

RSA Security Analytics

Guide de configuration de Broker et
Concentrator
pour la Version 10.6

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

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 configuration de Broker et Concentrator

• Guide de configuration de Broker et Concentrator	4
◦ Présentation de Broker et Concentrator	5
◦ Configuration de Broker et Concentrator	6
▪ Étape 1. Vérifier la configuration système d'un service	7
▪ Étape 2. Configurer le processus d'agrégation	9
▪ Étape 3. Configurer les services agrégés	11
▪ Étape 4. Démarrer et arrêter l'agrégation	16
◦ Références	19
▪ Agrégation de groupes	20
▪ Vue Configuration des services - onglet Général des Brokers/Concentrators	24
▪ Vue Système de services - Broker	32



Guide de configuration de Broker et Concentrator

Ce guide présente RSA Broker et Concentrator, fournit des instructions précises sur le mode de configuration des services dans votre réseau ainsi que des supports de référence décrivant l'interface utilisateur de configuration du service Broker et Concentrator.



Présentation de Broker et Concentrator

Cette rubrique présente le Broker et les Concentrators dans le réseau Security Analytics.

Contrairement aux Decoders qui capturent des données, les Concentrators et les Brokers agrègent des données capturées ou agrégées par d'autres services. Les Brokers agrègent les données provenant des Concentrators configurés ; les Concentrators agrègent les données provenant des Decoders.



Configuration de Broker et Concentrator

Cette rubrique présente les étapes générales de configuration du Broker et des Concentrators.

L'installation d'un Broker ou d'un Concentrator implique de configurer le service de base, les services d'agrégation et le processus d'agrégation entre un Broker ou un Concentrator et les services d'agrégation.

Liste de contrôle de configuration

La liste de contrôle suivante précise l'ordre des tâches nécessaires à la configuration d'un Broker ou d'un Concentrator ajouté à Security Analytics et dispose d'une habilitation allouée par le serveur de licences local.

Séquence	Tâche générale
1	Les valeurs par défaut de Vérifier la configuration système pour l'hôte et le service sont appropriées.
2	Configurer les paramètres qui régissent l'ensemble du processus d'agrégation .
3	Configurer les services d'agrégation .
4	Démarrer et arrêter l'agrégation .



Étape 1. Vérifier la configuration système d'un service

Cette rubrique propose une procédure pour vérifier la configuration système d'un service Core.


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

System Configuration	
Name	Config Value
Compression	0
Port	50003
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56003
Stat Update Interval	1000
Threads	20

Dans la plupart des cas, les valeurs par défaut pour la compression, l'intervalle de mise à jour des statistiques et le nombre de threads dans le pool de threads sont configurées de façon à optimiser les performances système.

Procédure

Pour modifier les paramètres de configuration système pour un Broker ou un Concentrator :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services**, sélectionnez un Broker ou un Concentrator, et dans la colonne Actions, cliquez sur  > **Vue > Config**.

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

The screenshot displays the configuration page for the 'Broker - Broker' service. The interface is organized into three main panels:

- Aggregate Services:** A table with columns: Address, Port, Rate, Max, Behind, Collection, Status.
- System Configuration:** A table with columns: Name, Config Value.

Name	Config Value
Compression	0
Port	50003
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56003
Stat Update Interval	1000
Threads	20
- Aggregation Configuration:** A table with columns: Name, Config Value.

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

An 'Apply' button is located at the bottom center of the configuration area. The bottom status bar shows 'admin | English (United States) | GMT+00:00' and 'Send Us Feedback | 10.6.0.0.21975-1'.

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



Étape 2. Configurer le processus d'agrégation


Cette rubrique décrit la procédure permettant de configurer le comportement d'agrégation de Broker ou Concentrator.

La configuration du processus d'agrégation comprend la configuration des éléments suivants :

- Démarrage automatique de l'agrégation
- Paramètres de temps et de performance tels que le nombre de sessions par lot d'agrégation et le temps entre les lots
- Nombre maximum de fichiers méta et de fichiers de session ouverts
- Temps des tentatives de redémarrage, de reconnexion et de mise hors ligne dans le cas où le service d'agrégation ne répondrait pas

Procédure

Pour configurer le processus d'agrégation de Broker ou Concentrator :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services**, sélectionnez un Broker ou un Concentrator, puis sélectionnez  > **Vue > Configuration**.
La vue Configuration des services, qui comprend la section Configuration de l'agrégation, s'affiche.

The screenshot displays the RSA Security Analytics configuration page for 'Aggregate Services'. The interface includes a top navigation bar with various system and security options. The main configuration area is split into three panels:

- Aggregate Services:** A table with columns: Address, Port, Rate, Max, Behind, Collection, Status.
- System Configuration:** A table with columns: Name, Config Value.

Name	Config Value
Compression	0
Port	50003
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56003
Stat Update Interval	1000
Threads	20
- Aggregation Configuration:** A table with columns: Name, Config Value.

Name	Config Value
Aggregate Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

An 'Apply' button is located at the bottom center of the configuration area. The footer shows the user 'admin', language 'English (United States)', and time zone 'GMT+00:00'. The version number '10.6.0.0.21975-1' is also present.

3. (Facultatif) Sélectionnez **Démarrage automatique de l'agrégation** pour activer le démarrage automatique de l'agrégation quand un service est en ligne.
4. (Facultatif) Modifiez l'un des paramètres d'agrégation : les heures à partir desquelles l'agrégation doit commencer, les millisecondes entre les cycles d'agrégation et le nombre maximal de sessions par cycle d'agrégation.
5. (Facultatif) Modifiez l'un des paramètres du service Heartbeat, qui indique la durée de la première tentative de reconnexion à un service après une erreur, la prochaine tentative de reconnexion, et la prise du service hors ligne après l'échec de reconnexion.
6. Lorsque la modification des paramètres est terminée, cliquez sur **Appliquer**. Les paramètres prennent effet immédiatement.



