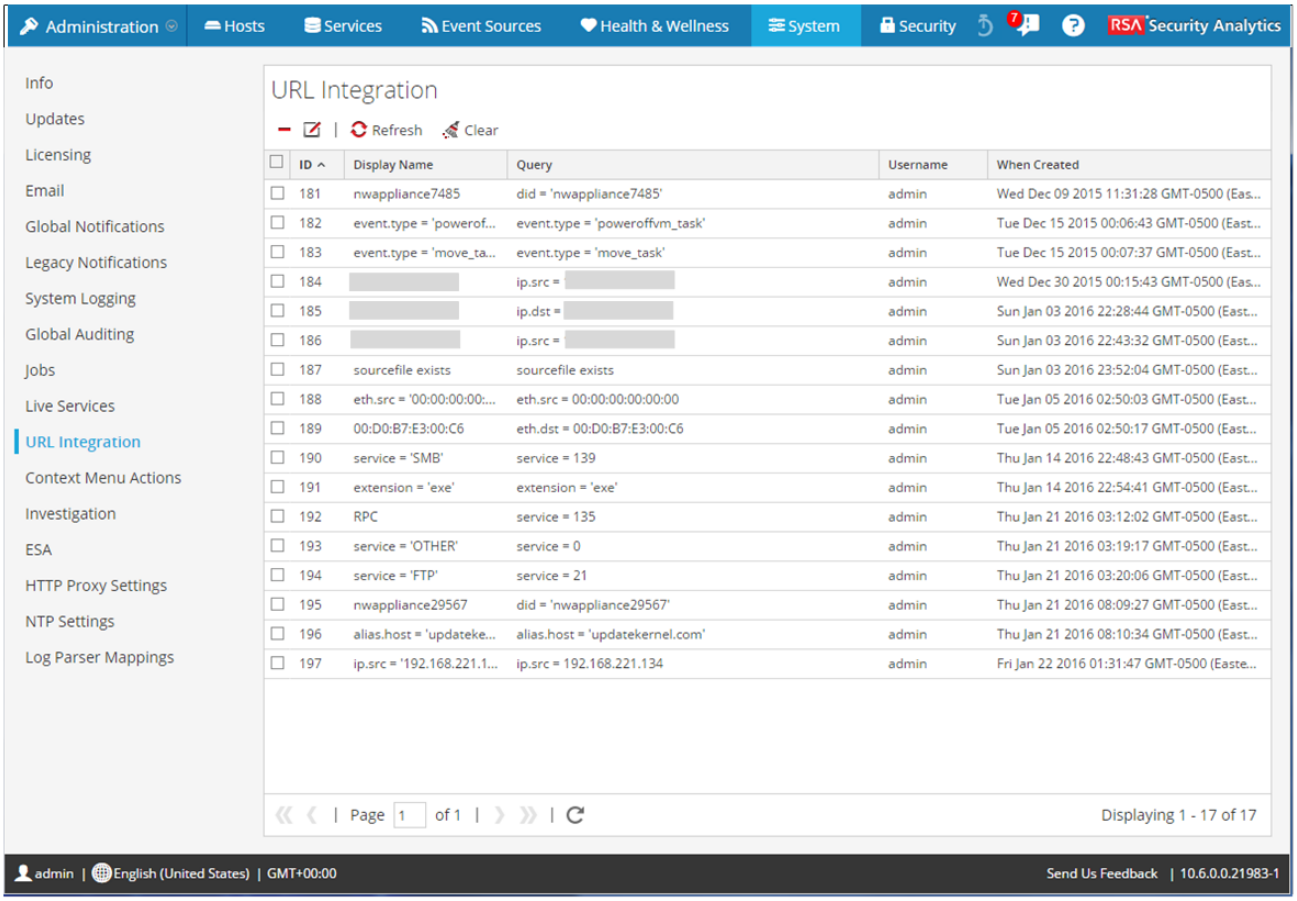
L'intégration d'URL fournit un moyen de représenter des fils d'Ariane ou des chemins de requête. L'utilisateur l'utilise lorsqu'il effectue une procédure d'enquête active d'un service dans la vue Navigation. La nécessité de consulter et de modifier ces objets se produit rarement.

> ⚠ **Caution:** Lorsqu'une requête est supprimée du système, les URL de procédure d'enquête comprenant l'ID de cette requête ne fonctionnent plus.

Pour accéder à cette vue :

1. Dans le menu **Security Analytics**, cliquez sur **Administration > Système**.
2. Dans le panneau des options, sélectionnez **Intégration d'URL**.

Last Modified: August 10 2016, 9:33AM



Composants

Le panneau Intégration d'URL comprend une grille et une barre d'outils. Ce tableau décrit les informations de la grille.

Colonne	Description
ID	Identifiant unique utilisé pour rechercher la requête dans le datastore Security Analytics.
Nom d'affichage	Chaîne qui s'affiche dans le fil d'Ariane.
Requête	Extrait de requête sous-jacente.
Nom d'utilisateur	Nom de l'utilisateur qui a effectué la requête.
Date de création	Date et heure auxquelles la requête a été effectuée.

La barre d'outils présente ces options.

Option	Description
	Supprime les requêtes sélectionnées. Security Analytics demande une confirmation pour la suppression des requêtes. Vous pouvez répondre **Oui** ou **Non**.
	Affiche la boîte de dialogue Modifier la requête.
	Actualise la liste.
	Efface la liste complète de requêtes. Security Analytics demande une confirmation pour l'effacement de la liste. Vous pouvez répondre **Oui** ou **Non**.

Last Modified: August 10 2016, 9:33AM

Paramètres de configuration des services

Cette rubrique présente les paramètres de configuration disponibles pour les services Core de RSA Security Analytics.

Les services RSA Security Analytics Core incluent des Brokers, des Concentrators, des Decoders, des Log Decoders, des Archivers et le service Appliance. Les paramètres de configuration de service répertoriés dans ces tableaux sont tous affichables et modifiables. Certains paramètres sont configurables en divers points de l'interface utilisateur Security Analytics et d'autres sont affichables ou configurables uniquement dans la vue Explorer les services.

Last Modified: August 10 2016, 9:33AM

Configuration du service Appliance

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour le service Core Appliance de RSA Security Analytics.

Le service Appliance de RSA Security Analytics Core surveille le matériel NetWitness existant.

Paramètres

Ce tableau décrit les paramètres de configuration Appliance.

Champ de configuration Appliance	Description
Logs	/logs/config, reportez-vous à la rubrique Configuration de la consignation de service Core
REST	/rest/config, reportez-vous à la rubrique Configuration de l'interface REST
Services	/services/<nom du service>/config, reportez-vous à la rubrique Configuration de service à service Core
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core

Last Modified: August 10 2016, 9:33AM

Configuration de service Archiver

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour RSA Security Analytics Archivers.

Paramètres de configuration d'Archiver

Ce tableau répertorie et décrit les paramètres de configuration d'Archiver.

Champ Configuration d'Archiver	Description
Archiver	/archiver/config, reportez-vous à la rubrique Nœuds de configuration pour l'agrégation
Base de données	/database/config, reportez-vous à la rubrique Nœuds de configuration de la base de données
Index	/index/config, reportez-vous à la rubrique Nœuds de configuration d'index
Logs	/logs/config, reportez-vous à la rubrique Configuration de la consignation de service Core
REST	/rest/config, reportez-vous à la rubrique Configuration de l'interface REST
SDK	/sdk/config, reportez-vous aux rubriques Nœuds de configuration SDK et Modes system.roles de service Security Analytics Core
Services	/services/<nom du service>/config, reportez-vous à la rubrique Configuration de service à service Core
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core

Last Modified: August 10 2016, 9:33AM

Configuration du service Broker

Cette rubrique répertorie et décrit les paramètres de configuration de RSA Security Analytics Brokers.

Paramètres de configuration

Ce tableau répertorie et décrit les paramètres de configuration de Broker.

Champ configuration de Broker	Description
Broker	/broker/config, reportez-vous à la rubrique Nœuds de configuration pour l'agrégation
aggregate.interval.behind	Nombre minimal de millisecondes avant qu'un autre lot d'agrégation ne soit demandé lorsque le service Broker est derrière. La modification prend effet immédiatement.
Base de données	/database/config, reportez-vous à la rubrique Nœuds de configuration de la base de données
Index	/index/config
index.dir	Répertoire dans lequel les fichiers de mappage du système de broker sont stockés. Les modifications prendront effet au redémarrage du service.
language.filename	Spécification de langage d'index (XML) qui est chargée au démarrage. Le service doit être redémarré en cas de modification.
Logs	/logs/config, reportez-vous à la rubrique Configuration de la consignation de service Core
REST	/rest/config, reportez-vous à la rubrique Configuration de l'interface REST

Last Modified: August 10 2016, 9:33AM

Champ configuration de Broker	Description
SDK	/sdk/config, reportez-vous aux rubriques Nœuds de configuration SDK et Modes system.roles de service Security Analytics Core
Services	/services/<nom du service>/config, reportez-vous à la rubrique Configuration de service à service Core
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core

RSA

Nœuds de configuration pour l'agrégation

Cette rubrique affiche et décrit les paramètres de configuration disponibles qui sont communs aux services qui effectuent l'agrégation, comme les RSA Security Analytics Concentrators et Archivers.

Paramètres de configuration de l'agrégation

Ce tableau affiche et décrit les paramètres qui contrôlent l'agrégation sur un service d'agrégation.

Chemin de configuration	/concentrator/config ou /archiver/config
aggregate.autostart	Redémarre automatiquement l'agrégation après un redémarrage de service, si activé. La modification prend effet immédiatement.
aggregate.buffer.size	Affiche la taille de la mémoire tampon (l'unité par défaut est le Ko) utilisée par lot d'agrégation. Les mémoires tampons plus grandes peuvent améliorer les performances de l'agrégation, mais pourraient avoir un impact sur les performances des requêtes. La modification prend effet au redémarrage de l'agrégation.
aggregate.crc	En cas d'activation, tous les flux d'agrégation seront validés par le contrôle de redondance cyclique (CRC). La modification prend effet immédiatement.
aggregate.hours	Affiche le nombre maximal d'heures au cours desquelles un service est autorisé à lancer l'agrégation. La modification prend effet immédiatement.
aggregate.interval	Affiche le nombre minimal de millisecondes entre deux demandes d'agrégation. La modification prend effet immédiatement.
aggregate.meta.page.factor	Affiche le nombre de pages de métadonnées allouées par session dans le cadre de l'agrégation. Les modifications prendront effet au redémarrage du service.
aggregate.meta.perpage	Affiche le nombre alloué de métadonnées stockées sur une page de données. Les modifications prendront effet au redémarrage du service.
aggregate.precache	Détermine si le Concentrator placera en précache le prochain cycle d'agrégation de services en amont. Peut améliorer les performances de l'agrégation, mais pourrait affecter les performances de la requête. La modification prend effet immédiatement.

Last Modified: August 10 2016, 9:33AM

Chemin de configuration	/concentrator/config ou /archiver/config
aggregate.sessions.max	Affiche le nombre de sessions à agréger à chaque fois. La modification prend effet au redémarrage de l'agrégation.
aggregate.sessions.perpage	Affiche le nombre de sessions stockées sur une page de données. Les modifications prendront effet au redémarrage du service.
aggregate.time.window	Affiche la période +/- maximale, en secondes, dans laquelle tous les services doivent se trouver avant qu'un autre cycle d'agrégation soit demandé. Zéro désactive la période. La modification prend effet immédiatement.
consume.mode	Détermine si le Concentrator peut uniquement effectuer une agrégation localement ou sur un réseau en fonction des restrictions de licences. Les modifications prendront effet au redémarrage du service.
export.enabled	Lorsqu'elle est activée, cette option permet d'exporter les données de la session. Les modifications prendront effet au redémarrage du service.
export.expire.minutes	Répertorie le nombre de minutes avant l'expiration et le vidage des fichiers cache d'exportation. La modification prend effet immédiatement.
export.format	Détermine le format de fichier utilisé lors de l'exportation des données. Les modifications prendront effet au redémarrage du service.
export.local.path	Affiche l'emplacement local pour mettre en cache les données exportées. Taille maximale assignée en option (=#unit), les unités sont : t pour To, g pour Go, m pour Mo. Les modifications prendront effet au redémarrage du service.
export.meta.fields	Détermine les champs méta qui sont exportés. Liste de champs avec virgule. L'étoile indique tous les champs. L'étoile plus la liste de champs indique tous les champs SAUF les champs répertoriés. Une simple liste de champs indique d'inclure uniquement ces champs. La modification prend effet immédiatement.
export.remote.path	Affiche le protocole distant (nfs://) et l'emplacement pour exporter les données. Les modifications prendront effet au redémarrage du service.
export.rollup	Détermine l'intervalle cumulatif pour exporter les champs. Les modifications prendront effet au redémarrage du service.
export.session.max	Affiche les sessions maximales par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
export.size.max	Affiche le nombre maximal d'octets par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce

Chemin de configuration	/concentrator/config ou /archiver/config
	paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
export.usage.max	Affiche le pourcentage maximal d'espace de cache utilisé avant l'arrêt de l'agrégation. Zéro indique aucune limite. La modification prend effet immédiatement.
heartbeat.error	Affiche le temps d'attente (en secondes) après une erreur de service avant de tenter la reconnexion du service. La modification prend effet immédiatement.
heartbeat.interval	Affiche le nombre de millisecondes entre les vérifications du service heartbeat. La modification prend effet immédiatement.
heartbeat.next.attempt	Affiche le temps d'attente (en secondes) avant de tenter la reconnexion du service. La modification prend effet immédiatement.
heartbeat.no.response	Affiche le temps d'attente (en secondes) avant de mettre hors ligne un service qui ne répond pas. La modification prend effet immédiatement.

Last Modified: August 10 2016, 9:33AM

Configuration du service Concentrator

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour RSA Security Analytics Concentrators.

Paramètres de configuration de Concentrator

Ce tableau répertorie et décrit les paramètres de configuration de Concentrator.

Champ Configuration de Concentrator	Description
Concentrator	/concentrator/config, reportez-vous à la rubrique Nœuds de configuration pour l'agrégation
Base de données	/database/config, reportez-vous à la rubrique Nœuds de configuration de la base de données
Index	/index/config, reportez-vous à la rubrique Nœuds de configuration d'index
Logs	/logs/config, reportez-vous à la rubrique Configuration de la consignation de service Core
REST	/rest/config, reportez-vous à la rubrique Configuration de l'interface REST
SDK	sdk/config, reportez-vous aux rubriques Nœuds de configuration SDK et Modes system.roles de service Security Analytics Core
Services	/services/<nom du service>/config, reportez-vous à la rubrique Configuration de service à service Core
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core

Last Modified: August 10 2016, 9:33AM

Configuration de la consignation de service Core

Cette rubrique répertorie et décrit les paramètres de configuration de la consignation disponibles pour tous les services RSA Security Analytics Core.

La configuration de la consignation est identique sur tous les services Security Analytics Core.

Paramètres

Le tableau suivant décrit les paramètres de configuration de la consignation :

Dossier de configuration des logs	/logs/config
log.dir	Affiche le répertoire dans lequel est stockée la base de données des logs. La taille maximale assignée en option (=#) est exprimée en Mo. Les modifications prendront effet au redémarrage du service.
log.levels	Contrôle les types de messages de log qui sont stockés (au format CSV). Les paramètres propres aux différents modules sont définis comme suit : <Module>=[debug|info|audit|warning|failure|all|none]. La modification prend effet immédiatement.
log.snmp.agent	Définit un agent distant de réception de messages de trap SNMP.
snmp.trap.version	Définit la version SNMP à utiliser pour les demandes GET et les traps (2c ou 3).
snmpv3.engine.boots	Affiche le nombre de démarrages du moteur SNMPv3. Ce champ s'incrémente automatiquement au démarrage. Il ne doit donc normalement pas être défini par l'utilisateur.
snmpv3.engine.id	Définit l'ID du moteur SNMPv3 sur un nombre hexadécimal 10-64, éventuellement précédé de 0x. Vous pouvez ajouter des valeurs de suffixe à la fin de l'ID du moteur pour chacun des services Core SA exécutés sur le même hôte. Par exemple, si l'ID de moteur généré pour l'hôte Core SA est 0x1234512345, vous pouvez le définir sur 0x123451234501 pour le service Decoder et sur 0x123451234504 pour le service Appliance.
snmpv3.trap.auth.local.key	Définit la clé locale d'authentification trap SNMPv3 sous la forme d'un nombre hexadécimal de 16 à 20 chiffres (selon le protocole utilisé) précédé de 0x. Pour MD5, cette clé comporte 16 chiffres hexadécimaux. Pour SHA, elle en comporte 20. Vous pouvez utiliser l'algorithme de votre choix pour générer les clés locales. Il est recommandé de préférer une méthode de génération aléatoire à la sélection manuelle des valeurs de clé.
snmpv3.trap.auth.protocol	Affiche le protocole d'authentification trap SNMPv3 (aucun, MD5 ou SHA).

Last Modified: August 10 2016, 9:33AM

snmpv3.trap.priv.local.key	Définit la clé locale de confidentialité trap SNMPv3, qui comporte 16 chiffres hexadécimaux précédés de 0x.
snmpv3.trap.priv.protocol	Affiche le protocole de confidentialité trap SNMPv3 (aucun ou AES).
snmpv3.trap.security.level	Affiche le niveau de sécurité trap SNMPv3, qui indique si l'authentification et la confidentialité sont utilisées. Valeurs possibles : noAuthNoPriv, authNoPriv et authPriv.
snmpv3.trap.security.name	Définit le nom de sécurité trap SNMPv3 utilisé pendant l'authentification trap SNMPv3.
syslog.size.max	Affiche la taille maximale d'un log envoyé à syslog (certains processus syslog rencontrent des problèmes avec les messages très volumineux). Zéro indique aucune limite. La modification prend effet immédiatement.

Configuration de service à service Core

Cette rubrique répertorie et décrit les paramètres de configuration qui contrôlent la façon dont un service Core se connecte à un autre service Core. Par exemple, lorsqu'un Concentrator se connecte à un Decoder, les paramètres de cette connexion sont contrôlés par ces paramètres.

Chaque fois qu'un service Core établit une connexion à un autre service Core, le service qui agit en tant que **client** crée un nouveau sous-dossier dans le dossier des /services de l'arborescence de configuration. Le nom du sous-dossier correspond au nom du service et le format est `host:port`. Par exemple, le dossier de connexion du service pour une connexion Concentrator vers un Decoder pourrait être `/services/reston-va-decoder:50004`. Dans chaque dossier de connexion de service, un sous-dossier `config` détient des paramètres configurables.

Paramètres

Le tableau suivant décrit les paramètres de Configuration du service.

Services	/services/host:port/config
allow.nonssl.to.ssl	Permet une connexion non-SSL pour se connecter à un service SSL, lorsqu'il est défini sur la valeur true. Sinon, s'il est défini sur false, les connexions non sécurisées à sécurisées seront refusées. La modification prend effet immédiatement.
compression	Affiche un nœud de configuration qui détermine si les données sont compressées avant des les envoyer. Une valeur positive détermine le nombre d'octets qui doivent être envoyés avant d'être compressés. Zéro signifie aucune compression.
crc.checksum	Affiche un nœud de configuration qui détermine si les flux de données sont validés avec une somme de contrôle CRC. Une valeur positive détermine le nombre d'octets qui doivent être envoyés avant d'être validés par CRC. Zéro signifie aucune validation CRC.
ssl	Affiche un nœud de configuration qui active ou désactive le chiffrement SSL sur la connexion.

Last Modified: August 10 2016, 9:33AM

Configuration système de service Core

Cette rubrique répertorie et décrit les paramètres de configuration communs à tous les services Core Security Analytics RSA.

Paramètres

Le tableau suivant répertorie et décrit les paramètres de configuration du système :

Dossier de configuration du système	/sys/config
compression	Affiche le montant minimal d'octets avant la compression d'un message, lorsqu'il est défini sur une valeur positive. Zéro indique aucune compression de message. La modification prend effet aux connexions suivantes.
crc.checksum	Affiche les octets minimum avant d'envoyer un message sur le réseau avec une somme de contrôle CRC (à valider par le client), lorsqu'il est défini sur une valeur positive. Zéro indique aucune validation de somme de contrôle CRC avec un message. La modification prend effet aux connexions suivantes.
Lecteurs	Affiche les lecteurs afin de surveiller les statistiques d'utilisation. Les modifications prendront effet au redémarrage du service.
port	Affiche le port sur lequel écoutera ce service. Les modifications prendront effet au redémarrage du service.
scheduler	Affiche le dossier des tâches planifiées.
service.name.override	Affiche le nom d'un service facultatif utilisé par les services en amont pour l'agrégation au lieu du nom d'hôte.
ssl	Chiffre tout le trafic via le protocole SSL, s'il est activé. Les modifications prendront effet au redémarrage du service.
stat.compression	Compresse les statistiques si elles sont écrites dans la base de données, si activé. Les modifications prendront effet au redémarrage du service.
stat.dir	Affiche le répertoire de stockage de l'historique de la base de données des statistiques (plusieurs répertoires séparés par des points-virgules). Taille maximale assignée en option (=#unit), les unités sont : t pour To, g pour Go, m pour Mo. Les modifications prendront effet au redémarrage du service.
stat.exclude	Répertorie les chemins d'accès des statistiques à exclure de la base de données des statistiques. Les caractères génériques suivants sont autorisés : ? correspond à tout

Last Modified: August 10 2016, 9:33AM

	caractère unique, * correspond à zéro ou plusieurs caractères jusqu'au délimiteur /, ** correspond à zéro ou plusieurs caractères, y compris le délimiteur. La modification prend effet immédiatement.
stat.interval	Détermine la fréquence (en millisecondes) à laquelle les nœuds statistiques sont mis à jour dans le système. La modification prend effet immédiatement.
threads	Répertorie le nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. La modification prend effet immédiatement.

RSA

Configuration du service Decoder

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour RSA Security Analytics Decoders.

Paramètres de configuration Decoder

Ce tableau répertorie et décrit les paramètres de configuration de Decoder.

Champ de configuration Decoder	Description
Decoder	/decoder/config, reportez-vous à la rubrique Configuration commune à Decoder et Log Decoder
Base de données	/database/config, reportez-vous à la rubrique Nœuds de configuration de la base de données
Index	/index/config, reportez-vous à la rubrique Nœuds de configuration d'index
Logs	/logs/config, reportez-vous à la rubrique Configuration de la consignation de service Core
REST	/rest/config, reportez-vous à la rubrique Configuration de l'interface REST
SDK	/sdk/config, reportez-vous aux rubriques Nœuds de configuration SDK et Modes system.roles de service Security Analytics Core
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core

Last Modified: August 10 2016, 9:33AM

RSA

Configuration commune à Decoder et Log Decoder

Cette rubrique répertorie et décrit les paramètres de configuration qui sont identiques dans les services Packet Decoder et Log Decoder.

Paramètres de configuration Decoder

Ce tableau affiche et décrit les paramètres de configuration partagés de Decoder et Log Decoder.

Chemin de configuration de Decoder	/decoder/config
aggregate.buffer.size	Affiche la taille de la mémoire tampon (l'unité par défaut est le Ko) utilisée par lot d'agrégation. Les mémoires tampons plus grandes peuvent améliorer les performances de l'agrégation, mais pourraient avoir un impact sur les performances de la capture. La modification prend effet au redémarrage de la capture.
aggregate.precache	Détermine si le Decoder placera en précache le prochain cycle d'agrégation de services en amont. Peut améliorer les performances de l'agrégation, mais pourrait affecter les performances de la capture. La modification prend effet immédiatement.
assembler.pool.ratio	Affiche le pourcentage de pages de pool gérées et utilisées par l'assembleur pour le processus d'assemblage. Les modifications prendront effet au redémarrage du service.
assembler.session.flush	Vide les sessions une fois exécutées (1) ou vide les sessions lorsqu'elles sont analysées (2). Les modifications prendront effet au redémarrage du service.
assembler.session.pool	Affiche le nombre d'entrées dans le pool de sessions. Les modifications prendront effet au redémarrage du service.
assembler.size.max	Affiche la taille maximale d'une session. Un paramètre 0 supprime la limite de taille de la session. La modification prend effet immédiatement.
assembler.size.min	Affiche la taille minimale qu'une session doit avoir avant d'être persistante. La modification prend effet immédiatement.
assembler.timeout.packet	Affiche le nombre de secondes qui s’écoulent avant l’expiration des paquets. La modification prend effet immédiatement.
assembler.timeout.session	Affiche le nombre de secondes qui s’écoulent avant l’expiration des sessions. La modification prend effet immédiatement.
assembler.voting.weights	Affiche les pondérations permettant de déterminer le flux de sessions marqués client et serveur. La modification prend effet immédiatement.

Last Modified: August 10 2016, 9:33AM

capture.autostart	Détermine si la capture commence automatiquement lorsque le service démarre. Les modifications prendront effet au redémarrage du service.
capture.buffer.size	Affiche la taille d'allocation de la mémoire tampon pour la capture (l'unité par défaut est le Mo). Les modifications prendront effet au redémarrage du service.
capture.device.params	Affiche les paramètres spécifiques au service de capture. Les modifications prendront effet au redémarrage du service. Les paramètres compris par ce champ sont spécifiques au périphérique de capture actuellement sélectionné. Si les paramètres ne sont pas reconnus par le périphérique de capture actuel, ils sont ignorés. Sur les Log Decoders, il n'y a que le périphérique de capture des événements consignés. Il accepte certains paramètres facultatifs. • **use-envision-time** : si ce paramètre est défini sur 1, la méta de temps de chaque événement sera importée à partir du flux Log Collector. Si le paramètre est défini sur 0 ou non défini, l'heure de l'événement importé est stockée dans la méta event.time. • **port** : ce paramètre peut être défini sur une valeur numérique afin de remplacer le port d'écoute syslog par défaut (514).
capture.selected	Affiche le service et l'interface de capture actuels. La modification prend effet immédiatement.
export.expire.minutes	Répertorie le nombre de minutes avant l'expiration et le vidage des fichiers cache d'exportation. La modification prend effet immédiatement.
export.packet.enabled	Lorsqu'elle est activée, cette option permet d'exporter les données des paquets. Les modifications prendront effet au redémarrage du service.
export.packet.local.path	Affiche l'emplacement local pour la mise en cache des données exportées des paquets. Taille maximale assignée en option (=#unit), les unités sont : t pour To, g pour Go, m pour Mo. Les modifications prendront effet au redémarrage du service.
export.packet.max	Affiche le nombre maximal de paquets par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
export.packet.remote.path	Affiche le protocole distant (nfs://) et l'emplacement pour exporter les données. Les modifications prendront effet au redémarrage du service.
export.packet.size.max	Affiche le nombre maximal d'octets de paquets par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
export.rollup	Détermine l'intervalle cumulatif pour exporter les champs. Les modifications prendront effet au redémarrage du service.
export.session.enabled	Lorsqu'elle est activée, cette option permet d'exporter les données de la session. Les modifications prendront effet au redémarrage du service.
export.session.format	Détermine le format de fichier utilisé lors de l'exportation des sessions. Les modifications prendront effet au redémarrage du service.

export.session.local.path	Affiche l'emplacement local pour la mise en cache des données exportées des sessions. Taille maximale assignée en option (=#unit), les unités sont : t pour To, g pour Go, m pour Mo. Les modifications prendront effet au redémarrage du service.
export.session.max	Affiche les sessions maximales par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
export.session.meta.fields	Détermine les champs méta qui sont exportés. Liste de champs avec virgule. L'étoile indique tous les champs. L'étoile plus la liste de champs indique tous les champs SAUF les champs répertoriés. Une simple liste de champs indique d'inclure uniquement ces champs. La modification prend effet immédiatement.
export.session.remote.path	Affiche le protocole distant (nfs://) et l'emplacement pour exporter les données. Les modifications prendront effet au redémarrage du service.
export.session.size.max	Répertorie le nombre maximum d'octets de la session par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
export.usage.max	Répertorie le nombre maximum d'octets de la session par fichier exporté. Pour les types de fichier d'exportation qui se mettent en cache, ce paramètre détermine les tailles de la mémoire cache. Zéro indique aucune limite. La modification prend effet immédiatement.
parse.threads	Affiche le nombre de threads d'analyse à utiliser pour l'analyse de session. Zéro signifie que le serveur décide. Les modifications prendront effet au redémarrage du service.
pool.packet.page.size	Affiche la taille d'une page de paquet (la valeur par défaut s'exprime en Ko). Les modifications prendront effet au redémarrage du service.
pool.packet.pages	Affiche le nombre de pages de paquets allouées et utilisées par le Decoder. Les modifications prendront effet au redémarrage du service.
pool.session.page.size	Affiche la taille d'une page de session (la valeur par défaut s'exprime en Ko). Les modifications prendront effet au redémarrage du service.
pool.session.pages	Affiche le nombre de pages de sessions allouées et utilisées par le Decoder. Les modifications prendront effet au redémarrage du service.

Configuration de service Log Decoder

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour les services RSA Security Analytics Log Decoder.

Paramètres de configuration de Log Decoder

Ce tableau répertorie et décrit les paramètres de configuration de Log Decoder.

Champ Configuration de Log Decoder	Description
Base de données	/database/config, reportez-vous à la rubrique Nœuds de configuration de la base de données
Decoder	/decoder/config, reportez-vous à la rubrique Configuration commune à Decoder et Log Decoder
Index	/index/config, reportez-vous à la rubrique Nœuds de configuration d'index
Logs	/logs/config, reportez-vous à la rubrique Configuration de la consignation de service Core
REST	/rest/config, reportez-vous à la rubrique Configuration de l'interface REST
SDK	/sdk/config Reportez-vous aux rubriques Nœuds de configuration SDK et Modes du service de base Security Analytics Core system.roles
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core

Paramètres de configuration du générateur de tokens pour les logs

Le service Log Decoder comprend un ensemble d'éléments de configuration qui contrôlent la manière dont le générateur de tokens crée les éléments méta pour les logs non analysés.

Le générateur de tokens associés aux logs ajoute les éléments méta `word` aux logs. Ces éléments word forment un index de texte intégral lorsqu'ils sont introduits dans le moteur d'indexation sur les services Concentrator et Archiver.

Last Modified: August 10 2016, 9:33AM

Ces éléments de configuration sont situés dans le dossier **/decoder/parsers/config**.

