RSA NETWITNESS® SUITE

Guide de configuration de Log Collection

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

À propos de la collecte de logs

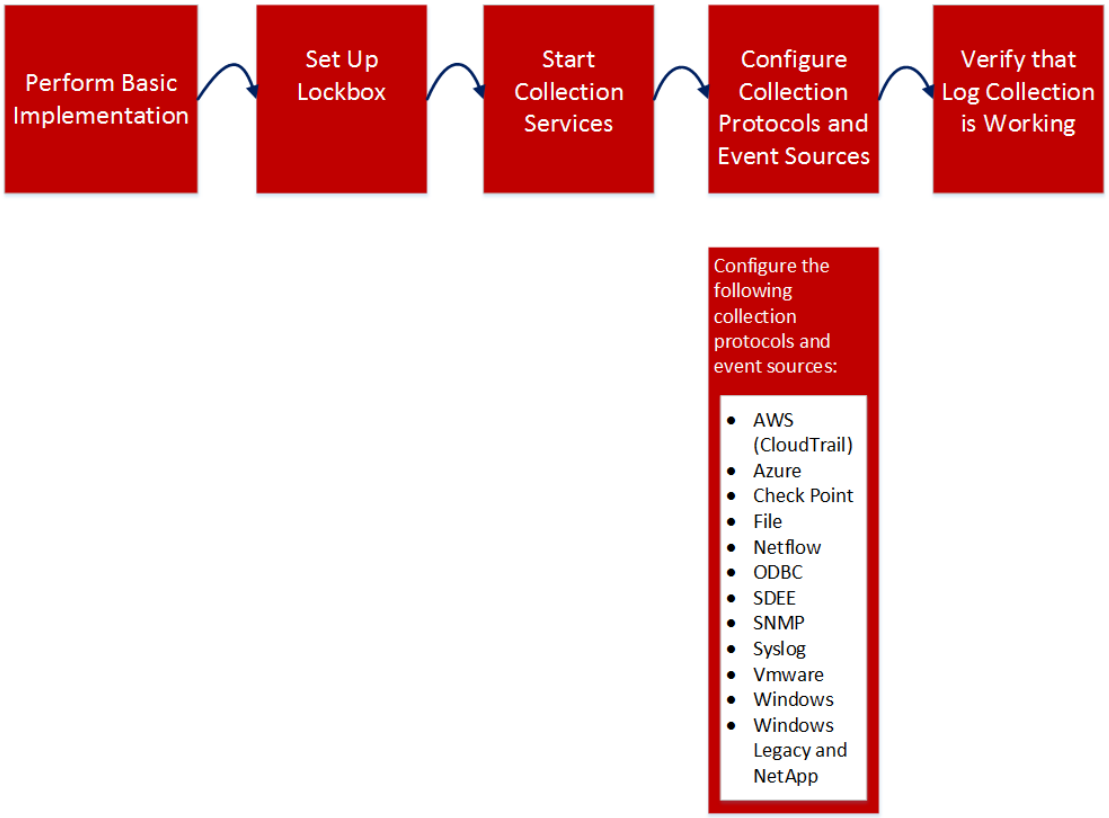
Ce guide décrit les étapes générales et les sous-tâches pour définir et configurer la collecte de logs des sources d'événements qui incluent :

- Ce que Log Collection fait, comment il fonctionne à un haut niveau, et comment il fournit des diagrammes de déploiement de haut niveau.
- Comment démarrer la collecte des événements.
- Où trouver les instructions pour configurer des déploiements plus complexes.
- Comment démarrer un protocole de collecte.
- Quelle est la structure de l'interface utilisateur de configuration de Log Collection.
- Quels sont les outils à utiliser pour résoudre les problèmes de Log Collection, ainsi que les instructions de dépannage générales.
- Comment affiner et personnaliser Log Collection dans votre environnement.
- Comment configurer des protocoles de collecte individuels. Vous trouverez des instructions dans les différentes rubriques de la collecte de logs.

Workflow

Ce workflow présente les tâches de base qui vous permettent de commencer la collecte

d'événements via la collecte de logs.



Procédure générale

Il s'agit de manière générale, voici les procédures à suivre pour la collecte de logs :

I. Ajouter des local et remote collectors à RSA NetWitness Suite.

   Configurer un Log Collector localement sur un Log Decoder (à savoir, un collecteur local). Vous pouvez également définir des Log Collector dans autant de sites distants (à savoir Remote Collectors) que vous en avez besoin pour votre entreprise. Pour plus d'informations, reportez-vous à la rubrique Implémentation de base.

II. Télécharger la dernière version de contenu à partir de Live. Il s'agit d'une tâche que vous effectuez régulièrement, puisque le contenu fourni sur Live est mis à jour régulièrement.

   LIVE est un système de gestion de contenu de RSA NetWitness® Suite à partir duquel vous pouvez télécharger le contenu le plus récent. Les deux types de ressources à utiliser pour le téléchargement du contenu Log Collection sont :

   - **RSA Log Collector** - contenu activant la collecte des types de sources d'événements.
   - **RSA Log Device** - derniers analyseurs de sources d'événements pris en charge.

Vous pouvez également vous abonner au contenu sur Live. Pour plus d'informations, consultez le *Guide de gestion des services Live*.

III. Configurer les paramètres : configurer le lockbox et les certificats.

Pour plus d'informations, reportez-vous à la rubrique Configurer un Lockbox et Configurer des certificats.

IV. Configurer des sources d'événements.

Vous configurez toutes les sources d'événements sur votre réseau pour envoyer leurs informations de log vers RSA NetWitness Suite. Chaque fois que vous ajoutez de nouvelles sources d'événements, vous devez également effectuer cette procédure. Tous les guides de configuration de sources d'événements sont trouvent dans l'espace Sources d'événements prises en charge RSA dans RSA Link.

V. Démarrer et arrêter les services des protocoles configurés. Parfois, il peut que vous deviez arrêter et redémarrer les services en fonction des nouvelles sources d'événements que vous ajoutez à RSA NetWitness Suite.

VI. Vérifier le fonctionnement de Log Collection.

Lorsque vous configurez une nouvelle source d'événement ou ajoutez un nouveau protocole de collecte, vous devez vérifier que les bons logs sont envoyés à RSA NetWitness Suite.

Architecture de collecte de logs

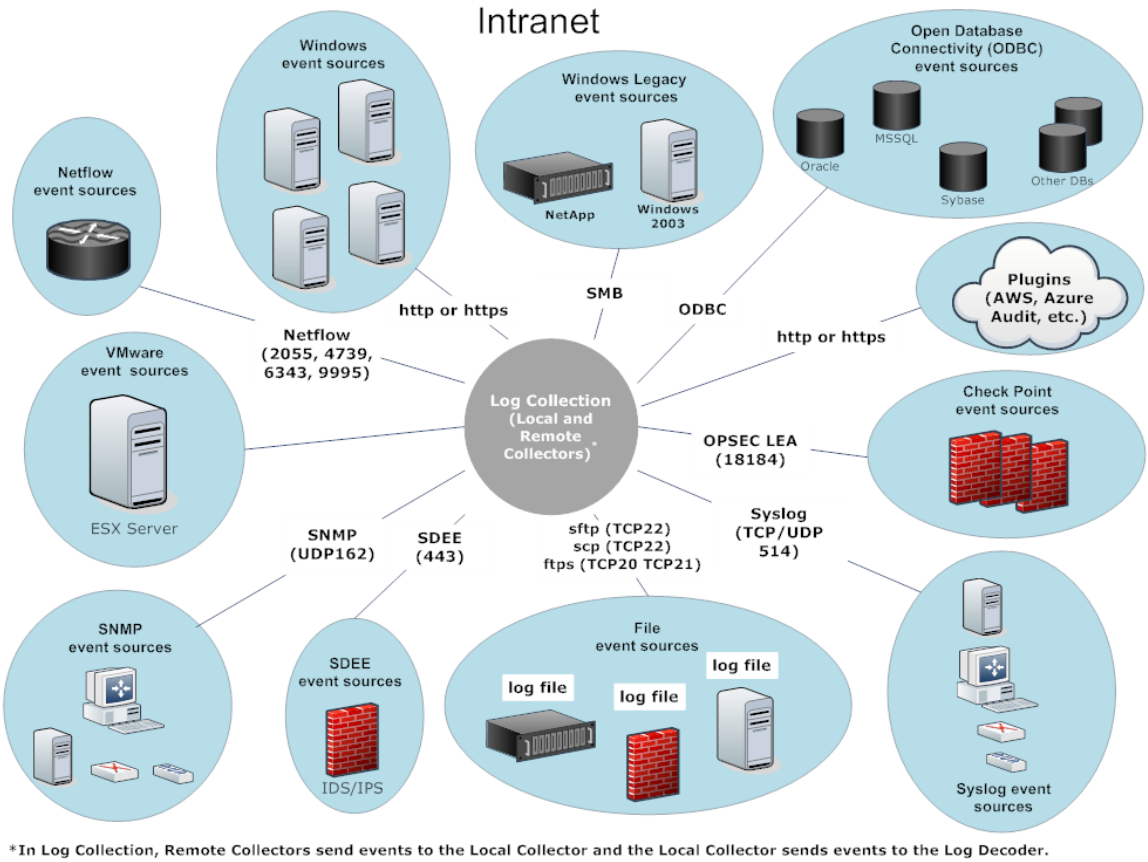
Cette rubrique décrit comment NetWitness Suite effectue la collecte des logs.