Étape 3. Configurer les services agrégés


Cette rubrique présente les tâches relatives à l'agrégation de données sur les Brokers et Concentrators. Pour plus d'informations sur la création d'une agrégation de groupe, voir [Configurer l'agrégation de groupes](#).

La configuration des services agrégés (dont les données sont consommées et agrégées) comprend :

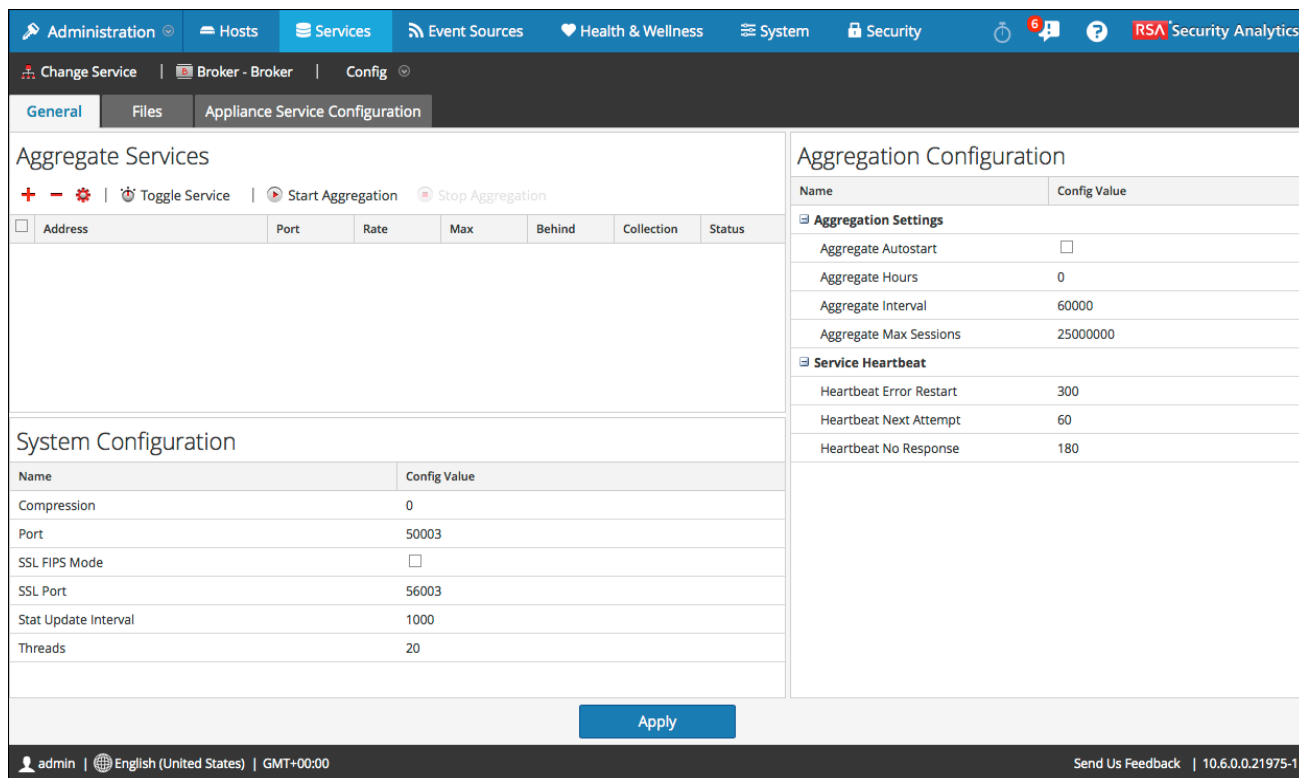
- l'ajout, la modification et la suppression de Concentrators et de Decoders en tant que services agrégés
- Basculement d'un service agrégé en ligne et hors ligne

Procédures

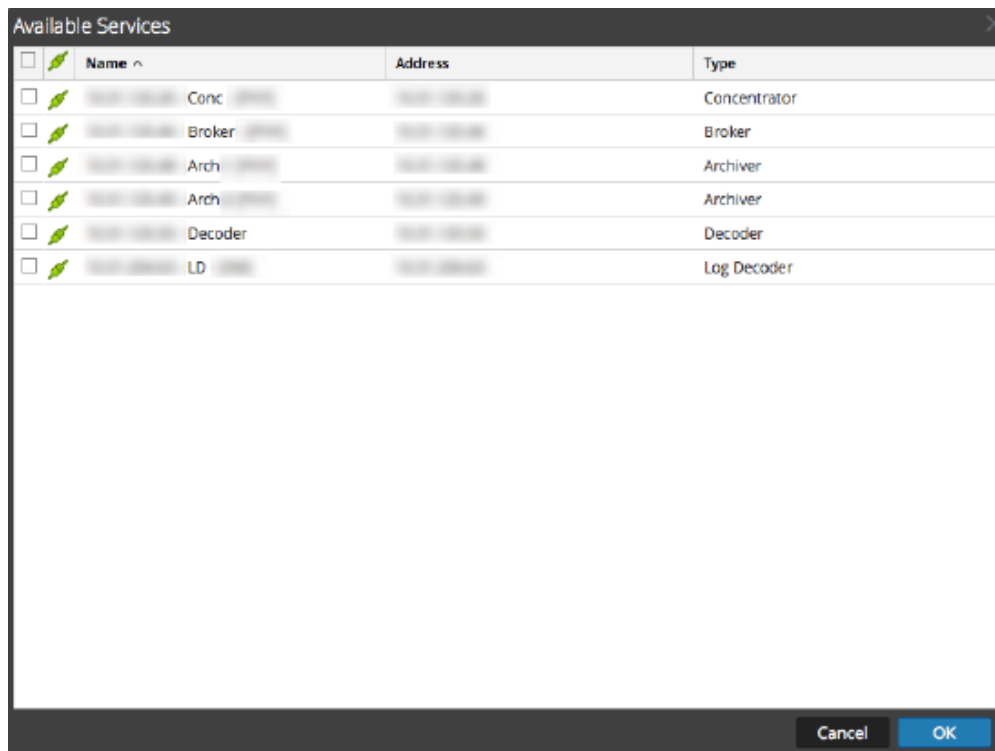
Ajouter des services agrégés à un Broker ou Concentrator

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services d'administration**, sélectionnez un Broker ou un Concentrator, puis sélectionnez  > **Vue > Configuration**.