Champ Configuration des analyseurs Log Decoder	Description
token.device.types	Ensemble de types de périphériques qui seront scannés pour les tokens de texte brut. Par défaut, ce paramètre est configuré sur `unknown`, ce qui signifie que seuls les logs qui ne sont pas analysés seront scannés pour le texte brut. Vous pouvez ajouter des types de logs supplémentaires à cet emplacement afin d'enrichir les logs analysés avec les informations de tokens de texte. Si ce champ est vide, alors le générateur de tokens pour les logs est désactivé.
token.char.classes	Ce champ contrôle le type de tokens qui sont générés. Il peut s'agir d'une combinaison de valeurs `alpha`, `digit`, `space` et `punct`. La valeur par défaut est `alpha`. • **alpha** : Les tokens peuvent contenir des caractères alphanumériques • **digit** : Les tokens peuvent contenir des nombres • **space** : Les tokens peuvent contenir des espaces et des tabulations • **punct** : Les tokens peuvent contenir des marques de ponctuation
token.max.length	Ce champ permet de limiter la longueur des tokens. La valeur par défaut est de 5 caractères. Le paramètre de longueur maximale permet au Log Decoder de limiter l'espace nécessaire pour stocker les méta word. L'utilisation de jetons plus longs nécessite de l'espace supplémentaire dans la base de métadonnées, mais garantit des recherches de texte brut légèrement plus rapides. L'utilisation de jetons plus courts contraint le programme de résolution de requête de texte à effectuer plus d'accès en lecture dans les logs bruts au cours des recherches, mais cela a pour effet d'utiliser beaucoup moins d'espace dans la base de métadonnées et l'index.
token.min.length	Il s'agit de la longueur minimale d'un token de texte de recherche. La longueur de token minimale correspond au nombre minimum de caractères qu'un utilisateur peut saisir dans la zone de recherche afin de localiser les résultats. La valeur recommandée est la valeur par défaut, 3.
token.unicode	Ce paramètre booléen contrôle si les règles de classification Unicode sont appliquées lors de la classification des caractères en fonction du paramètre token.char.classes. Si ce paramètre est défini sur true, chaque log sera traité comme une séquence de points de code chiffrés UTF-8 , et donc la classification sera effectuée après l'exécution du déchiffrement UTF-8. Si ce paramètre est défini sur false, alors chaque log sera traité en mode ASCII et seule la classification des caractères ASCII sera effectuée. La classification des caractères Unicode nécessite plus de ressources CPU sur le service Log Decoder. Si l'indexation du texte dans une autre langue que l'anglais vous est inutile, vous pouvez désactiver ce paramètre pour réduire l'utilisation du processeur sur le service Log Decoder. Le mode par défaut est activé.

RSA

Configuration de l'interface REST

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour l'interface REST, intégrée dans tous les services Core de RSA Security Analytics.

Paramètres

Le tableau suivant répertorie et décrit les paramètres de configuration de l'interface REST.

Chemin de configuration de REST	/rest/config
cache.dir	Affiche le répertoire hôte à utiliser pour créer et stocker provisoirement les fichiers. La modification prend effet au redémarrage du service.
cache.size	Affiche le taille totale maximale (unité par défaut = Mo) de tous les fichiers du répertoire cache avant la suppression des plus anciens. La modification prend effet au redémarrage du service.
enabled	Bascule sur activer ou désactiver les services REST. 1 correspond à activé et 0 à désactivé. La modification prend effet au redémarrage du service.
port	Affiche le port sur lequel le service REST écoute. La modification prend effet au redémarrage du service.
ssl	Chiffre l'ensemble du trafic REST à l'aide du protocole SSL s'il est activé. La méthode par défaut est l'utilisation de la configuration issue de /sys/config/ssl. La modification prend effet au redémarrage du service.

Last Modified: August 10 2016, 9:33AM

RSA

Modes system.roles de service Security Analytics Core

Tous les services Security Analytics Core proposent des modes d'autorisation basés sur des rôles. Cette rubrique décrit les modes disponibles et leur configuration au sein de chaque service.

system.roles

Le nœud de configuration `/sdk/config/system.roles` définit les autorisations d'interrogation et d'affichage des métadonnées et du contenu basées sur des clés. Ce paramètre prend en charge la fonction de gestion de la confidentialité des données et, lorsqu'il est activé, l'utilisation de l'une des valeurs différente de zéro permet à un responsable de la confidentialité des données de contrôler l'accès aux clés et contenu des métadonnées. Ce paramètre est configurable dans l'interface utilisateur Security Analytics (pour plus de détails, voir Onglet Confidentialité des données). Lorsque la valeur est modifiée, la modification est appliquée immédiatement.

Zéro signifie que les autorisations de service basées sur les métaclés SDK sont désactivées.

- 0 = désactivé.

Lorsque l'une des valeurs différentes de zéro est spécifiée, le responsable de la confidentialité des données peut sélectionner une métaclé pour autoriser ou interdire l'affichage de la métadonnée ou du contenu associé, ou des deux, pour un rôle d'utilisateur spécifique sur un service.

- 1 - autoriser métadonnée et contenu filtrés
- 2 - autoriser métadonnée filtrée
- 3 - autoriser contenu filtré
- 4 - interdire métadonnée et contenu filtrés
- 5 - interdire métadonnée filtrée
- 6 - interdire contenu filtré

Last Modified: August 10 2016, 9:33AM

RSA

Vue Hôtes

Vous pouvez gérer et configurer les hôtes et les groupes d'hôtes qui sont disponibles dans les modules RSA Security Analytics. Utilisez cette vue pour effectuer les tâches suivantes :

- Rechercher et localiser rapidement un hôte ou un type d'hôte spécifique, comme Decoder, Broker ou Concentrator
- Ajouter, modifier ou supprimer des hôtes
- Rechercher les mises à jour sur les hôtes
- Mettre à jour un hôte vers une nouvelle version.
- Ajouter, modifier ou supprimer des groupes d'hôtes
- Trier les hôtes par nom et par hôte
- Filtrer les hôtes par nom et par hôte
- Effacer les provisions relatives aux hôtes

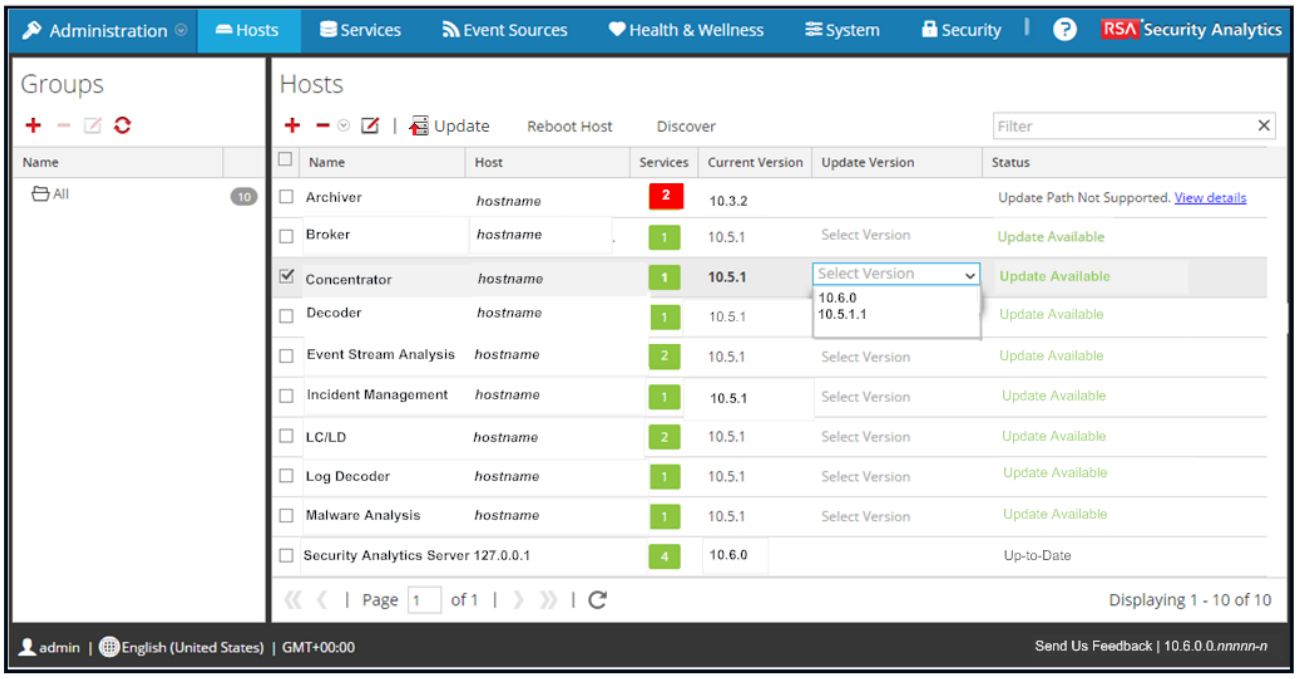
Les hôtes peuvent être physiques ou virtuels. Ils peuvent être mappés à un ou plusieurs des services suivants :

- Archiver
- Broker
- Concentrator
- Decoder
- Event Stream Analysis
- Gestion des incidents
- IPDB Extractor
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Warehouse Connector
- Workbench

Vous pouvez accéder aux services sur n'importe quel hôte en cliquant sur le bouton de la colonne Services de cet hôte.

Sélectionnez **Administration > Hôtes** dans le menu **Security Analytics** pour accéder à la vue Hôtes d'un module Security Analytics.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

La vue Hôtes contient deux panneaux :

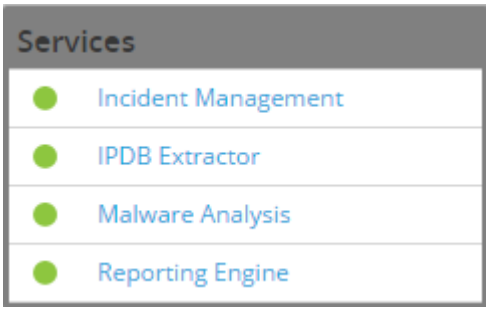
- Panneau Hôtes
- Panneau Groupes

Panneau Hôtes

Dans le panneau Hôtes, vous pouvez afficher des informations sur les hôtes et effectuer des opérations liées aux hôtes, telles que l'ajout, la suppression, la modification, la découverte, la mise à jour et le redémarrage. Vous pouvez rapidement basculer vers la vue Services pour obtenir des informations détaillées sur ces services. Le panneau Hôtes contient la liste des hôtes Security Analytics de votre déploiement Security Analytics et la barre d'outils du panneau Hôtes.

Colonne	Description
☐	Sélectionnez un ou plusieurs hôtes. Si vous activez la case à cocher dans le titre de la colonne, tous les hôtes sont sélectionnés.
Nom	Nom de l'hôte.
Hôte	Saisissez le nom d'hôte ou l'adresse IP de l'hôte.
Services	Affiche le nombre de services connectés à l'hôte dans la case. La couleur de la case indique l'état des services. Le vert indique que tous les services connectés sont démarrés (par exemple, la capture ou

Last Modified: August 10 2016, 9:33AM

Colonne	Description
	l'agrégation des données). Le jaune indique que certains des services connectés sont démarrés. Le rouge indique que les services connectés sont arrêtés. Cliquer sur la case sous **Services**indique le type de services connectés à l'hôte. Les services Security Analytics sont les suivants : Archiver, Broker, Concentrator, Context Hub, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Decoder, Log Collector, Malware Analysis, Reporting Engine, Warehouse Connector, et Workbench. Un rond coloré en vert indique que le service connecté a démarré. Un rond blanc indique que le service connecté est arrêté.  Vous pouvez cliquer sur les liens des services pour basculer vers la vue Services afin d'obtenir plus d'informations sur les services connectés.
Version actuelle	Affiche la version actuelle de l'hôte.
Mettre à jour la version	Affiche la ou les versions vers laquelle vous pouvez mettre à jour l'hôte. Sélectionnez la version vers laquelle vous souhaitez mettre à jour l'hôte. • Lorsqu'il n'y a qu'une seule version disponible, Security Analytics affiche *numéro de version*. Cliquez dessus pour la sélectionner. • Lorsque plusieurs versions sont disponibles, Security Analytics affiche Sélectionner la version. Cliquez sur Sélectionner la version, puis sélectionnez une version dans le menu déroulant.
État	Pour chaque hôte, affiche la disponibilité des mises à jour et la progression de la mise à jour après l'avoir lancée. Reportez-vous à la rubrique Mise à jour d'une version hôte pour une illustration de la vue Hôte avec ses états de mise à jour. • Mise à jour disponible - Une ou plusieurs mises à jour sont disponibles, mais pas appliquées. • **Chemin de mise à jour non pris en charge** - Si vous disposez d'un hôte de serveur autre que Security Analytics exécutant une version qui est antérieure au chemin de mise à jour 10.6.0 (par exemple, 10.4.0) et que vous avez mis à jour votre hôte de serveur Security Analytics vers la version 10.6.0, l'hôte de serveur autre que Security Analytics affichera le “chemin de mise à jour non pris en charge” dans la colonne État de la vue Hôtes. La mise à jour ne peut pas être effectuée depuis cette vue. Pour mettre l'hôte de serveur autre que Security Analytics sur le chemin non pris en charge : 1. Vérifiez que votre référentiel de mises à jour local dispose du fichier rpm compressé pour la version minimale prise en charge (par exemple, 10.4.1.0) (voir la rubrique Renseigner le référentiel de mises à jour local pour obtenir des instructions).

Colonne	Description
	2. Ouvrez une session SSH sur l'hôte de serveur autre que Security Analytics et remplacez le fichier `/etc/yum/vars/sarelease` par la version de mise à jour, par exemple '10.6.0.0'. (baseurl = http/smcupdate.netwitness.com/rsa/updates.10.4.1). 3. Exécutez `yum clean all` Avant d'exécuter la commande `yum update`, vérifiez que la mise à jour peut être effectuée vers cette version. 4. Exécutez la commande `yum update` • **La version de l'hôte ne peut pas être déterminée** - Contactez le Support Clients. • **Dans la file d'attente pour la mise à jour** - Si vous sélectionnez plusieurs hôtes à mettre à jour (affiche **Dans la file d'attente pour la mise à jour** - pendant que la version est appliquée à chaque hôte • **Téléchargement *n* sur *n*** - Suit la progression du téléchargement de la mise à jour par fichier. • **Exécution des vérifications pré-mise à jour sur l'hôte** - Vérification de la configuration de votre version actuelle pour s'assurer qu'il n'y a pas de conflit. • Avertissement de mise à jour. Voir les détails - Problème identifié dans votre configuration existante qui ne vous empêche pas d'effectuer la mise à jour vers la nouvelle version. Cliquez sur Voir les détails pour afficher la fenêtre du message d'avertissement. • Conflit de mise à jour. Voir les détails - Conflit identifié dans votre version actuelle qui bloque la mise à jour. Cliquez sur Voir les détails pour afficher la fenêtre du message de conflit. Vous devez résoudre ce conflit pour poursuivre la mise à jour. Pour obtenir des instructions sur le mode de résolution des conflits de configuration, reportez-vous à la rubrique Dépannage suite aux avertissements et erreurs liés à la pré-mise à jour et mise à jour vers la version 10.6. • Erreur de téléchargement. Voir les détails - Impossible de télécharger le fichier de mise à jour de version issu de votre référentiel de mise à jour local. • **Début de la mise à jour** - Démarrage de la mise à jour. • **Mise à jour des packages *n* sur *n*** - Suit la progression package par package de la mise à jour. • Erreur de mise à jour. Voir les détails - Erreur détectée lors de la mise à jour. Cliquez sur Voir les détails pour afficher la fenêtre du message d'erreur. Vous devez résoudre ce conflit pour poursuivre la mise à jour. Pour obtenir des instructions sur le mode de résolution des erreurs de mise à jour, reportez-vous à la rubrique Dépannage suite aux avertissements et erreurs liés à la pré-mise à jour et à la mise à jour vers la version 10.6. • **Redémarrer l'hôte** - Cliquez sur **Redémarrer l'hôte** dans la barre d'outils pour réinitialiser l'hôte et que les mises à jour prennent effet.

Panneau Groupes

Le panneau Groupes permet de créer des groupes d'hôtes logiques. Une fois que les hôtes sont regroupés, il est plus facile d'effectuer des opérations sur plusieurs hôtes en interagissant avec chaque hôte d'un groupe plutôt qu'avec chaque hôte d'une liste dégroupée.

Note: Dans Security Analytics Live, les groupes peuvent s'abonner aux ressources contrairement aux hôtes individuels qui ne peuvent pas effectuer l'opération.

Le panneau Groupes est composé d'une grille renseignée à l'aide de la liste des groupes d'hôtes définis et de la barre d'outils du panneau Groupes.

Colonne	Description
Nom	Nom du groupe d'hôtes. Un clic sur le nom du groupe dans le panneau Groupes permet d'afficher les hôtes de ce groupe dans le panneau hôtes.
<Vide>	Indique le nombre d'hôtes contenus dans le groupe. Un clic sur le nombre d'hôtes disponibles dans le groupe au sein du panneau Groupes permet d'afficher les hôtes de ce groupe dans le panneau Hôtes.

Last Modified: August 10 2016, 9:33AM

Barre d'outils du panneau Hôtes

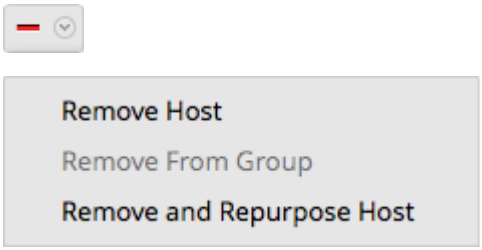
La barre d'outils de la vue Hôte contient les outils nécessaires pour assurer le maintien en conditions opérationnelles des hôtes de votre déploiement Security Analytics

Sélectionnez **Administration > Hôtes** dans le menu **Security Analytics** pour accéder à la vue Hôtes**.** La barre d'outils du panneau Hôtes se trouve en haut de la grille du même nom dans la vue Hôtes.

Caractéristiques

Le tableau suivant décrit les fonctions de la barre d'outils du panneau Hôtes.

Fonction	Description
+	Permet d'ouvrir la boîte de dialogue Ajouter un hôte pour y ajouter un hôte (reportezvous à Étape 1 : Ajouter ou mettre à jour un hôte). Les fonctions de cette boîte de dialogue sont les suivantes : **Nom** Nom que vous attribuez à l'hôte. **Nom d'hôte** Nom d'hôte ou adresse IP de la machine physique ou virtuelle de l'hôte. **Annuler** Ferme la boîte de dialogue sans ajouter l'hôte. **Enregistrer** Ajoute l'hôte.

Fonction	Description
	Permet d'afficher les options suivantes : • **Supprimer l'hôte** : Supprime un hôte inutile dans l'interface utilisateur Security Analytics et ses services associés. Si vous sélectionnez cette option, vous ne pourrez plus voir l'hôte et ses services associés dans Security Analytics. • **Retirer du groupe** : Si l'hôte fait partie d'un groupe d'hôtes, vous pouvez le supprimer de ce groupe. • **Supprimer et réaffecter l'hôte** : Cette option est disponible uniquement sur l'hôte d'applications primaire. Utilisez cette option pour reconstruire complètement un hôte.
	Permet d'ouvrir la boîte de dialogue Modifier l'hôte dans laquelle vous modifiez l'identification d'un hôte ou d'un service, ainsi que les paramètres de communication de base. Cette boîte de dialogue comporte les mêmes fonctions que la boîte de dialogue Ajouter un hôte. Procédures associées : • Étape 1 : Ajouter ou mettre à jour un hôte • Modifier le nom ou le nom d'hôte d'un hôte. • Modifier l'adresse IP ou le nom d'hôte d'un hôte
Mettre à jour	Permet de démarrer le processus de mise à jour.
Redémarrer l'hôte	Permet de redémarrer l'hôte.
Découvrir	La plupart du temps, la découverte est automatique. Il n'est donc pas nécessaire de cliquer sur le bouton Découvrir. Pour une nouvelle installation, cliquez sur Découvrir afin d'accéder à la boîte de dialogue Provisionner et de terminer la phase de provisionnement. Une fois terminée la phase de provisionnement via Security Analytics, la découverte des services exécutés sur l'hôte est automatique. Il n'est donc pas nécessaire de cliquer sur ce bouton.
	Permet de filtrer les hôtes par nom ou par hôte.

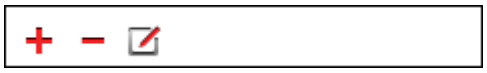
Barre d'outils du panneau Groupes

La barre d'outils du panneau Groupes contient les options de gestion des groupes d'hôtes. Utilisez la barre d'outils pour créer, modifier et supprimer des groupes. Lorsque vous créez un groupe, vous pouvez faire glisser des hôtes individuels du panneau Hôtes vers ce groupe.

Utilisez des groupes pour organiser les hôtes par fonction, géographie, projet ou tout autre système d'organisation utile. Un hôte peut appartenir à plusieurs groupes.

Sélectionnez **Administration > Hôtes** dans le menu **Security Analytics** pour accéder à la vue Hôtes. La barre d'outils du panneau Groupes se trouve en haut de la grille Groupes de la vue Hôtes.

Caractéristiques



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

Option	Description
+	Affiche une nouvelle ligne dans la grille Groupe dans laquelle vous entrez le nom d'un nouveau groupe.
−	Vous invite à confirmer que vous souhaitez supprimer le groupe ou l'hôte. Vous pouvez confirmer ou annuler la suppression.
	Ouvre le champ de nom d'une ligne dans la grille Groupe afin que vous puissiez saisir le nouveau nom d'un groupe existant.

Last Modified: August 10 2016, 9:33AM

Vue Services

La vue Services vous permet d'administrer les services et les groupes de services qui sont disponibles dans les modules RSA Security Analytics. Vous pouvez exécuter un ou plusieurs services sur un hôte. Chaque service est mappé à un hôte et effectue différentes tâches continues.

Vous pouvez administrer les services Security Analytics suivants :

- Archiver
- Broker
- Concentrator
- Context Hub
- Decoder
- Event Stream Analysis
- Gestion des incidents
- IPDB Extractor
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Warehouse Connector
- Workbench

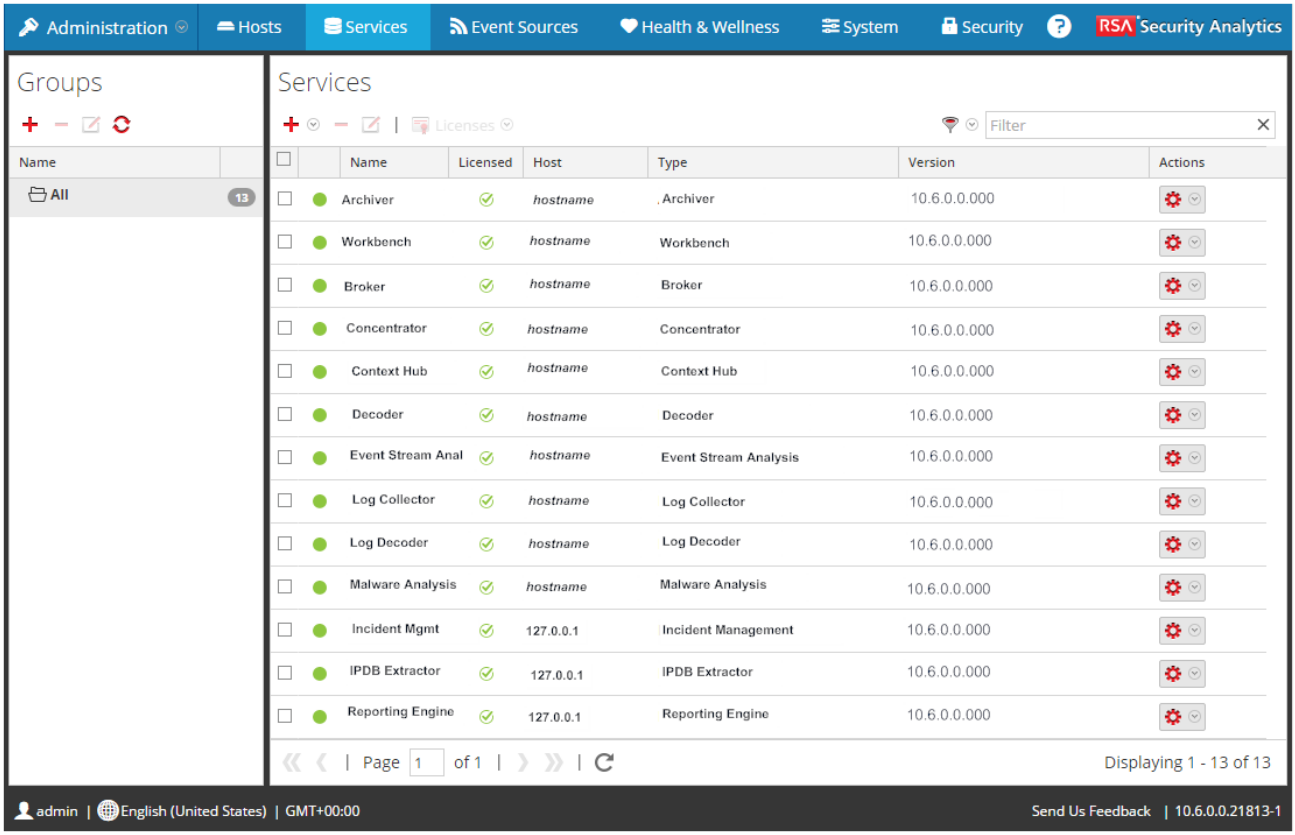
Dans la vue Services, vous pouvez :

- Rechercher et localiser rapidement un service ou un type de service spécifique, tel que Log Decoder ou Warehouse Connector
- Utiliser des raccourcis pour accéder aux tâches d'administration
- Ajouter, modifier et supprimer des services
- Gérer les licences et consulter l'état des licences d'un service (sous licence ou sans licence)
- Trier les services par nom et par hôte
- Filtrer les services par type et par nom et hôte
- Démarrer, arrêter ou redémarrer les services

Vous pouvez accéder à l'hôte sur lequel est exécuté un service en cliquant sur le lien dans la colonne Hôte de ce service.

Pour accéder à la vue Administration - Services depuis n'importe quel module Security Analytics, sélectionnez **Administration > Services** sous le menu **Security Analytics**.

Last Modified: August 10 2016, 9:33AM



Vous pouvez également afficher les services du tableau de bord par défaut dans la section Services disponibles.

Les procédures associées aux services sont décrites dans Ajouter un service à un hôte, Gérer l'accès à un service et Procédures de service supplémentaires.

Caractéristiques

La vue Services contient deux panneaux :

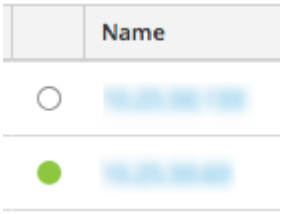
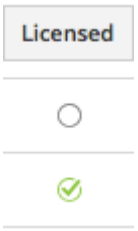
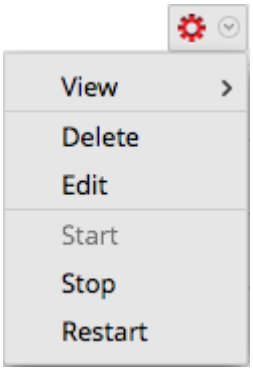
- Panneau Services
- Panneau Groupes

Panneau Services

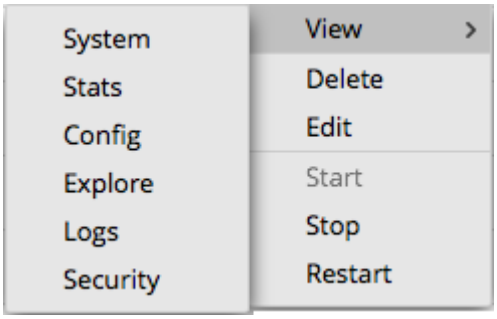
Dans le panneau Services, vous pouvez accéder aux différentes vues d'un service et effectuer des opérations de maintenance telles que l'ajout, la suppression, la modification et l'administration. Le panneau Services se compose d'une grille renseignée à l'aide de la liste des services Security Analytics définis et de la barre d'outils du panneau Services.

Ce tableau décrit les colonnes de la grille.

Last Modified: August 10 2016, 9:33AM

Colonne	Description
☐	Permet de sélectionner une ligne pour effectuer une action dans la barre d'outils. Cochez la case dans le titre de la colonne pour sélectionner ou désélectionner toutes les lignes de la grille.
<Vide>	Indique si le service est démarré (capture ou agrégation de données) ou arrêté. Un rond coloré en vert indique que le service connecté a démarré. Un rond blanc indique que le service connecté est arrêté. 
Nom	Le nom du service.
Sous licence	Indique si le service est sous licence. Un cercle coché désigne un service sous licence et un cercle vide désigne un service sans licence. 
Hôte	Nom de l'hôte sur lequel se trouve le service.
Type	Type de service Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector et Workbench.
Version	Version logicielle du service.
Actions	Fournit un menu Actions  pour le service sélectionné avec les actions pouvant être menées sur le service et l'hôte associé. Le menu Actions vous permet de supprimer, de modifier, de démarrer, d'arrêter et de redémarrer le service. Une boîte de dialogue vous demande de confirmer l'opération avant le redémarrage. 

Last Modified: August 10 2016, 9:33AM

Colonne	Description
	Le sous-menu Vue du menu Actions vous permet d'accéder aux vues Système, Statistiques, Config., Explorer, Logs et Sécurité du service sélectionné. 

Panneau Groupes

Le panneau Groupes permet de créer des groupes de services logiques. Une fois que les services sont regroupés, il est plus facile d'effectuer des opérations sur plusieurs services en interagissant avec chaque service d'un groupe plutôt qu'avec chaque service d'une liste dégroupée. Dans Security Analytics Live, les groupes peuvent s'abonner aux ressources contrairement aux services individuels qui ne peuvent pas effectuer l'opération.

Le panneau Groupes est composé d'une grille renseignée à l'aide de la liste des groupes de services définis et de la barre d'outils du panneau Groupes. Ce tableau décrit les colonnes de la grille.

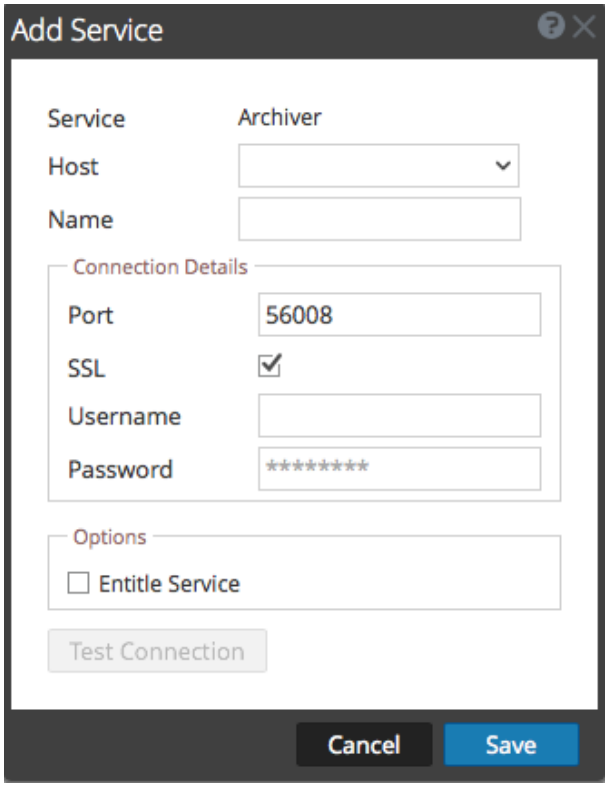
Colonne	Description
Nom	Nom du groupe de services. Cliquer sur le nom du groupe dans le panneau Groupes permet d'afficher les services de ce groupe dans le panneau Services.
<Vide>	Indique le nombre de services contenus dans le groupe. Cliquer sur le nombre de services disponibles dans le groupe au sein du panneau Groupes, permet d'afficher les services de ce groupe dans le panneau Services.

Boîte de dialogue Ajouter un service ou Modifier le service

Cette rubrique présente les boîtes de dialogue Ajouter un service ou Modifier le service accessibles dans la vue Services d'administration (Administration > Services).

