

RSA

NETWITNESS®
SUITE



Guide de configuration de Broker et Concentrator

pour la version 11.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

février 2018

Sommaire

| | |
|--|-----------|
| Notions de base de Broker et Concentrator | 5 |
| Étape 1. Vérifier la configuration système d'un service | 6 |
| Configuration de Broker et Concentrator | 9 |
| Liste de contrôle de configuration de base | 9 |
| Étape 1. Vérifier la configuration système d'un service | 10 |
| Étape 2. Configurer le processus d'agrégation | 12 |
| Étape 3. Configurer les services agrégés | 15 |
| Ajouter des services agrégés à un Broker ou Concentrator | 15 |
| Supprimer des services agrégés sur un Broker ou Concentrator | 17 |
| Modifier les services agrégés sur un Concentrator | 18 |
| Changer de service | 20 |
| Étape 4. Démarrer et arrêter l'agrégation | 21 |
| Démarrer et arrêter l'agrégation des données dans la vue Système de services | 21 |
| Démarrer et arrêter l'agrégation dans la vue Configuration des services | 23 |
| Références de configuration de Broker et Concentrator | 26 |
| Vue Configuration des services - onglet Général des Brokers/Concentrators | 27 |
| Que voulez-vous faire ? | 27 |
| Rubriques connexes | 28 |
| Onglet Général | 28 |
| Section Services agrégés | 29 |
| Section Configuration de l'agrégation | 33 |
| Vue Système de services - Broker ou Concentrator | 36 |
| Que voulez-vous faire ? | 36 |
| Rubriques connexes | 36 |
| Vue Système de services | 36 |

Notions de base de Broker et Concentrator

Les Concentrators et les Brokers agrègent des données capturées ou agrégées par d'autres services différents des Decoders, qui eux capturent les données.

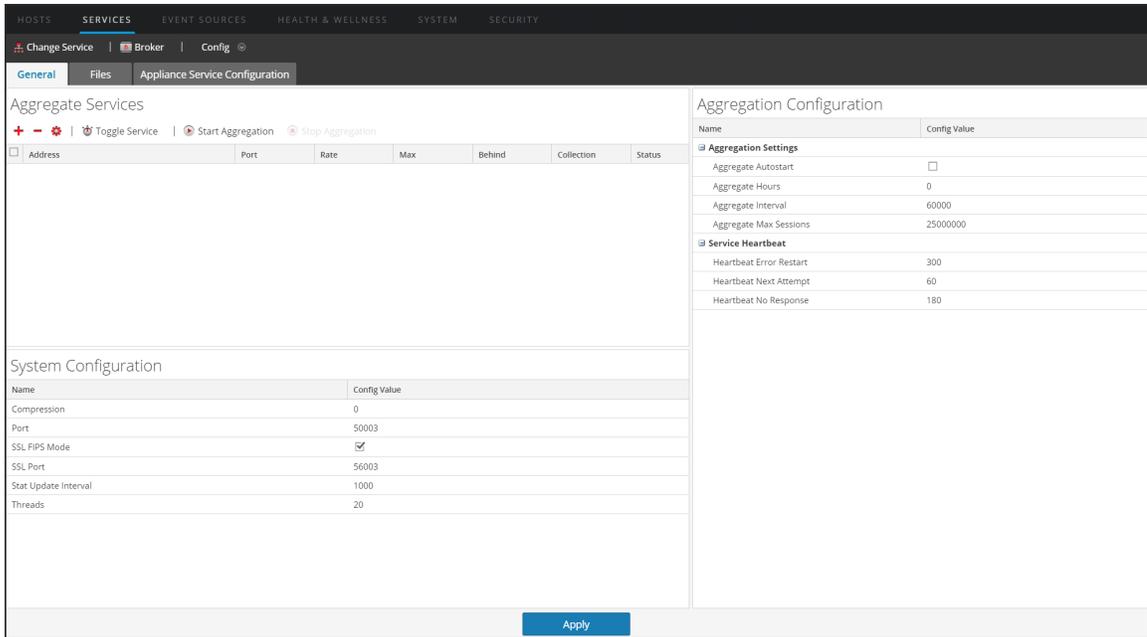
RSA NetWitness Suite prend en charge les services Broker et Concentrator :

- Brokers : regroupent les données de toute l'infrastructure à partir des Concentrators configurés. Vous pouvez avoir plusieurs services Concentrator agrégés en un seul broker. Vous pouvez également avoir plusieurs services Broker agrégés en un seul broker.
- Concentrators : agrègent et analysent les données dans plusieurs emplacements de capture à partir des Decoders. indexent et dirigent les requêtes.

Vous pouvez configurer différents Brokers et Concentrators ensemble sous un Broker. Les Brokers peuvent extraire rapidement les données des Concentrators, car ils acquièrent uniquement les informations d'index. Cette configuration s'effectue à l'aide de l'interface utilisateur RSA NetWitness Suite. La majorité de la configuration s'effectue dans la vue Services d'administration (Admin > Services).

