RSA NETWITNESS® SUITE

Guide de mise en route des hôtes et des services

pour la version 11,1

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

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

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

juillet 2018

Sommaire

Notions de base sur les hôtes et les services

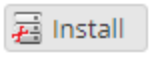
Ce guide indique aux administrateurs les procédures standard d'ajout et de configuration d'hôtes et de services dans NetWitness Suite. Après une présentation de l'objectif de base des hôtes et services et de leur fonctionnement dans le réseau NetWitness Suite, ce guide décrit :

- Tâches 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

Qu'est-ce qu'un hôte ?

L'hôte est la machine sur laquelle un service s'exécute. Ce peut être une machine physique ou virtuelle. Consultez la section « Schéma détaillé de déploiement des hôtes RSA NetWitness Suite » dans le *Guide de déploiement de RSA Netwitness Suite* pour une illustration de la manière dont les hôtes sont déployés. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Qu'est-ce qu'un type d'hôte ?

Un type d'hôte affecte un ou des services à un hôte lorsque vous installez un hôte à partir de la vue Hôtes. Choisissez un **type d'hôte** dans la boîte de dialogue **Installer les services** qui s'affiche au moment de sélectionner un hôte dans la vue Hôtes, puis cliquez sur 

(icône Installer). Le tableau suivant répertorie chaque type d'hôte, ainsi que le ou les services qu'il installe. Consultez la section « Schéma détaillé de déploiement des hôtes RSA NetWitness Suite » dans le *Guide de déploiement de RSA Netwitness Suite* pour une illustration de la manière dont les hôtes sont déployés. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Type d'hôte	Services installés
Archiver	Workbench et Archiver
Broker	Broker
Cloud Gateway	Cloud Gateway
Concentrator	Concentrator

Type d'hôte	Services installés
Endpoint Hybrid	Log Decoder, Endpoint et Concentrator
Endpoint Log Hybrid	Log Collector, Log Decoder, Endpoint et Concentrator
ESA primaire	Context Hub, Entity Behavior Analysis et Event Stream Analysis
ESA secondaire	Entity Behavior Analysis et Event Stream Analysis
Log Collector	Log Collector
Log Decoder	Log Collector et Log Decoder
Log Hybrid	Log Collector, Log Decoder, Endpoint et Concentrator
Malware Analysis	Malware Analysis et Broker
Packet Decoder	Decoder
Packet Hybrid	Concentrator et Decoder
Warehouse Connector	Warehouse Connector

Qu'est-ce qu'un service ?

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.

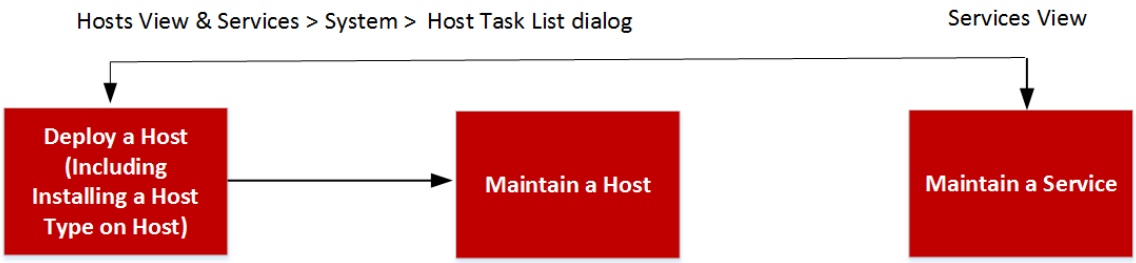
Vous devez commencer par configurer les services Core suivants :

- Decoder
- Concentrator
- Broker
- Log Decoder

Tous les services sont répertoriés ci-dessous et chaque service, excepté le Log Collector, possède son propre guide ou en partage un dans les *Guides de configuration de l'hôte et des services*. Le Log Collector possède son propre ensemble de guides de configuration pour gérer la configuration de tous les protocoles de collecte d'événements pris en charge. Pour plus d'informations sur Log Collector, reportez-vous à la section *Guides de Log Collection*.

- Archiver
- Broker
- Cloud Gateway
- Concentrator
- Context Hub
- Decoder (paquets)
- Endpoint
- Entity Behavior Analysis
- Event Stream Analysis
- Investigate
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Respond
- 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.



Configuration d'un hôte

La vue Hôtes permet d'ajouter un hôte à NetWitness Suite. Reportez-vous à l'Étape 1. Déployer un hôte pour obtenir des instructions détaillées.

Maintenance des hôtes

Utilisez la vue principale Hôtes pour effectuer des ajouts, des modifications, des suppressions et d'autres tâches de maintenance pour les hôtes présents dans votre déploiement. Utilisez la boîte de dialogue Liste des tâches pour réaliser des tâches relatives aux hôtes et à leurs communications avec le réseau. Reportez-vous à la section Hôtes et procédures de services pour obtenir des instructions détaillées.

Après avoir exécuté l'implémentation initiale de NetWitness Suite, la tâche principale à effectuer dans la vue Hôtes est la mise à jour de votre déploiement NetWitness Suite 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 section **Gérer les mises à jour NetWitness Suite** dans *Maintenance du système* 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 11.6.1.2, vous appliquerez la version suivante à l'hôte.

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

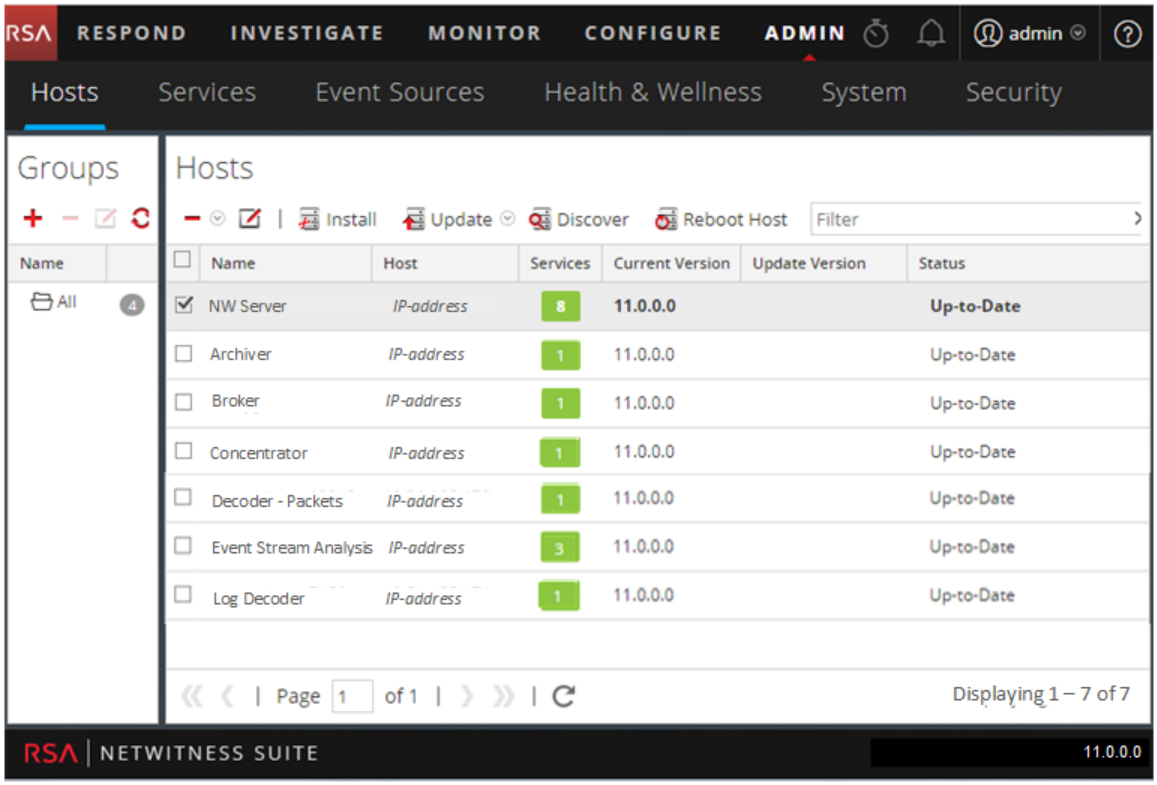
NetWitness Suite prend en charge plusieurs versions dans votre déploiement. L'hôte du serveur Serveur NetWitness (NW) est mis à jour en premier et tous les autres hôtes doivent avoir une version identique ou antérieure à celle de l'hôte Serveur NW.

Remarque : Vous devez d'abord mettre à jour l'hôte Serveur NW et tous les autres hôtes doivent avoir une version identique ou antérieure à celle de l'hôte Serveur NW.

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 11.0.2.0 et 11.0.1.0 pour les hôtes Broker, LC/LD et Log Decoder.
- L'hôte Serveur NW et tous les autres hôtes sont actuellement mis à jour vers la version 11.0.2.0.

Cela signifie que vous pouvez mettre à jour les hôtes Broker, LC/LD et Log Decoder vers la version 11.0.2.0 ou 11.0.2.0.



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. Reportez-vous à la section Hôtes et procédures de services pour obtenir des instructions détaillées.

Services mis en œuvre avec Serveur NetWitness

Les services dans le tableau suivant sont mis en œuvre lorsque vous déployez Serveur NW pour prendre en charge :

- l'extension des plates-formes de déploiement physique et virtuel et des améliorations apportées aux hôtes et aux services de maintenance.
- l'amélioration des fonctions Enquêter et Répondre.

Attention : Il est inutile de configurer ces services pour déployer NetWitness Suite. RSA recommande de surveiller l'état de fonctionnement de ces services à l'aide de l'Intégrité. N'essayez pas de modifier les paramètres dans la vue Explorer sans contacter le support client (https://community.rsa.com/docs/DOC-1294).

Service	Objectif
Admin	Le serveur d'administration (**serveur Admin**) est le service back-end pour les tâches d'administration dans l'interface utilisateur NetWitness Suite (UI). Il permet d'extraire l'authentification, la gestion des préférences globales et la prise en charge de l'autorisation pour l'interface utilisateur. Le **serveur de configuration** et le **serveur de sécurité** doivent être en ligne pour que le **serveur d'administration** soit en mesure de remplir son rôle.
Config	Le serveur de configuration (**serveur Config**) stocke et gère les ensembles de configurations. Un ensemble de configurations est un groupe de configurations logiques géré de manière indépendante. Le **serveur Config** facilite le partage de propriétés parmi les services, comprend des fonctions de sauvegarde et de restauration de configuration, et suit les modifications apportées aux propriétés.
Intégration	Le serveur d'intégration gère les interactions avec les systèmes externes. Le service gère les canaux sortants ou entrants suivants. • REST API Gateway : passerelle vers les clients externes REST attribuant des appels à l'interface de programmation d'application (API) NetWitness. • Notifications Dispatcher - répartiteur centralisé pour toutes les notifications sortantes provenant du déploiement NetWitness.
Investigate	Le serveur Investigate est co-localisé sur l'hôte du serveur NW avec le **serveur d'administration**, le **serveur de configuration**, le **serveur d'intégration, le serveur d'orchestration**, le **serveur Respond** et le **serveur de sécurité**. Le serveur Investigate est co-localisé sur l'hôte du serveur NW avec le serveur d'administration, le serveur de configuration, le serveur d'intégration, le serveur d'orchestration, le serveur Respond et le serveur de sécurité. Consultez le *Guide d'utilisation RSA NetWitness Suite Investigate et Malware Analysis* pour plus d'informations. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.
Orchestration	Le serveur Investigate est un service interne de gestion du système qui s'exécute sur Serveur NW afin de provisionner, installer et configurer tous les services dans votre déploiement NetWitness Suite.

Service	Objectif
Respond	Le service Respond est co-localisé sur l'hôte de serveur NW avec le **serveur d'administration**, le **serveur de configuration**, le **serveur de procédure d'enquête**, le **serveur d'orchestration** et le **serveur de sécurité**. Reportez-vous au *Guide de configuration de RSA NetWitness Respond* pour plus d'informations. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.
Sécurité	Le NetWitness Suite Security Server (**serveur de sécurité**) gère l'infrastructure de sécurité d'un déploiement NetWitness Suite. Il gère les problèmes suivants liés à la sécurité. • Utilisateurs et comptes d'authentification • Contrôle d'accès basé sur les rôles (RBAC) • Le déploiement de l'infrastructure à clé publique (PKI) Un déploiement NetWitness Suite comprend des utilisateurs disposant de comptes d'authentification. Indépendamment de la manière de vérifier l'identité de l'analyste (par exemple, Active Directory), NetWitness Suite doit conserver l'état de l'utilisateur qui n'est pas fourni par tous les fournisseurs d'authentification (par exemple, la dernière heure de connexion, les tentatives de connexion ayant échoué et les rôles). Le concept d'un utilisateur est distinct de l'identité associée à l'utilisateur et le **serveur de sécurité** conserve ces éléments en tant qu'entités Utilisateur et Compte distinctes. Outre les comptes locaux prêts à l'emploi NetWitness disponibles pour tous les déploiements de NetWitness, le serveur prend en charge les fournisseurs d'authentification externe. Le **Serveur de sécurité** permet également d'implémenter RBAC grâce à la gestion des entités de rôle et d'autorisation. Les autorisations peuvent être attribuées à des rôles, et des rôles peuvent être attribués aux utilisateurs. Ensemble, ils permettent une règle d'autorisation flexible pour le déploiement. Le serveur permet également de générer des jetons sécurisés par chiffrement qui codent l'autorisation appropriée pour un utilisateur. Ces jetons constituent la base des autorisations à l'échelle du déploiement.

Fonctionnement en mode Mixte

Le mode Mixte se produit lorsque certains services sont mis à jour vers la dernière version et que d'autres services fonctionnent toujours avec des versions plus anciennes. Cela se produit lorsque vous mettez à jour les hôtes de votre déploiement vers la dernière version en plusieurs phases (ou lorsque vous échelonnez la mise à jour).

Problèmes de fonctionnalité rencontrés lors de mises à jour échelonnées

Si vous échelonnez la mise à jour :

- 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 ;
- les fonctions d'administration des services ne seront peut-être pas disponibles avant de mettre à jour tous les hôtes de votre déploiement ;
- il se peut que la capture des données ne fonctionne pas pendant un certain temps.

Exemples de mises à jour échelonnées

Dans les exemples suivants, tous les hôtes fonctionnent avec la version 11.1.0.x et vous souhaitez échelonner les mises à jour de l'hôte vers la version 11.1.1.0.

Exemple 1. Plusieurs services Decoder et Concentrator : solution alternative 1

Dans cet exemple, le déploiement 11.1.0.x inclut 1 hôte NW Server, 2 hôtes Decoder, 2 hôtes Concentrator, 1 hôte Archiver, 1 hôte Broker, 1 hôte Event Stream Analysis et 1 hôte Malware Analysis.

Vous devez d'abord terminer la Phase 1 et mettre à jour les hôtes dans l'ordre indiqué dans cette Phase 1.

RSA vous recommande de mettre à jour les hôtes de la Phase 2 dans l'ordre indiqué pour la Phase 1.

Phase 1 - Session 1

1. Mettez à jour l'hôte Security Analytics Server.
2. Mettez à jour l'hôte Event Stream Analysis.
3. Mettez à jour l'hôte Malware Analysis.
4. Hôte Broker ou Concentrator.

Phase 2 - Session 2

1. Mettez à jour les 2 hôtes Decoder.
2. Mettez à jour les 2 hôtes Concentrator et l'hôte Archiver.

Phase 2 - Session 3

1. Mettez à jour tous les autres hôtes.

Exemple 2. Plusieurs services Decoder et Concentrator : solution alternative 2

Dans cet exemple, le déploiement 11.1.0.x inclut 1 hôte NW Server, 2 hôtes Decoder, 2 hôtes Concentrator, 1 hôte Broker, 1 hôte Event Stream Analysis et 1 hôte Malware Analysis. RSA vous recommande de mettre à jour les hôtes de la Phase 2 dans la séquence suivante (vous devez d'abord terminer la Phase 1 et mettre à jour les hôtes dans l'ordre indiqué).

Phase 1 - Session 1

1. Mettez à jour l'hôte Security Analytics Server.
2. Mettez à jour l'hôte Event Stream Analysis.
3. Mettez à jour l'hôte Malware Analysis.
4. Mettez à jour l'hôte Broker.

Phase 2 - Session 2

1. Mettez à jour 1 hôte Decoder et 1 hôte Concentrator.
   Temps écoulé au cours duquel NetWitness Suite traite une quantité importante de données.

Phase 2 - Session 3

1. Mettez à jour 1 hôte Decoder, 1 hôte Concentrator et un hôte Broker.
2. Log Decoders
   Mettez à jour tous les hôtes Log Decoder avant de mettre à jour les Virtual Log Collectors
3. Mettez à jour tous les autres hôtes.

Exemple 3. Plusieurs régions

Dans cet exemple, le déploiement 11.1.0.x inclut 1 hôte NW Server, 1 hôte Event Stream Analysis, 1 hôte Malware Analysis, 4 hôtes Decoder, 4 hôtes Concentrator, 2 hôtes Broker, (2 sites, chacun comprenant 2 Decoders, 2 Concentrators et 1 Broker).

Phase 1 - Mise à jour du site 1

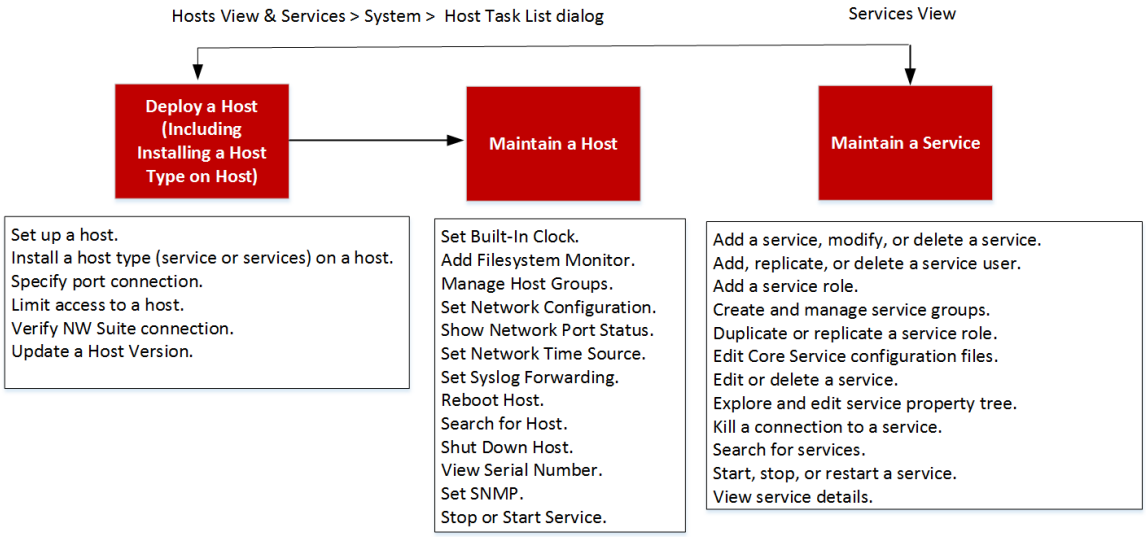
1. Mettez à jour l'hôte NW Server.
2. Mettez à jour l'hôte Event Stream Analysis.
3. Mettez à jour l'hôte Malware Analysis.
4. Mettez à jour 1 hôte Broker, 2 hôtes Decoder et 2 hôtes Concentrator.
5. Mettez à jour tous les autres hôtes.

Phase 2 - Mise à jour du site 2

1. Mettez à jour les hôtes Broker.
2. Mettez à jour les 2 hôtes Decoders.
3. Mettez à jour les 2 hôtes Concentrator.
4. Mettez à jour tous les autres hôtes.

Hôte GS : Procédures des hôtes et des services

Chaque service requiert un hôte. Après avoir configuré un hôte, vous pouvez attribuer des services vers et depuis cet hôte, vers d'autres hôtes de votre déploiement NetWitness Suite.



Tâche générale	Description
Configurer un hôte	Effectuez les tâches suivantes dans l'ordre indiqué pour configurer un hôte. Étape 1. Déployer un hôte. Étape 2. Installer un service sur un hôte. Étape 3. Passer en revue les ports SSL pour les connexions approuvées. Étape 4. Gérer l'accès à un service.

Tâche générale	Description

Effectuer la maintenance d'un hôte - notions de base	Les tâches de maintenance suivantes ne sont pas obligatoires et sont affichées par ordre alphabétique.
	• Appliquer les mises à jour de version à un hôte.
	  • Renseigner le référentiel de mises à jour local
	  • Configurer un référentiel externe avec RSA et les mises à jour du système d'exploitation.
	• Créer et gérer des groupes d'hôtes.
	• Rechercher des hôtes.
	• Définir la configuration réseau.
	• Définir la source de l'heure réseau.
	• Afficher l'état du port réseau.
	• Afficher le numéro de série.
	• Arrêter un hôte.
	• Arrêter et démarrer un service sur un hôte.

Tâche générale	Description
Effectuer la maintenance d'un hôte à partir de la boîte de dialogue Liste des tâches de l'hôte	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. • Exécuter une tâche à partir de la Liste des tâches de l'hôte. • Ajouter et Supprimer le moniteur du système de fichiers. • Redémarrer un hôte. • Paramétrer l'heure prédéfinie de l'hôte. • Définir la configuration réseau. • Définir la source de l'heure réseau. • Configurer SNMP. • Définir le transfert Syslog. • Afficher l'état du port réseau. • Afficher le numéro de série. • Arrêter l'hôte. • Arrêter et démarrer un service sur un hôte.

Tâche générale	Description
Effectuer la maintenance d'un service	Les procédures ci-dessous décrivent comment effectuer la maintenance des services. • Ajouter, répliquer ou supprimer un utilisateur de service. • Ajouter un Rôle d'utilisateur de service. • Changer le mot de passe d'un utilisateur de service. • Créer et gérer des groupes de services. • Dupliquer ou répliquer un rôle de service. • Modifier les fichiers de configuration de service Core. • Modifier ou supprimer un service. • Explorer et modifier l'arborescence des propriétés du service. • Supprimer la connexion à un service. • Rechercher des services. • Démarrer, arrêter ou redémarrer un service. • Voir les détails d'un service.

Étape 1. Déployer un hôte

1. Déployer un hôte.
   Vous pouvez déployer un hôte physique (appliance RSA), un hôte virtuel sur site, un hôte virtuel dans AWS ou un hôte virtuel dans Azure. Consultez les guides suivants pour obtenir des instructions sur la façon de déployer des hôtes.
   - *Guide de déploiement d'un hôte physique RSA NetWitness® Suite*
   - *Guide de déploiement d'un hôte virtuel RSA NetWitness® Suite*
   - *Guide de déploiement RSA NetWitness® Suite AWS*
   - *Guide de déploiement Azure RSA NetWitness® Suite*
2. Accédez à **Administration** > **Hôtes**.
   La boîte de dialogue **Nouveaux hôtes** s'affiche avec les hôtes que vous avez déployés.
3. Sélectionnez l'hôte à activer.
   L'option de menu **Activer** devient active.

4. Cliquez sur **Activer**.

5. Sélectionnez l'hôte que vous avez activé.
   L'hôte s'affiche dans la vue Hôtes. À ce stade, vous pouvez installer un service sur l'hôte.

Étape 2. Installer un service sur un hôte

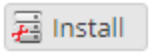
Chaque service se présente comme un plug-in à activer ou désactiver selon la fonction de l'hôte.

Conditions préalables

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

Procédure

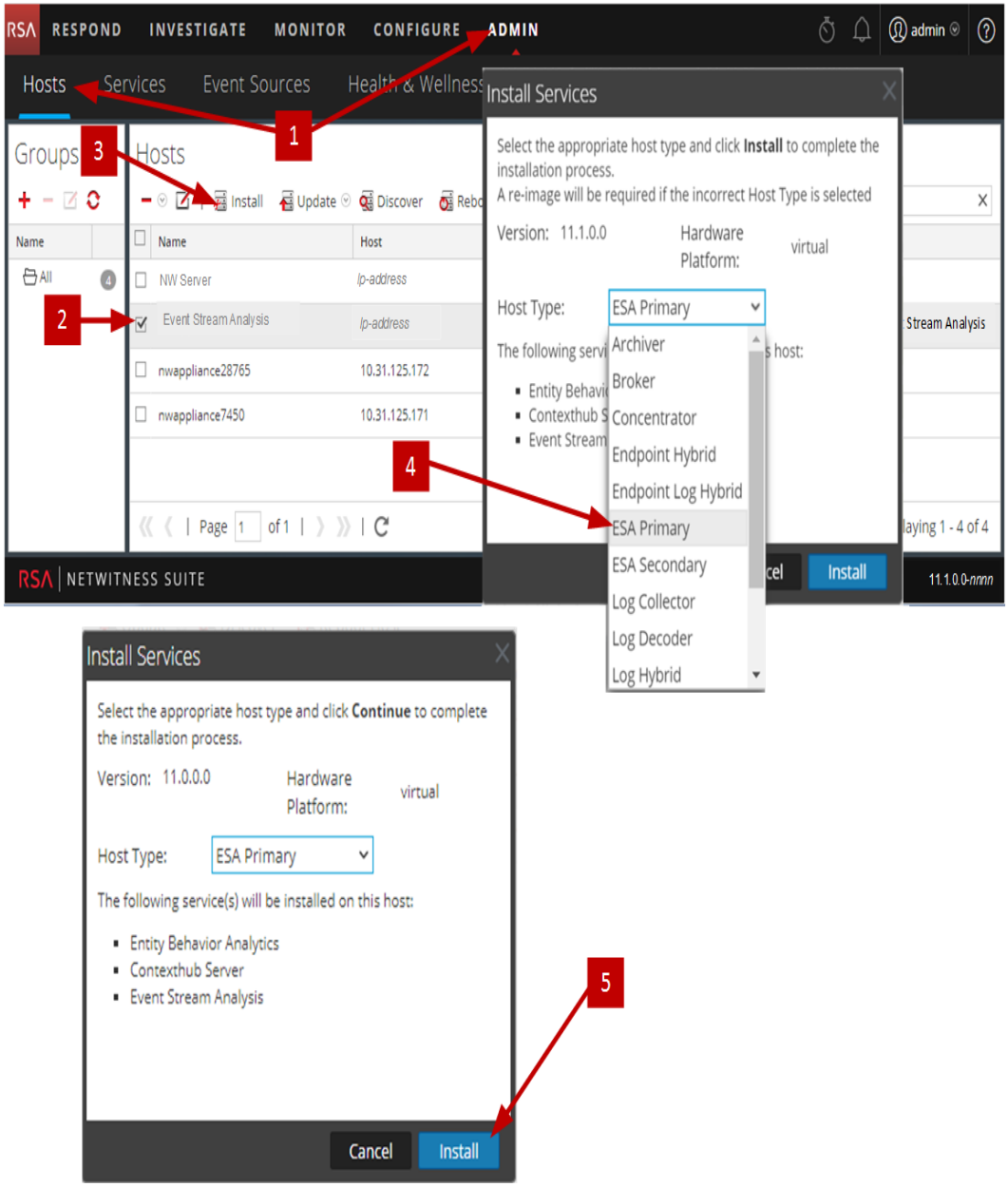
Pour ajouter un service à un hôte, effectuez les étapes suivantes :

1. Dans NetWitness Suite, accédez à **ADMIN > Hôtes**.
   La vue **Hôtes** s'affiche.
2. Sélectionnez l'hôte sur lequel vous souhaitez installer le service (par exemple, **Event Stream Analysis**).
3. Dans la barre d'outils, cliquez sur l'icône 

(Installer).
   La boîte de dialogue **Installer les services** s'affiche.
4. Sélectionnez un service à partir de la liste déroulante **Type d'hôte** (par exemple, **ESA primaire**).
   Le (bouton de commande Installer) 

devient actif dans la boîte de dialogue **Installer les services**.

5. Cliquez sur Install (bouton de commande Installer).



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 NetWitness Suite Core doit être mis à niveau vers la version 10.4 ou ultérieure. Les connexions approuvées ne sont pas rétrocompatibles avec NetWitness Suite Core 10.3.x ou versions antérieures.

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 NetWitness Suite Core dispose de 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 NetWitness Suite avec leurs ports respectifs et indique que chaque service Core a deux ports. Tous les numéros de port répertoriés sont des ports TCP.

Service	Port non SSL non chiffré	Port SSL chiffré	Remarques
Archiver	50008	56008	
Broker	50003	56003	
Passerelle Cloud	S/o	S/o	
Concentrator	50005	56005	
Context Hub	S/o	50022	
Decoder (paquets)	50004	56004	
Endpoint	N/A	N/A	

Service	Port non SSL non chiffré	Port SSL chiffré	Remarques
Analytique comportementale de l'entité	S/o	S/o	
Event Stream Analysis	S/o	50030	
Enquêter	S/o	S/o	Implémenté avec le Serveur NW.
Log Collector	50001	56001	
Log Decoder	50002	56002	
Malware Analysis	S/o	60007	
Reporting Engine	S/o	S/o	Implémenté avec le Serveur NW.
Respond	S/o	S/o	Implémenté avec le Serveur NW.
Warehouse Connector	50020	56020	
Workbench	50007	56007	

Étape 4. Gérer l'accès à un service

Dans une connexion approuvée, un service fait explicitement confiance à Serveur NW pour gérer et authentifier les utilisateurs. Avec cette confiance, les services dans **Admin > Services** n'exigent plus la définition d'informations d'identification pour chaque service NetWitness Suite Core. Au lieu de cela, les utilisateurs qui ont été authentifiés par le serveur peuvent accéder au service sans saisir 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*.

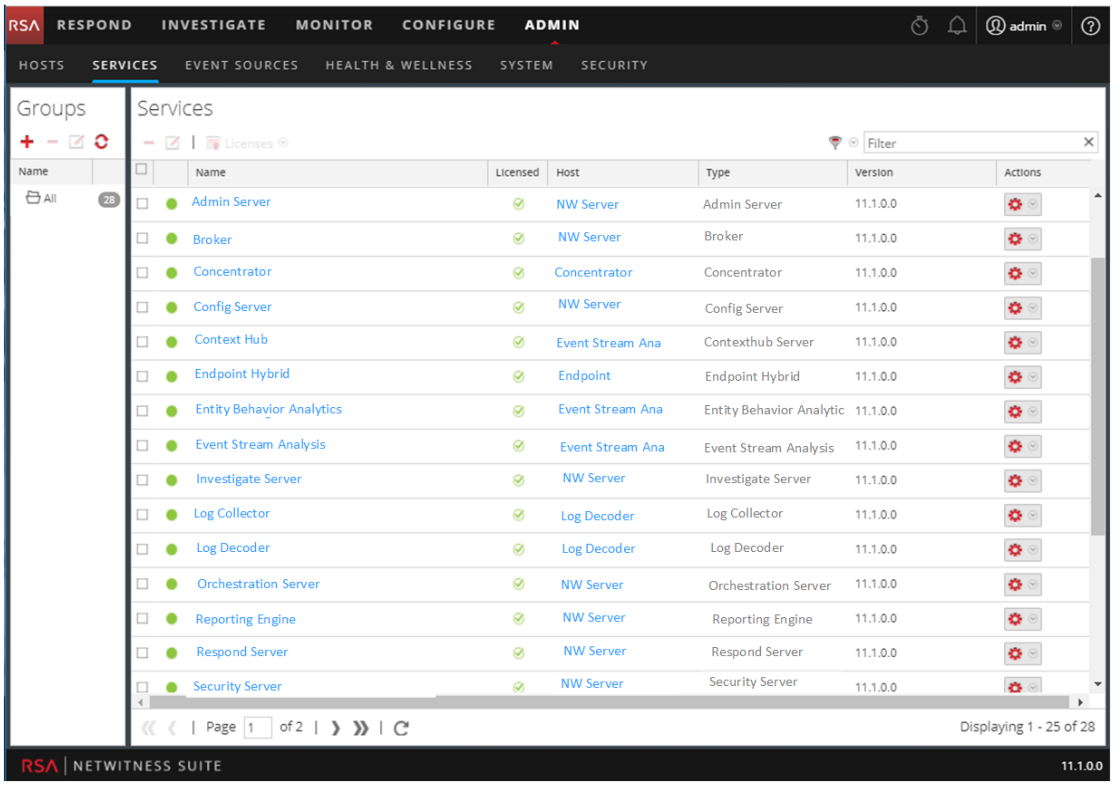
2. L'utilisateur doit :

   - Se connecter à NetWitness Suite pour être authentifié par le serveur
   - Avoir accès au service

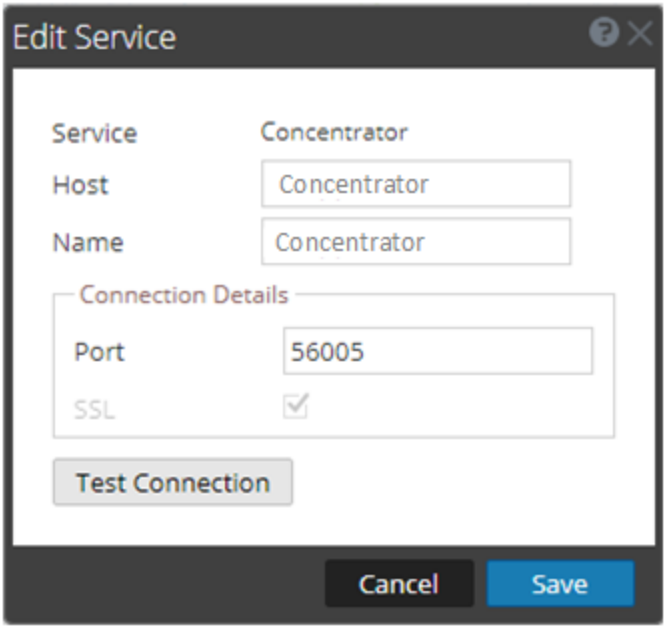
PROCÉDURE

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.

   La vue Services s'affiche.

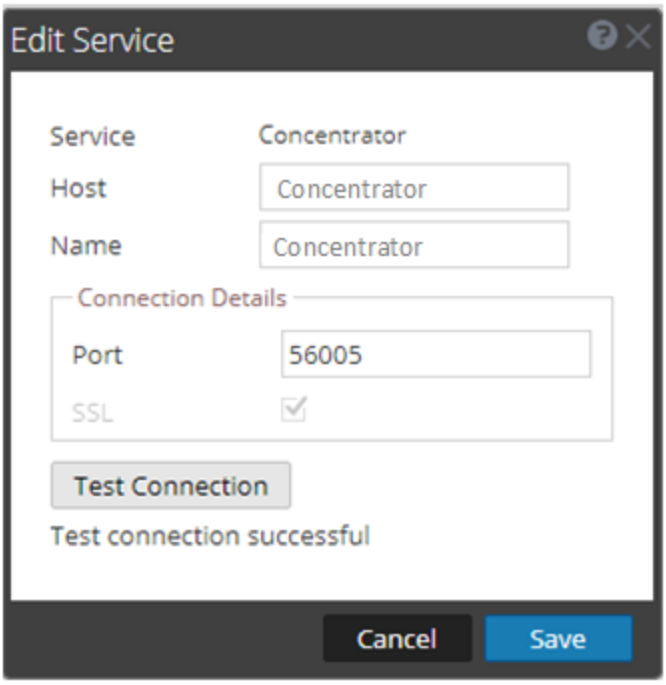


2. Sélectionnez le service (par exemple, un Concentrator) à tester, puis cliquez sur .
   La boîte de dialogue **Modifier le service** s'affiche.



3. Si vous avez fait une nouvelle installation 11.0.0.0, 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 11.0.0.0 ou si vous possédez un environnement mixte de serveur 11.0.0.0 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.
4. Supprimez le **Nom d'utilisateur** pour tester la connexion sans informations d'identification.

5. 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 saisir un nom d'utilisateur et un mot de passe sur le service.

6. Cliquez sur **Enregistrer**.

Appliquer les mises à jour de version à un hôte

Effectuez les tâches suivantes pour mettre à jour un hôte vers une mise à jour de version.

Deux méthodes permettent d'appliquer les mises à jour de version à un hôte.

Remarque : Si vous avez modifié votre emplacement du référentiel, reportez-vous à la section Configurer un référentiel externe avec RSA et les mises à jour du système d'exploitation pour obtenir des instructions.

- Appliquer les mises à jour à partir de la vue Hôte (accès Web)
- Appliquer les mises à jour à partir de la ligne de commande (sans accès Web)

Appliquer les mises à jour à partir de la vue Hôtes (Accès Web)

Tâche 1. Renseigner le référentiel local ou Configurer un référentiel externe

Lorsque vous configurez votre serveur NW, vous sélectionnez le référentiel local ou un référentiel externe. La vue Hôtes récupère les mises à jour de version dans le référentiel que vous sélectionnez.

Si vous avez sélectionné le référentiel local, il est inutile de le configurer, mais vous devez vous assurer qu'il est renseigné avec les dernières mises à jour de version. Reportez-vous à la section Renseigner le référentiel Local pour obtenir des instructions sur la façon de le renseigner avec la mise à jour de version.

Remarque : Si vous avez sélectionné un référentiel externe, vous devez le configurer. Reportez-vous à la section Configurer un référentiel externe avec RSA et les mises à jour du système d'exploitation pour obtenir des instructions sur la façon de configurer un référentiel externe.

Tâche 2. Appliquer les mises à jour à chaque hôte à partir de la vue Hôtes

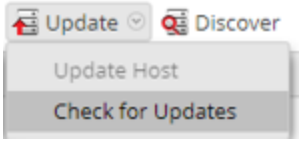
La vue Hôtes affiche les mises à jour de version logicielle disponibles dans votre référentiel de mises à jour local. Vous pouvez choisir d'appliquer les mises à jour que vous souhaitez à partir de cette vue.

Attention : Si vous tentez de mettre à jour des serveurs non NW avec des correctifs 11.0.0.x après la mise à jour du serveur NW vers 11.1, la mise à jour de l'hôte du serveur non NW échouera. Reportez-vous à la section « Mise à jour de <hôte>, » « Erreur lors de la préparation de l'hôte <nom de l'hôte> à mettre à jour vers la version 11.0.0.x. Consultez les logs » dans Hôte GS : Dépannage des installations et mises à jour de version pour plus d'informations.

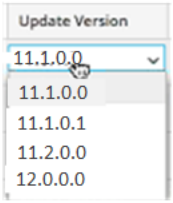
Cette procédure vous indique comment mettre à jour un hôte vers une nouvelle version de NetWitness Suite.

Remarque : Cette rubrique utilise NetWitness Suite 11.0.x.x à 11.1.0.0 comme exemple.

1. Connectez-vous à NetWitness Suite.
2. Accédez à **ADMIN > HÔTES**.
3. (Conditionnel) Vérifiez les dernières mises à jour.

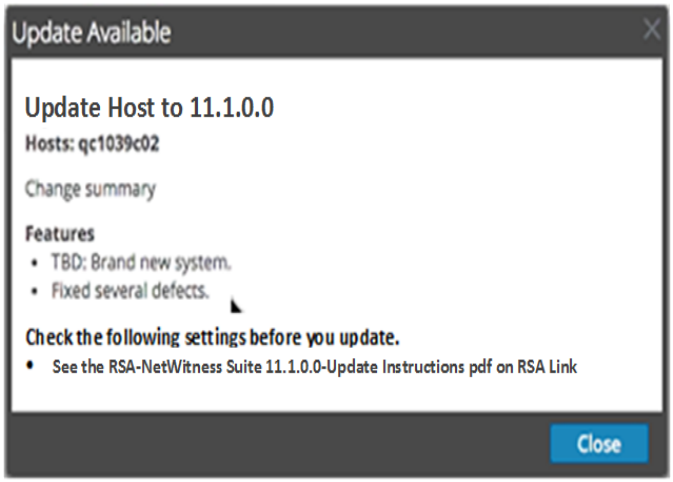


4. Sélectionnez un ou plusieurs hôtes.
   Vous devez d'abord mettre à jour le serveur NW vers la version la plus récente. Vous pouvez mettre à jour les autres hôtes dans n'importe quelle séquence que vous préférez, mais RSA vous recommande de suivre les instructions figurant dans « Fonctionnement en mode Mixte » du *Guide de mise en route des hôtes et des services RSA NetWitness Suite* pour plus d'informations.
   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.
5. Sélectionnez la version que vous souhaitez appliquer à partir de la colonne **Mettre à jour la version**.



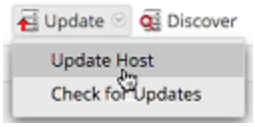
   Si vous :

   - Souhaitez mettre à jour un ou plusieurs hôtes de cette version après la mise à jour de l'hôte du Serveur NW, cochez la case à gauche des hôtes. Seules les versions des mises à jour actuellement prises en charge sont répertoriées.
   - Pour afficher une boîte de dialogue avec les principales caractéristiques de la mise à jour et les informations sur les mises à jour, cliquez sur l'icône d'informations ( ) à droite du numéro de version de mise à jour. La figure suivante donne un exemple de cette boîte de dialogue.

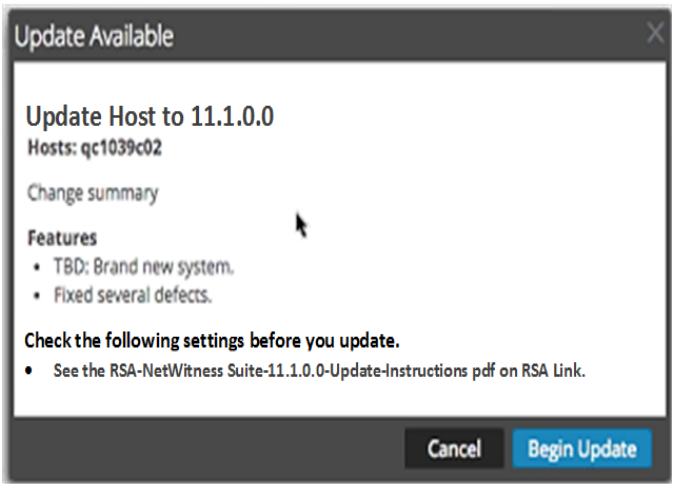


- Impossible de trouver la version souhaitée, sélectionnez **Mettre à jour > Rechercher les mises à jour** pour vérifier le référentiel pour les mises à jour disponibles. Si une mise à jour est disponible, le message « Les nouvelles mises à jour sont disponibles » s'affiche et la colonne **État** se met automatiquement à jour pour afficher les mises à jour disponibles. Par défaut, seules les mises à jour prises en charge par l'hôte sélectionné sont affichées.

6. Cliquez sur **Mettre à jour > Mettre à jour l'hôte** dans la barre d'outils.



Une boîte de dialogue s'affiche avec des informations sur la mise à jour sélectionnée.
Cliquez sur **Commencer la mise à jour**.



La colonne **État** vous indique ce qui se passe dans chacune des phases suivantes de la mise à jour :

- Phase 1 - **Téléchargement des packages de mises à jour** -Télécharge les artéfacts du référentiel sur le Serveur NW applicable aux services sur l'hôte que vous avez choisi.
- Phase 2 - **Configuration des packages de mise à jour** -Configure les fichiers de mise à jour au format approprié.
- Phase 3 - **Mise à jour en cours** - Met l'hôte à jour vers la nouvelle version.

7. Lorsque vous voyez **Mise à jour en cours d'exécution**, actualisez le navigateur.
   Cela peut vous envoyer vers l'écran de connexion NetWitness. Si cela se produit, connectez-vous et revenez à la vue Hôte.
   Une fois l'hôte mis à jour, NetWitness Suite vous invite à **Redémarrer l'hôte**.
8. Cliquez sur **Redémarrer l'hôte** dans la barre d'outils.
   NetWitness Suiteindique l'état **Redémarrage...** jusqu'à ce que l'hôte soit de nouveau en

ligne. Une fois que l'hôte est de nouveau en ligne, l'**État** affiche **À jour**. Contactez le support client si l'hôte ne revient pas en ligne.

Remarque : si vous avez activé DISA STIG, l'ouverture des services de base peut prendre environ 5 à 10 minutes. Ce délai est dû à la génération de nouveaux certificats.