Comment déployer Log Collection

Vous pouvez déployer Log Collection selon les besoins et préférences de votre entreprise. Vous pouvez ainsi déployer Log Collection sur plusieurs sites et collecter des données de différents jeux de sources d'événements. Pour cela, vous devez configurer un collecteur local avec un ou plusieurs collecteurs distants.

Composants de Log Collection

La figure suivante illustre l'ensemble des composants impliqués dans la collecte d'événements via NetWitness Suite Log Collector.



Collecteurs locaux et distants

La figure suivante explique comment les collecteurs locaux et distants interagissent pour collecter des événements auprès de tous vos sites.

Dans ce scénario, la collecte des journaux à partir de différents protocoles comme Windows, ODBC, etc. est effectuée via les services du collecteur distant et Log Collector. Si la collecte des journaux est effectuée par le collecteur local, elle est transmise au service Log Decoder, comme dans le cas d'un déploiement local. Si elle est effectuée par un collecteur distant, elle peut être transmise de deux façons au collecteur local :

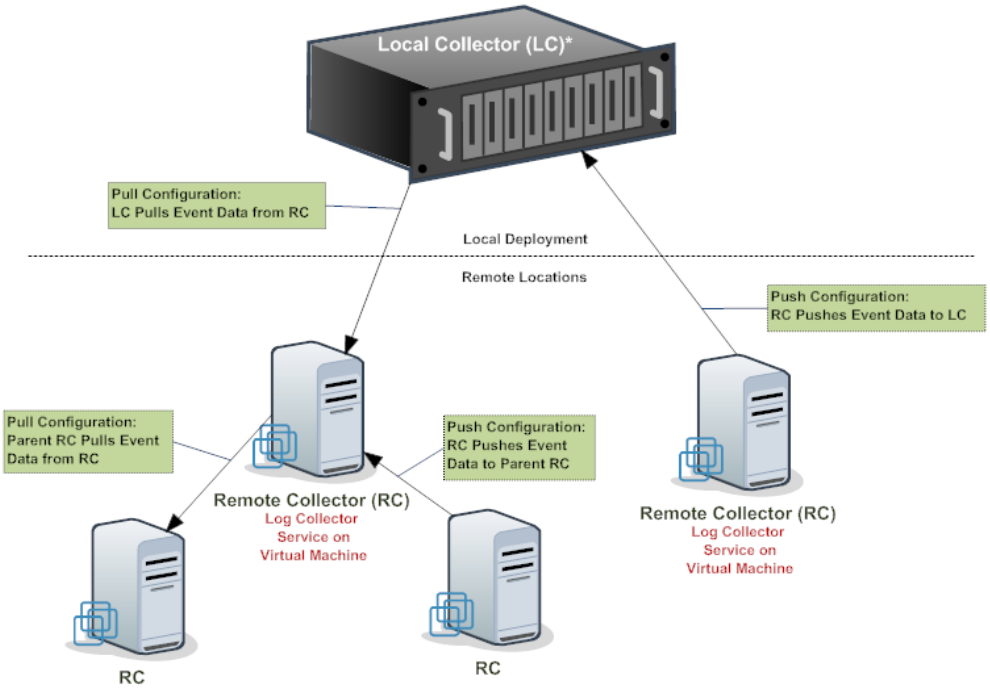
- **Par extraction** : à partir d'un collecteur local, vous sélectionnez les collecteurs distants desquels extraire les événements.
- **Par transmission** : à partir d'un collecteur distant, vous sélectionnez le collecteur local auquel transmettre les événements.

Remarque : l'exemple d'utilisation classique est par transmission. L'extraction est disponible si vous disposez d'une zone démilitarisée dans votre environnement. Les segments réseau moins sécurisés ne peuvent pas établir de connexions avec des segments de réseau plus sécurisés. Avec l'extraction, le Log Collector (ou Virtual Log Collector) sur le réseau sécurisé établit la connexion au VLC sur le réseau moins sécurisé et les logs sont ensuite transférés sans rompre les règles de connexion.

Vous pouvez configurer un ou plusieurs collecteurs distants pour transmettre les données d'événements à un collecteur local, ou vous pouvez configurer un collecteur local pour extraire les données d'événements d'un ou de plusieurs collecteurs distants.

En outre, vous pouvez configurer une chaîne de Remote Collectors pour laquelle vous pouvez configurer :

- Un ou plusieurs collecteurs distants pour transmettre les données d'événement à un collecteur distant.
- Un collecteur distant pour extraire les données à partir d'un ou plusieurs collecteurs distants.



* The Local Collector (LC) is the Log Collector service on the Log Decoder appliance.

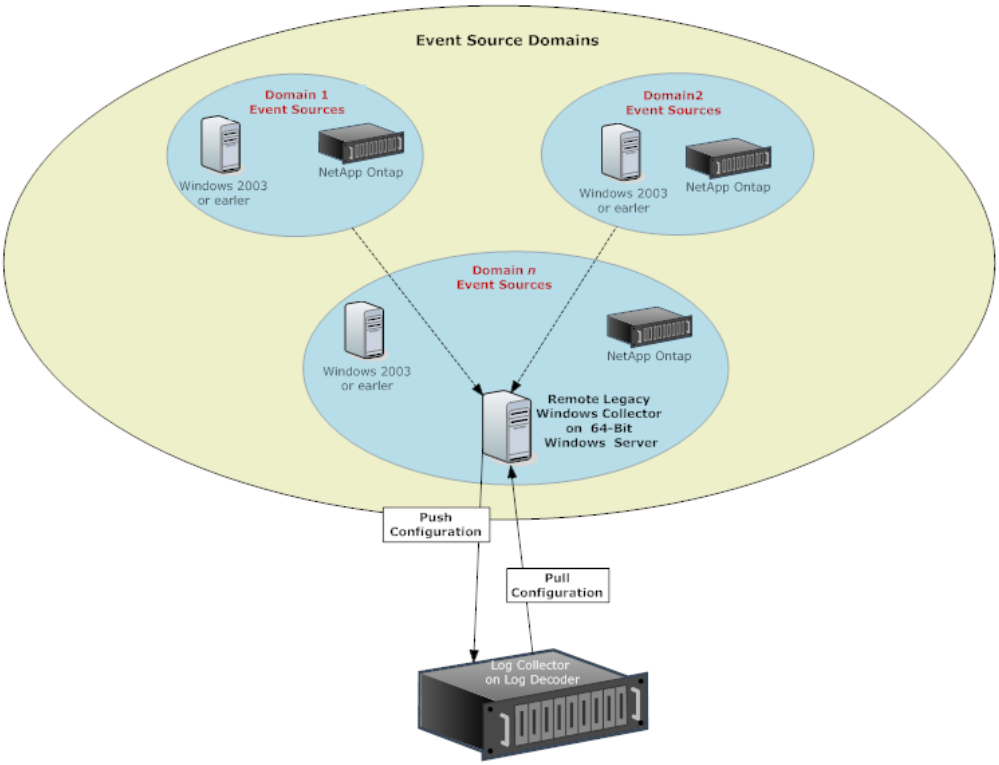
Windows Legacy Remote Collector

Le Collector RSA NetWitness® Suite Windows d'ancienne génération est un Remote Log Collector (RC) basé sur Microsoft Windows qui peut être installé sur un domaine Windows.

Il prend en charge :

- Les sources d'événements Windows 2003 et versions antérieures
- Les fichiers evt d'hôte NetApp ONTAP

La figure suivante illustre le déploiement requis pour collecter des événements auprès des sources d'événements Windows d'ancienne génération.


Event Source Domains
Domain 1
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain2
Event Sources
Windows 2003
or earlier
NetApp Ontap
Domain n
Event Sources
Windows 2003
or earlier
NetApp Ontap
Remote Legacy
Windows Collector
on 64-Bit
Windows Server
Push
Configuration
Pull
Configuration
Log Collector
on Log Decoder

Configuration

Implémentation de base

Cette rubrique indique comment effectuer la configuration initiale des Local Collectors et des Remote Collectors.

Conditions préalables

Vérifier que le Log Decoder est configuré :

- capture des données.
- le contenu actif est chargé dans le {{nld}}.
- est doté d'une licence adéquate.

Rôles de Collectors locaux et distants

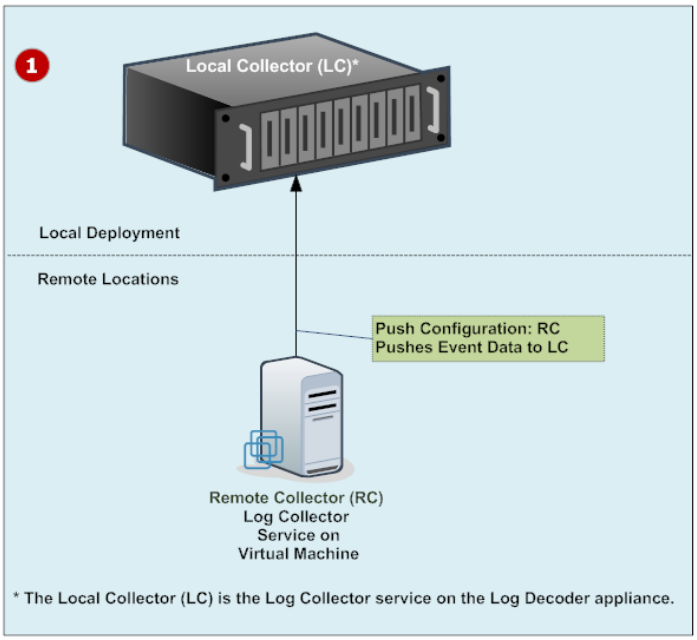
Le collecteur local Local Collector (LC) est un service Log Collector sur un hôte Log Decoder. Dans un scénario de déploiement local, le service Log Collector est déployé sur un hôte Log Decoder, avec le service Log Decoder. La collecte de logs depuis plusieurs protocoles tels que Windows, ODBC etc, est réalisée via le service Log Collector, et des événements sont transférés au service Log Decoder. Le collecteur local envoie toutes les données d'événements collectées au service Log Decoder.