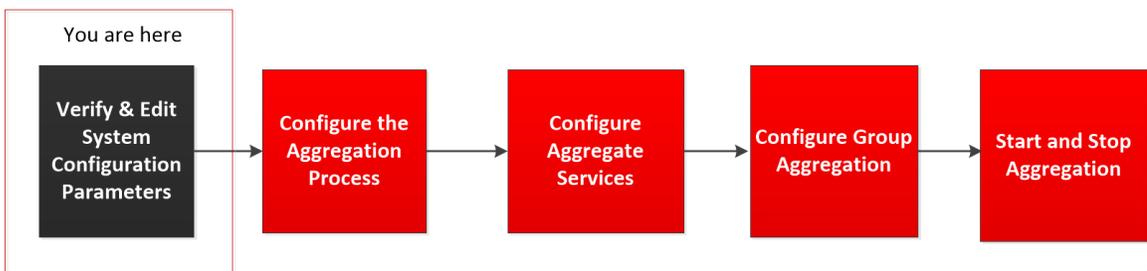
| Name | Licensed | Host | Type | Version | Actions |
|-------------------------------|----------|------------------|---------------------------|------------------------|------------------|
| Admin Server | ✓ | NWAPPLIANCE9 | Admin Server | 11.0.0.0 | [Stop] [Refresh] |
| Archiver | ✓ | NWAPPLIANCE25988 | Archiver | 11.0.0.0 | [Stop] [Refresh] |
| Broker | ✓ | NWAPPLIANCE2943 | Broker | 11.0.0.0 | [Stop] [Refresh] |
| Broker | ✓ | NWAPPLIANCE9 | Broker | 11.0.0.0 | [Stop] [Refresh] |
| Broker | ✓ | NWAPPLIANCE7952 | Broker | 11.0.0.0 | [Stop] [Refresh] |
| Concentrator | ✓ | NWAPPLIANCE22655 | Concentrator | 11.0.0.0 | [Stop] [Refresh] |
| Config Server | ✓ | NWAPPLIANCE9 | Config Server | 11.0.0.0 | [Stop] [Refresh] |
| ContextHub Server | ✓ | NWAPPLIANCE10604 | ContextHub Server | 11.0.0.0 | [Stop] [Refresh] |
| Decoder | ✓ | NWAPPLIANCE23912 | Decoder | 11.0.0.0 | [Stop] [Refresh] |
| Event Stream Analysis | ✓ | NWAPPLIANCE10604 | Event Stream Analysis | 11.0.0.401-1 | [Stop] [Refresh] |
| Event Stream Analytics Server | ✓ | NWAPPLIANCE10604 | Entity Behavior Analytics | 11.0.0.0 | [Stop] [Refresh] |
| Investigate Server | ✓ | NWAPPLIANCE9 | Investigate Server | 11.0.0.0 | [Stop] [Refresh] |
| Log Collector | ✓ | NWAPPLIANCE21301 | Log Collector | 11.0.0.14515.1.4427309 | [Stop] [Refresh] |
| Log Collector | ✓ | NWAPPLIANCE11639 | Log Collector | 11.0.0.14515.1.4427309 | [Stop] [Refresh] |
| Log Decoder | ✓ | NWAPPLIANCE11639 | Log Decoder | 11.0.0.0 | [Stop] [Refresh] |
| Malware Analytics | ✓ | NWAPPLIANCE2943 | Malware Analysis | 11.0.0.8254-1 | [Stop] [Refresh] |
| Orchestration Server | ✓ | NWAPPLIANCE9 | Orchestration Server | 11.0.0.0 | [Stop] [Refresh] |
| Reporting Engine | ✓ | NWAPPLIANCE9 | Reporting Engine | 11.0.0.5639.1.bc166dd | [Stop] [Refresh] |
| Respond Server | ✓ | NWAPPLIANCE9 | Respond Server | 11.0.0.0 | [Stop] [Refresh] |
| Security Server | ✓ | NWAPPLIANCE9 | Security Server | 11.0.0.0 | [Stop] [Refresh] |
| Warehouse Connector | ✓ | NWAPPLIANCE11639 | Warehouse Connector | 11.0.0.1940.1 | [Stop] [Refresh] |

Vous pouvez également configurer les services agrégés et exécuter l'ensemble du processus d'agrégation à l'aide de la vue Services. Cela permet de configurer les paramètres de démarrage automatique, de délai et de performances, le nombre maximal de métadonnées et de fichiers de session ouverts. De plus, vous pouvez définir le délai des tentatives de redémarrage, de reconnexion et de mise hors ligne d'un service agrégé qui ne répond pas. La configuration des services agrégés comprend la gestion des services Concentrator et Decoder en tant que services agrégés. Vous pouvez également utiliser des champs de métadonnées et des filtres pour limiter les données utilisées à partir d'un service agrégé. Les tâches d'agrégation sont effectuées dans l'onglet Général de la vue Services d'administration (Administrateur > Services).



Étape 1. Vérifier la configuration système d'un service

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



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.

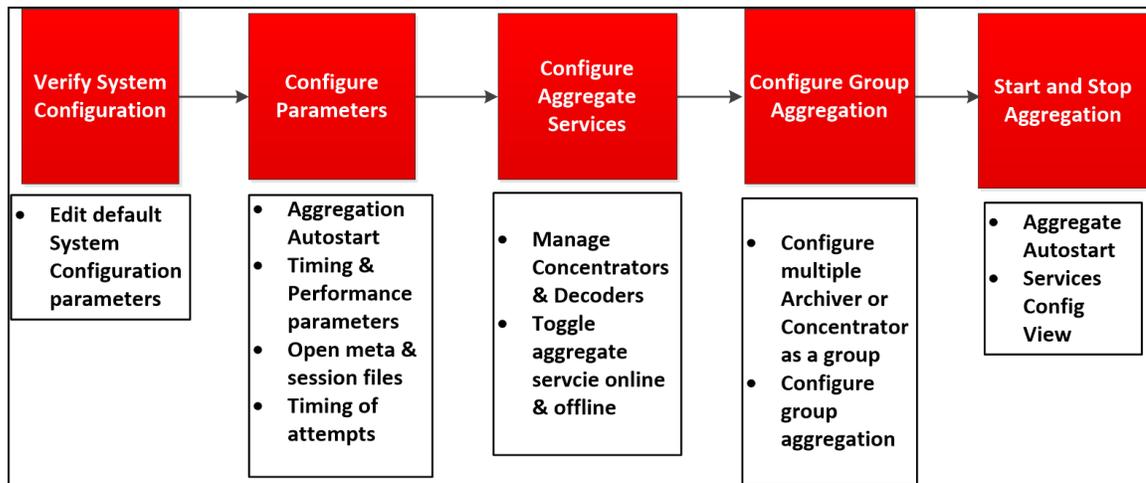
Pour modifier les paramètres de configuration système pour un Broker ou un Concentrator :

1. Dans le **Menu principal**, sélectionnez ADMIN > **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.
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.

Configuration de Broker et Concentrator

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

Il s'agit des étapes de configuration requises pour un nouveau Broker ou Concentrator, et de modification de la configuration d'un Broker existant. Suivez les étapes de la section dans l'ordre où elles sont indiquées.