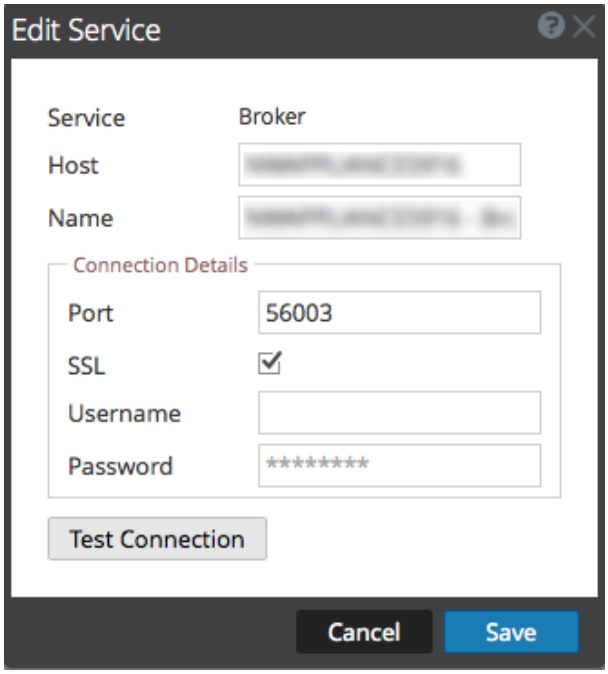
Les services Security Analytics sont automatiquement découverts dans RSA Security Analytics. Vous pouvez ajouter un service manuellement à l'aide de la boîte de dialogue Ajouter un service afin que les services soient disponibles pour les modules Security Analytics.

Pour accéder à la boîte de dialogue Ajouter un service, accédez à la vue **Services Administration**et sélectionnez **Ajouter** (+) dans la barre d'outils du **panneau Services**.



Vous pouvez utiliser la boîte de dialogue Modifier le service pour modifier les services. La boîte de dialogue Modifier le service est semblable à la boîte de dialogue Ajouter un service. Pour accéder à la boîte de dialogue Modifier le service, accédez à la vue **Services Administration**et sélectionnez **Modifier** ( ) dans la barre d'outils du **panneau Services**.

Last Modified: August 10 2016, 9:33AM



Les procédures associées aux services sont décrites dans Ajouter un service à un hôte, Gérer l'accès à un service et Procédures de service supplémentaires.

Caractéristiques

Ce tableau décrit les fonctions des boîtes de dialogue Ajouter un service ou Modifier le service.

Champ ou Option	Description
Service	Indique le type de service. Vous pouvez ajouter les services suivants : Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector et Workbench.
Hôte	Spécifie l'hôte sur lequel le service réside.
Nom	Spécifie le nom utilisé pour identifier le service ; par exemple, **HQ Broker** ou **Broker-10.10.201.99**. Utilisez une convention de dénomination facile à comprendre pour faciliter les tâches administratives. Certains administrateurs préfèrent utiliser le nom d'hôte ou l'adresse IP (spécifiée dans le champ **Hôte**) pour le **Nom** également.
Port	Spécifie le port utilisé pour communiquer avec ce service. Le port par défaut basé sur le type de service sélectionné dans le champ **Service** est automatiquement rempli ici. Si vous sélectionnez **SSL** ci-dessous, ce port devient un port SSL. Si vous ne sélectionnez pas **SSL**, il devient un port non SSL. Vous pouvez personnaliser ce port en ouvrant un pare-feu pour le port que vous ajoutez. Pour plus d'informations sur les ports, voir Architecture et ports du réseau.
SSL	Indique que Security Analytics utilise SSL pour les communications avec ce service.
Nom d'utilisateur	Spécifie le nom d'utilisateur utilisé pour la connexion à ce service. Le nom d'utilisateur par défaut est **admin**.

Last Modified: August 10 2016, 9:33AM

Champ ou Option	Description
Mot de passe	Spécifie le mot de passe utilisé pour la connexion à ce service. Le mot de passe par défaut est **netwitness**.
Autoriser le service	(Facultatif) Attribue des licences à partir du serveur de licence local (LLS) aux services sélectionnés. Pour plus d'informations, reportezvous à Afficher l'attribution de droits actuelle.
Tester la connexion	Le fait de cliquer sur ce bouton teste la connexion d'un service que vous ajoutez.
Enregistrer	Le fait de cliquer sur ce bouton enregistre le nouveau service.
Annuler	Le fait de cliquer sur ce bouton ferme la boîte de dialogue Ajouter un service ou Modifier le service. Si vous n'enregistrez pas le service avant de fermer la boîte de dialogue, le service n'est pas ajouté ni modifié.

Last Modified: August 10 2016, 9:33AM

Barre d'outils du panneau Groupes

Cette rubrique présente les fonctions et options de la vue Services d'administration > barre d'outils du panneau Groupes.

La barre d'outils du panneau Groupes contient les options de gestion des groupes de services. Cette barre d'outils comporte les options de création, de modification et de suppression des groupes. Lorsque les groupes sont créés, vous pouvez faire glisser des services individuels du panneau Services vers un groupe.

Les groupes peuvent refléter de manière utile une logique de fonctions, de géographie, de projets ou d'organisation. Un service peut appartenir à plusieurs groupes.

Pour accéder à la vue Services, cliquez sur le menu **Security Analytics** et sélectionnez **Administration > Services.** La barre d'outils du panneau Groupes se trouve en haut de la grille Groupes de la vue Services.

Caractéristiques

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

Option	Description
+	Affiche une nouvelle ligne dans la grille Groupe dans laquelle vous entrez le nom d'un nouveau groupe.
−	Vous invite à confirmer que vous souhaitez supprimer le groupe ou le service. Vous pouvez confirmer ou annuler la suppression.
	Ouvre le champ de nom d'une ligne dans la grille Groupe afin que vous puissiez saisir le nouveau nom d'un groupe existant.
	Actualise le groupe sélectionné.

Last Modified: August 10 2016, 9:33AM

Barre d'outils du panneau Services

Cette rubrique présente les options de la barre d'outils du panneau Service pour l'ajout, la suppression, la modification et l'attribution de licences pour les services. Vous pouvez également filtrer les services répertoriés dans le panneau Services.

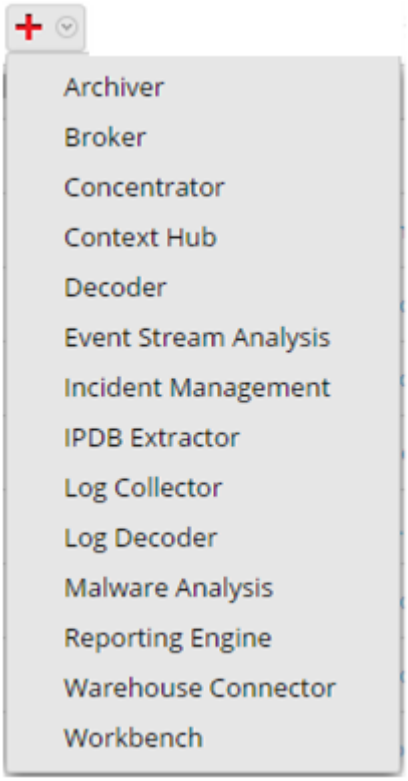
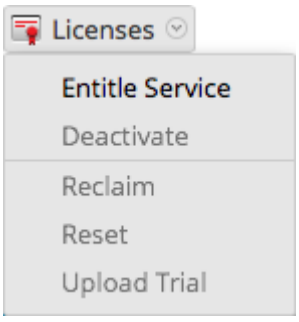
La barre d'outils du panneau Services comporte des options permettant d'ajouter, de supprimer, de modifier et de concéder sous licence des services. Vous pouvez filtrer les services répertoriés sur la base d'un ou de plusieurs types et noms de service ou hôtes.

Pour accéder à la vue Services d'administration, sélectionnez **Administration > Services dans le menu Security Analytics .** La barre d'outils du panneau Services se trouve en haut de la grille du même nom dans la vue Services.

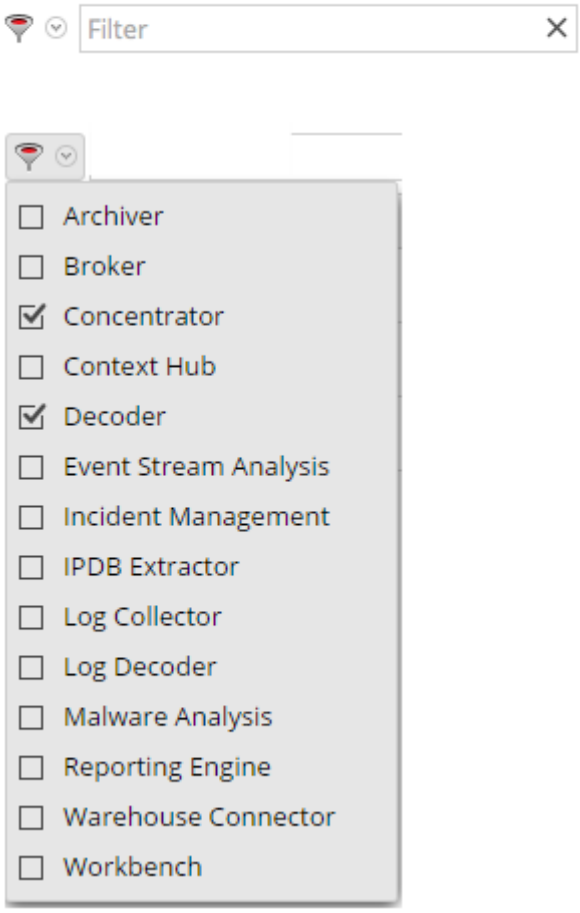
Caractéristiques

Ce tableau décrit les fonctions de la barre d'outils du panneau Services.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
	Ajoute un service pour cette instance de RSA Security Analytics à gérer (voir Ajouter un service à un hôte).
	Supprime un service de cette instance de Security Analytics (voir Modifier ou supprimer un service).
	Modifie l'identification du service et les paramètres de communication de base (voir Modifier ou supprimer un service).
	• Autoriser le service Attribue des licences du serveur LLS (Local License Server, serveur de licences local) aux services sélectionnés (voir Onglet Présentation). • Désactiver Non utilisé(e) dans Security Analytics 10.6 • Récupérer Récupère une licence désactivée auprès du serveur LLS pour le service sélectionné. • Réinitialiser Non utilisé(e) dans Security Analytics 10.6 • Télécharger la version d'évaluation Non utilisé(e) dans Security Analytics 10.6

Last Modified: August 10 2016, 9:33AM

Fonction	Description
	Filtre les services répertoriés dans la vue Services. Dans le menu déroulant Filtrer, vous pouvez filtrer les services en fonction d'un ou de plusieurs des types de services sélectionnés. Dans cet exemple, lorsque vous sélectionnez Concentrator et Decoder, seuls ces services apparaissent dans la vue Services. Dans le champ Filtre, vous pouvez filtrer les services par nom et hôte. Vous pouvez utiliser simultanément le menu déroulant Filtrer et le champ Filtre pour filtrer les services répertoriés dans la vue Services.

Vue Configuration des Services

Cette rubrique présente les fonctions et caractéristiques de la vue Configuration des services.

La vue Configuration des Services est l'une des vues disponibles dans le menu Vue Services> Actions (). Elle constitue une interface utilisateur pour configurer tous les aspects d'un service Core ou d'un service Security Analytics.

Les options de configuration de la vue Configuration des Services sont organisées sous forme d'onglets, chaque onglet contenant une série de paramètres connexes. À la différence de la vue Explorer les services, qui permet d'accéder directement à tous les fichiers de configuration d'un service, ces onglets présentent, dans une vue conviviale, les paramètres de configuration de service les plus couramment modifiés.

En raison des besoins de configuration des différents services, chaque type de service a des variantes sous les onglets disponibles et dans les paramètres de configuration de cette vue. Différentes rubriques présentent les paramètres de configuration spécifiques d'un hôte (Brokers et Concentrators, Decoders et Log Decoders) ou d'un service (par exemple Reporting Engine, IPDB Extractor, Log Collector et Warehouse Connector).

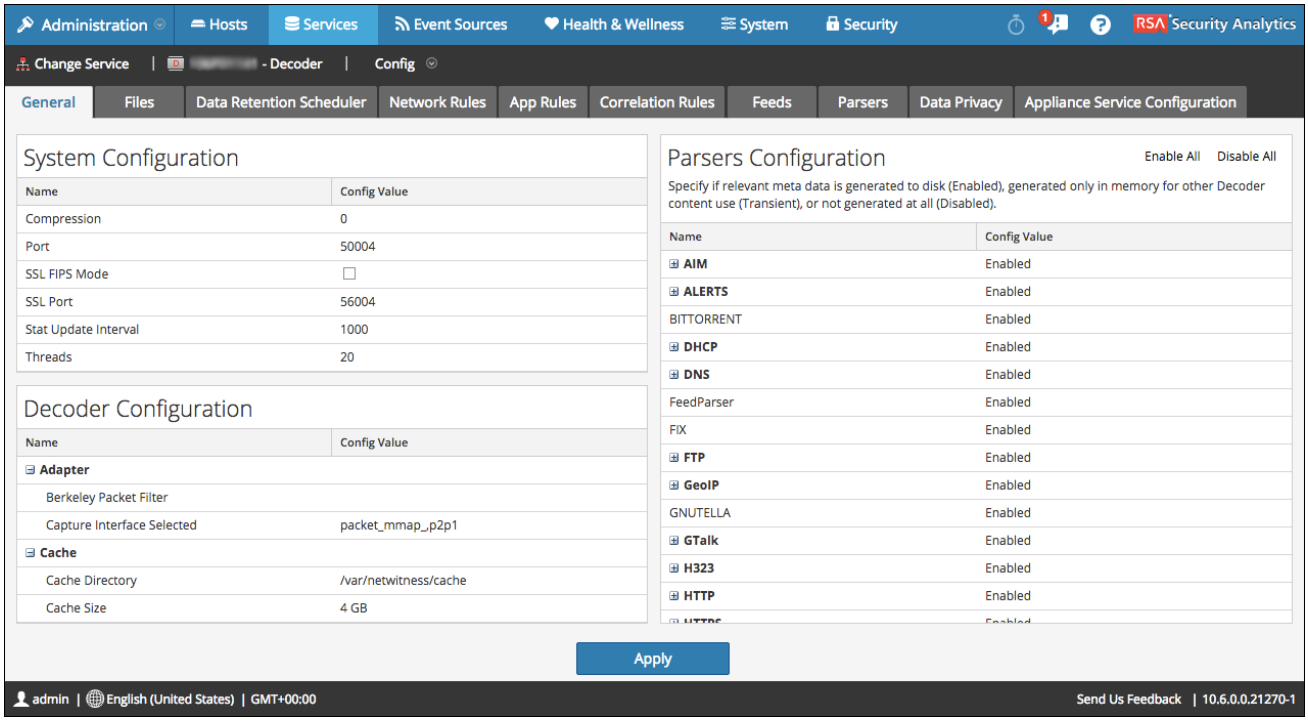
Pour accéder à la vue Configuration des Services :

1. Dans le menu **Security Analytics** , sélectionnez **Administration > Services**.
   La vue Services d'administration s'affiche.

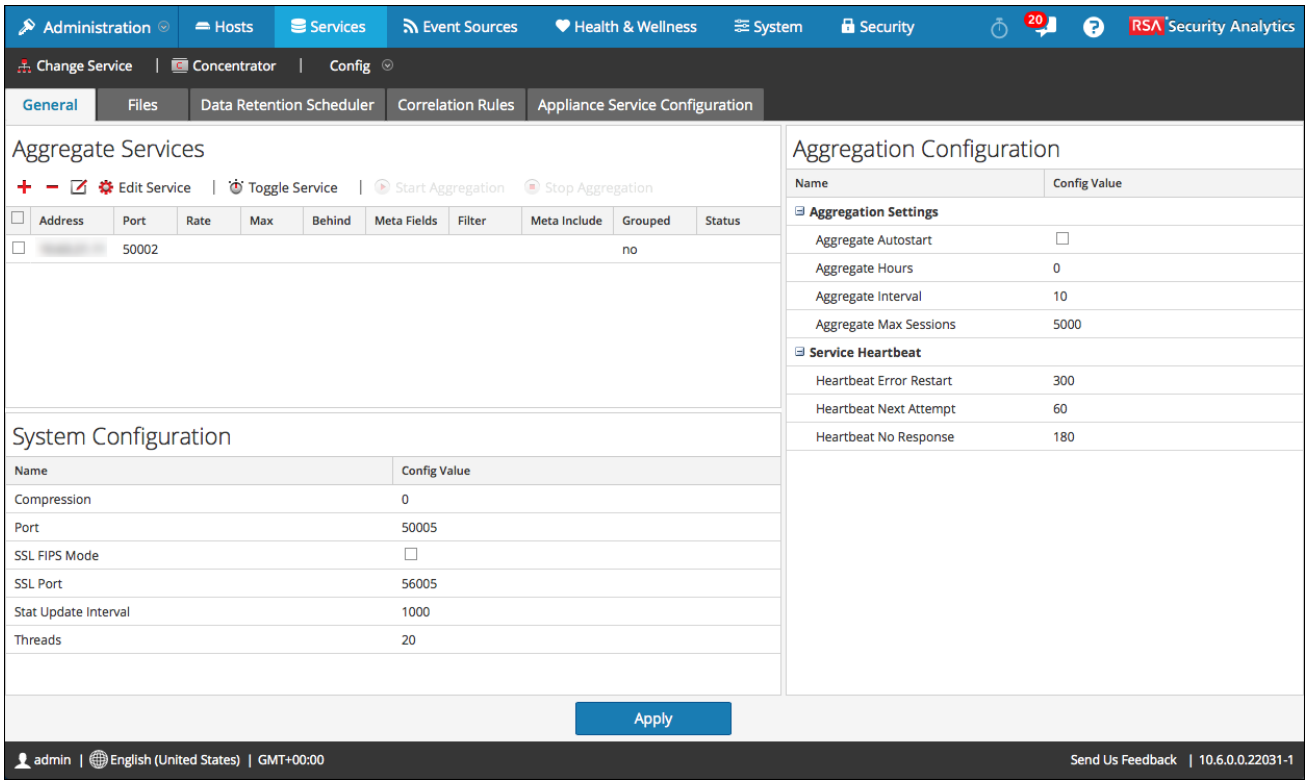
2. Sélectionnez un service et cliquez sur  **> Vue > Config**.
   La vue Configuration des Services s'affiche pour le service sélectionné.

Exemple de vue Configuration des Services pour un Decoder.

Last Modified: August 10 2016, 9:33AM



Exemple de vue Configuration des Services pour un Concentrator.



Vue Configuration des services - onglet Configuration du service Appliance

Présentation

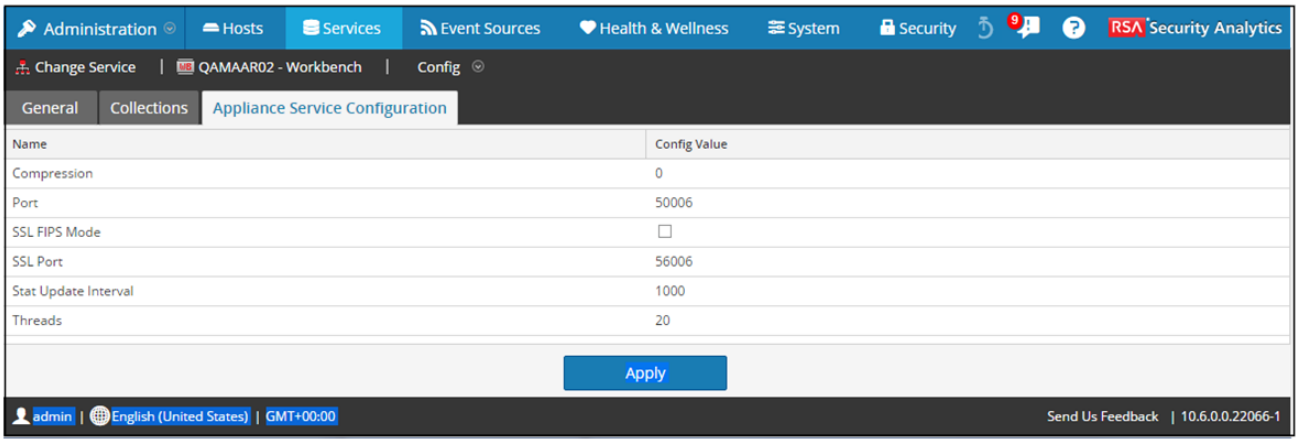
Cette rubrique fournit une description de la vue Configuration des services > onglet Configuration du service Appliance du service Workbench Security Analytics.

Contexte

L'onglet Configuration du service Appliance du service Workbench permet de visualiser, ajouter et supprimer des services. Lorsque vous avez apporté des modifications aux services configurés, si vous cliquez sur Appliquer, la configuration prend effet immédiatement.

Pour accéder à cette vue :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service et sélectionnez **> Vue > Configuration**.
   La vue Configuration des services s'ouvre sur l'onglet Configuration du service Appliance.
3. Sélectionnez l'onglet **Configuration du service Appliance**.



Last Modified: August 10 2016, 9:33AM

Caractéristiques

L'onglet Configuration du service Appliance comporte une grille qui répertorie des informations pertinentes concernant les configurations de Workbench.

Grille

Le tableau suivant décrit les fonctionnalités de la grille.

Paramètre	Description
Compression	Lorsque sa valeur est positive, elle indique le nombre minimum d'octets avant la compression d'un message. 0 indique aucune compression pour aucun message. La modification prend effet aux connexions suivantes.
Port	Port chiffré sur lequel écoutera ce service. 0 indique désactivé. Les modifications prendront effet au redémarrage du service.
Mode FIPS SSL	Détermine si la bibliothèque OpenSSL entrera en mode FIPS. Les modifications prendront effet au redémarrage du service.
Port SSL	Port SSL sur lequel écoutera ce service. 0 indique désactivé. Les modifications prendront effet au redémarrage du service.
Intervalle de mise à jour des statistiques	Détermine la fréquence (en millisecondes) à laquelle les nœuds statistiques sont mis à jour dans le système. La modification prend effet immédiatement.
Threads	Détermine le nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. La modification prend effet immédiatement.
Valeur de configuration	Détermine la valeur de configuration du service. La modification prend effet immédiatement.
Appliquer	Met à jour les configurations modifiées dans la grille.

Last Modified: August 10 2016, 9:33AM

Onglet Planificateur de rétention des données

Cette rubrique décrit les options configurables sous l'onglet Planificateur de rétention des données pour Decoder, Log Decoder et Concentrator.

Sous l'onglet Planificateur de rétention des données, vous pouvez définir les critères de suppression des enregistrements de base de données du stockage primaire dans les services Decoder, Log Decoder et Concentrator, et planifier la vérification du seuil.

Pour plus d'informations sur l'onglet Rétention de données pour Archiver, reportezvous à Onglet Rétention de données Archiver.

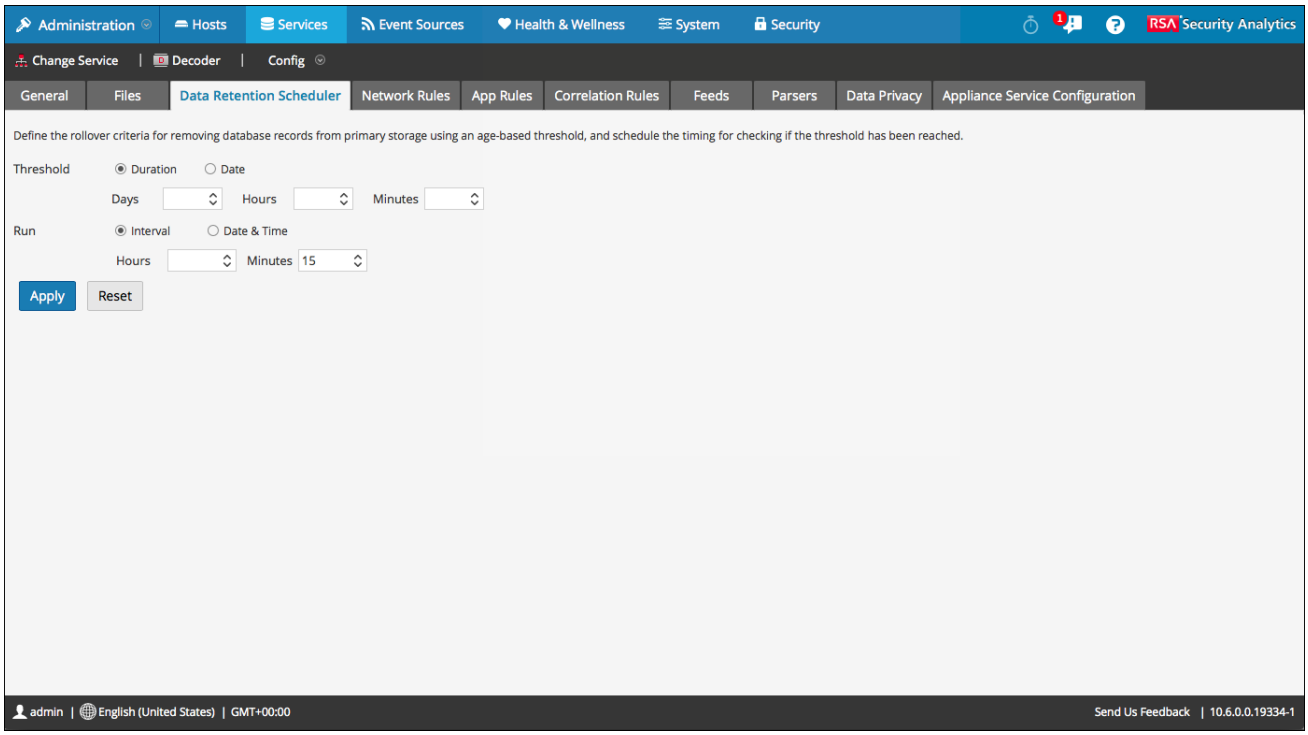
Note: Si une personnalisation supplémentaire est nécessaire, elle peut être effectuée avec le planificateur sous l'onglet Fichiers dans la vue Configuration des services. Par exemple, si un stockage supplémentaire est disponible pour l'enregistrement des données RAW par rapport aux métadonnées, il peut paraître plus logique d'utiliser la Capacité en tant que seuil et de définir des seuils différents par base de données (métadonnées ou paquet).

Pour accéder à l'onglet Planificateur de rétention des données :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez Decoder, Log Decoder ou Concentrator, puis sélectionnez  **> Vue > Config**.
3. Dans la vue **Configuration des services** pour le service, cliquez sur l'onglet **Planificateur de rétention des données**.

La figure suivante illustre les paramètres sous l'onglet Planificateur de rétention des données pour Decoder.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

L'onglet Planificateur de rétention des données possède des sections permettant de spécifier les paramètres Seuil et Exécution. Le tableau suivant répertorie les paramètres pris en charge pour la configuration de rétention des données.

Paramètre	Description
Seuil	Le seuil est basé sur l'ancienneté des données, la durée pendant laquelle les données ont été stockées ou la date à laquelle les données ont été stockées. La date est issue du fichier de base de données, et non de la durée de session réelle. • **Durée** : Durée de stockage des données avant leur suppression. Spécifie le nombre de jours (365 au maximum), d'heures (24 au maximum) et de minutes (60 au maximum) écoulés depuis l'horodatage des données. • **Date** : Suppression des données basées sur la date de l'horodatage. Spécifie la date et l'heure mensuelles dans les champs **Calendrier** et **Heure**.
Exécuter	Planning pour l'exécution de la tâche qui vérifie les critères de déploiement. • **Intervalle** : Planifier la vérification de base de données pour qu'elle se produise à intervalles réguliers. Spécifie les **Heures** et **Minutes** entre les vérifications planifiées. • **Date et heure** : Planifier la vérification de base de données pour qu'elle se produise à une date et une heure régulières. Spécifie la journée à partir de la liste déroulante et l'heure du système au format `hh:mm:ss`. Les valeurs possibles pour la journée sont **Tous les jours**, **Jours de la semaine**, **Week-ends** et **Personnalisé**, où **Personnalisé** vous permet de sélectionner un ou plusieurs jours spécifiques de la semaine.
Appliquer	Écrase tout planning précédent pour ce service et applique les nouveaux paramètres immédiatement.

Last Modified: August 10 2016, 9:33AM

Paramètre	Description
	⚠ **Caution:** Une fois ces paramètres appliqués et le seuil respecté, les anciennes données seront supprimées de la base de données et ne seront plus accessibles.
Réinitialiser	Réinitialise le planning au dernier état appliqué.

Onglet Fichiers

Cette rubrique décrit les fichiers de configuration des services qui s'affichent dans la vue Configuration des services > onglet Fichiers.

L'onglet Fichiers de la vue Configuration des services est l'interface utilisateur permettant de modifier des fichiers de configuration de service (Decoders, Log Decoders, Brokers, Archivers et Concentrators) sous forme de fichiers texte.

Les fichiers qu'il est possible de modifier dépendent du type de service en cours de configuration. Les fichiers communs à tous les services Core sont :

- le fichier d'index du service ;
- le fichier Netwitness ;
- le fichier du rapporteur d'incidents ;
- le fichier du planificateur.
- Fichier de définitions de feed.

De plus, le Decoder dispose de fichiers qui permettent de configurer les parsers et les définitions de feed. Il dispose également d'un adaptateur de réseau local sans fil.

Note: Les valeurs par défaut de ces fichiers de configuration sont généralement adaptées aux situations les plus courantes. Toutefois, il est nécessaire de les modifier en partie pour les services facultatifs, comme le rapporteur d'incidents ou le planificateur. Seuls les administrateurs disposant d'une bonne compréhension des réseaux et des facteurs qui affectent la façon dont les services collectent et analysent les données devraient apporter des modifications à ces fichiers sous l'onglet Fichiers.