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



3. Cliquez sur **+** dans la barre d'outils **Services agrégés**. La boîte de dialogue Services disponibles s'affiche.



- Sélectionnez un ou plusieurs services à ajouter, puis cliquez sur **OK**. Les services ajoutés sont répertoriés dans la liste Services agrégés.

Aggregate Services


+ - ⚙️
🔄 Toggle Service
▶ Start Aggregation
⏹ Stop Aggregation

	Address	Port	Rate	Max	Behind	Collection	Status
<input checked="" type="checkbox"/>		50005					

- Pour enregistrer les modifications, cliquez sur **Appliquer**.

Supprimer des services agrégés sur un Broker ou Concentrator


Note: Cette option ne s'applique qu'aux services hors ligne. Si le service agrégé est en ligne, vous devez d'abord le mettre hors ligne.

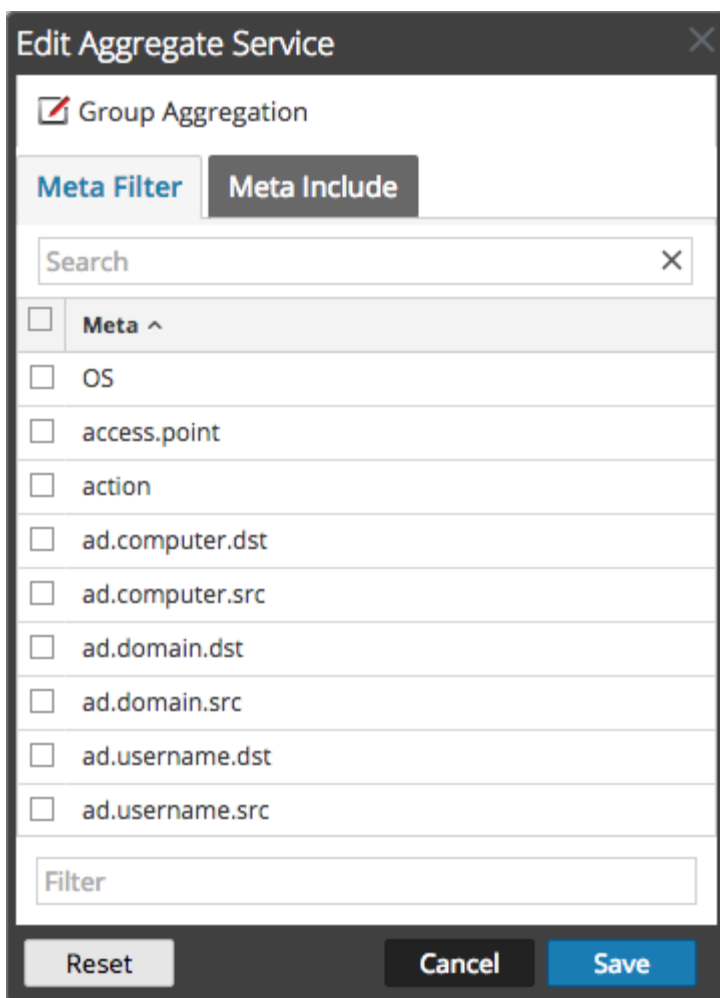
- Dans la grille **Services agrégés**, sélectionnez un service ou plus.
- Cliquez sur  dans la barre d'outils. Le service est supprimé de la grille Services agrégés.
- Pour enregistrer la modification, cliquez sur **Appliquer**.

Modifier les services agrégés sur un Concentrator

Note: Cette option ne s'applique qu'aux services hors ligne. Si le service agrégé est en ligne, vous devez d'abord le mettre hors ligne.

Vous pouvez limiter les données consommées à partir d'un service agrégé à l'aide de champs de métadonnées et de filtres. Pour procéder à la configuration :

- Dans la grille **Services agrégés**, sélectionnez un service ou plus.
- Cliquez sur  dans la barre d'outils.
 - Si le service a été ajouté sur une instance différente de Security Analytics, vous devez l'ajouter à cette instance de Security Analytics pour le modifier. Une boîte de dialogue d'avertissement permet d'ajouter le service. Si vous cliquez sur **Oui**, la boîte de dialogue Ajouter un service s'affiche.
 - Si le service est en ligne, une boîte de dialogue indique que le service doit être hors ligne et vous demande de confirmer que vous souhaitez continuer. Si vous cliquez sur **Oui**, Security Analytics met le service hors ligne et la boîte de dialogue Modifier le service agrégé s'affiche.
 - Si le service est hors ligne, la boîte de dialogue Modifier le service agrégé s'affiche avec les propriétés modifiables pour un service agrégé sur un Concentrator.



3. Cliquez sur un type de métadonnées sous l'onglet **Inclure des métadonnées** pour sélectionner le type de métadonnées pour le Concentrator afin d'effectuer la consommation à partir de ce service.
4. Pour spécifier une règle visant à filtrer les données que le Concentrator consomme à partir de ce service, composez une règle sous l'onglet **Filtrer les métadonnées**.
5. Cliquez sur **Fermer**.
La boîte de dialogue Modifier le service agrégé se ferme et les modifications sont affichées dans la grille Services agrégés. Dans cet exemple, deux métadonnées ont été sélectionnées sous l'onglet Inclure des métadonnées. Lorsque vous cliquez sur

l'icône d'informations dans le champ Inclure des métadonnées, elle affiche les sélections.