Liste de contrôle de configuration de base

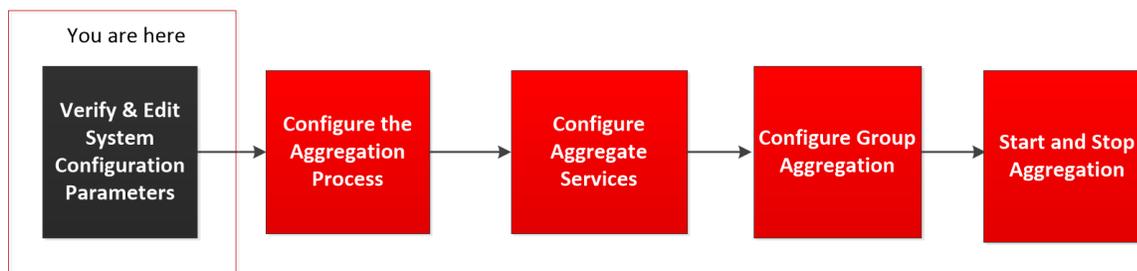
La liste de contrôle suivante précise l'ordre des tâches requises pour configurer un Broker ou un Concentrator ayant été ajouté à RSA NetWitness Suite conformément au *Guide des hôtes et services*.

| Étape de configuration | Description |
|---|---|
| Étape 1 - Vérifier la configuration système | Vérifiez que les valeurs par défaut de la configuration système sont appropriées, comme le décrit la rubrique Étape 1. Vérifier la configuration système d'un service |
| Étape 2 - Configurer les paramètres | Configurez les paramètres qui régissent l'ensemble du processus d'agrégation, comme le décrit la rubrique Étape 2. Configurer le processus d'agrégation |

| Étape de configuration | Description |
|--|---|
| Étape 3 - Configurer les services agrégés | Configurez les services agrégés, comme le décrit la rubrique Étape 3. Configurer les services agrégés |
| Étape 4 - Configurer l'agrégation de groupes | (Facultatif) Configurez l'agrégation de groupes, comme le décrit la rubrique Étape 4. (Facultatif) Configurer l'agrégation de groupes |
| Étape 5 - Démarrer et arrêter l'agrégation | Démarrez et arrêtez l'agrégation, comme le décrit la rubrique Étape 4. Démarrer et arrêter l'agrégation |

Étape 1. Vérifier la configuration système d'un service

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



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.

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

1. Dans le **Menu principal**, sélectionnez **ADMIN > 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.
3. Dans Configuration système, cliquez sur le champ que vous souhaitez modifier et saisissez

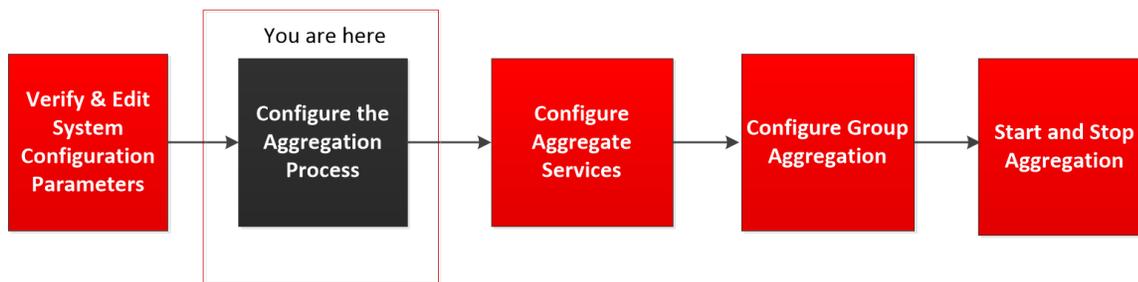
la nouvelle valeur.

4. Lorsque la modification est terminée, cliquez sur Appliquer.

Étape 2. Configurer le processus d'agrégation

La configuration du processus d'agrégation comprend la configuration des éléments suivants pour un Broker ou un Concentrator :

- 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

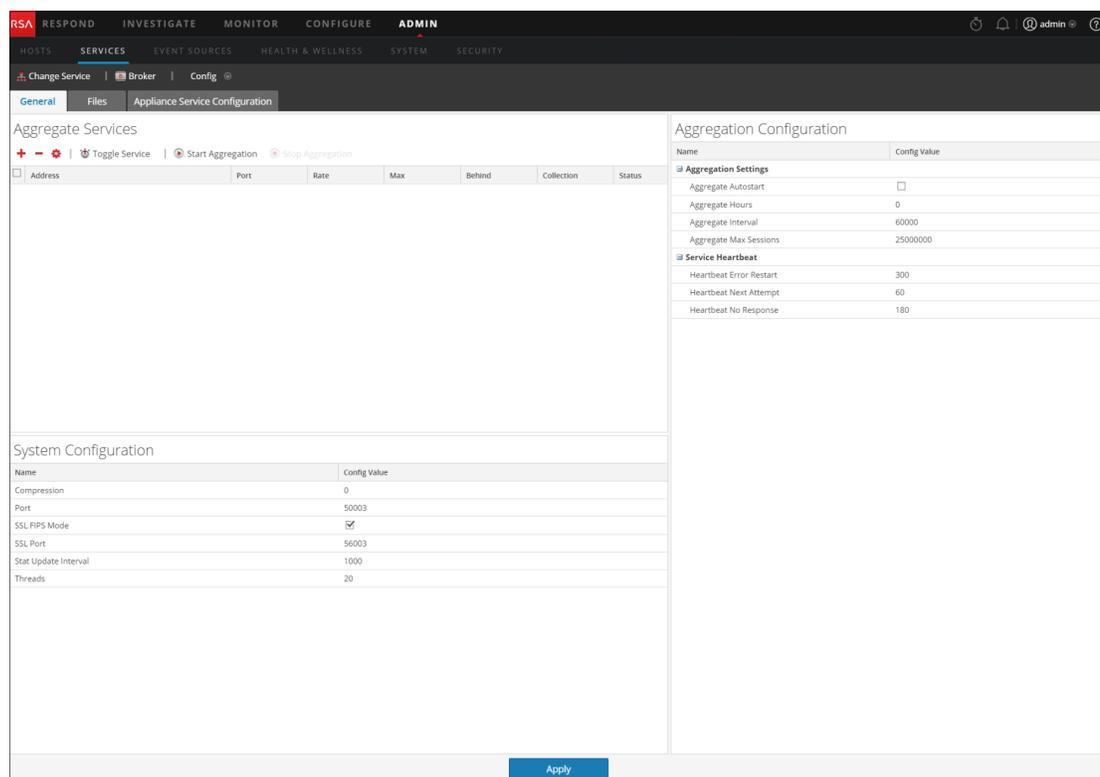


Pour configurer le processus d'agrégation de Broker ou Concentrator :

1. Dans le **Menu principal**, sélectionnez ADMIN > **Services**.
2. Dans la vue **Services**, sélectionnez un Broker ou un Concentrator, puis  > **Vue > Config.**

La vue Configuration des services, qui comprend la section Configuration de l'agrégation,

s'affiche.