Appliquer les mises à jour à partir de la ligne de commande (sans accès Web)

Si votre déploiement de RSA NetWitness Suite n'a pas d'accès Web, exécutez la procédure suivante pour appliquer une mise à jour de version.

Remarque : Dans la procédure suivante, la version 11.1.0.0 est la version utilisée comme exemple dans les chaînes de code.

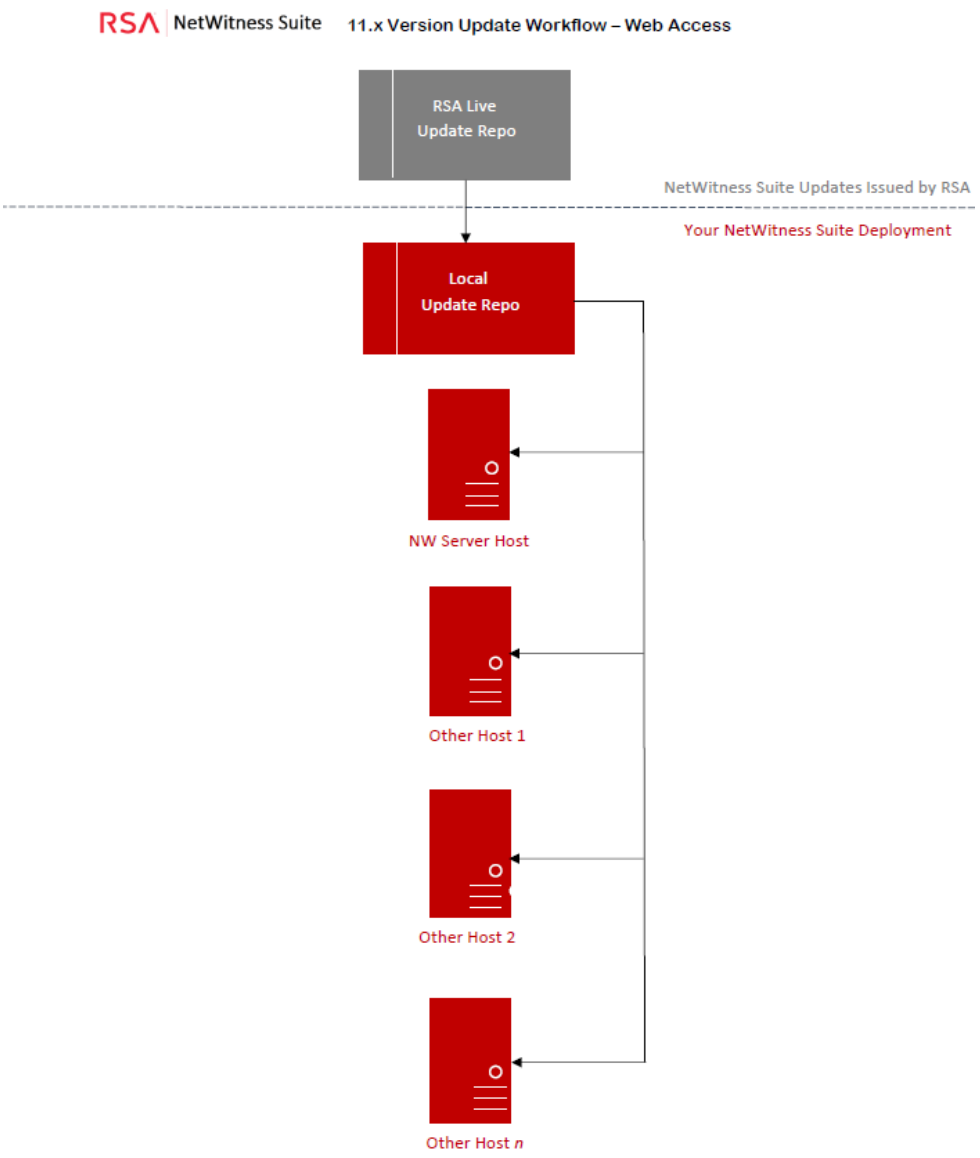
1. Téléchargez le package de mise à jour `.zip` pour la version souhaitée (par exemple, `netwitness-11.1.0.0.zip`) à partir de RSA Link vers un répertoire local.
2. Ouvrez une session SSH sur l'hôte du serveur NW.
3. Créez un répertoire intermédiaire `tmp/upgrade/<version>` pour la version que vous souhaitez (par exemple, `tmp/upgrade/11.1.0.0`).
   ```
   mkdir -p /tmp/upgrade/11.1.0.0
   ```
4. Décompressez le package dans le répertoire temporaire que vous avez créé (par exemple, `tmp/upgrade/11.1.0.0`).
   ```
   cd /tmp/upgrade/11.1.0.0
   unzip /tmp/upgrade/11.1.0.0/netwitness-11.1.0.0.zip
   ```
5. Initialisez la mise à jour sur le serveur NW.
   ```
   upgrade-cli-client --init --version 11.1.0.0 --stage-dir
   /tmp/upgrade/
   ```
6. Appliquez la mise à jour au serveur NW.
   ```
   upgrade-cli-client --upgrade --host-addr <NW Server IP> --version
   11.1.0.0
   ```
7. Connectez-vous à NetWitness Suite et redémarrez l'hôte du Serveur NW dans la vue Hôte.
8. Appliquez la mise à jour à chaque hôte du serveur NW.
   ```
   upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> -
   -version 11.1.0.0
   ```
   La mise à jour est terminée lorsque l'interrogation est terminée.

9. Connectez-vous à NetWitness Suite et redémarrez l'hôte dans la vue Hôte.
   Vous pouvez vérifier la version appliquée à l'hôte avec la commande suivante :
   `upgrade-cli-client --list`

Renseigner le référentiel de mises à jour local

NetWitness Suite envoie les mises à jour de version dans le référentiel des mises à jour local à partir du référentiel Live Update. L'accès au référentiel de mises à jour Live Update nécessite et utilise les informations d'identification du compte Live configurées sous **ADMIN > SYSTÈME > Live**. En outre, vous devez cocher la case `Automatically download information about new updates every day` sous **ADMIN > SYSTÈME > Mises à jour** pour renseigner le référentiel local tous les jours.

Le schéma suivant illustre le mode d'obtention des mises à jour de version si votre déploiement NetWitness Suite dispose d'un accès au Web.



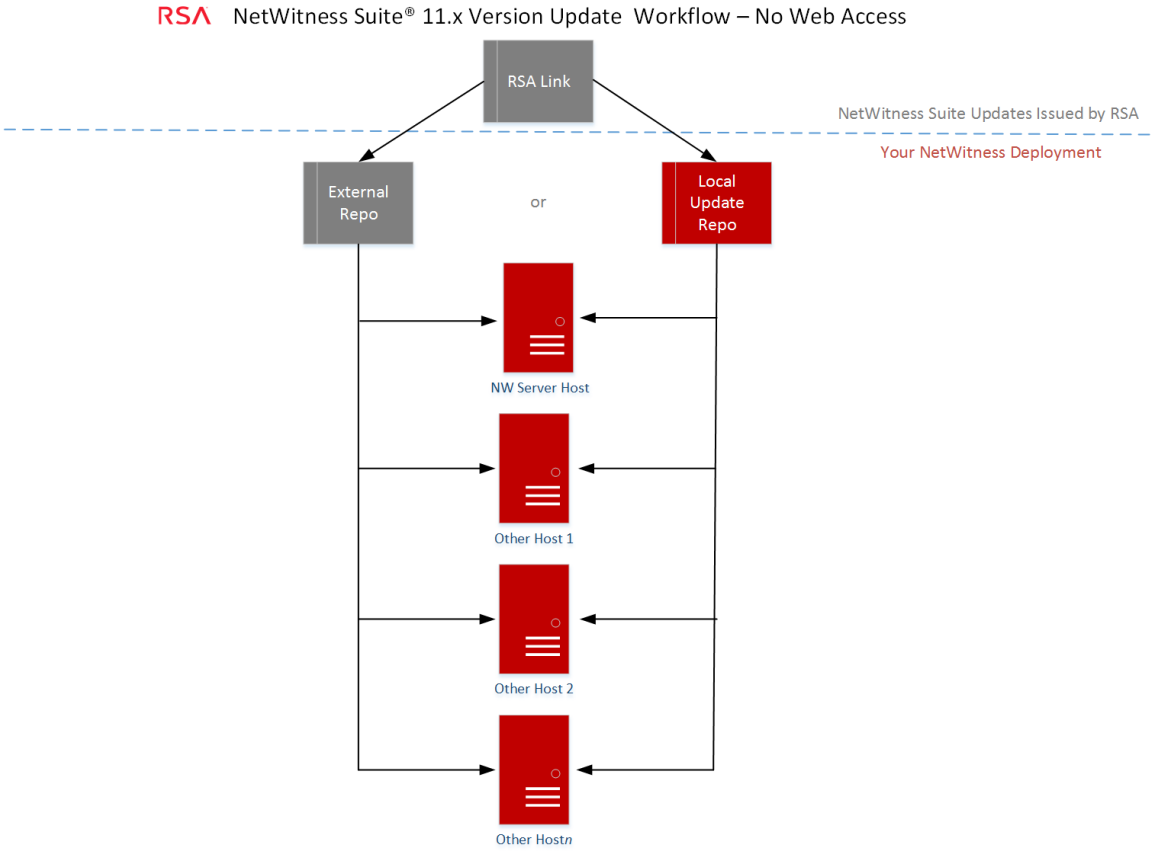
Remarque : Lorsque vous établissez la connexion initiale avec le référentiel Live Update, vous avez accès à tous les packages du système CentOS 7 et aux packages de production RSA. Ce téléchargement de plus de 2,5 Go de données nécessitera une durée indéterminée en fonction de la connexion Internet de votre serveur NW et du trafic du référentiel RSA. Il n'est pas obligatoire d'utiliser le référentiel Live Update. Vous pouvez également utiliser un référentiel externe, comme décrit dans la section « Configurer un référentiel externe ».

Pour vous connecter au référentiel Live Update, accédez à la vue **ADMIN > SYSTÈME**, sélectionnez **Live** dans le panneau d'options et assurez-vous que les informations d'identification sont configurées (le voyant de **connexion** doit être vert). S'il n'est pas vert, cliquez sur **Démarrer la session** et connectez-vous.

Remarque : Si vous devez utiliser le serveur proxy pour accéder au référentiel Live Update, vous pouvez configurer l'hôte proxy, le nom d'utilisateur proxy et le mot de passe du proxy. Reportez-vous à la section « Configurer un serveur proxy pourNetWitness Suite » dans le *Guide de configuration du système NetWitness Suite 1.1*.Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Reportez-vous à la section « Appliquer les mises à jour à partir de la ligne de commande » si votre déploiement NetWitness Suite n'a pas accès au Web.

Le schéma suivant illustre le mode d'obtention des mises à jour de version si votre déploiement NetWitness Suite ne dispose pas d'un accès au Web.



Configurer un référentiel externe avec RSA et les mises à jour du système d'exploitation

Remarque : Dans la procédure suivante, la version 11.1.0.0 est la version utilisée comme exemple dans les chaînes de code.

Exécutez la procédure suivante pour configurer un référentiel externe (référentiel).

Remarque : 1.) Pour effectuer cette procédure, un utilitaire de décompression doit être installé sur l'hôte. 2.) Vous devez savoir comment créer un serveur Web avant d'effectuer la procédure suivante.

1. (Conditionnel) Effectuez cette étape si vous disposez d'un référentiel externe et que vous souhaitez le remplacer.
   - Exemple 1 : Vous avez démarré l'hôte à partir d'un référentiel externe et vous souhaitez effectuer une mise à niveau à l'aide d'un référentiel local sur le serveur Admin.
     a. Créez le fichier `/etc/netwitness/platform/repobase`.
        `vi /etc/platform/netwitness/repobase`
     b. Modifiez le fichier `repobase` de sorte que la seule information dans le fichier est l'URL suivante.
        `https://nw-node-zero/nwrpmrepo`
     c. Suivez les instructions sur l'exécution de la mise à niveau à l'aide de l'outil `upgrade-cli-client .`
        Reportez-vous aux instructions.
   - Exemple 2 : Vous avez démarré l'hôte à partir du référentiel local sur le serveur Admin (hôte du serveur NW) et vous souhaitez utiliser un référentiel externe pour la mise à niveau.
     a. Créez le fichier `/etc/netwitness/platform/repobase`.
        `vi /etc/platform/netwitness/repobase`
     b. Modifiez le fichier `repobase` de sorte que la seule information dans le fichier est l'URL suivante.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Suivez les instructions sur l'exécution de la mise à niveau à l'aide de l'outil `upgrade-cli-client`.
        Les instructions figurent dans la rubrique « Appliquer les mises à jour à partir de la ligne de commande ».
2. Configurez le référentiel externe.
   a. Connexion à l'hôte du serveur Web
   b. Créez le répertoire destiné à héberger le référentiel NW (`netwitness-11.1.0.0.zip`), par exemple `ziprepo`, sous `web-root` sur le serveur Web. Par exemple, /var/netwitness est la racine Web, soumettez la chaîne de commande suivante.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`

c. Créez le répertoire 11.1.0.0 sous `/var/netwitness/<your-zip-file-repo>`.
```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0
```

d. Créez les répertoires `OS` et `RSA` sous `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

e. Décompressez le fichier `netwitness-11.1.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
```
unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0
```
La décompression de `netwitness-11.1.0.0.zip` résulte en deux fichiers zip (`OS-11.1.0.0.zip` et `RSA-11.1.0.0.zip`) et d'autres fichiers.

f. Décompressez le fichier :

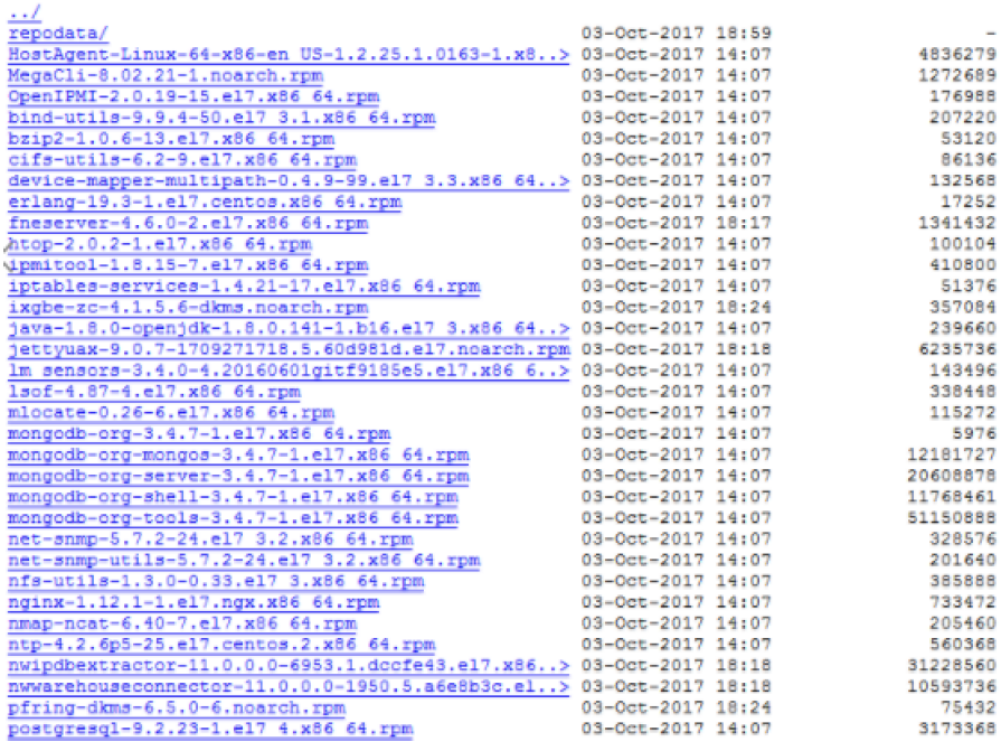
1. `OS-11.1.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`.
```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS
```
L'exemple suivant illustre la façon dont la structure de fichiers du système d'exploitation (OS) s'affiche une fois que vous décompressez le fichier.

../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

2. `RSA-11.1.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`.
```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-
```

repo>/11.1.0.0/RSA

L'exemple suivant illustre l'affichage de la structure du fichier de mise à jour de la version de RSA après décompression du fichier.



../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

L'URL externe pour le référentiel est `http://<web server IP address>/<your-zip-file-repo>`.

g. (Conditionnel - Pour Azure) Procédez comme suit pour mettre à jour Azure

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

ii. `unzip nw-azure-11.1-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`

iv. `createrepo .`

h. Utilisez `http://<web server IP address>/<your-zip-file-repo>` en réponse à l'invite **Entrez l'URL de base des référentiels de mises à jour externes** émanant du programme d'installation NW 11.1.0.0 (`nwsetup-tui`).

Créer et gérer des groupes d'hôtes

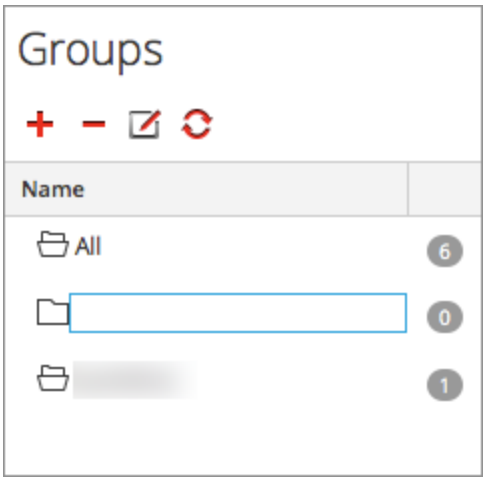
La vue Hôtes fournit les options permettant de créer et de gérer les groupes d'hôtes. La barre d'outils du panneau Groupes inclut les options de création, de modification et de suppression des groupes d'hôtes. Lorsque les groupes sont créés, vous pouvez faire glisser des hôtes individuels du panneau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

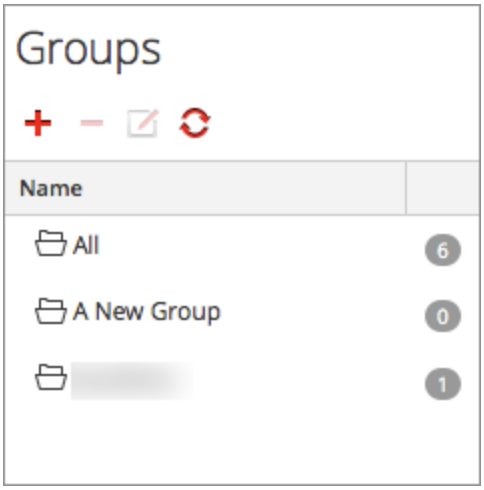
Créer un groupe

1. Sélectionnez **Admin** > **Hôtes**.
   La vue Hôtes s'affiche.
2. Dans la barre d'outils du volet **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 contenus dans ce groupe.



Modifier le nom d'un groupe

1. Dans la vue Hôtes, volet **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**.

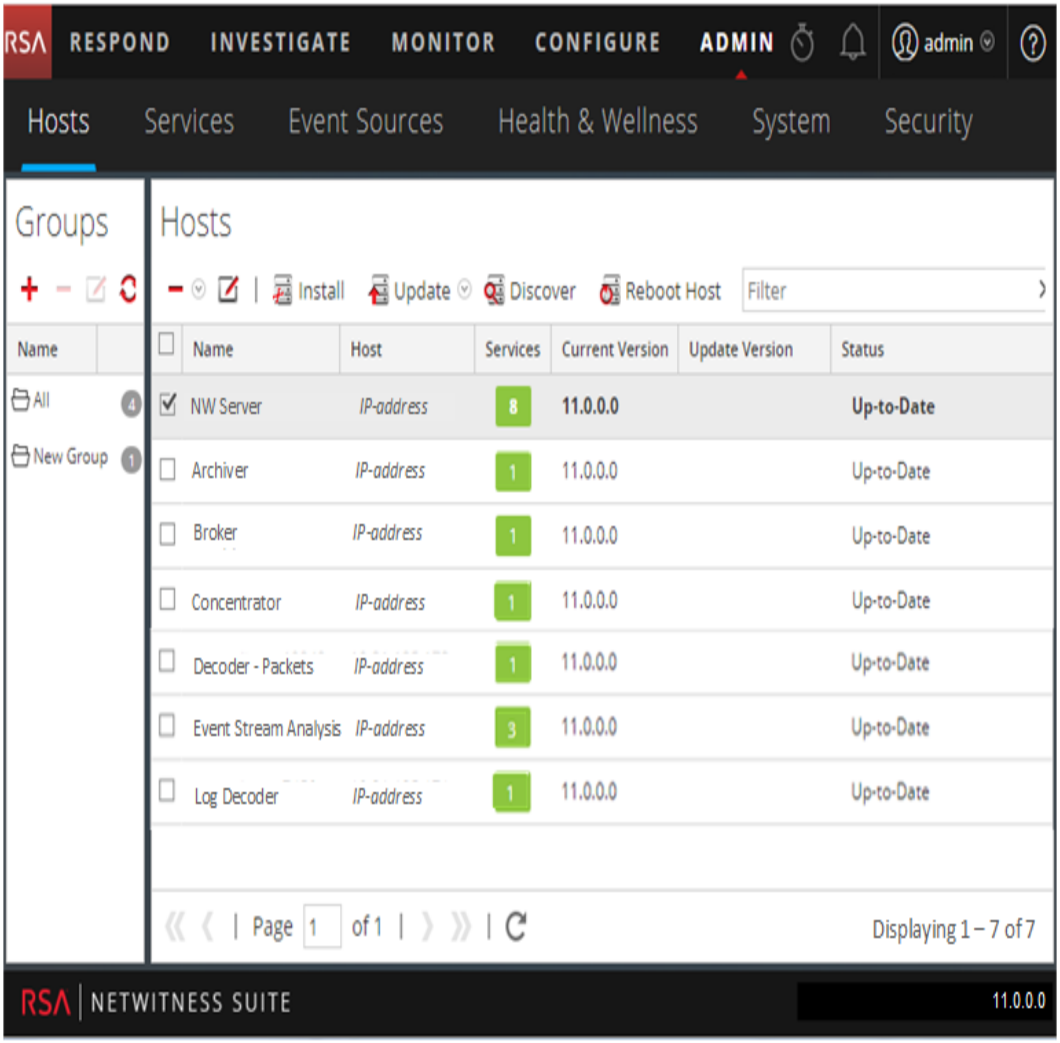
   Le champ du nom se ferme et le nouveau nom de groupe s'affiche dans l'arborescence.

Ajouter un hôte à un groupe

Dans la vue Hôtes, panneau **Hôtes**, sélectionnez un hôte et faites-le glisser vers un dossier de groupe dans le panneau Groupes.
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.



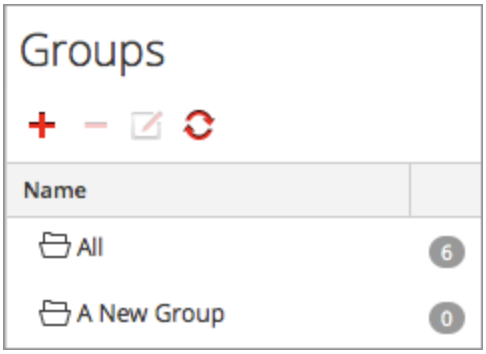
Supprimer un hôte d'un groupe

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 dugroupe**.

   Les hôtes sélectionnés sont supprimés du groupe, mais ne sont pas retirés de l'interface utilisateur NetWitness Suite. 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 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 supprimés de l'interface utilisateur de NetWitness Suite. Le groupe **Tout** contient les hôtes du groupe supprimé.

Rechercher des hôtes

Vous pouvez rechercher des hôtes dans une liste d'hôtes dans la vue Hôtes. 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 NetWitness Suite 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, vous pouvez rechercher un service et trouver rapidement l'hôte qui exécute ce service.

Rechercher un hôte

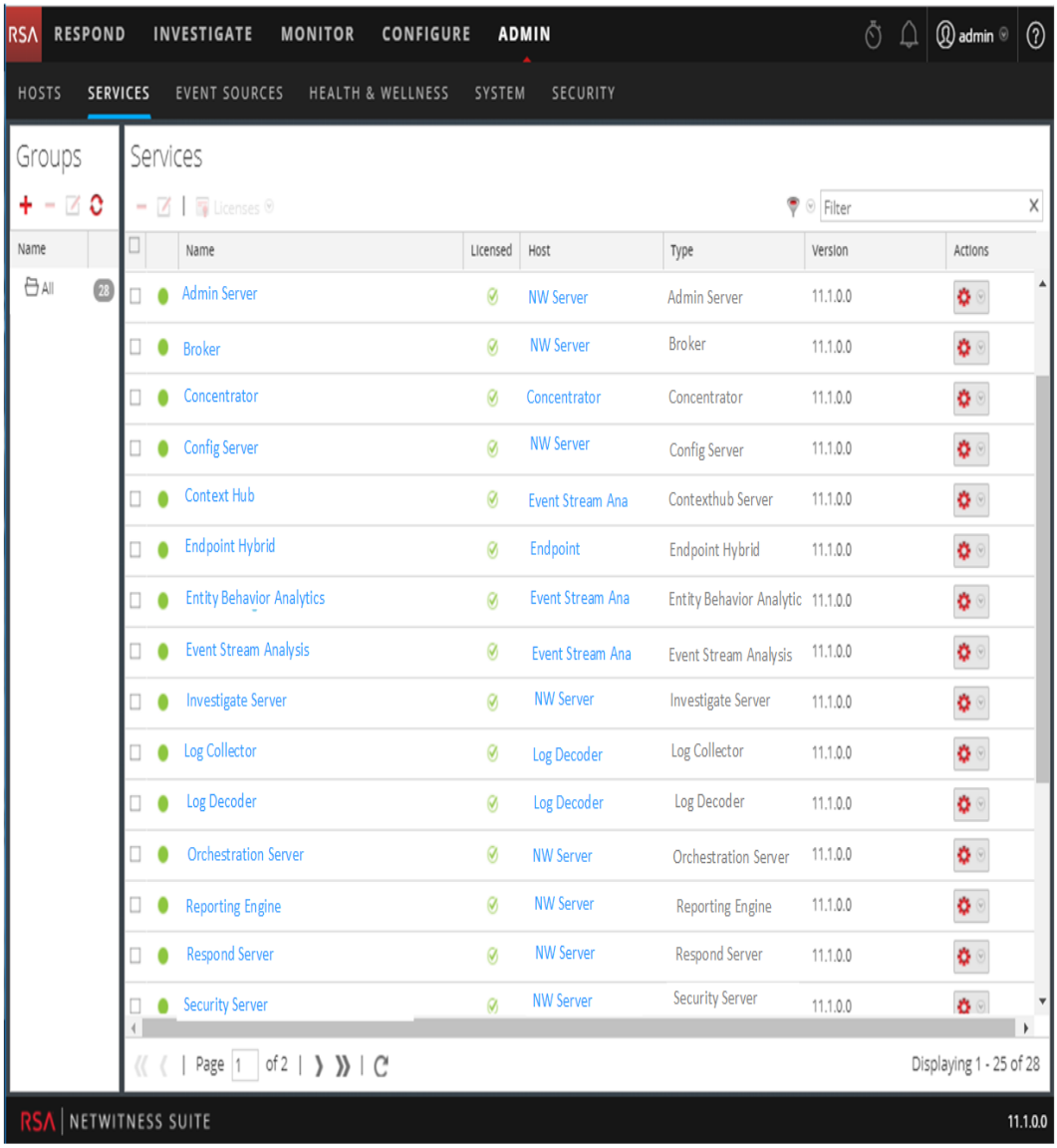
1. Sélectionnez **ADMIN** > **Hôtes**.
2. Dans la barre d'outils du panneau **Hôtes**, saisissez un **Nom** d'hôte ou **Nom d'hôte** dans le champ **Filtre**.

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

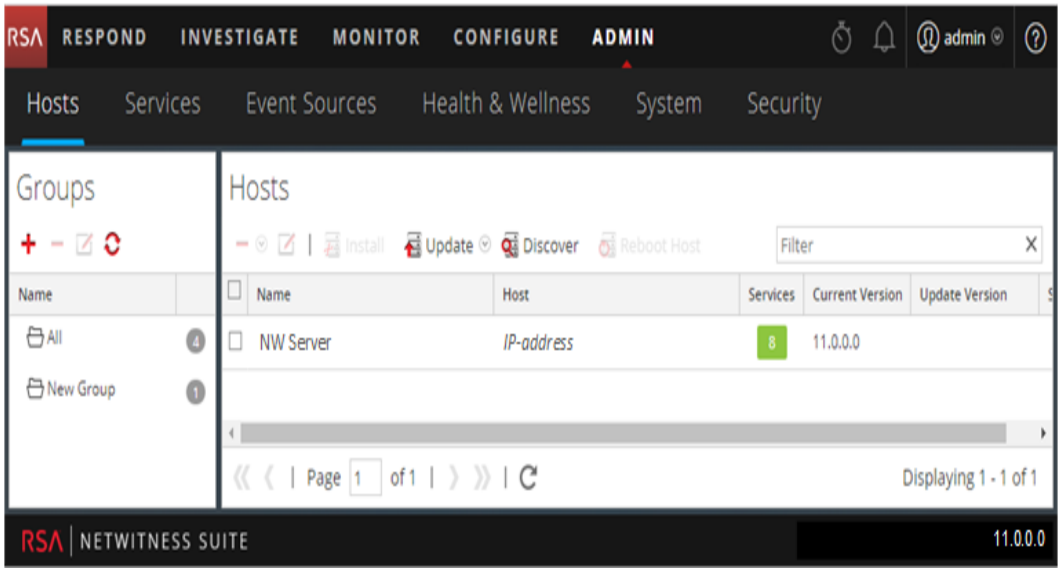
Rechercher l'hôte qui exécute un service

1. Sélectionnez **Admin > Services**.
2. Dans la vue Services, sélectionnez un service. L'hôte associé est répertorié dans la colonne **Hôte** pour ce service.



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

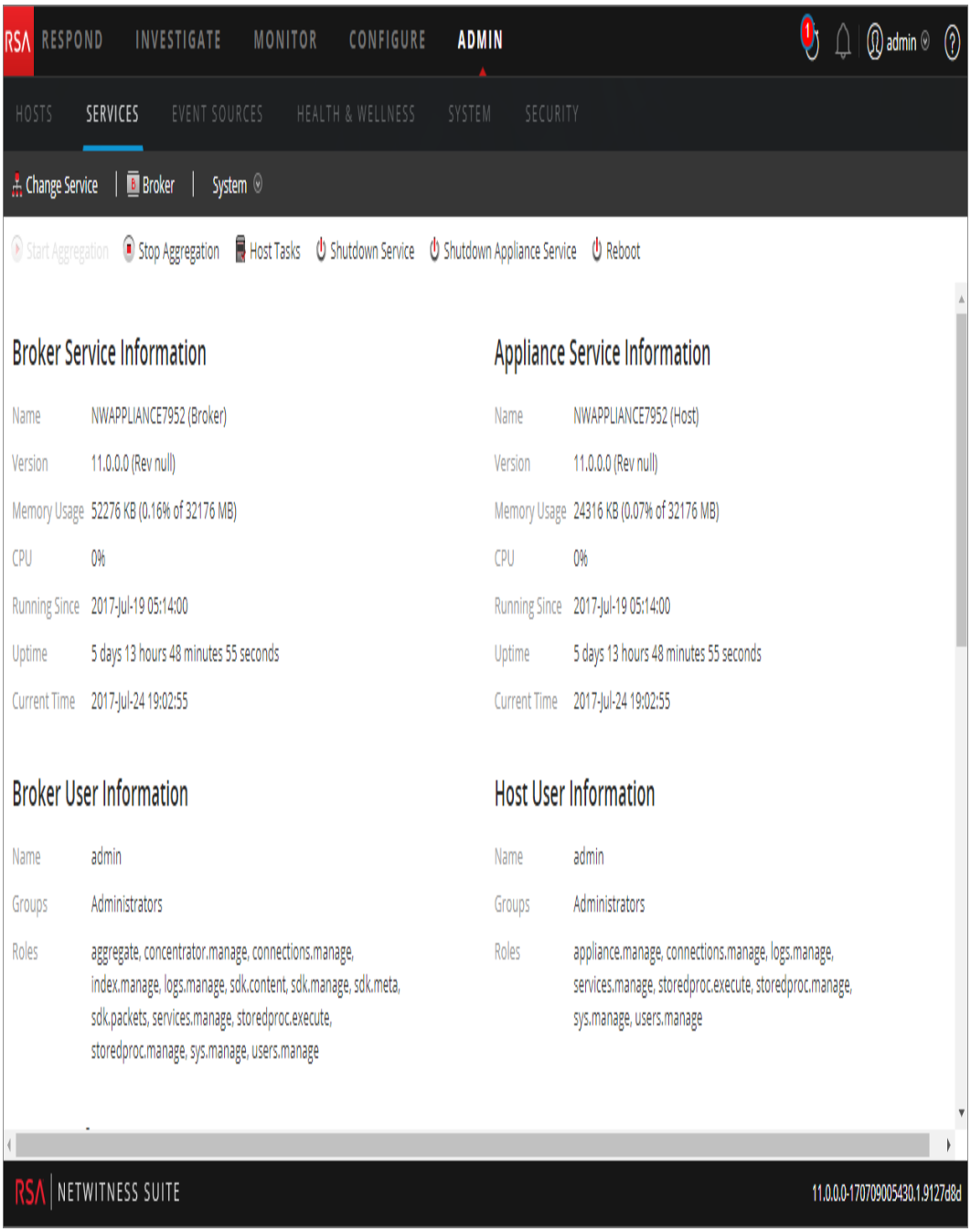
Hôtes.



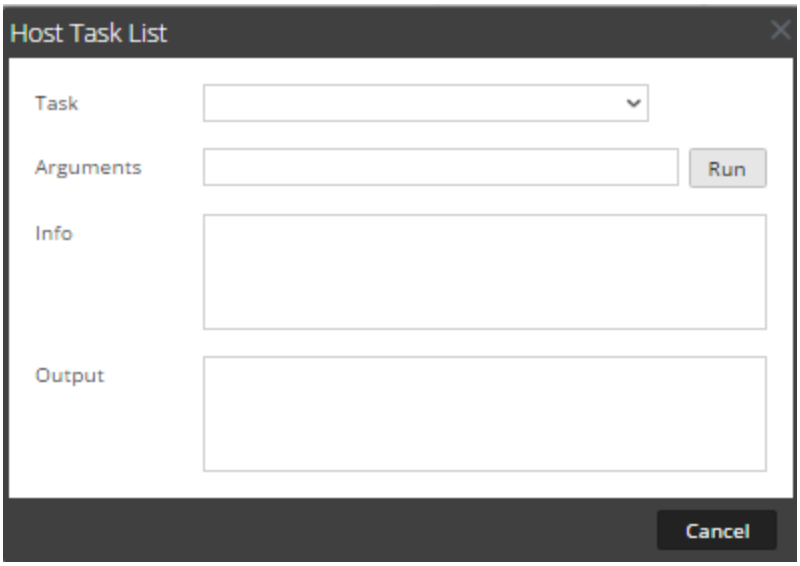
Exécuter une tâche à partir de la Liste des tâches de l'hôte

1. Sélectionnez **Admin > Services**.
2. Dans la grille **Services**, sélectionnez un service et > **Vue** > **Système**.

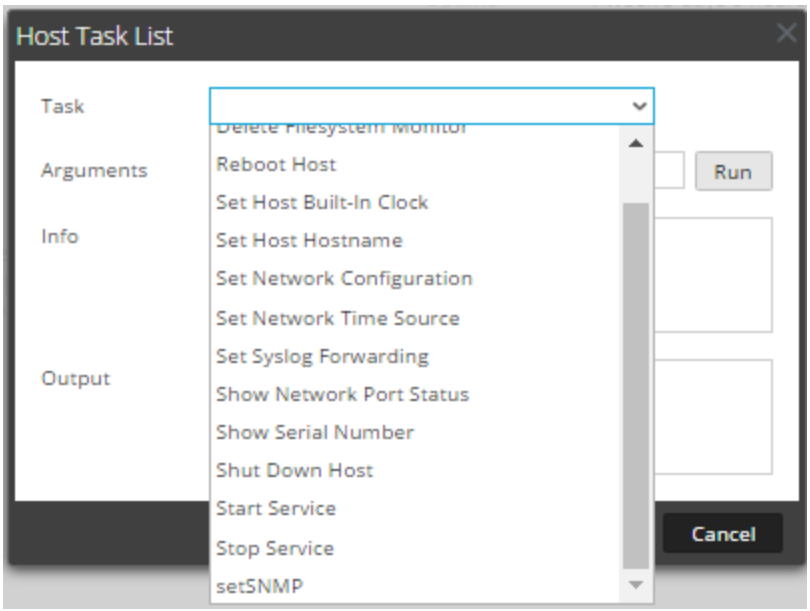
Remarque : Les services Admin, Config, Orchestration, Sécurité, Enquêter et Répondre ont accès à la vue Système. Ils ont uniquement accès à la vue Explorer.
La vue Système du service s'affiche.


RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN
admin
HOSTS SERVICES EVENT SOURCES HEALTH & WELLNESS SYSTEM SECURITY
Change Service | Broker | System
Start Aggregation Stop Aggregation Host Tasks Shutdown Service Shutdown Appliance Service Reboot
Broker Service Information
Name NWAPPLIANCE7952 (Broker)
Version 11.0.0.0 (Rev null)
Memory Usage 52276 KB (0.16% of 32176 MB)
CPU 0%
Running Since 2017-Jul-19 05:14:00
Uptime 5 days 13 hours 48 minutes 55 seconds
Current Time 2017-Jul-24 19:02:55
Appliance Service Information
Name NWAPPLIANCE7952 (Host)
Version 11.0.0.0 (Rev null)
Memory Usage 24316 KB (0.07% of 32176 MB)
CPU 0%
Running Since 2017-Jul-19 05:14:00
Uptime 5 days 13 hours 48 minutes 55 seconds
Current Time 2017-Jul-24 19:02:55
Broker User Information
Name admin
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
Host User Information
Name admin
Groups Administrators
Roles appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
RSA | NETWITNESS SUITE
11.0.0.0-170709005430.1.9127d8d

3. Dans la barre d'outils **Vue Système de services**, cliquez sur Host Tasks .

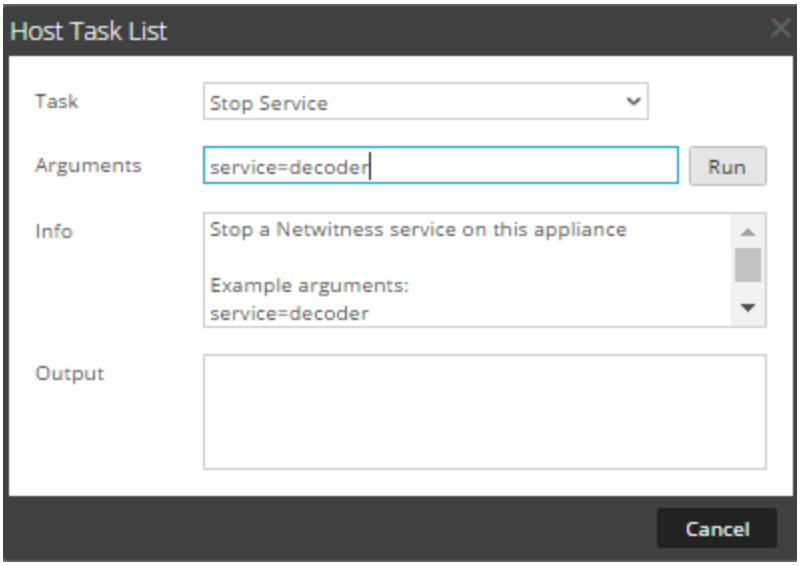


4. Dans la **Liste des tâches de l'hôte**, cliquez dans le champ **Tâche** pour afficher la liste déroulante des tâches qui s'exécutent sur un hôte.



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**.

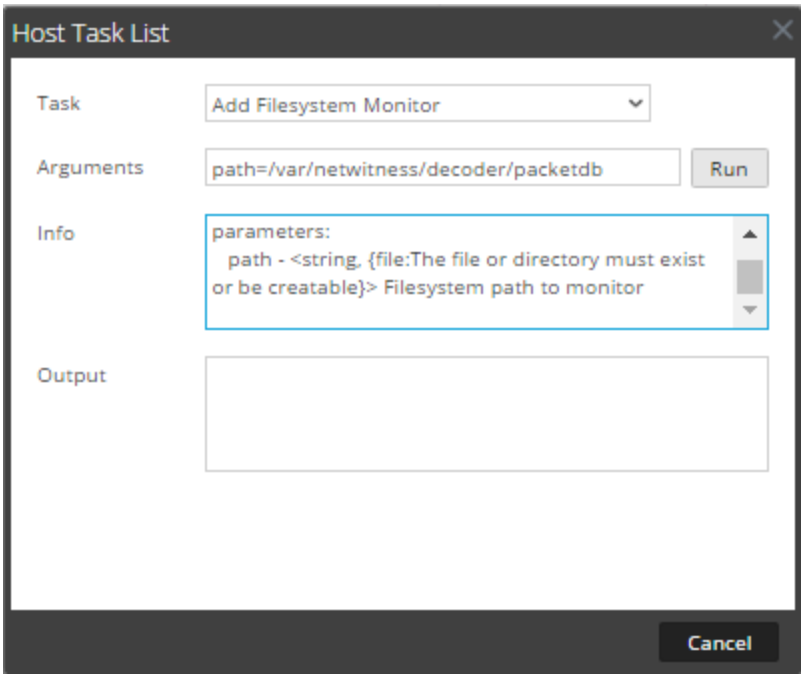
Ajouter et Supprimer le moniteur du système de fichiers

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. Sélectionnez **Admin** > **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, saisissez le chemin dans le champ **Arguments**. Par exemple :

path=/var/netwitness/decoder/packetdb

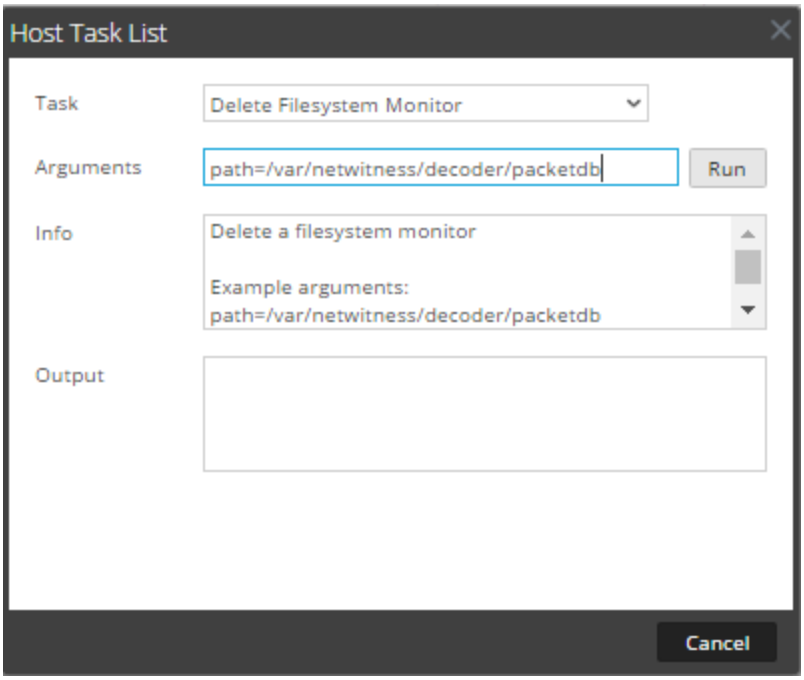


6. Cliquez sur **Exécuter**.
   Le résultat s'affiche dans la zone **Sortie**. Le service commence à surveiller le système de fichiers et continue à le faire jusqu'à ce que vous supprimiez la surveillance du système de fichiers.

Supprimer le moniteur du 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, saisissez 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 arrête la surveillance du système de fichiers.

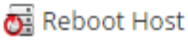
Redémarrer un hôte

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 Rechercher des hôtes), 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.