Vous devez avoir au moins un Local Collector pour collecter des événements non Syslog.

Le collecteur distant Remote Collector (RC), également appelé Virtual Log Collector (VLC), est un service Log Collector s'exécutant sur une machine virtuelle autonome. Les collecteurs distants sont optionnels et doivent envoyer les événements qu'ils collectent à un collecteur local. Le déploiement de collecteur distant est idéal lorsque vous devez collecter des logs depuis des sites distants. Les collecteurs distants compressent et chiffrent les logs avant de les envoyer à un collecteur local.

Déploiement et configuration de Log Collection

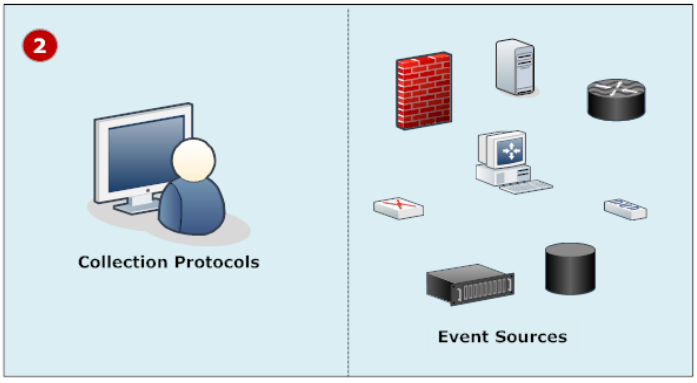
La figure suivante illustre les tâches de base que vous devez réaliser pour déployer et configurer Log Collection. Pour déployer Log Collection, vous devez configurer un Collector local. Vous pouvez également déployer un ou plusieurs collecteurs distants. Une fois que vous déployez la collecte de logs, vous devez configurer les sources d'événements dans NetWitness Suite et sur les sources d'événements elles-mêmes. Le schéma suivant illustre le collecteur local avec un collecteur distant qui pousse les événements vers le collecteur local.



1 Configurez des collecteurs locaux et distants.

Le collecteur local est le service Log Collector s'exécutant sur l'hôte Log Decoder.

Le collecteur distant est le service Log Collector s'exécutant sur une machine virtuelle ou un serveur Windows dans un site distant.



2 Configurez des sources d'événements :

- Configurez les protocoles de collecte dans C:\Temp\Malware Analysis Configuration Guide for Version 11.0.
- Configurez chaque source d'événement pour communiquer avec NetWitness Suite Log Collector.

Ajout d'un collecteur local et d'un collecteur distant àNetWitness Suite

Pour ajouter un collecteur local ou distant à NetWitness Suite :

1. Accédez à **ADMIN > Services**.
2. Cliquez sur + et sélectionnez **Log Collector** dans le menu.

   La boîte de dialogue **Ajouter un service** s'affiche.
3. Définissez les détails du service **Collecte de logs**.
4. Sélectionnez **Tester la connexion** pour vérifier que votre collecteur local ou distant est ajouté.

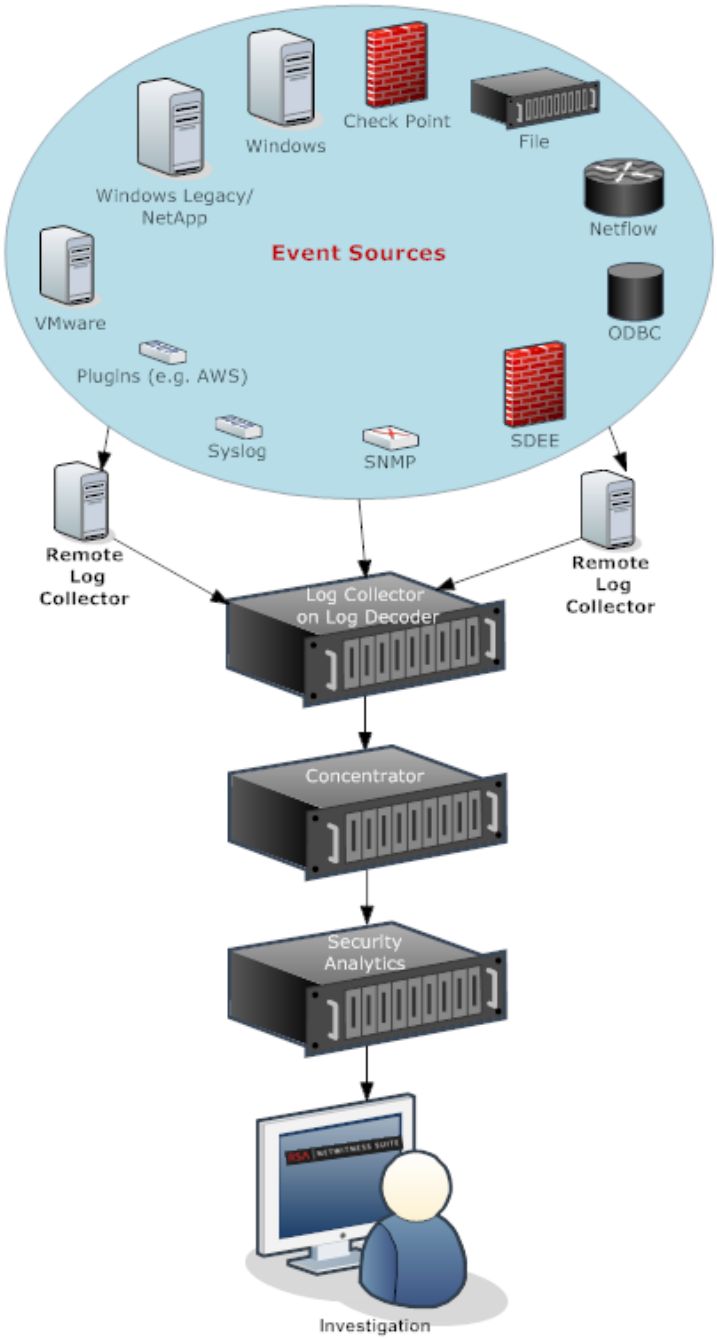
Configuration de Log Collection

Vous choisissez le Log Collector, à savoir un collecteur local (Local Collector) ou le collecteur distant (Remote Collector), pour lequel vous voulez définir des paramètres dans la vue Services. La figure suivante indique comment accéder à la vue Services, sélectionner un service Log Collector, puis afficher l'interface de paramètre de configuration pour ce service.

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Cliquez sur ⚙ sous **Actions**, puis sélectionnez **Vue** > **Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Définissez les paramètres globaux de Log Collection dans l'onglet **Général**.
5. Pour un :
   - collecteur local, NetWitness Suite affiche l'onglet **Collecteurs distants**. Sélectionnez les collecteurs distants à partir desquels le collecteur local extrait les événements dans cet onglet.
   - collecteur distant, NetWitness Suite affiche l'onglet **Collecteurs locaux**. Sélectionnez les collecteurs locaux à partir desquels le collecteur distant extrait les événements dans cet onglet.
6. Remplacez les fichiers de configuration par des fichiers texte dans l'onglet **Fichiers**.
7. Définissez les paramètres du protocole de collecte dans l'onglet **Sources d'événements**.
8. Définissez le lockbox, les clés de chiffrement et les certificats dans l'onglet Paramètres.
9. Définissez les paramètres du service Appliance dans l'onglet **Configuration du service Appliance**.

Schéma du flux de données

Vous utilisez les données de log collectées par le service Log Collector pour surveiller la santé de votre entreprise et mener des investigations. La figure suivante illustre la manière dont les données circulent dans la collecte de logs NetWitness Suite pour l'investigation.