3. (Facultatif) Sélectionnez **Démarrage automatique de l'agrégation** pour activer le démarrage automatique de l'agrégation quand un service est en ligne.

| Aggregation Configuration | |
|-----------------------------|-------------------------------------|
| Name | Config Value |
| Aggregation Settings | |
| Aggregate Autostart | <input checked="" 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 |

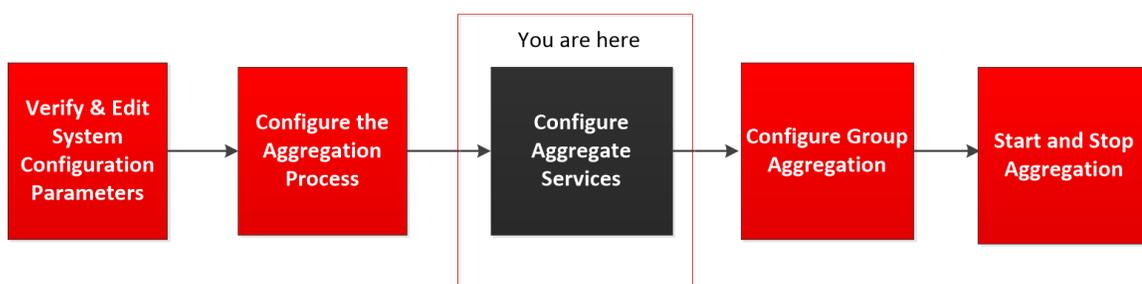
4. (Facultatif) Modifiez l'un des paramètres d'agrégation : les heures à partir desquelles l'agrégation doit commencer, les millisecondes entre les cycles d'agrégation et le nombre maximal de sessions par cycle d'agrégation.
5. (Facultatif) Modifiez l'un des paramètres du service Heartbeat, qui indique 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 de base relatives à l'agrégation de données sur les Brokers et Concentrators. Pour plus d'informations sur la configuration facultative de l'agrégation de groupes, reportez-vous à la section [Étape 4. \(Facultatif\) Configurer l'agrégation de groupes.](#)

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

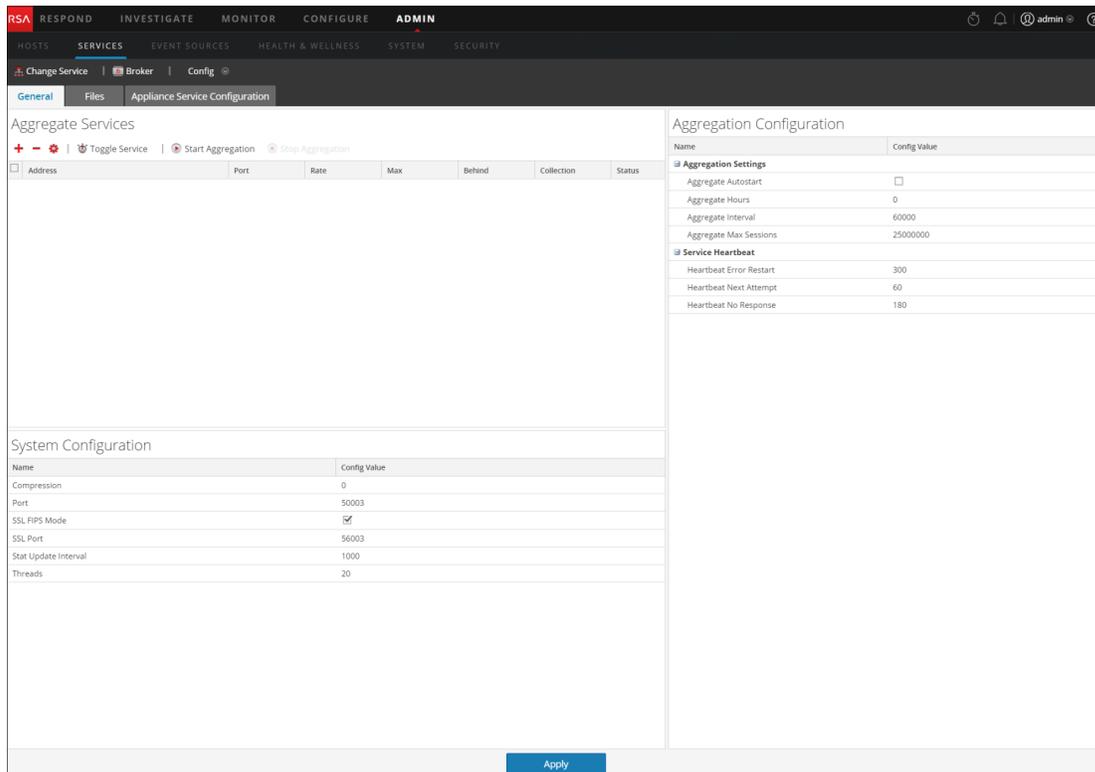
- l'ajout, la modification et la suppression de Concentrators et de Decoders en tant que services agrégés
- Basculement d'un service agrégé en ligne et hors ligne



Ajouter des services agrégés à un Broker ou Concentrator

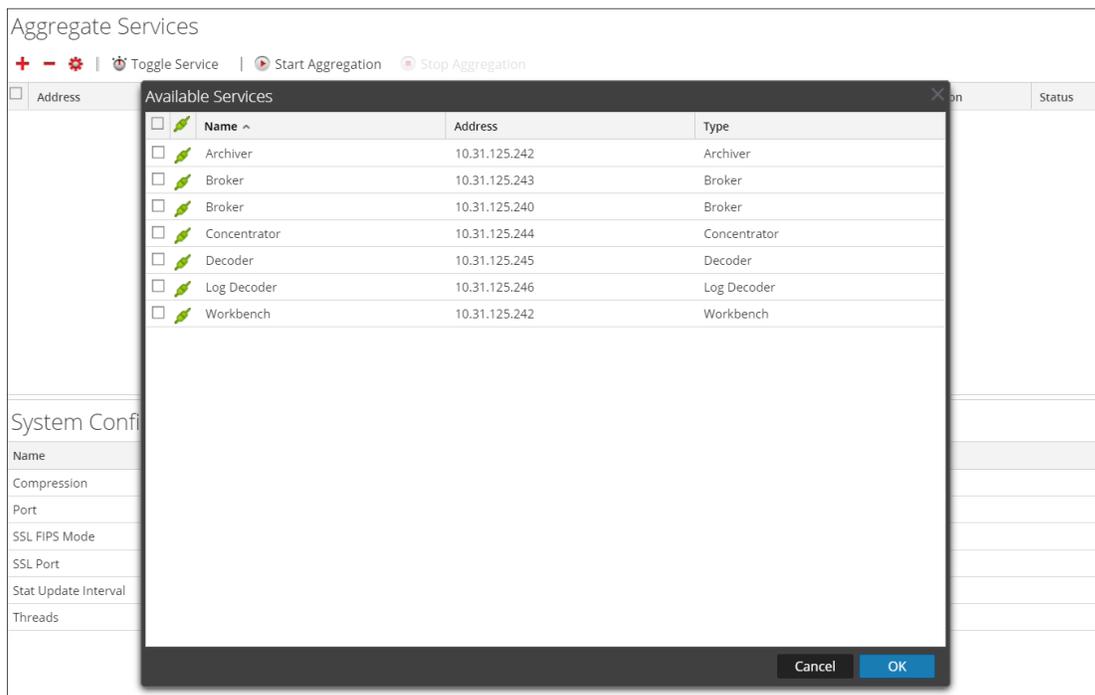
1. Dans le menu **Menu principal**, sélectionnez **ADMIN > Services**.
2. Dans la vue **Services ADMIN**, sélectionnez un Broker ou un Concentrator, puis sélectionnez   > **Vue > Config**.