The screenshot shows the 'Aggregate Services' interface. At the top, there are several action buttons: a plus sign (+), a minus sign (-), an edit icon, 'Edit Service', a toggle icon, 'Toggle Service', a play icon, 'Start Aggregation', and a stop icon, 'Stop Aggregation'. Below these is a table with the following columns: 'Address', 'Port', 'Rate', 'Max', 'Behind', 'Meta Field', 'Filter', 'Meta Inclu', 'Grouped', and 'Status'. The first row of the table is highlighted and contains a checkmark in the first column, a partially visible address, '50...', '0', '0', '0', and '2' in the 'Meta Inclu' column. A tooltip is displayed over the '2' in the 'Meta Inclu' column, showing 'Meta Include: action ad.computer.src'.

6. Pour enregistrer les modifications, cliquez sur **Appliquer**.

Basculer le service

Lorsque l'agrégation de données commence, les Brokers et Concentrators consomment des données de services agrégés en ligne. Lors de l'ajout sur un Broker ou Concentrator pour la première fois, les services agrégés sont hors ligne. Pour basculer un service entre les modes en ligne et hors ligne :

1. Sélectionnez un service dans la grille **Services agrégés**.

2. Cliquez sur  **Toggle Service** .
L'état est modifié.



Étape 4. Démarrer et arrêter l'agrégation

Cette rubrique présente la procédure permettant de démarrer et d'arrêter l'agrégation sur le Broker et les Concentrators.


Lorsqu'un Broker ou un Concentrator démarre, il commence automatiquement à agréger des données si l'option **Démarrage automatique de l'agrégation** est activée. Lorsque le démarrage automatique n'est pas activé, vous pouvez démarrer et arrêter l'agrégation de données manuellement.

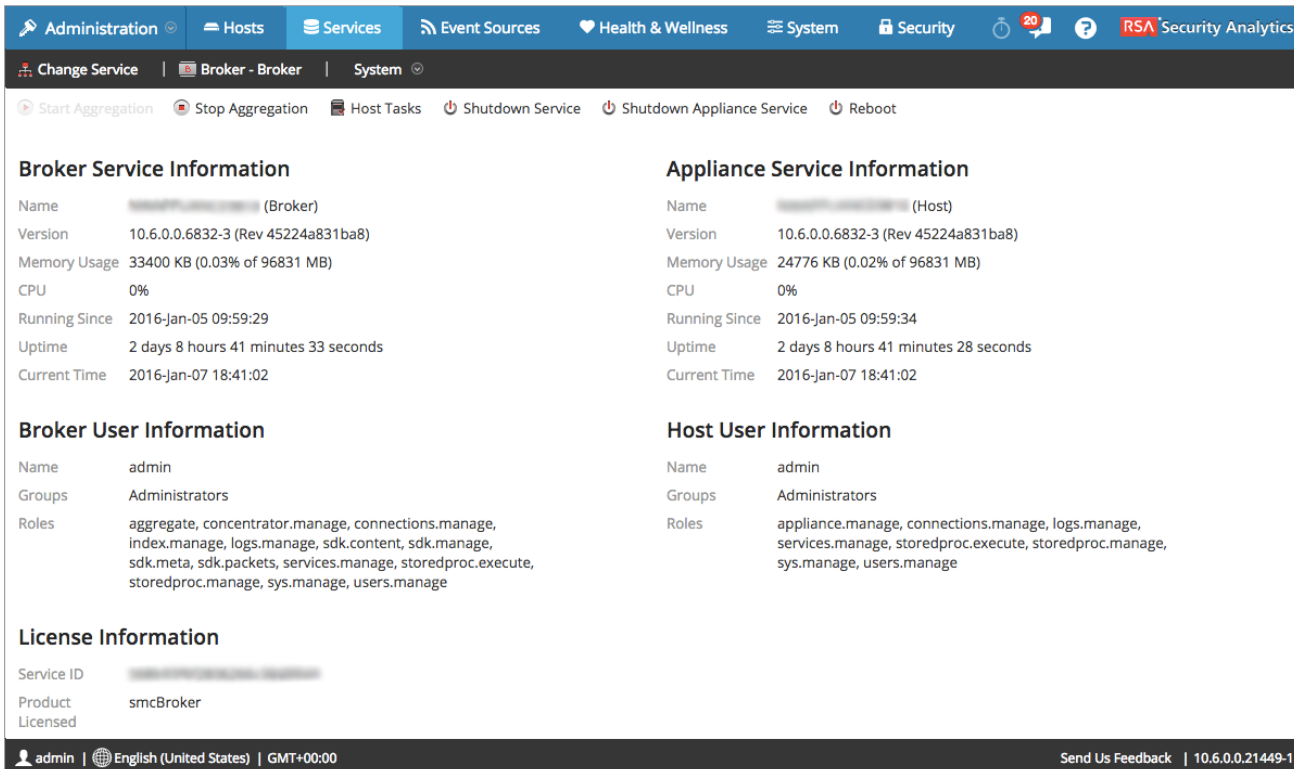
Note: Les paramètres de configuration de l'agrégation de la [vue Configuration des services](#) d'un Broker ou d'un Concentrator déterminent si le Démarrage automatique de l'agrégation est activé, ainsi que la taille d'un cycle d'agrégation et le temps entre les cycles.

Procédures

Démarrer et arrêter l'agrégation des données dans la vue Système de services



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

2. Dans la vue **Services d'administration**, sélectionnez un Broker ou un Concentrator, puis sélectionnez  > **Vue > Système**.




3. Pour arrêter un Broker ou un Concentrator qui capture des données, cliquez sur **Arrêter l'agrégation** dans la barre d'outils. Le service cesse l'agrégation des données et l'option **Arrêter l'agrégation** de la barre d'outils n'est pas disponible. L'option **Démarrer l'agrégation** devient active.
4. Si vous voulez que le service lance l'agrégation des données à nouveau, cliquez sur **Démarrer l'agrégation**. Vous pouvez maintenant étudier les données saisies dans le module d'enquête.