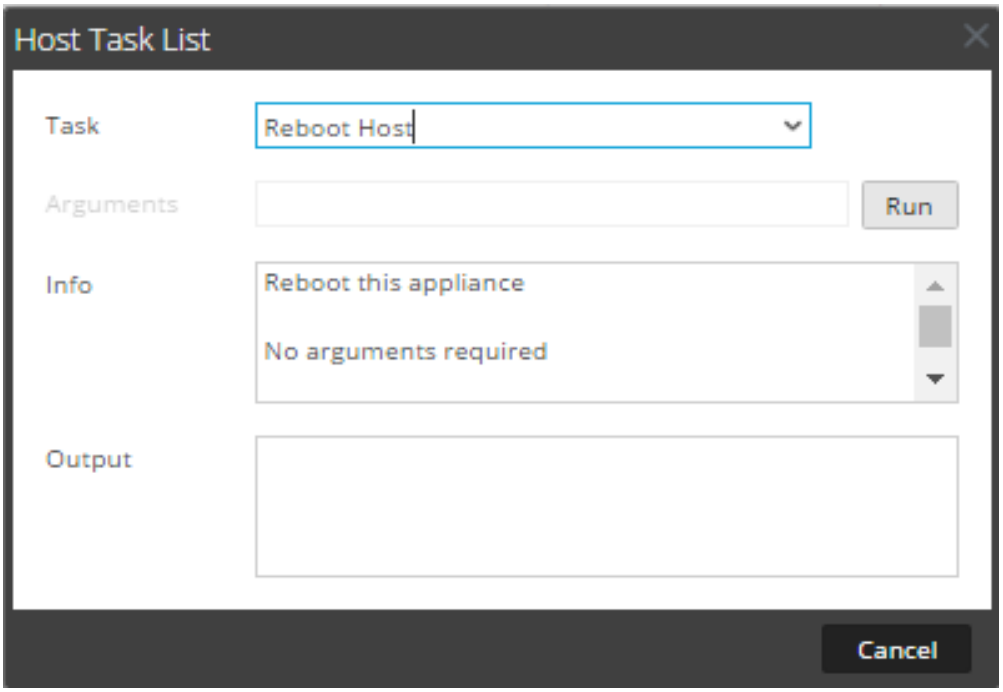
Arrêter et redémarrer un hôte à partir de la vue Hôtes

1. Sélectionnez **ADMIN > 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. Sélectionnez **Admin** > **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**.
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**.

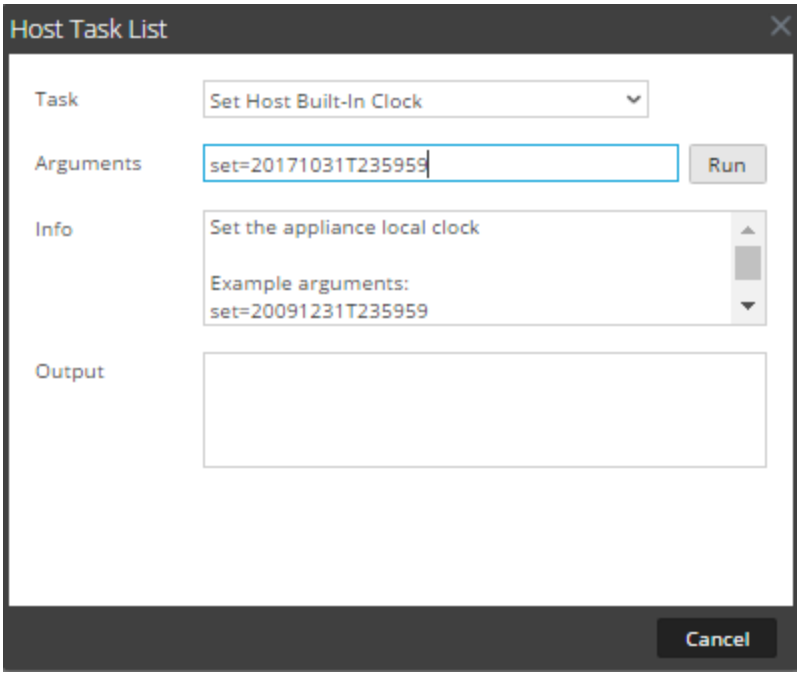
Paramétrer l'heure prédéfinie de l'hôte

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. Sélectionnez **Admin** > **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. Saisissez les arguments de date et d'heure dans le champ **Arguments**. Par exemple, pour spécifier 31 octobre 2017 à 23:59:59, saisissez :
   set=20171031T235959



6. Cliquez sur **Exécuter**.
   L'horloge est définie sur l'heure spécifiée et un message s'affiche dans la zone **Sortie**.

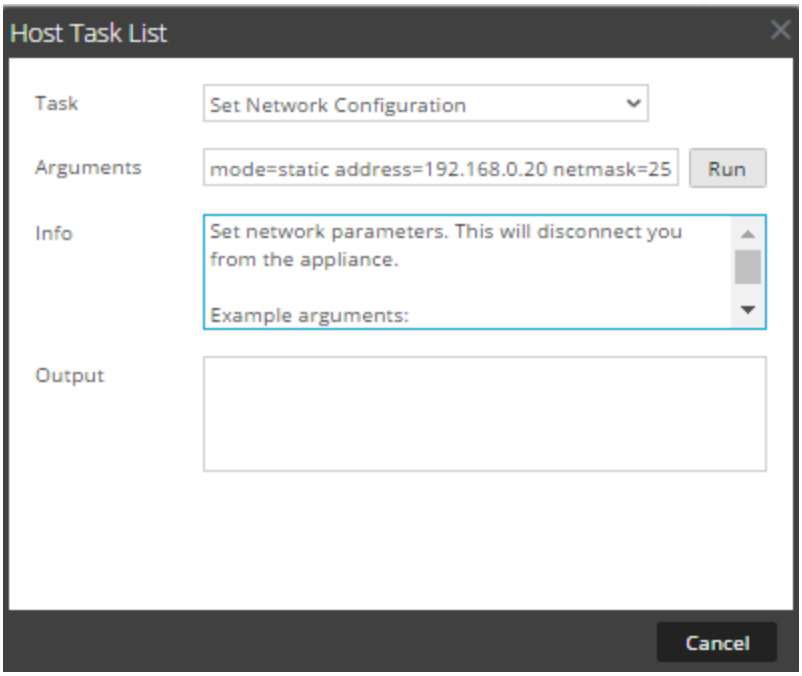
Définir la configuration réseau

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**.

Attention : 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. Sélectionnez **Admin > 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**.
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.

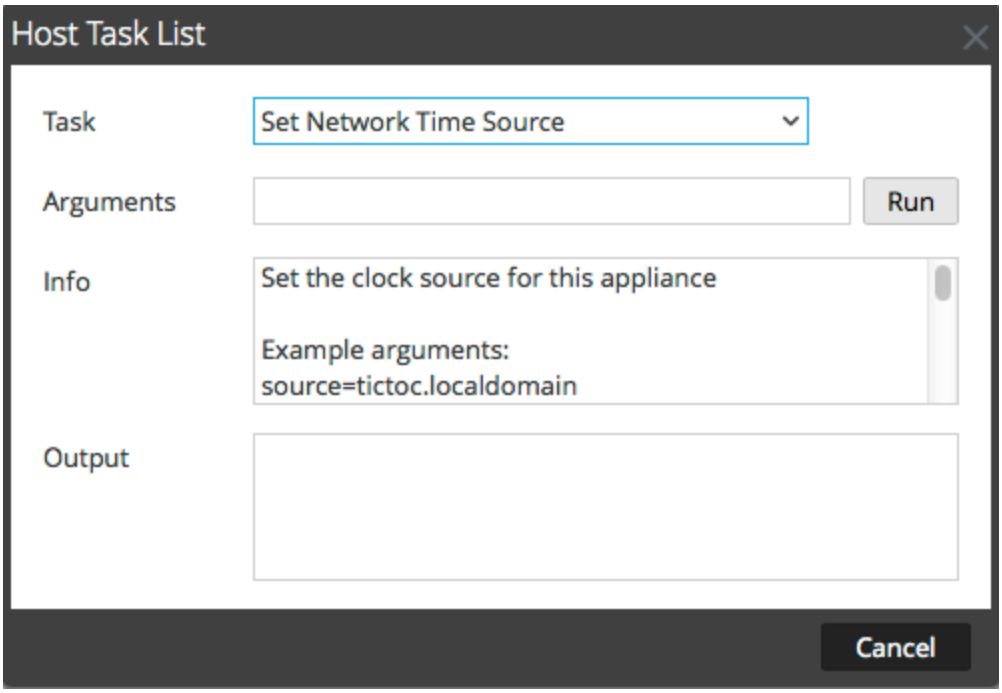
Remarque : Si vous choisissez le mode DHCP, il sera impossible de déterminer la nouvelle adresse. Il peut être nécessaire de se connecter à l'hôte directement pour déterminer la nouvelle adresse.

Définir la source de l'heure 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 de l'horloge réseau

1. Sélectionnez **Admin > 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 **Définir la source de l'heure 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**
6. Cliquez sur **Exécuter**.
   La source d'horloge est définie et un message s'affiche dans la zone **Sortie**.

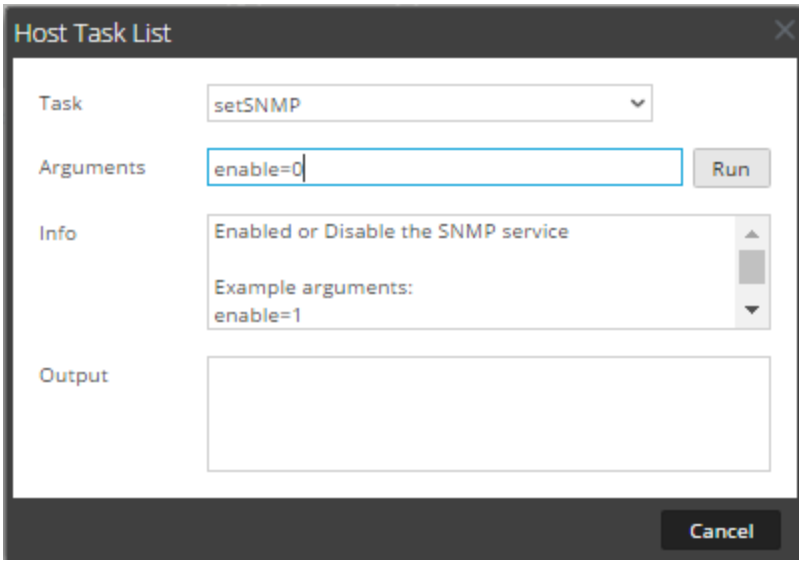
Remarque : Si vous avez spécifié une source d'horloge NTP **locale**, l'horloge hôte sert de source d'horloge et l'heure est configurée à l'aide de Paramétrer l'heure prédéfinie de l'hôte.

Configurer SNMP

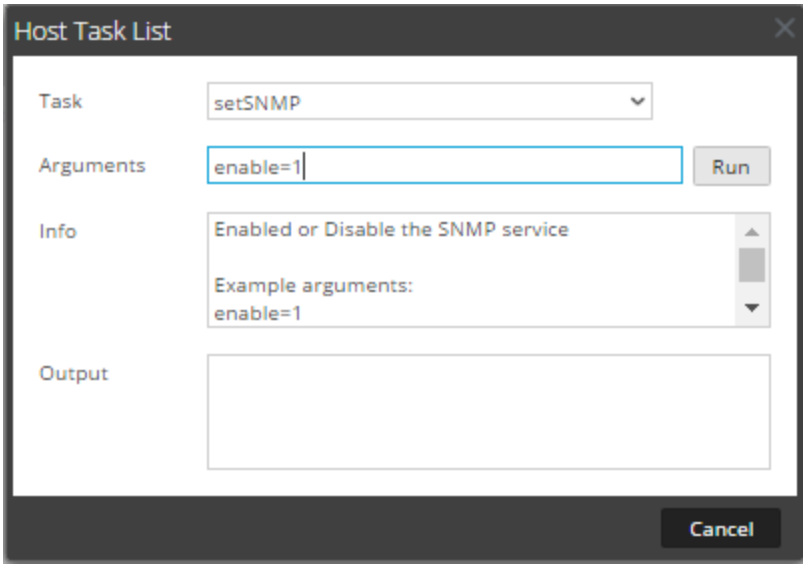
Dans la liste des tâches de l'hôte, l'option Configurer SNMP active ou désactive le service SNMP sur l'hôte. Pour qu'un hôte reçoive des notifications SNMP, le service SNMP doit être activé. Si vous n'utilisez pas SNMP pour les notifications NetWitness Suite, il n'est pas nécessaire d'activer le service.

Basculer le service SNMP sur l'hôte

1. Sélectionnez **Admin** > **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 **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**.



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

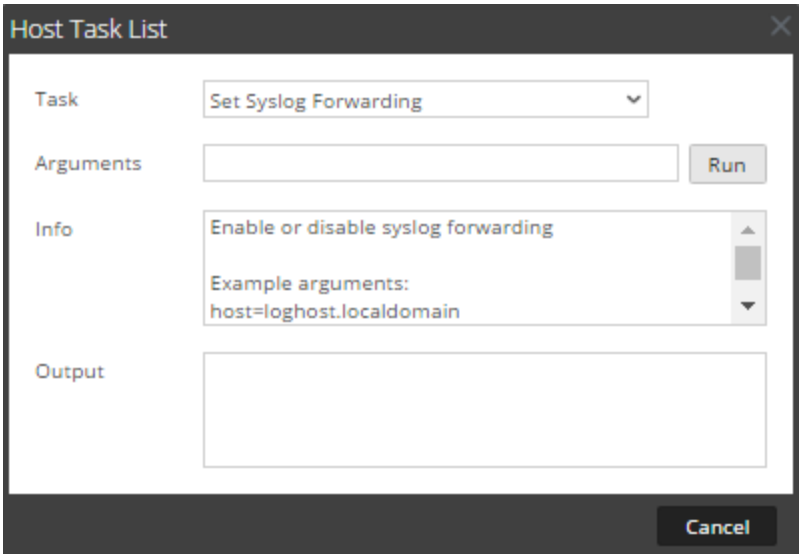
Définir le transfert Syslog

Vous pouvez configurer le transfert Syslog pour envoyer les logs du système d'exploitation de vos hôtes NetWitness Suite 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. Sélectionnez **Admin** > **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 **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).
     - **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.

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

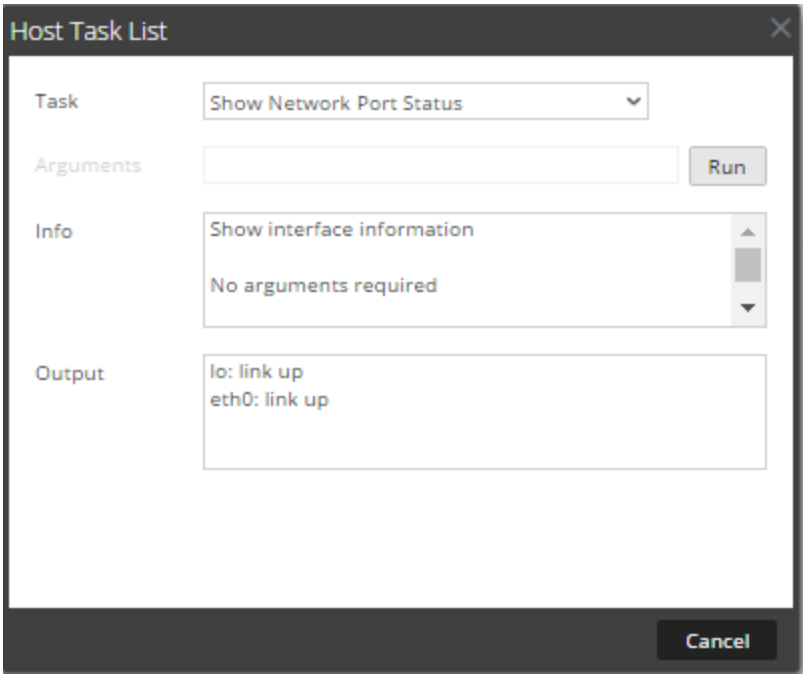
Afficher l'état du port réseau

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. Sélectionnez **Admin** > **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**.



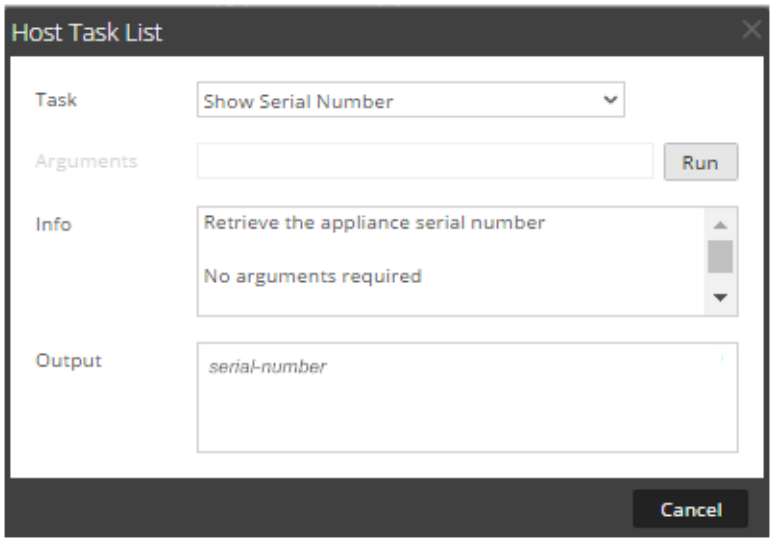
Afficher le numéro de série

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. Sélectionnez **Admin > 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** Afficher le numéro de série
   .Dans la zone **Info**, une brève explication de la tâche et des arguments de la tâche s'affiche.

5. 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**.



Arrêter l'hôte

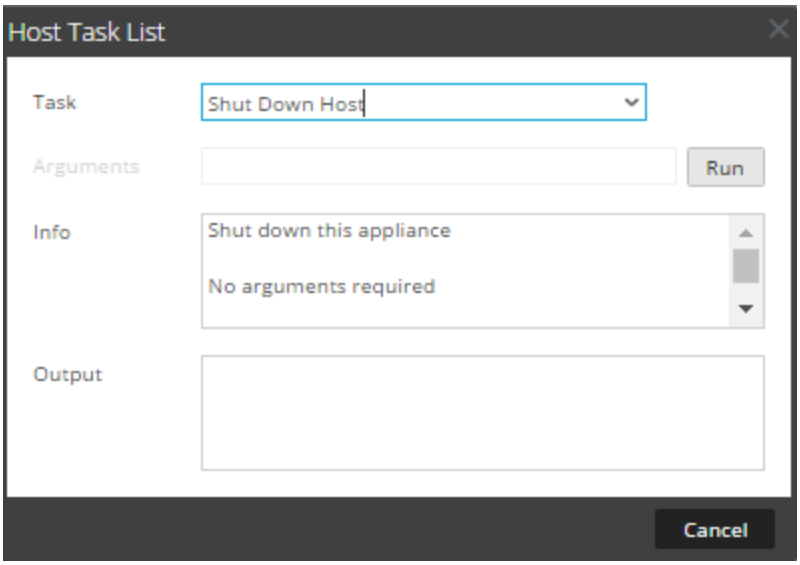
Dans certaines circonstances, par exemple lors d'une mise à niveau matérielle ou d'une coupure de courant prolongée dépassant la capacité électrique de secours, il peut être nécessaire d'arrêter un hôte physique. Lorsque vous arrêtez un hôte, tous les services exécutés sur cet hôte sont arrêtés et l'hôte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

Redémarrer un hôte pour démarrer et stopper un hôte sans l'arrêter complètement.

Arrêter l'hôte

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



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

Arrêter et démarrer un service sur un hôte

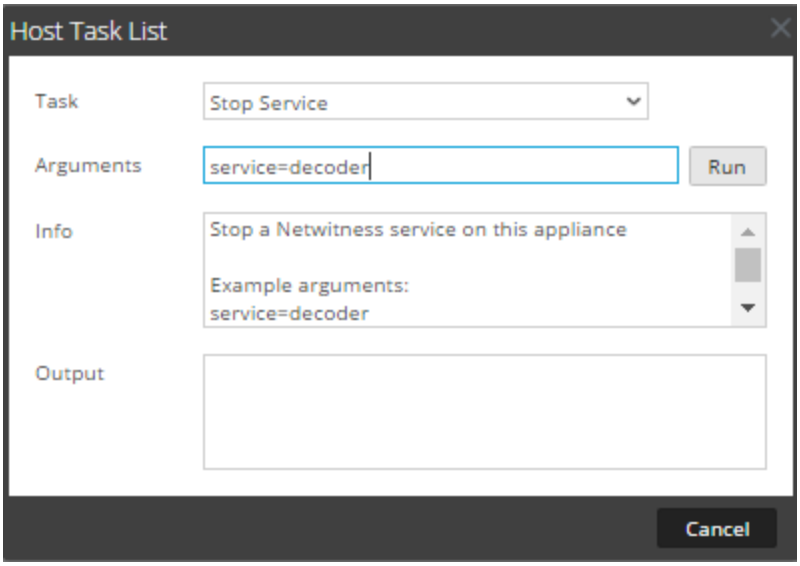
La liste des tâches de l'hôte comporte deux options pour arrêter et démarrer un service sur un hôte. Lorsque vous arrêtez un service à l'aide du message **Arrêter le service**, tous les processus s'y rapportant sont arrêtés et les utilisateurs connectés au service sont déconnectés. À moins d'un problème 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. Sélectionnez **Admin** > **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**.

5. Dans le champ **Arguments**, spécifiez le service (decoder, concentrator, broker, logdecoder, logcollector) à arrêter. Par exemple, **service=decoder**.

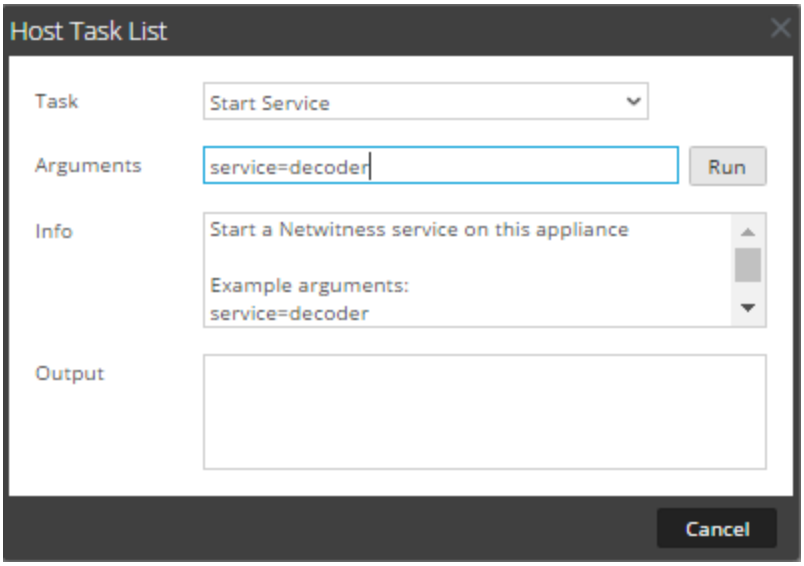


6. Pour exécuter la tâche, cliquez sur **Exécuter**.
   Le service s'arrête et l'état s'affiche dans la zone **Sortie**. Tous les processus du service sont arrêtés et les utilisateurs connectés au service en sont déconnectés. À moins d'un problème avec le service, il redémarre automatiquement.

Démarrer un service sur un hôte

1. Dans la liste déroulante **Liste des tâches de l'hôte**, sélectionnez **Démarrer le service** dans le menu déroulant Tâche.
   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**.

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

Remarque : Cette rubrique ne s'applique pas aux utilisateurs qui accèdent aux services via l'interface utilisateur sur Serveur NetWitness. Vous devez ajouter ces utilisateurs au système et non au service. Pour plus d'informations, consultez la section **Configuration d'un utilisateur** dans *Sécurité du système et gestion des utilisateurs*.

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 Changer 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 NetWitness Suite 10.5 ou ultérieur vers un service NetWitness Suite 10.4, Délai d'expiration 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 NetWitness Suite 10.4 vers un service NetWitness Suite 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

Procédures

ACCÉDER À LA VUE SÉCURITÉ

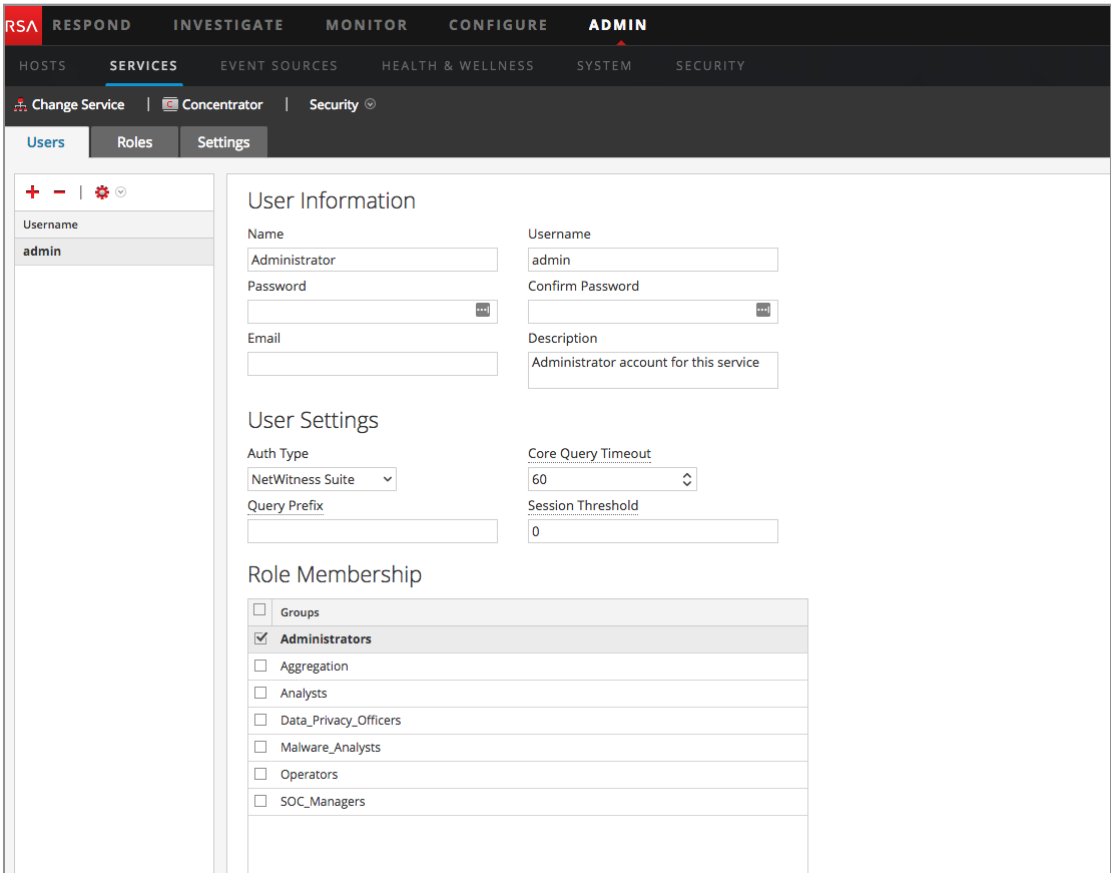
Chacune des procédures suivantes débute dans la vue Sécurité des services.

Pour accéder à la vue Sécurité des services :

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.

2. Sélectionnez un service, puis cliquez sur  > **Vue** > **Sécurité**.

   La vue Sécurité du service sélectionné s'affiche avec l'onglet Utilisateurs ouvert.



Remarque : Pour NetWitness Suite 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 Core**.

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 NetWitness Suite
- Adresse **e-mail**
- **Description** de l'utilisateur

5. Dans la section Paramètres utilisateur, procédez comme suit :
   - **Type d'authentification**
     - Si NetWitness Suite authentifie l'utilisateur, sélectionnez NetWitness.
     - Si Active Directory ou le module PAM est configuré sur le serveur Serveur NetWitness pour authentifier l'utilisateur, sélectionnez Externe.

Remarque : 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 Serveur NetWitness.

   - **Expiration du délai de requête Core** est le nombre maximal de minutes qu'un utilisateur peut utiliser pour exécuter une requête sur le service. Ce champ s'applique à NetWitness Suite 10.5 et versions de service supérieures et il ne s'affiche pas pour 10.4 et versions antérieures.

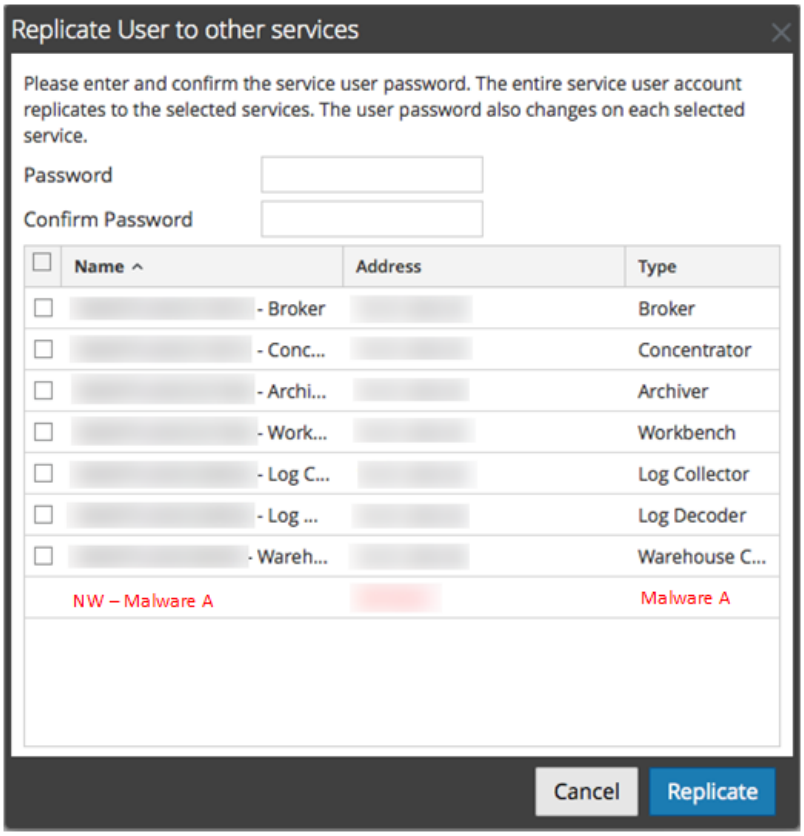
6. (Facultatif) Spécifier des critères de requête :
   - Le **Préfixe de requête** permet de filtrer les requêtes. Saisissez un préfixe pour restreindre les résultats visibles par l'utilisateur.
   - Le **Seuil de sessions** contrôle la façon dont le service analyse les métavaleurs pour déterminer le 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** et cliquez sur . NetWitness Suite demande de confirmer que vous souhaitez supprimer l'utilisateur sélectionné.
2. Pour confirmer, cliquez sur **Oui**.

L'utilisateur est supprimé du service immédiatement.

Ajouter un Rôle d'utilisateur de service

Dans NetWitness Suite, il existe des rôles préconfigurés qui 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 ni de session
Analystes	Accès au contenu méta et de session mais pas aux configurations
SOC_Managers (Responsables de SOC)	Même accès que les Analystes avec des autorisations supplémentaires pour gérer les incidents
Malware_Analysts (Analystes du malware)	Accès aux événements de malware et au contenu méta et de sessions
Data_Privacy_Officers (Responsables 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 Serveur NetWitness** 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 Junior Analysts au serveur, vous devez ajouter un rôle Junior Analysts sur chaque service auquel le rôle accédera. Pour plus d'informations, consultez la section **Ajouter un rôle et attribuer des autorisations** dans *Sécurité du système et gestion des utilisateurs*.

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.

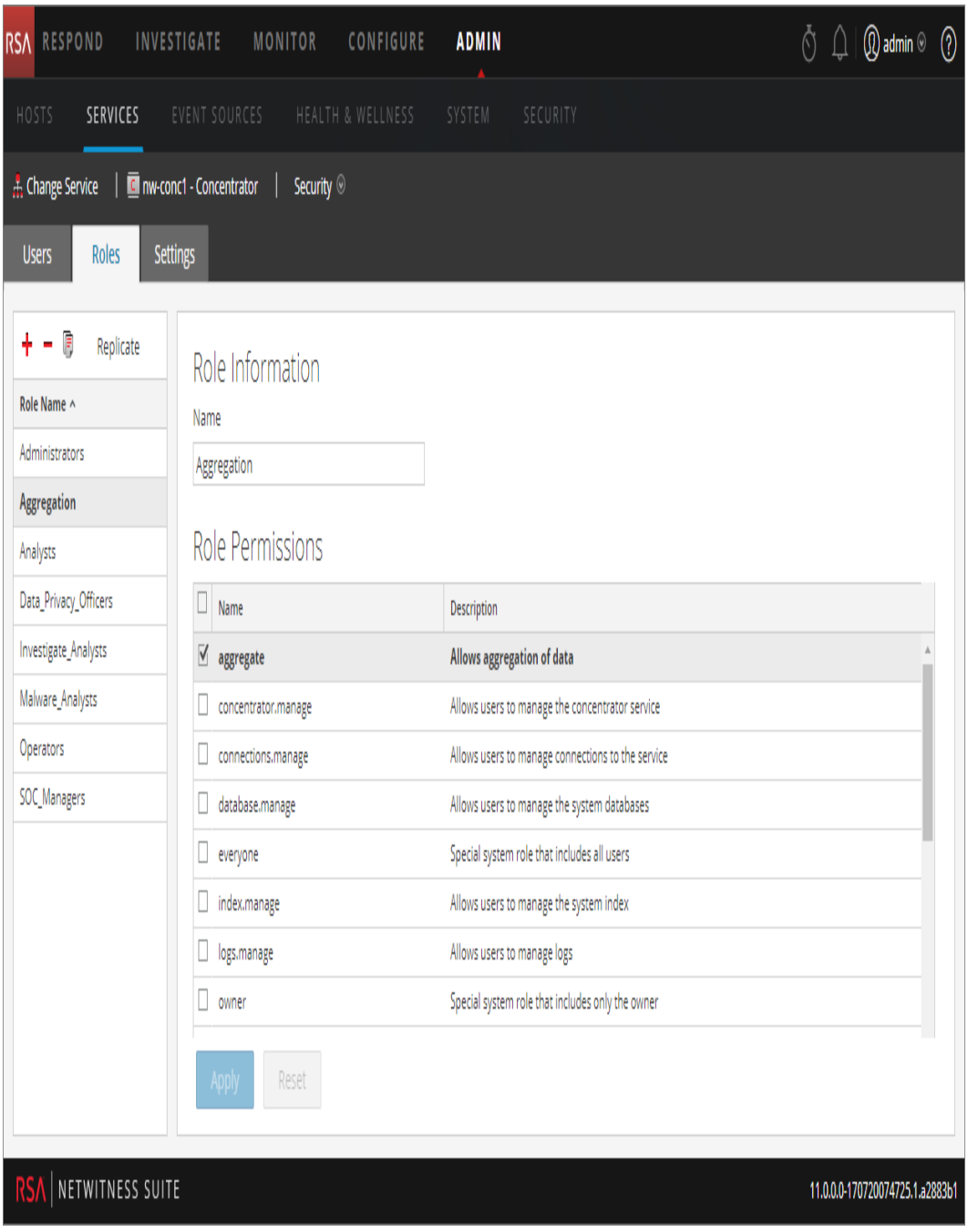
Procédure

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

1. Dans NetWitness Suite, accédez à **ADMIN > 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** et 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 **Autorisations du 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**.

Changer le mot de passe d'un utilisateur de service

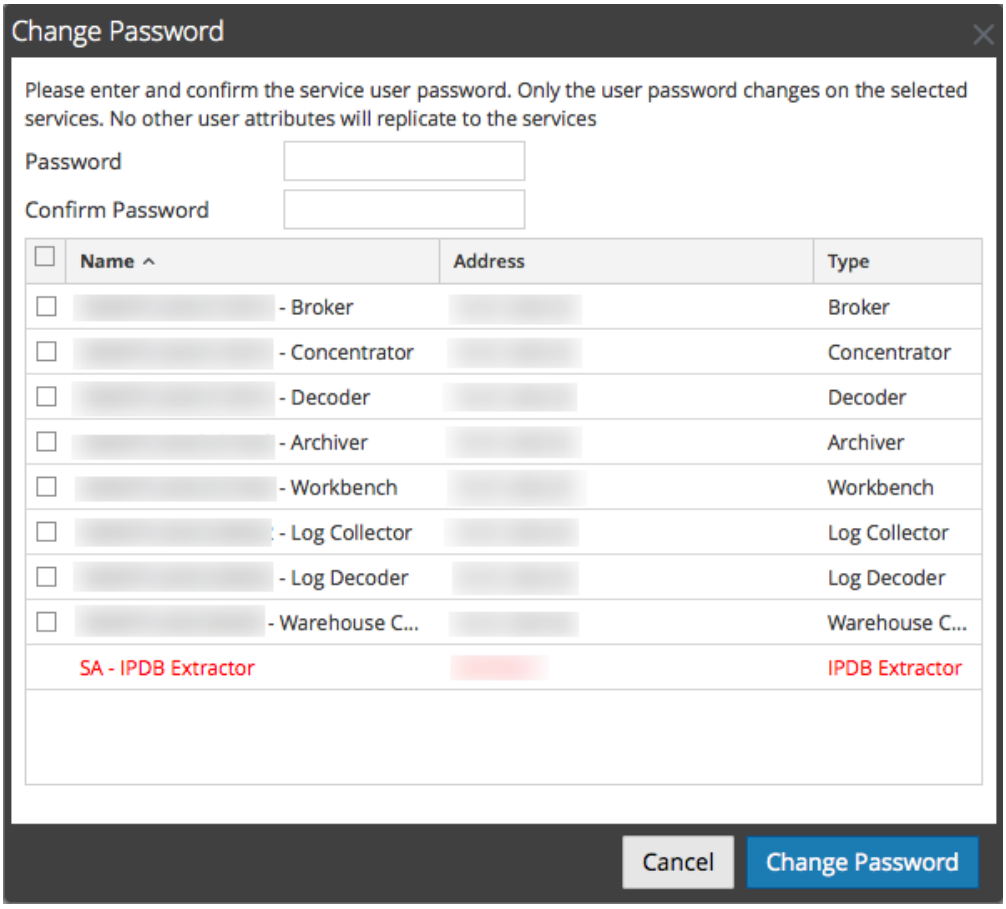
Cette procédure permet aux administrateurs de modifier le mot de passe d'un utilisateur de service et de répliquer le nouveau mot de passe sur tous les services principaux pour lesquels ce compte utilisateur est défini. Seule la modification du mot de passe est répliquée sur les services principaux sélectionnés.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

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

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

1. Dans NetWitness Suite, accédez à **ADMIN > 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.
3. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur et cliquez sur **Changer le mot de passe** à partir de l'icône Actions.

La boîte de dialogue **Changer 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 **Changer le mot de passe**.
   L'état de modification du mot de passe sur les services sélectionnés s'affiche.

Créer et gérer des groupes de services

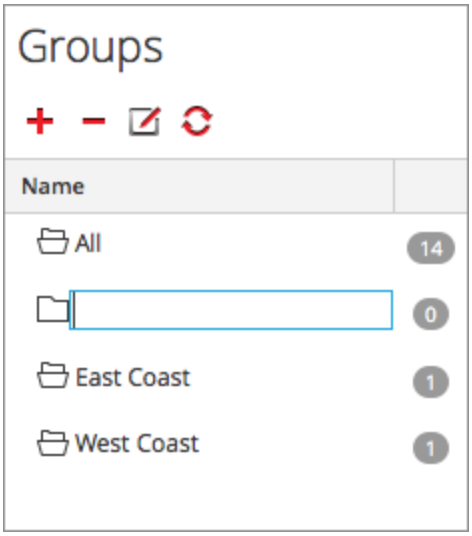
La vue Administration - Services fournit les options permettant de créer et de gérer les groupes de services. Le panneau Services inclut les options de création, de modification et de suppression des groupes de services. Lorsque les groupes sont créés, vous pouvez faire glisser des services individuels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

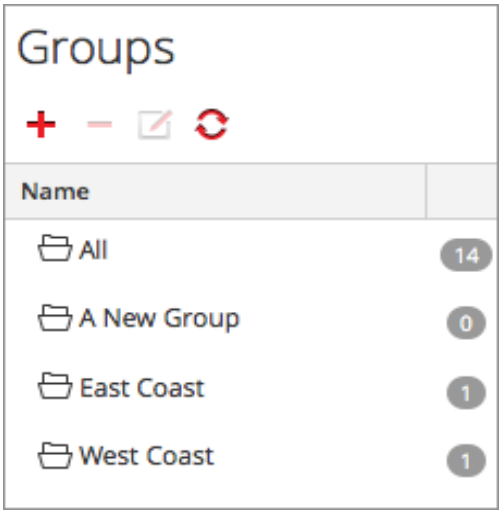
Créer un groupe

1. Dans NetWitness Suite, accédez à **ADMIN** > **Services**.
   La vue Services d'administration s'affiche.
2. Dans la barre d'outils du volet **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 contenus dans ce groupe.



Modifier le nom d'un groupe

1. Dans la vue **Services**, volet **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 faites-le glisser vers un dossier de groupe dans le panneau Groupes, par exemple **Log Collectors**.
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**.

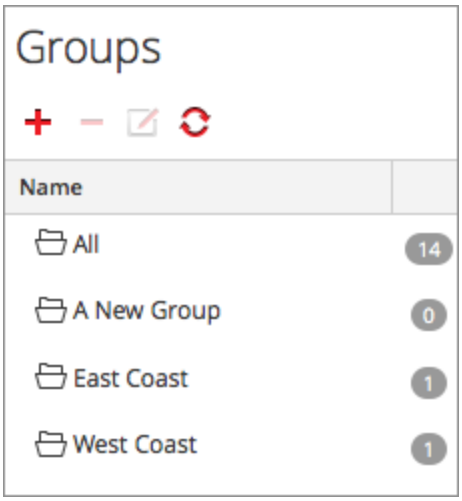
Le panneau **Services** affiche les services contenus dans ce groupe.

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.
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 NetWitness Suite. 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 supprimés de l'interface utilisateur de NetWitness Suite. Le groupe **Tout** contient les hôtes 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.