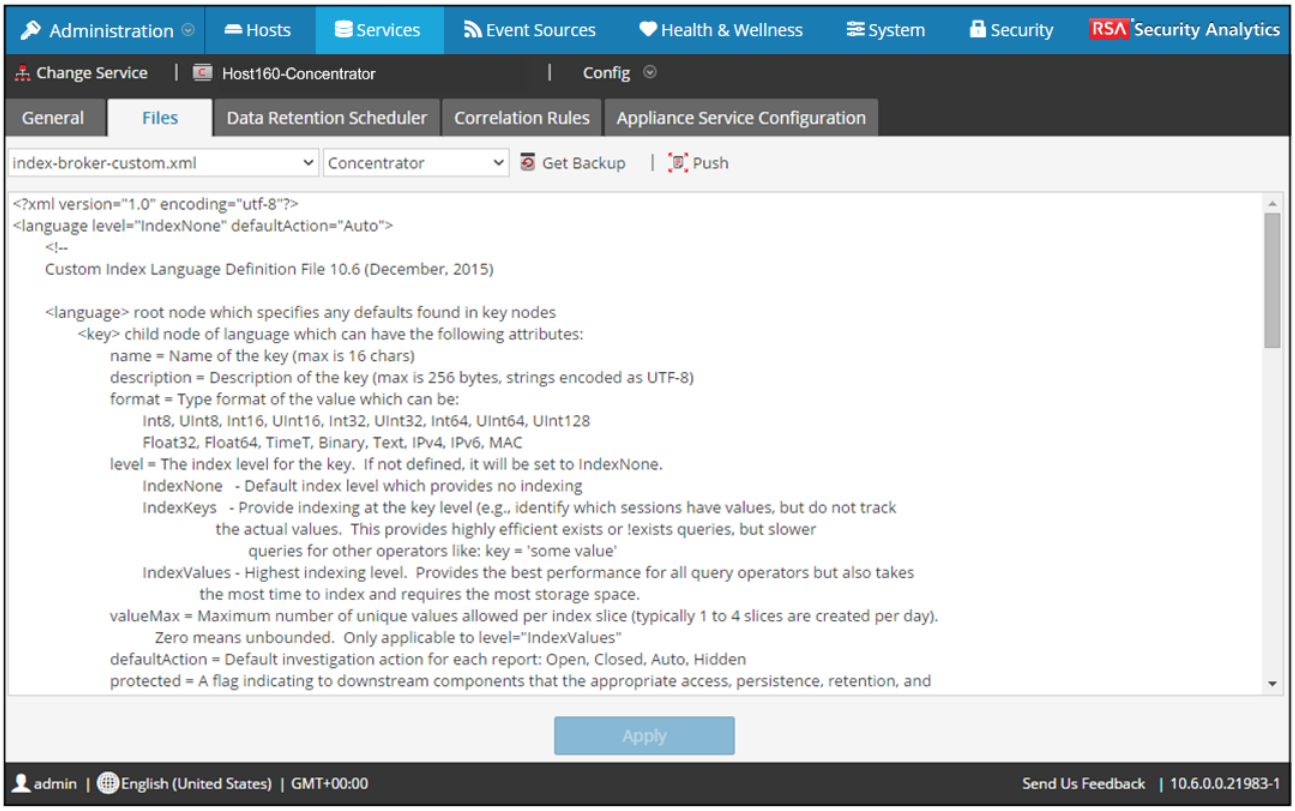
Vous trouverez plus de détails sur les paramètres de configuration de service dans les paramètres de configuration des services.

Pour accéder à l'onglet Fichiers :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service et sélectionnez  **> Vue > Configuration**.
   La vue Configuration des services s'ouvre sur l'onglet **Général**.
3. Cliquez sur l'onglet **Fichiers**.

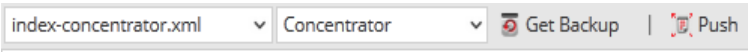
Voici un exemple de l'onglet Fichiers.

Last Modified: August 10 2016, 9:33AM



Barre d'outils onglet Fichiers

L'onglet Fichiers possède une barre d'outils et une fenêtre de modification. Voici un exemple de la barre d'outils.



Il s'agit des fonctionnalités de la barre d'outils de l'onglet Fichiers.

Fonction	Description
Liste déroulante **Fichier**	Affiche la liste des fichiers que le système utilise actuellement. Lorsque vous sélectionnez un fichier, le texte du fichier s'affiche dans la fenêtre de modification de texte. Dans la fenêtre de texte, vous pouvez modifier le fichier et enregistrer les modifications, ou créer d'autres fichiers à utiliser.
Liste déroulante **Service/Hôte**	Affiche le type de service et l'hôte. Vous pouvez ouvrir un fichier à partir du service ou de l'hôte pour modification.
Get Backup	Récupère la dernière sauvegarde du fichier en cours, ce qui peut s'avérer utile lorsque vous avez effectué des modifications et souhaitez rétablir la version précédente du fichier. La sauvegarde ne remplace pas le fichier en cours, sauf si vous cliquez sur **Enregistrer**.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
	Affiche une boîte de dialogue dans laquelle vous pouvez sélectionner des services du même type et transférer le fichier actuellement affiché vers les services.
Appliquer	Écrase le fichier en cours et crée un fichier de sauvegarde.

Vue Explorer les services

Cette rubrique présente les fonctions de la vue Explorer les services de Security Analytics, une interface utilisateur puissante et flexible permettant d'afficher et de modifier des configurations d'hôte et de service.

La vue Explorer les services offre un accès et un contrôle avancés pour tous les hôtes et services Security Analytics. Tous les services exposent leur fonctionnalité via une série de nœuds en arborescence, semblable à la vue Windows Explorer de votre système de fichiers. Ici, vous pouvez :

- Afficher une arborescence de répertoires présentant des fichiers communs pour tous les services sélectionnés.
- Accéder à un fichier dans le répertoire.
- Ouvrir le même fichier pour chaque service et afficher le contenu côte à côte.
- Sélectionner une entrée dans le fichier et modifier sa valeur.
- Appliquer une valeur de propriété à partir d'un service aux autres services.

  La vue Explorer les services peut également afficher une boîte de dialogue Propriétés, une interface simple pour afficher les propriétés de tout nœud dans le système et envoyer les messages au nœud, affiché dans la figure ci-dessous.

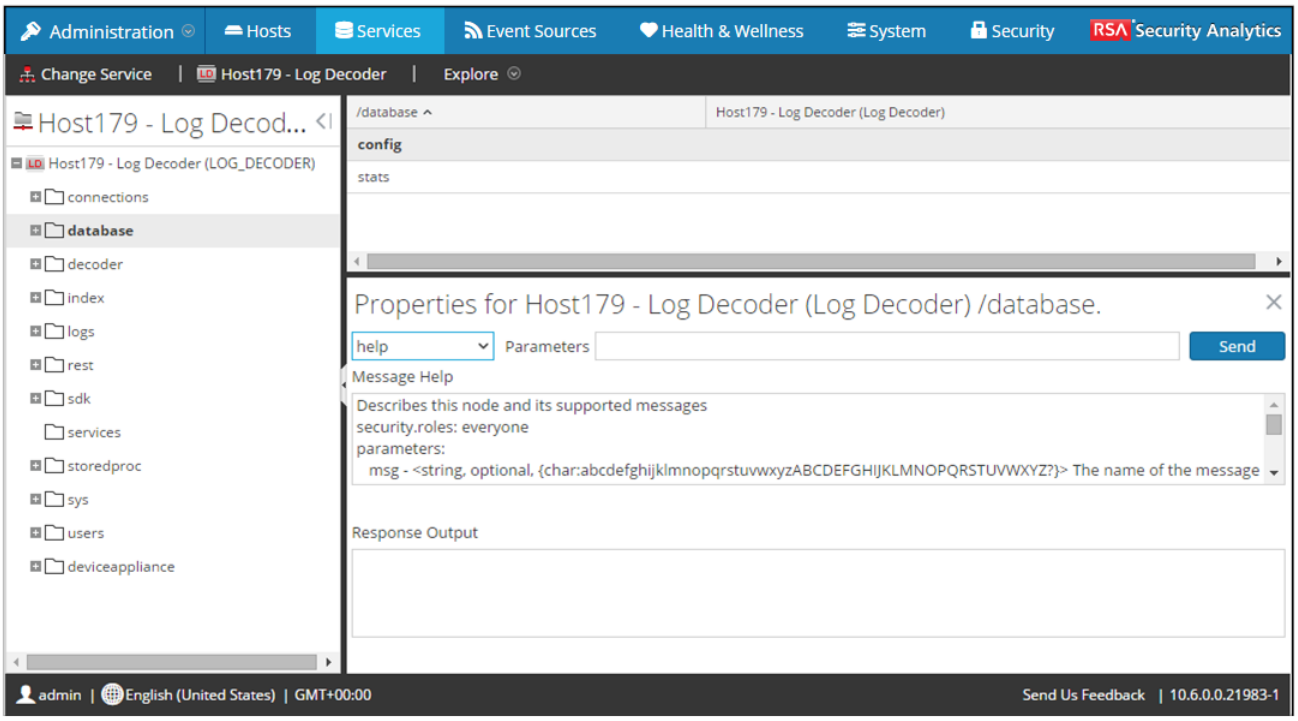
Caution: Une bonne compréhension des nœuds et paramètres est requise lors de l'apport de modifications dans cette vue. Des paramètres incorrects peuvent causer des problèmes de performances.

Pour accéder à la vue Explorer les services :

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

Voici un exemple de la vue Explorer les services.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

La **vue Explorer les services** possède deux panneaux principaux :

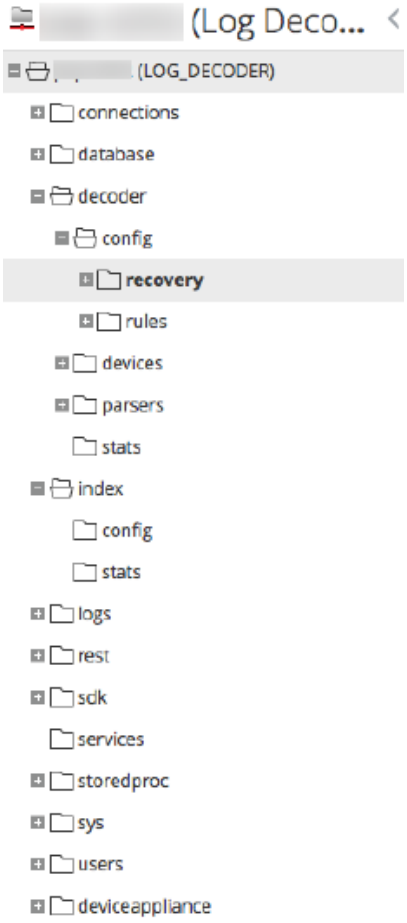
- Liste de nœuds
- Panneau Surveillance

Vous pouvez accéder aux Propriétés d'un fichier en cliquant avec le bouton droit sur le fichier et en sélectionnant Propriétés.

La liste de nœuds

La liste de nœuds affiche les services en tant que série de nœuds et de dossiers sous forme d'arborescence. Les niveaux de la liste de nœuds se développent et se réduisent pour afficher la hiérarchie complète.

Last Modified: August 10 2016, 9:33AM



Le nom de chaque dossier racine s'appuie sur la fonctionnalité qu'il expose. Par exemple, le dossier **/connections** affiche toutes les adresses IP connectées. Sous chaque **IP/Port** se trouvent deux dossiers, **sessions** et **stats**.

- Le dossier **sessions** affiche toutes les sessions d'utilisateur authentifiées provenant de l'IP/Port.
- Le dossier **stats** affiche des valeurs, telles que le nombre de messages envoyés/reçus, les octets envoyés/reçus, etc., définies par le service. Elles ne sont pas modifiables.

Le fait de sélectionner un dossier dans l'arborescence affiche ses enfants dans le panneau **Surveillance**. Chaque nœud présent dans l'arborescence est surveillé activement. Ainsi, lorsque la valeur d'une statistique ou d'un nœud de configuration change, elle est immédiatement reflétée dans l'arborescence et le panneau Surveillance.

Panneau Surveillance

Le panneau **Surveillance** affiche des propriétés et valeurs pour un nœud sélectionné (tel qu'**index**) et un dossier enfant (tel que **config**). Il existe deux moyens de modifier des valeurs :

- Cliquer sur la valeur et en saisir une nouvelle
- Envoyer un message **set** dans la boîte de dialogue Propriétés

/Index/Config	(Concentrator)
index.dir	/var/netwitness/concentrator/index=7.08 GB
index.dir.cold	
index.dir.warm	
page.compression	huffhybrid
save.session.count	0

Boîte de dialogue Propriétés

Cette rubrique explique comment envoyer des messages à un nœud système dans la vue Explorer les services > boîte de dialogue Propriétés.

La boîte de dialogue Propriétés apparaît en dessous du panneau Surveiller lorsque vous sélectionnez Propriétés dans le menu contextuel. La boîte de dialogue Propriétés fournit un outil de messagerie facile à utiliser pour communiquer avec les nœuds du système. Ceci peut être utile pour obtenir et définir des valeurs pour une propriété de plusieurs services.

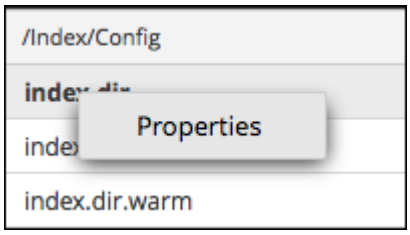
Tous les nœuds prennent en charge le message d'aide, qui contient :

- Une description du nœud.
- La liste des messages pris en charge avec une description correspondante.
- Les rôles de sécurité nécessaires pour accéder aux messages.

Les messages disponibles varient selon le dossier racine et du service. La plupart de ces messages sont également accessibles en tant qu'options avec un tableau de bord ou une vue Security Analytics.

Pour accéder à la boîte de dialogue Propriétés :

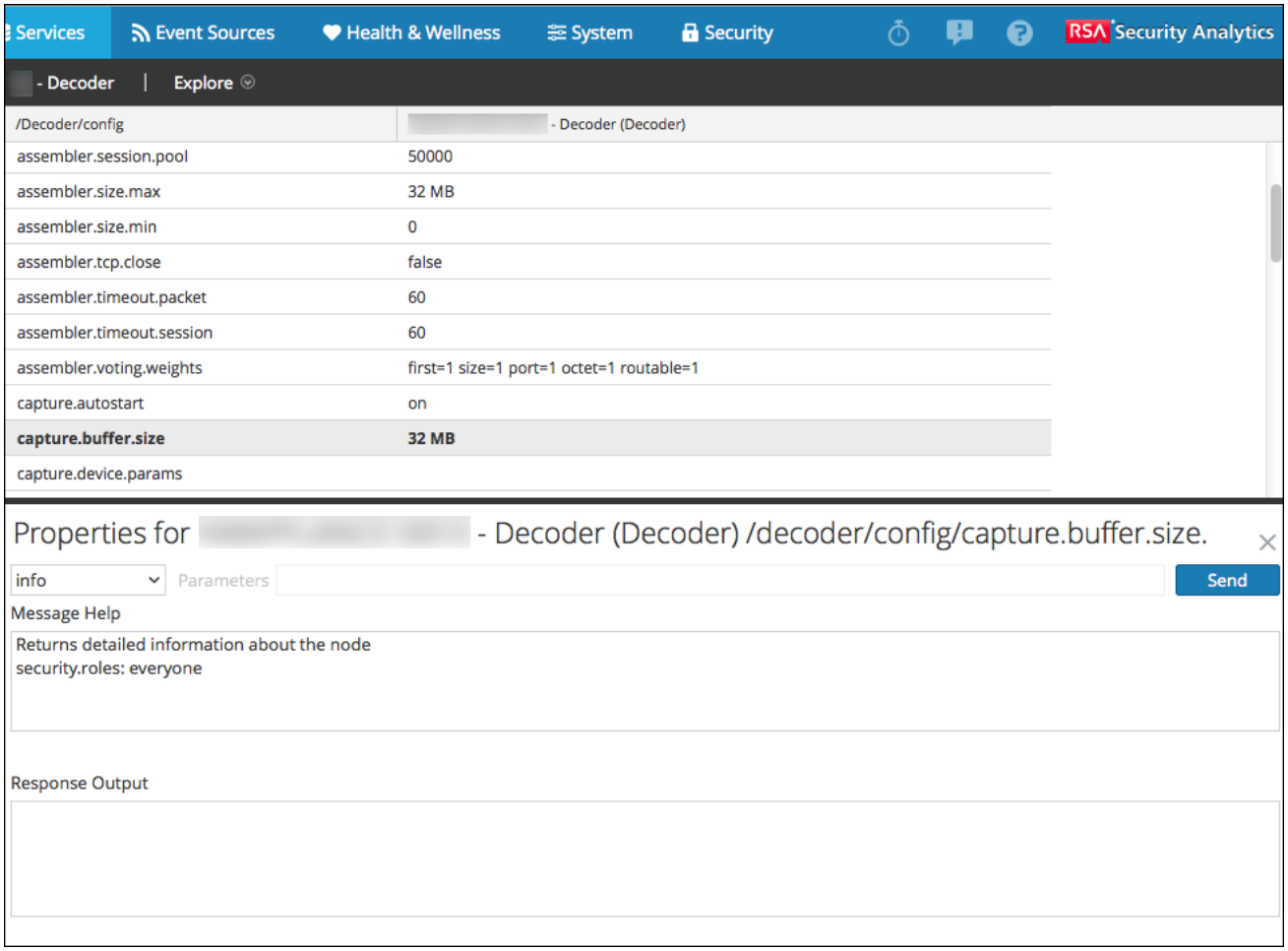
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service, puis **> Vue > Explorer**.
3. Dans la liste **Nœud**, sélectionnez un fichier.
4. Dans le panneau **Surveiller**, cliquez avec le bouton droit de la souris sur une propriété et sélectionnez **Propriétés**.



La boîte de dialogue Propriétés s'affiche. Vous pouvez également cliquer avec le bouton droit de la souris sur un fichier dans la liste des nœuds pour afficher la boîte de dialogue Propriétés.

L'exemple suivant affiche la boîte de dialogue Propriétés avec l'affichage de l'aide d'un message (**info**).

Last Modified: August 10 2016, 9:33AM



Caractéristiques

La boîte de dialogue Propriétés possède les fonctions suivantes.

Fonction	Description
Liste déroulante **Message**	Répertorie tous les messages disponibles du nœud en cours. Sélectionnez un message à envoyer au nœud.
Champ de saisie **Paramètres**	Tapez les paramètres du message dans ce champ.
Bouton **Envoyer**	Envoie le message au nœud.
Aide relative aux messages	Affiche l'aide du message en cours.
Sortie de réponse	Affiche la réponse à un message ou la sortie d'un message.

Last Modified: August 10 2016, 9:33AM

Vue Logs de services

Cette rubrique présente la vue Logs de services.

la vue Logs de services permet d'afficher et de rechercher les logs d'un service spécifique. La vue Logs de services est identique au panneau de consignation système, à deux exceptions près :

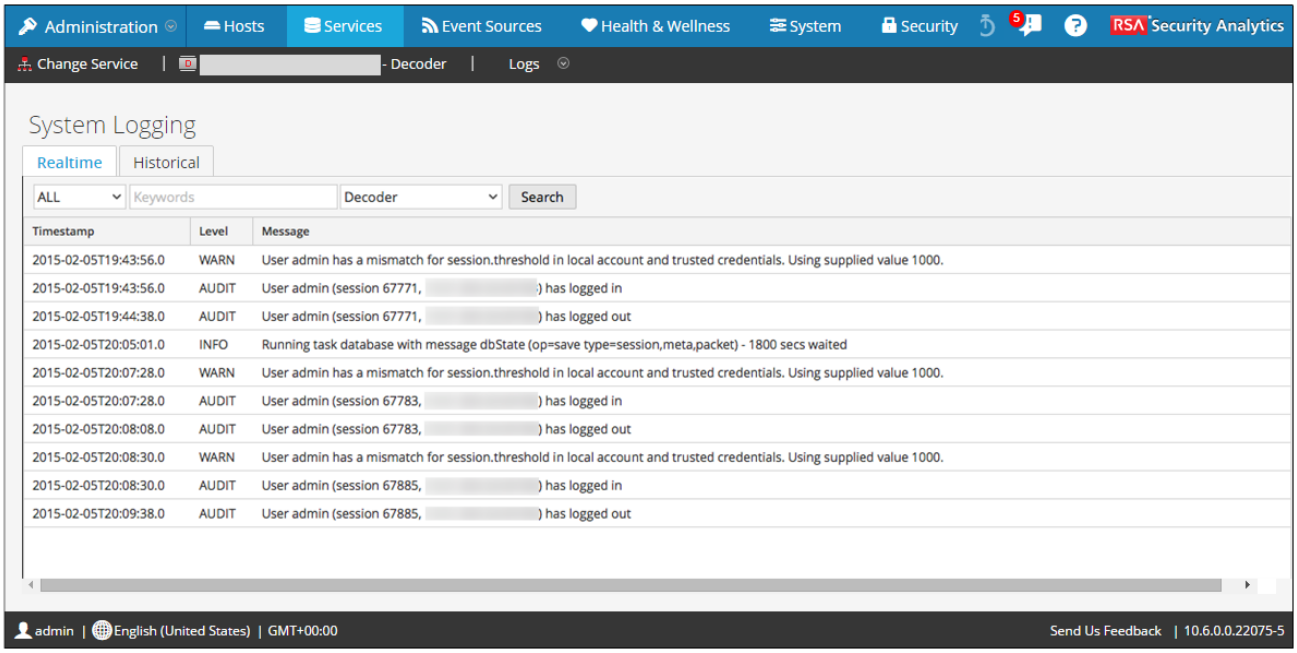
- Les logs de services disposent d'un filtre supplémentaire pour sélectionner les messages pour le service ou l'hôte.
- Le panneau de consignation système contient un onglet supplémentaire pour les paramètres.

Pour consulter la description complète des fonctionnalités de consignation Security Analytics, reportez-vous à Panneau de consignation système.

Pour afficher un log de service :

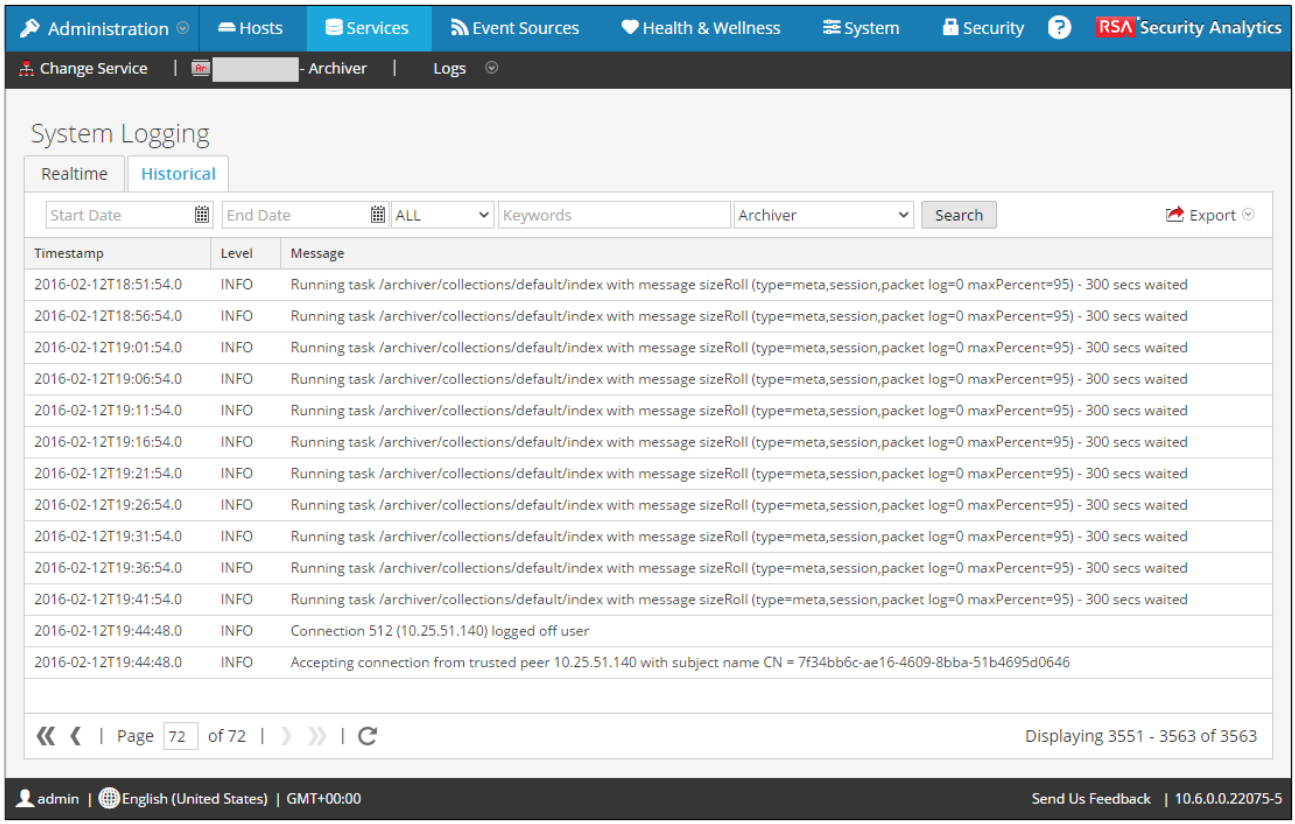
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service et cliquez sur  **> Vue > Logs**.

La figure suivante illustre l'onglet En temps réel de la vue Logs de services.



La figure suivante illustre l'onglet Historique de la vue Logs de services.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

Le panneau de consignation système contient les onglets suivants, et les fonctions de consignation sont décrites comme faisant partie de la maintenance du système (voir Contrôler l'intégrité dans Security Analytics).

Fonction	Description
Onglet En temps réel	C'est le mode surveillance du log de service.
Onglet Historique	C'est une vue du log de service dans laquelle une recherche peut être effectuée.

Last Modified: August 10 2016, 9:33AM

Vue Sécurité des services

Cette rubrique présente le service de gestion de la sécurité dans la vue Sécurité des services.

Dans Security Analytics, chaque service dispose de sa propre configuration d'utilisateurs, de rôles et d'autorisations de rôle, que vous pouvez gérer dans la vue Sécurité des services.

Pour accéder aux informations d'un service et effectuer des opérations de service via Security Analytics, un utilisateur doit appartenir à un rôle doté d'autorisations sur le service en question. Pour les services Security Analytics Core 10.4 ou version ultérieure qui utilisent des connexions de confiance, il n'est plus nécessaire de créer des comptes utilisateurs Security Analytics Core pour les utilisateurs qui se connectent via le client Web. Vous n'avez besoin de créer de comptes utilisateurs Security Analytics Core que pour l'agrégation, les utilisateurs de clients Thick et les utilisateurs de l'API REST.

Note: Dans Security Analytics, seul l'utilisateur administrateur par défaut est automatiquement créé dans tous les services. Pour pouvoir gérer la sécurité des services, le compte de l'utilisateur administrateur par défaut doit apparaître dans la vue Security Analytics Administration > Services. Pour tous les autres utilisateurs, vous devez configurer l'accès à chacun des services via Security Analytics.

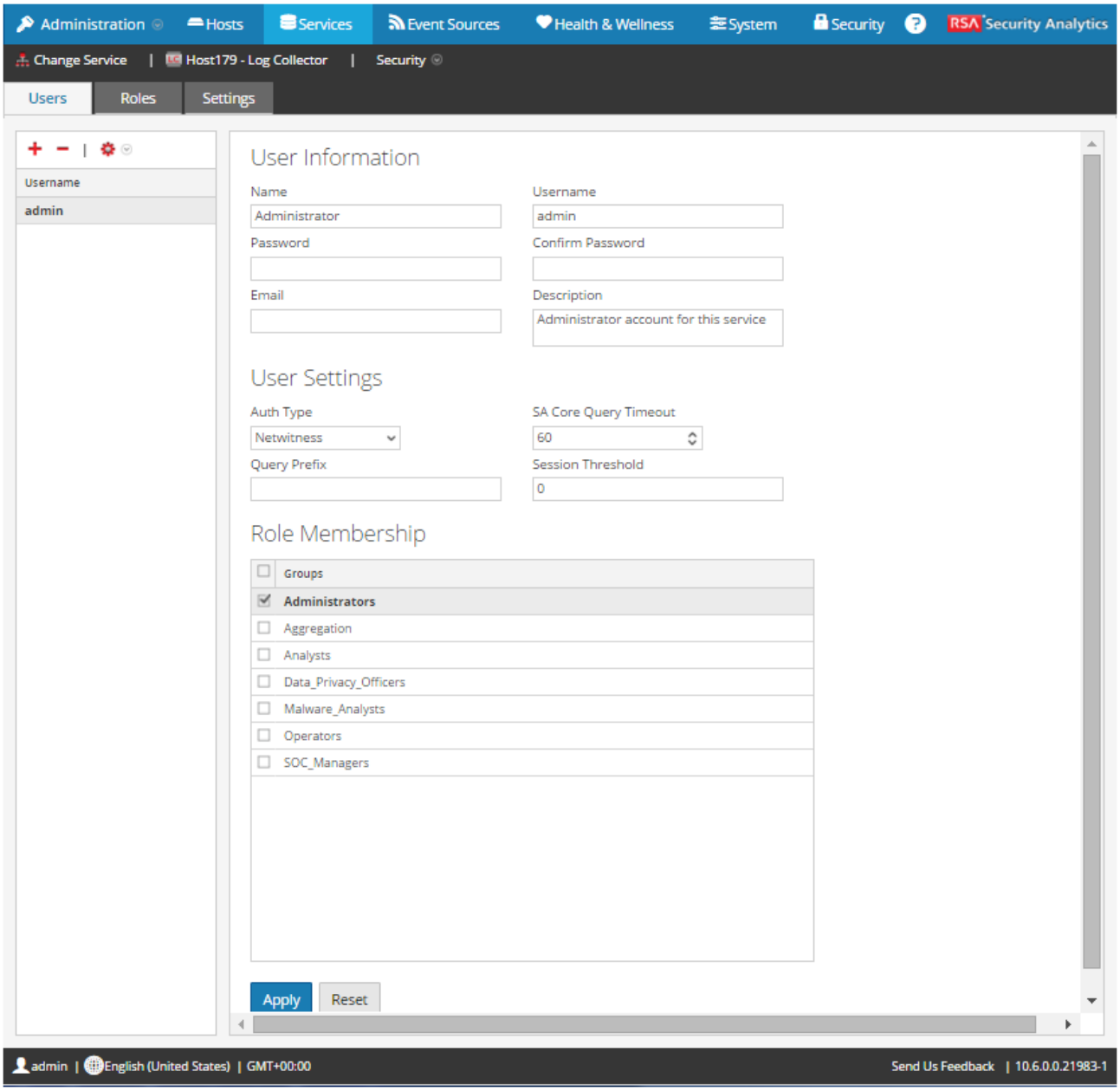
Les procédures liées à cet onglet sont décrites dans la section Procédures supplémentaires relatives aux services.

Pour accéder à la vue Sécurité des services :

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

Last Modified: August 10 2016, 9:33AM

2. Sélectionnez un service, puis > Vue > Sécurité.
   La vue Sécurité des services du service sélectionné s'affiche.



Caractéristiques

La vue Sécurité des services comporte trois onglets : UtilisateursUsersTab, RôlesRolesTab et Paramètres.

Accès aux rôles et au service

Pour configurer la sécurité des services, il est important de définir des rôles et de leur associer des utilisateurs. La vue Sécurité des services distingue ces deux fonctions dans deux onglets : Utilisateurs et Rôles.

- Sous l'onglet Rôles, vous pouvez créer des rôles et leur attribuer des autorisations pour un service donné.
- Sous l'onglet Utilisateurs, vous pouvez ajouter un utilisateur, modifier les paramètres d'un utilisateur, modifier le mot de passe d'un utilisateur et l'appartenance d'un utilisateur à un rôle pour un service donné. Même si vous sélectionnez un seul service dans la vue Sécurité des services, vous pouvez appliquer aux autres services les paramètres du service sélectionné.

Last Modified: August 10 2016, 9:33AM

Onglet Rôles

Cette rubrique présente les fonctions de la vue Sécurité des services > onglet Rôles.

L'onglet **Rôles** vous permet de créer des rôles et de leur attribuer des autorisations. Chaque rôle peut être associé à des autorisations différentes pour les différents services. Par exemple, le rôle Analystes peut être associé à des autorisations différentes en fonction du service sélectionné.

Avant d'ajouter des utilisateurs à des rôles, vous devez définir les rôles d'utilisateur, généralement par fonction, et attribuer des autorisations à ces rôles.