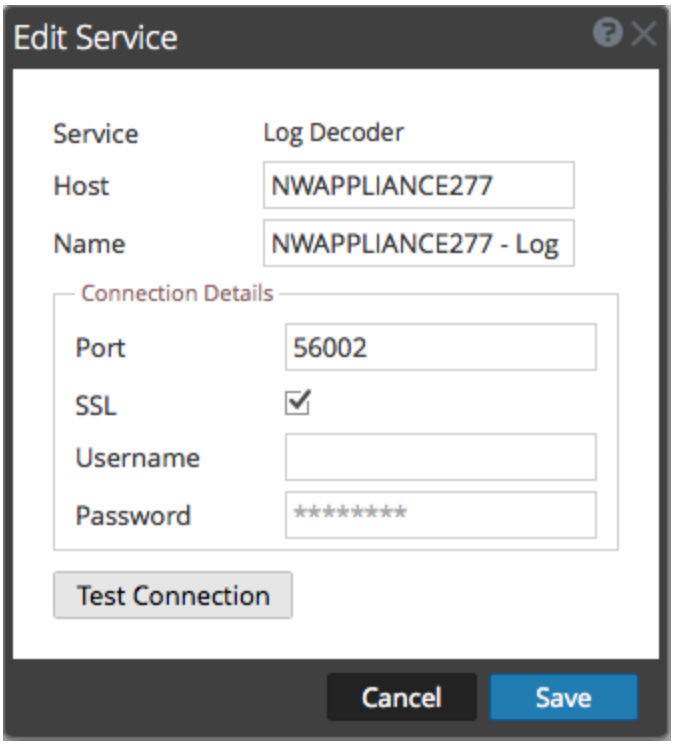
Provisionner des collecteurs locaux et des collecteurs distants

Le serveur NetWitness Suite vérifie si une appliance dispose d'un service Log Decoder. S'il y a un service Log Decoder, elle devient un collecteur local. S'il n'y a pas de service Log Decoder, elle devient un collecteur distant. Un Log Collector local a une destination d'événement et par défaut accède au service Log Decoder local. Un collecteur distant n'a pas de destination d'événement. Le serveur Serveur NW identifie un collecteur Windows d'ancienne génération en tant que collecteur distant.

Pour modifier un collecteur local ou un collecteur distant :

1. Accédez à **ADMIN > Services**.
2. Dans la vue **Services**, sélectionnez dans la barre d'outils.

   La boîte de dialogue **Modifier le service** s'affiche.



3. Dans la boîte de dialogue **Modifier le service**, fournissez les informations suivantes :

Champ	Description
Service	Sélectionnez Log Collector en tant que type de service.
Hôte	Sélectionnez un hôte Log Decoder.
Nom	Saisissez le nom à attribuer au service.

Champ	Description
Port	Le port par défaut est 50001 pour le texte en clair et 56001 pour le texte crypté SSL.
SSL	Sélectionnez **SSL** si vous souhaitez que NetWitness Suite communique avec l'hôte utilisant le protocole SSL. La sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL.
(Facultatif) Nom d'utilisateur	Saisissez le nom d'utilisateur du collecteur local.
(Facultatif) Mot de passe	Saisissez le mot de passe du collecteur local.

4. Cliquez sur **Tester la connexion** pour déterminer si NetWitness Suite se connecte au service.
5. Si le résultat réussit, cliquez sur **Enregistrer**.

   Si le test échoue, modifiez les informations du service et réessayez.

Configurer des collecteurs locaux et des collecteurs distants

Cette rubrique décrit comment configurer des collecteurs locaux et distants.

Lorsque vous déployez Log Collection, vous devez configurer les Log Collectors pour qu'ils collectent les événements de log auprès des diverses sources d'événements, puis pour qu'ils fournissent de manière fiable et sécurisée ces événements au service Log Decoder, dans lequel ils sont décryptés et stockés pour analyse ultérieure.

Vous pouvez configurer un ou plusieurs collecteurs distants pour transmettre les données d'événements à un collecteur local, ou vous pouvez configurer un collecteur local pour extraire les données d'événements d'un ou de plusieurs collecteurs distants.

Cette section explique comment :

- **Configurer un collecteur local pour qu'il extraie des événements d'un collecteur distant**

  Si vous souhaitez qu'un collecteur local extraie des événements à partir d'un collecteur distant, configurez ce paramètre dans l'onglet Collecteurs distants de la vue Configuration du collecteur local.

- **Configurer un collecteur distant pour qu'il transmette des événements à des collecteurs locaux**

Si vous souhaitez qu'un collecteur distant extraie des événements à partir d'un collecteur local, configurez ce paramètre dans l'onglet Collecteur local de la vue Configuration du collecteur distant. Dans la configuration de transmission, vous pouvez aussi :

- **Configurer un collecteur local de basculement pour le collecteur distant**

  Configurez une destination composée de collecteurs locaux. Lorsque le collecteur local principal est injoignable, le collecteur distant tente de se connecter à chaque collecteur local de cette destination jusqu'à ce qu'il réussisse à établir la connexion.

- **Configurer la réplication**

  Vous configurez plusieurs groupes de destinations afin que NetWitness réplique les données d'événements dans chaque groupe. Si la connexion à l'un des groupes de destinations échoue, vous pouvez restaurer les données requises, car elles sont répliquées dans l'autre groupe de destinations.

- **Configurer le routage de logs pour des protocoles spécifiques**

  Vous configurez plusieurs destinations dans un groupe de destinations afin de diriger les données d'événements vers des emplacements spécifiques en fonction du type de protocole.

- **Configurer une chaîne de collecteurs distants**

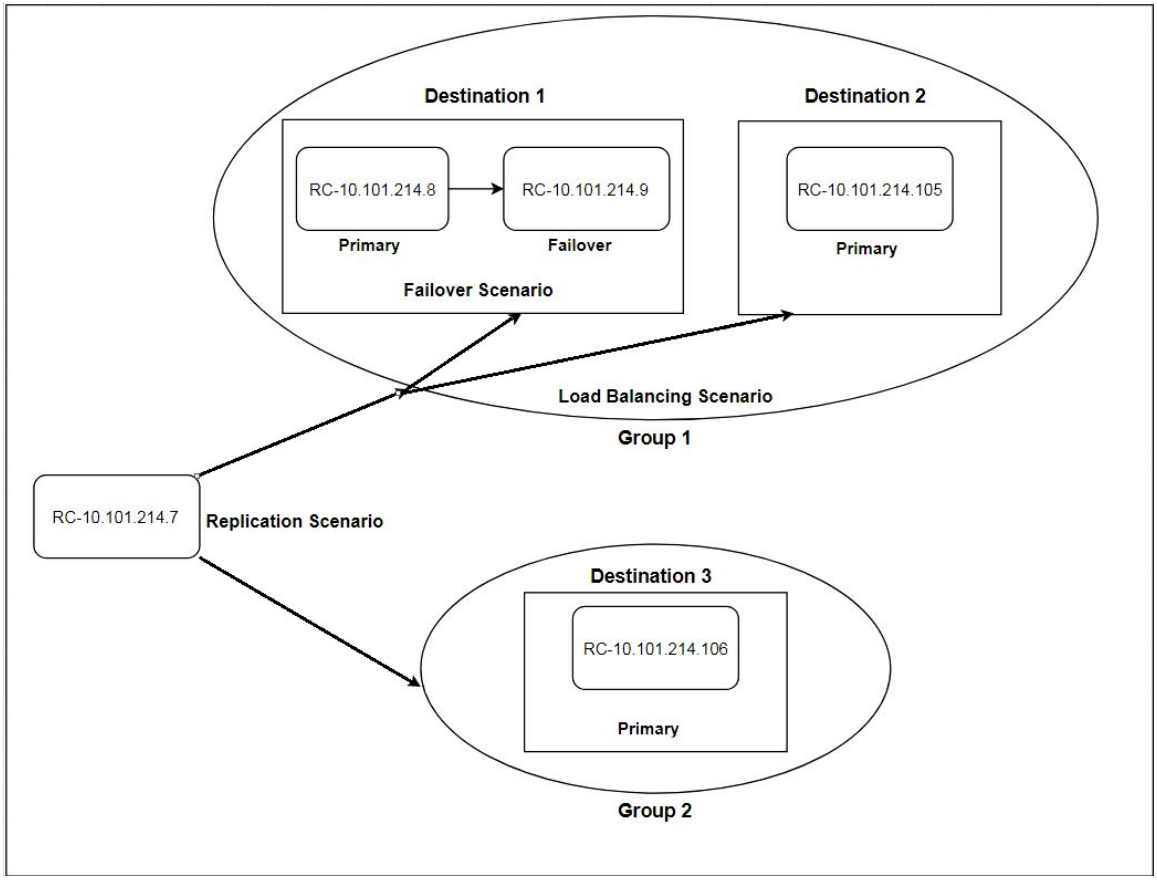
  Vous pouvez configurer une chaîne de collecteurs distants pour transmettre les données d'événements à un collecteur local, ou vous pouvez configurer un collecteur local pour extraire les données d'événements d'une chaîne de collecteurs distants.

  - Vous pouvez configurer un ou plusieurs collecteurs distants pour transmettre les données d'événement à un collecteur distant.
  - Vous pouvez configurer un collecteur distant pour qu'il extraie les données d'événement d'un ou plusieurs collecteurs distants.

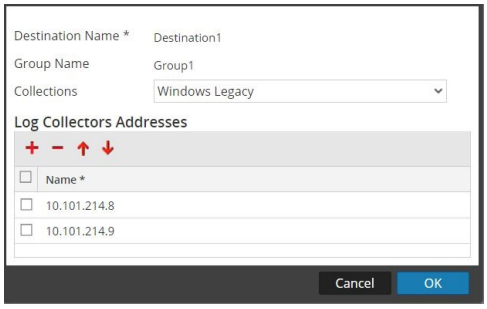
Basculement sur incident, réplication et équilibrage de charge

Cette rubrique décrit le basculement sur incident, la réplication et l'équilibrage de travail dans RSA NetWitness Suite.

La figure suivante illustre un collecteur distant configuré pour l'équilibrage de charge, le basculement sur incident et la réplication.