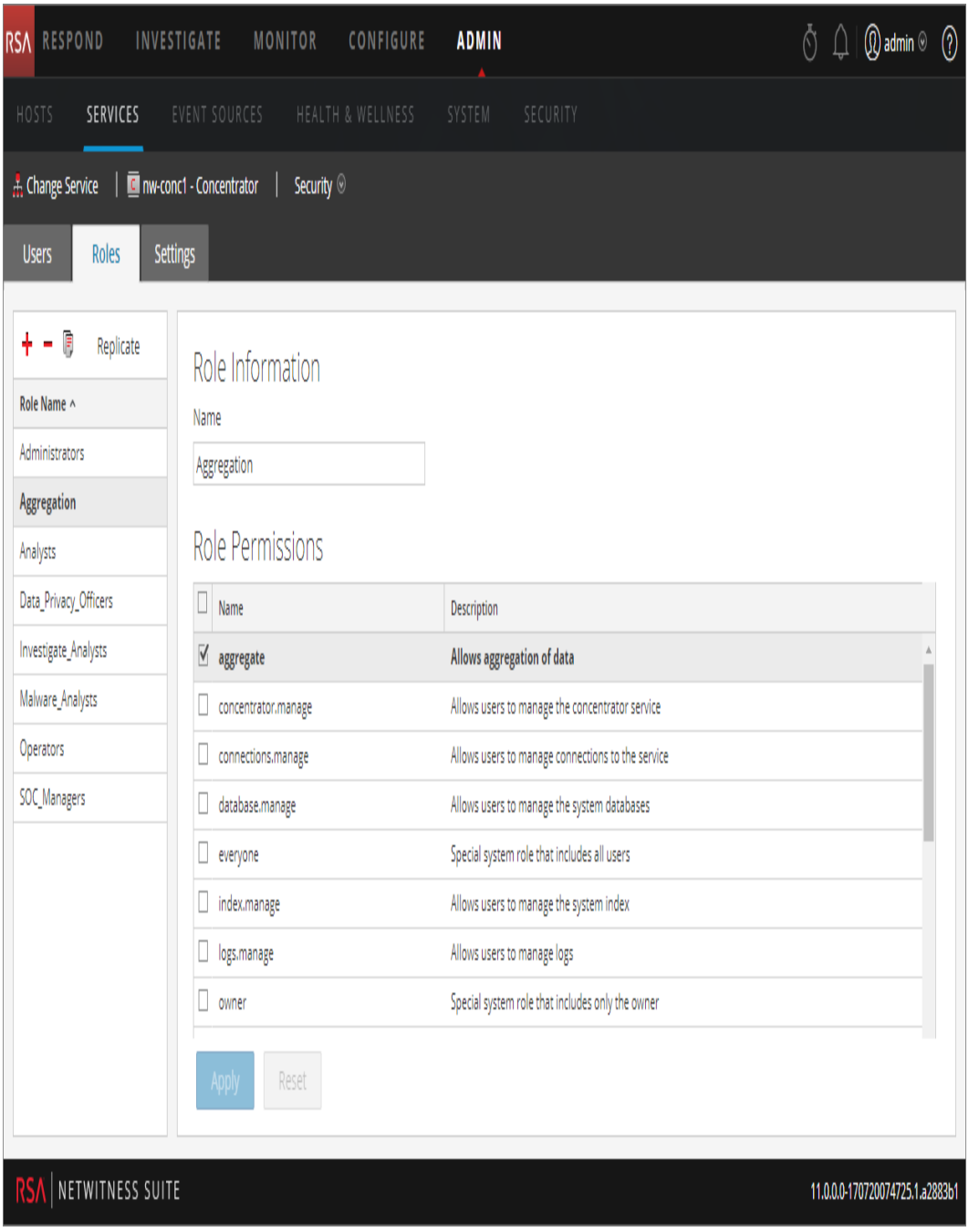
Chacune des procédures suivantes débute dans la vue Sécurité des services.

Pour accéder à la vue Sécurité des services :

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Sélectionnez un service, puis cliquez sur  **> Vue > Sécurité**.
   La vue Sécurité du service sélectionné s'affiche avec l'onglet Utilisateurs ouvert.
3. Sélectionnez l'onglet **Rôles**.

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 **Appliquer**.
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 NetWitness Suite.
- 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 les suivants :

- 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.

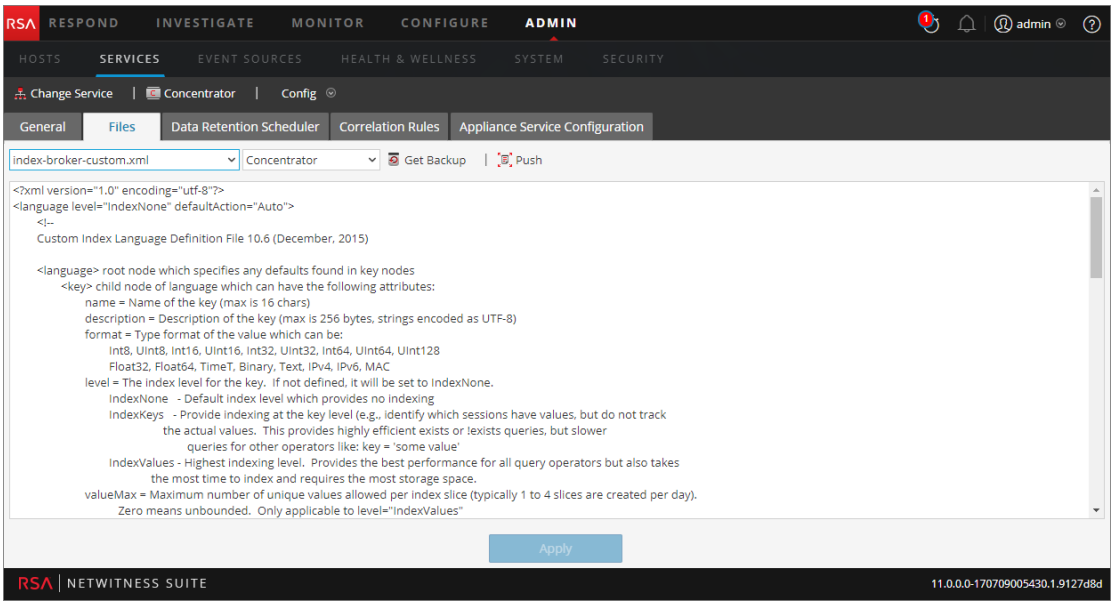
Remarque : Les valeurs par défaut de ces fichiers de configuration sont généralement adaptées aux situations les plus courantes. Toutefois, il est nécessaire de les modifier en partie pour les services facultatifs, comme le rapporteur d'incidents ou le planificateur. Seuls les administrateurs disposant 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 NetWitness Suite, accédez à **ADMIN > Services**.
2. Dans la grille Services, sélectionnez un service.
3. Sélectionnez  **> Vue > Config**.
   La vue Configuration des services s'ouvre sur l'onglet Général.
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 **Appliquer**.

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. Sélectionnez un fichier de configuration en suivant les étapes 1 à 6 de la procédure **Modifier les fichiers de configuration de service** au début de cette rubrique.
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.

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. Sélectionnez un fichier de configuration en suivant les étapes 1 à 6 de la procédure **Modifier un fichier de configuration de service** au début de cette rubrique.
2. Cliquez sur Push. 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.

   Attention : 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.

CONFIGURER LE PLANIFICATEUR DE TÂCHES

Fichier du planificateur

Vous pouvez modifier le fichier du **planificateur** qui se trouve dans la vue Configuration des services > onglet Fichiers. 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 tâches 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.

Syntaxe	Description
hours: <uint32, optional, {range:1 to 8760}>	Nombre d'heures entre les exécutions.
logOutput: <string, optional>	Sort la réponse à consigner avec le nom de module spécifié.
minutes: <uint32, optional, {range:1 to 525948}>	Nombre de minutes entre les exécutions.
msg: <string>	Message pour envoyer le nœud.
params: <string, optional>	Paramètres du message.
pathname: <string>	Chemin du nœud qui reçoit le message.
seconds: <uint32, optional, {range:1 to 31556926}>	Nombre de secondes entre les exécutions.
time: <string>	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

Message	Description
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 1 heure du matin tous les jours ouvrables : 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.
sauvegarde	Indiquer un nœud à enregistrer