Démarrer et arrêter l'agrégation dans la vue Configuration des services

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue **Services admin**, sélectionnez un Broker ou un Concentrator, puis sélectionnez  > **Vue > Configuration**. La vue Configuration des services, qui comprend la section Services agrégés, s'affiche.
3. Pour lancer l'agrégation sur le Broker ou Concentrator sélectionné, cliquez sur  **Start Aggregation** dans la barre d'outils **Services agrégés**. Lorsque l'agrégation commence, l'état de tous les services agrégés en ligne est remplacé par **consommation**. Le bouton

Démarrer l'agrégation est désactivé et le bouton Arrêter l'agrégation est activé.

<input checked="" type="checkbox"/>	Address	Port	Rate	Max	Behind	Collection	Status
<input checked="" type="checkbox"/>	[blurred]	50002					

4. Pour arrêter l'agrégation, cliquez sur  Stop Aggregation dans la barre d'outils **Services agrégés**. Lorsque l'agrégation s'arrête, l'état consommation de tous les services agrégés est remplacé par **en ligne**. Le bouton Arrêter l'agrégation est indisponible et le bouton Démarrer l'agrégation est disponible.



Références

Cette rubrique rassemble des références qui décrivent l'interface utilisateur de configuration des Archiver et des Concentrator dans **Security Analytics**.

Utilisez cette section si vous recherchez les descriptions des Broker et des Concentrator ainsi que les définitions des fonctions de l'interface utilisateur. Pour plus d'informations sur la vue Explorer les services, reportez-vous à la rubrique [Vue Explorer les services](#).

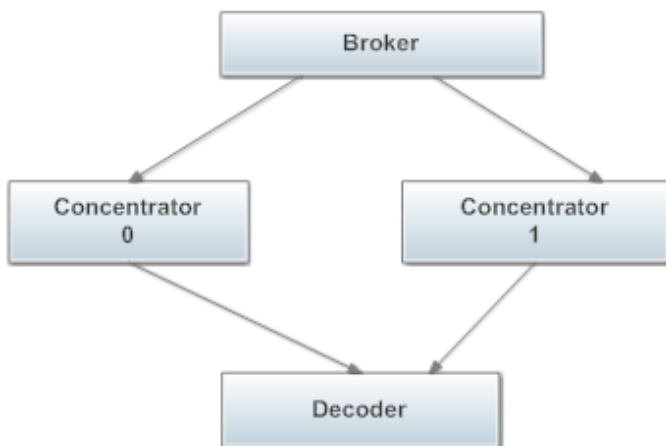


Agrégation de groupes

Cette rubrique explique comment les Concentrators peuvent être regroupés en clusters qui partagent la tâche d'agrégation entre plusieurs hôtes.

Note: L'agrégation en clusters ne s'applique pas aux Brokers.

L'agrégation en clusters (également connue sous le nom d'agrégation en « gang »), permet à plusieurs concentrators d'effectuer une agrégation efficace à partir d'un seul Decoder. Certains concentrators peuvent être regroupés pour former un gang d'agrégation. Les concentrators contenus dans le gang divisent toutes les sessions entre elles. L'agrégation de groupes ou l'agrégation en clusters permet à plusieurs concentrators d'effectuer une agrégation efficace à partir d'un seul Decoder dans le type d'architecture illustré ci-dessous :



Exemple

Certains concentrators peuvent être regroupés pour former une agrégation en clusters. Les concentrators du cluster partagent toutes les sessions entre eux.

Dans un gang de deux concentrators, les sessions agrégées par chaque concentrator pourrait ressembler à ceci :

Concentrator 0	Concentrator 1
1 - 9 999	10 000 - 19 999
20 000 - 29 999	30 000 - 39 999

Concentrator 0	Concentrator 1
40 000 - 49 999	50 000 - 59 999

Paramètres de l'agrégation de groupes

Vous pouvez configurer le cluster dans le cadre de la configuration des services Concentrator et Archiver sous la vue Configuration des services de Security Analytics. Ce tableau répertorie les paramètres que vous pouvez également configurer dans la vue Explorer les services.

Paramètre	Où le paramètre est défini	Description
Sessions d'agrégation maximum	<code>/concentrator/config/aggregate.sessions.max</code>	Nombre de sessions qu'un concentrator reçoit d'un autre concentrator à un moment donné. Lorsqu'un Concentrator fait partie d'un gang, il est également utilisé pour déterminer la façon dont les sessions des Decoders seront réparties au sein du gang. Les sessions des Decoders sont divisées en fragments de taille <code>aggregate.sessions.max</code> , puis les fragments sont uniformément répartis entre les Concentrators. Par exemple, <code>aggregate.sessions.max</code> correspond à 10 000, puis les sessions 1-9 999 passent aux premiers Concentrator et sessions 10 000-19 999 passent au deuxième concentrator. Tous les concentrators du gang doivent utiliser la même valeur pour <code>aggregate.sessions.max</code> .
conGangName	<code>/concentrator/devices/<device>/config/options,gang=<gang name></code>	Le nom du gang est utilisé pour déterminer l'appartenance à un gang particulier. Il peut y avoir un nombre illimité de gangs agrégés à partir d'un Decoder. Le paramètre gang est tout simplement un mécanisme qui permet au decoder d'identifier les concentrators qui travaillent ensemble. Tous les membres du gang doivent avoir le même nom de gang. Si le paramètre nom du gang n'est pas défini, l'agrégation des gangs sera désactivée. Le nom du gang peut être un identificateur de chaîne.
Taille du gang	<code>/concentrator/devices/<device>/config/options,gangSize=<number of devices in gang></code>	Ce paramètre définit la taille du gang. Tous les Concentrators doivent avoir la même valeur pour la taille du gang. La taille du gang est illimitée.
ID de membre de gang	<code>/concentrator/devices/<device>/config/options,gangMember=<id number of concentrator in gang></code>	Ce paramètre définit la position du concentrator dans le groupe. Pour les gangs de taille N, les ID des membres de gang de 0 à N-1 doivent être définis sur chacun des membres du gang. Par exemple, si la taille du gang est 2, un membre obtient l'ID de membre