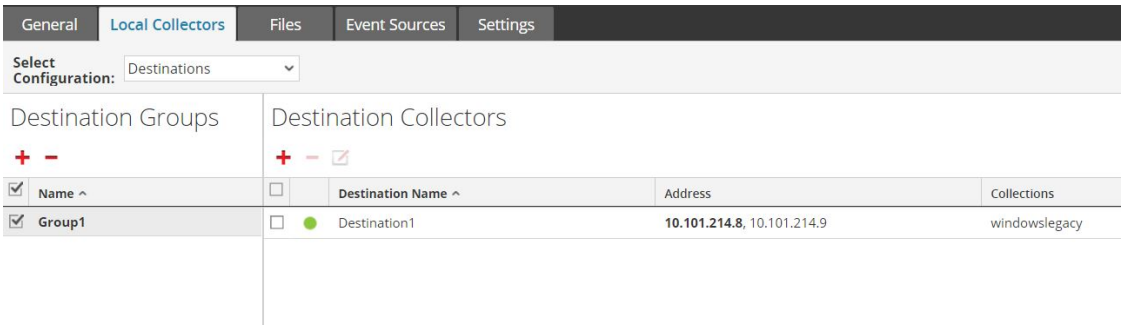


- Le **basculement sur incident** est obtenu en configurant plusieurs collectors dans la même destination. La destination 1 a un Collector primaire et la seconde, un Collector de basculement sur incident. Cela s'effectue dans NetWitness Suite en ajoutant différents Log Collectors vers la même destination.

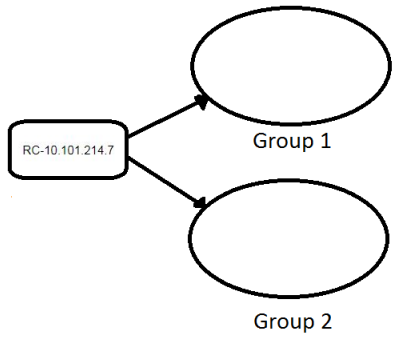


  Étant donné que la valeur 10.101.214.8 est répertoriée en première, elle devient le collector primaire et 10.101.214.9 devient le basculement sur incident. Pour faire de 10.101.214.9 le collector primaire, utilisez la flèche vers le haut pour modifier l'ordre.

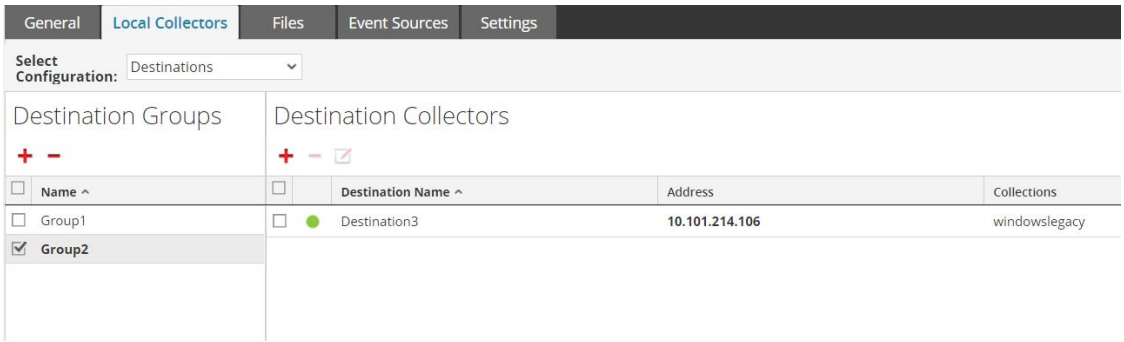
  Ci-dessous, vous pouvez voir les deux collectors répertoriés pour la destination 1. Le collector primaire (10.101.214.8) est en gras.



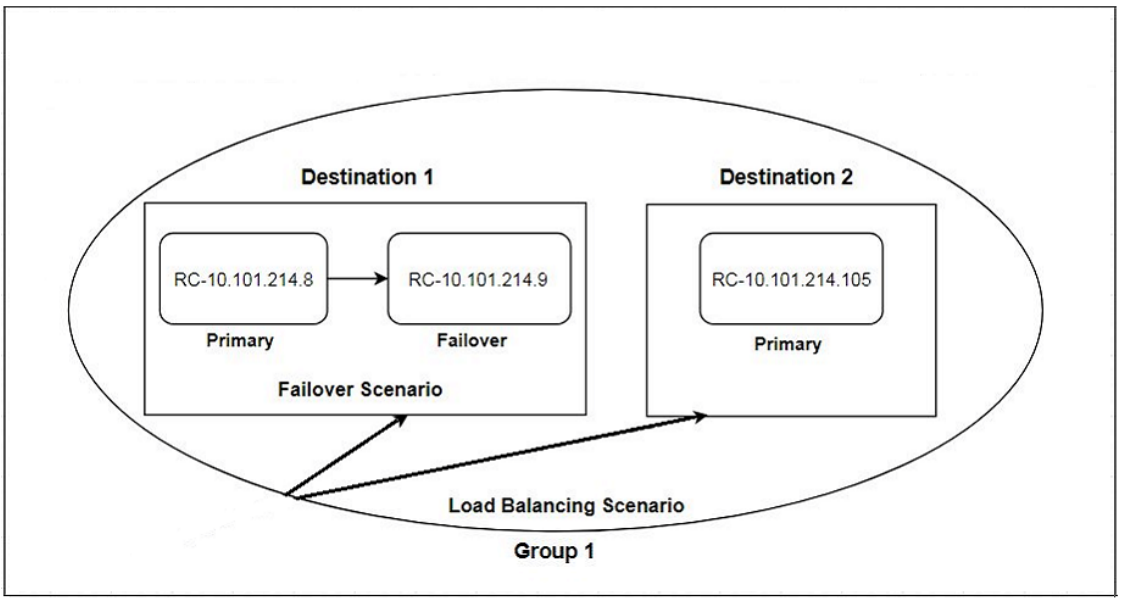
- La **réplication** s'effectue en ayant plusieurs groupes de destination : chaque groupe reçoit l'ensemble des données du message.



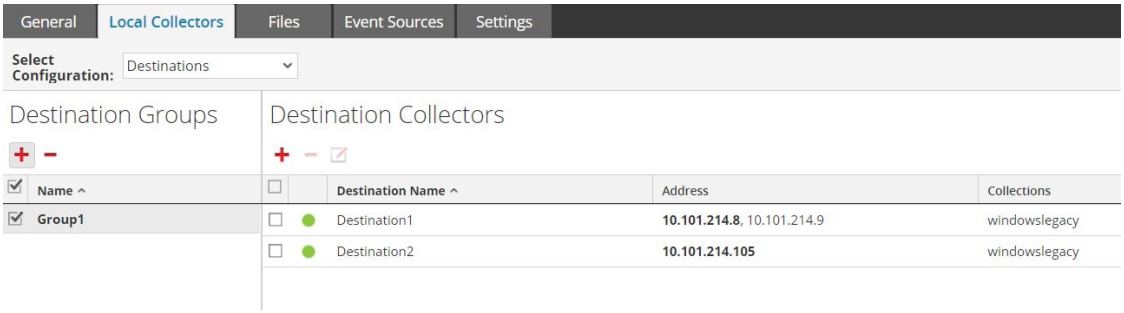
Dans l'écran suivant, vous pouvez voir que les données du message sont envoyées aux collectors du groupe 1 *et* du groupe 2.



- L'**équilibrage de charge** est obtenu en configurant plusieurs destinations dans un groupe.



Dans l'écran suivant, vous pouvez voir que le groupe 1 a deux destinations, Destination 1 et Destination 2. Les données du message sont équitablement divisées entre les destinations dans le groupe.



Avec deux destinations, chaque destination reçoit la moitié des données du message. Avec trois destinations, chacune reçoit 1/3 du total des données du message. Continuez d'ajouter des destinations pour réduire davantage la charge sur les collectors dans chaque destination.

Remarque : Vous pouvez également configurer le routage des logs afin que ces données d'événements pour des protocoles spécifiques soient envoyées vers des destinations.

Configurer un collecteur local ou un collecteur distant

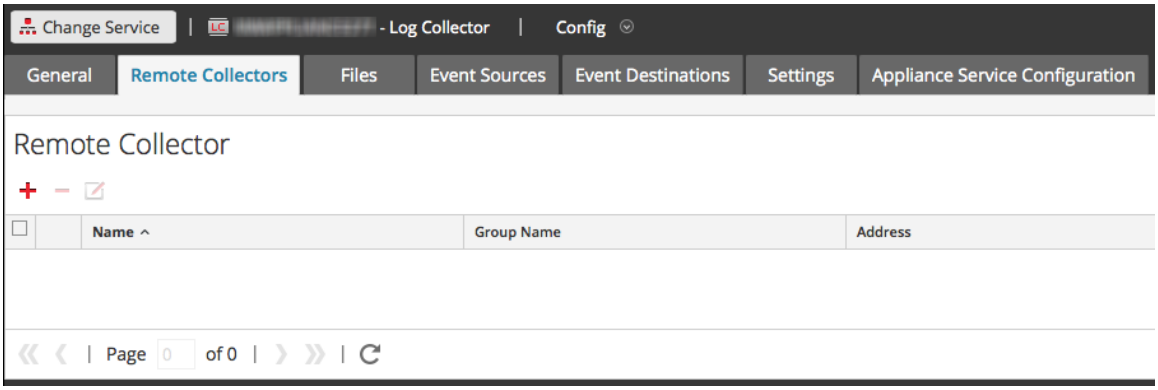
Vous choisissez le Log Collector, qui est un collecteur local (LC) ou distant (RC), pour lequel vous souhaitez définir des paramètres de déploiement dans la vue Services. La procédure suivante indique comment accéder à la vue Services, sélectionner un connecteur local ou distant, puis afficher l'interface des paramètres de déploiement pour ce service.