Exemple de ligne de tâche

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"
```

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 Core. L'accès au fichier d'index dans la vue Configuration des services dans NetWitness Suite ouvre le fichier dans un éditeur de texte, où vous pouvez modifier le fichier.

Remarque : 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 et index-brokercustom.xml
- index-concentrator.xml et index-concentratorcustom.xml
- index-decoder.xml et index-decodercustom.xml
- index-logdecoder.xml et index-logdecodercustom.xml
- index-archiver.xml et index-archivercustom.xml
- index-workbench.xml et index-workbenchcustom.xml

Fichiers d'index et fichiers d'index personnalisés

Tous les changements d'index spécifiques au client sont apportés dans **index-<service>-custom.xml**. Ce fichier remplace tous les paramètres de index-<service>.xml, qui est exclusivement contrôlé par RSA.

Remarque : Les clients utilisant les versions antérieures à la version 10.1 de NetWitness Suite devaient personnaliser les fichiers d'index en modifiant et enregistrant le fichier d'index. Cette méthode reposait sur NetWitness Suite 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 est effectuée 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, ce 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 index-<service>-custom.xml remplacent les définitions trouvées dans index-<service>.xml.
- Les clés qui sont ajoutées à index-<service>custom.xml et ne figurant pas dans index-<service>.xml sont ajoutées à la langue en tant que 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 NetWitness Suite.

- 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 NetWitness Suite Core comme décrit dans le *Guide d'optimisation de la base de données NetWitness Suite Core*.

Remarque : Pour les versions NetWitness Suite 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.

Attention : Ne définissez jamais le niveau d'index sur `IndexKeys` ou `IndexValues` pour un Decoder si vous disposez d'un Concentrator ou d'un Archiver effectuant l'agrégation du Decoder. La taille de partition d'index est trop petite pour prendre en charge une indexation au-delà de la valeur par défaut de clé de méta `time` par défaut.

ACTIVER LE SERVICE DE RAPPORT SUR LES INCIDENTS

Le service de rapport sur les incidents est un service facultatif pour les services NetWitness Suite. 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 les données capturées. Ce package d'informations comprend les 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.
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.

Paramètre	Description
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.

Paramètre	Description
deletecores=1	Indique si les fichiers mémoire doivent être supprimés après le rapport. 0 = No 1 = Yes **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 = No 1 = Yes **REMARQUE :** S'il n'est pas supprimé, le répertoire sera inclus dans chaque package ultérieur.

Paramètre	Description
debug=1	Indique si les messages de débogage sont activés ou désactivés dans la sortie de consignation **crashreporter**. 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 :

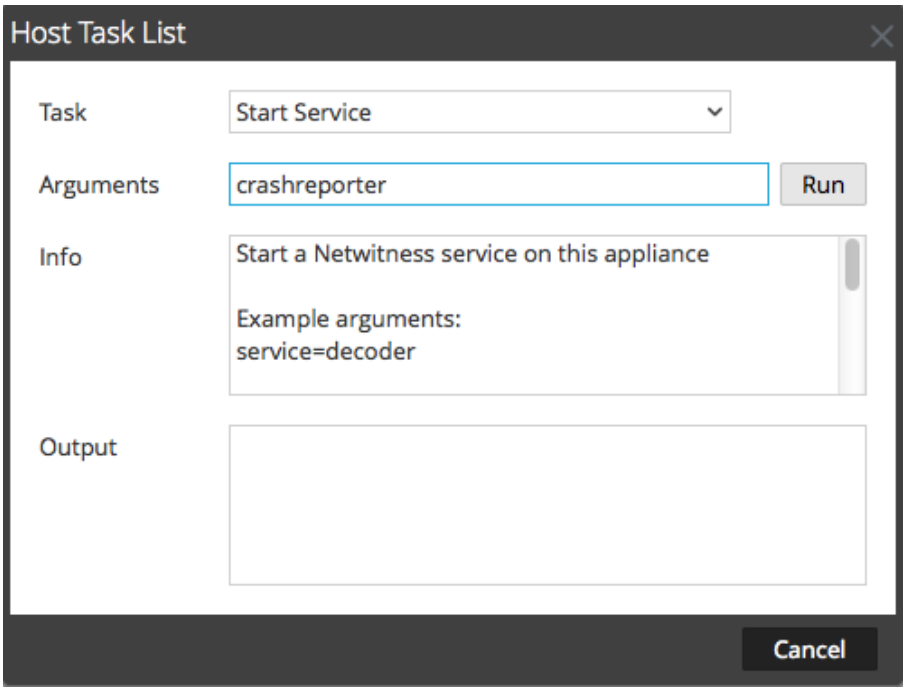
1. Sélectionnez **Admin > Services**.
2. Sélectionnez un service, puis cliquez sur  **> Vue > Config**.
3. Sélectionnez l'onglet **Fichiers**.
4. Modifiez le fichier **crashreporter.cfg**.

5. Cliquez sur **Enregistrer**.
6. Pour afficher la vue Système de services, sélectionnez **Config > Système**.
7. Pour redémarrer le service, cliquez sur Shutdown Service.
   Le service s'arrête et redémarre.

Démarrage et arrêt du service de rapport sur les incidents

Pour démarrer le service de rapport sur les incidents :

1. Sélectionnez **ADMIN > Services**.
2. Sélectionnez un service, puis cliquez sur > **Vue > Système**.
3. Dans la barre d'outils, cliquez sur Host Tasks.
   La liste des tâches de l'hôte s'affiche.
4. Dans la liste déroulante Tâche, sélectionnez **Démarrer le service**.
5. 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 `table-map.xml`, certaines clés méta sont définies sur `Transient` et certaines sont définies sur `None`. Pour stocker et indexer une clé méta spécifique, la clé doit être définie sur `None`. Pour apporter des modifications au mappage, vous devez créer une copie du fichier nommé `table-map-custom.xml` sur 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 `table-map.xml` dans le Log Decoder, elle est indexée.
- Lorsqu'une clé est définie sur `Transient` au sein du fichier **`table-map.xml`** dans le Log Decoder, 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 Log Decoder.

Attention : Ne remplacez pas le fichier `table-map.xml` car une mise à niveau pourrait l'écraser. Ajoutez tous les changements que vous souhaitez apporter au fichier **`table-map-custom.xml`** .

Conditions préalables

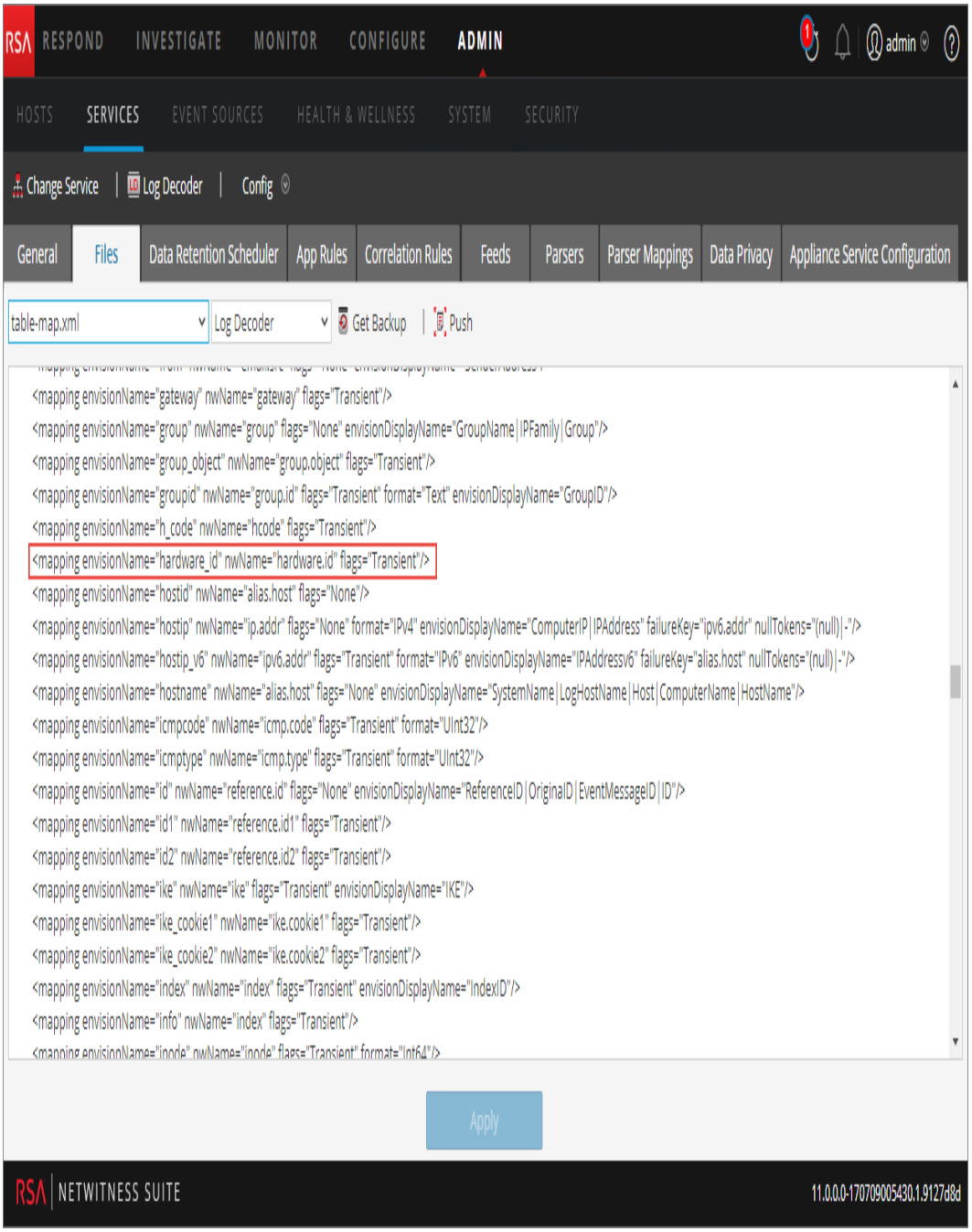
Si vous n'avez pas de fichier `table-map-custom.xml` dans le Log Decoder, créez une copie de `table-map.xml` et renommez-la `table-map-custom.xml`.

Procédure

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

1. Accédez à **ADMIN** > **Services**.
2. Dans la grille Services, sélectionnez un Log Decoder, puis cliquez sur > **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 avez besoin de modifier une entrée, ne modifiez pas le fichier `table-map.xml` . Au lieu de cela, copiez l'entrée, sélectionnez le fichier `table-map-custom.xml`, recherchez l'entrée dans le fichier `table-map-custom.xml` et remplacez le mot-clé de balise `Transient` par `None`.
   Par exemple, l'entrée suivante pour la clé méta `hardware.id` dans le fichier `table-`

`map.xml` fichier n'est pas indexé et le mot-clé de balise s'affiche comme `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 `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**.

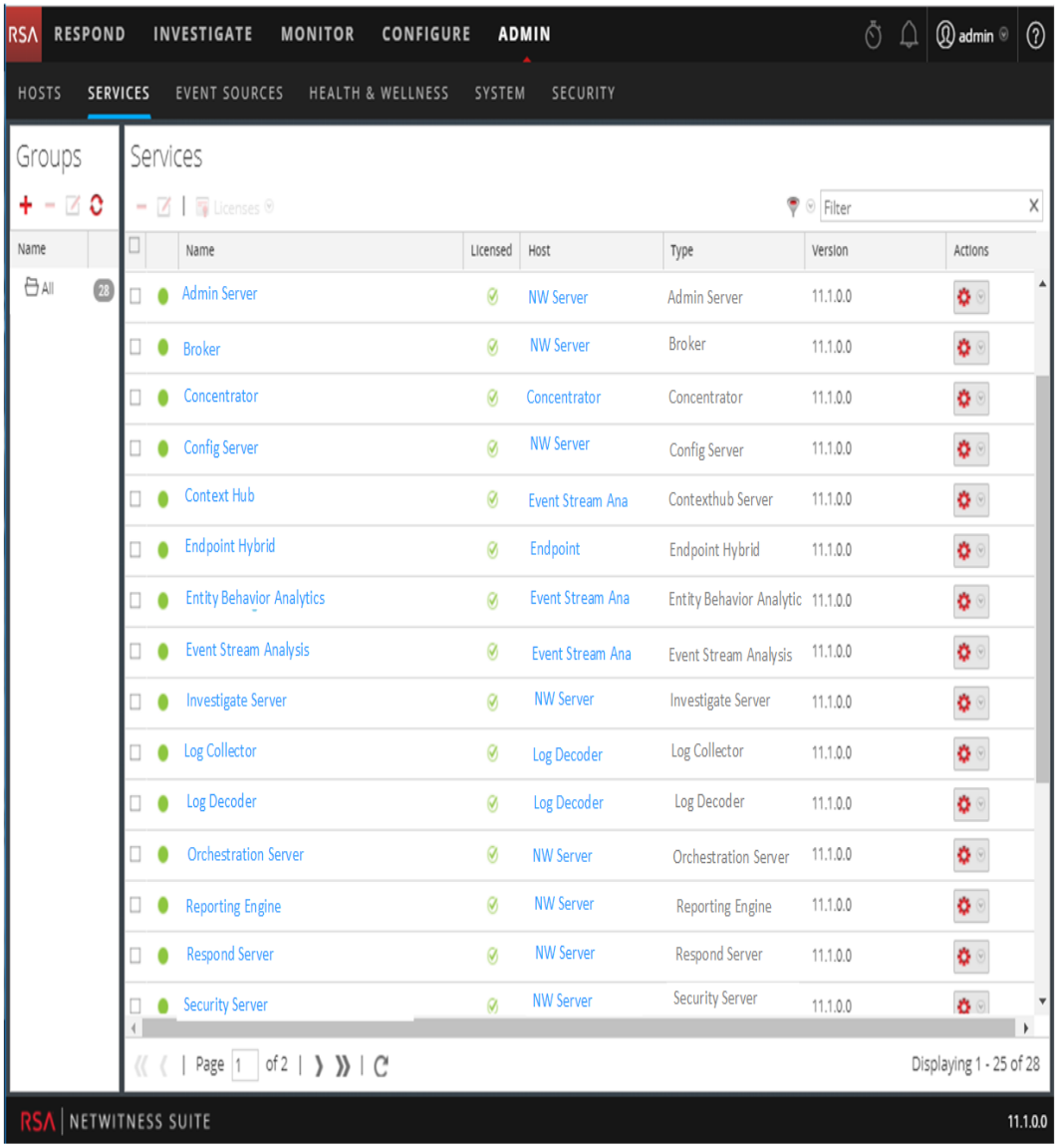
Attention : Avant de modifier les fichiers de mappage de tables, examinez attentivement l'effet de la modification de l'index suite au remplacement de `Transient` en `None`, car il peut y avoir un impact sur la capacité de stockage disponible et les performances du Log Decoder. C'est pour cette raison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

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.

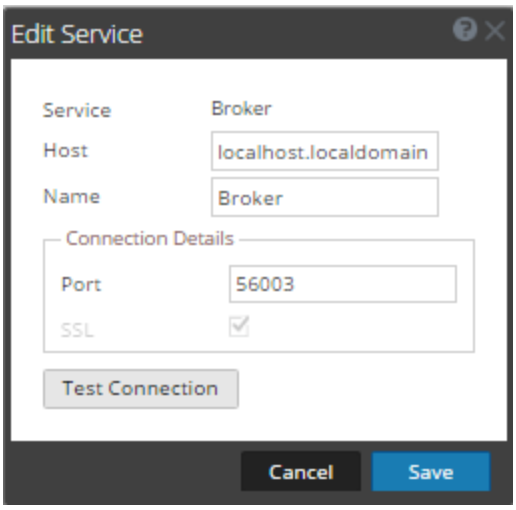
Pour accéder à la vue Services, dans NetWitness Suite, accédez à **ADMIN > Services**.



Procédures

MODIFIER UN 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 Autoriser le 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 NetWitness Suite.

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 NetWitness Suite, accédez à **ADMIN > Services**.
2. Sélectionnez un service et sélectionnez  **>Vue > Explorer**.

   La vue Explorer s'affiche. La liste des nœuds se trouve sur la gauche et le panneau

Surveiller sur la droite.

Procédures

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, sélectionnez 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**.

Supprimer la connexion à un service

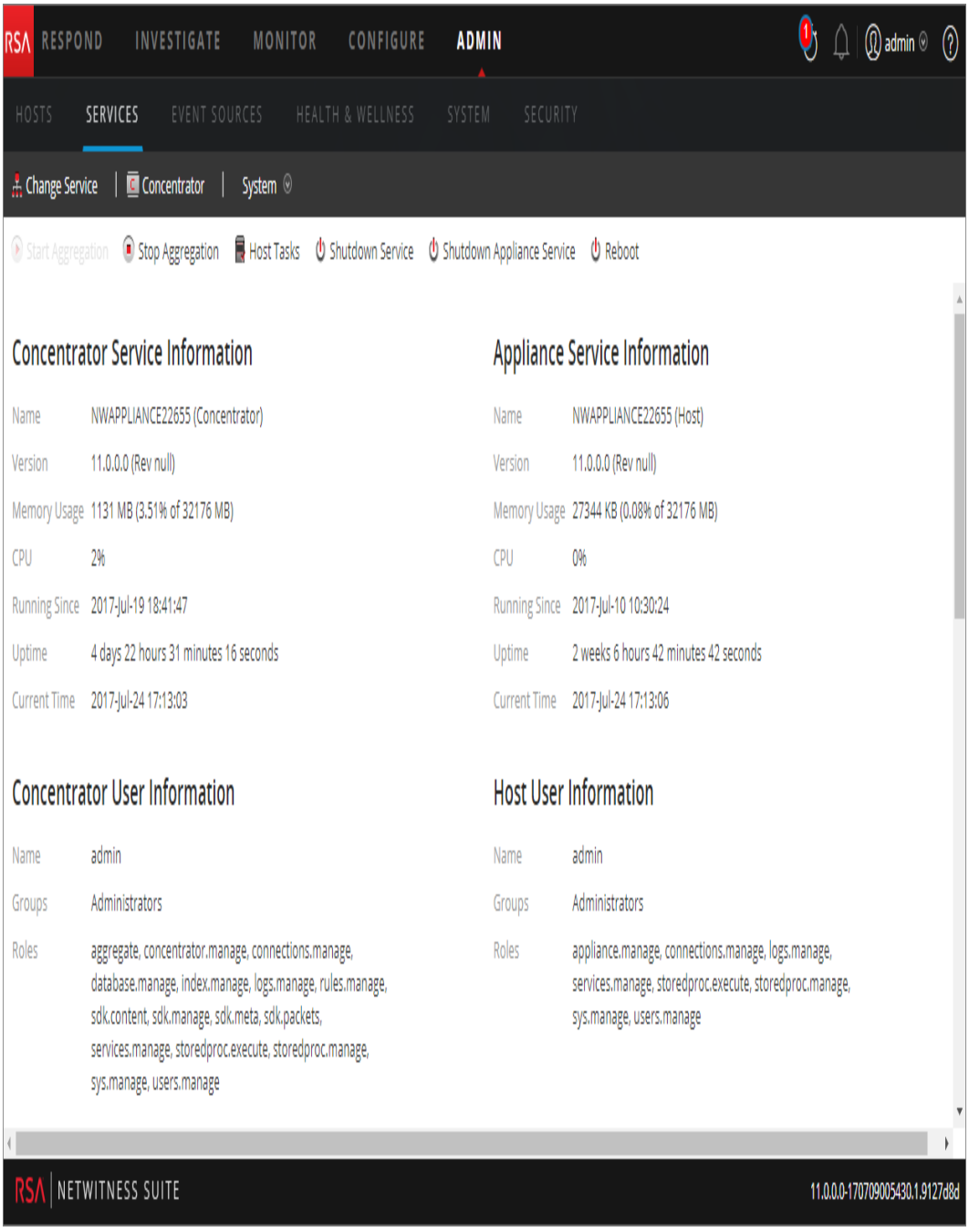
Dans la vue Système de services, vous pouvez afficher les sessions en cours d'exécution sur un service. Dans la liste des sessions, vous pouvez mettre fin à la session et aux requêtes actives d'une session.

Mettre fin à une session sur un service

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
   La vue Services ADMIN s'affiche.

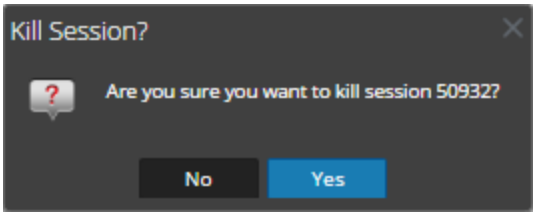
2. Sélectionnez un service et cliquez sur  **> Vue > Système**.

   La vue Système de services s'affiche.



3. Dans la grille **Informations de session** située dans la partie inférieure, cliquez sur un ***numéro de session***.

La boîte de dialogue suivante s'affiche.

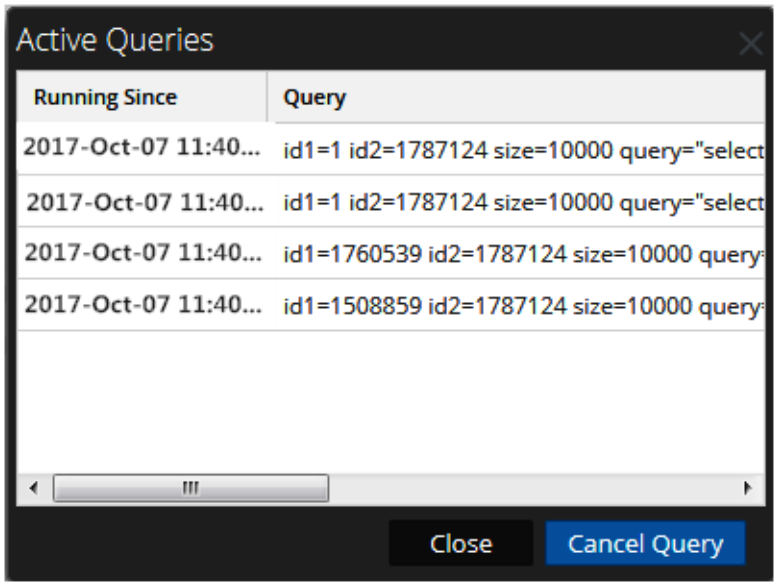


4. Cliquez sur **Yes**.

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. 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.

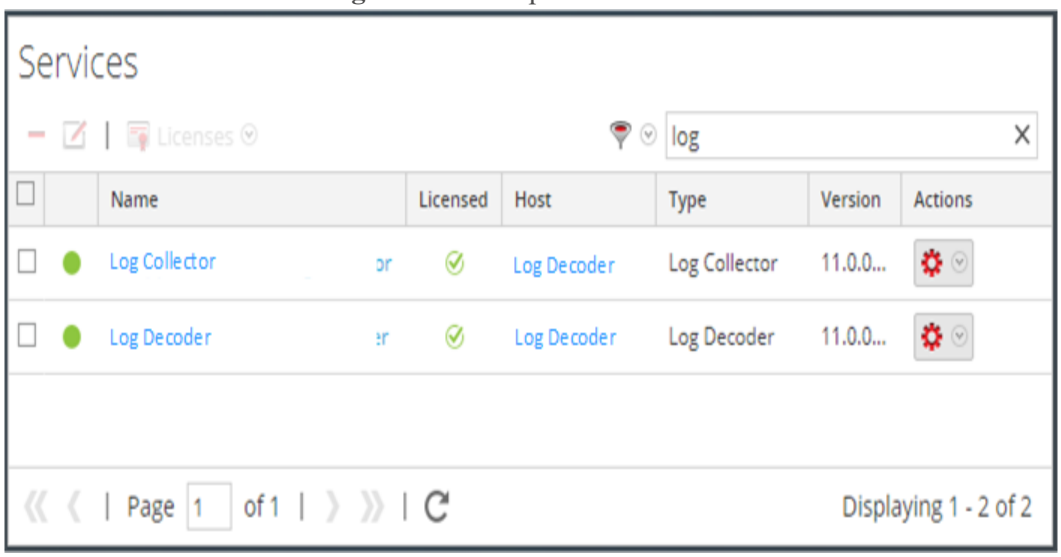
En plus de localiser les services d'un hôte dans la vue Services, vous pouvez aussi trouver rapidement les services qui s'exécutent sur un hôte dans la vue Hôtes.

Rechercher un service

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Dans la barre d'outils du panneau **Services**, saisissez un **nom** de service ou un nom d'**hôte** dans le champ **Filtre**.

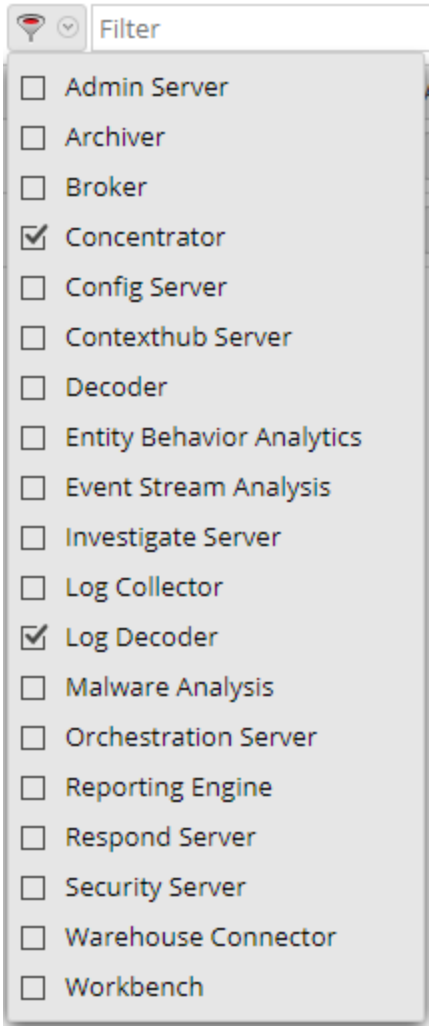
   

   Le panneau Service répertorie les services correspondant aux noms saisis dans le champ Filtre. L'exemple suivant illustre les résultats de recherche qui apparaissent lorsque vous commencez à saisir le mot **log** dans le champ de filtre.

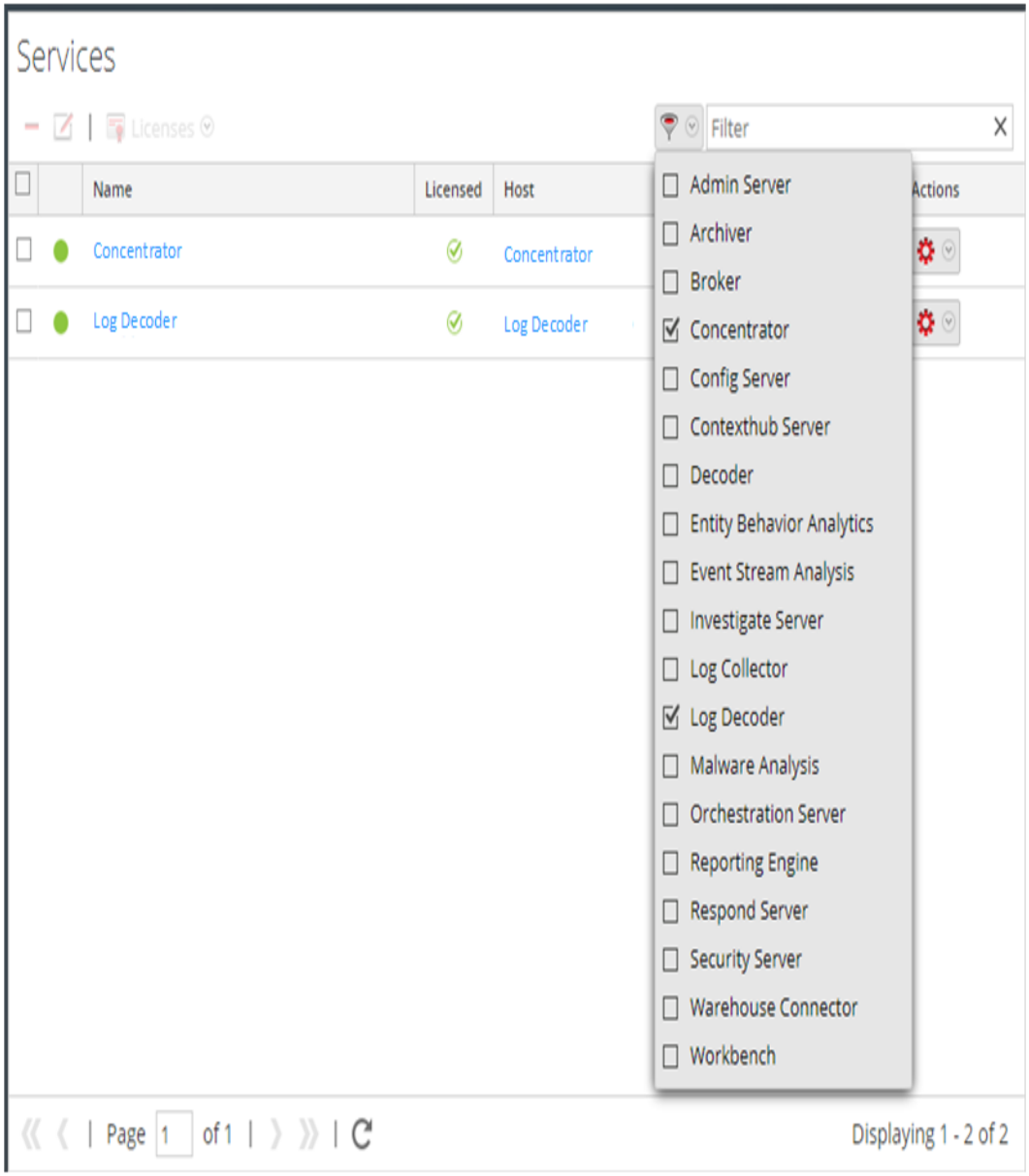
   

Filtrer les services par type

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Dans la vue Services, cliquez sur , puis sélectionnez le type de service que vous souhaitez faire apparaître dans cette vue.



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

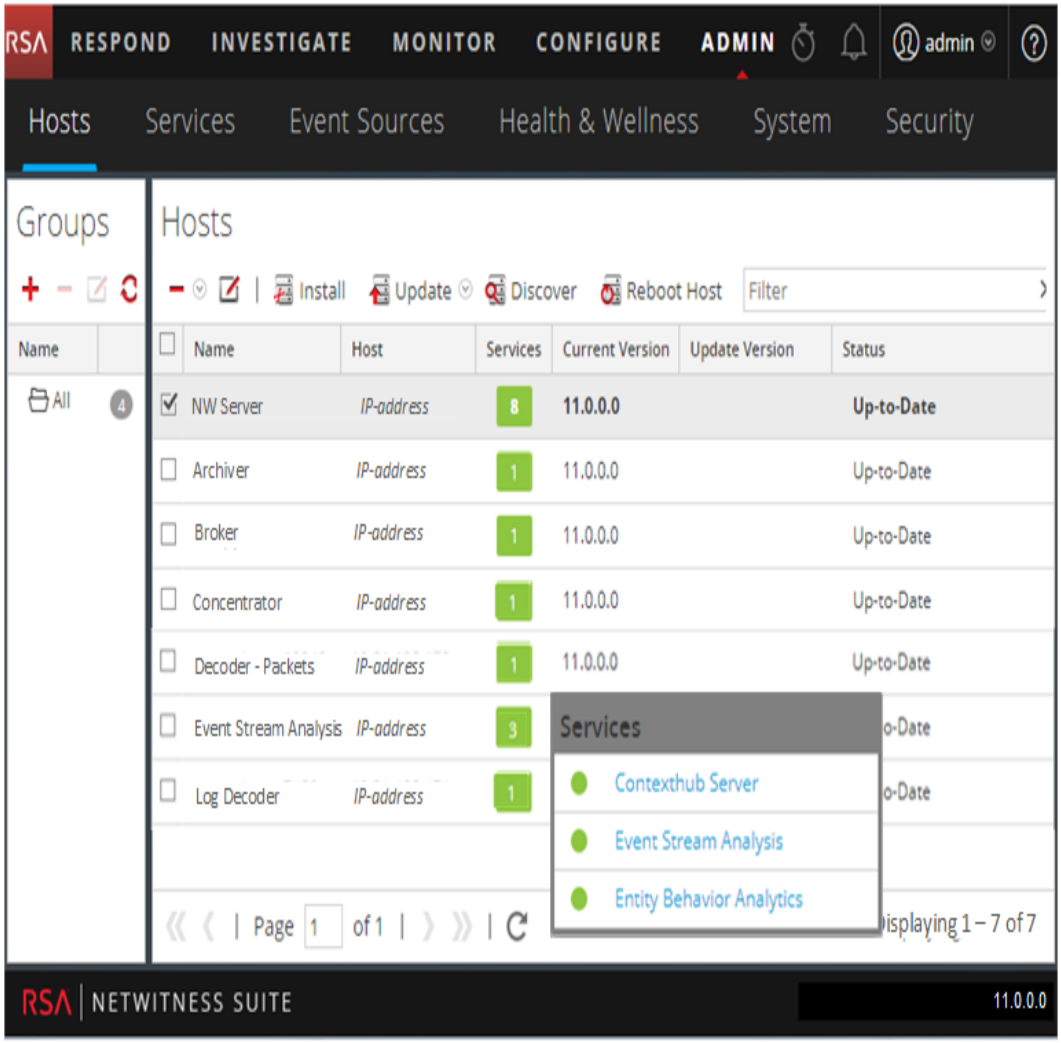


Trouver les services sur un hôte

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 NetWitness Suite, accédez à **ADMIN > 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.



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

Démarrer, arrêter ou redémarrer un service

Ces procédures s'appliquent uniquement aux services principaux.

Chacune des procédures suivantes démarre dans la vue Services. Dans NetWitness Suite, accédez à **ADMIN > 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, NetWitness Suite affiche un message.

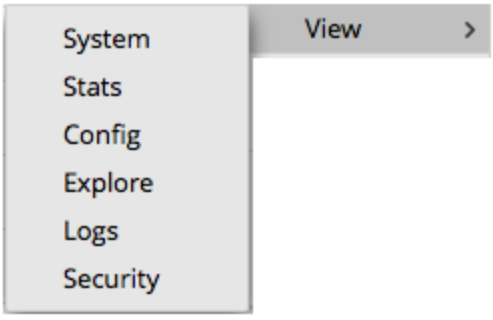
Pour redémarrer un service :

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.

Voir 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.

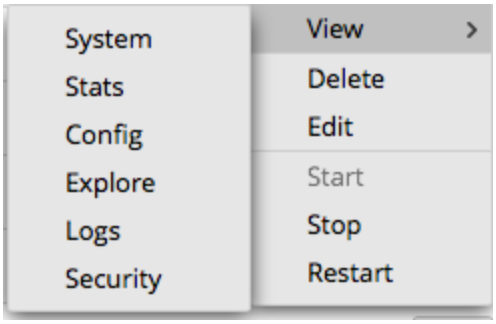
- La vue Statistiques des services donne un moyen de surveiller les opérations et l'état du service.
- La vue Configuration des services permet de configurer tous les aspects d'un service.
- La vue Explorer les services permet d'afficher et de modifier les configurations des hôtes et des services.
- Le panneau Consignation système affiche les logs du service dans lesquels vous pouvez effectuer une recherche.
- La vue Sécurité des services est un moyen d'ajouter des comptes utilisateur Security Analytics Core 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 :

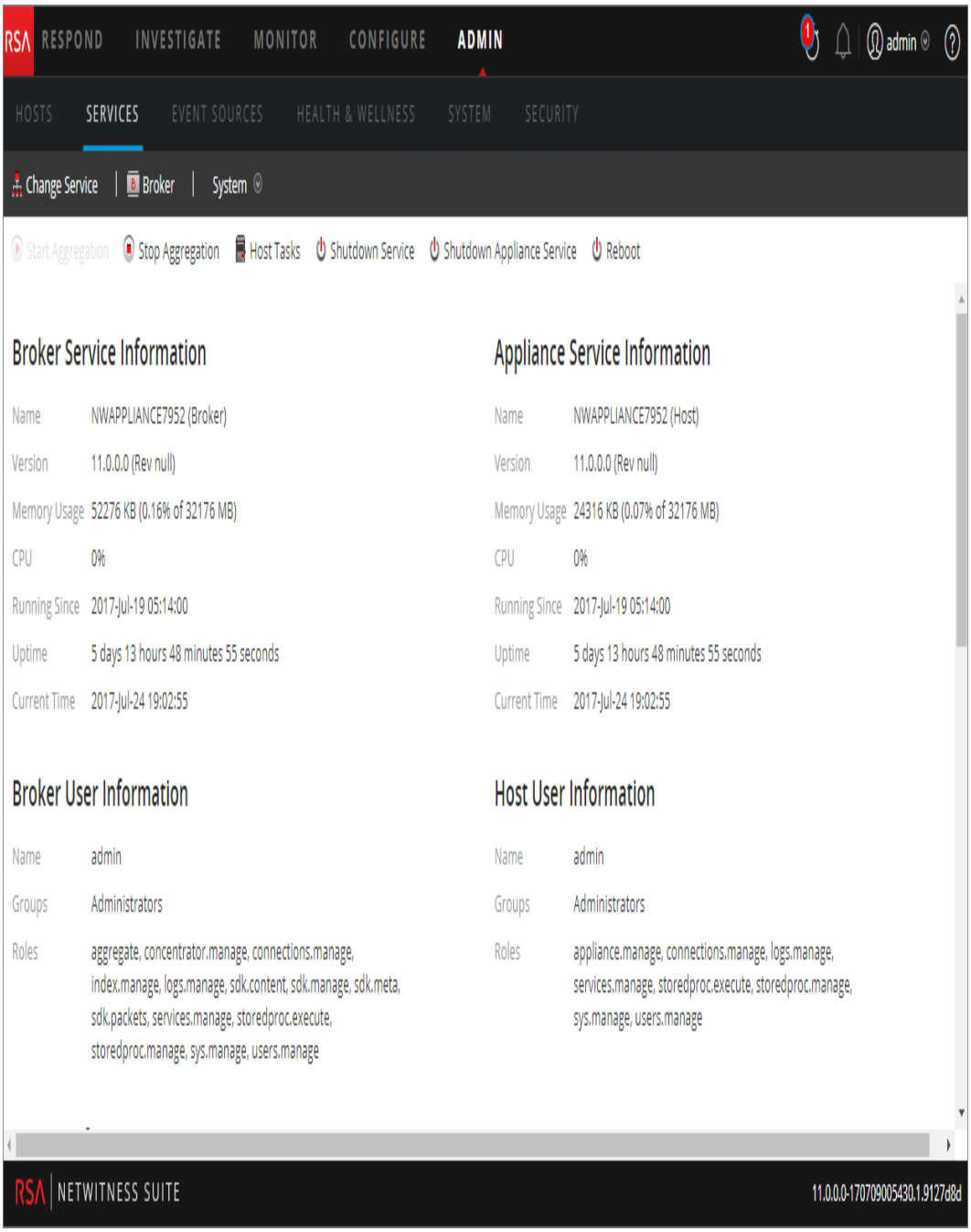
1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Sélectionnez un service, puis cliquez sur  **> Affichage**.

   Le menu Affichage s'affiche.

3. Parmi les options situées sur la gauche, sélectionnez une vue.

   Il s'agit d'une vue du système pour un Broker.

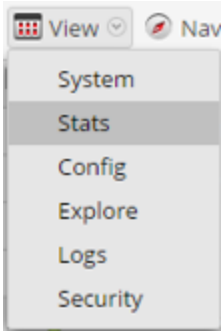


4. Utilisez la barre d'outils pour naviguer :

   a. Cliquez sur **Modifier le service** pour sélectionner un autre service.
      La boîte de dialogue **Administrer le service** s'affiche.

   b. Cochez la case à gauche du service que vous souhaitez sélectionner.

c. Sélectionnez la vue souhaitée pour le service que vous avez sélectionné dans le menu déroulant Vue.



La nouvelle vue (par exemple, Statistiques) s'affiche pour le service que vous avez sélectionné.

Références liées aux vues Hôtes et Services

Cette rubrique constitue une référence concernant les fonctions de l'interface utilisateur ADMIN de NetWitness Suite.

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

Rubriques

Vue Hôtes

Configurez et mettez à jour la machine physique ou virtuelle sur laquelle les services NetWitness Suite s'exécutent dans la vue **Hôtes**.

Important : Reportez-vous à la section Dépannage des installations et mises à jour de version pour obtenir de l'aide sur la résolution des erreurs que vous recevez lors de l'installation et de la mise à jour de la version.

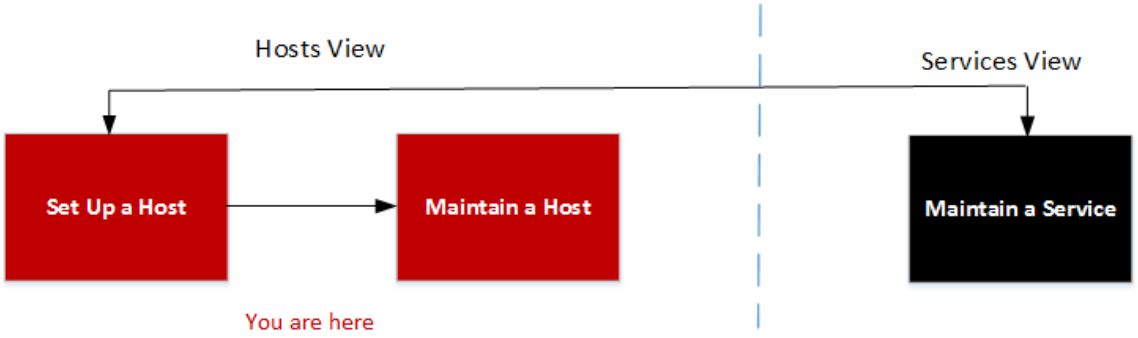
Un service exécute une fonction spécifique, par exemple la collecte des logs ou l'archivage des données. Chaque service s'exécute sur un port dédié et se présente comme un plug-in à activer ou désactiver selon la fonction de l'hôte. Vous devez commencer par configurer les services Core suivants :

Core	Autre	Autre	Autre
Decoder	Log Decoder	Context Hub	Reporting Engine
Concentrator	Archiver	Log Collector	Warehouse Connector
Broker	Event Stream Analysis	Malware Analysis	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.

Workflow

Ce workflow présente les procédures à suivre pour configurer un hôte, le maintenir en conditions opérationnelles et le mettre à jour avec les nouvelles versions de NetWitness Suite. La configuration d'un hôte est la première tâche de ce workflow. Les hôtes dotés des services Core sont prêts à l'emploi. Ensuite, vous pouvez configurer des hôtes supplémentaires afin d'améliorer votre déploiement de NetWitness Suite. Les deux autres tâches, la maintenance d'un hôte et la mise à jour des versions d'un hôte, sont effectuées à la demande et pas selon un ordre précis.

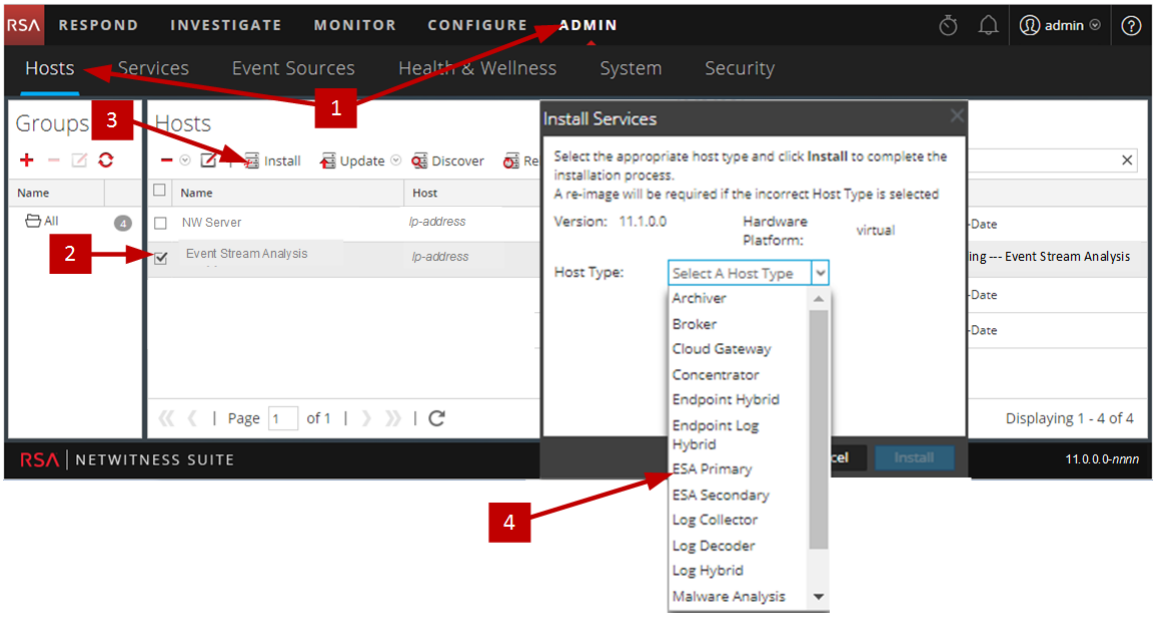


Que voulez-vous faire ?

Reportez-vous à la section Hôte GS : Procédures des hôtes et des services pour obtenir des instructions détaillées.

Rôle	Je souhaite...
Administrateur	Configurer un hôte.
Administrateur	Mettre à jour un hôte.
Administrateur	Appliquer les mises à jour de version à un hôte.

Aperçu rapide



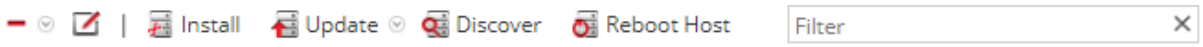
L'exemple suivant vous montre comment configurer un hôte.

1. Sélectionnez ADMIN > Hôtes.
2. Sélectionnez l'hôte que vous avez déployé (par exemple, **Event Stream Analysis**).
3. Cliquez sur Install (icône Installer).
4. Sélectionnez le type d'hôte à installer à partir de la boîte de dialogue **Installer les services** (par exemple, **ESA primaire**). Ce type d'hôte installe les services Analytique comportementale de l'entité, Context Hub et Event Stream Analysis sur cet hôte.

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 NetWitness Suite.

Dans NetWitness Suite, naviguez vers **Admin** > **Hôtes** 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.



Fonctionnalités

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

Fonctionnalités	Description
	Retirer du groupe : Si l'hôte fait partie d'un groupe d'hôtes, vous pouvez le supprimer de ce groupe.
	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. Procédure associée : Étape 1. Déployer un hôte
Installation	Permet d'ouvrir la boîte de dialogue **Installer les services** à partir de laquelle vous pouvez installer un service sur un hôte déployé. Procédures associées : Étape 2. Installer un service sur un hôte

Fonctionnalités	Description
Mettre à jour	• **Mise à jour** - met à jour les hôtes que vous avez sélectionnés avec la version que vous sélectionnez dans la colonne **Mettre à jour la version**. • **Rechercher les mises à jour** - recherche les dernières mises à jour disponibles à partir de RSA dans le référentiel des mises à jour local. Procédure associée : Appliquer les mises à jour de version à un 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 la phase de provisionnement terminée, NetWitness Suite découvre automatiquement les services exécutés sur l'hôte, 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 la phase de provisionnement terminée, NetWitness Suite découvre automatiquement les services exécutés sur l'hôte.
Redémarrer l'hôte	Redémarrez l'hôte.
Filtrer	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. Après avoir créé 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.

Dans NetWitness Suite, accédez à **ADMIN > Hôtes**. La barre d'outils du panneau Groupes se trouve en haut de la grille Groupes de la vue Hôtes.

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 non groupée.

Remarque : Dans NetWitness 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
	Affiche une nouvelle ligne dans la grille Groupe, sur laquelle vous saisissez 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 sur une ligne de la grille Groupe pour que vous puissiez saisir le nouveau nom d'un groupe existant.
	Actualise le groupe sélectionné.
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.

Hôte GS : Vue Services

Vous configurez et gérez les services NetWitness Suite qui s'exécutent dans la vue **Services**. Avec 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

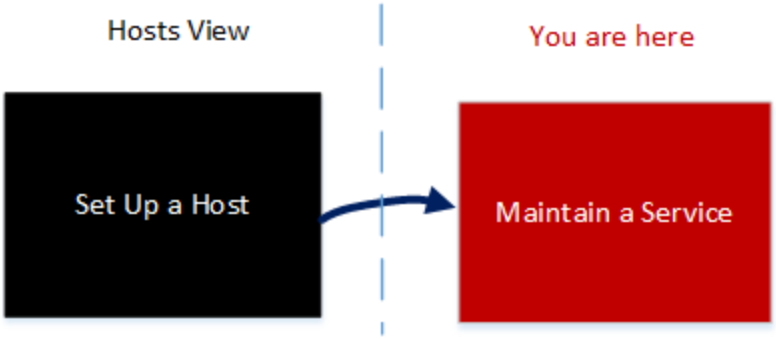
Un service exécute une fonction spécifique, par exemple la collecte des logs ou l'archivage des données. Chaque service s'exécute sur un port dédié et se présente comme un plug-in à activer ou désactiver selon la fonction de l'hôte. Vous devez commencer par configurer les services Core suivants :

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

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.

Workflow

Ce workflow affiche les procédures à effectuer pour configurer et gérer un service. L'ajout d'un service à un hôte est la première tâche de ce workflow. Les hôtes avec des services de base sont définis et prêts à l'emploi. Ensuite, vous pouvez configurer des services supplémentaires sur les hôtes afin d'améliorer votre déploiement NetWitness Suite.



Que voulez-vous faire ?

Reportez-vous à la section Hôte GS : Procédures des hôtes et des services pour obtenir des instructions détaillées.

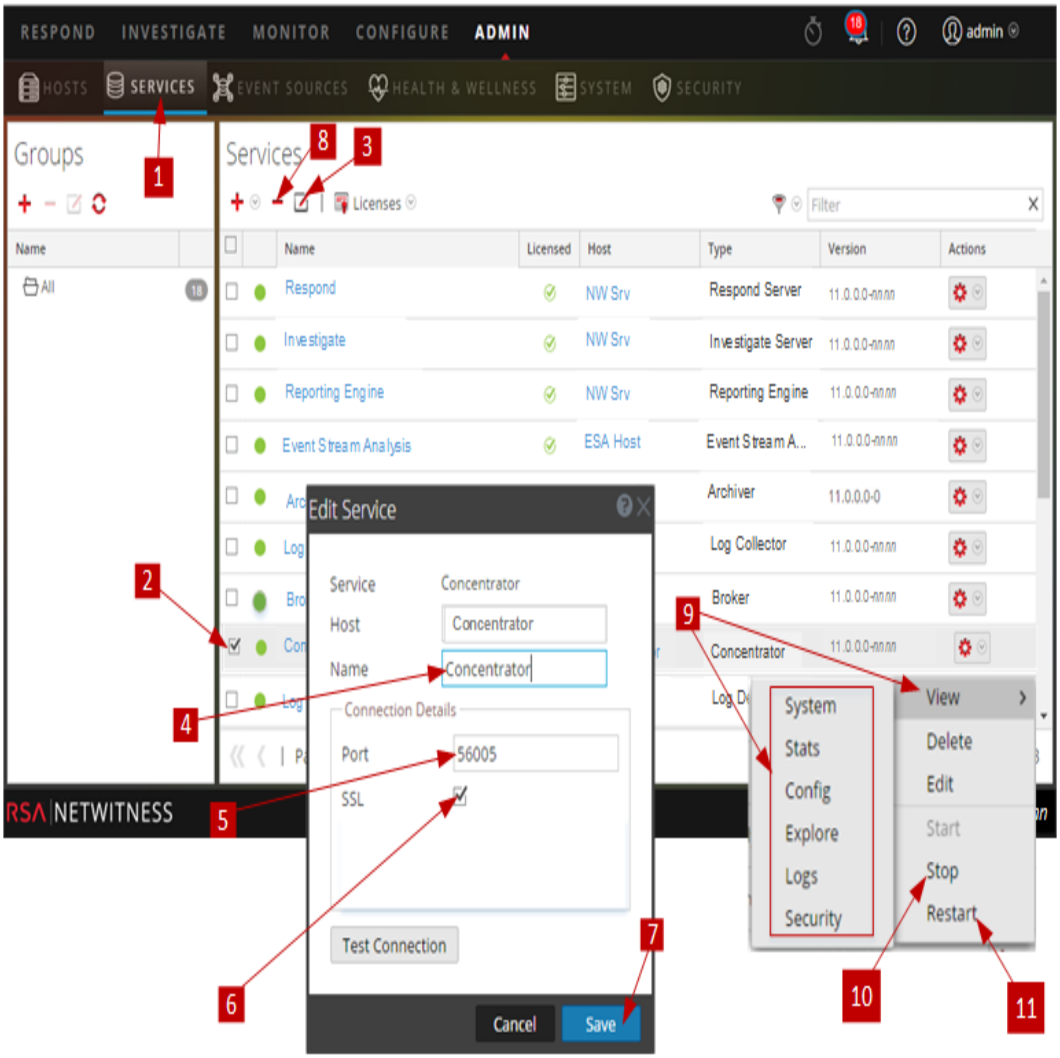
Rôle	Je souhaite...
Administrateur	Gérer un service.
Administrateur	Configurer un hôte.

Rubriques connexes

- Bonnes pratiques
- Résolution des problèmes liés aux mises à jour des hôtes

Aperçu rapide

L'exemple suivant vous montre comment maintenir un service.



Sélectionnez un service.

1. Accédez à la vue **ADMIN** > **Services**.
2. Cochez la case à gauche du service que vous souhaitez sélectionner.

Modifiez le nom du service et la connexion.

3. Cliquez sur (sinon, sélectionnez Modifier dans (menu déroulant Action).
4. Modifiez le **nom** de l'hôte.
5. Modifiez le **nom** du service.
6. Saisissez le **numéro** de port.
7. Désélectionnez ou sélectionnez une connexion de communication SSL.

8 Cliquez sur **Tester la connexion**.

Supprimez un service.

9 **Sélectionnez un service**, puis cliquez sur l'icône Supprimer.

Affichez les statistiques des services et configurer les paramètres.

10 Procédez comme suit pour afficher les statistiques liées aux services et configurer les paramètres des services.

a. **Sélectionnez un service**, puis cliquez sur l'icône Actions.

b. Cliquez sur **Vue**, puis sélectionnez :

- **Système** pour :
  - Afficher les informations de haut niveau actuelles sur le service et son hôte.
  - Accéder à la barre d'outils Vue système.
- **Statistiques** pour afficher les statistiques détaillées liées aux services.