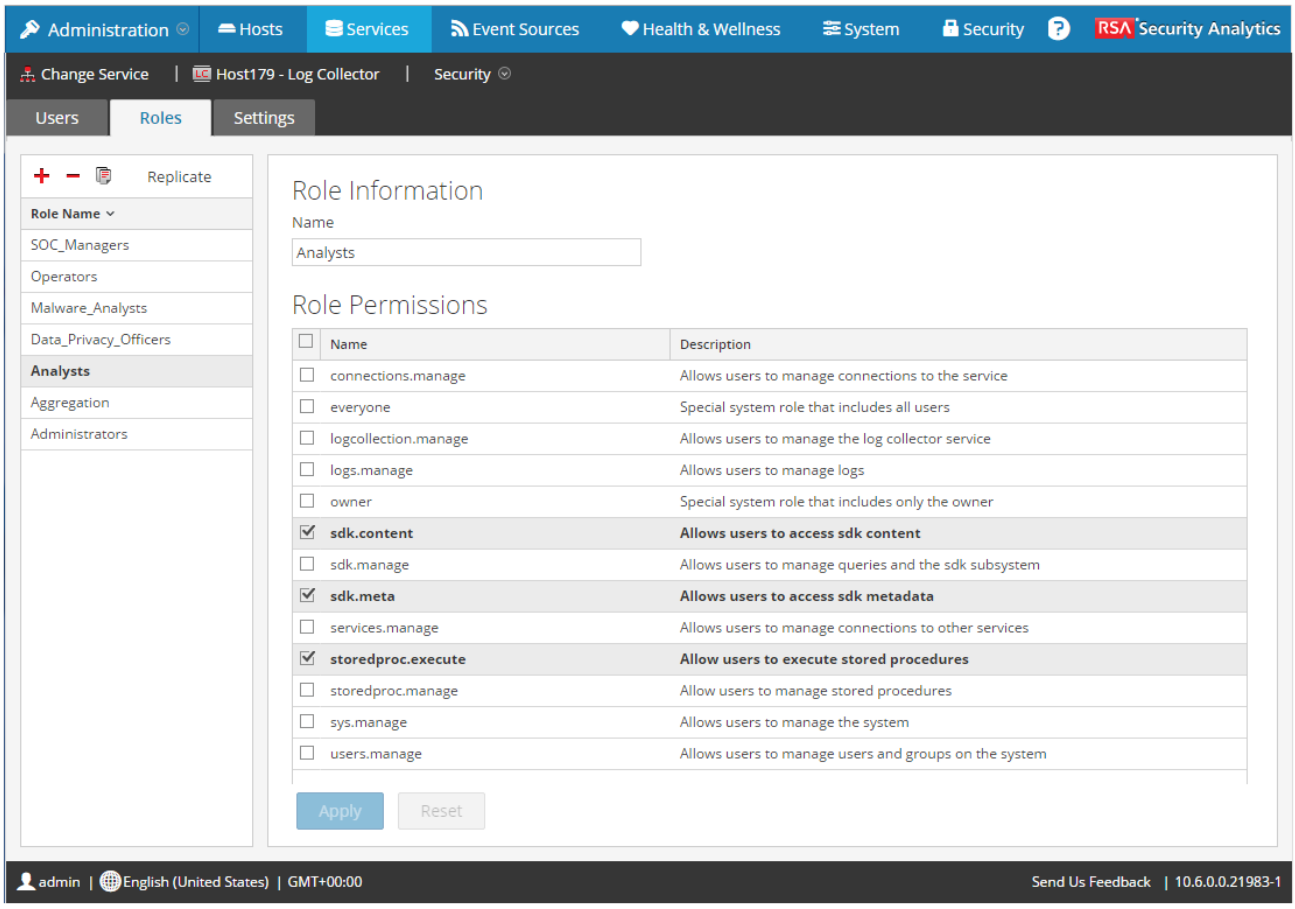
Les procédures liées à cet onglet sont décrites dans la section Procédures supplémentaires relatives aux services.

Pour afficher l'onglet Rôles de la vue **Sécurité des services** :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez le service auquel vous voulez ajouter un utilisateur, puis sélectionnez  **> > Vue > Sécurité**.
3. Sélectionnez l'onglet **Rôles**.

La figure suivante illustre l'onglet Rôles de la vue Sécurité des services.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

Le panneau **Nom du rôle** apparaît sur la gauche de l'onglet Rôles. Sélectionnez un nom de rôle pour faire apparaître sur la droite un panneau d'informations correspondant au rôle sélectionné.

Panneau Nom du rôle

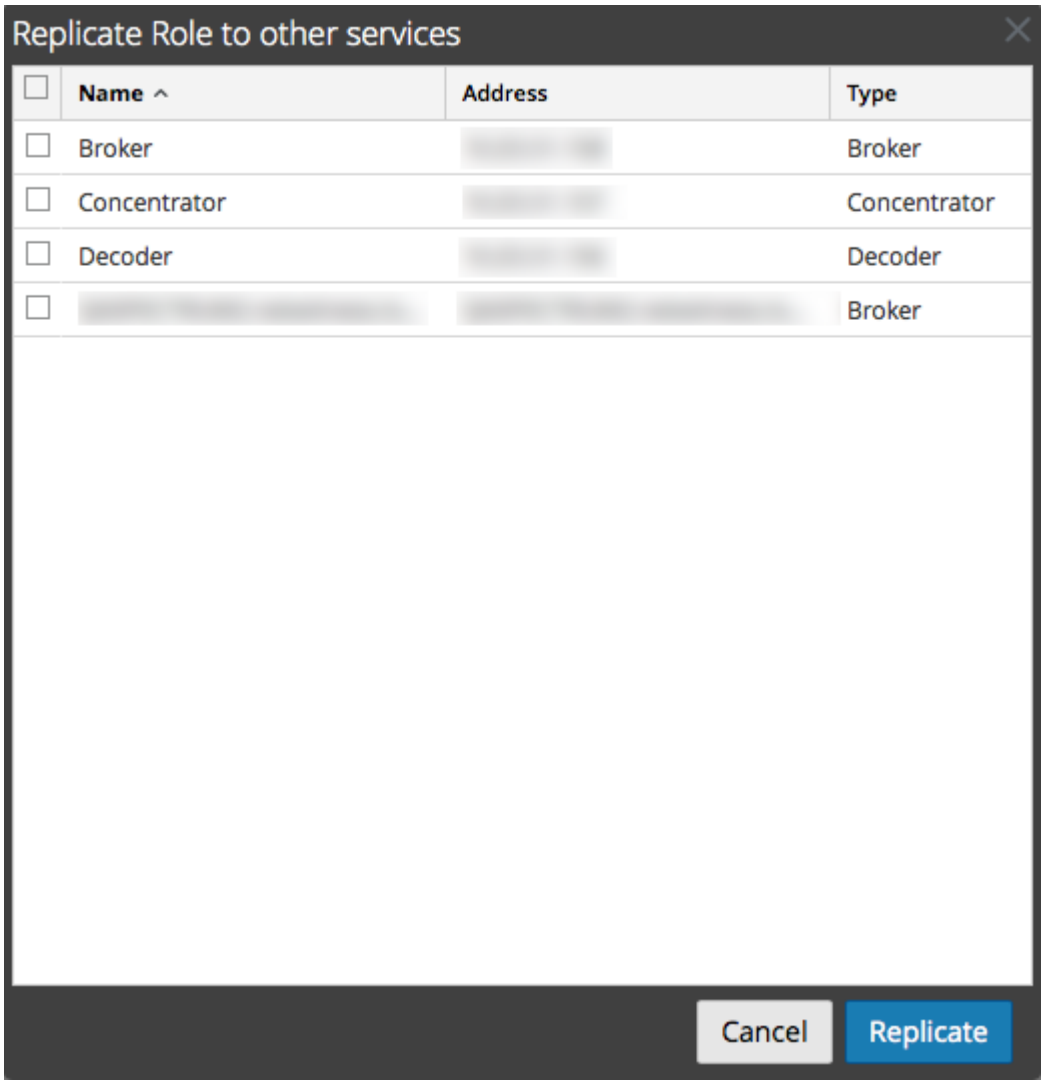
Ce panneau est doté des fonctionnalités suivantes.

Fonction	Description
+	Ajoute un nouveau groupe au service en cours.
−	Supprime le groupe sélectionné du service en cours.
	Copie un rôle et les autorisations qui lui sont associées dans un nouveau rôle. Le nom de ce nouveau rôle doit être unique. Par exemple, vous pouvez copier le rôle **Analystes** et en créer un autre intitulé **Responsables_analystes**.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
Replicate	Transmet un rôle et les autorisations qui lui sont associées à d'autres services. Sélectionnez un rôle, puis cliquez sur **Répliquer** pour afficher la boîte de dialogue **Répliquer le rôle sur les autres services**. Dans cette boîte de dialogue, vous pouvez sélectionner les services sur lesquels vous souhaitez répliquer le rôle.

La figure suivante illustre la boîte de dialogue **Répliquer le rôle sur les autres services**.



Panneau d'informations sur le rôle

Le panneau d'informations sur le rôle permet de définir les autorisations associées à un rôle.

Il y a deux boutons :

- Le bouton **Appliquer** permet d'enregistrer les modifications apportées dans le panneau Autorisations et de les appliquer immédiatement.

- Si vous n'avez pas enregistré les modifications dans ce panneau, cliquez sur le bouton **Réinitialiser** pour rétablir la valeur de tous les champs et paramètres avant modification.

Last Modified: August 10 2016, 9:33AM

Rôles et autorisations de l'utilisateur de service

Cette rubrique décrit les autorisations et rôles préconfigurés des utilisateurs de services.

L'onglet Rôles de la vue Sécurité des services vous permet de créer des rôles d'utilisateur de service et d'attribuer des autorisations. Vous pouvez également utiliser les rôles préconfigurés inclus avec Security Analytics pour attribuer des autorisations utilisateur.

Rôles utilisateur de maintenance

Security Analytics possède les rôles utilisateur de service préconfigurés suivants.

Rôle	Autorisations attribuées	Personnel/Compte
Administrateurs	Toutes les autorisations	Administrateur système Security Analytics
Agrégation	aggregate sdk.content sdk.meta sdk.packets	Vous pouvez utiliser ce rôle pour créer un compte Agrégation. Ce rôle fournit les autorisations minimales nécessaires pour effectuer l'agrégation des données. Il n'est disponible que sur les services Security Analytics 10.5 et versions ultérieures.
Analysts, Malware_Analysts et SOC_Managers	sdk.meta sdk.content sdk.packets storedproc.execute	Les utilisateurs peuvent utiliser des applications spécifiques, exécuter des requêtes et afficher du contenu à des fins d'analyse.
Spécialistes de la confidentialité des données	sys.manage users.manage sdk.meta sdk.content sdk.packets sdk.manage logs.manage database.manage index.manage dpo.manage	Agent de protection des données Les agents de protection des données possèdent l'autorisation dpo.manage sur Decoders et Log Decoders.

Last Modified: August 10 2016, 9:33AM

Rôle	Autorisations attribuées	Personnel/Compte
Opérateurs	sys.manage services.manage connections.manage users.manage logs.manage parsers.manage rules.manage database.manage index.manage sdk.manage decoder.manage archiver.manage concentrator.manage storedproc.manage	Les opérateurs sont responsables du fonctionnement quotidien des services.

Autorisations d'utilisateur de maintenance

Vous pouvez attribuer de nombreuses permissions à un rôle de service dans Security Analytics. Les utilisateurs peuvent avoir différentes autorisations sur chaque service, selon leurs attributions de rôle et les autorisations sélectionnées pour chaque rôle. Ce tableau décrit les autorisations que vous pouvez attribuer à un rôle.

Autorisation	Définition
sys.manage	Permet à l'utilisateur de modifier les paramètres de configuration du service.
services.manage	Permet à l'utilisateur de gérer les connexions à d'autres services.
connections.manage	Permet à l'utilisateur de gérer les connexions au service.
users.manage	Permet à l'utilisateur de créer des utilisateurs et rôles d'utilisateurs individuels et de spécifier les autorisations d'utilisateur.
aggregate	Permet à l'utilisateur d'effectuer l'agrégation des données.
sdk.meta	Permet à l'utilisateur d'exécuter des requêtes dans les applications Procédure d'enquête et Reporting et d'afficher les métadonnées renvoyées par la requête.
sdk.content	Permet à l'utilisateur d'accéder à des paquets et logs bruts de toute application client (Procédures d'enquête et Reporting).
sdk.packets	Permet aux utilisateurs d'accéder à des paquets et logs bruts de toute application client.

Last Modified: August 10 2016, 9:33AM

Autorisation	Définition
appliance.manage	Permet à l'utilisateur de gérer les tâches de l'appliance (hôte). Cette autorisation est requise par le service Appliance.
decoder.manage	Permet à l'utilisateur de modifier les paramètres de configuration pour le service Decoder.
concentrator.manage	Permet à l'utilisateur de modifier les paramètres de configuration pour le service Concentrator/Broker.
logs.manage	Permet à l'utilisateur d'afficher les logs de service et de modifier les paramètres de configuration de consignation pour le service spécifié.
parsers.manage	Permet à l'utilisateur de gérer tous les attributs sous les nœuds des analyseurs.
rules.manage	Permet à l'utilisateur d'ajouter et de supprimer toutes les règles.
database.manage	Permet à l'utilisateur de définir des emplacements de base de données, des tailles et les différents paramètres de configuration pour la session, les métabases de données et/ou paquet/log.
index.manage	Permet à l'utilisateur de gérer tous les attributs liés à l'index.
sdk.manage	Permet à l'utilisateur d'afficher et de définir tous les éléments de configuration SDK.
storedproc.execute	Permet à l'utilisateur d'exécuter une procédure stockée Lua.
storedproc.manage	Permet à l'utilisateur de gérer des procédures stockées Lua.
archiver.manage	Permet à l'utilisateur de modifier la configuration Archiver.
dpo.manage	Permet à l'utilisateur de gérer les configurations de transformation et les clés applicables.

Last Modified: August 10 2016, 9:33AM

Rôle d'agrégation

Cette rubrique décrit le rôle et les autorisations Agrégation qui permettent aux utilisateurs des services de réaliser des agrégations.

Le rôle d'agrégation est un rôle d'utilisateur de service destiné uniquement à l'agrégation des données. Il est doté des autorisations de rôle minimales pour réaliser une agrégation de données :

- aggregate
- sdk.meta
- sdk.packets
- sdk.content

Le rôle d'agrégation n'est disponible que sur les services Security Analytics 10.5 et version ultérieure, et il est utilisable pour un compte d'agrégation. Les membres de ce rôle ou les utilisateurs de services dotés de ces autorisations peuvent réaliser des agrégations sur les Decoders, Concentrators, Archivers et Brokers. L'autorisation **aggregate** permet aux utilisateurs de services de réaliser une agrégation des sessions et des métadonnées, ainsi que des paquets et logs bruts.

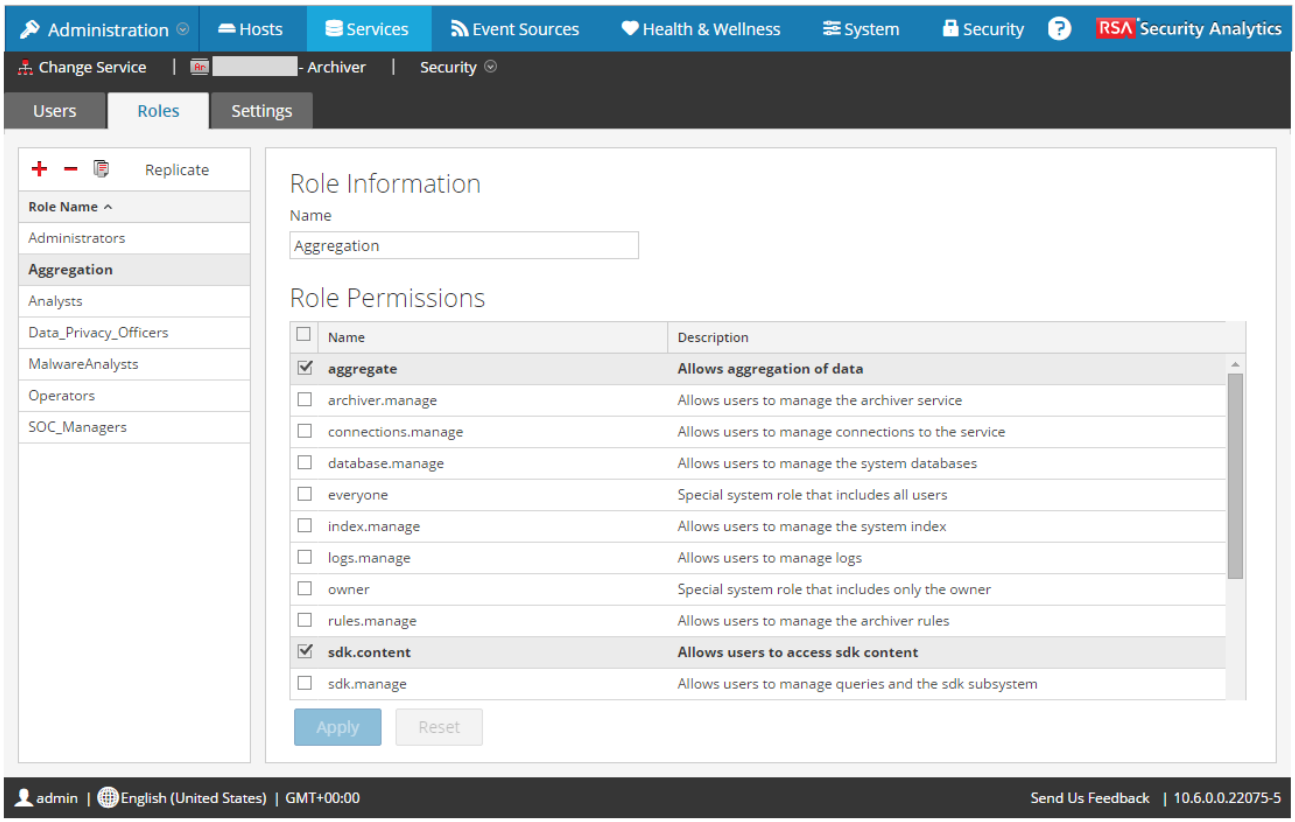
Vous pouvez toujours utiliser les autorisations decoder.manage, concentrator.manage et archiver.manage, mais les autorisations du rôle d'agrégation ne permettent de réaliser que des agrégations et empêchent d'effectuer les autres opérations disponibles.

Pour accéder aux rôles des utilisateurs de services, cliquez sur Administration > Services (sélectionnez un service) > Actions > Vue > Sécurité > onglet Rôles.

Les procédures liées aux rôles sont décrites dans la section Procédures supplémentaires relatives aux services. La rubrique Rôles et autorisations de l'utilisateur de service contient des informations détaillées relatives aux rôles préconfigurés.

La figure ci-dessous illustre les autorisations du rôle d'agrégation.

Last Modified: August 10 2016, 9:33AM

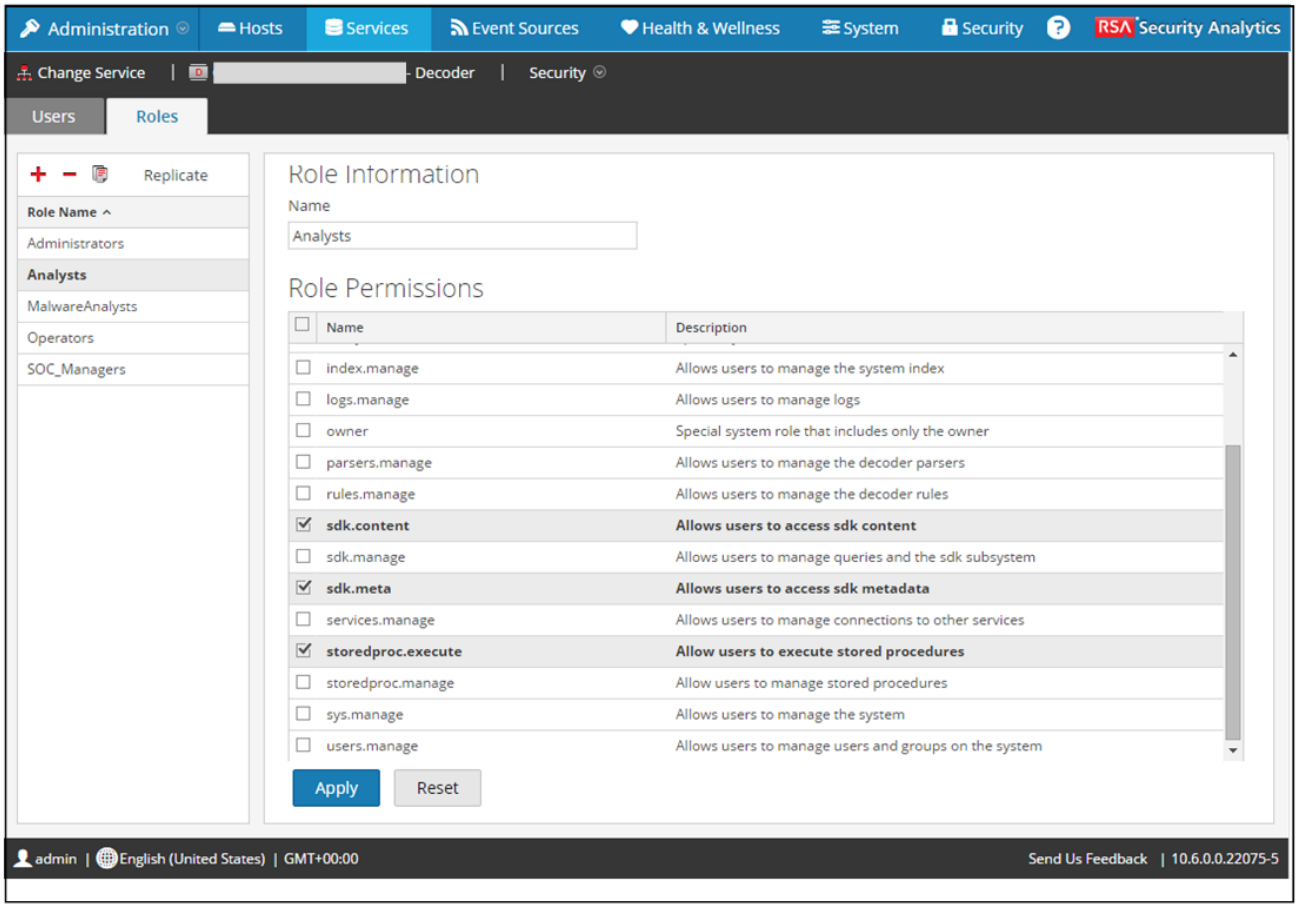


Le script Guide génère automatiquement la liste des rubriques enfants. Il est formaté sous la forme d'un commentaire jusqu'à son utilisation. Lorsque vous écrivez une rubrique contenant des sous-rubriques, modifiez le style en « dekiscript ». Laissez une ligne vide au-dessus de ce script.

Onglet Paramètres

Cette rubrique décrit les fonctions de la vue Sécurité des services > onglet Paramètres.

Sous l'onglet Paramètres de la vue Sécurité des services, les administrateurs peuvent activer et configurer les rôles de système qui définissent des permissions sur une base de clé par métadonnées pour les Broker, Concentrator, Decoder et Log Decoder individuels. La configuration de cette fonction ajoute des clés méta configurables dans la vue Sécurité des services > onglet Rôles pour que les clés méta individuelles puissent être appliquées à des rôles spécifiques sur un service spécifique. La figure suivante illustre le résultat des rôles de clé méta activés pour un Decoder.

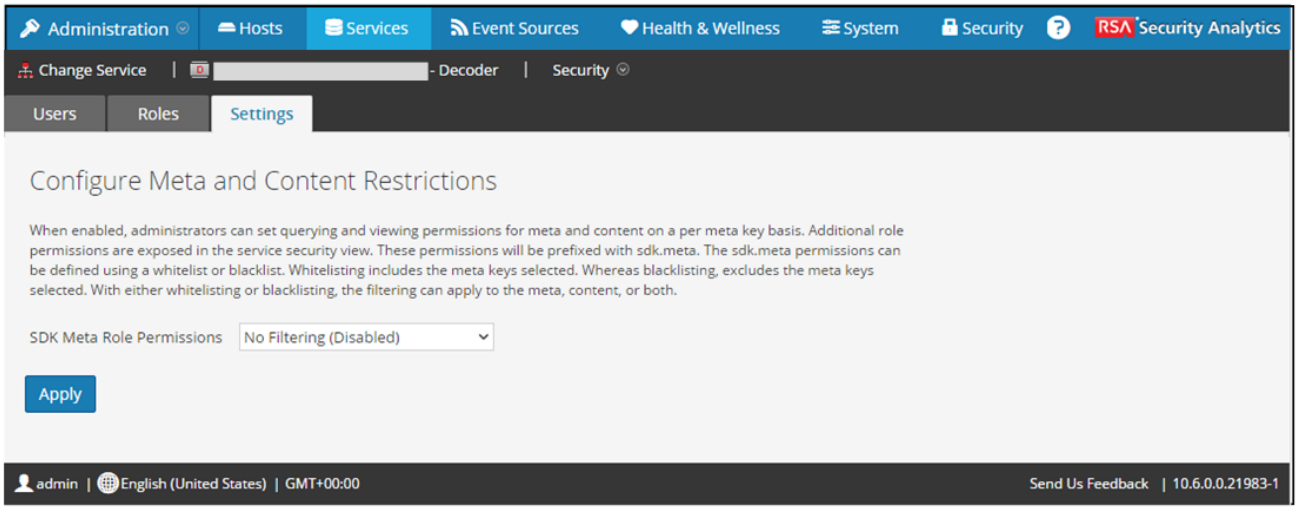


Cette configuration fait généralement partie d'un plan de confidentialité des données implémenté visant à s'assurer que des types de contenu spécifiques consommés ou agrégés par un service sont maintenus en sécurité, en limitant la visibilité des métadonnées et le contenu pour les utilisateurs privilégiés (voir Gestion de la confidentialité des données).

Last Modified: August 10 2016, 9:33AM

Pour afficher l'onglet :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la grille **Services**, sélectionnez un service Decoder ou Log Decoder et **> Vue > Sécurité** et cliquez sur l'onglet **Paramètres**.



Caractéristiques

L'onglet comprend deux fonctions.

Fonction	Description
Champ Autorisations de rôle méta SDK	Fournit l'option pour désactiver ou configurer les restrictions de clé méta et de contenu. Les options de filtrage sont décrites.
Bouton Appliquer	Applique immédiatement la configuration sélectionnée. Si elles ne sont pas désactivées, les clés méta sont ajoutées à l'onglet Rôle pour pouvoir être appliquées à des rôles spécifiques.

Options de permissions de rôle de métadonnées SDK

Le tableau suivant répertorie les options de filtrage disponibles dans la liste de sélection Permissions de rôle de métadonnées SDK, et les valeurs numériques utilisées pour la désactivation (0) et les types de filtrage (1 sur 6).

Note: Il n'est pas nécessaire de connaître la valeur numérique à moins de configurer la visibilité manuelle du contenu et méta dans le nœud system.roles.

Valeur du nœud system.roles	Option de l'onglet Paramètres	Description

0	Aucun filtrage (Désactivé)	Les rôles système qui définissent les autorisations sur la base d'une clé méta sont désactivés.
1	Liste blanche méta et contenu	Les métadonnées et le contenu pour les rôles de métadonnées SDK spécifiés sont sur liste blanche, ou visibles pour les utilisateurs auxquels le rôle système est attribué.
2	Liste blanche méta uniquement	Les métadonnées pour les rôles de métadonnées SDK spécifiés sont sur liste blanche, ou visibles pour les utilisateurs auxquels le rôle système est attribué.
3	Liste blanche contenu uniquement	Le contenu des rôles de métadonnées SDK spécifiés est sur liste blanche, ou visible pour les utilisateurs auxquels le rôle système est attribué.
4	Liste noire méta et contenu	Les métadonnées et le contenu pour les rôles de métadonnées SDK spécifiés sont sur liste noire, ou ne sont pas visibles pour les utilisateurs auxquels le rôle système est attribué.
5	Liste noire méta uniquement	Les métadonnées pour les rôles de métadonnées SDK spécifiés sont sur liste noire, ou ne sont pas visibles pour les utilisateurs auxquels le rôle système est attribué.
6	Liste noire contenu uniquement	Le contenu pour les rôles de métadonnées SDK spécifiés est sur liste noire, ou n'est pas visible pour les utilisateurs auxquels le rôle système est attribué.

Onglet Utilisateurs

Cette rubrique explique les fonctions de la vue Sécurité des services > onglet Utilisateurs.

Dans la vue Sécurité des services, l'onglet Utilisateurs vous permet de configurer les éléments suivants pour un service :

- Ajouter des comptes utilisateur.
- Modifier les mots de passe d'un utilisateur de service.
- Configurer les propriétés d'authentification utilisateur et les propriétés de gestion des requêtes pour le service.
- Spécifier l'appartenance au rôle d'utilisateur, qui détermine les rôles auxquels l'utilisateur appartient sur le service sélectionné.

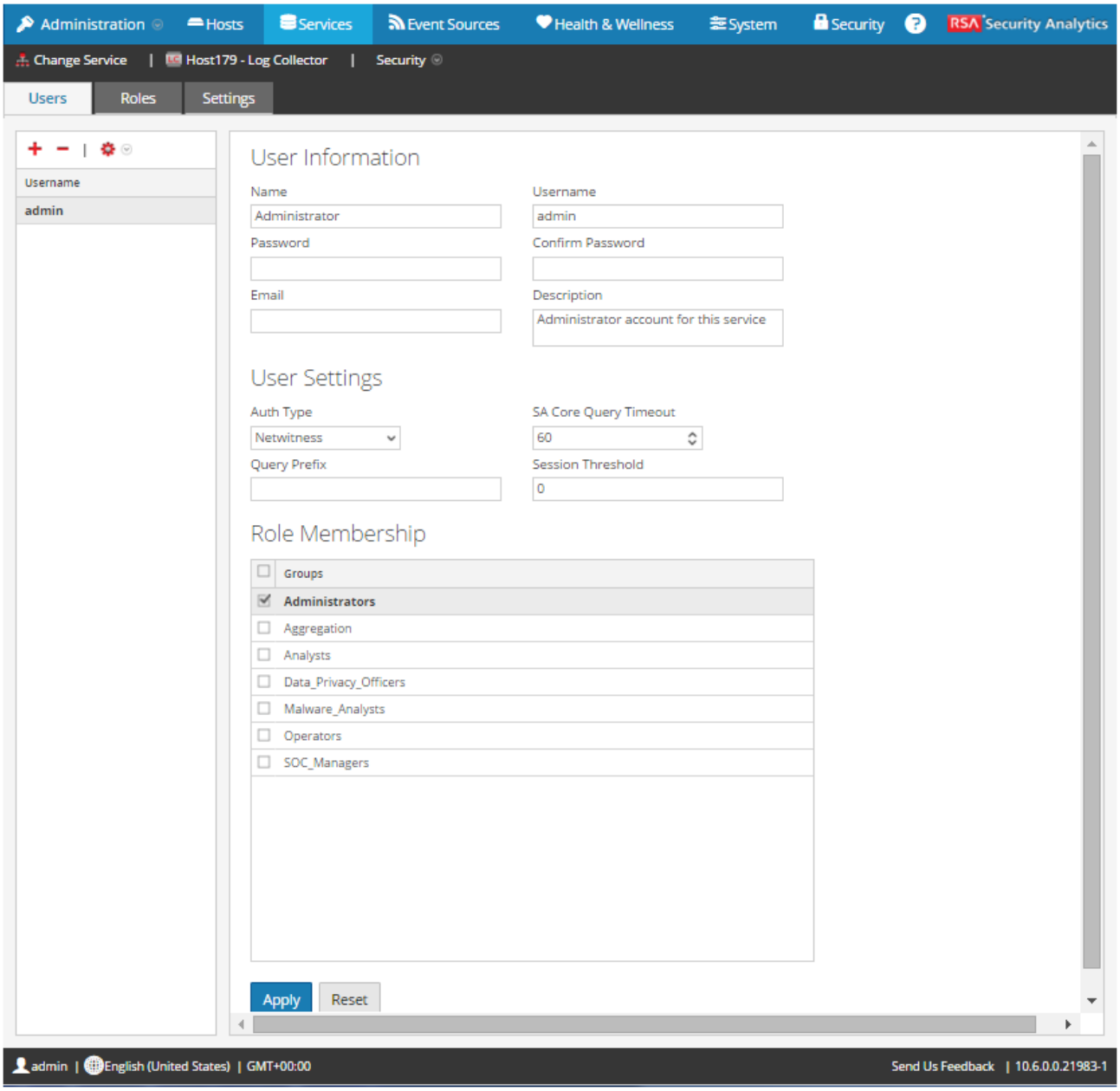
Note: Pour les services Security Analytics Core 10.4, ou version supérieure, qui utilisent des connexions approuvées, il n'est plus nécessaire de créer des comptes utilisateur Security Analytics Core pour les utilisateurs qui se connectent via le client Web. Vous n'avez besoin de créer de comptes utilisateurs Security Analytics Core que pour l'agrégation, les utilisateurs de clients Thick et les utilisateurs de l'API REST.