Pour configurer un collecteur local ou un collecteur distant :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs local ou à distance.
3. Sous Actions, sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. En fonction de votre sélection à l'étape 2 :
   - Si vous avez sélectionné un collecteur local, l'onglet **Collecteurs distants** s'affiche. Sélectionnez les collecteurs distants à partir desquels le collecteur local extrait les événements dans cet onglet.
   - Si vous avez sélectionné un collecteur distant, les **Collecteurs locaux** s'affichent. Sélectionnez les collecteurs locaux vers lesquels le collecteur distant envoie des événements dans cet onglet.

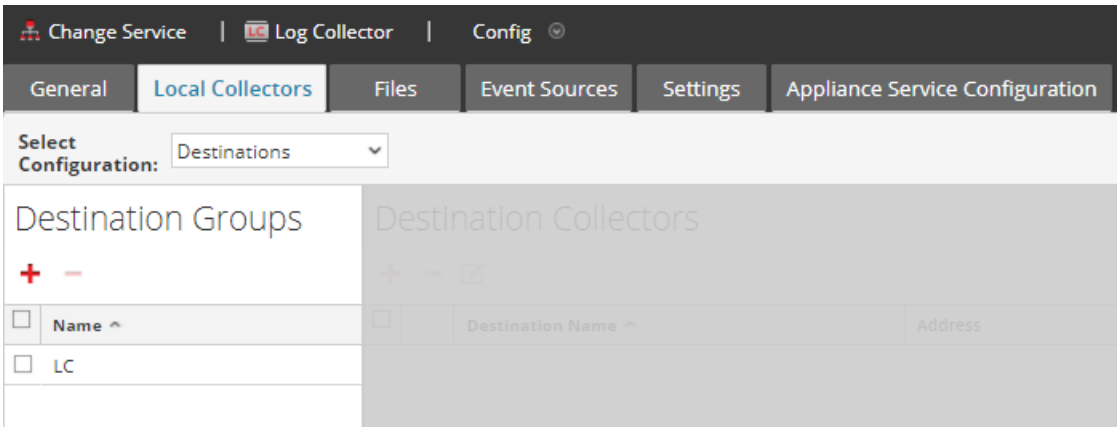
Onglets Collecteurs distants

La figure suivante illustre l'onglet **Collecteurs distants** pour un collecteur local qui est configuré pour extraire les événements d'un collecteur distant. NetWitness Suite affiche cet onglet lorsque vous avez sélectionné un collecteur local dans **Admin > Services**.

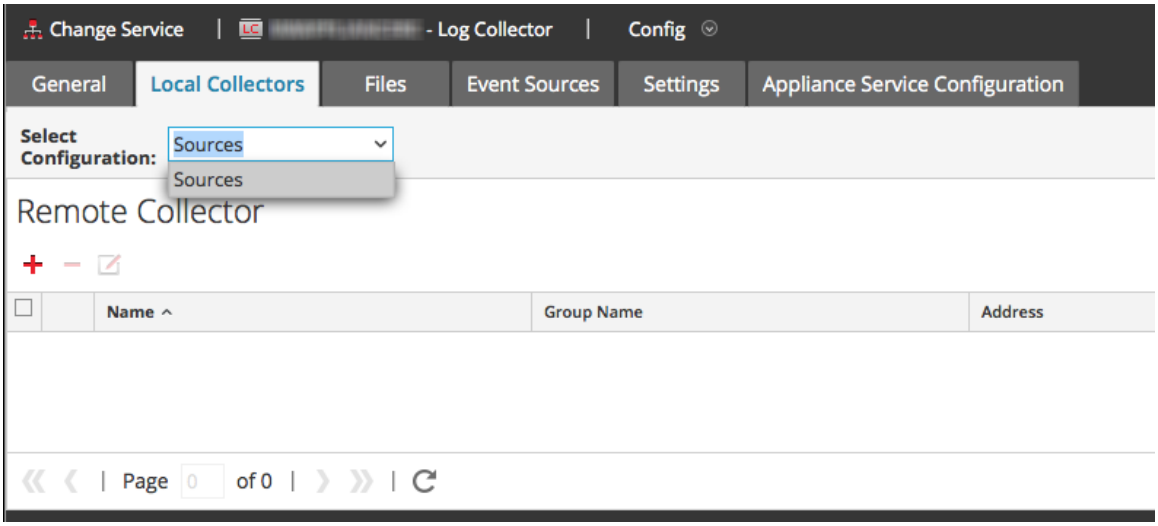


Onglet Local Collectors pour un Remote Collector

La figure suivante présente un onglet **Collecteurs locaux** concernant un collecteur distant configuré pour transmettre des événements à un collecteur local ou à un autre collecteur distant.



La figure suivante illustre l'onglet Collecteurs locaux pour un collecteur local qui est configuré pour extraire les événements d'un collecteur distant. NetWitness Suite affiche cet onglet lorsque vous avez sélectionné un collecteur distant dans **Admin > Services**.



Paramètres

Paramètres de configuration du collecteur distant et du collecteur local

Configurer le Local Collector de basculement

Cette rubrique indique comment configurer un Local ou Remote Collector de basculement sur incident.

Configurer un service Local Collector de basculement

Vous pouvez configurer un service Local Collector de basculement vers lequel RSA NetWitness® Suite basculera si votre Local Collector principal cesse de fonctionner pour une raison quelconque.

1. Accédez à **ADMIN> Services**.
2. Dans **Services**, sélectionnez un service Remote Collector.
3. Cliquez sur sous **Actions**, puis sélectionnez **Vue > Config**.

   La vue Configuration des services s'affiche avec l'onglet **Log CollectorGénéral** ouvert.
4. Sélectionnez l'onglet **Collecteurs locaux**.
5. Dans la rubrique **Panneau Groupes de destination**, sélectionnez .

   La boîte de dialogue Ajouter une destination distante s'affiche.
6. Définissez un groupe de destination et sélectionnez un Local Collector principal (par exemple, **LC-PRIMARY**).
7. Sélectionnez le groupe (par exemple, **Primary_Standby_LCs**) dans le panneau Groupes de destination et cliquez sur .

   Le groupe que vous avez sélectionné s'affiche dans le panneau Collecteurs locaux.
8. Ajoutez le Local Collector de basculement (par exemple, **LC-STANDBY**).

   Les exemples suivants affichent les services Local Collector principaux et de basculement nouvellement ajoutés, en affichant le Local Collector principal en tant qu'**Actif** et le Local Collector de basculement en tant que **Veille**. Le Local Collector est mis en évidence (par exemple, **LC-PRIMARY**).
9. (Facultatif) Ajoutez, supprimez et modifiez l'ordre des collecteurs locaux pour chaque destination distante.

   a. Cliquez sur pour ajouter un Log Collector en tant que destination distante de basculement sur incident.

   b. Lorsque vous vous connectez à une destination distante, le Local Collector tentera de se connecter à chaque Local Collector dans l'ordre de la liste, jusqu'à ce qu'il établisse une connexion réussie.

   c. Sélectionnez un Local Collector et utilisez les flèches pointant vers le haut ( ) et vers le bas ( ) pour modifier l'ordre de la connexion.

   d. Sélectionnez un ou plusieurs collecteurs locaux et cliquez sur pour les supprimer de la liste.

   Les services Local Collector sélectionnés sont ajoutés à la section Log Collector. Lorsque le service Remote Collector démarre la collecte des données, il transmet les données à ces services Log Collectors.

Configurer un service Remote Collector de basculement :

Vous pouvez configurer un Remote Collector de basculement vers lequel RSA NetWitness® Suite basculera si votre Remote Collector principal cesse de fonctionner pour une raison quelconque.

1. Accédez à **ADMIN > Services.**
2. Dans **Services**, sélectionnez un service Remote Collector.
3. Cliquez sur  sous **Actions**, puis sélectionnez **Vue > Config**.

   La vue Configuration des services s'affiche avec l'onglet **Log CollectorGénéral** ouvert.
4. Sélectionnez l'onglet **Collecteurs locaux**.
5. Sélectionnez **Sources** dans le menu déroulant **Sélectionner la configuration**.
6. Cliquez sur  pour afficher dans la boîte de dialogue **Ajouter une source** .
7. Définissez le Remote Collector de basculement et cliquez sur **OK**.

Paramètres

Paramètres de configuration du collecteur distant et du collecteur local

Configurer la réplication

Cette rubrique vous indique comment répliquer les données d'événements envoyées par un collecteur distant.