- **Config** pour afficher et configurer les paramètres du service.
- **Explorer** pour afficher et configurer les paramètres de service dans la vue Explorer NetWitness Suite.
- **Logs** pour afficher les messages de journal envoyés par le service.

10 **Sélectionnez un service**, cliquez sur l'icône Actions, puis sur **Arrêter** pour arrêter un service en cours d'exécution.

11 **Sélectionnez un service**, cliquez sur l'icône Actions, puis sur **Redémarrer** pour redémarrer un service arrêté.

Rubriques

Consultez les guides RSA NetWitness Suite suivants pour plus d'informations sur les différents services. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Guide de configuration d'Archiver

Guide de configuration de Broker et Concentrator

Guide de configuration de la passerelle Cloud Behavioral Analytics

Guide de configuration de Context Hub

Guide de configuration de Decoder et Log Decoder

Guide de configuration d'Endpoint Insights

Guide de configuration d'Event Stream Analysis (ESA)

Guide d'utilisation d'Investigate et de Malware Analysis

Guide de configuration de Log Collection

Guide de configuration de Malware Analysis

Guide d'utilisation Reporting Engine

Guide de configuration de Respond

Guide de configuration de Workbench

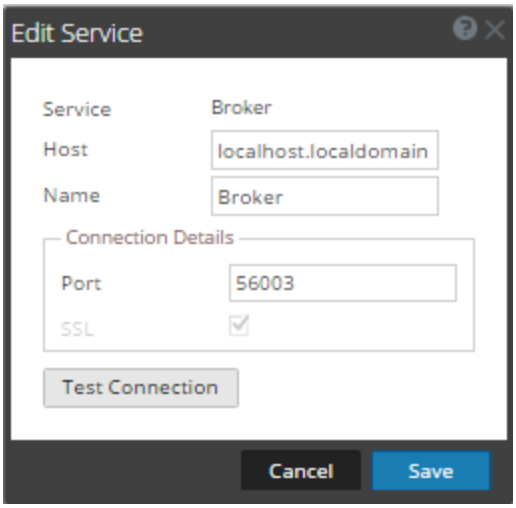
Guide de configuration de Warehouse Connector

Boîte de dialogue Modifier le service

Cette rubrique présente la boîte de dialogue Modifier le service accessible dans la vue Services ADMIN (ADMIN > Services).

Les services NetWitness Suite sont automatiquement découverts dans NetWitness Suite.

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



Les procédures liées à cet onglet sont décrites dans la section Hôte GS : Procédures des hôtes et des services.

Fonctionnalités

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.

Champ ou Option	Description
Nom	Spécifie le nom utilisé pour identifier le service ; par exemple, **Broker**. 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, consultez la section **Architecture réseau et ports** dans le *Guide de déploiement*.
SSL	Indique que NetWitness Suite 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**.
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 Local License Server (LLS) aux services sélectionnés. Pour plus d'informations, consultez la section **Afficher les droits** dans le *Guide d'octroi de licence*.
Tester la connexion	Le fait de cliquer sur ce bouton teste la connexion d'un service que vous ajoutez.
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.
Sauvegarder	Le fait de cliquer sur ce bouton enregistre le nouveau service.

Barre d'outils du panneau Groupes

Cette rubrique présente les fonctions et options de la vue **ADMIN > Services** > 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 afficher la vue Services, dans **NetWitness Suite**, accédez à la vue **ADMIN > Services.** La barre d'outils du panneau Groupes se trouve en haut de la grille Groupes de la vue Services.

Fonctionnalités

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

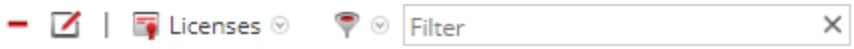
Option	Description
+	Affiche une nouvelle ligne dans la grille Groupe dans laquelle vous saisissez le nom d'un nouveau groupe.
−	Vous invite à confirmer que vous souhaitez supprimer le groupe ou le service. Vous pouvez confirmer ou annuler la suppression.
	Ouvre le champ de nom d'une ligne dans la grille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

Barre d'outils du panneau Services

Cette section 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.

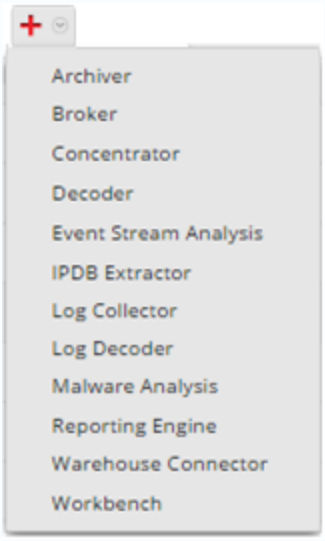
La barre d'outils du panneau Services comporte des options permettant d'ajouter, de supprimer, de modifier et de concéder sous licence des services. Vous pouvez filtrer les services répertoriés sur la base d'un ou de plusieurs types et noms de service ou hôtes.

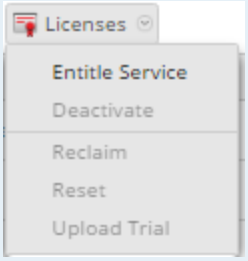
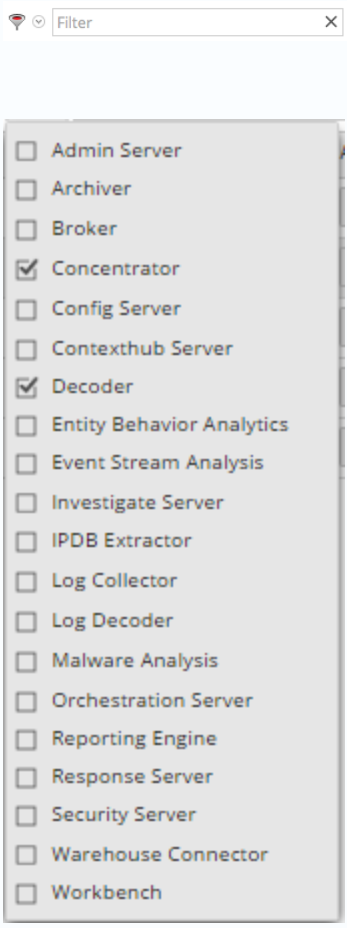
Pour accéder à la vue Services d'administration, dans **NetWitness Suite**, accédez à **ADMIN > Services.** La barre d'outils du panneau Services se trouve en haut de la grille Services de la vue Services.



Fonctionnalités

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

Fonctionnalité	Description
	Ajoute un service pour cette instance de RSA NetWitness Suite à gérer (voir l' Étape 2. Installer un service sur un hôte).
	Supprime un service de cette instance de NetWitness Suite (voir Modifier ou supprimer un service).
	Modifie l'identification du service et les paramètres de communication de base.

Fonctionnalité	Description
	• Autoriser le service : Attribue des licences du serveur LLS (Local License Server, serveur de licences local) aux services sélectionnés (voir la rubrique **Onglet Présentation** dans le *Guide d'octroi de licence*). • Désactiver : Non utilisé(e) dans NetWitness Suite 10.6 • Récupérer : Récupère une licence désactivée auprès du serveur LLS pour le service sélectionné. • Redémarrer : Non utilisé(e) dans NetWitness Suite 10.6 • Télécharger la version d'évaluation Non utilisé dans NetWitness Suite 10.6
	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 les services Concentrator et Decoder, seuls ces derniers 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 fonctionnalités et fonctions de la vue Configuration des services.

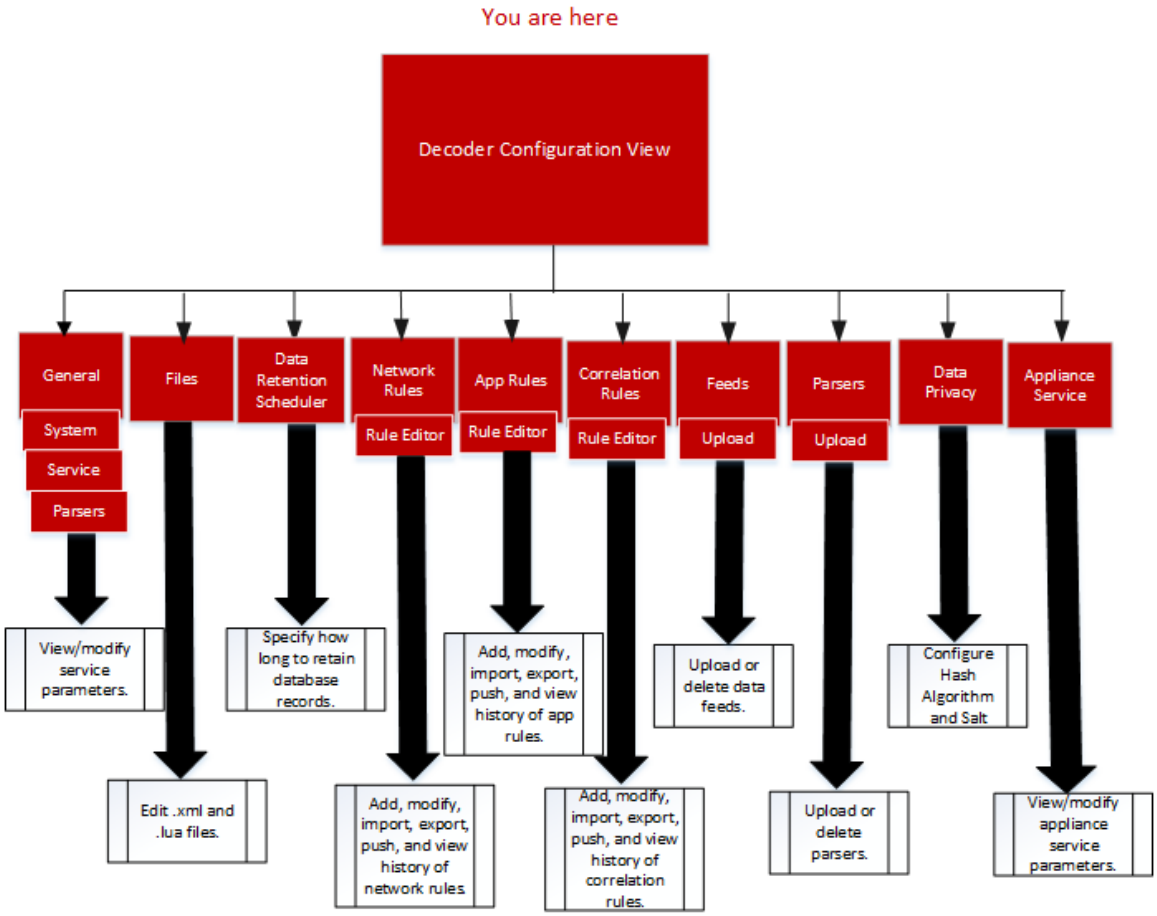
La vue Configuration des services est l'une des vues disponibles dans le menu **Services** > Actions (). Elle fournit une interface utilisateur pour la configuration de tous les aspects d'un service Core ou d'un service NetWitness Suite.

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).

Workflows

Le workflow suivant présente les tâches de configuration pour le service Decoder en tant qu'un exemple de cette vue. Consultez les guides de configuration de chaque service (par exemple, *RSA NetWitness® Suite Guide de configuration des services Broker et Concentrator*) pour en savoir plus sur leurs vues **ADMIN > Services > Config**.

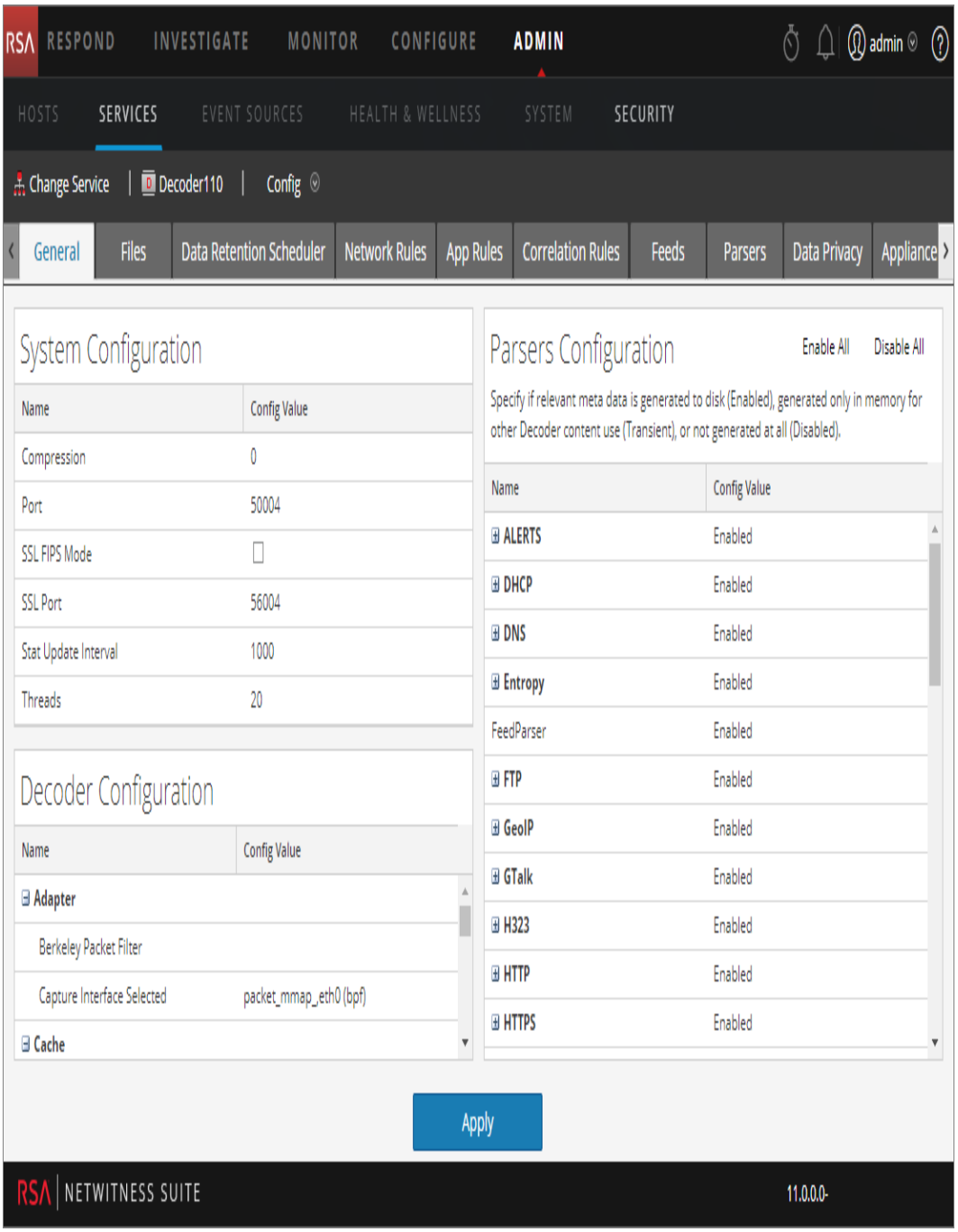


Pour accéder à la vue Configuration des Services :

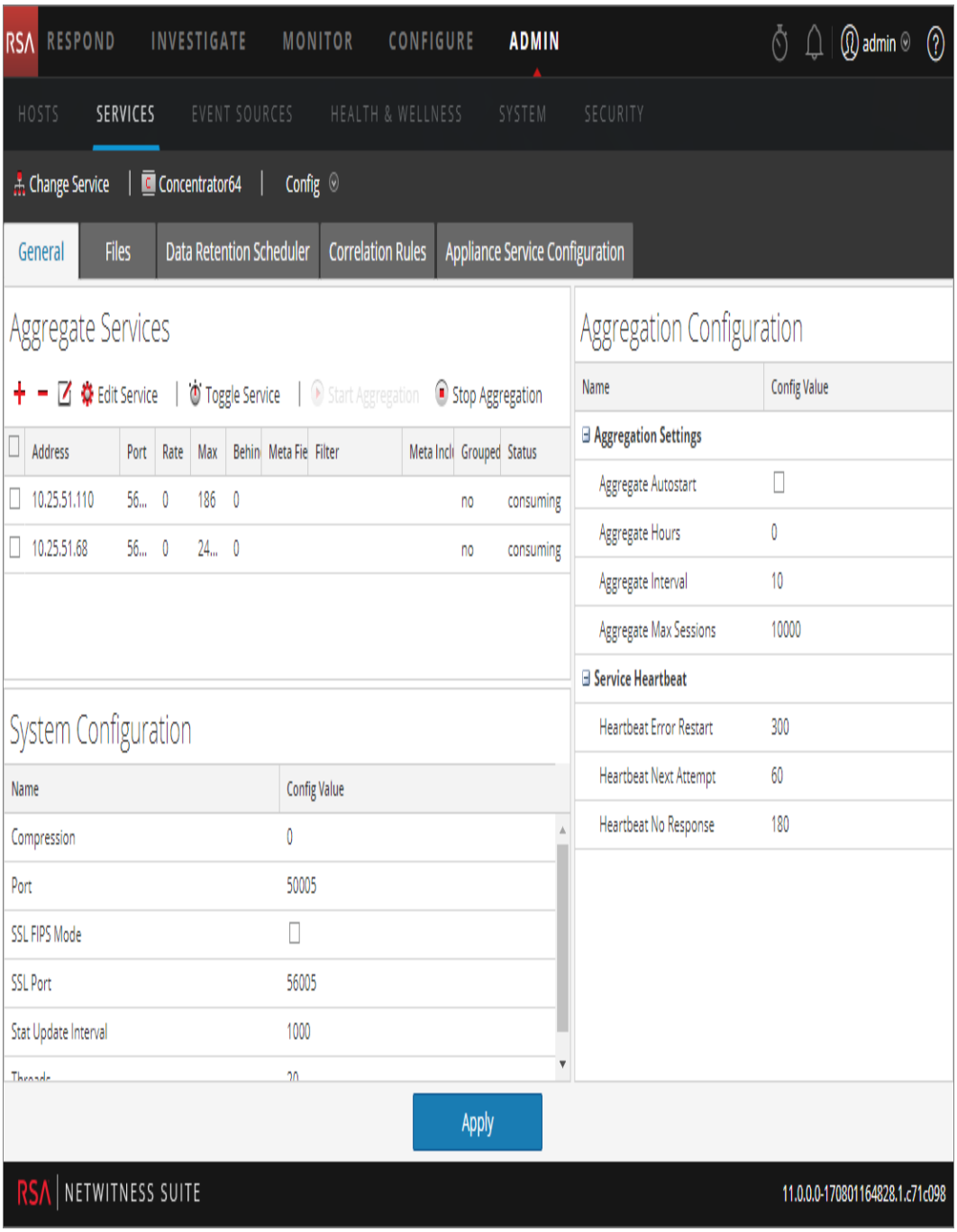
1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
   La vue Services Administration s'affiche.
2. Sélectionnez un service et cliquez sur  **>Vue > Config**.
   La vue Configuration des services s'affiche pour le service sélectionné.

Aperçu rapide

Exemple de vue Configuration des Services pour un Decoder.



Exemple de vue Configuration des Services pour un Concentrator.



Rubriques

- Rubrique
- Fonctionnalités
- Modifier un fichier de configuration de service

Onglet Configuration du service Appliance

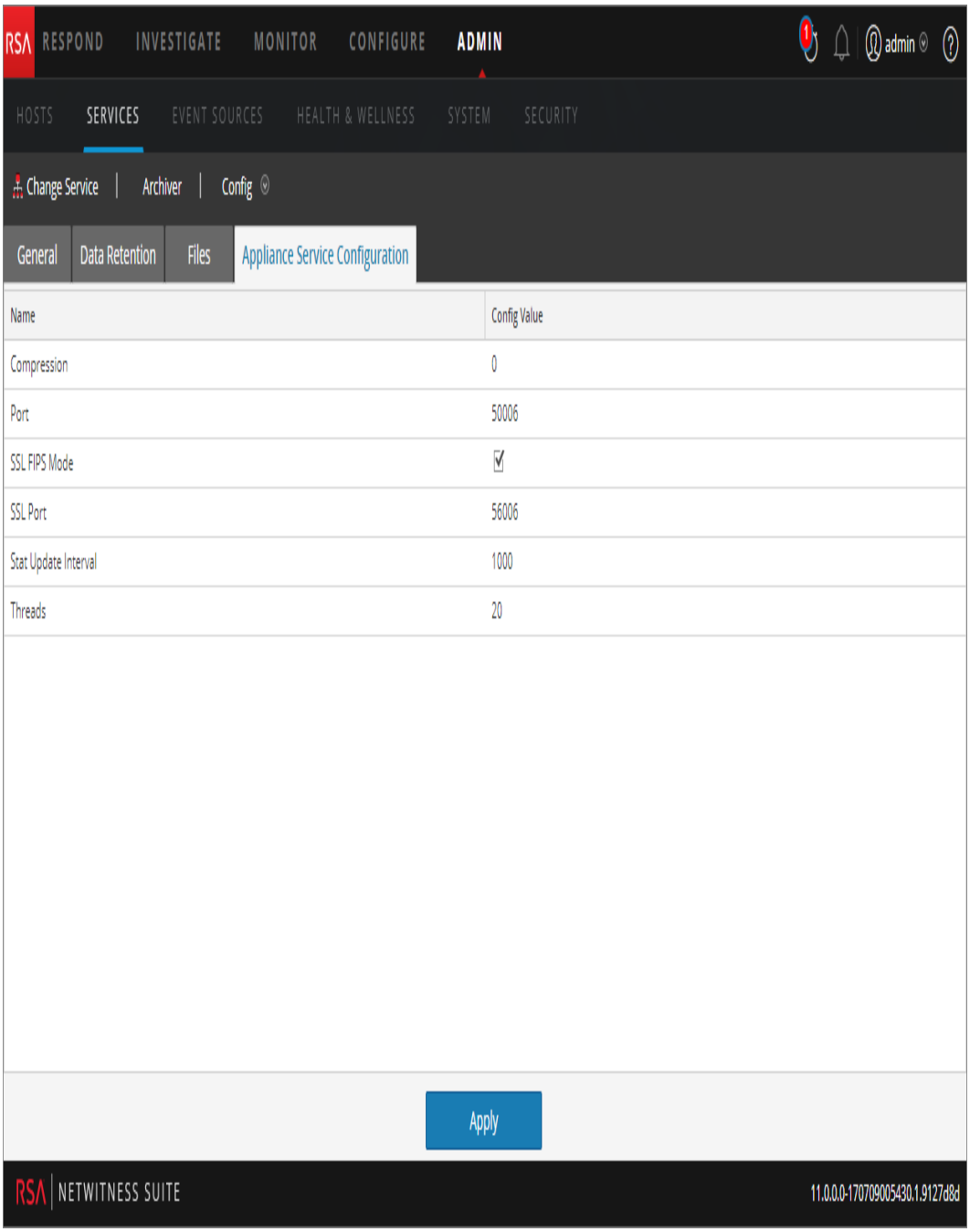
Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour le service NetWitness Suite Core Appliance. Le service NetWitness Suite Core Appliance surveille le matériel NetWitness existant.

La vue Configuration pour les services Archiver, Broker, Concentrator, IPDB Extractor, Decoder, Log Collector ou Log Decoder possède un onglet intitulé Configuration du service Appliance.

Pour accéder à l'onglet Configuration du service Appliance :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
   La vue Services Administration s'affiche.
2. Sélectionnez un service et cliquez sur  **>Vue > Config**.
   La vue Configuration des services correspondant au service Archiver s'affiche.
3. Cliquez sur l'onglet **Configuration du service Appliance**.

Exemple de l'onglet Configuration du service Appliance pour un service Archiver.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Archiver
Config
General
Data Retention
Files
Appliance Service Configuration
Name
Config Value
Compression
0
Port
50006
SSL FIPS Mode
SSL Port
56006
Stat Update Interval
1000
Threads
20
Apply
RSA
NETWITNESS SUITE
11.0.0.0-170709005430.1.9127d8d

Nom	Description de la valeur de configuration	Quand les modifications prennent effet
Compression	Compresse un message lorsqu'il atteint le nombre positif (en octets) que vous spécifiez.	La prochaine fois que vous vous connectez à ce service.
Port	Port d'écoute chiffré. **0** indique que le port est désactivé.	Lors du redémarrage du service.
Mode FIPS SSL	Un des paramètres nécessaires à l'activation ou la désactivation de la norme FIPS (Federal Information Processing Standards). Reportez-vous à « Activer ou désactiver la norme FIPS » dans le Guide de maintenance du système RSA NetWitness® Suite pour obtenir des instructions détaillées.	Lors du redémarrage du service.
Port SSL	Port d'écoute SSL (Secure Sockets Layer). **0** indique que le port est désactivé. SSL est la technologie de sécurité standard pour l'établissement d'un lien chiffré entre un serveur web et d'un navigateur Web. Ce lien garantit que toutes les données transitant entre le serveur Web et les navigateurs restent privées et intégrales.	Lors du redémarrage du service.
Intervalle de mise à jour des statistiques	La fréquence (en millisecondes) à laquelle le système met à jour les nœuds statistiques pour la surveillance de l'intégrité.	Immédiatement.

Nom	Description de la valeur de configuration	Quand les modifications prennent effet
Threads	Threads dans le pool de threads requis utilisés pour traiter les demandes. Le paramètre **Threads** fonctionne avec le paramètre **Intervalle d'interrogation** pour les threads de log et d'événements.	Immédiatement.

Rubrique

Paramètres de configuration du service Appliance

Onglet Planificateur de rétention des données

Cette rubrique décrit les options configurables disponibles 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.

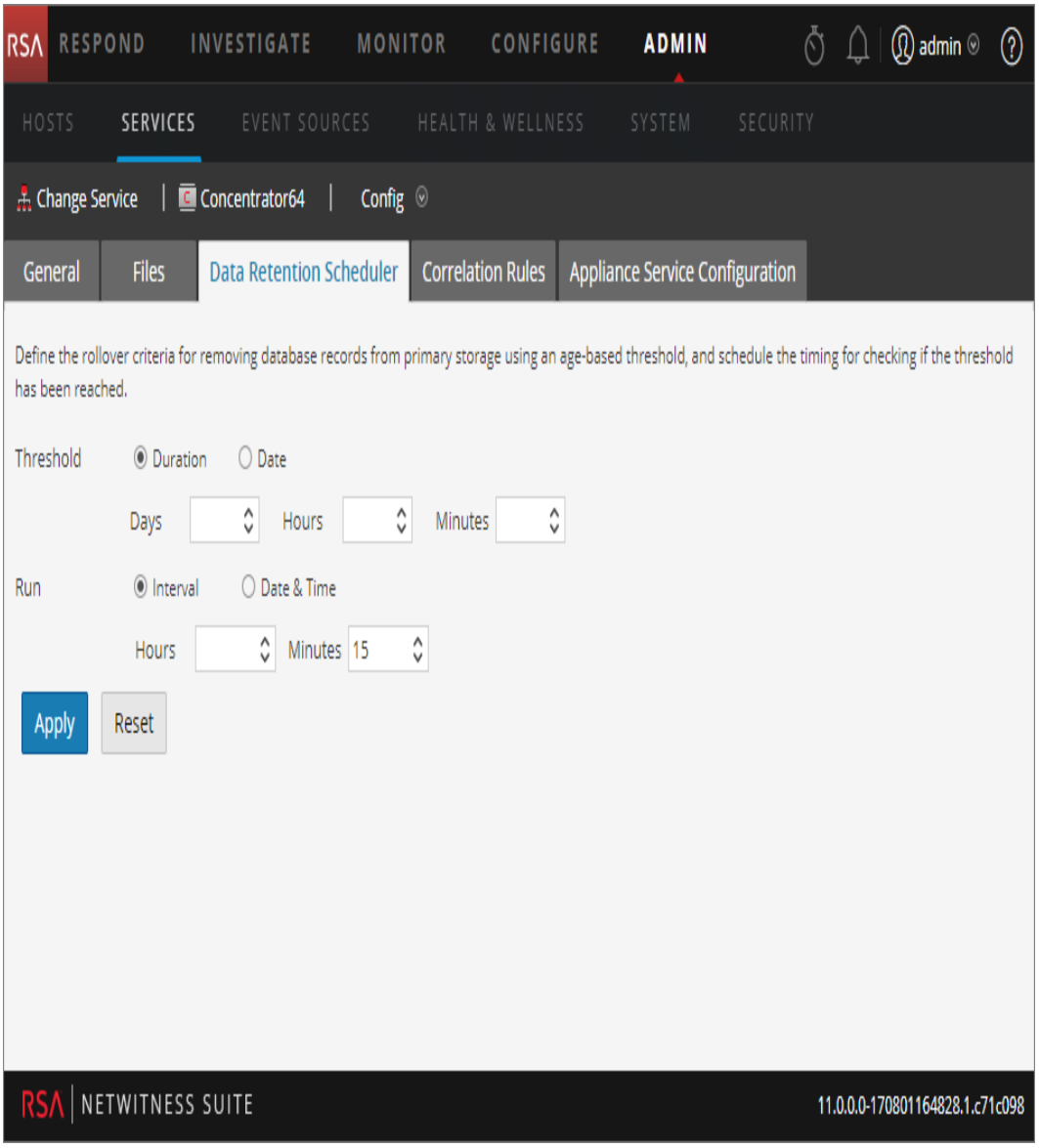
Pour des informations sur l'onglet Rétention de données pour Archiver, consultez la rubrique **Onglet Rétention de données - Archiver** dans le *Guide de configuration d'Archiver*.

Remarque : 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 **NetWitness Suite**, accédez à **ADMIN > 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 un service Concentrator.



Fonctionnalités

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
Threshold	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. **Attention :** 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 les suivants :

- 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.

Remarque : 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.

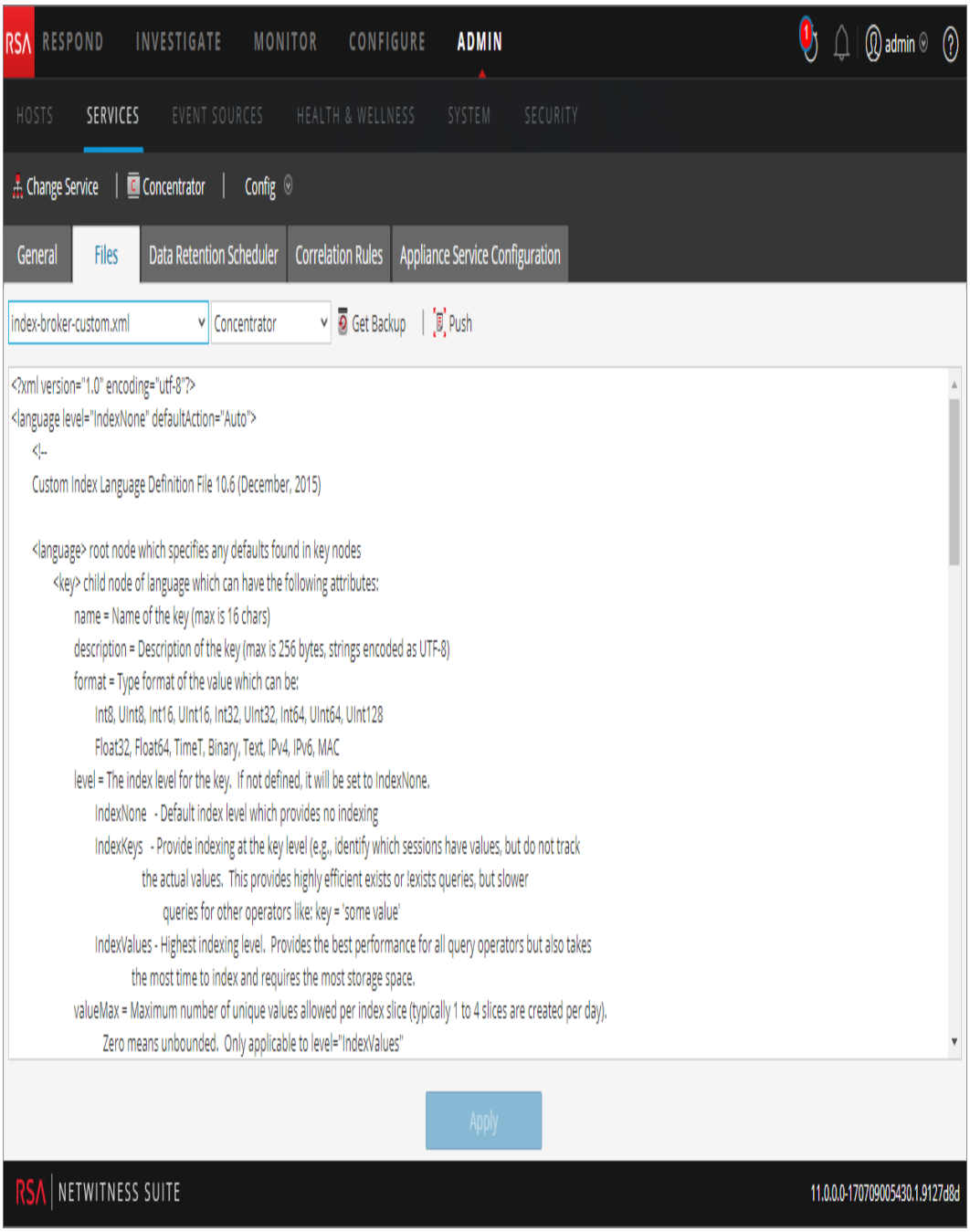
Pour accéder à l'onglet Fichiers :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
2. Sélectionnez un service, puis sélectionnez  **> Vue > Config**.
   La vue Configuration des services s'ouvre sur l'onglet **Général**.
3. Cliquez sur l'onglet **Fichiers**.

Rôle	Je souhaite...
Administrateur	Modifier un fichier de configuration de service.

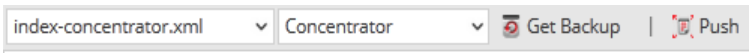
Modifier un fichier de configuration de service

Exemple de l'onglet Fichiers.



Barre d'outils onglet Fichiers

L'onglet Fichiers possède une barre d'outils et une fenêtre de modification. Exemple de la barre d'outils.



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

Fonctionnalité	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.
	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**.
	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 NetWitness Suite, 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 NetWitness Suite. 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 :

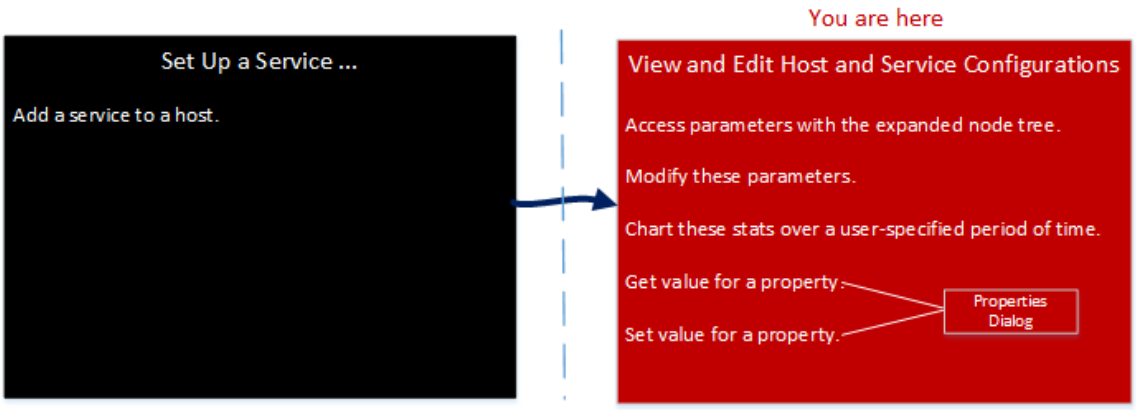
- Afficher une arborescence de répertoires présentant des fichiers communs pour tous les services sélectionnés.
- Accéder à un fichier dans le répertoire.
- Ouvrir le même fichier pour chaque service et afficher le contenu côte à côte.
- Sélectionner une entrée dans le fichier et modifier sa valeur.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

Attention : 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.

Workflow

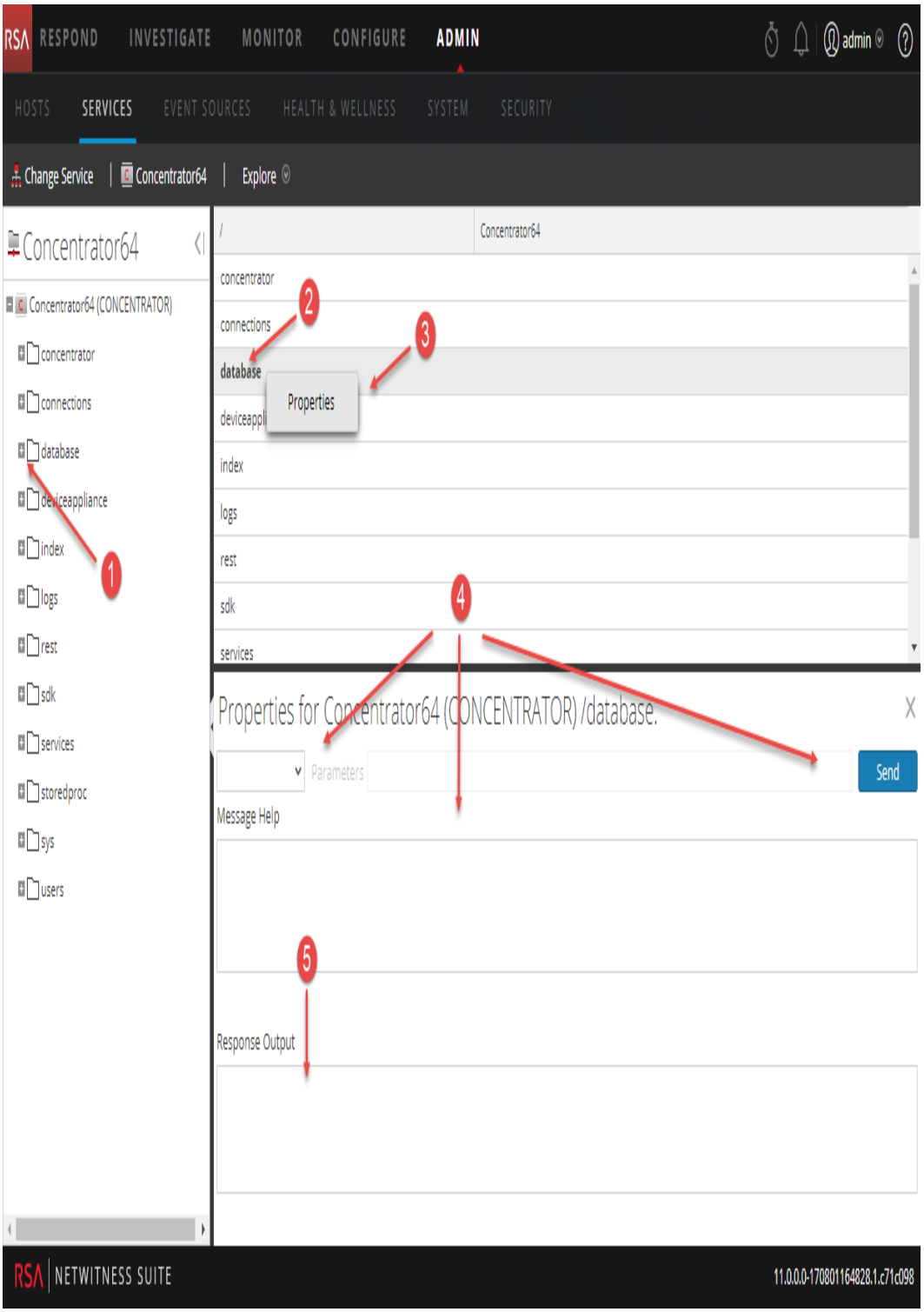
Ce workflow présente les tâches que vous effectuez à partir de la vue Explorer.



Aperçu rapide

Pour accéder à la vue Explorer les services :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
2. Sélectionnez un service, puis > **Vue > Explorer**.



1. Développez le nœud pour afficher ses catégories de paramètres.
2. Cliquez sur une propriété (par exemple, **meta.dir**) pour la sélectionner.
3. Cliquez sur un nœud ou une catégorie avec le bouton droit de la souris et sélectionnez **Propriétés** pour afficher la boîte de dialogue Propriétés.
4. Effectuez une opération sur un nœud ou une catégorie :
   a. Sélectionnez une commande dans la liste déroulante.
   b. Saisissez une chaîne de commande (si nécessaire).
   c. Cliquez sur **Envoyer**.
5. Vérifiez le résultat de la commande.

Fonctionnalités

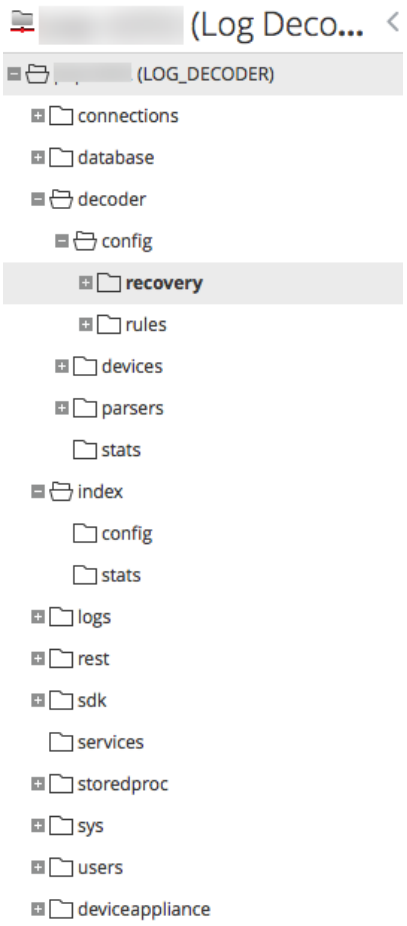
La **vue Explorer les services** possède deux panneaux principaux :

- 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.

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.



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

Rubriques

- Fonctionnalités
- Hôte GS : Paramètres de configuration du service Log Decoder

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.

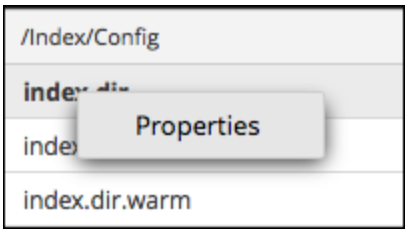
Tous les nœuds prennent en charge le message d'aide, qui contient :

- 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 NetWitness Suite.

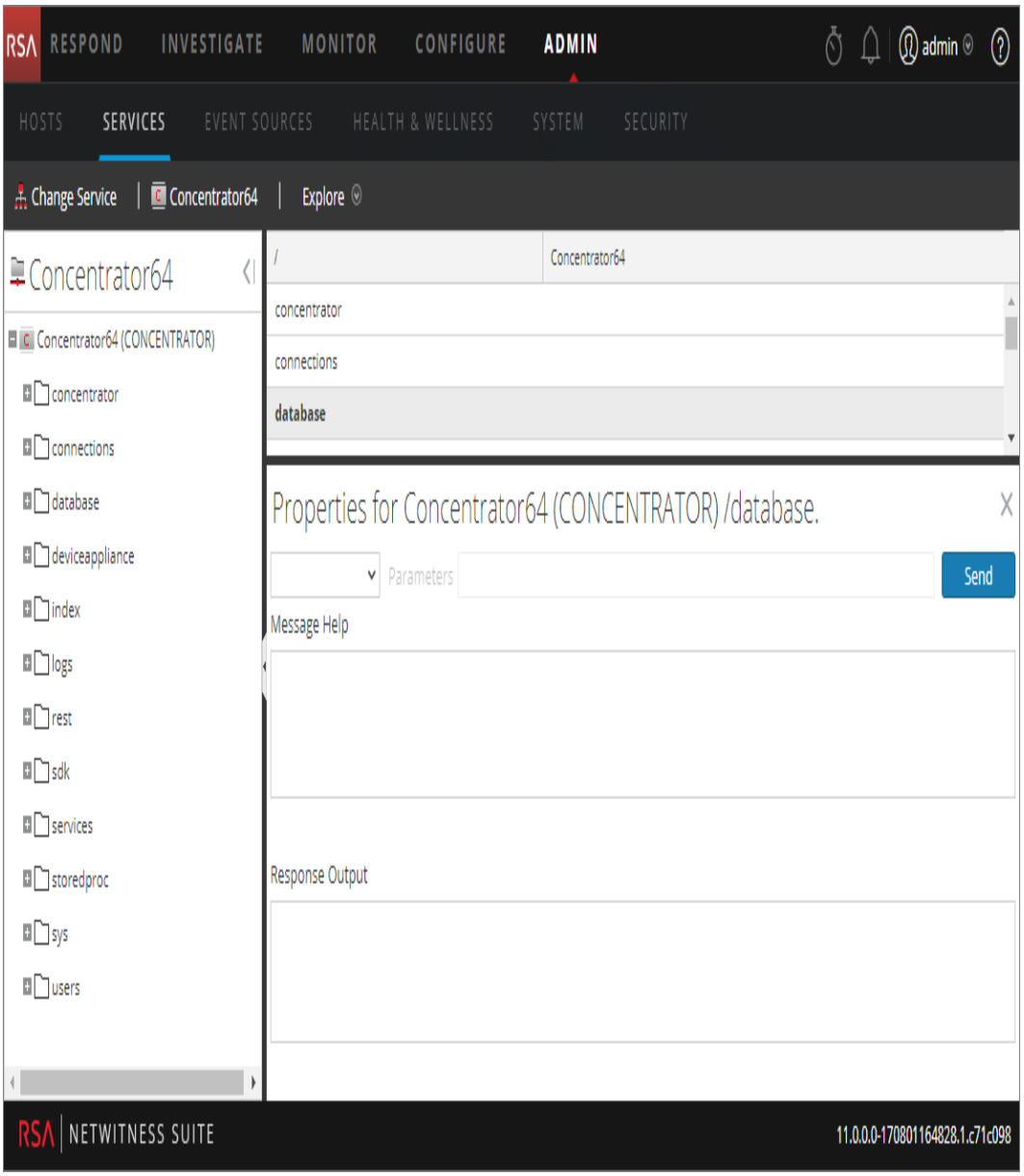
Pour accéder à la boîte de dialogue Propriétés :

1. Dans **NetWitness Suite**, accédez à **ADMIN > 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**).



Fonctionnalités

La boîte de dialogue Propriétés possède les fonctions suivantes.

Fonctionnalité	Description
Liste déroulante **Message**	Répertorie tous les messages disponibles du nœud en cours. Sélectionnez un message à envoyer au nœud.
Champ de saisie **Paramètres**	Saisissez 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.

Vue Logs de services

Cette section 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 :

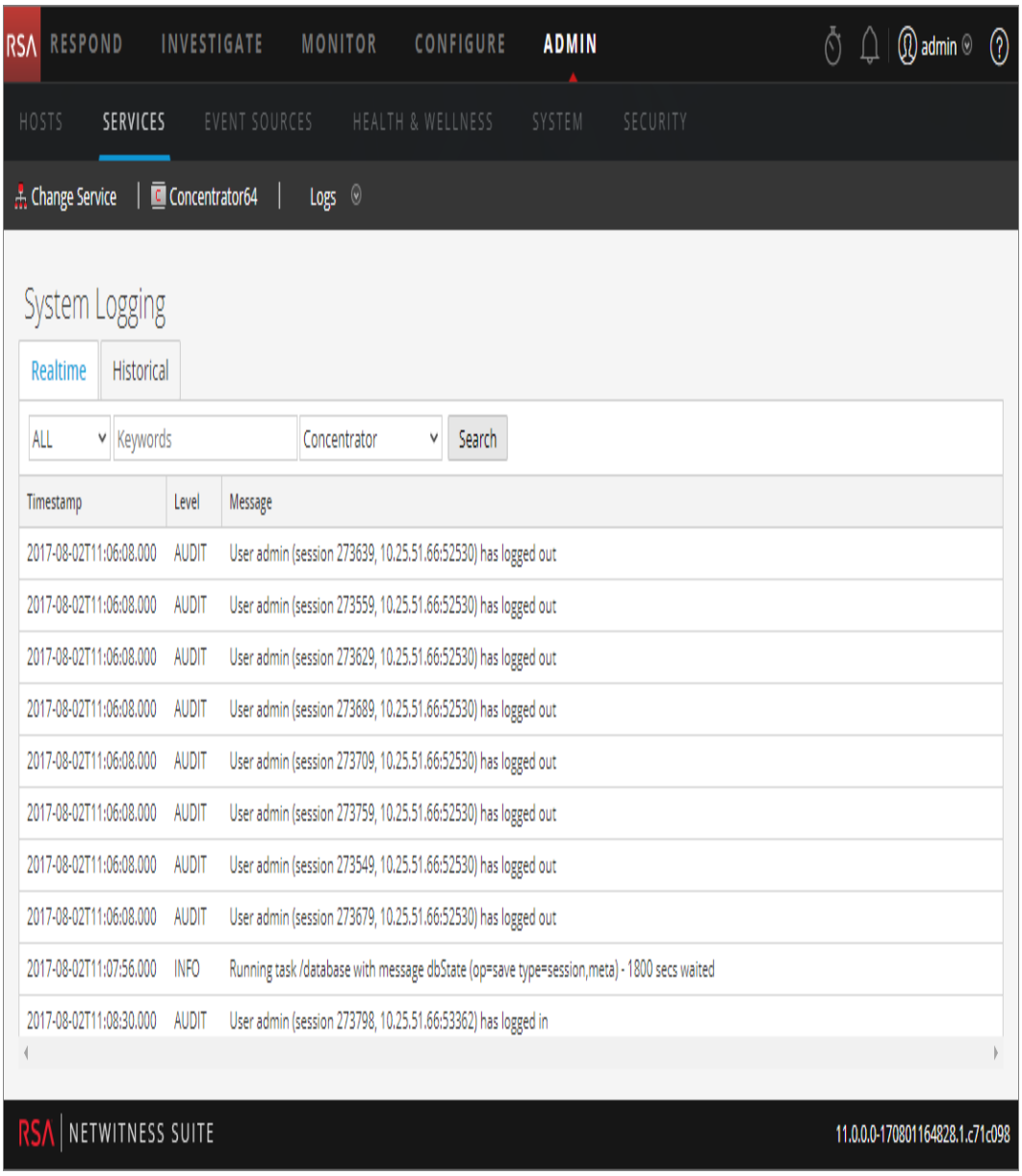
- Les logs de services disposent d'un filtre supplémentaire pour sélectionner les messages pour le service ou l'hôte.
- Le panneau de consignation système contient un onglet supplémentaire pour les paramètres.

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

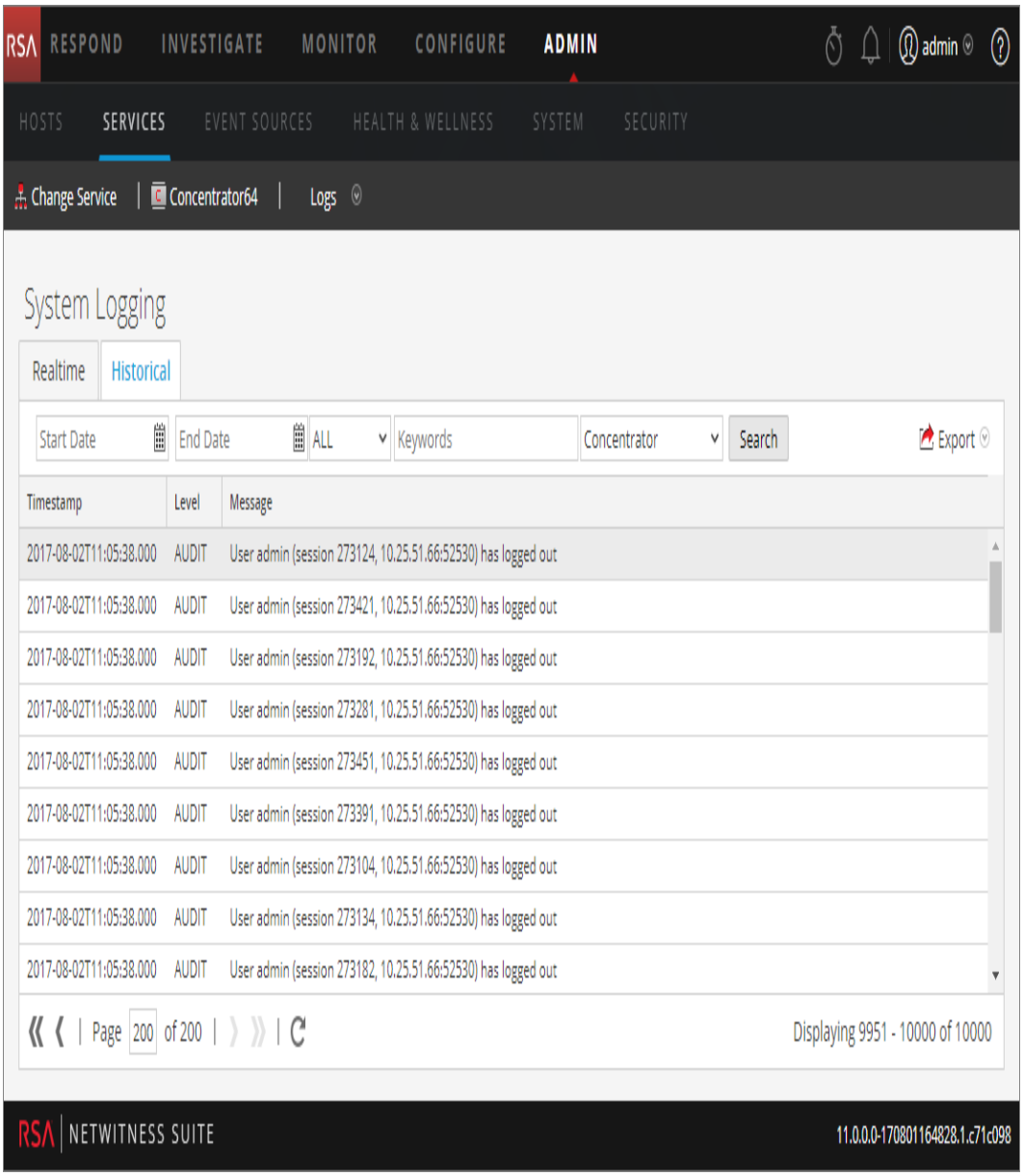
Pour afficher un log de service :

1. Dans **NetWitness Suite**, accédez à **ADMIN > 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.



Fonctionnalités

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** dans le *Guide de maintenance du système*).

Fonctionnalité	Description
Onglet En temps réel	C'est le mode surveillance du log de service.

Fonctionnalité	Description
Onglet Historique	C'est une vue du log de service dans laquelle une recherche peut être effectuée.

Vue Sécurité des services

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

Dans NetWitness Suite, 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 NetWitness Suite, un utilisateur doit appartenir à un rôle doté d'autorisations sur le service en question. Pour les services NetWitness Suite Core 10.4 ou version ultérieure qui utilisent des connexions de confiance, il n'est plus nécessaire de créer des comptes utilisateurs NetWitness Suite Core pour les utilisateurs qui se connectent via le client Web. Vous devez simplement créer des comptes utilisateur NetWitness Suite Core pour l'agrégation, les utilisateurs clients thick et les utilisateurs de l'API REST.

Remarque : Dans NetWitness Suite, 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 NetWitness Suite Administration > Services. Pour tous les autres utilisateurs, vous devez configurer l'accès à chacun des services via NetWitness Suite.

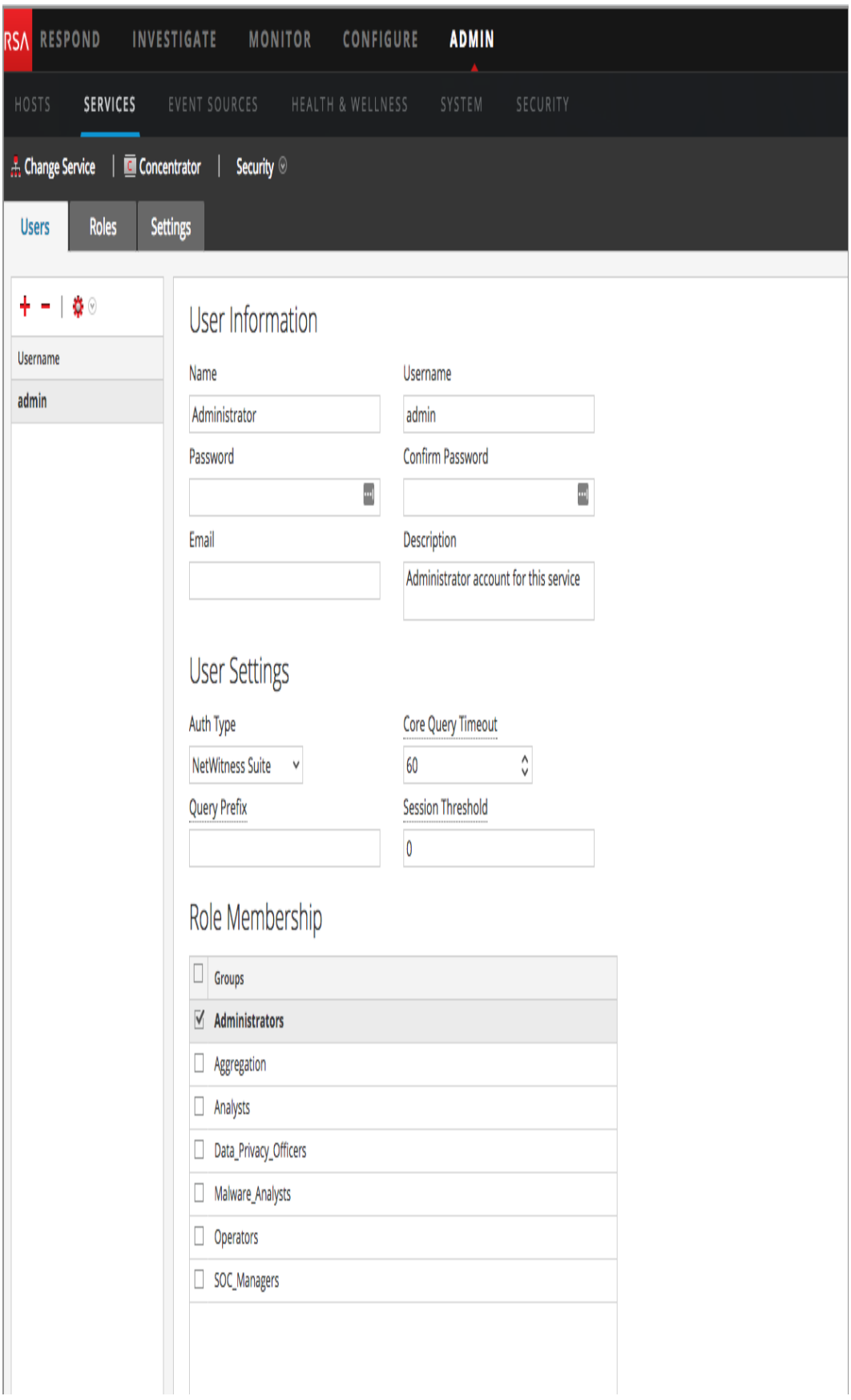
Les procédures liées à cet onglet sont décrites dans la section Hôte GS : Procédures des hôtes et des services.

Pour accéder à la vue Sécurité des services :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.

2. Choisissez un service, puis sélectionnez  **> Vue > Sécurité**.

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


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Concentrator
Security
Users
Roles
Settings
Username
admin
User Information
Name
Administrator
Username
admin
Password
Confirm Password
Email
Description
Administrator account for this service
User Settings
Auth Type
NetWitness Suite
Core Query Timeout
60
Query Prefix
Session Threshold
0
Role Membership
Groups
Administrators
Aggregation
Analysts
Data_Privacy_Officers
Malware_Analysts
Operators
SOC_Managers

Fonctionnalités

La vue Sécurité des services comporte trois onglets : Utilisateurs, Rôles 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.

Rubriques

- Onglet Rôles
- Rôles et autorisations de l'utilisateur de service
- Rôle d'agrégation
- Onglet Paramètres
- Onglet Utilisateurs

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 Hôte GS : Procédures des hôtes et des services.

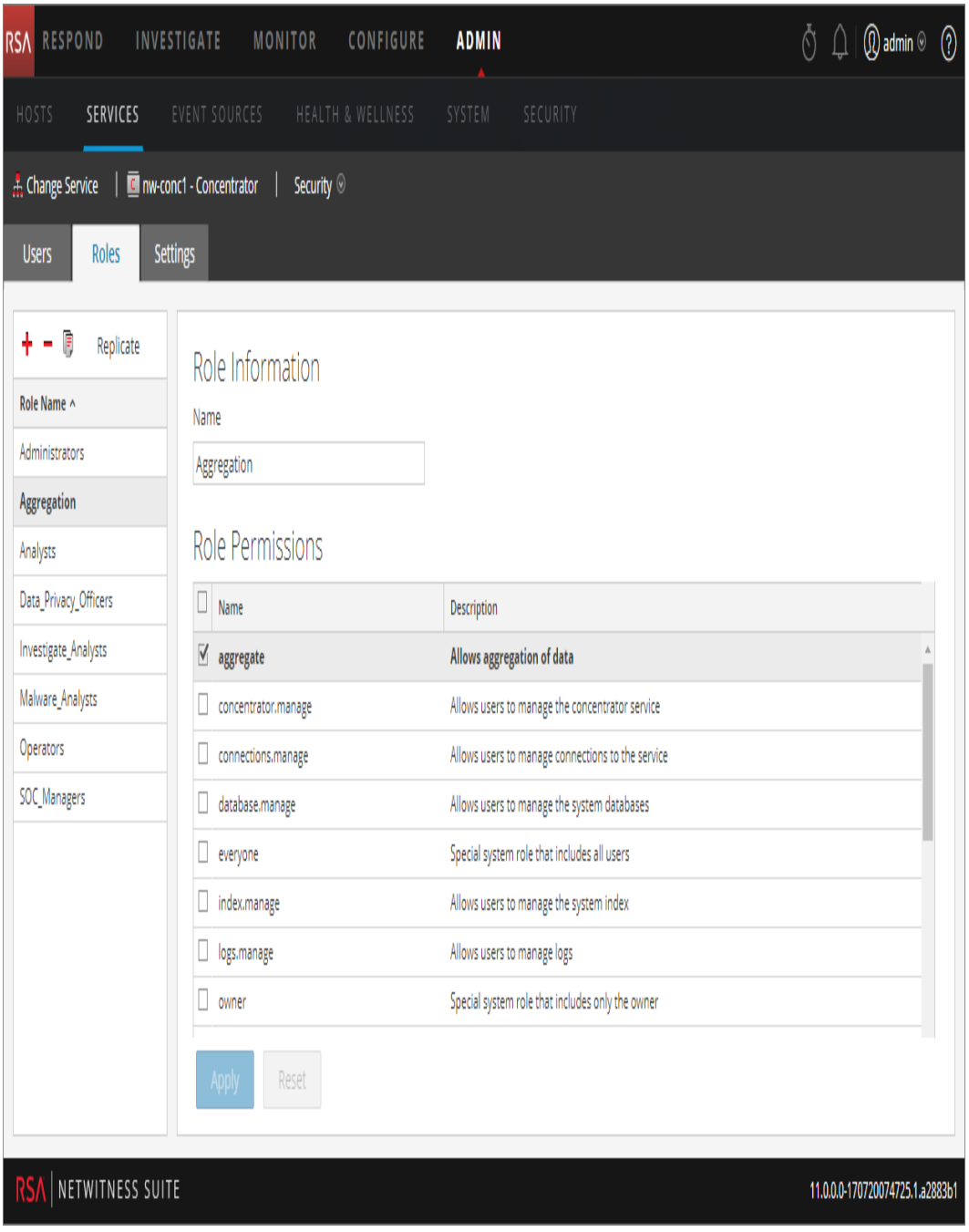
Pour afficher l'onglet Rôles de la vue **Sécurité des services** :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
2. Choisissez un 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.



Fonctionnalités

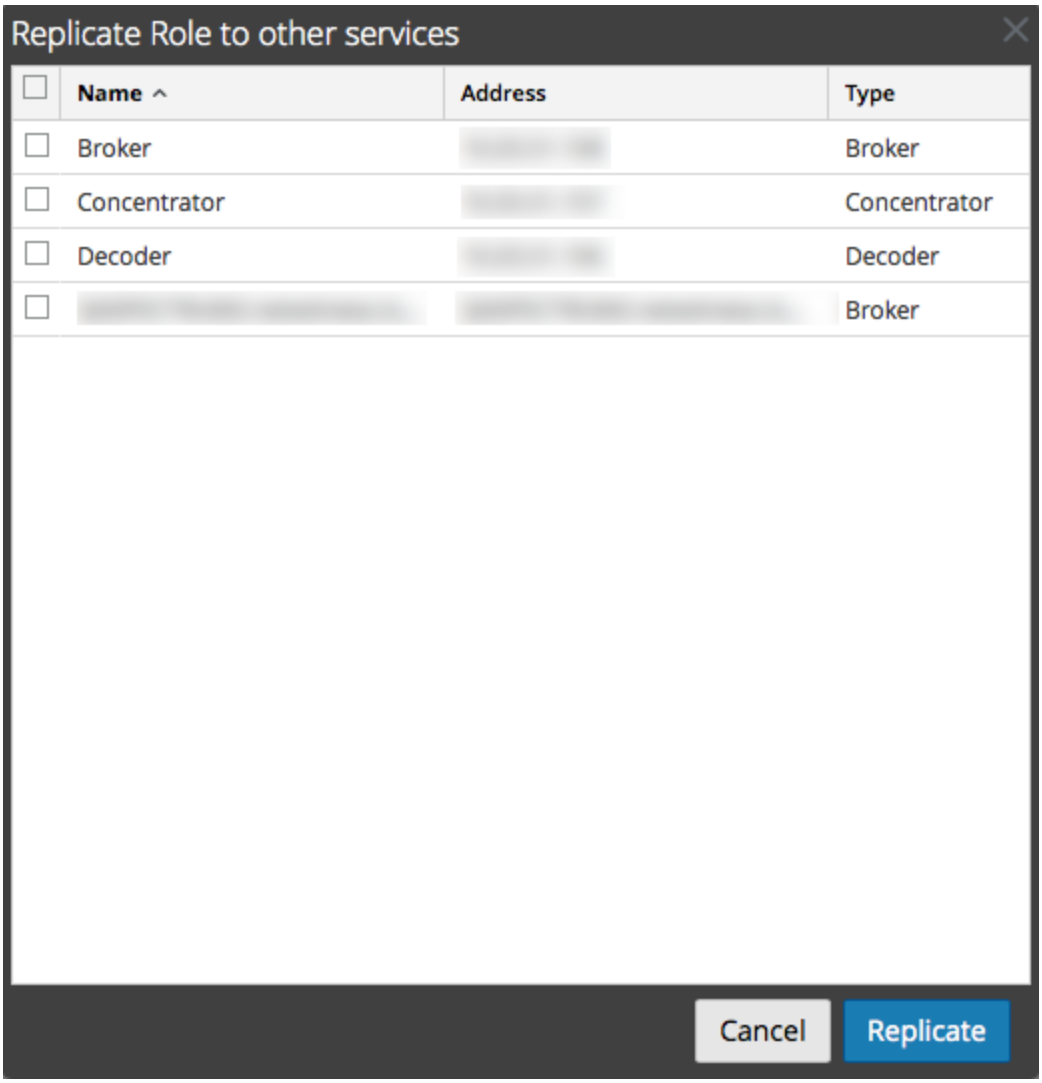
Le panneau **Nom du rôle** apparaît sur la gauche de l'onglet Rôles. Sélectionnez un nom de rôle pour faire apparaître sur la droite le panneau Informations sur le rôle correspondant au rôle sélectionné.

Panneau Nom du rôle

Le panneau **Nom du rôle** est doté des fonctionnalités suivantes.

Fonctionnalité	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**.
Répliquer	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 Informations et autorisations liées aux rôles

Le panneau **Informations et autorisations liées aux rôles** permet de définir les autorisations associées aux rôles.

Il comporte deux boutons :

- Le bouton **Appliquer** permet d'enregistrer les modifications apportées dans le panneau Autorisations du rôle et de les appliquer immédiatement.
- Si vous n'avez pas enregistré les modifications dans le panneau Autorisations du rôle, cliquez sur le bouton **Réinitialiser** pour rétablir la valeur de tous les champs et paramètres avant modification.

Rôles et autorisations de l'utilisateur de service

Cette rubrique décrit les rôles et les autorisations utilisateur de service préconfigurés.

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 NetWitness Suite pour attribuer des autorisations utilisateur.

Rôles utilisateur de maintenance

NetWitness Suite possède les rôles utilisateur de service préconfigurés suivants.