Les procédures liées à cet onglet sont décrites dans la section Procédures supplémentaires relatives aux services.

Pour accéder à la vue Sécurité des services > onglet Utilisateurs :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services.**
2. Sélectionnez un service auquel vous voulez ajouter un utilisateur, puis sélectionnez  **> Vue > Sécurité**.

Last Modified: August 10 2016, 9:33AM



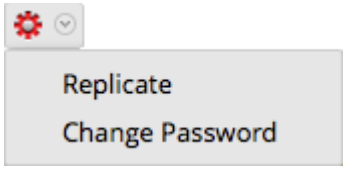
Caractéristiques

L'onglet Utilisateurs est doté d'un volet Liste d'utilisateurs sur la gauche. Le choix d'un nom d'utilisateur rend disponible le volet Définition de l'utilisateur sur la droite.

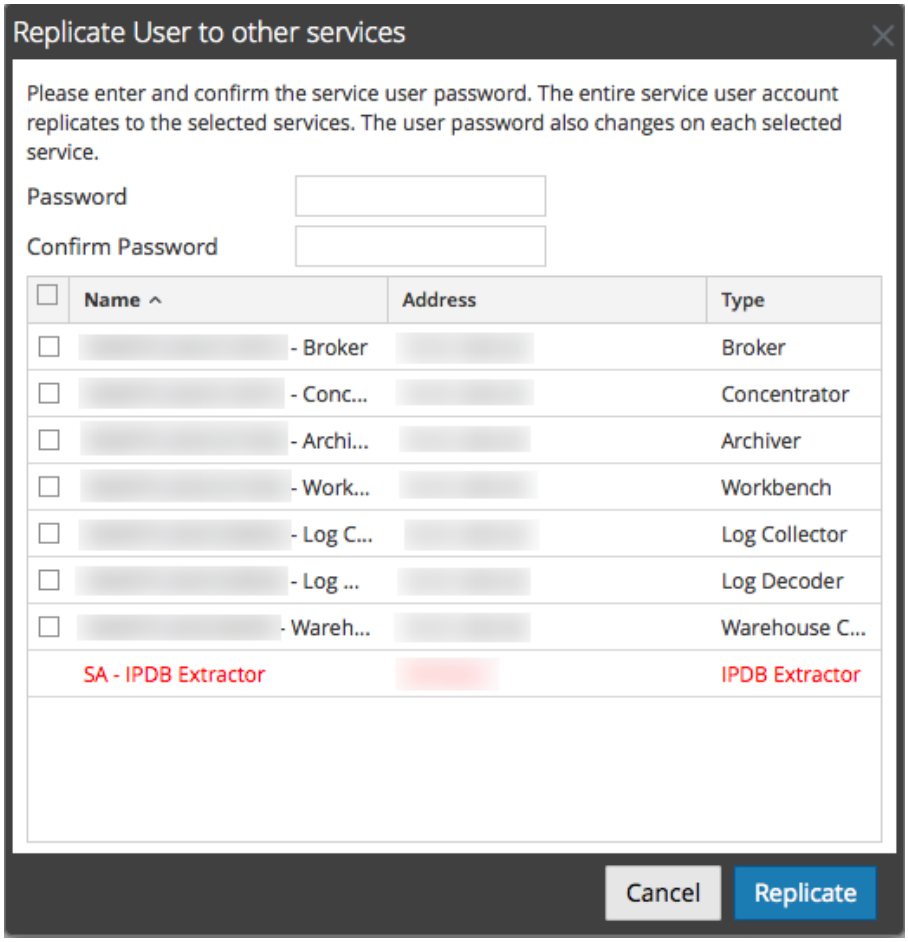
Volet Liste d'utilisateurs

Le volet Liste d'utilisateurs est doté des fonctionnalités suivantes.

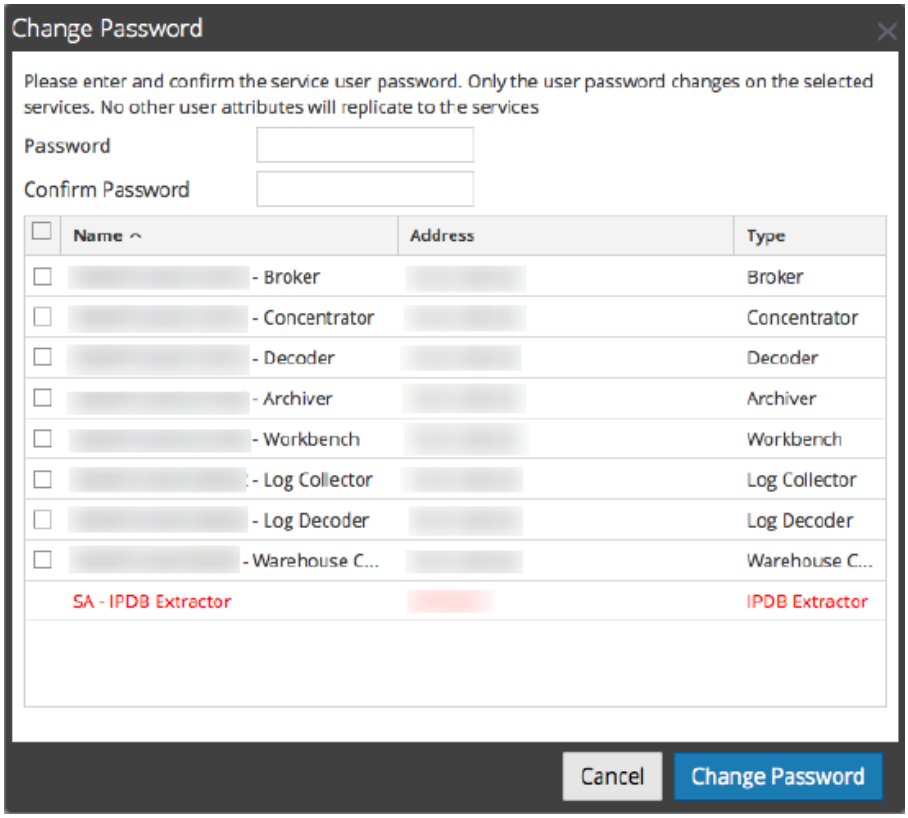
Last Modified: August 10 2016, 9:33AM

Fonction	Description
+	Ajoute un nouvel utilisateur au service en cours.
−	Supprime les utilisateurs sélectionnés du service.
	Effectue l'une des actions suivantes sur le compte utilisateur de service sélectionné : • **Répliquer :** Réplique l'intégralité du compte utilisateur du service sur les services sélectionnés. • **Modifier le mot de passe :** Modifie le mot de passe pour un utilisateur du service et réplique le nouveau mot de passe sur les services de base avec ce compte utilisateur défini. L'option Modifier le mot de passe réplique uniquement la modification du mot de passe sur les services de base sélectionnés et ne réplique pas l'intégralité du compte utilisateur.
Nom d'utilisateur	Les noms d'utilisateur de tous les comptes utilisateur qui accèdent au service. Le nom d'utilisateur doit être l'un de ceux utilisé pour ouvrir une session sur Security Analytics.

La figure suivante illustre la boîte de dialogue **Répliquer l'utilisateur sur les autres services**.



La figure suivante illustre la boîte de dialogue **Modifier le mot de passe**.



Volet Définition de l’utilisateur

Le volet Définition de l’utilisateur comporte trois sections :

- Information utilisateur identifie l'utilisateur tel qu'il a été créé dans la vue Administration - Sécurité.
- Paramètres utilisateur définit des paramètres qui s'appliquent à cet accès utilisateur pour le service.
- Adhésion aux rôles définit des rôles d'utilisateur auxquels l'utilisateur appartient.

Il y a deux boutons :

- Le bouton **Enregistrer** qui enregistre les modifications apportées dans le volet Définition de l'utilisateur et qui prennent effet immédiatement.
- Si vous n'avez pas enregistré les modifications dans le volet Définition de l'utilisateur, le bouton **Réinitialiser** réinitialise tous les champs et les paramètres sur leurs valeurs avant modification.

Informations utilisateur

La section Information utilisateur est dotée des fonctionnalités suivantes.

Champ	Description
Nom	Nom de l’utilisateur.

Champ	Description
Nom d'utilisateur	Le nom d'utilisateur que saisit cet utilisateur pour ouvrir une session du service. Il s'agit du nom d'utilisateur Security Analytics généré lorsque l'administrateur a ajouté l'utilisateur et les informations d'identification associées dans la vue **Administration - Sécurité** (Administration > Sécurité).
Mot de passe (et **Confirmer le mot de passe**)	Le mot de passe que l'utilisateur saisit pour ouvrir une session du service. Il s'agit du mot de passe Security Analytics généré lorsque l'administrateur a ajouté l'utilisateur et les informations d'identification associées dans la vue **Administration - Sécurité**. Le mot de passe du compte Security Analytics et celui du service doivent correspondre afin que l'utilisateur puisse se connecter au service via Security Analytics.
E-mail	(Facultatif) L'adresse e-mail de l'utilisateur.
Description	(Facultatif) Un champ de description générale pour décrire cet utilisateur.

Paramètres utilisateur

La section Paramètres utilisateur est dotée des fonctionnalités suivantes.

Champ	Description
Type auth.	Le schéma d'authentification pour cet utilisateur. La ligne de produits prend en charge une authentification interne et externe. • **Netwitness** indique une authentification interne ; elle est activée par défaut. Dans ce mode, tous les utilisateurs doivent s'authentifier avec le compte utilisateur et les mots de passe qui sont générés lorsque l'administrateur utilise la vue Administration - Sécurité (Administration > Sécurité) de Security Analytics pour créer l'utilisateur et ses informations d'identification associées. • **Externe** indique que l'authentification est activée via l'interface hôte avec les modules PAM (Pluggable Authentication Modules). Pour plus d'informations, reportez-vous à la rubrique Configurer la fonctionnalité de connexion PAM.
Préfixe de requête	(Facultatif) Ajoutez toujours la syntaxe de requête à toutes les requêtes de cet utilisateur. Par exemple, le fait d'ajouter le préfixe de requête **email != 'ceo@company.com'** empêche l'affichage des résultats de cet e-mail dans les sessions.
Expiration du délai de requête de base QA	**Note:** Ce champ s'applique à Security Analytics 10.5 et versions de service supérieures, et il ne s'affiche pas pour 10.4 et versions de service antérieures. Security Analytics 10.4 et services antérieurs utilisent Niveau de requête au lieu de Expiration du délai de requête de base QA. Spécifie le nombre maximal de minutes qu'un utilisateur peut utiliser pour exécuter une requête sur le service. Si cette valeur est définie sur zéro (0), l'expiration du délai de la requête n'est pas appliquée pour l'utilisateur sur le service. Lors de la réplication d'un utilisateur à partir d'un service Security Analytics 10.5 ou ultérieure vers un service Security Analytics 10.4, Expiration du délai de la requête migre vers Niveau de requête selon le niveau le plus proche. Par exemple, si un utilisateur obtient un Délai d'expiration de la requête de 15 minutes, son Niveau de requête sera de 3 après la migration. Si un utilisateur obtient un Délai d'expiration de la requête de 35 minutes, son Niveau de requête sera de 2 après la migration. Si un

Champ	Description
	utilisateur obtient un Délai d'expiration de la requête de 45 minutes, son Niveau de requête sera de 2 après la migration.
Seuil de session	(Facultatif) Contrôle le comportement de l'application lors de l'analyse des métavaleurs pour déterminer le nombre de sessions. Toute métavaleur avec un nombre de sessions supérieur au seuil établi arrête sa détermination du véritable nombre de sessions lorsque le seuil est atteint. Si un seuil est défini pour une session, la vue Navigation montre que le seuil a été atteint et affiche le pourcentage de temps de requête utilisé pour atteindre le seuil.

Adhésion aux rôles

La section Adhésion aux rôles affiche les rôles dont un utilisateur est membre pour le service sélectionné.

Vue Statistiques des services

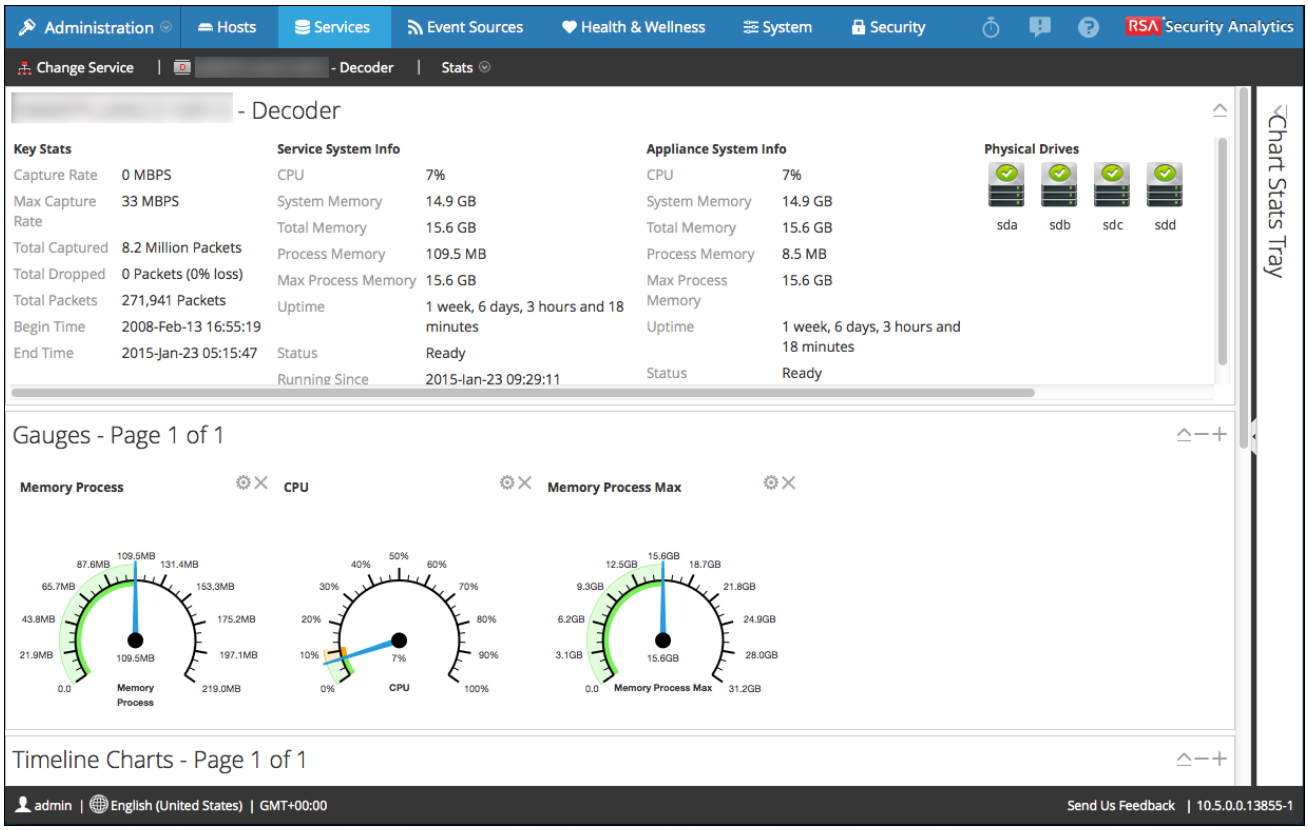
Cette rubrique décrit les fonctionnalités disponibles dans la vue Statistiques des services de Security Analytics.

La vue Statistiques des services propose une façon de surveiller l'état et les opérations d'un service. Cette vue affiche les principales informations relatives aux statistiques, au système de service et au système hôte d'un service spécifique. De plus, plus de 80 statistiques sont disponibles sous forme de jauges et de graphiques chronologiques. Dans les graphiques chronologiques de l'historique, seules les statistiques relatives à la taille des sessions, aux sessions et aux paquets peuvent être affichés.

Pour accéder à la vue Statistiques des services :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Sélectionnez un service et sélectionnez  **> Vue > Statistiques**.

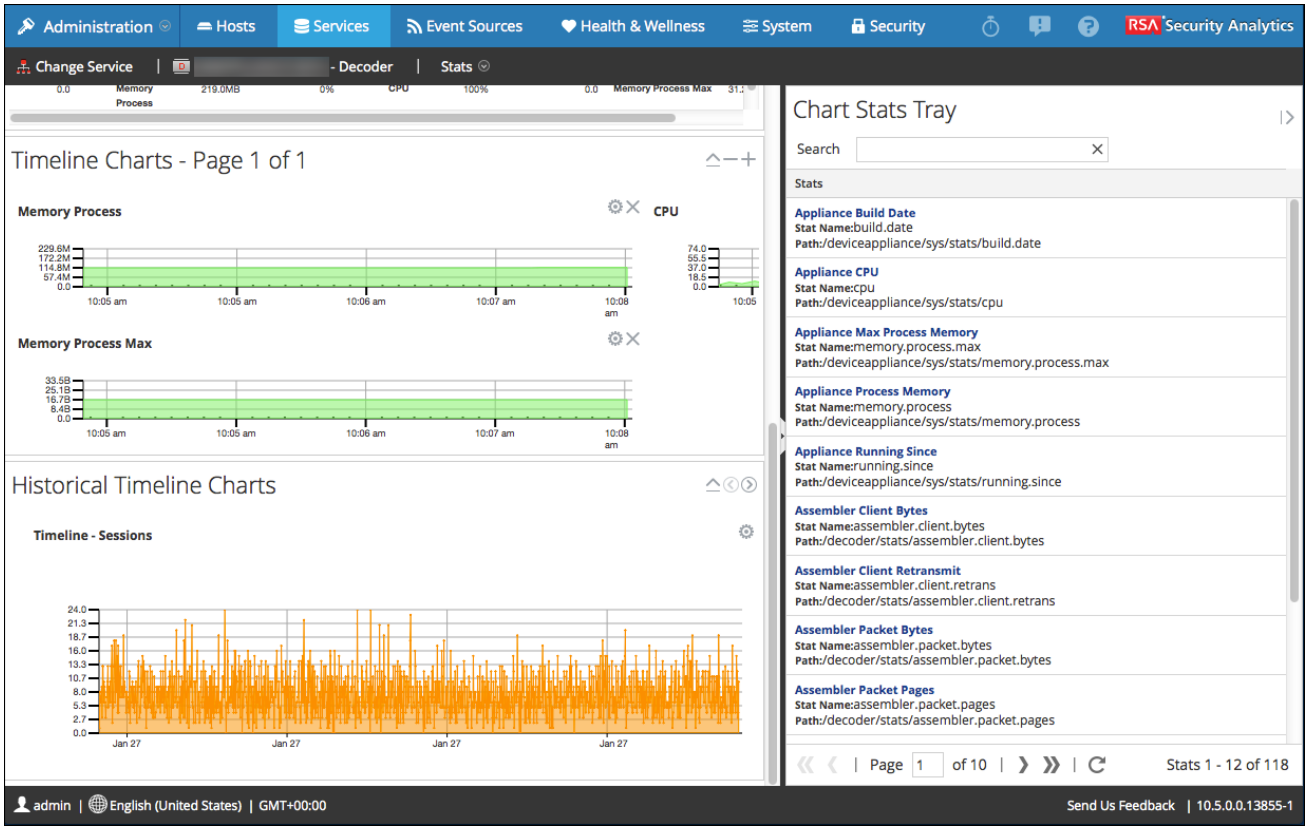
L'exemple suivant affiche la vue Statistiques des services pour un Decoder.



Last Modified: August 10 2016, 9:33AM

L'exemple suivant montre les autres graphiques disponibles en faisant défiler l'écran vers le bas.

L'exemple suivant montre la barre de statistiques graphiques développée.



Caractéristiques

Bien que différentes statistiques soient disponibles pour différents types de services, certains éléments sont communs à la vue Statistiques des services pour les services Core :

- Section Statistiques de synthèse
- Section Jauges
- Section Chronologies
- Section Graphiques chronologiques
- Barre d'état Statistiques graphiques

Section Statistiques de synthèse

La section Statistiques de synthèse apparaît en haut de la vue par défaut et ne dispose pas de champs modifiables.

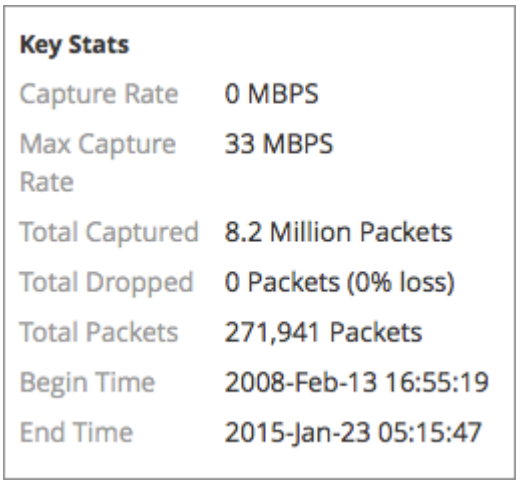
Cette section contient cinq panneaux. Le panneau **Statistiques clés** affiche des statistiques différentes pour des types de services différents. Les autres panneaux de la section Statistiques de synthèse sont les mêmes pour tous les types de services.

Last Modified: August 10 2016, 9:33AM

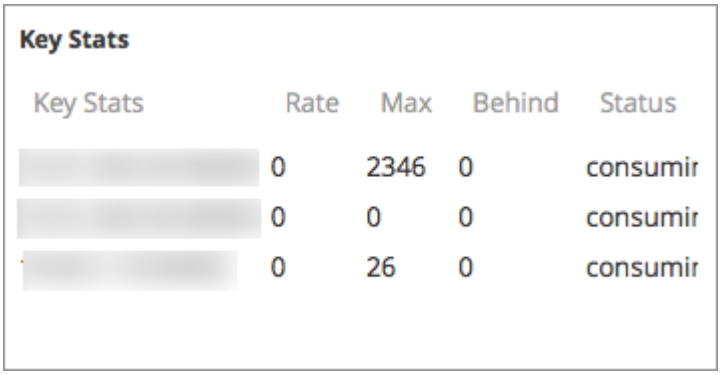
Statistiques clés

Le panneau Statistiques clés affiche des statistiques différentes pour des types de services différents.

- Pour Decoder ou Log Decoder, les statistiques clés comprennent les statistiques de capture telles que le taux de capture, le nombre total de paquets ou logs capturés, le nombre total de paquets ou logs abandonnés, l'heure de début et de fin des données capturées.

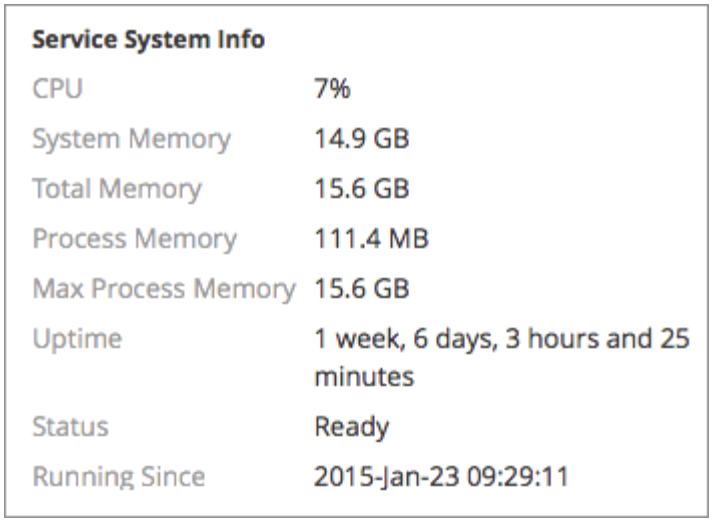


- Un Broker ou Concentrator agrège les données de plusieurs services. De ce fait, les statistiques clés de tous les services agrégés sont présentées dans une grille. Les colonnes de la grille indiquent le nom du service, le taux de capture, le nombre de sessions devant être agrégées et l'état du service.



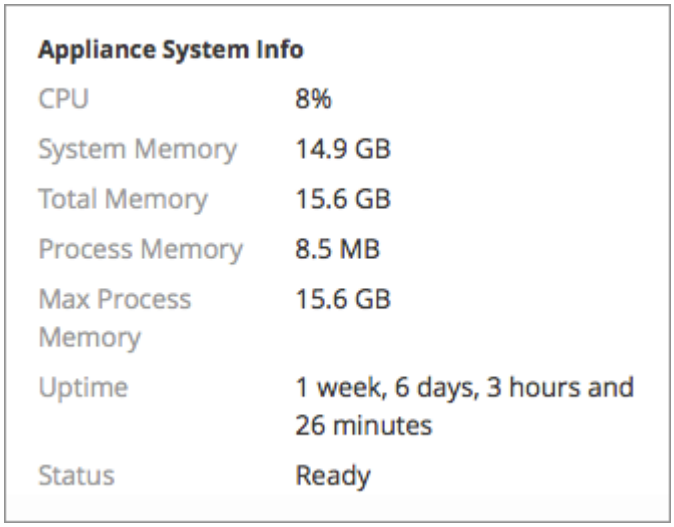
Informations sur le système

Le panneau Informations sur le système comprend le pourcentage d'utilisation du CPU par le service, les statistiques d'utilisation de la mémoire (système, total, processus et maximum), le temps de disponibilité du service, l'état, l'heure du début de fonctionnement et l'heure actuelle.



Service System Info	
CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	111.4 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 25 minutes
Status	Ready
Running Since	2015-Jan-23 09:29:11

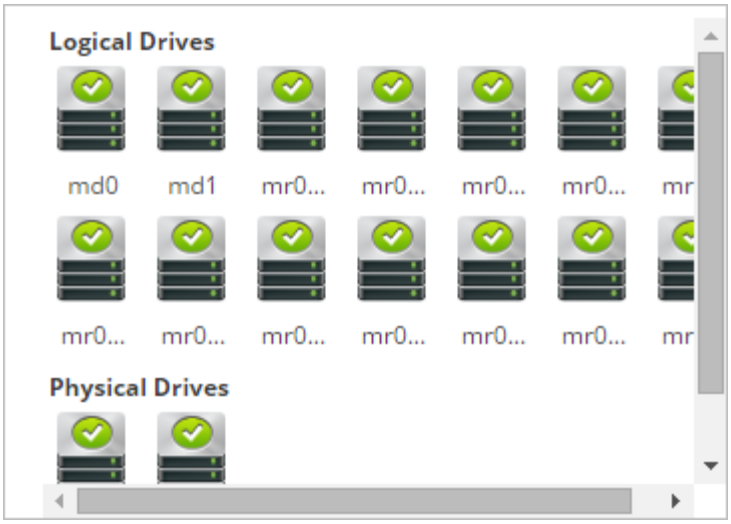
Les **Informations système de l'hôte** comprennent le pourcentage d'utilisation du CPU par l'hôte, les statistiques d'utilisation de la mémoire (système, total, processus et maximum), le temps de disponibilité de l'hôte, l'état, l'heure du début de fonctionnement et l'heure actuelle.



Appliance System Info	
CPU	8%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	8.5 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 26 minutes
Status	Ready

Les **Disques logiques** et les **Disques physiques** sont affichés avec une icône indiquant le nom et l'état du disque. Les types de disques utilisés dans les options de nom et d'état du disque apparaissent ci-dessous.

Last Modified: August 10 2016, 9:33AM



Types et état du disque

Type de disque	Description	Comment	Options d'état
sd	Périphérique de bloc SCSI	Directement connecté aux volumes SAS, SATA MegaRAID	OK (vert) ÉCHEC (rouge)
ld	Volume logique MegaRAID	Défini dans le BIOS ou avec l'outil MegaCLI	OK (vert) DÉTÉRIORÉ (jaune) EN ÉLABORATION (jaune) ÉCHEC (rouge)
pd	Disques physiques MegaRAID	Non directement exposés dans Linux	OK (vert) ÉCHEC (rouge)
md	Volume RAID pour le logiciel Linux		OK (vert) DÉTÉRIORÉ (jaune) EN ÉLABORATION (jaune) ÉCHEC (rouge)

Jauges

La section Jauges de la vue Statistiques des services présente les statistiques sous la forme de jauges analogiques. Voir Jauges pour plus de détails sur la configuration des jauges.

Chronologies

Les graphiques chronologiques affichent les statistiques sélectionnées dans une chronologie au fil du temps avec un focus sur la période en cours. C'est le même cas pour tous les types de services, et seul le nom d'affichage de la chronologie est modifiable. Voir les Graphiques chronologiques pour des détails sur la configuration de la chronologie.

Last Modified: August 10 2016, 9:33AM

Graphiques chronologiques de l'historique

Les graphiques chronologiques de l'historique affichent les statistiques relatives à la taille des sessions, aux sessions et aux paquets dans un graphique chronologique. C'est le même cas pour tous les types de services. Le nom d'affichage, la date de début et la date de fin sont modifiables. Voir les Graphiques chronologiques pour des détails sur la configuration de la chronologie.

Barre d'état Statistiques graphiques

La barre d'état Statistiques graphiques répertorie toutes les statistiques disponibles pour le type de service sélectionné. Les différents services ont différentes statistiques à surveiller. Voir Barre de statistiques graphiques pour une description détaillée.

Last Modified: August 10 2016, 9:33AM

Barre d'état Statistiques graphiques

Cette rubrique décrit la barre d'état Statistiques graphiques dans la vue Statistiques des services.