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**.
- Saisissez le nom d'utilisateur et le mot de passe administrateur pour authentifier l'ajout d'un service.

Add Service Concentrator

Please provide administrator credentials for the service:

Username

Password

Please configure the SSL settings for this service:

SSL

Port Number

Cancel OK

Les services ajoutés sont répertoriés dans la liste Services agrégés.

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

Supprimer des services agrégés sur un Broker ou Concentrator

Remarque : 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 liste **Services agrégés**, sélectionnez un ou plusieurs services.
- Cliquez sur  dans la barre d'outils.

Aggregate Services

   |  Toggle Service |  Start Aggregation |  Stop Aggregation

| <input type="checkbox"/> | Address | Port | Rate | Max | Behind | Collection | Status |
|-------------------------------------|---------------|-------|------|-----|--------|------------|--------|
| <input checked="" type="checkbox"/> | 10.31.125.240 | 50003 | | | | | |
| <input type="checkbox"/> | 10.31.125.244 | 56005 | | | | | |

Le service est supprimé de la liste Services agrégés.

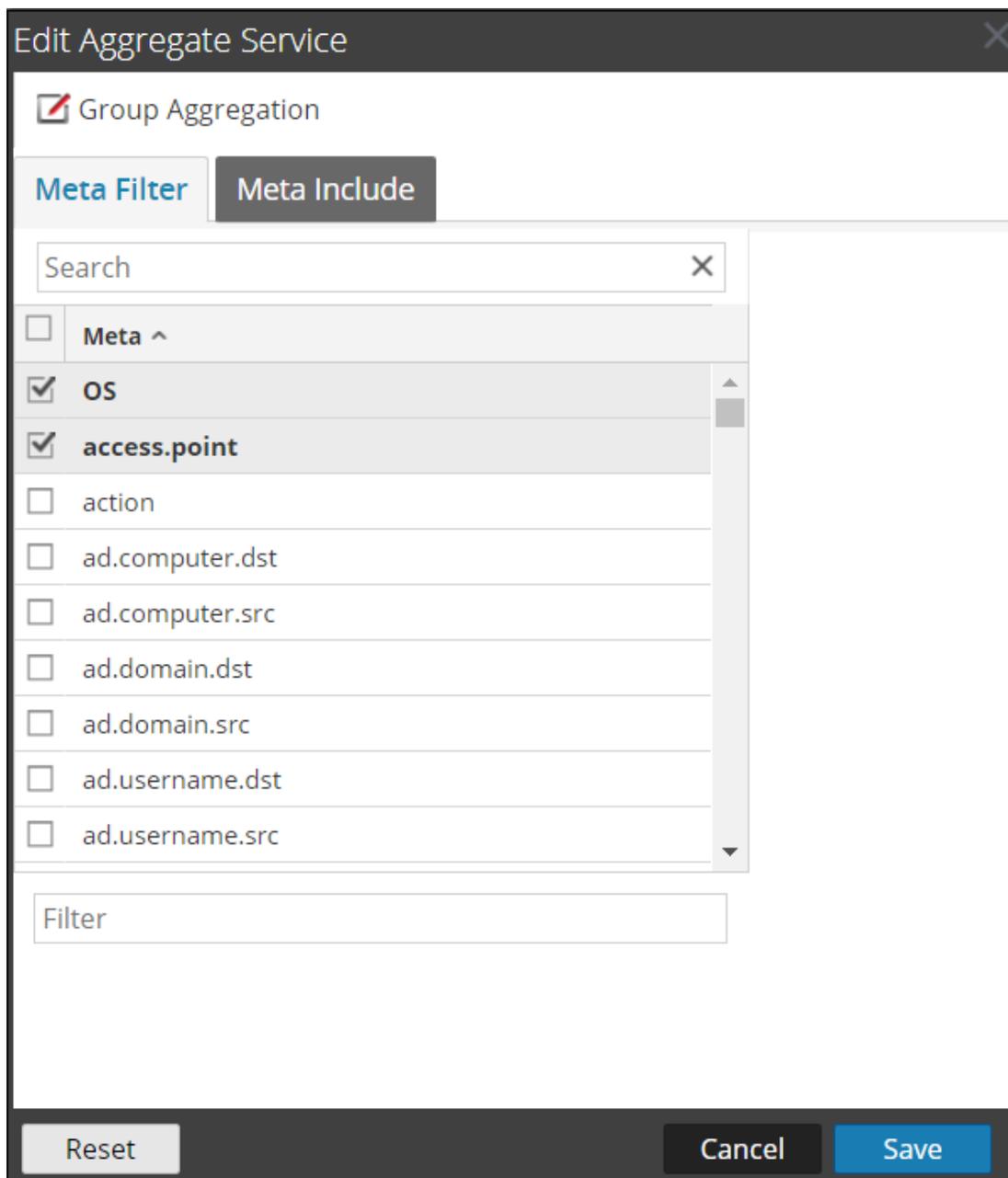
- Pour enregistrer la modification, cliquez sur **Appliquer**.

Modifier les services agrégés sur un Concentrator

Remarque : 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 ne pouvez modifier qu'une seule liste à la fois.