Rôle	Autorisations attribuées	Personnel/Compte
Administrateurs	Toutes les autorisations	Administrateur système NetWitness Suite
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 NetWitness Suite 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.
Data_Privacy_ Officers (Agents de protection 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.

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 NetWitness Suite. 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.

Autorisation	Définition
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.
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.

Autorisation	Définition
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.

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

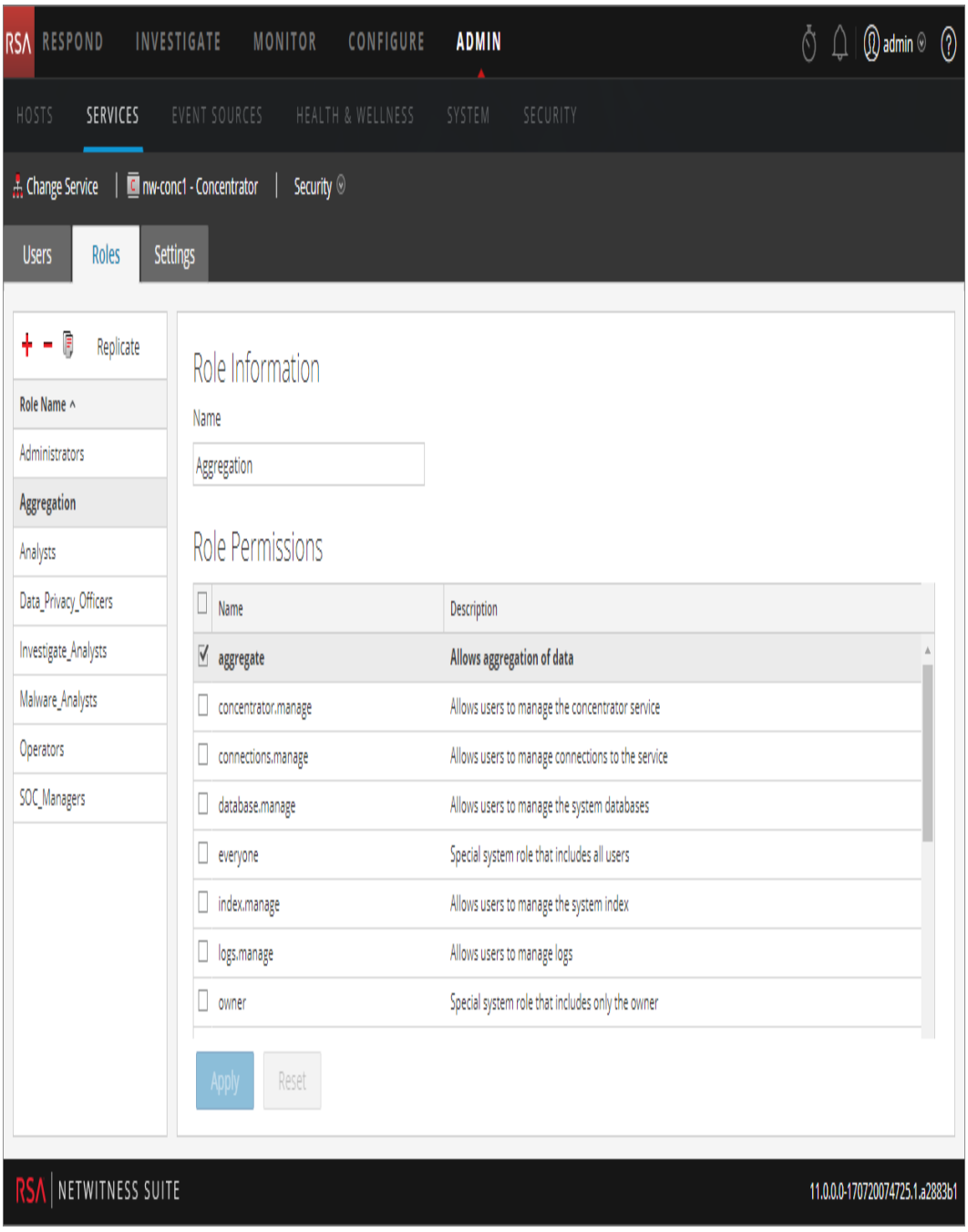
Le rôle d'agrégation n'est disponible que sur les services NetWitness Suite 10.5 et version ultérieure, et il est utilisable pour un compte d'agrégation. Les membres de ce rôle ou les utilisateurs de services dotés de ces autorisations peuvent réaliser des agrégations sur les Decoders, Concentrators, 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 ADMIN > Services (sélectionnez un service) > Actions > Vue > Sécurité > onglet Rôles.

Les procédures liées à cet onglet sont décrites dans la section Hôte GS : Procédures des hôtes et des services. La rubrique Rôles et autorisations de l'utilisateur de service contient des informations détaillées relatives aux rôles préconfigurés.

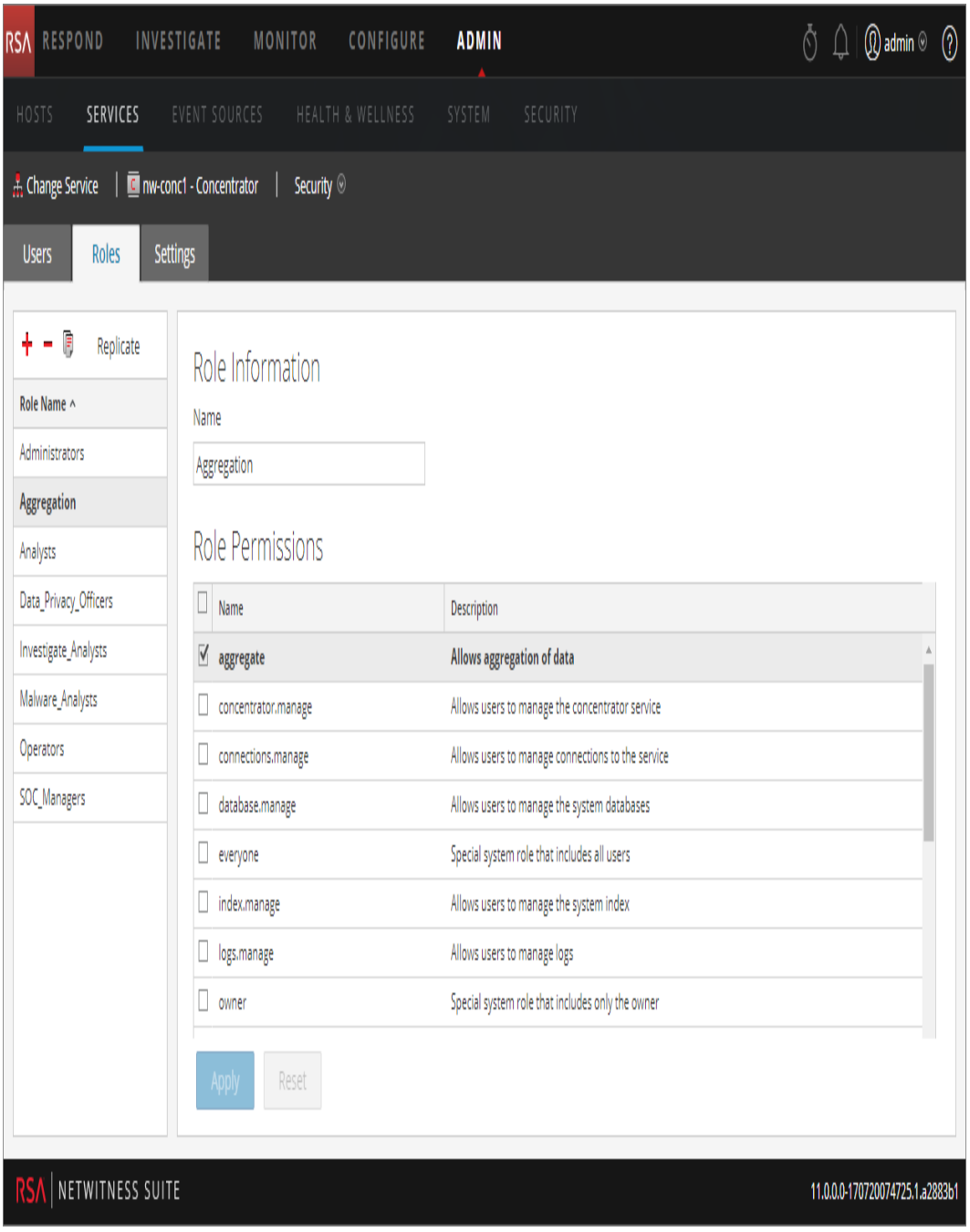
La figure ci-dessous illustre les autorisations du rôle d'agrégation.



Onglet Paramètres

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

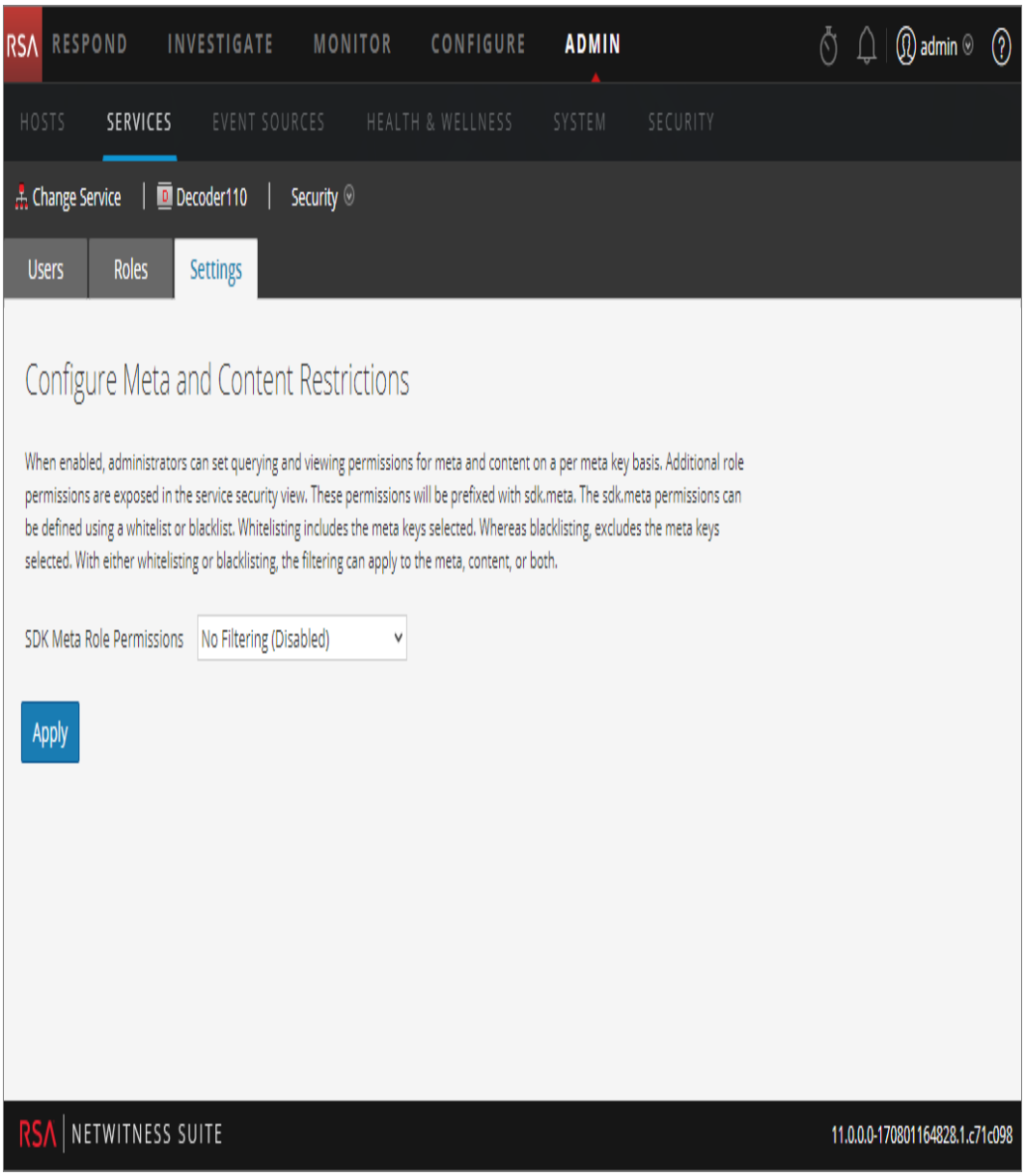
Sous l'onglet Paramètres de la vue Sécurité des services, les administrateurs peuvent activer et configurer les rôles de système qui définissent des permissions sur une base de clé par métadonnées pour les Brokers, Concentrators, Decoders et Log Decoders.individuels. La configuration de cette fonction 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 en est l'illustration.



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*).

Pour afficher l'onglet :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
2. Dans la grille **Services**, sélectionnez un service Decoder ou Log Decoder, cliquez sur  **> Vue > Sécurité,** puis cliquez sur l'onglet **Paramètres**.



Fonctionnalités

L'onglet comprend deux fonctions.

Fonctionnalité	Description
Champ Autorisations du 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 liées aux autorisations de rôle méta SDK

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

Remarque : 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.

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

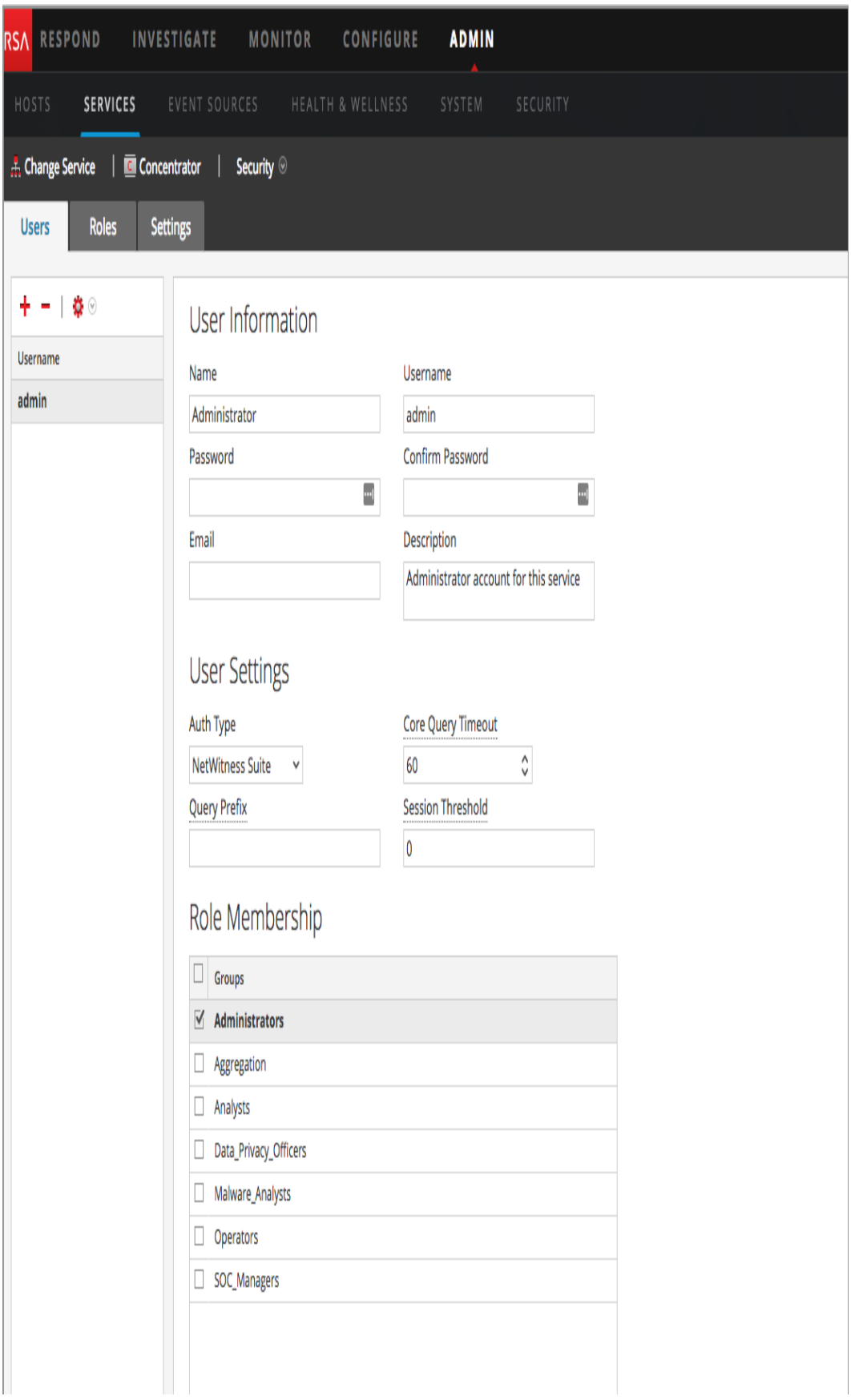
Remarque : pour les services NetWitness Suite Core 10.4 ou version ultérieure qui utilisent des connexions de confiance, il n'est plus nécessaire de créer des comptes utilisateurs NetWitness Suite Core pour les utilisateurs qui se connectent via le client Web. Vous devez simplement créer des comptes utilisateur NetWitness Suite Core pour l'agrégation, les utilisateurs clients thick et les utilisateurs de l'API REST.

Les procédures liées à cet onglet sont décrites dans la section Hôte GS : Procédures des hôtes et des services.

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

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.

2. Choisissez un service auquel vous voulez ajouter un utilisateur, puis sélectionnez  **> Vue > Sécurité**.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Concentrator
Security
Users
Roles
Settings
Username
admin
User Information
Name
Administrator
Username
admin
Password
Confirm Password
Email
Description
Administrator account for this service
User Settings
Auth Type
NetWitness Suite
Core Query Timeout
60
Query Prefix
Session Threshold
0
Role Membership
Groups
Administrators
Aggregation
Analysts
Data_Privacy_Officers
Malware_Analysts
Operators
SOC_Managers

Fonctionnalités

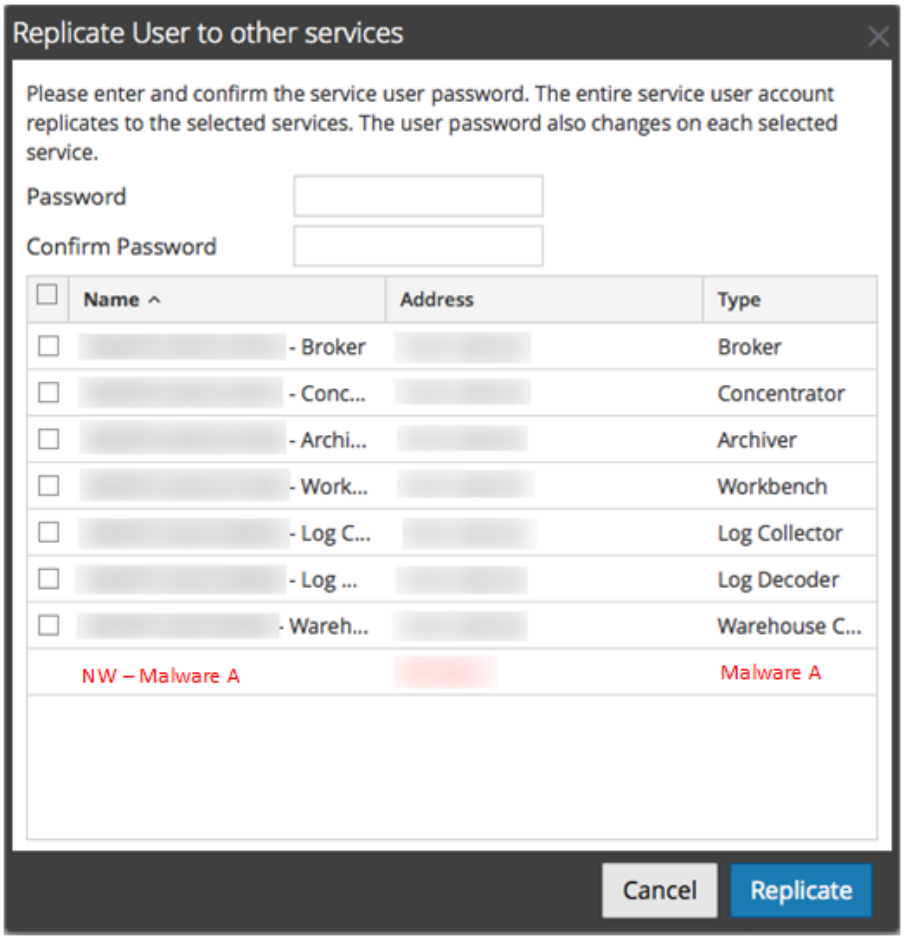
L'onglet Utilisateurs est doté d'un volet Liste d'utilisateurs sur la gauche. Le choix d'un nom d'utilisateur rend disponible le volet Définition de l'utilisateur sur la droite.

Volet Liste d'utilisateurs

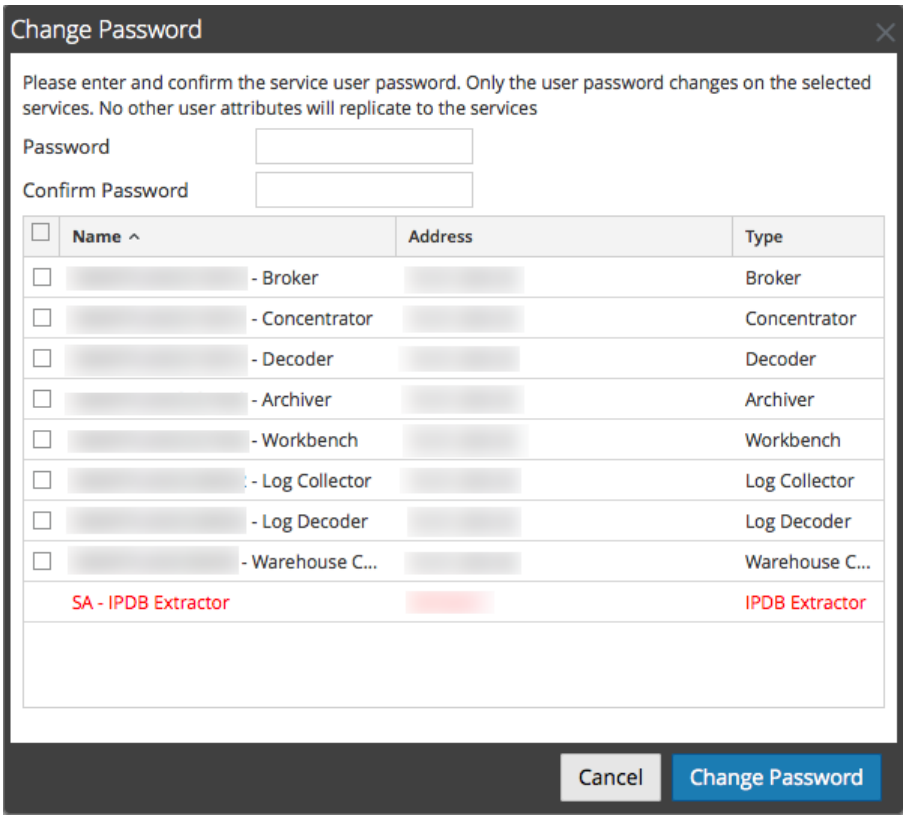
Le volet Liste d'utilisateurs est doté des fonctionnalités suivantes.

Fonctionnalité	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. • **Changer 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 Changer 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 utilisés pour ouvrir une session sur NetWitness Suite.

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



La figure suivante illustre la boîte de dialogue **Changer 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 comporte 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.
Nom d'utilisateur	Le nom d'utilisateur que saisit cet utilisateur pour ouvrir une session du service. Il s'agit du nom d'utilisateur NetWitness Suite 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 NetWitness Suite 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 NetWitness Suite et celui du service doivent correspondre afin que l'utilisateur puisse se connecter au service via NetWitness Suite.
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 Sécurité sous Administration (Administration > Sécurité) de NetWitness Suite 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 section **Configurer la fonctionnalité de connexion PAM** dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Champ	Description
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 SA Core	**Remarque :** ce champ s'applique à NetWitness Suite 10.5 et versions de service ultérieures, il ne s'affiche pas pour la version 10.4 et les versions de service antérieures. NetWitness Suite 10.4 et les services antérieurs utilisent le niveau de requête au lieu de l'expiration du délai de requête SA Core. 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 NetWitness Suite 10.5 ou ultérieur vers un service NetWitness Suite 10.4, Délai d'expiration 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.
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.

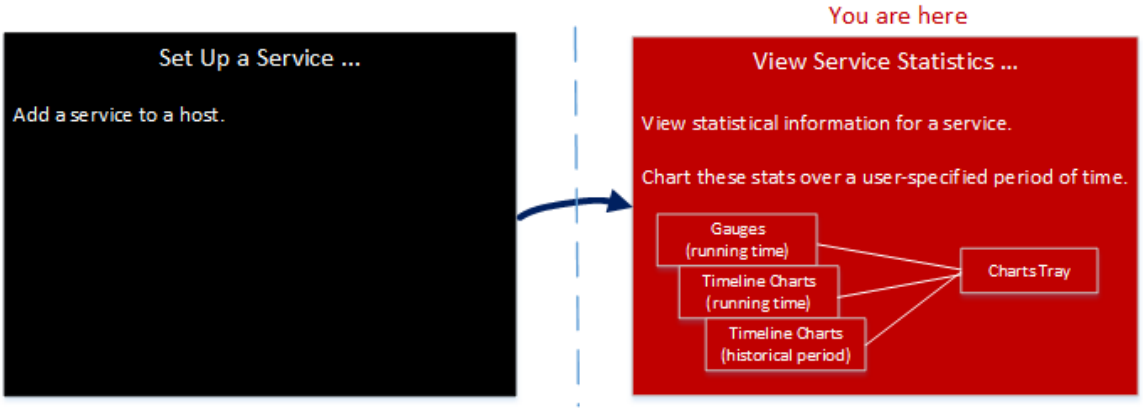
Vue Statistiques des services

Cette rubrique décrit les fonctionnalités disponibles dans la vue Statistiques des services de NetWitness Suite.

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.

Workflow

Ce workflow présente les tâches que vous effectuez à partir de la vue Statistiques.

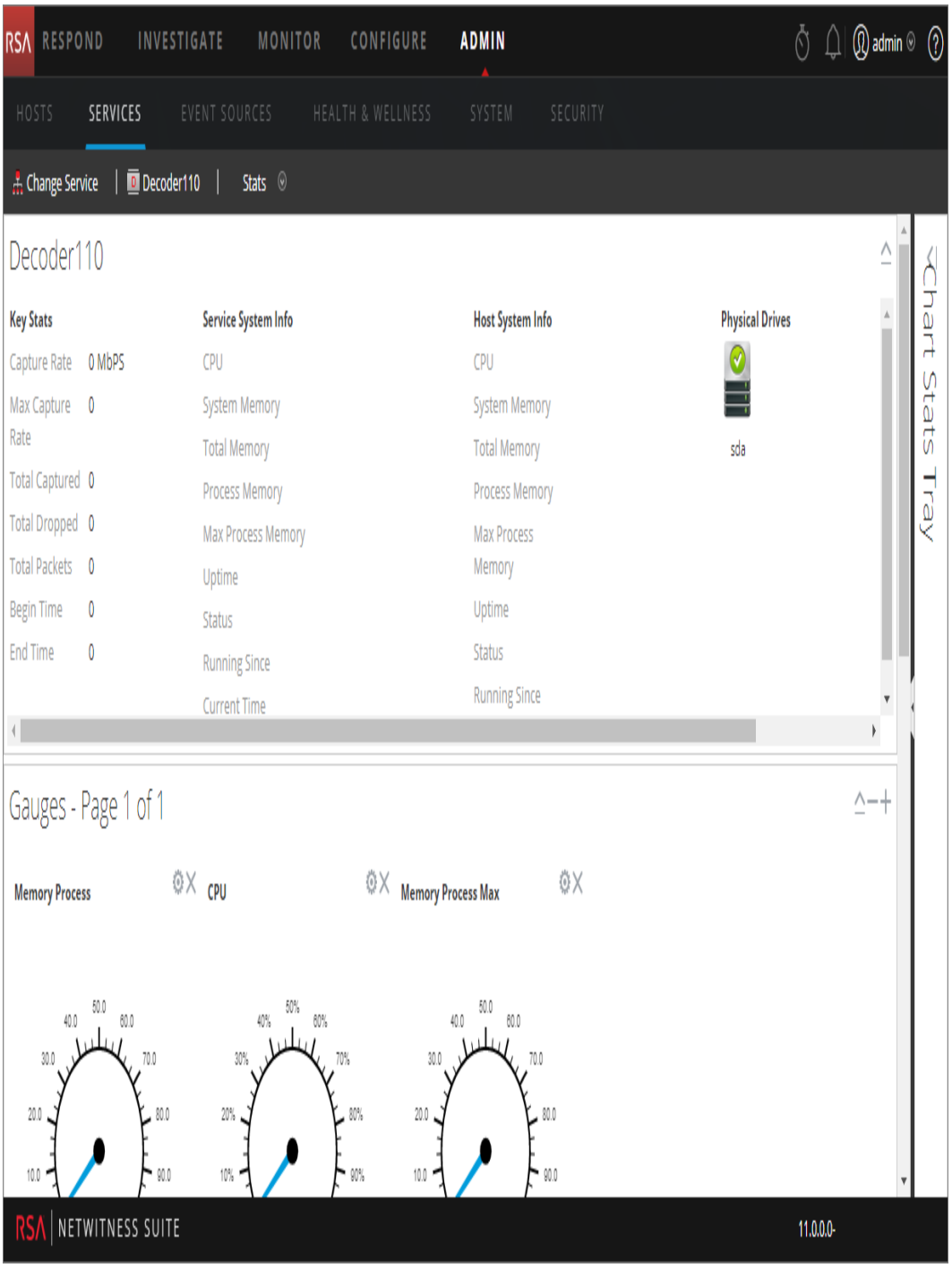


Dans la vue Statistiques, vous pouvez personnaliser les statistiques surveillées pour les différents services.

L'exemple suivant vous montre comment utiliser l'affichage des statistiques pour un Decoder. La vue Statistiques de tous les services vous fournit les mêmes informations pour chaque service.

Pour accéder à la vue Statistiques des services :

1. Dans **NetWitness Suite**, accédez à **ADMIN > Services**.
   La vue Services s'affiche.
2. Sélectionnez un service et sélectionnez  **> Vue > Statistiques**.



Fonctionnalités

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 de statistiques graphiques

Section Statistiques de synthèse

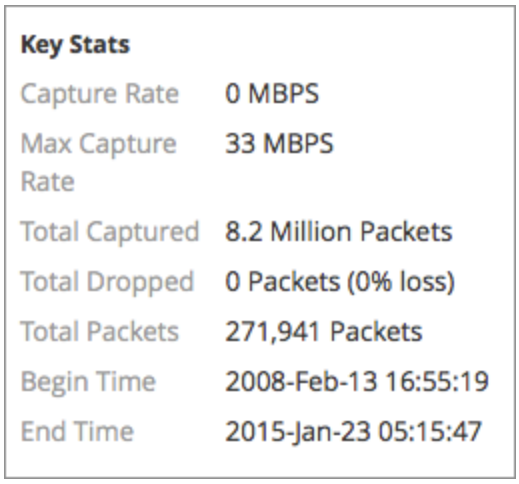
La section Statistiques de synthèse apparaît en haut de la vue par défaut et ne dispose pas de champs modifiables.

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.

Statistiques clés

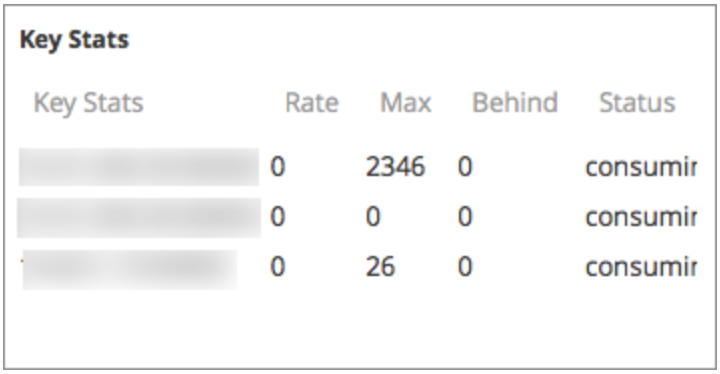
Le panneau Statistiques clés affiche des statistiques différentes pour des types de services différents.

- Pour un service 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.



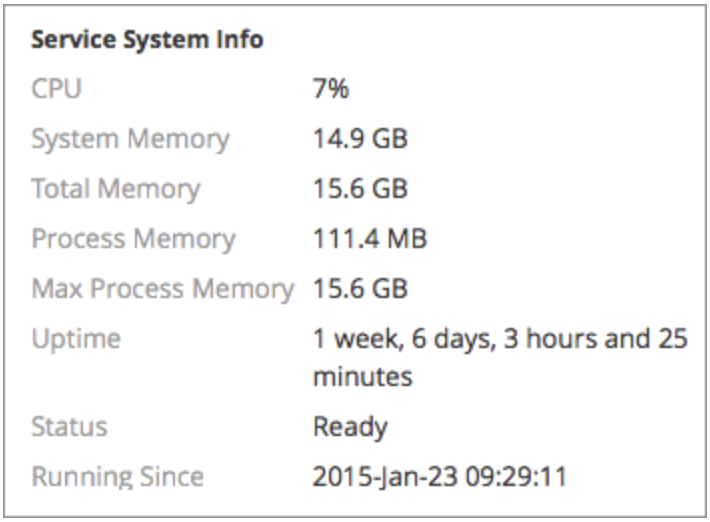
- Un Broker ou Concentrator agrège les données de plusieurs services. De ce fait, les statistiques clés de tous les services agrégés sont présentées dans une grille. Les colonnes de la grille indiquent le nom du service, le taux de capture, le nombre de sessions devant être

agrégées et l'état du service.

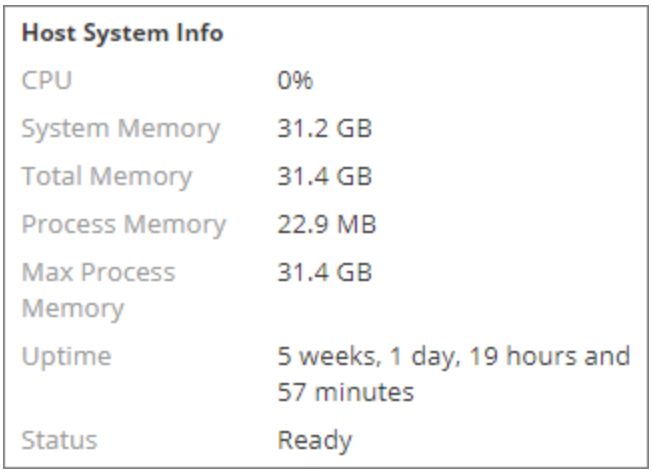


Info maintenance système

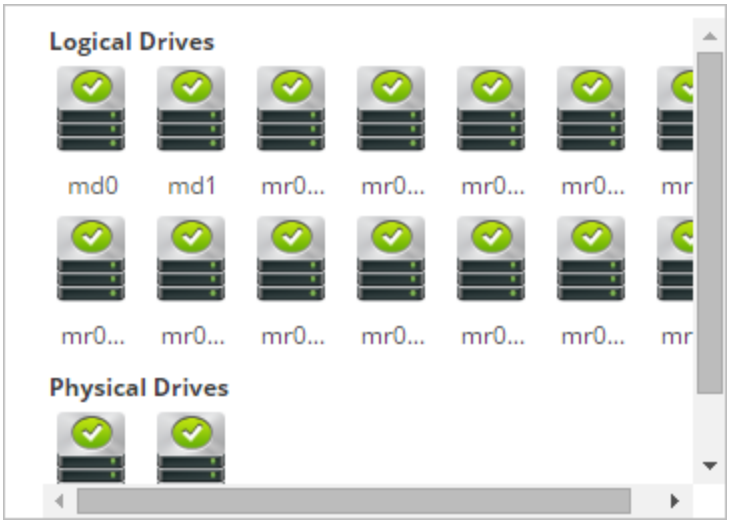
Le panneau Informations de maintenance du système comprend le pourcentage de CPU utilisé par le service, les statistiques d'utilisation de la mémoire (système, total, processus et processus maximum), la disponibilité, l'état, la durée d'exécution et l'heure actuelle du service.



Info sur le système hôte comprend 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.



Les **Lecteurs logiques** et les **Lecteurs 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.



Types et état du disque

Type de disque	Description	Commentaire	Options d'état
sd	Périphérique de bloc SCSI	Directement connecté aux volumes SAS, SATA MegaRAID	OK (vert) ÉCHEC (rouge)

Type de disque	Description	Commentaire	Options d'état
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 Fonctionnalités 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.

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.

Remarque : Les graphiques de chronologie historique est obsolète pour les services Log Collector, Virtual Log Collector (VLC) et collecteur Windows d'ancienne génération.

Barre de statistiques graphiques

La barre de statistiques graphiques répertorie toutes les statistiques disponibles pour le type de service sélectionné. Les différents services ont différentes statistiques à surveiller. Reportez-vous à la section Composants pour une description détaillée.

Rubriques

- Composants
- Fonctionnalités
- Graphiques chronologiques

Barre de statistiques graphiques

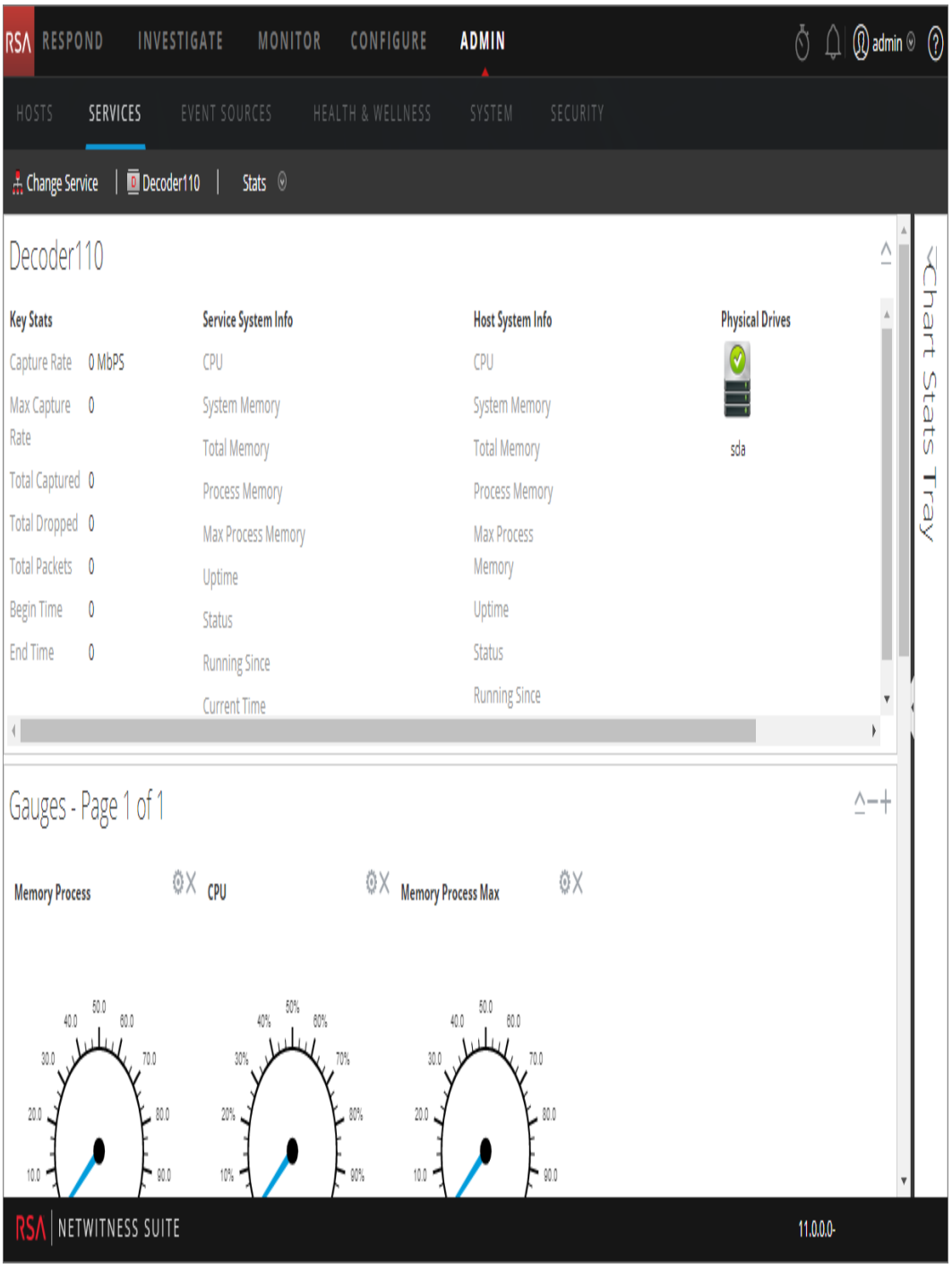
Cette rubrique décrit la barre de statistiques graphiques dans la vue Statistiques des services.

Dans la vue Statistiques des services, la barre de statistiques graphiques offre un moyen de personnaliser les statistiques surveillées des différents services. La barre de 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 de 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 :

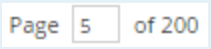
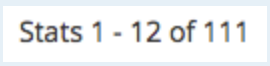
1. Dans le menu **NetWitness Suite**, sélectionnez **ADMIN > Services**.
   La vue Services d'administration s'affiche.
2. Sélectionnez un service, puis  **> Vue > Statistiques.**
   . La barre de statistiques graphiques se situe sur le côté droit.
3. Si cette barre est réduite, cliquez sur pour consulter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

L'exemple suivant affiche la vue Statistiques des services pour un Decoder. La barre de statistiques graphiques est réduite.



Composants

La barre de 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 de statistiques graphiques.

Fonctionnalité	Description
	Cliquez pour développer le panneau horizontalement.
	Cliquez pour réduire le panneau horizontalement.
Rechercher	Saisissez 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.
	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.
	Affiche la plage de statistiques. Le nombre total de statistiques varie selon le type de service.

Jauges

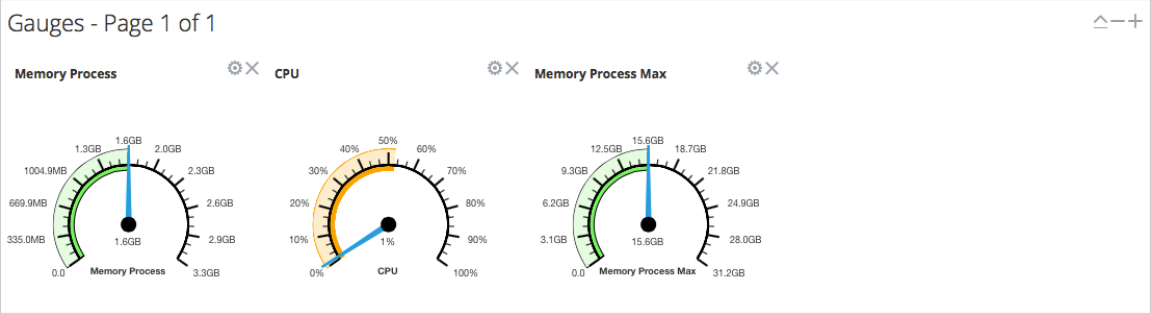
Cette rubrique présente les fonctions de la section Jauges dans la vue Statistiques des services.

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 de 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 **NetWitness Suite** , sélectionnez **ADMIN > Services**
   La vue Services d'administration s'affiche.
2. Sélectionnez un service et sélectionnez  **> 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.



Fonctionnalités

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.

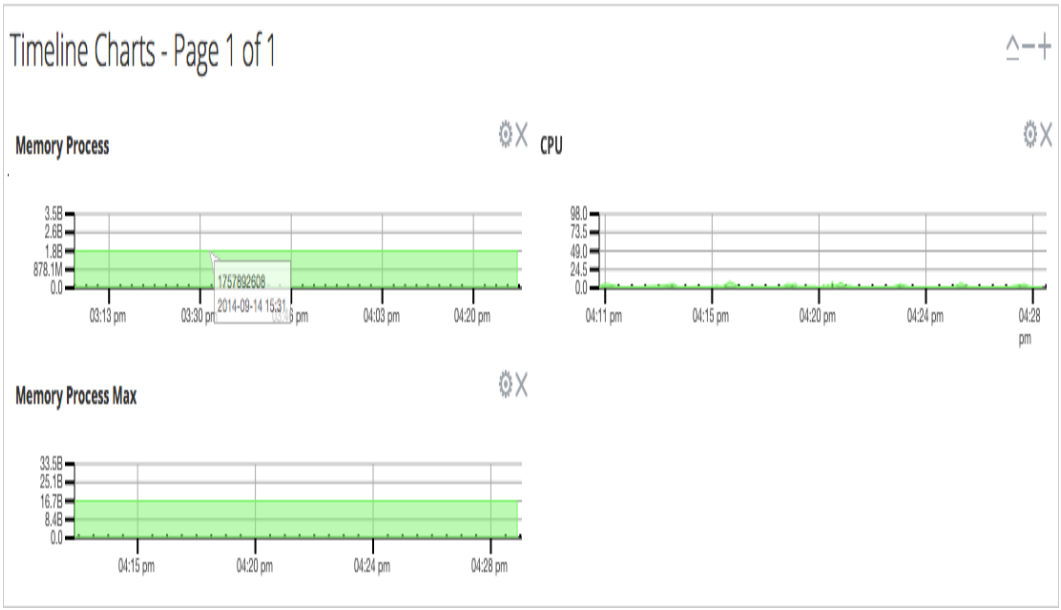
- Dans la barre de titre Jauges, vous pouvez réduire et développer la section et avancer ou reculer d'une page.
- Dans chaque jauge, vous pouvez modifier les propriétés ( ) et supprimer ( ) la jauge.

Graphiques chronologiques

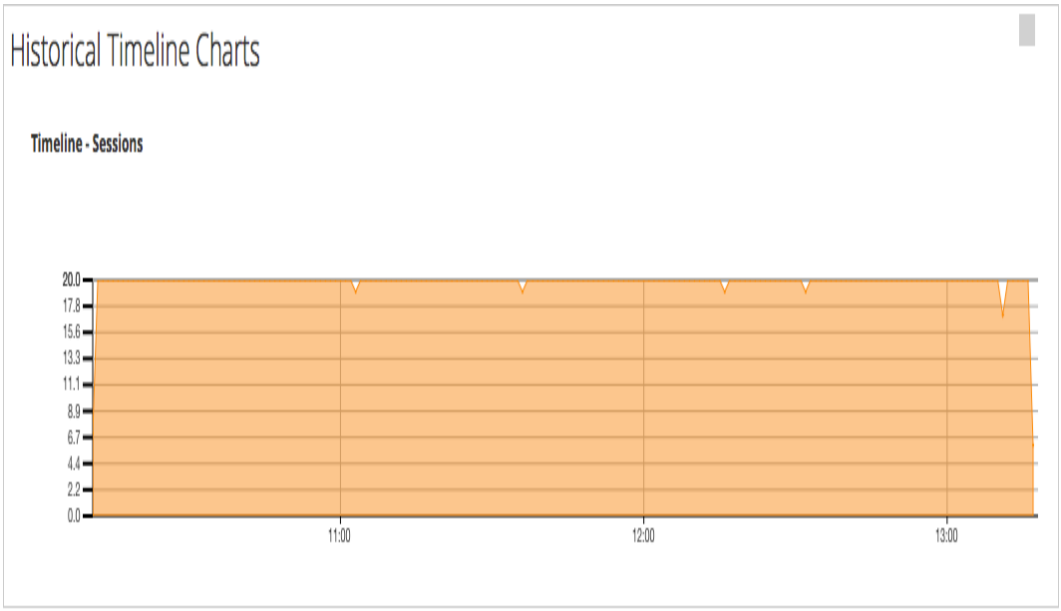
Cette rubrique décrit les fonctions des graphiques chronologiques dans la vue Statistiques des services.

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 de 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 :

- 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 système

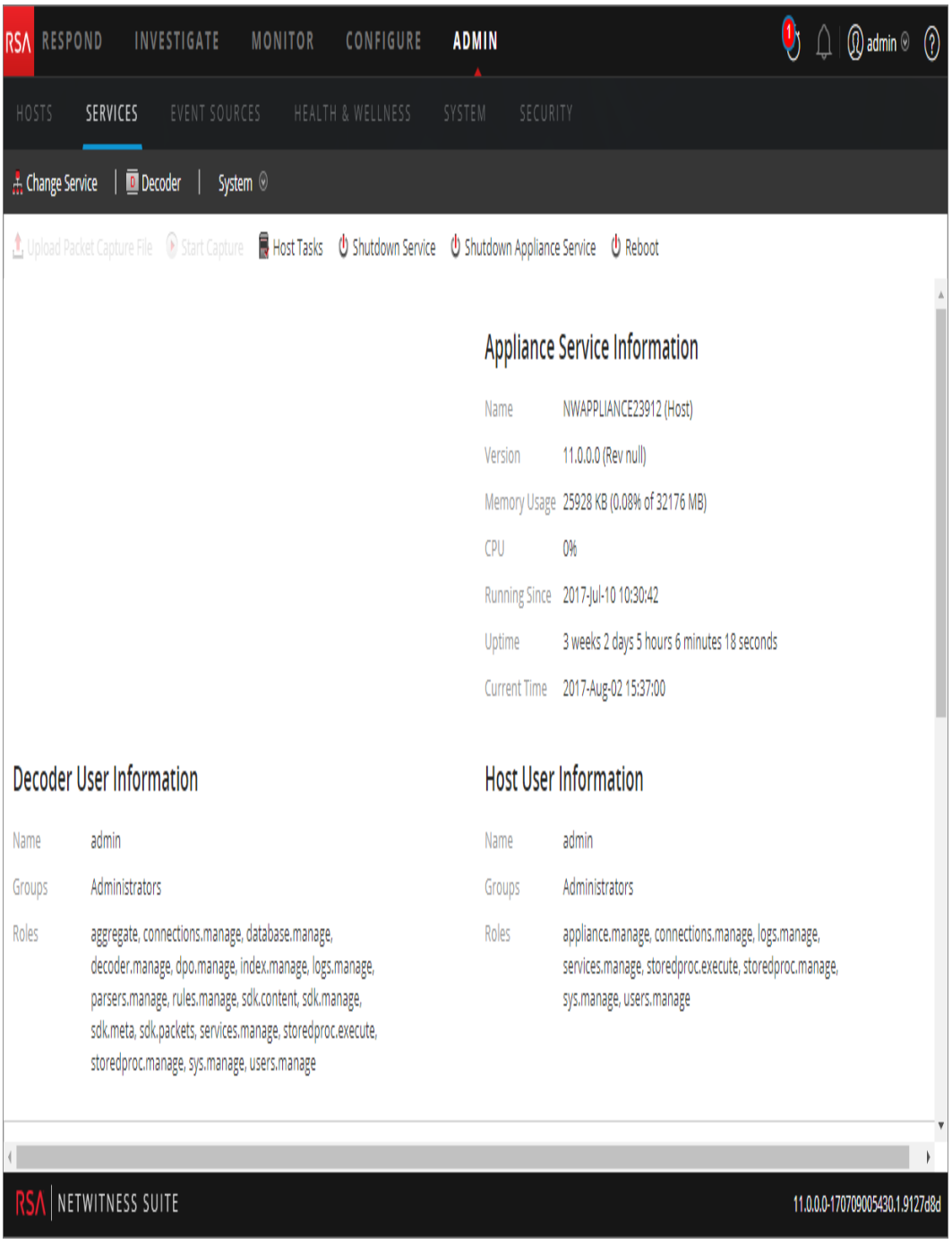
Cette section présente les fonctions dans la vue système à l'aide du Decoder et Log Decoder en tant qu'un exemple. Consultez les guides de configuration de chaque service (par exemple, *RSA NetWitness® Suite Guide de configuration des services Broker et Concentrator*) pour en savoir plus sur leurs vues **ADMIN > Services > Système**.

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.

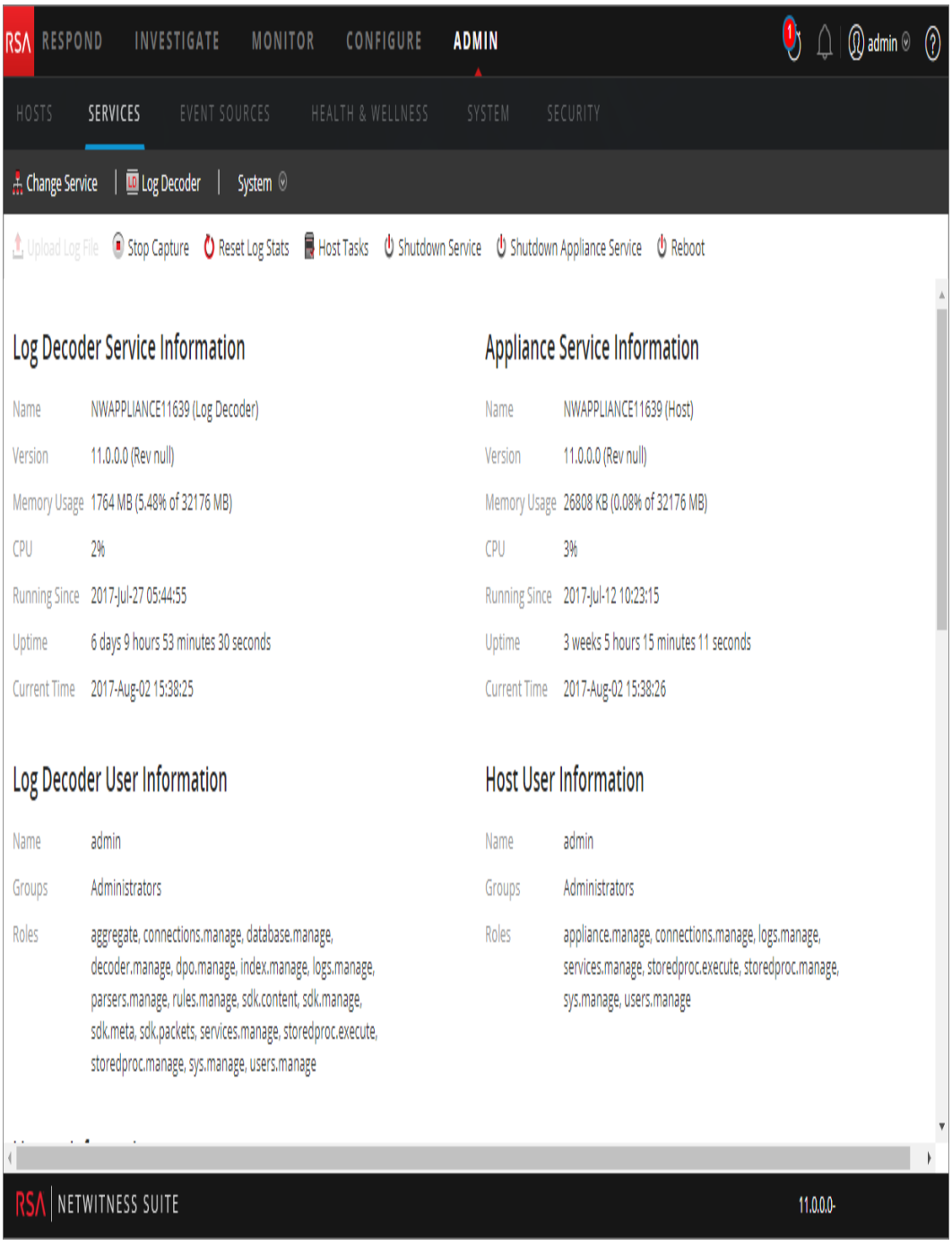
Pour accéder à la vue Système de services pour un Decoder :

1. Dans **NetWitness Suite** , accédez à **ADMIN > Services**.
   La vue Services s'affiche.
2. Choisissez un service, puis sélectionnez  **> Vue> Système**.

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



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



Fonctionnalités

Barre d'outilsInfo services

Les barres d'outils suivantes affichent les options spécifiques aux services Log Decoder et Decoder.

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 section **Télécharger le fichier de capture de paquets** dans le *Guide de configuration de Decoder et Log Decoder*. **Remarque :** Cette option ne s'applique pas aux Log Decoders.
Télécharger le fichier log	Affiche une boîte de dialogue qui propose une façon de sélectionner un fichier log (.log) à télécharger vers le Log Decoder sélectionné. Pour plus d'informations, reportez-vous à la section **Télécharger le fichier log vers un Log Decoder** dans le *Guide de configuration de Decoder et 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.

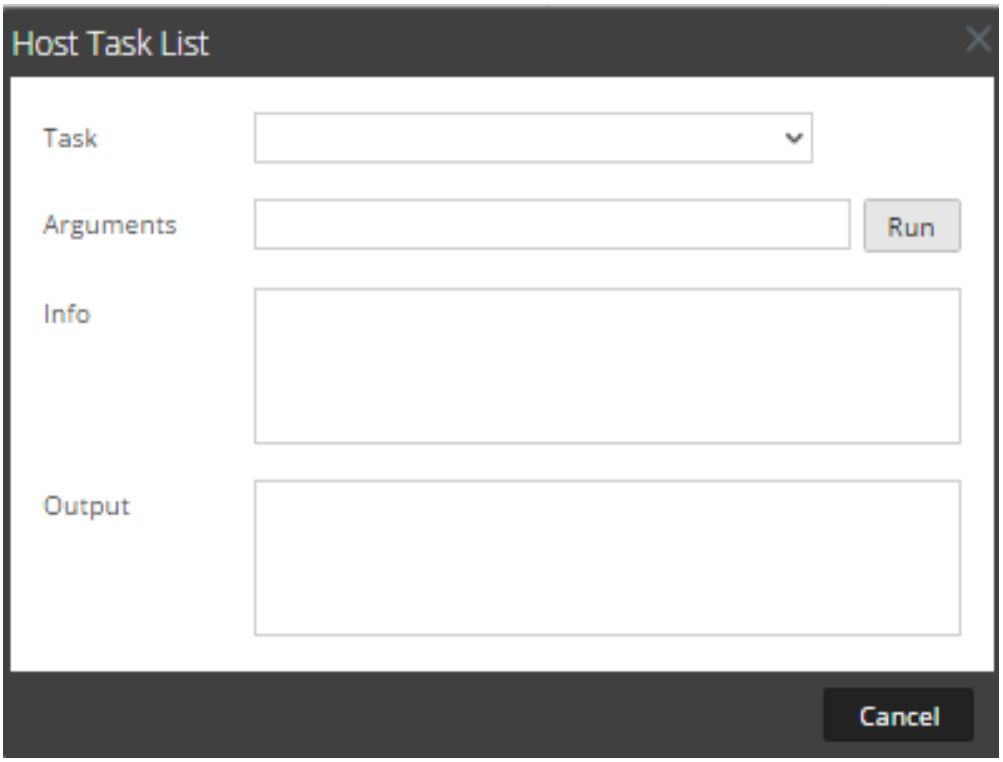
Boîte de dialogue Liste des tâches de l'hôte

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

Dans la vue Système de services RSA NetWitness Suite, 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 **NetWitness Suite**, sélectionnez **ADMIN >Services**.
2. Choisissez un service, puis 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 des tâches de l'hôte s'affiche. La liste **Tâche** propose une liste des messages pris en charge pour l'hôte associé.



Fonctionnalités

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.
Info	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 le moniteur du système de fichiers	Commence à surveiller les services de stockage ajoutés au système de fichiers spécifié (voir Ajouter et Supprimer le moniteur du système de fichiers).
Supprimer le moniteur du système de fichiers	Arrête de surveiller les services de stockage ajoutés au système de fichiers spécifié.
Redémarrer l'hôte	Arrête et redémarre l'hôte (voir Redémarrer un hôte).

Tâche	Description
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 NetWitness Suite 10.6 ; remplacée par la procédure décrite dans la section Hôte GS : Procédures des hôtes et des services.
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).
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 Démarrer, arrêter ou redémarrer un service).
Arrêter le service	Arrête un service sur cet hôte.
setSNMP	Active ou désactive le service SNMP sur un hôte (voir Configurer SNMP).

Paramètres de configuration des services

Cette rubrique présente les paramètres de configuration disponibles pour les services RSA NetWitness Suite Core.

Les services NetWitness Suite 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 NetWitness Suite et d'autres sont affichables ou configurables uniquement dans la vue Explorer les services.

Paramètres de configuration du service Appliance

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour le service NetWitness Suite Core Appliance.

Le service NetWitness Suite Core Appliance surveille le matériel NetWitness existant.

Ce tableau décrit les paramètres de configuration Appliance.

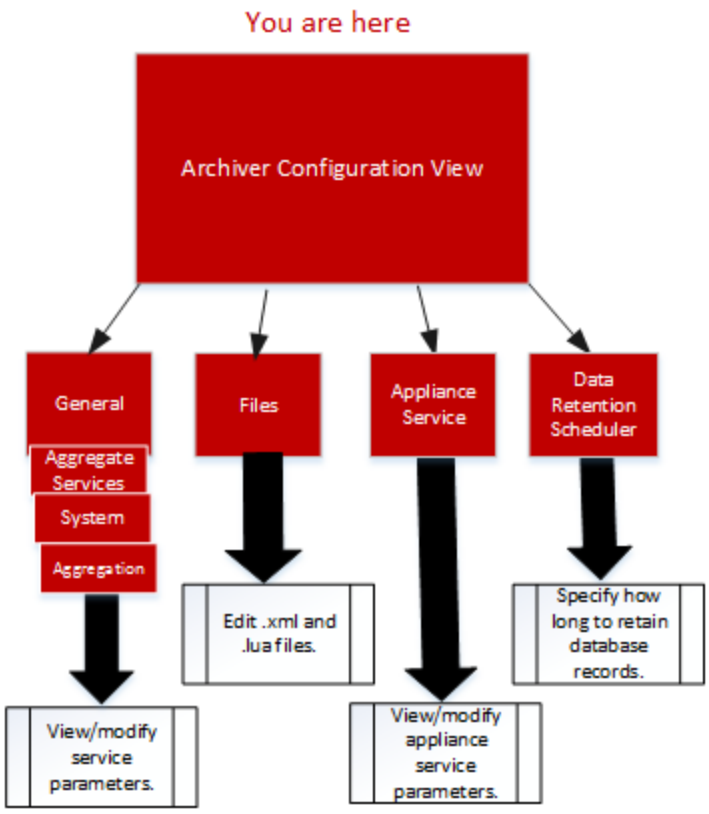
Champ de paramètre Appliance	Description
Logs	/logs/config, reportez-vous à la rubrique Paramètres de configuration de la consignation du service Core
REST	/rest/config, reportez-vous à la rubrique Paramètres de configuration de l'interface REST
Services	/services/<nom du service>/config, reportez-vous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

Vue Configuration des services Archiver

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour les services Archiver NetWitness Suite.

Workflow

Le workflow suivant affiche les tâches de configuration pour le service Archiver.



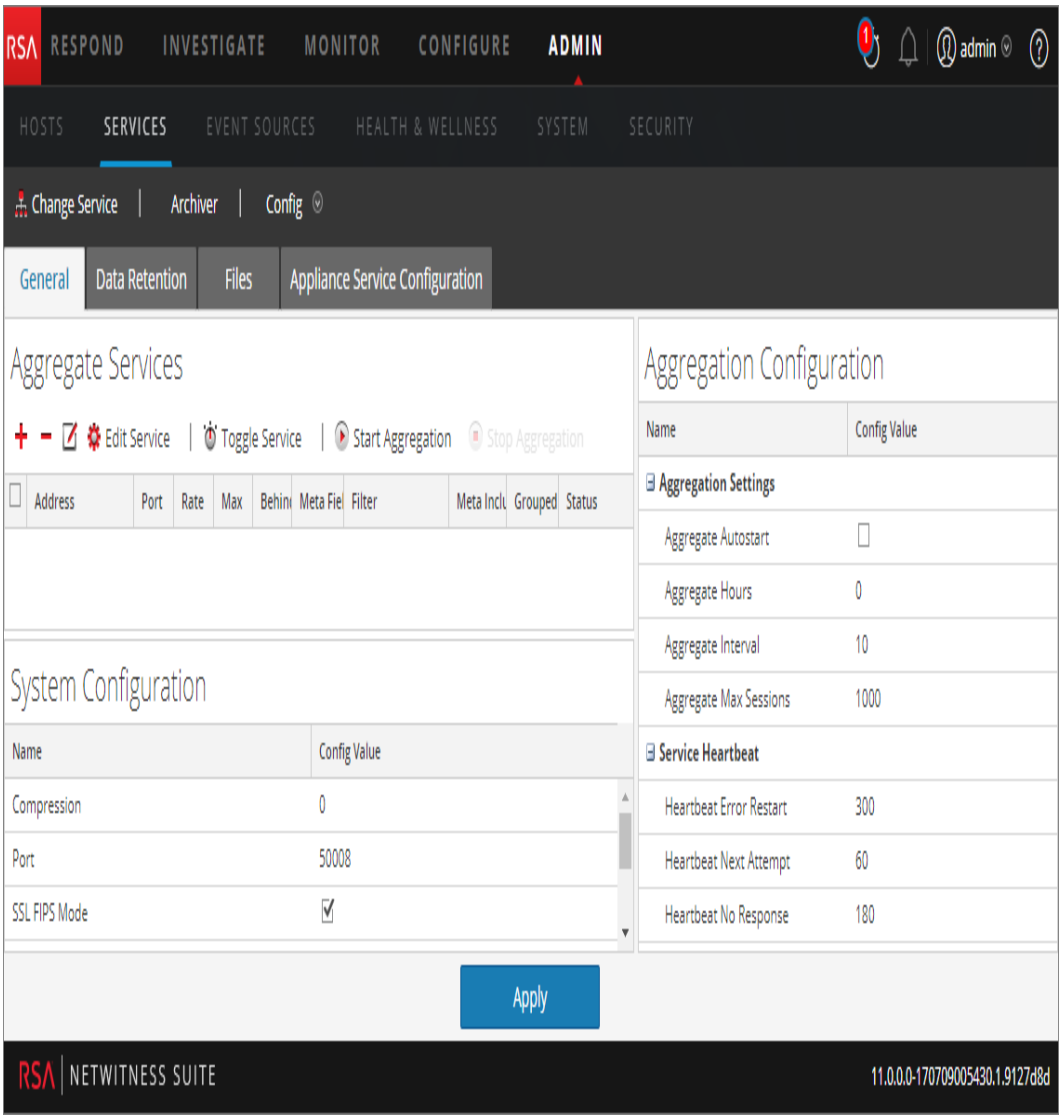
Rôle	Je souhaite...
Administrateur	Configurer des filtres méta pour l'agrégation. Reportez-vous à « (Facultatif) Configurer des filtres méta pour l'agrégation » dans le *Guide de configuration de RSA NetWitness Suite Archiver* pour obtenir des instructions.
Administrateur	Configurer l'agrégation de groupes. Reportez-vous à « Configurer l'agrégation de groupes » dans le *Guide de déploiement RSANetWitness Suite* pour obtenir des instructions.

Aperçu rapide

Pour accéder à la vue Configuration des services :

1. Dans **NetWitness Suite**, sélectionnez **ADMIN > Services**.
   La vue Services ADMIN s'affiche.
2. Choisissez un service Archiver et sélectionnez  **>Vue > Config**.
   La vue Configuration des services correspondant au service Archiver s'affiche.

Exemple de la vue Configuration des services pour un service Archiver.



Paramètres de configuration du service Broker

Cette rubrique répertorie et décrit les paramètres de configuration de NetWitness Suite Brokers.

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

Champ de paramètre du Broker	Description
Broker	/broker/config, reportez-vous à la rubrique Paramètres de configuration de l'agrégation

Champ de paramètre du Broker	Description
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** dans le *Guide d'optimisation de la base de données des services NetWitness Suite Core*
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. La modification requiert le redémarrage du service.
Logs	/logs/config, reportez-vous à la rubrique Paramètres de configuration de la consignation du service Core
REST	/rest/config, reportez-vous à la rubrique Paramètres de configuration de l'interface REST
SDK	/sdk/config, reportez-vous à la rubrique **Nœuds de configuration SDK** dans le *Guide d'optimisation de la base de données des services NetWitness Suite Core* et Hôte GS : Modes system.roles du service NetWitness Platform Core