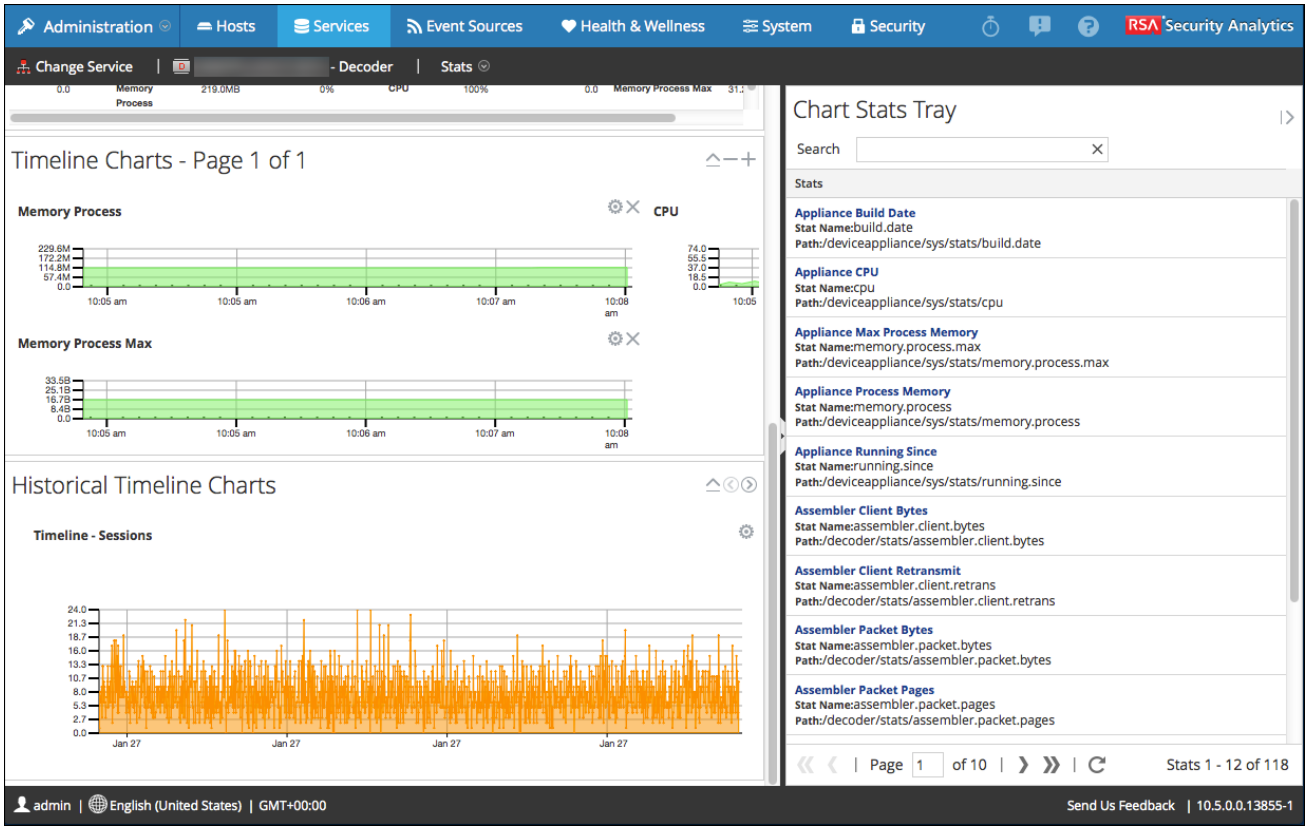
Dans la vue Statistiques des services, la barre d'état Statistiques graphiques offre un moyen de personnaliser les statistiques surveillées des différents services. La barre d'état Statistiques graphiques répertorie toutes les statistiques disponibles pour le service. Le nombre de statistiques varie en fonction du type de service en cours de surveillance. Toute statistique de la barre d'état Statistiques graphiques peut être affichée sous forme de graphique en jauge ou chronologique. Seules les statistiques relatives à la taille des sessions, aux sessions et aux paquets peuvent être affichés sous forme de graphiques chronologiques et historiques.

Pour accéder à la vue Statistiques des services :

1. Dans le menu **Security Analytics** , sélectionnez **Administration > Services**
   La vue Services d'administration s'affiche.
2. Sélectionnez un service, puis  **> Vue > Statistiques.**.
   La barre d'état Statistiques graphiques se situe sur le côté droit.
3. Si cette barre est réduite, cliquez sur  pour consulter la liste des statistiques disponibles.

L'exemple suivant affiche la vue Statistiques des services pour un Decoder. La barre d'état Statistiques graphiques est ouverte dans le panneau de droite.

Last Modified: August 10 2016, 9:33AM



Composants

La barre d'état Statistiques graphiques comporte différentes statistiques pour différents types de services. Dans l'exemple ci-dessus, 111 statistiques sont disponibles pour le Decoder. Le tableau suivant décrit les fonctions de la barre d'état Statistiques graphiques.

Fonction	Description
	Cliquez pour développer le panneau horizontalement.
	Cliquez pour réduire le panneau horizontalement.
Rechercher	Tapez un terme de recherche dans le champ et appuyez sur **RETOUR**. Lorsque les statistiques correspondent, le mot correspondant s'affiche en surbrillance.
	Cliquez pour accéder à la première page.
	Cliquez pour accéder à la page précédente.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
| Page 3 of 10 |	Saisissez un numéro de page dans le champ Page.
›	Cliquez pour passer à la page suivante.
»	Cliquez pour passer à la dernière page.
	Cliquez ici pour actualiser la vue.
Stats 1 - 12 of 111	Affiche la plage de statistiques. Le nombre total de statistiques de nombre varie selon le type de service.

Last Modified: August 10 2016, 9:33AM

Jauges

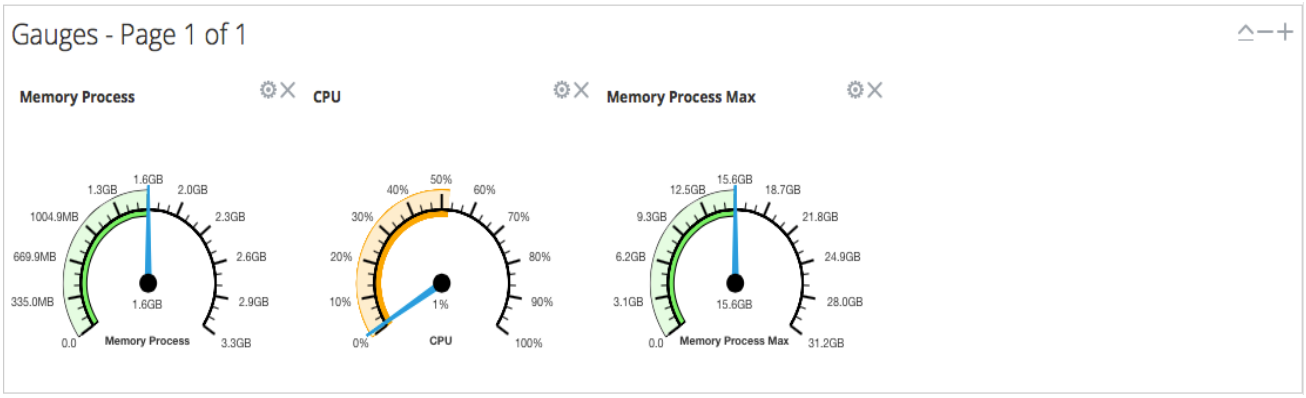
Cette rubrique présente les fonctions de la section Jauges dans la vue Statistiques des services.

La section Jauges de la vue Statistiques des services présente les statistiques sous la forme d'une jauge analogique. Vous pouvez faire glisser les statistiques disponibles dans la barre d'état Statistiques graphiques vers la section Jauges. Les propriétés de chaque jauge sont modifiables, comme leur titre, mais aussi, pour certaines d'entre elles, d'autres propriétés encore.

Pour accéder à la vue Statistiques des services :

1. Dans le menu **Security Analytics** , sélectionnez **Administration > Services**
   La vue Services d'administration s'affiche.
2. Sélectionnez un service et cliquez sur **> Vue > Statistiques**.
   La vue Statistiques des services contient la section Jauges.

La figure ci-dessous illustre les jauges par défaut de la vue Statistiques des services pour un Log Decoder.



Caractéristiques

Les jauges par défaut indiquent les statistiques suivantes :

- Utilisation de la mémoire du processus
- Utilisation du CPU
- Mémoire de processus maximale utilisée

Les contrôles de la barre de titre Jauges et de chaque jauge sont les contrôles de dashlet standard.

- Dans la barre de titre Jauges, vous pouvez réduire et développer la section et avancer ou reculer d'une page.

Last Modified: August 10 2016, 9:33AM

- Dans chaque jauge, vous pouvez modifier les propriétés ( ) et supprimer ( ) la jauge.

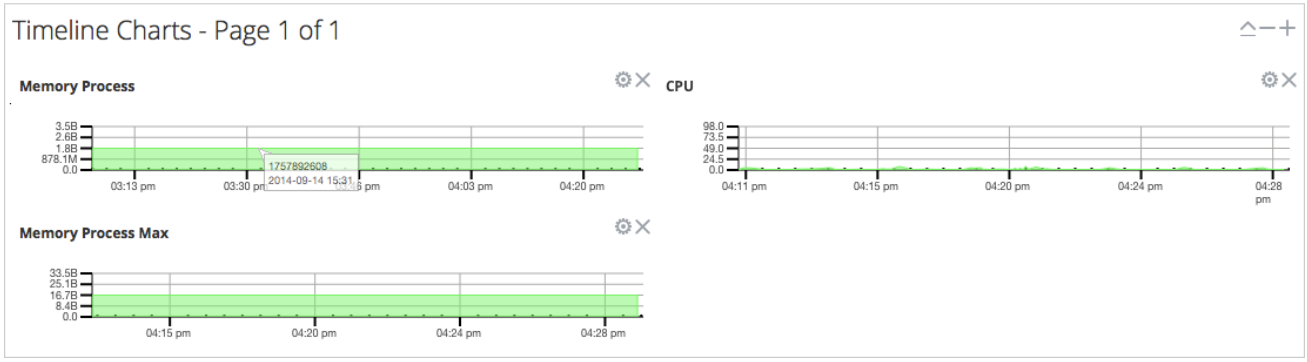
Last Modified: August 10 2016, 9:33AM

Graphiques chronologiques

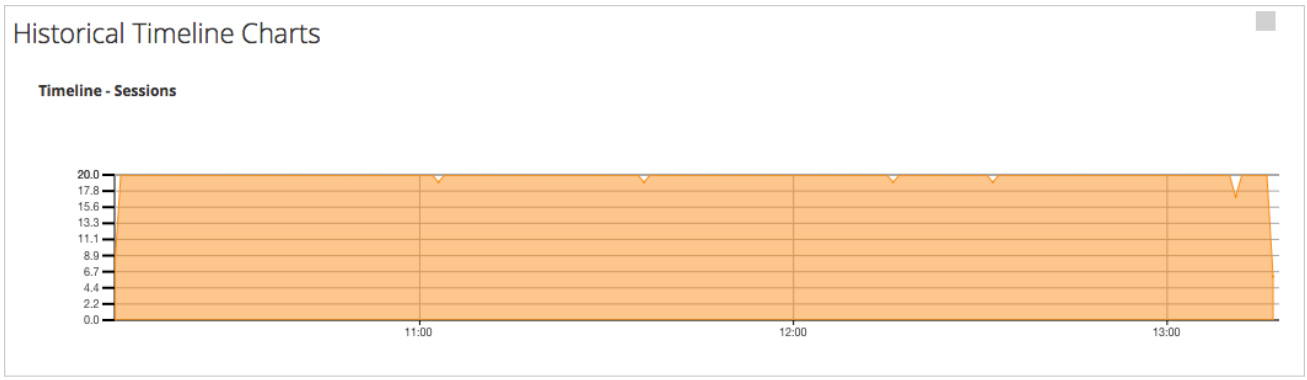
Cette rubrique décrit les fonctions des graphiques chronologiques dans la vue Statistiques des services.

Les graphiques chronologiques affichent les statistiques au fil du temps. La vue Statistiques des services contient deux types de chronologies : actuelle et historique. Vous pouvez faire glisser les statistiques disponibles dans la barre d'état Statistiques graphiques vers la section Graphiques chronologiques. Seules les statistiques relatives à la taille des sessions, aux sessions et aux paquets peuvent être affichés sous forme de graphiques chronologiques et historiques. Les propriétés de chaque graphique chronologique sont modifiables, comme leur titre, mais aussi, pour certains d'entre eux, d'autres propriétés encore.

La figure ci-dessous illustre un exemple de graphique de chronologie actuelle indiquant la valeur et l'horodatage d'un point de données.



La figure ci-après présente un exemple de graphique de chronologie historique.



Les graphiques de chronologie actuelle contiennent les statistiques suivantes :

Last Modified: August 10 2016, 9:33AM

- Mémoire processus
- CPU
- Mémoire processus max.

Les graphiques de chronologie historique contiennent les statistiques suivantes :

- Sessions
- Paquets
- Taille des sessions

Les contrôles de la barre de titre Graphiques chronologiques et de chaque chronologie sont les contrôles de dashlet standard.

- Dans la barre de titre Graphiques chronologiques, vous pouvez réduire et développer la section et avancer ou reculer d'une page.
- Dans chaque chronologie, vous pouvez modifier Propriétés () et supprimer () la chronologie.
- Lorsque vous survolez un point de données du graphique, la valeur et l'horodatage du point sélectionné s'affichent.

Vue Statistiques des services - Malware Analysis

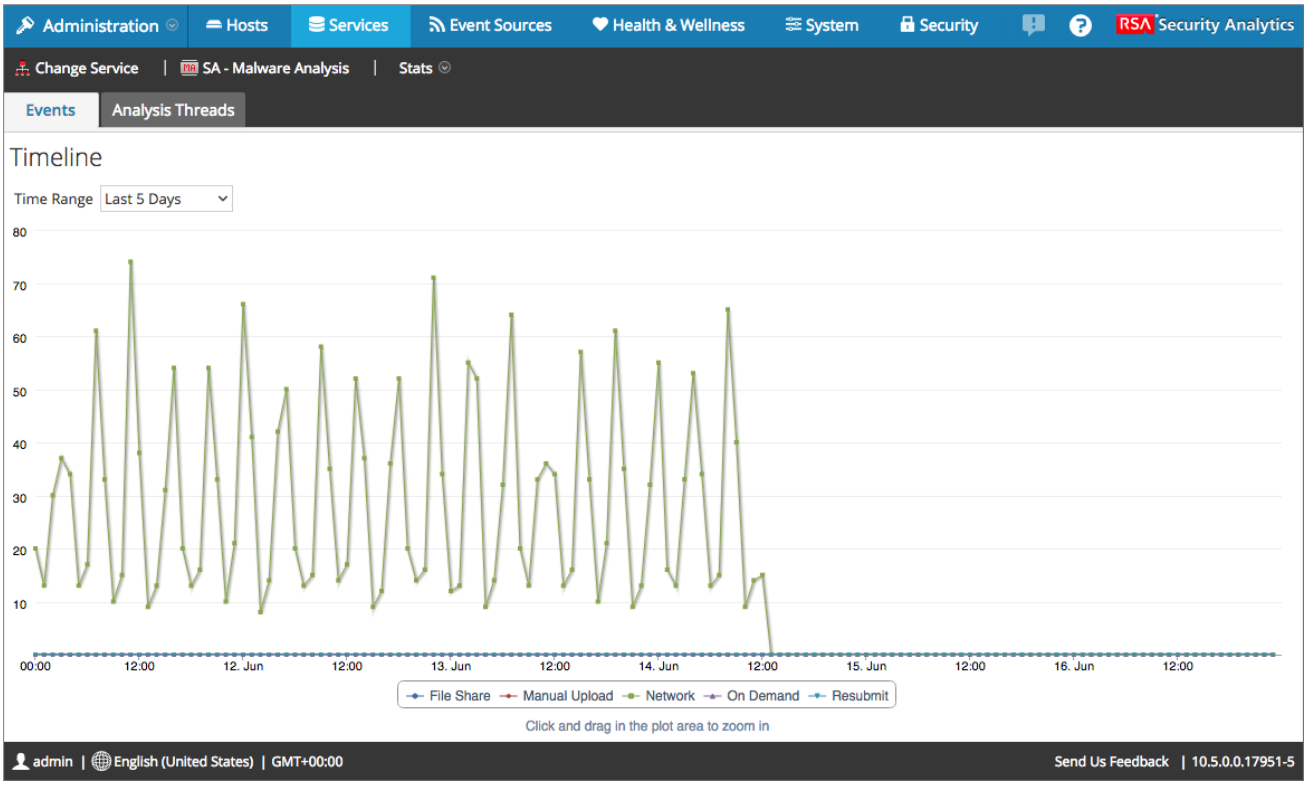
Cette rubrique décrit les fonctions disponibles dans la vue Statistiques des services Security Analytics pour Malware Analysis.

La vue Statistiques des services propose une façon de surveiller l'état et les opérations d'un service.

Pour accéder à la vue Statistiques des services pour Malware Analysis :

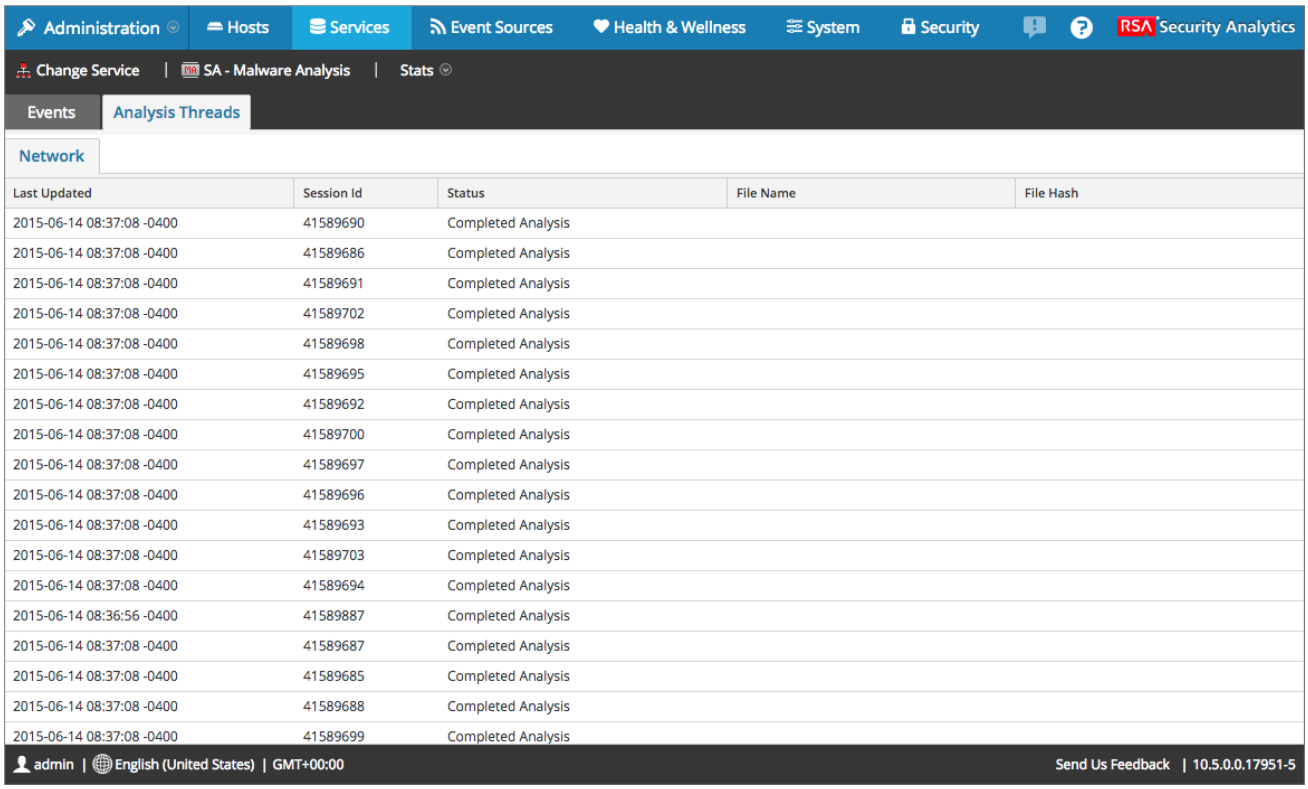
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Sélectionnez un service et sélectionnez **> Vue > Statistiques**.

La figure suivante affiche la vue Statistiques des services pour Malware Analysis. L'onglet par défaut est l'onglet Événements.



La figure suivante présente l'onglet Threads d'analyse.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

La vue Statistiques des services pour Malware Analysis comporte deux onglets :

- Onglet Événements
- Onglet Threads d'analyse

Onglet Events

L'onglet Événements contient le graphique Chronologie, qui affiche le nombre d'événements à différentes heures tout au long de la journée.

Le tableau suivant décrit les fonctions de l'onglet Événements.

Fonction	Description
Menu déroulant Période	Ce menu propose différentes options pour la période affichée sur le graphique. Vous pouvez choisir une période personnalisée en sélectionnant **Personnalisé** et en choisissant une date de début et de fin dans les menus déroulants.
Zone de tracé	Chaque type d'événement est représenté par une couleur différente sur le graphique. Vous pouvez zoomer sur des sections du graphique en cliquant et en faisant glisser pour sélectionner la section que vous souhaitez afficher de plus près.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
Clé Type d'événement	En bas de l'onglet, les types d'événements affichés dans la zone de tracé s'affichent, avec leurs couleurs de ligne respectives. Par exemple, la ligne Réseau est verte et la ligne À la demande est violette. Pour désactiver l'une des options sur le graphique, cliquez dessus. Elle est alors grisée et sa ligne est retirée du graphique.

Onglet Threads d'analyse

Malware Analysis peut analyser de nombreux fichiers simultanément. Chacun est représenté par un thread. Chaque fichier suit un processus linéaire lorsqu'il est analysé :

1. Analyse de métadonnées du réseau
2. Demander le fichier à Decoder
3. Statique
4. Communauté (si activé)
5. Sandbox (si activé)

Cet onglet vous présente l'état de chaque thread pour déterminer où se trouve actuellement le fichier dans le processus d'analyse. Les états de thread sont triés par le type d'analyse de fichier, qui est la méthode par laquelle Malware Analysis reçoit le fichier, comme une Session réseau, un Téléchargement manuel du fichier ou une analyse À la demande.

Ceci est particulièrement utile pour déterminer quelle partie de l'analyse est le facteur limitant pour la durée. Par exemple, vous pouvez accéder à l'onglet et voir les 20 threads de Fichiers en demande de NextGen. Cela signifie que Decoder rencontre des problèmes ou est débordé, et ne peut pas effectuer la livraison rapidement.

Si les threads n'ont pas mis à jour leur état depuis une longue période, cela peut indiquer que Malware Analysis est bloqué.

Le tableau suivant fournit les descriptions des colonnes de la liste.

Colonne	Description
Dernière mise à jour	Date et heure les plus récentes auxquelles le thread s'est mis à jour.
ID de session	ID de la session.
État	État de l'analyse des fichiers.
Nom de fichier	Nom du fichier analysé.
Hachage de fichier	Hachage du fichier analysé.

Vue Système de services

Cette rubrique présente les fonctions et caractéristiques de la vue Système de services.

La vue Système de services fournit un résumé des services Security Analytics Core et d'autres services, par exemple Reporting Engine.

Les informations récapitulatives des services Security Analytics Core (Broker, Concentrator, Decoder et Log Decoder) sont similaires, notamment les informations relatives à ce qui suit :

- Service
- Service Appliance
- Informations utilisateur sur les services
- Informations utilisateur sur les hôtes
- Informations sur les licences
- Informations de session

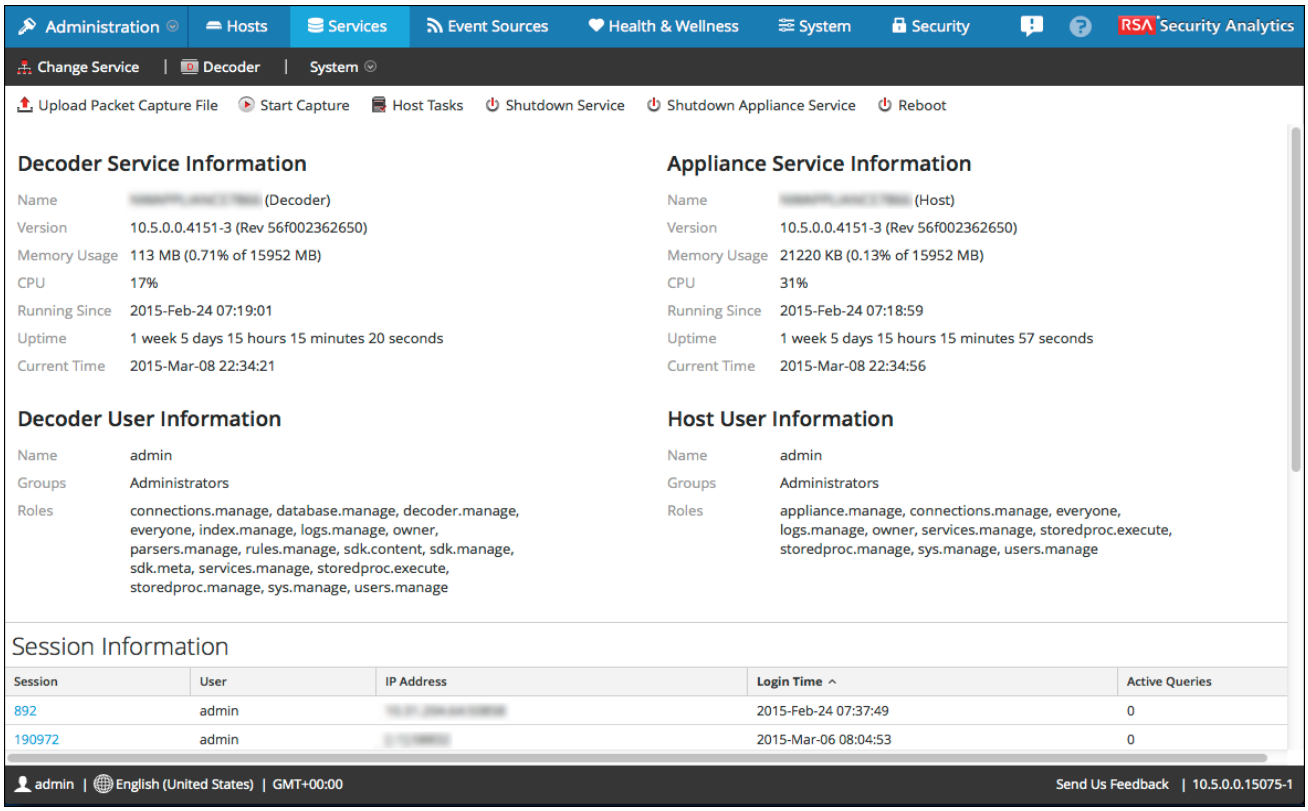
La barre d'outils des services Security Analytics Core est également similaire. Les options permettent d'exécuter les tâches de l'hôte via la ligne de commande, de contrôler les services et les hôtes, et d'autres tâches spécifiques aux services telles que le téléchargement des fichiers de capture de paquets et de fichiers logs vers un service.

Pour accéder à la vue Système de services :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services d'administration s'affiche.
2. Sélectionnez un service et sélectionnez  **> Vue > Système**.

Voici un exemple de la vue Système de services d'un Decoder.

Last Modified: August 10 2016, 9:33AM



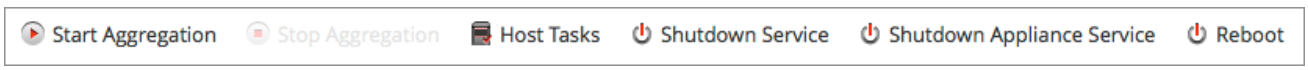
Caractéristiques

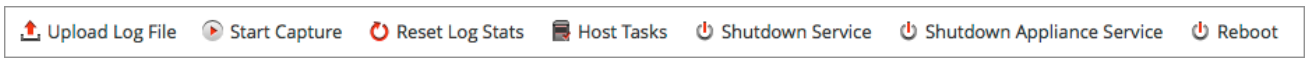
Cette section décrit les fonctions communes aux types de services Security Analytics Core.

- Les fonctions spécifiques aux Brokers et Concentrators sont décrites dans la rubrique Brokers et Concentrators.
- Les fonctions spécifiques aux services Decoder et Log Decoder sont décrites dans la rubrique Decoders.

Barre d'outils de la vue Système de services

Une barre d'outils s'affiche en haut de la vue Système de services. Certaines options de la barre d'outils s'appliquent à un type de service spécifique, mais quatre options sont communes à tous les types de services. Les exemples ci-dessous montrent les options relatives à un Concentrator, à un Decoder et un Log Decoder.





Last Modified: August 10 2016, 9:33AM

Ce tableau décrit les options de la barre d'outils de la vue Système de services communes à tous les services Core.

Action	Description
Tâches de l'hôte	Affiche la boîte de dialogue Liste des tâches de l'hôte qui permet d'exécuter des tâches de l'hôte via la ligne de commande depuis une liste de sélection. Pour obtenir des informations détaillées, reportez-vous à la rubrique Boîte de dialogue Liste des tâches de l'hôte.
Arrêter le service	Arrête et redémarre le service d'un Decoder, Log Decoder, Broker ou Concentrator.
Arrêt du service Appliance	Arrête tous les services s'exécutant sur l'hôte, puis redémarre le service Appliance pour un Log Decoder, Log Decoder, Broker ou Concentrator.
Redémarrer	Arrête et redémarre l'hôte sur lequel les services Core sont en cours d'exécution.

Informations récapitulatives des services

La partie supérieure de la vue Système de services résume les informations sur le service sélectionné. Cela s'applique à tous les types de services Core : Decoders, Brokers, Concentrators et Log Decoders.

Catégorie	Description
Informations sur les services et le service Appliance	Les informations concernent le nom du service, la version du service, l'utilisation de la mémoire en mégaoctets, l'utilisation de la mémoire en pourcentage par rapport à la mémoire totale, l'heure et la date de début d'exécution du service, la durée d'exécution du service, et l'heure actuelle.
Informations utilisateur sur les services et les hôtes	Affiche les utilisateurs qui ont accès à ce service et le rôle de l'utilisateur auquel ils appartiennent.
Informations sur les licences	Affiche l'ID de l'ordinateur relatif au service et aux licences installés. • Dans Security Analytics 10.1 et version ultérieure, les informations sur les licences concernent la clé de licence fournie pour le service par le serveur de licences local de Security Analytics. • Dans Security Analytics 10.0, chaque licence a une date d'expiration et certaines ont d'autres paramètres, comme le stockage maximal sur le système.

Grille Informations de session

La partie inférieure de la vue Système de services fournit une liste des sessions actives. Cette vue vous permet d'effectuer les opérations suivantes :

- Fermer une session
- Mettre fin à une requête active

Le tableau décrit les colonnes de la grille Informations de session.

Catégorie	Description
Session	ID de la session. Cliquer sur l'ID de la session permet d'afficher une boîte de dialogue contenant l'option de suppression de la session. Vous pouvez approuver ou annuler l'action.
Utilisateur	Nom du propriétaire de la session.
Adresse IP	Adresse IP du service où la session s'exécute.
Heure de connexion	Heure à laquelle l'utilisateur s'est connecté.
Requêtes actives	Nombre de requêtes actives. Cliquer sur un nombre autre que zéro permet d'afficher une boîte de dialogue dans laquelle vous pouvez arrêter l'exécution d'une requête.