Paramètre	Où le paramètre est défini	Description
		du gang 0 et l'autre reçoit l'ID de membre 1. Si la taille du gang est 3, alors les membres se voient attribuer les ID 0, 1 et 2.
Mode d'appartenance au gang	<code>/concentrator/ devices/<device>/config/ options, gangMembership=(new replace)</code>	Ce paramètre détermine comment ce Concentrator est capturé lorsque l'agrégation est démarrée pour la première fois. Le comportement par défaut est <code>replace</code> . Cela signifie que lorsque ce Concentrator commence l'agrégation, il est destiné à remplacer un membre d'un gang existant, ou tous les membres du gang sont en cours d'initialisation dans le même temps. Cela signifie que le Concentrator commence l'agrégation à partir de la session la plus ancienne disponible sur l'hôte à partir duquel l'agrégation est effectuée. Si ce paramètre est défini sur <code>new</code> , cela signifie que ce Concentrator est ajouté en tant que nouveau membre d'un groupe existant. Ce Concentrator ne tentera pas d'agréger toutes les sessions existantes du service. Les autres membres du groupe ont déjà agrégé toutes les sessions sur le service. Ce Concentrator n'agrégera que les nouvelles sessions telles qu'elles apparaissent sur le service.

Exemples

Le tableau suivant affiche un exemple de paramètres d'un gang composé de deux membres avec l'ID de gang `foo`.

Paramètre	Concentrator 0	Concentrator 1
<code>aggregate.max.sessions</code>	10 000	10 000
<code>device options</code>	<code>gang=foo gangSize=2 gangMember=0</code>	<code>gang=foo gangSize=2 gangMember=1</code>

Le tableau suivant affiche un exemple de paramètres d'un gang composé de trois membres avec l'ID de gang `baz`.

Paramètre	Concentrator 0	Concentrator 1
<code>aggregate.max.sessions</code>	10 000	10 000
<code>device options</code>	<code>gang=baz gangSize=3 gangMember=0</code>	<code>gang=baz gangSize=3 gangMember=2</code>

Taille du cluster

Lorsque la division des sessions d'un cluster doit changer, que ce soit pour augmenter ou réduire la taille du cluster, vous devez basculer à l'état hors ligne. À l'état hors ligne, tous les membres doivent être mis à jour pour avoir le même paramètre `gangSize`. L'hôte de remplacement agrège uniquement sa fraction de sessions. De la même façon, il est possible de réinitialiser et de réagrèger les données de tout membre du cluster à n'importe quel moment sans que cela ait d'impact sur les autres membres du cluster.

Membre de cluster

Un membre de cluster peut être remplacé à tout moment en définissant le paramètre `gangMember` de l'hôte de remplacement pour être identique au paramètre `gangMember` de l'ancien hôte. L'hôte de remplacement agrège uniquement sa fraction de sessions. De la même façon, il est possible de réinitialiser et de réagrèger les données de tout membre du cluster à n'importe quel moment sans que cela ait d'impact sur les autres membres du cluster.



Vue Configuration des services - onglet Général des Brokers/Concentrators

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

L'onglet Général de la vue Configuration des services correspondant à un Broker ou un Concentrator permet de gérer la configuration basique d'un service, de définir le service agrégé mais également de paramétrer le processus d'agrégation entre un Broker ou un Concentrator et le service agrégé.

La configuration du service agrégé (dont les données sont consommées et agrégées) englobe les tâches suivantes :

- Ajout, modification et suppression de Concentrators et de Brokers en tant que services agrégés
- Basculement d'un service agrégé en ligne et hors ligne
- Surveillance des statistiques relatives aux services agrégés
- Démarrage et arrêt de l'agrégation

La configuration du processus d'agrégation comprend la configuration des éléments suivants :

- Démarrage automatique de l'agrégation
- Paramètres de temps et de performance tels que le nombre de sessions par lot d'agrégation et le temps entre les lots
- Temps des tentatives de redémarrage, de reconnexion et de mise hors ligne dans le cas où le service d'agrégation ne répondrait pas

Voici une capture d'écran de l'onglet Général d'un Concentrator.

The screenshot shows the RSA Security Analytics interface for a Concentrator configuration page. The top navigation bar includes Administration, Hosts, Services, Event Sources, Health & Wellness, System, and Security. The main content area is divided into three sections: Aggregate Services, System Configuration, and Aggregation Configuration.

Aggregate Services

Buttons: +, -, Edit Service, Toggle Service, Start Aggregation, Stop Aggregation

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
	50002							no	

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56005
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Apply

admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.6.0.0.22031-1

Voici une capture d'écran de l'onglet Général d'un Broker.

The screenshot shows the RSA Security Analytics interface for a Broker configuration page. The top navigation bar includes Administration, Hosts, Services, Event Sources, Health & Wellness, System, and Security. The main content area is divided into three sections: Aggregate Services, System Configuration, and Aggregation Configuration.

Aggregate Services

Buttons: +, -, Toggle Service, Start Aggregation, Stop Aggregation

Address	Port	Rate	Max	Behind	Collection	Status

System Configuration

Name	Config Value
Compression	0
Port	50003
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56003
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	25000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Apply

admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.6.0.0.21975-1








Caractéristiques

L'onglet Général correspondant aux Brokers et aux Concentrators inclut trois sections principales :






- Services agrégés
- Configuration système
- Configuration de l'agrégation



Services agrégés

La section Services agrégés permet de lancer et d'arrêter l'agrégation, mais également d'ajouter, de modifier, de supprimer et de basculer un service agrégé. Voici une capture d'écran de la section Services agrégés d'un Concentrator.