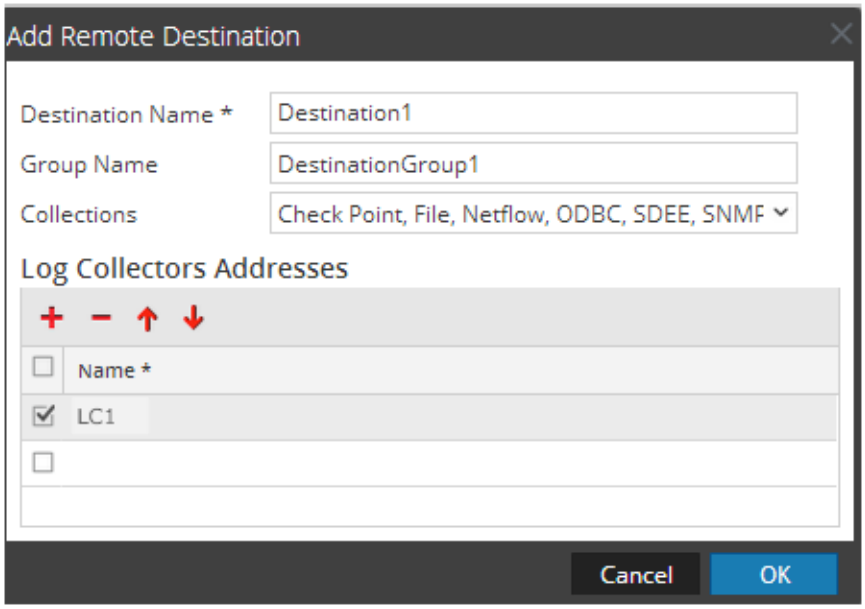
Vous pouvez spécifier plusieurs groupes de destination afin de répliquer les données d'événements dans chacun d'entre eux.

Pour répliquer les données d'événements sur plusieurs Local Collectors :

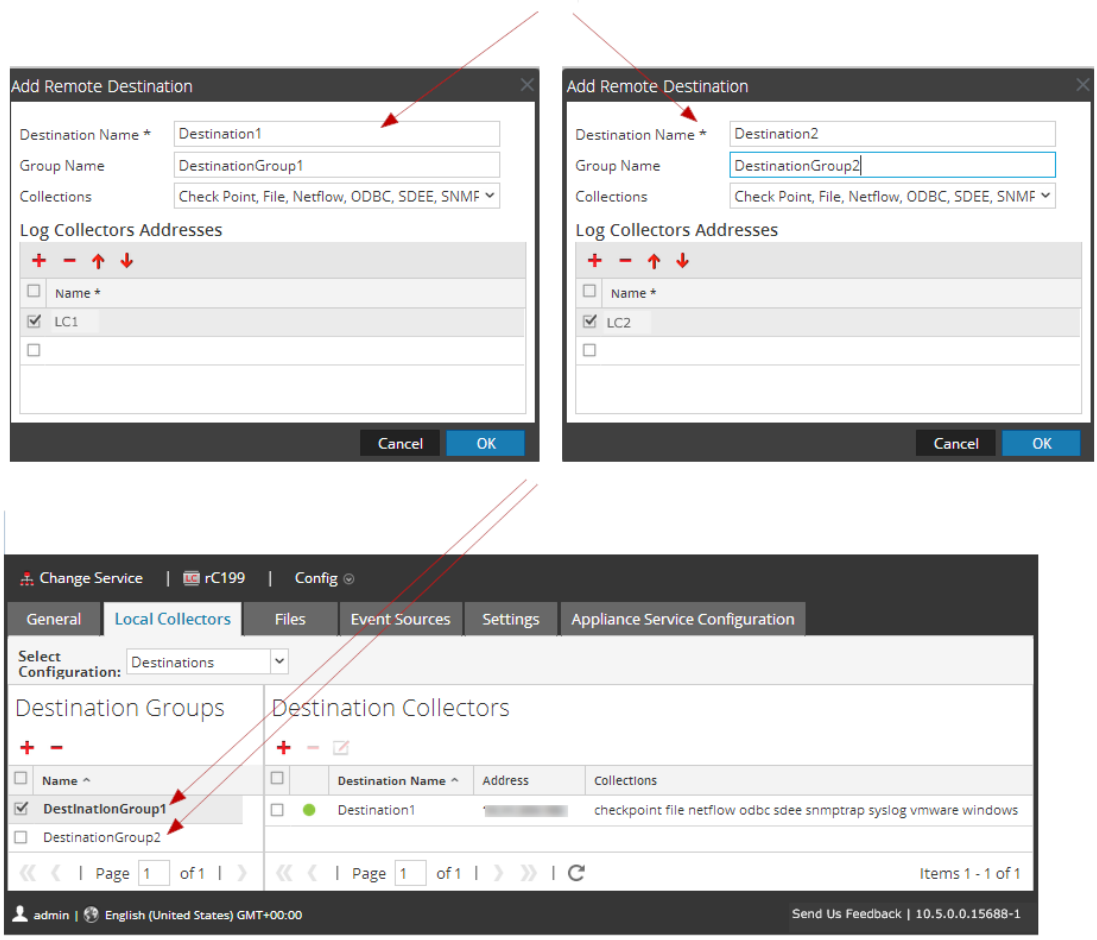
1. Accédez à **ADMIN > Services.**
2. Sélectionnez un service collecte de logs à distance.
3. Sous Actions, sélectionnez  **> Afficher > Config**.

   La vue Configuration des services s'affiche avec l'onglet **Log CollectorGeneral** ouvert.
4. Sélectionnez l'onglet **Collecteurs locaux**.
5. Dans la rubrique Panneau **Groupes de destination**, cliquez sur  .

   La boîte de dialogue **Ajouter une destination distante** s'affiche.



6. Configurez une destination différente pour chaque Local Collector et définissez les protocoles pour lesquels vous souhaitez transmettre des messages d'événements au Local Collector en question. Les exemples suivants illustrent l'ajout de deux Local Collectors de destination (**Destination1** et **Destination2**) pour les protocoles de collecte **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog** et **Windows** :



a. Saisissez le **nom de la destination**.

b. Saisissez le **nom du groupe**. Si vous n'indiquez aucun nom de groupe, le nom de la destination est utilisé par défaut.

c. Sélectionnez les protocoles de collecte dans la liste déroulante.

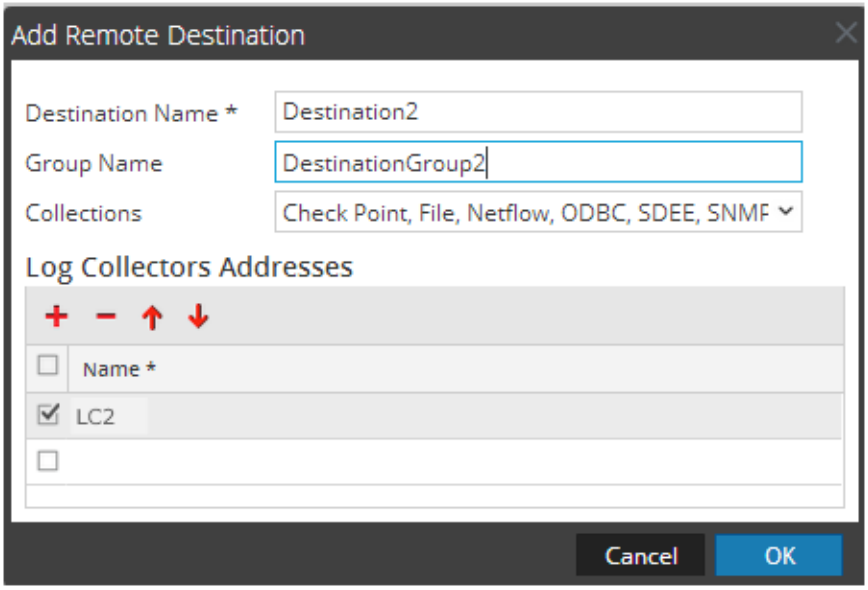
d. Sélectionnez un Local Collector (par exemple, **LC1**).

e. Cliquez sur **OK**.

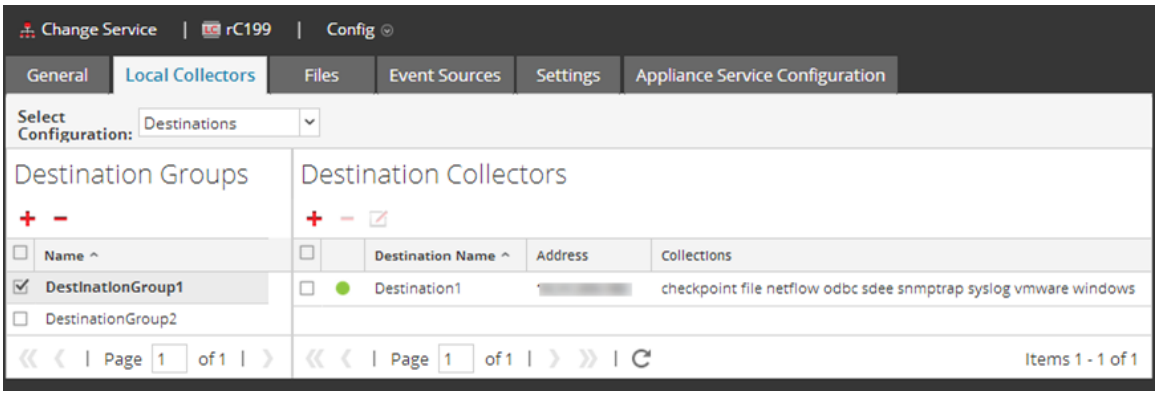
f. Sélectionnez le nouveau groupe (par exemple, **GroupeDestination2**) dans le panneau **Groupes de destination**, puis cliquez sur + dans le panneau **Local Collector**.

g. Dans le panneau **Local Collector**, cliquez sur +, puis complétez la boîte de dialogue

Ajouter une destination distante, comme illustré dans la figure suivante.