Services	/services/<nom du service>/config, reportez-vous à la section Paramètres de configuration de service à service Core
Système	/sys/config, reportez-vous à la rubrique Paramètres de configuration système du service Core

Paramètres de configuration de l'agrégation

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

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.

Chemin de configuration	/concentrator/config ou /archiver/config
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.
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.

Chemin de configuration	/concentrator/config ou /archiver/config
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.

Chemin de configuration	/concentrator/config ou /archiver/config
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 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.

Paramètres de configuration du service Concentrator

Cette rubrique répertorie et décrit les paramètres de configuration disponibles de NetWitness Suite Concentrators.

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

Champ de paramètre du Concentrator	Description
Concentrator	/concentrator/config, reportez-vous à la rubrique Paramètres de configuration de l'agrégation
Base de données	/database/config fait référence à la section **Nœuds de configuration de la base de données** dans le *Guide d'optimisation de la base de données NetWitness Suite Core*
Index	/index/config, reportez-vous à la section **Nœuds de configuration d'index** dans le *Guide d'optimisation de la base de données NetWitness Suite Core*
Logs	/logs/config, reportez-vous à la rubrique Paramètres de configuration de la consignation du service Core
REST	/rest/config, reportez-vous à la rubrique Paramètres de configuration de l'interface REST
SDK	/sdk/config, reportez-vous à la section **Nœuds de configuration SDK** dans le *Guide d'optimisation de la base de données NetWitness Suite Core* et Hôte GS : Modes system.roles du service NetWitness Platform Core
Services	/services/<nom du service>/config, reportez-vous à la rubrique Paramètres de configuration de service à service Core
Système	/sys/config, reportez-vous à la rubrique Paramètres de configuration système du service Core

Paramètres de configuration de la consignation du service Core

Cette rubrique répertorie et décrit les paramètres de configuration de la consignation pour tous les services NetWitness Suite Core.

La configuration de la consignation est identique sur tous les services NetWitness Suite Core.

Le tableau suivant décrit les paramètres de configuration des logs :

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 SA Core exécutés sur le même hôte. Par exemple, si l'ID de moteur généré pour l'hôte SA Core est 0x1234512345, vous pouvez le définir sur 0x123451234501 pour le service Decoder et sur 0x123451234504 pour le service Appliance.

Dossier de configuration des logs	/logs/config
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).
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.

Paramètres de 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, au format `host:port`. Par exemple, le dossier de connexion au service pour la connexion d'un Concentrator vers un Decoder pourrait être `/services/reston-va-decoder:50004`. À l'intérieur de chaque dossier de connexion au service, il existe un sous-dossier `config` qui contient les paramètres configurables.

Le tableau ci-dessous 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.

Paramètres de configuration système du service Core

Cette rubrique répertorie et décrit les paramètres de configuration communs à tous les services NetWitness Suite Core.

Le tableau suivant décrit les paramètres de Configuration 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.

Dossier de configuration du système	/sys/config
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 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.

Paramètres de configuration du service Decoder

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour NetWitness Suite Decoders.

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

Champ de paramètre du Decoder	Description
Decoder	/decoder/config, reportez-vous à la rubrique Paramètres de configuration de Decoder et Log Decoder
Base de données	/database/config fait référence à la section **Nœuds de configuration de la base de données** dans le *Guide d'optimisation de la base de données NetWitness Suite Core*
Index	/index/config, reportez-vous à la section **Nœuds de configuration d'index** dans le *Guide d'optimisation de la base de données NetWitness Suite Core*
Logs	/logs/config, reportez-vous à la rubrique Paramètres de configuration de la consignation du service Core
REST	/rest/config, reportez-vous à la rubrique Paramètres de configuration de l'interface REST
SDK	/sdk/config, reportez-vous à la section **Nœuds de configuration SDK** dans le *Guide d'optimisation de la base de données NetWitness Suite Core* et Hôte GS : Modes system.roles du service NetWitness Platform Core
Système	/sys/config, reportez-vous à la rubrique Paramètres de configuration système du service Core

Paramètres de configuration de 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.

Chemin de configuration de Decoder	/decoder/config
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.
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.

Chemin de configuration de Decoder	/decoder/config
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.

Chemin de configuration de Decoder	/decoder/config
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.

Chemin de configuration de Decoder	/decoder/config
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.

Hôte GS : Paramètres de configuration du service Log Decoder

Cette rubrique répertorie et décrit les paramètres de configuration disponibles pour RSA NetWitness Suite Log Decoders.

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 fait référence à la section **Nœuds de configuration de la base de données** dans le *Guide d'optimisation de la base de données NetWitness Suite Core*.
Decoder	/decoder/config, reportez-vous à la rubrique Paramètres de configuration de Decoder et Log Decoder
Index	/index/config fait référence à la section **Nœuds de configuration d'index** dans le *Guide d'optimisation de la base de données NetWitness Suite Core*.
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 à la section **Nœuds de configuration SDK** dans le *Guide d'optimisation de la base de données NetWitness Suite Core* et Modes system.roles du service Core.
Système	/sys/config, reportez-vous à la rubrique Configuration système de service Core.

Paramètres de configuration du Log Tokenizer

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 Log Tokenizer est mis en œuvre en tant qu'ensemble d'analyseurs intégrés par chaque analyse pour un sous-ensemble de tokens reconnaissables. La fonctionnalité de chacun de ces analyseurs natifs est indiquée dans le tableau ci-dessous. Ces éléments word forment un index de texte intégral lorsqu'ils sont introduits dans le moteur d'indexation sur les services Concentrator et Archiver. En modifiant l'entrée de configuration parsers.disabled, vous pouvez contrôler l'activation des générateurs de logs.

Nom de l'analyseur	Description	Paramètres de configuration
Tokens de logs	Recherche des séquences de caractères consécutifs pour produire des éléments méta 'word'.	token.device.types, token.char.classes, token.max.length, token.min.length, token.unicode
IPSCAN	Recherche de texte sous forme d'adresse IPv4 pour produire des éléments méta 'ip.addr'.	token.device.types
IPV6SCAN	Recherche de texte sous forme d'adresse IPv6 pour produire des éléments méta 'ipv6'.	token.device.types
URLSCAN	Recherche de texte sous forme d'URI pour produire des éléments méta 'alias.host', 'filename', 'username' et 'password'.	token.device.types
DOMAINSCAN	Recherche de texte sous forme de nom de domaine pour produire les éléments méta 'alias.host', 'tld', 'cctld' et 'sld'.	token.device.types

Nom de l'analyseur	Description	Paramètres de configuration
EMAILSCAN	Recherche de texte sous forme d'adresse e-mail pour produire les éléments méta 'email' et 'username'.	token.device.types
SYSLOGTIMESTAMPSCAN	Recherche de texte sous forme d'horodatages au format syslog. Il manque l'année et le fuseau horaire dans syslog. Lorsque ce texte est identifié, il est normalisé en heure UTC pour créer les éléments méta 'event.time'.	token.device.types
INTERNETTIMESTAMPSCAN	Recherche de texte sous forme d'horodatages au format RFC 3339 pour créer des éléments méta 'event.time'.	token.device.types

Voici les paramètres de configuration du Log Tokenizer.

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 de n'importe quelle combinaison des 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

Champ Configuration des analyseurs Log Decoder	Description
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.

Paramètres de configuration de l'interface REST

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

Paramètres

Le tableau suivant répertorie et décrit les paramètres de Configuration REST :

Chemin de configuration de REST	/rest/config
cache.dir	Affiche le répertoire hôte à utiliser pour créer et stocker provisoirement les fichiers. Les modifications prendront 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. Les modifications prendront effet au redémarrage du service.
enabled	Bascule sur activer ou désactiver les services REST. 1 correspond à activé et 0 à désactivé. Les modifications prendront effet au redémarrage du service.
port	Affiche le port sur lequel le service REST écoute. Les modifications prendront 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. Les modifications prendront effet au redémarrage du service.

Hôte GS : Modes system.roles du service NetWitness Platform Core

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

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 NetWitness Platform (voir Onglet **Confidentialité des données** dans le *Guide de gestion de la confidentialité des données* pour plus de détails). Lorsque la valeur est modifiée, la modification est appliquée immédiatement.

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

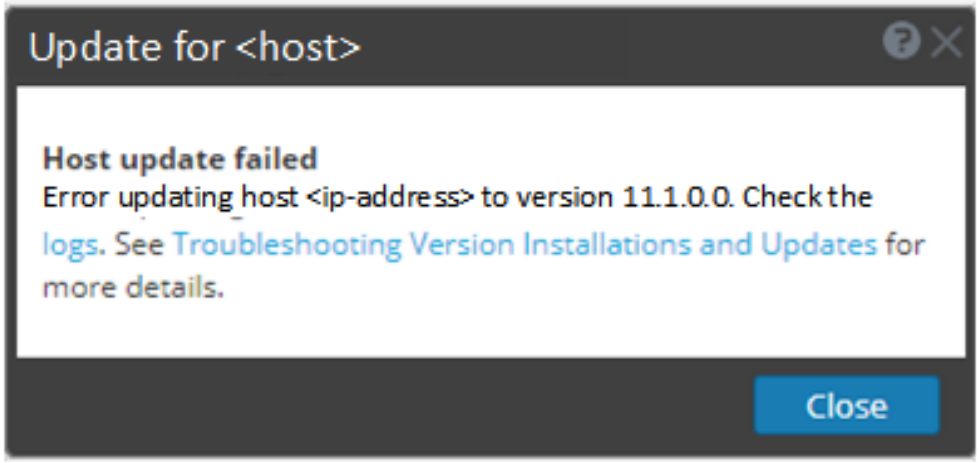
- 0 = désactivé.

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

Hôte GS : Dépannage des installations et mises à jour de version

Cette section décrit les messages d'erreur qui s'affichent dans la vue **Hôtes** en cas de problèmes de mise à jour des versions de l'hôte et d'installation de services sur les hôtes dans la vue **Hôtes**. Si les solutions de dépannage suivantes ne vous permettent pas de résoudre un problème de mise à jour ou d'installation, contactez le Support client (https://community.RSA.com/docs/DOC-1294).

Message d'erreur	
Problème	Lorsque vous sélectionnez une version de mise à jour, puis cliquez sur **Mettre à jour** > **Mettre à jour l'hôte**, le processus de téléchargement réussit, mais le processus de mise à jour échoue.

Solution	1. **Essayez de nouveau d'appliquer la mise à jour de version à l'hôte**. Souvent, cela est suffisant.
	2. Si vous ne pouvez pas appliquer la nouvelle mise à jour de version :
	a. Surveillez les journaux suivants sur le serveur NW lors de sa progression (par exemple, utilisez la chaîne de commande `tail -f` à partir de la ligne de commande) :
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`

L'erreur s'affiche dans un ou plusieurs de ces logs.

b. Essayez de résoudre le problème et de réappliquer la mise à jour de version.

- Cause 1 - Le mot de passe `deploy_admin` a expiré.
  Solution - Réinitialisez votre mot de passe `deploy_admin`.
  Pour résoudre la Cause 1, procédez comme suit.

  1. Dans le menu NetWitness Suite, sélectionnez **ADMIN** > **Sécurité** > onglet **Utilisateurs**.
  2. Sélectionnez `deploy_admin` et cliquez sur **Réinitialiser le mot de passe**.
  3. (Conditionnel) Si NetWitness Suite ne vous permet pas d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe**, procédez comme suit.

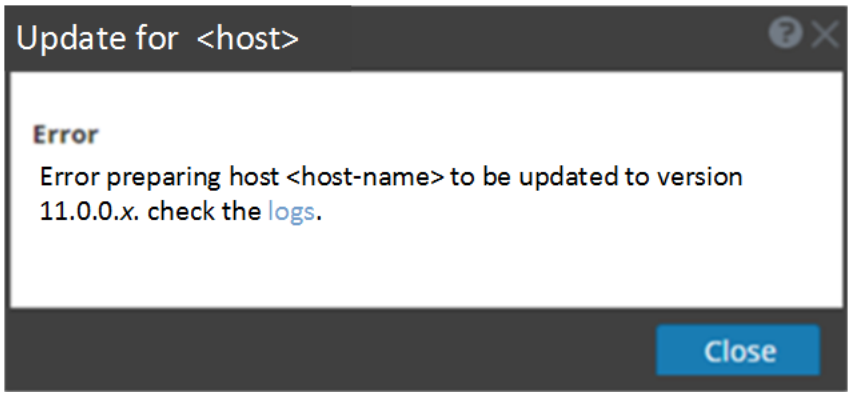
     a. Réinitialisez `deploy_admin` pour utiliser un nouveau mot de passe.

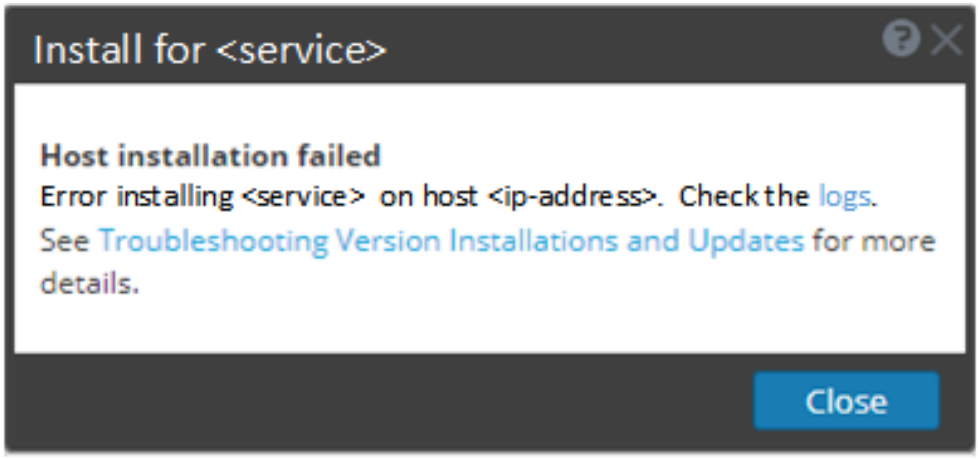
     b. Sur tous les hôtes serveur autres que NW sur la version 11.x, exécutez la commande suivante à l'aide du mot de passe `deploy_admin` de correspondance à partir de l'hôte du serveur NW.
     `/opt/rsa/saTools/bin/set-deploy-admin-password`

- Cause 2 - Le mot de passe `deploy_admin` a été modifié sur l'hôte du serveur NW, mais pas sur les hôtes de serveurs autres que NW.
  Pour résoudre la Cause 2, procédez comme suit.

  - Sur tous les hôtes de serveurs autres que NW (version 11.x), exécutez la commande suivante à l'aide du mot de passe `deploy_admin` correspondant à partir de l'hôte du serveur NW.
    `/opt/rsa/saTools/bin/set-deploy-admin-password`

3. Si vous ne pouvez toujours pas appliquer la mise à jour, collectez les logs comme indiqué à l'étape 2 et contactez le support client (https://community.rsa.com/docs/DOC-1294).

Message d'erreur	 `var/log/netwitness/orchestration-server/orchestration-server.log` présente une erreur similaire au message d'erreur suivant : `API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.0.0.x' is not supported`
Problème	Après la mise à jour de l'hôte du serveur NW vers la version 11.1, la seule stratégie de mise à jour pour les hôtes de serveurs autres que NW est la version 11.1. Si vous tentez de mettre à jour un hôte de serveur autre que NW vers un correctif 11.0.0.n (par exemple de 11.0.0.0 à 11.0.0.3), vous obtiendrez ce message d'erreur dans le log /var/log/netwitness/orchestration-server/orchestration-server.log.
Solution	Effectuez une mise à jour de l'hôte du serveur autre que NW vers la version 11.1.

Message d'erreur	
Problème	Lorsque vous sélectionnez un hôte, puis cliquez sur **Installer**, le processus du

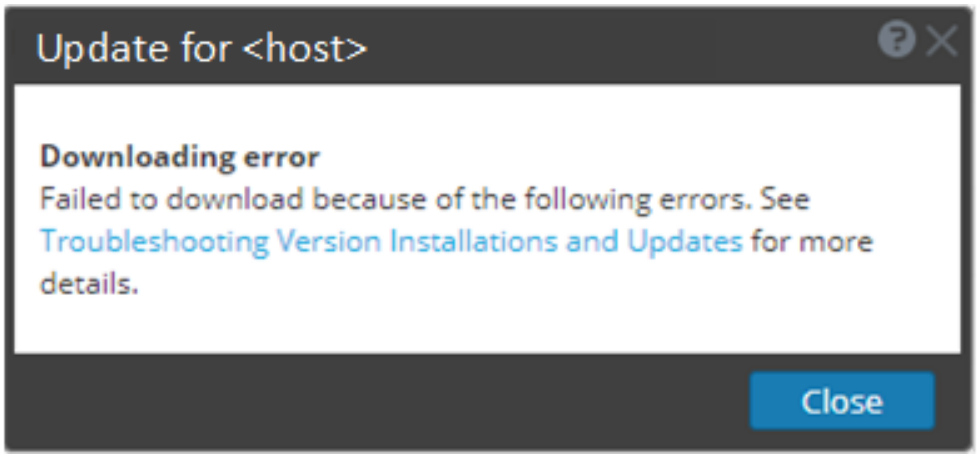
	service d'installation échoue.

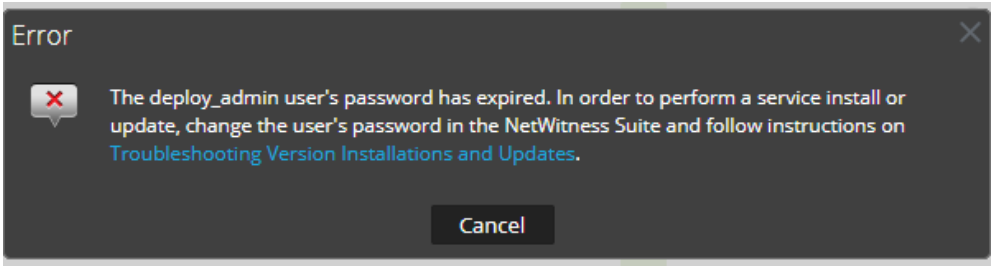
Solution	1. **Essayez de réinstaller le service**.
	Souvent, cela est suffisant.
	2. Si vous ne pouvez toujours pas installer le service :
	a. Surveillez les logs suivants sur le serveur NW lors de sa progression (par exemple, exécutez la chaîne de commande `tail -f` à partir de la ligne de commande) :
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	L'erreur s'affiche dans un ou plusieurs de ces logs.
	b. Tentez de résoudre le problème et réinstallez le service.
	• Cause 1 - Saisie du mot de passe `deploy_admin` erroné dans nwsetup-tui.
	Solution - Récupérez votre mot de passe `deploy_admin` .
	Pour résoudre la Cause 1, procédez comme suit.
	1. Dans le menu NetWitness Suite, sélectionnez **ADMIN** > **Sécurité** > onglet **Utilisateurs**.
	2. Sélectionnez `deploy_admin`, puis cliquez sur **Réinitialiser le mot de passe**.
	3. (Conditionnel) Si NetWitness Suite ne vous permet pas d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe**, procédez comme suit.
	a. Ouvrez une session SSH sur l'hôte du serveur NW.
	`security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name platform.deployment.password -quiet`
	b. Ouvrez une session SSH sur l'hôte pour lequel l'installation/orchestration a échoué.
	c. Exécutez la commande nwsetup-tui à l'aide du mot de passe

deploy_admin approprié.

- Cause 2 - Le mot de passe deploy_admin a expiré.
  Pour résoudre la Cause 2, procédez comme suit.
  1. Dans le menu NetWitness Suite, sélectionnez **ADMIN** > **Sécurité** > onglet **Utilisateurs**.
  2. Sélectionnez deploy_admin, puis cliquez sur **Réinitialiser le mot de passe**.
  3. (Conditionnel) Si NetWitness Suite vous permet d'entrer le mot de passe deploy_admin ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe**, procédez comme suit.
     a. Saisissez le mot de passe deploy_admin ayant expiré.
     b. Désactivez la case à cocher Forcer le changement du mot de passe à la prochaine connexion.
     c. Cliquez sur **Enregistrer**.
  4. (Conditionnel) Si NetWitness Suite ne vous permet pas d'entrer le mot de passe deploy_admin ayant expiré dans la boîte de dialogue Réinitialiser le mot de passe, procédez comme suit.
     a. Réinitialisez deploy_admin pour utiliser un nouveau mot de passe.
     b. Sur tous les hôtes du serveur NW et tous les autres hôtes 11.x, exécutez la commande suivante à l'aide du nouveau mot de passe deploy_admin.
     /opt/rsa/saTools/bin/set-deploy-admin-password
     c. Sur l'hôte où l'installation/orchestration a échoué, exécutez la commande nwsetup-tui et utilisez le nouveau mot de passe deploy_admin.

3. Si vous ne pouvez toujours pas appliquer la mise à jour, collectez les logs comme indiqué à l'étape 2 et contactez le support client (https://community.rsa.com/docs/DOC-1294).

Message d'erreur	
Problème	Lorsque vous sélectionnez une version de mise à jour, puis cliquez sur **Mettre à jour** >**Mettre à jour l'hôte**, le téléchargement démarre, mais ne parvient pas à terminer.
Cause	Les fichiers de téléchargement de version peuvent être volumineux et prendre beaucoup de temps à télécharger. S'il existe des problèmes de communication pendant le téléchargement, celui-ci échoue.
Solution	1. Tentez un nouveau téléchargement. 2. Si le téléchargement échoue, relancez le téléchargement en dehors de NetWitness Suite, comme décrit dans Appliquer les mises à jour à partir de la ligne de commande (sans accès Web). 3. Si vous ne pouvez toujours pas télécharger le fichier de mise à jour, contactez le Support Clients (https://community.rsa.com/docs/DOC-1294).

Message d'erreur	
Cause	Le mot de passe de l'utilisateur `deploy_admin` a expiré.
Solution	Réinitialisez votre mot de passe `deploy_admin`. 1. Dans le menu NetWitness Suite, sélectionnez **ADMIN** > **Sécurité** > onglet **Utilisateurs**. 2. Sélectionnez **deploy_admin**, puis cliquez sur **Réinitialiser le mot de passe**. • Si NetWitness Suite vous permet d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe**, procédez comme suit. a. Saisissez le mot de passe `deploy_admin` ayant expiré. b. Désactivez la case à cocher **Forcer le changement du mot de passe à la prochaine connexion**. c. Cliquez sur **Enregistrer**. • Si NetWitness Suite ne vous permet pas d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe** : a. Sur les hôtes du serveur NW et tous les autres hôtes 11.x, exécutez la commande suivante à l'aide du nouveau mot de passe `deploy_admin`. `/opt/rsa/saTools/bin/set-deploy-admin-password` b. Sur l'hôte où l'installation/orchestration a échoué, exécutez la commande nwsetup-tui et utilisez le nouveau mot de passe `deploy_admin`.