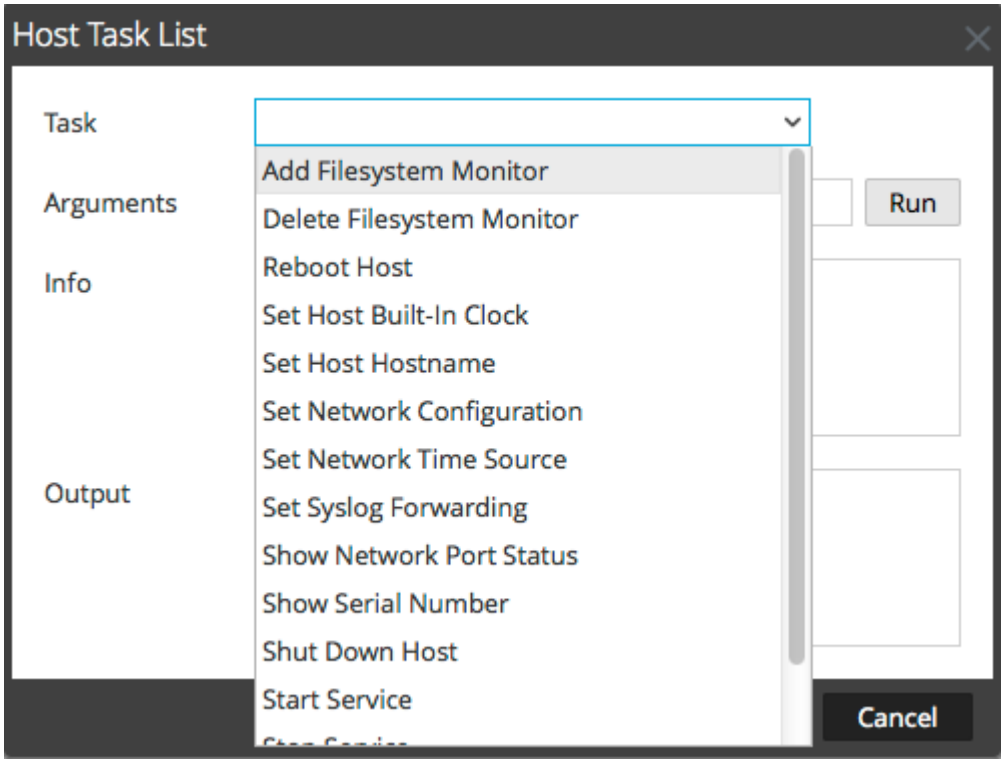
Boîte de dialogue Liste des tâches de l'hôte

Cette rubrique présente la vue Système de services > boîte de dialogue Liste des tâches de l'hôte.

Dans la vue Système de services RSA Security Analytics, vous pouvez utiliser l'option Tâches de l'hôte pour gérer les tâches liées à un hôte et à ses communications avec le réseau. Plusieurs options de configuration de service et d'hôte sont disponibles pour les services Core.

Pour accéder à la boîte de dialogue Tâches de l'hôte :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service et sélectionnez > **Vue > Système**.
   La vue Système du service s'affiche.
3. Dans la barre d'outils **Vue Système de services,** cliquez sur **Tâches de l'hôte**.
   La boîte de dialogue Liste de tâches d'hôte s'affiche. La liste **Tâche** propose une liste des messages pris en charge pour l'hôte associé.



Last Modified: August 10 2016, 9:33AM

Caractéristiques

Le tableau ci-dessous décrit les fonctions de la boîte de dialogue.

Champ	Description
Tâche	Champ d'entrée dans lequel vous saisissez ou sélectionnez un message pour un hôte Core. Lorsque vous cliquez dans ce champ, une liste déroulante de tâches d'hôtes disponibles s'affiche.
Arguments	Champ d'entrée dans lequel vous saisissez les arguments, le cas échéant, pour le message.
Exécuter	Exécute la tâche et les arguments dans les champs d'entrée.
Informations	Informations sur l'objectif et la syntaxe du message.
Résultat	Sortie ou résultat d'une tâche exécutée.
Annuler	Ferme la boîte de dialogue de tâche d'hôte.

Liste de sélection de tâche d'hôte

Ces tâches sont affichées sous forme de liste déroulante dans le champ Tâche. Les options disponibles sont régulées par le rôle de sécurité requis pour exécuter l'option.

Tâche	Description
Ajouter la surveillance du système de fichiers	Commence à surveiller les services de stockage ajoutés au système de fichiers spécifié (voir Ajouter et supprimer la surveillance du système de fichiers).
Supprimer la surveillance d'un système de fichiers	Arrête de surveiller les services de stockage ajoutés au système de fichiers spécifié (voir Ajouter et supprimer la surveillance du système de fichiers).
Redémarrer l'hôte	Arrête et redémarre l'hôte (voir Redémarrer un hôte).
Paramétrer l'heure prédéfinie de l'hôte	Règle l'horloge locale de l'hôte (voir Paramétrer l'heure prédéfinie de l'hôte).
Définir le nom de l'hôte	Cette méthode de modification du nom d'hôte est déconseillée dans Security Analytics 10.6 ; remplacée par la procédure décrite dans la rubrique Modifier le nom ou le nom d'hôte d'un hôte.
Définir la configuration réseau	Définit les paramètres d'adresse réseau (voir Définir la configuration réseau).
Définir la source de l'heure réseau	Définit la source de l'heure pour cet hôte (voir Définir la source de l'heure réseau).
Définir le transfert Syslog	Active ou désactive le transfert syslog à partir d'un serveur distant sur le service sélectionné (voir Définir le transfert Syslog).

Last Modified: August 10 2016, 9:33AM

Tâche	Description
Afficher l'état du port réseau	Affiche les informations d'interface réseau pour un hôte (voir Afficher l'état du port réseau).
Afficher le numéro de série	Obtient un numéro de série d'hôte (voir Afficher le numéro de série).
Arrêter l'hôte	Arrête l'hôte physique, qui reste éteint (voir Arrêter l'hôte).
Démarrer le service	Démarre un service sur cet hôte (voir Arrêter et démarrer un service sur un hôte).
Arrêter le service	Arrête un service sur cet hôte (voir Arrêter et démarrer un service sur un hôte).
setSNMP	Active ou désactive le service SNMP sur un hôte (voir Configurer SNMP).

Last Modified: August 10 2016, 9:33AM

Vue Système de services Decoder

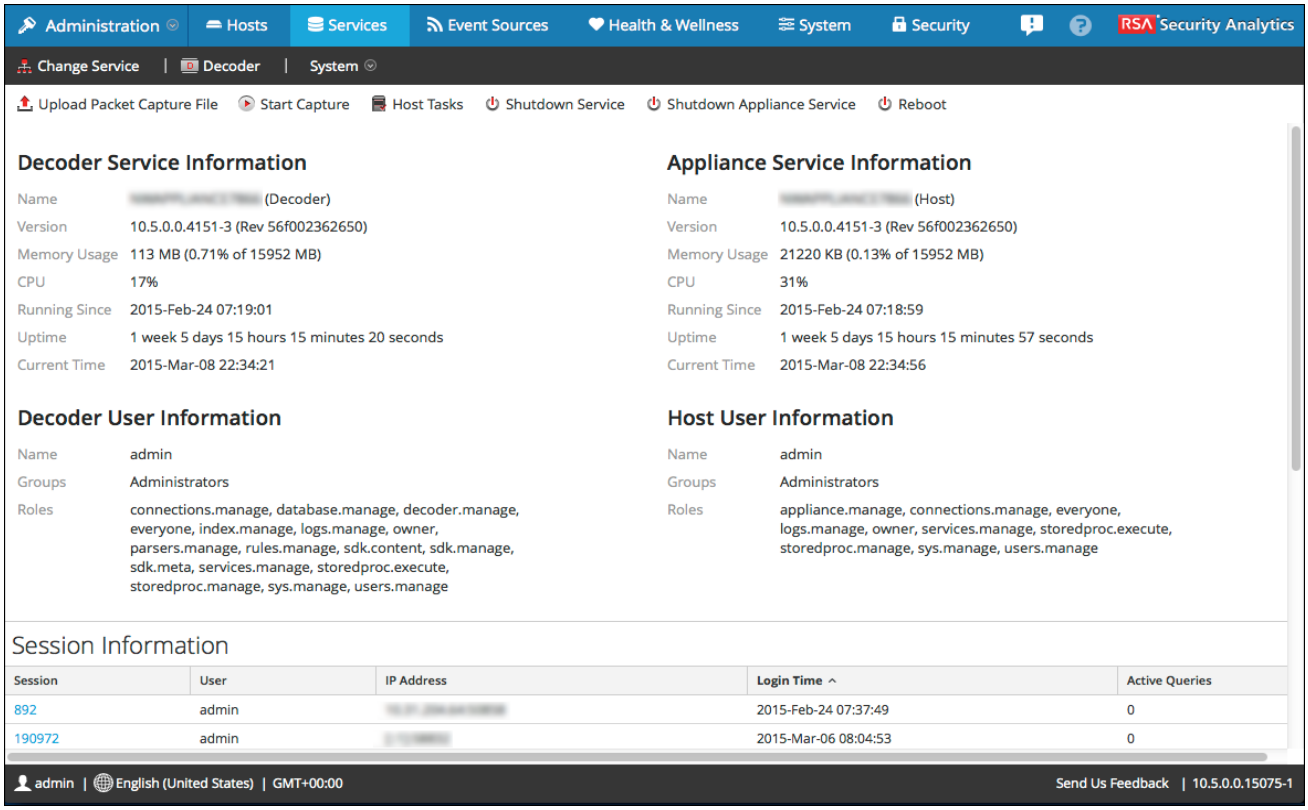
Cette rubrique présente les fonctions de la vue Système qui appartiennent spécifiquement aux Decoders et Log Decoders.

Un Log Decoder est un type particulier de Decoder, et il est configuré et géré de manière équivalente à un Decoder. Ainsi, la plupart des informations de cette section se rapportent aux deux types de Decoders. Les différences concernant les Log Decoders sont annotées.

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

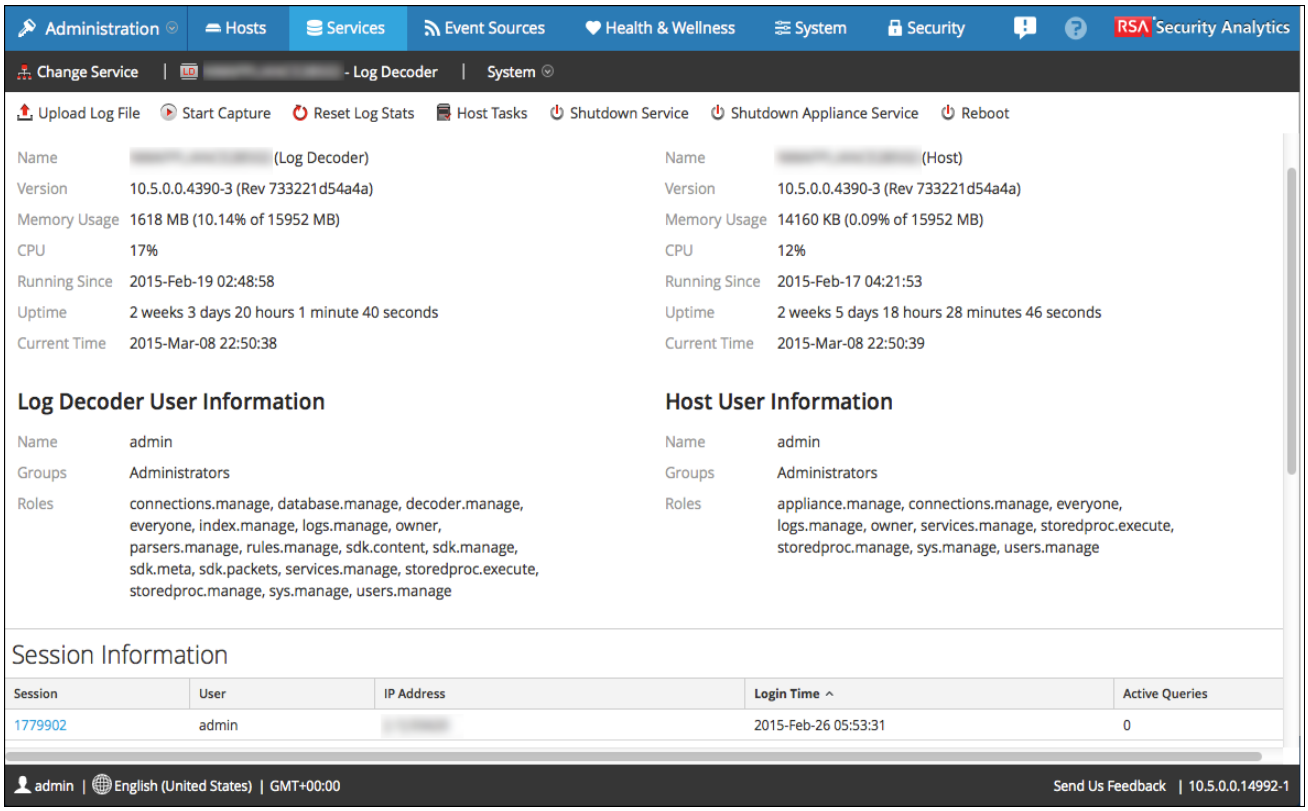
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services d'administration s'affiche.
2. Sélectionnez un service, puis sélectionnez  **> Vue > Système**.

La figure suivante affiche un exemple de la vue Système de services d'un décodeur.



Last Modified: August 10 2016, 9:33AM

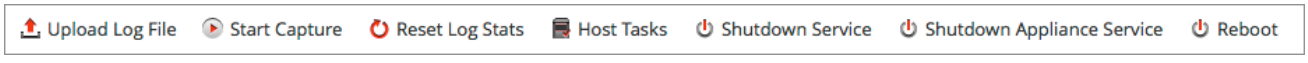
La figure suivante affiche la vue Système de services d'un Log Decoder.



Caractéristiques

Barre d'outilsInfo services

Les barres d'outils suivantes affichent les options spécifiques aux Decoders et aux Logs Decoders.



En plus des options classiques dont vous disposez dans la barre d'outils de la vue Système de services, vous pouvez démarrer et arrêter la capture de paquets ou de logs. Les options de téléchargement de fichier sont différentes de celles du Decoder standard (fichier de capture de paquet) et du Log Decoder (fichier log).

Action	Description
Télécharger le fichier de capture de paquets	Affiche une boîte de dialogue qui propose une façon de sélectionner un fichier de capture de paquet (.pcap) à télécharger vers le Decoder sélectionné. Pour plus d'informations, reportez-vous à la rubrique Télécharger le fichier de capture de paquets. **Note:** Cette option ne s'applique pas aux Log Decoders.
Télécharger le fichier log	Affiche une boîte de dialogue qui propose un moyen de sélectionner un fichier log (.log) à télécharger vers le Log Decoder sélectionné. Pour plus d'informations, reportez-vous à la rubrique Télécharger un fichier log vers un Log Decoder.
Démarrer/arrêter la capture	Démarre la capture de paquet sur le Decoder sélectionné. Lorsque la capture de paquets est en cours, l'option de la barre d'outils se change en Arrêter la capture, et l'option pour télécharger un fichier est disponible.

Dépanner les mises à jour de l'hôte

Cette rubrique contient des instructions sur la résolution des problèmes liés aux mises à jour de l'hôte.

Elle répertorie les conflits avant la mise à jour, les erreurs de mise à jour et les messages de log qui peuvent se produire lors de la mise à jour d'un hôte. Elle identifie également la cause des conflits, des erreurs de mise à jour et des messages d'erreur et propose des solutions.

Last Modified: August 10 2016, 9:33AM

RSA

Dépannage suite aux avertissements, conflits et erreurs liés à la préparation de la mise à jour et la mise à jour vers la version 10.6

Cette section contient les messages d'erreur concernant la vérification de la préparation de la mise à jour, ainsi que la mise à jour vers la version 10.6.0 au sein de la vue Hôtes avec une description de chaque message et des instructions sur le mode de réponse à ces messages.

Avertissements liés à la préparation de la mise à jour

Les avertissements liés à la préparation de la mise à jour concernent les anomalies et les problèmes potentiels de configuration qui ne vous empêchent pas d'effectuer la mise à jour vers la nouvelle version. Si Security Analytics rencontre un problème potentiel, il affiche un avertissement lié à la préparation de la mise à jour. Voir les détails dans la colonne **État** de la vue Hôtes. Cliquez sur **Voir les détails** pour afficher la fenêtre du message complet.

Messages d'avertissement	**Avertissement pré-mise à jour** Veuillez examiner les points suivants avant d'effectuer la mise à jour. 1. **La version du noyau sur l'hôte est plus ancienne que la version 2.6.32-504.1.3 prise en charge par Security Analytics Si vous cliquez sur Commencer la mise à jour, la version du noyau 2.6.32-504.1.3 sera installée sur l'hôte.** 2. **Après avoir installé la mise à jour 10.6.0.0, les règles de corrélation écrites dans une syntaxe obsolète peuvent provoquer le démarrage du service Concentrator en mode échec. Les règles qui correspondent à la mise en forme stricte ne génèrent pas ce problème.** **Pour plus d'informations, reportez-vous à la rubrique d'aide en ligne de Security Analytics 10.6 « Instructions relatives aux règles et requêtes ».**
Cause	1. Le noyau CentOS sur l'hôte est plus ancien que le noyau pris en charge par la version de mise à jour que vous avez choisie. 2. Si cet hôte correspond à un service Concentrator et qu'il commence à l'état d'échec, il se peut que les règles de corrélation soient écrites en utilisant la syntaxe obsolète. **Note: État actuel** affiche la version actuelle de Security Analytics ou du système d'exploitation de l'hôte avant la mise à jour vers 10.6.

Last Modified: August 10 2016, 9:33AM

Action recommandée	1. Cliquez sur **Commencer la mise à jour** dans la boîte de dialogue d'avertissement pour installer le noyau pris en charge. 2. Vérifiez que vos règles corrélées sont conformes à la mise en forme stricte, comme décrit dans la rubrique Instructions relatives aux règles et requêtes**.**

Avertissements liés à la préparation de la mise à jour

Les conflits de préparation de la mise à jour concernent les problèmes relatifs à votre configuration ou à votre référentiel de mises à jour local qui vous empêchent d'effectuer une mise à jour vers la nouvelle version. Si Security Analytics rencontre :

- Des paramètres de configuration incompatibles, le message Conflit de mise à jour s'affiche. Voir les détails dans la colonne **État**.
- Des problèmes de téléchargement des fichiers de mise à jour de version, le message Erreur de téléchargement. Voir les détails dans la colonne **État**.

Message Conflit	**Échec du téléchargement** Impossible d'effectuer le téléchargement en raison des erreurs suivantes. **Erreur de configuration des référentiels : Impossible de récupérer le référentiel de métadonnées (repomd.xml) pour le référentiel : SA. Vérifiez son chemin d'accès, puis réessayez.**
Cause	Security Analytics ne peut pas se connecter au référentiel Live Update à partir duquel RSA distribue les mises à jour du référentiel RSA Live Update via votre connexion Live.
Action recommandée	Veillez à : 1. Configurer les services en direct. 2. La case à cocher **Se connecter au référentiel Live Update** est activée sous **Administration** > **Système** > **onglet Mises à jour** .

Message Erreur de téléchargement	**Échec du téléchargement** Impossible d'effectuer le téléchargement en raison des erreurs suivantes. **Le référentiel de mise à jour local ne comporte pas de mises à jour valides. Pour obtenir des instructions sur l'obtention de mises à jour valides, reportez-vous à la rubrique Renseigner le référentiel de mises à jour local.**
Cause	Security Analytics n'a pas trouvé la mise à jour de version que vous avez sélectionnée dans votre référentiel de mises à jour local.

Last Modified: August 10 2016, 9:33AM

Action recommandée	Passez en revue les instructions sur la façon de **renseigner le référentiel de mises à jour local** avec la version de mise à jour souhaitée. Si vous ne pouvez pas corriger ce conflit après avoir examiné ces instructions, contactez le Support Clients.

Message Conflit	**Erreur de vérification pré-mise à jour** Impossible de lancer la mise à jour. Corrigez les erreurs suivantes et réessayez. **Échec de la vérification du système de fichiers** **Espace disque insuffisant dans la partition `/var/lib/rabbitmq`.** **L'espace utilisé pour cette partition doit être inférieur à 80 %.** **État actuel : *`Pourcentage utilisé`*%**
Cause	Les messages s'accumulent dans la partition `/var/lib/rabbitmq` .
Action recommandée	Recherchez la raison pour laquelle les messages s'accumulent dans la partition et résolvez le problème. Si vous ne parvenez pas à résoudre ce problème, contactez le Support Clients.

Message Conflit	**Erreur de vérification pré-mise à jour** Impossible de lancer la mise à jour. Corrigez les erreurs suivantes et réessayez. **La version du noyau sur l'hôte est plus récente que la version 2.6.32-504.1.3 prise en charge par Security Analytics** Contacter le Support Clients
Cause	Vous ne pouvez pas effectuer la mise à jour vers la version que vous avez choisie car la version du noyau sur l'hôte est plus récente que la version 2.6.32-504.1.3 prise en charge par Security Analytics pour cette version.
Action recommandée	Contacter le Support Clients pour résoudre le problème.

Message Conflit	**Chemin de mise à jour non pris en charge** Le chemin de mise à jour vers *`version-mise à jour-sélectionnée`* est :

	• *version-range* • *version-range* • . • . • . **Attention :** 1. Si vous exécutez la version 9.8, veuillez contacter le Supports Clients pour obtenir les instructions de mise à jour correspondantes. 2. Si vous exécutez la version 10.3.x, vous devez passer à la version 10.4.1 avant de pouvoir effectuer la mise à jour vers la version 10.6.x.x Reportez-vous au *Guide de mise à niveau de RSA Security Analytics 10.4.1* sur SCOL (https://knowledge.rsasecurity.com/) pour obtenir des instructions détaillées sur la mise à jour entre les versions 10.3.x et 10.4.1. Si vous utilisez Event Stream Analysis version 10.3.x, vous devez migrer vos règles vers la version 10.4.1. **Vous ne pouvez pas accéder aux fichiers RPM de la mise à jour 10.4.1 à partir du référentiel Live Update. Vous devez donc télécharger les fichiers RPM de la mise à jour 10.4.1 à partir de SCOL.**
Cause	La version sur l'hôte n'est pas prise en charge en tant que chemin de mise à jour pour la version de mise à jour de votre choix.
Action recommandée	Mettre à jour l'hôte sur un chemin pris en charge.

Erreurs de mise à jour

Les erreurs de mise à jour sont des erreurs qui arrêtent le processus de mise à jour. Si Security Analytics a rencontré une erreur de mise à jour, il affiche le message Erreur de mise à jour. Voir les détails dans la colonne **État** de la vue Hôtes. Cliquez sur **Voir les détails** pour afficher une des boîtes de dialogue suivantes contenant l'erreur de mise à jour :

Message d'erreur	**Le système n'a pas reçu la réponse attendue**
Cause	Security Analytics ne peut pas identifier l'état de l'hôte car un fichier **/var/lib/puppet/state/agent_catalog_run.lock** existe sur l'hôte. Lorsque l'agent Puppet est exécuté, il crée un fichier de verrouillage intitulé **agent_catalog_run.lock**. De temps en temps, ce fichier de verrouillage est présent sur l'hôte, même si l'agent Puppet n'est pas exécuté.
Action recommandée	Effectuez l'une de ces actions pour résoudre l'erreur :

Last Modified: August 10 2016, 9:33AM

- Supprimez le fichier **/var/lib/puppet/state/agent_catalog_run.lock** de l'hôte.
- Vérifiez l'heure sur les hôtes non liés au serveur Security Analytics et l'hôte Security Analytics Server et assurez-vous qu'ils sont synchronisés.
- Effectuez à nouveau la mise à jour par la suite. En cas d'échec, contactez le Support Clients pour résoudre le problème.

RSA

Résolution des problèmes liés aux messages logs du service de mise à jour 10.6

Cette section contient les messages logs concernant la préparation de la mise à jour, la mise à jour et l'après-mise à jour de la version 10.6.0 de Security Analytics avec une description de chaque message et des instructions sur le mode de réponse à ces messages.

System Management Service (SMS)

Les logs SMS sont publiés dans le fichier `/var/log/install/sms_install.log` sur l'hôte SA.

Version Java

Message	*timestamp host*: SMS_PostInstall: WARN: Java Keystore file /opt/rsa/carlos/keystore is missing
Cause	Le magasin de clés Java est manquant.
Action requise	Vérifiez que la version 1.8 de Java est installée sur l'hôte.
Messages	*timestamp host*: SMS_PostInstall: INFO: Installed Java version is : java version "1.7.0_71" *timestamp host*: WARN: La version Java est ancienne et non compatible avec le serveur SMS actif.
Cause	La version Java installée sur l'hôte n'est pas compatible avec Security Analytics 10.5.1.
Action requise	Vérifiez que la version 1.8 de Java est installée sur l'hôte.

Espace disque

Message	*timestamp host*: SMS_PostInstall: INFO: Free disk space on /opt is *n*GB *timestamp host*: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space *n*GB is less than the recommended minimum disk space of 10GB.
Cause	Espace disque faible ou insuffisant alloué par le service SMS.
Action requise	RSA vous recommande de fournir un minimum de 10 Go d'espace disque pour que le service SMS puisse s'exécuter de façon optimale.

Services

Message	*timestamp host*: INFO RabbitMQ server is not installed.
Cause	Le service RabbitMQ requis n'est **pas** installé.
Action requise	Installez et redémarrez le service RabbitMQ à l'aide des commandes suivantes. yum install rabbitmq-server service rabbitmq-server restart

Message	*timestamp host*: INFO RabbitMQ Server is not running.
Cause	Le service RabbitMQ requis n'est **pas** exécuté.
Action requise	Redémarrez le service RabbitMQ avec les commandes suivantes. service rabbitmq-server restart

Message	*timestamp host*: INFO TokuMX Server is not running.
Cause	Le service TokuMX requis n'est **pas** exécuté.
Action requise	Redémarrez le service TokuMX avec les commandes suivantes. service tokumx-server restart

Message	*timestamp host*: SMS_PostInstall: INFO: Le serveur Puppet ne fonctionne pas.

Cause	Le service `Puppet` requis n'est **pas** exécuté.
Action requise	Redémarrez le service Puppet avec les commandes suivantes. `service puppet-server restart`

Service Log Collector (nwlogcollector)

Les logs du Log Collector sont publiés dans le fichier `/var/log/install/nwlogcollector_install.log` sur l'hôte exécutant le service `nwlogcollector` .

Logs de vérification du Lockbox

Message	`timestamp.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	Le Lockbox du Log Collector n'a pas réussi à s'ouvrir après la mise à jour.
Action requise	Connectez-vous à Security Analytics et redéfinissez la trace du système en réinitialisant la valeur Système stable pour le Lockbox tel que décrit dans la rubrique **Réinitialiser la valeur du système stable** sous la rubrique **Configurer des paramètres de sécurité Lockbox** dans l'aide Security Analytics (https://sadocs.emc.com/fr-fr/088_SA106).

Message	`NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: Lockbox tampering was detected, so it cannot be read.` `NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: Lockbox tampering was detected, so it cannot be read.`
Cause	Le Lockbox du Log Collector est compromis.
Action requise	Connectez-vous à Security Analytics et reconfigurez le Lockbox comme décrit dans la rubrique **Configurer des paramètres de sécurité Lockbox** dans l'aide Security Analytics (https://sadocs.emc.com/fr-fr/088_SA106).

Message	*timestamp* `NwLogCollector_PostInstall: Lockbox Status : Not Found`

Cause	Le Lockbox du Log Collector n'a pas été configuré après la mise à jour.
Action requise	(Facultatif) Si vous utilisez le Lockbox du Log Collector, connectez-vous à Security Analytics et configurez le Lockbox comme décrit dans la rubrique **Configurer des paramètres de sécurité Lockbox** dans l'aide Security Analytics (https://sadocs.emc.com/fr-fr/088_SA106).

Message	`timestamp: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	Vous devez réinitialiser le champ du seuil de valeur stable pour le Lockbox du Log Collector.
Action requise	Connectez-vous à Security Analytics et réinitialisez la valeur Système stable pour le Lockbox tel que décrit dans la rubrique **Réinitialiser la valeur du système stable** sous la rubrique **Configurer des paramètres de sécurité Lockbox** dans l'aide Security Analytics (https://sadocs.emc.com/fr-fr/088_SA106).

Event Stream Analysis (ESA)

Vérification de la préparation de la mise à jour

Les logs de vérification de la préparation de la mise à jour sont publiés dans le fichier `/var/log/esa-rpm-pre-upgrade.log` sur l'hôte exécutant le service ESA.

Message	`Pre_upgrade_alert_count=`*`number-of-alerts`*
Cause	Indique le nombre d'alertes ESA présentes sur l'hôte lorsque vous lancez la mise à jour.
Action requise	Aucun (Information)

Message	`Pre_upgrade_rule_count=`*`number-of-rules`*
Cause	Indique le nombre de règles ESA présentes sur l'hôte lorsque vous lancez la mise à jour.
Action requise	Aucun (Information)

Message	`Pre_upgrade_enrichment_connection_count=`*`number-of-enrichment-sources`*
Cause	Indique le nombre de sources d'enrichissement ESA présentes sur l'hôte lorsque vous lancez la mise à jour.
Action requise	Aucun (Information)

Vérification de l'après-mise à jour

Les logs de vérification de l'après-mise à jour sont publiés dans le fichier `/var/log/esa-rpm-post-upgrade.log` sur l'hôte exécutant le service ESA.

Message	`Post_upgrade_alert_count=`*`number-of-alerts`*
Cause	Indique le nombre d'alertes ESA présentes sur l'hôte après la mise à jour de l'hôte.
Action requise	Aucun (Information)

Message	`Post_upgrade_rule_count=`*`number-of-rules`*
Cause	Indique le nombre de règles ESA présentes sur l'hôte après la mise à jour de l'hôte.
Action requise	Aucun (Information)

Message	`Post_upgrade_enrichment_connection_count=`*`number-of-enrichment-sources`*
Cause	Indique le nombre de sources d'enrichissement ESA présentes sur l'hôte après la mise à jour de l'hôte.
Action requise	Aucun (Information)

Service Reporting Engine

Vérification de la mise à jour

Les logs de mise à jour du Reporting Engine sont publiés dans le fichier `/var/log/re_install.log` sur l'hôte exécutant le service Reporting Engine.

Message	*timestamp* : Available free space in /home/rsasoc/rsa/soc/reporting-engine [*existing-GB*] is less than the required space [*required-GB*]
Cause	Échec de la mise à jour du Reporting Engine car vous ne disposez pas de suffisamment d'espace disque.
Action requise	Libérez de l'espace disque pour disposer de l'espace requis mentionné dans le message log. Reportez-vous à la rubrique Ajouter de l'espace supplémentaire pour les rapports volumineux afin d'obtenir des instructions sur la façon de libérer de l'espace.

Last Modified: August 10 2016, 9:33AM