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 :

1. Cliquez sur **Modifier le service** pour convertir le service en service Concentrator.
2. Dans la liste **Services agrégés**, sélectionnez un ou plusieurs services.
3. Cliquez sur  dans la barre d'outils. Dans la boîte de dialogue contextuelle, saisissez les informations d'authentification.
 - Si le service a été ajouté sur une instance différente de NetWitness Suite, vous devez l'ajouter à cette instance de NetWitness Suite pour la modifier. Une boîte de dialogue d'avertissement vous 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**, NetWitness Suite 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.
4. 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. Cliquez sur **Enregistrer**.



5. 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**. Cliquez sur **Enregistrer**.
6. 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.

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

Changer de service

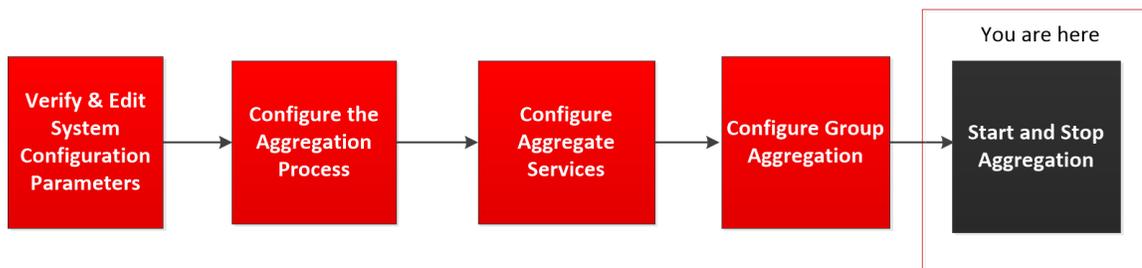
Lorsque l'agrégation de données commence, les Brokers et Concentrators consomment des données de services agrégés en ligne. Lors de l'ajout sur un Broker ou Concentrator pour la première fois, les services agrégés sont hors ligne. Pour basculer un service entre les modes en ligne et hors ligne :

1. Sélectionnez un service dans la liste **Services agrégés**.
2. Cliquez sur  **Toggle Service** .

L'état est modifié.

Étape 4. Démarrer et arrêter l'agrégation

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.

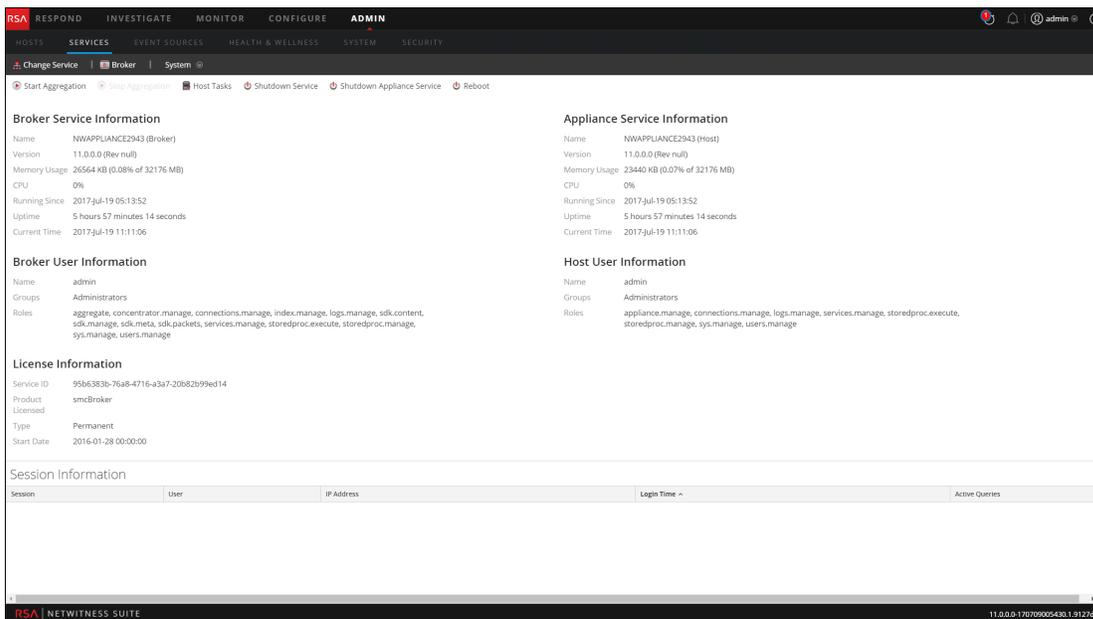


Remarque : Les paramètres de configuration de l'agrégation de la [vue Configuration des services](#) d'un Broker ou d'un Concentrator déterminent si le Démarrage automatique de l'agrégation est activé, ainsi que la taille d'un cycle d'agrégation et le temps entre les cycles.

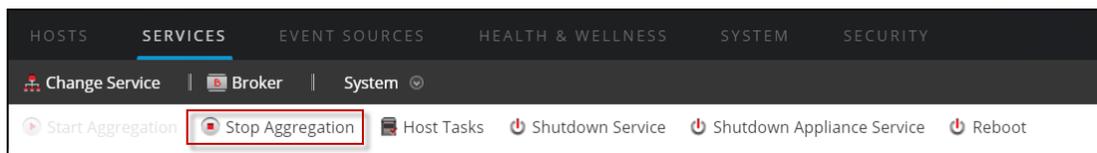
Démarrer et arrêter l'agrégation des données dans la vue Système de services

1. Dans **Menu principal**, sélectionnez **ADMIN > Services**.

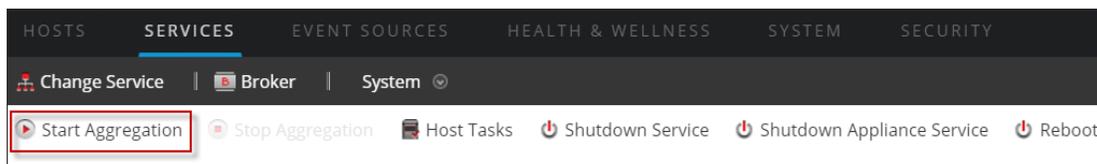
2. Dans la vue **ADMIN Services**, sélectionnez un Broker ou un Concentrator, puis   > **Vue > Système.**



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.