Aggregate Services										
    Edit Service  Toggle Service  Start Aggregation  Stop Aggregation										
<input type="checkbox"/>	Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
<input type="checkbox"/>	██████████	50002	5631	115511	43960304				no	consuming
<input type="checkbox"/>	██████████	50004	15317	45160	144258				no	consuming

La barre d'outils de la section Services agrégés comprend les options suivantes.

Option	Description
	Ouvre une boîte de dialogue permettant d'ajouter un Concentrator, un Decoder ou un Log Decoder en tant que service agrégé.
	Supprime le service agrégé sélectionné.
	Option réservée aux Concentrators. Ouvre une boîte de dialogue permettant de modifier les valeurs Champs de métadonnées et Filtre du Concentrator.
 Edit Service	Vous permet de saisir les informations d'identification d'administrateur du service agrégé sélectionné pour qu'il puisse communiquer avec le Broker ou le Concentrator.
 Start Aggregation	Lorsque l'agrégation a été interrompue ou n'a pas encore démarré, cette option lance l'agrégation de données du service en ligne figurant dans la grille en appliquant les règles définies pour ce service.

Option	Description
 Stop Aggregation	Lorsque l'agrégation est en cours, interrompt l'opération sur le Broker ou le Concentrator. Cela arrête tous les services et vide l'index, opération qui peut prendre plusieurs minutes. Il faut absolument arrêter les services agrégés afin de réaliser certaines procédures administratives.
 Toggle Service	Permet de modifier l'état du service pour activer le mode hors ligne ou en ligne. Seules les données provenant d'un service en ligne sont consommées lors de l'agrégation.

La grille de la section Services agrégés inclut les colonnes suivantes.

Colonne	Description
Adresse	Adresse du service.
Port	Port d'écoute du service. Les ports par défaut sont les suivants : <ul style="list-style-type: none"> • 50001 pour les Log Collectors • 50002 pour les Log Decoders • 50003 pour les Brokers • 50004 pour les Decoders • 50005 pour les Concentrators • 50007 pour les autres services
Vitesse	Nombre d'objets de métadonnées écrits dans la base de données chaque seconde. Les valeurs sont des échantillons moyens de transfert sur une courte période (10 secondes). Au terme de la capture, cette vitesse revient à 0 .
Max.	Nombre maximal d'objets de métadonnées écrits chaque seconde dans la base de données depuis le démarrage de la capture. Les valeurs sont des échantillons moyens de transfert sur une courte période (10 secondes). Au terme de la capture, le paramètre Max. affiche toujours la valeur maximale lors de l'opération.
Derrière	Répertorie le nombre de sessions du service qui doivent être agrégées.
Collecte	Réservée aux Brokers. Indique la collection sélectionnée lorsque le service Analyst Workbench a été ajouté à la section Services agrégés.
Champs de métadonnées	Réservée aux Concentrators. Répertorie les types de métadonnées consommées par le service agrégé.
Filtre	Réservée aux Concentrators. Répertorie les filtres éventuellement appliqués aux métadonnées consommées par le service agrégé.
Inclure des métadonnées	Réservée aux Concentrators. Indique le nombre de types de méta inclus dans le service agrégé.
Groupé(e)	Précise si le service agrégé fait partie d'un groupe.
État	Affiche l'état actuel du service :

Colonne	Description
	<ul style="list-style-type: none"> • en ligne = peut fournir des données en vue de leur utilisation par le Broker ou le Concentrator • hors ligne = ne peut pas fournir de données en vue de leur utilisation par le Broker ou le Concentrator • consommation = fournit des données en vue de leur utilisation par le Broker ou le Concentrator

Configuration système

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

System Configuration	
Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56005
Stat Update Interval	1000
Threads	20

La Configuration système dispose des paramètres suivants.

Paramètre	Description
Compression	Le nombre minimum d'octets devant être transmis par réponse avant la compression. Le paramètre 0 désactive la compression. La valeur par défaut est 0 . La modification d'une valeur prend effet immédiatement pour toutes les connexions suivantes.
Port	Port d'écoute du service. Les ports par défaut sont les suivants : <ul style="list-style-type: none"> • 50001 pour les Log Collectors • 50002 pour les Log Decoders • 50003 pour les Brokers • 50004 pour les Decoders • 50005 pour les Concentrators • 50007 pour les autres services

Paramètre	Description
Mode FIPS SSL	En cas d'activation (on), la sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL. La valeur par défaut est off .
Port SSL	Numéro de port SSL.
Intervalle de mise à jour des statistiques	Nombre de millisecondes entre les mises à jour statistiques sur le système. Les petites valeurs engendrent des mises à jour plus fréquentes et peuvent ralentir d'autres processus. La valeur par défaut est 1000 . La modification de la valeur prend effet immédiatement.
Threads	Nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. Le paramètre 0 laisse le système décider. La valeur par défaut est 15 . Les modifications prendront effet au redémarrage du service.

Configuration de l'agrégation

La section Configuration de l'agrégation fournit des paramètres qui déterminent différents aspects du processus d'agrégation. Les modifications apportées sont enregistrées lorsque vous cliquez sur **Appliquer**, mais les paramètres ne prennent pas tous effet immédiatement. Vous trouverez plus de détails dans les tableaux Paramètres d'agrégation et Heartbeat du service.