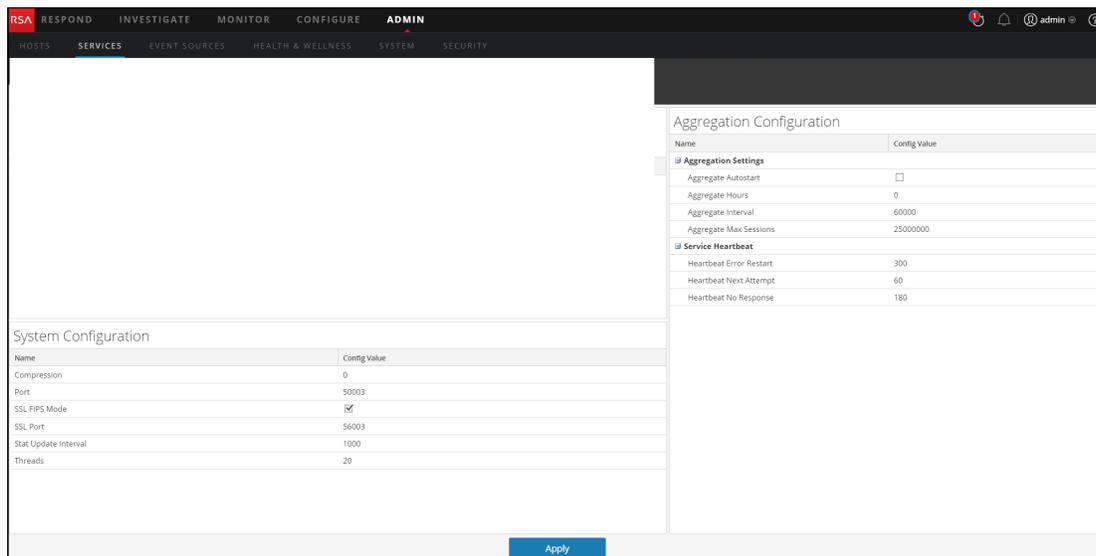
4. Si vous voulez que le service lance l'agrégation des données à nouveau, cliquez sur **Démarrer l'agrégation**. Vous pouvez maintenant étudier les données saisies dans le module Investigation.



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

1. Dans **Menu principal** , sélectionnez **ADMIN > Services**.
2. Dans la vue **Services admin**, sélectionnez un Broker ou un Concentrator, puis  > **Vue > Config**.

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**.

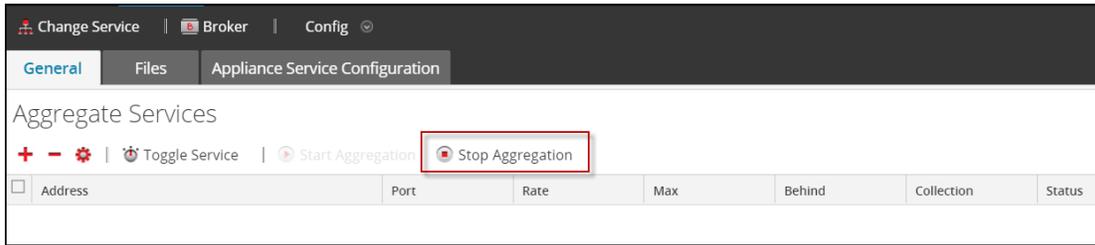
Lorsque l'agrégation commence, l'état de tous les services agrégés en ligne passe à **consommation**. Le bouton Démarrer l'agrégation est désactivé et le bouton Arrêter l'agrégation est activé.



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 passe à **en ligne**. Le bouton Arrêter l'agrégation est indisponible et le bouton Démarrer l'agrégation est

disponible.



Références de configuration de Broker et Concentrator

Vous pouvez configurer les Brokers et Concentrators à l'aide de l'interface utilisateur NetWitness Suite.

En plus des vues décrites ici, vous pouvez afficher les nœuds de service complets sous forme d'arborescence dans la vue Explorer les services. Consultez la rubrique « Vue Explorer les services » dans le *Guide de mise en route des hôtes et services*.

Rubriques

- [Vue Configuration des services - onglet Général des Brokers/Concentrators](#)
- [Vue Système de services - Broker](#)

Vue Configuration des services - onglet Général des Brokers/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

Que voulez-vous faire ?

| Rôle | Je souhaite... | Consultez... |
|----------------|---|---|
| Administrateur | Démarrer et arrêter l'agrégation Ajouter, modifier, supprimer et activer ou désactiver un service agrégé | Section Services agrégés |
| Administrateur | Gérer la configuration du système | Section Configuration système |

Rubriques connexes

- [Notions de base de Broker et Concentrator](#)
- [Configuration de Broker et Concentrator](#)

Onglet Général

Voici un exemple de l'onglet Général d'un Concentrator.

The screenshot shows the 'General' configuration page for a Concentrator. The interface includes a top navigation bar with 'ADMIN' selected, and a sub-navigation bar with 'Config' selected. The main content area is divided into three sections:

- Aggregate Services:** A table with columns: Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, Status. It includes action buttons: Edit Service, Toggle Service, Start Aggregation, Stop Aggregation.
- System Configuration:** A table with columns: Name, Config Value.

| Name | Config Value |
|----------------------|-------------------------------------|
| Compression | 0 |
| Port | 50005 |
| SSL FIPS Mode | <input checked="" type="checkbox"/> |
| SSL Port | 56005 |
| Stat Update Interval | 1000 |
| Threads | 20 |
- Aggregation Configuration:** A table with columns: Name, Config Value.

| Name | Config Value |
|-----------------------------|-------------------------------------|
| Aggregation Settings | |
| Aggregate Autostart | <input checked="" type="checkbox"/> |
| Aggregate Hours | 0 |
| Aggregate Interval | 10 |
| Aggregate Max Sessions | 10000 |
| 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.

Voici un exemple de l'onglet Général d'un Broker.

The screenshot shows the 'General' configuration page for a Broker. The interface is similar to the Concentrator page but with different settings:

- Aggregate Services:** A table with columns: Address, Port, Rate, Max, Behind, Collection, Status. It includes action buttons: Toggle Service, Start Aggregation, Stop Aggregation.
- System Configuration:** A table with columns: Name, Config Value.

| Name | Config Value |
|----------------------|-------------------------------------|
| Compression | 0 |
| Port | 50003 |
| SSL FIPS Mode | <input checked="" 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.