Aggregation Configuration	
Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Paramètres d'agrégation

Paramètre	Description
Démarrage automatique de l'agrégation	Option permettant de lancer automatiquement l'agrégation chaque fois que le Broker ou le Concentrator démarre. Une coche indique que cette option est activée. Sa modification prend effet immédiatement.
Heures d'agrégation	<p>Pour chaque service, nombre d'heures écoulées que le Concentrator ou le Broker tente de restaurer au début de l'agrégation. Cette modification prend effet immédiatement.</p> <ul style="list-style-type: none"> • Si la valeur 0 est définie, l'agrégation de chaque service débute là où elle s'était arrêtée, quel que soit le nombre d'heures écoulées. • Si la valeur est un entier positif, le Concentrator ou le Broker consomme uniquement les sessions antérieures correspondant à ce nombre d'heures. <p>Par exemple, si la session active d'un service est espacée de plus de 10 heures de la dernière session, voici ce qui se passe avec selon la valeur associée au paramètre Heures d'agrégation :</p> <ul style="list-style-type: none"> • Si la valeur 12 est définie, le Concentrator ou le Broker commence à consommer des sessions là où il s'était interrompu. • Si la valeur 4 est définie, toutes les sessions comprises dans la plage de 5 à 10 heures écoulées sont ignorées, et le Concentrator ou le Broker commence à consommer la session qui a démarré 4 heures plus tôt.
Intervalle d'agrégation	Nombre de millisecondes séparant deux lots d'agrégation de service. Tous les services gérés par le Broker ou le Concentrator nécessitent des lots supplémentaires pour que les sessions et les métadonnées soient agrégées. Si un Broker ou un Concentrator consomme toujours le précédent lot de données, il ne peut pas en demander un autre avant la fin de l'opération. La modification prend effet immédiatement.
Sessions d'agrégation maximum	Nombre maximal de sessions que le Broker ou le Concentrator demande dans un lot spécifique d'agrégation de données. La modification prend effet au redémarrage.

Heartbeat du service

Lorsqu'ils communiquent avec chacun des services agrégés, les Brokers et les Concentrators gèrent leur heartbeat. Ces paramètres précisent l'heure de la première tentative de reconnexion à un service après une erreur, la tentative de reconnexion suivante, ainsi que la mise hors ligne du service après l'échec de reconnexion.

Paramètre	Description
Redémarrage après erreur Heartbeat	Après la détection d'une erreur Heartbeat sur un service agrégé, ce paramètre spécifie le délai (en secondes) que doit respecter un Broker ou un Concentrator avant de tenter de se reconnecter au service.
Nouvelle tentative Heartbeat	Après l'échec d'une tentative de reconnexion à un service agrégé, ce paramètre spécifie le délai (en secondes) que doit respecter un Broker ou un Concentrator avant de tenter de se reconnecter au service. La modification prend effet immédiatement.
Pas de réponse Heartbeat	Après l'échec de reconnexion à un service qui ne répond pas, ce paramètre spécifie le délai (en secondes) que doit respecter un Broker ou un Concentrator avant de mettre le service hors ligne. La modification prend effet immédiatement.

Lorsque vous modifiez des paramètres sous l'onglet Général, il faut cliquer sur **Appliquer** pour enregistrer les modifications.





Vue Système de services - Broker

Cette rubrique décrit les fonctions de la vue Système de services qui sont spécifiques aux Brokers et Concentrators.

Bien que les informations affichées dans la vue Système des services soient identiques pour tous les types de services Core, plusieurs options dans la barre d'outils ne sont pertinentes que pour les Brokers et Concentrators.

Vous pouvez accéder à cette vue de la manière suivante :

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

Administration | **Hosts** | **Services** | **Event Sources** | **Health & Wellness** | **System** | **Security** | **20** | **?** | **RSA Security Analytics**

Change Service | **Broker - Broker** | **System**

Start Aggregation | **Stop Aggregation** | **Host Tasks** | **Shutdown Service** | **Shutdown Appliance Service** | **Reboot**

Broker Service Information		Appliance Service Information	
Name	(Broker)	Name	(Host)
Version	10.6.0.0.6832-3 (Rev 45224a831ba8)	Version	10.6.0.0.6832-3 (Rev 45224a831ba8)
Memory Usage	33400 KB (0.03% of 96831 MB)	Memory Usage	24776 KB (0.02% of 96831 MB)
CPU	0%	CPU	0%
Running Since	2016-Jan-05 09:59:29	Running Since	2016-Jan-05 09:59:34
Uptime	2 days 8 hours 41 minutes 33 seconds	Uptime	2 days 8 hours 41 minutes 28 seconds
Current Time	2016-Jan-07 18:41:02	Current Time	2016-Jan-07 18:41:02

Broker User Information		Host User Information	
Name	admin	Name	admin
Groups	Administrators	Groups	Administrators
Roles	aggregate, concentrator.manage, connections.manage, index.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

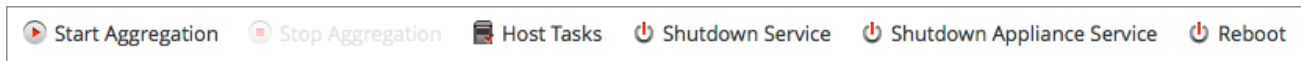
License Information

Service ID	
Product	smcBroker
Licensed	

admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.6.0.0.21449-1

Options de la barre d'outils

La figure suivante est un exemple de barre d'outils pour un service Broker ou Concentrator.



Les options Tâches de l'hôte, Arrêt du service, Arrêt du service de l'appliance ou (Arrêter l'appliance) et Redémarrer sont communes à l'ensemble des services et sont décrites dans la [vue Système des services](#).

Ce tableau décrit les options de la barre d'outils qui ne concernent qu'un Concentrator ou un Broker. Les deux boutons ne sont pas disponibles tant que les services d'agrégation sont configurés et qu'ils consomment des données.

Action	Description
Démarrer l'agrégation	Démarre l'agrégation des données consommées sur un Concentrator ou un Decoder configurée comme un service d'agrégation pour le Broker ou le Concentrator sélectionné. Le bouton Démarrer l'agrégation est disponible uniquement lorsque les services d'agrégation sont configurés et qu'ils consomment des données.
Arrêter l'agrégation	Met fin à l'agrégation des données consommées sur un Concentrator ou un Decoder configurée comme un service d'agrégation pour le Broker ou le Concentrator sélectionné. Le bouton Arrêter l'agrégation est disponible uniquement lorsque l'agrégation se produit.