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

- Services agrégés
- Configuration système

- Configuration de l'agrégation

Section 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 un exemple de la section Services agrégés d'un Concentrator.

| Aggregate Services | | | | | | | | | | |
|--------------------------|---------------|-------|------|-----|--------|-------------|--------|--------------|---------|-----------|
| | | | | | | | | | | |
| <input type="checkbox"/> | Address | Port | Rate | Max | Behind | Meta Fields | Filter | Meta Include | Grouped | Status |
| <input type="checkbox"/> | 10.31.125.245 | 50004 | 0 | 0 | 0 | | | | no | consuming |
| <input type="checkbox"/> | 10.31.125.246 | 50002 | 0 | 0 | 0 | | | | 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 Filtres 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 liste en appliquant les règles définies pour ce service. |
| 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, ce qui peut prendre plusieurs |

| Option | Description |
|--|--|
|  Toggle Service | minutes. Il est nécessaire d'arrêter les services agrégés afin de réaliser certaines procédures administratives. 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 liste 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 |
| Rate | 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. |

| Colonne | Description |
|--------------------------------|--|
| Collection | 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. Répertoire les types de métadonnées consommées par le service agrégé. |
| Filtres | Réservée aux Concentrators. Répertoire 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. |
| Groupee | Précise si le service agrégé fait partie d'un groupe. |
| État | <p>Affiche l'état actuel du service :</p> <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 |

Section 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 | <p>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.</p> <p>La modification d'une valeur prend effet immédiatement pour toutes les connexions suivantes.</p> |
| Port | <p>Port d'écoute du service. Les ports par défaut sont les suivants :</p> <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 |
| Mode FIPS SSL | <p>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.</p> |
| Port SSL | <p>Numéro de port SSL.</p> |
| Intervalle de mise à jour des statistiques | <p>Nombre de millisecondes entre les mises à jour statistiques sur le système. Les petites valeurs engendrent des mises à jour plus fréquentes et peuvent ralentir d'autres processus. La valeur par défaut est 1 000.</p> <p>La modification de la valeur prend effet immédiatement.</p> |
| Threads | <p>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.</p> <p>Les modifications prendront effet au redémarrage du service.</p> |

Section 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.

Attention : Ne modifiez pas ces paramètres, sauf si vous y êtes invité par les développeurs ou l'équipe du support client. Contactez le support client, pour toute question avant de modifier ces paramètres.

| 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 |

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. |

| Paramètre | Description |
|--------------------------------------|--|
| 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 immédiatement effet.</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. 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 : <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 | <p>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.</p> |
| Sessions d'agrégation maximum | <p>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.</p> |

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 ou Concentrator

La vue Système de services affiche des informations spécifiques à certains services Broker et Concentrator.

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

Que voulez-vous faire ?

| Rôle | Je souhaite... | Consultez... |
|----------------|---|--|
| Administrateur | Démarrer et arrêter l'agrégation Ajouter, modifier, supprimer et activer ou désactiver un service agrégé | Vue Système de services - Broker ou Concentrator |
| Administrateur | Gérer la configuration du système | Vue Système de services - Broker ou Concentrator |

Rubriques connexes

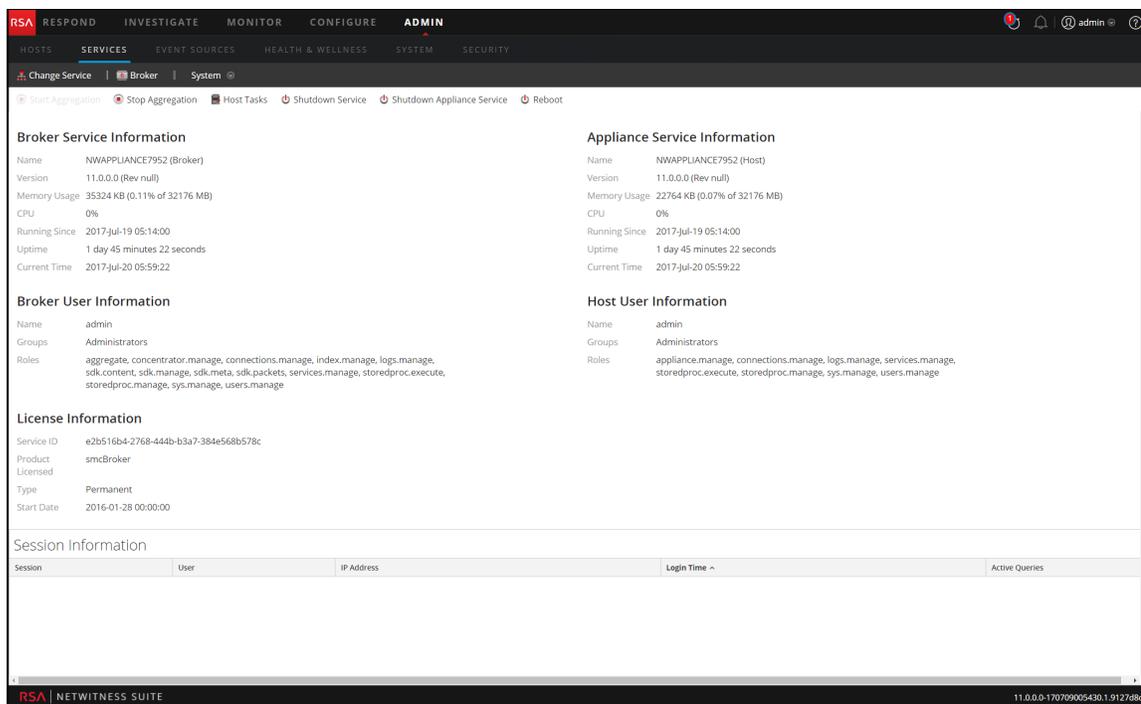
- [Notions de base de Broker et Concentrator](#)
- [Configuration de Broker et Concentrator](#)

Vue Système de services

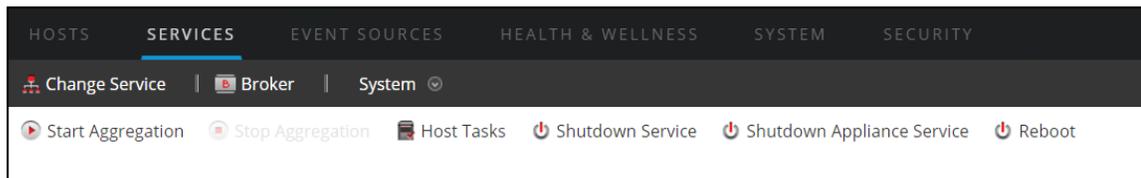
Vous pouvez accéder à cette vue de la manière suivante :

1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Sélectionnez un Concentrator ou un Broker, puis sélectionnez  > **Vue > Système**.

La vue Système du Concentrator ou Broker sélectionné s'affiche.



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** dans le *Guide de mise en route de l'hôte et 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. |

| Action | Description |
|-----------------------------|---|
| 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. |