Les protocoles de collecte **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog** et **Windows** sont envoyés à deux collecteurs locaux (**LC1** et **LC2**). Ces deux collecteurs sont actifs et collectent des données d'événements.



Configurer une chaîne de collecteurs distants

Cette rubrique décrit comment configurer une chaîne de collecteurs distants (également nommés VLC).

Vous pouvez configurer une chaîne de collecteurs distants pour transmettre les données d'événements à un collecteur distant, ou vous pouvez configurer un collecteur distant pour extraire les données d'événements d'une chaîne de collecteurs distants.

- **Remote Collectors pour transmettre les données.** Transmettre les données d'un Remote Collector à d'autres Remote Collectors ou Local Collectors.

- **Remote Collector pour extraire les données.** Utilisez un collecteur distant pour extraire les données à partir d'un ou plusieurs collecteurs distants.

Configurer un collecteur distant pour qu'il transmette des données d'événement à des collecteurs distants

Vous pouvez configurer un collecteur distant pour transmettre les données d'événement à un collecteur distant.

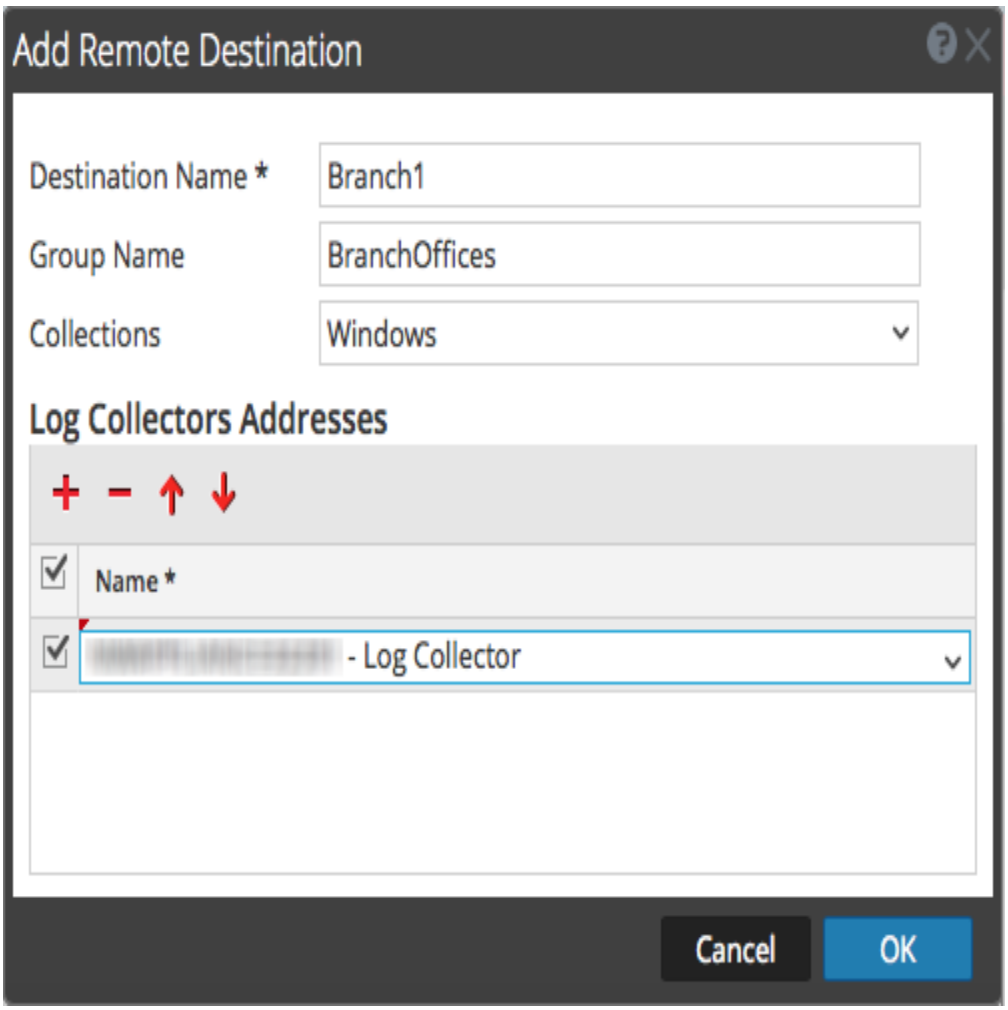
Configurer un collecteur distant pour qu'il transmette des événements au collecteur distant spécifié

1. Accédez à **ADMIN > Services**.
2. Dans **Services**, sélectionnez un **Collecteur distant**.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

   La vue **Log CollectorConfiguration des services** s'affiche avec l'onglet **Log Collector Général** ouvert.
4. Sélectionnez l'onglet **Collecteurs locaux**.
5. Sélectionnez **Destinations** dans le menu déroulant **Sélectionner les configurations**.
6. Dans la rubrique **Panneau Groupes de destination**, sélectionnez  .

   La boîte de dialogue **Ajouter une destination distante** s'affiche.
7. Configurer un **groupe de destination** :
   a. Saisissez le **Nom de la destination**.
   b. (Facultatif) **Saisissez un nom de groupe**. Si vous laissez le champ Nom du groupe vide, NetWitness Suite définit la valeur que vous avez spécifiée dans la zone Nom de la destination.
   c. Sélectionnez un ou plusieurs protocoles de collecte dans la liste déroulante **Collectes**.
   d. Sous **Adresses des Log Collectors**, cliquez sur  pour sélectionner un collecteur

distant.



Remarque : Si vous ne sélectionnez aucun protocole de collecte, le collecteur distant transmet tous les protocoles de collecte aux collecteurs distants.

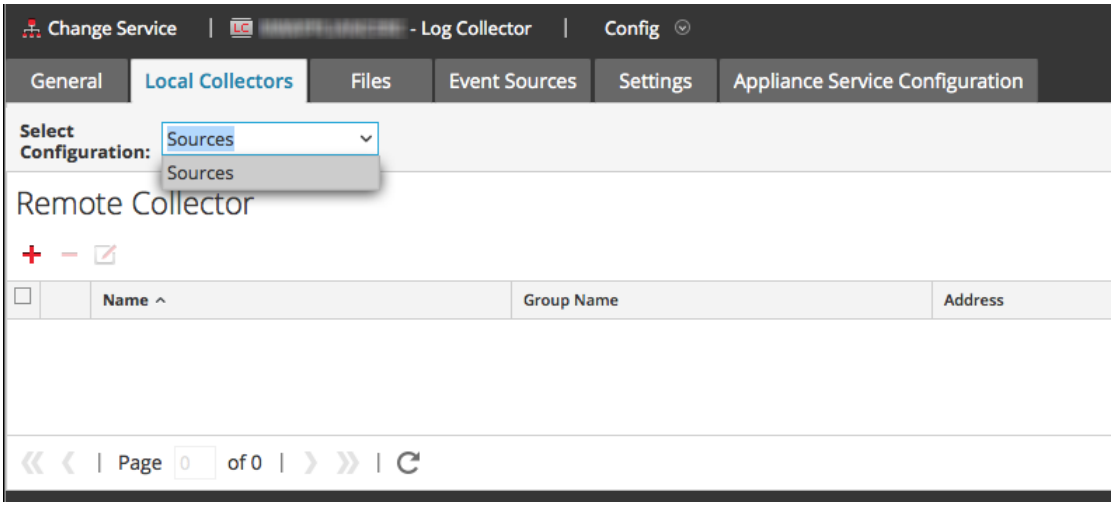
Configurer un collecteur distant pour qu'il extraie des données d'événement d'un collecteur distant

Configurer le collecteur distant sélectionné pour qu'il extraie des événements du collecteur distant spécifié

1. Accédez à **ADMIN > Services**.
2. Dans **Services**, sélectionnez un **Collecteur distant**.
3. Sous Actions, puis sélectionnez > **Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

   La vue **Configuration des services** s'affiche avec l'onglet **Log Collector Général** ouvert.

4. Sélectionnez l'onglet **Collecteurs locaux**.
5. Sélectionnez **Sources** dans le menu déroulant **Sélectionner les configurations**.



6. Dans le panneau **Collecteurs distants**, cliquez sur +.

   La boîte de dialogue **Ajouter une source** s'affiche.
7. Dans la boîte de dialogue **Ajouter une source** :
   a. Sélectionnez un ou plusieurs protocoles de collecte.

      Si vous ne sélectionnez aucun protocole de collecte, le collecteur distant extrait tous les protocoles de collecte du collecteur distant.
   b. Cliquez sur **OK**.

      Le collecteur distant est ajouté à la section Collecteur distant. Lorsque le Log Collector commence la collecte des données, il extrait les données d'événements de ce collecteur distant.

Réguler la bande passante entre le Remote Collector et le Local Collector

Pour améliorer les performances, vous pouvez réguler la bande passante afin de contrôler la vitesse à laquelle le Remote Collector envoie des données au Local Collector ou entre les courtiers de messages. Pour cela, configurez la fonctionnalité de filtrage du noyau Linux et la fonctionnalité IpTable.

Cela s'applique aux deux configurations de transmission (Push) et d'extraction (Pull) du Remote Collector. Le script shell **set-shovel-transfer-limit.sh** situé dans le dossier **/opt/netwitness/bin** automatise la configuration de Iptables et du filtre de noyau liés à ce port.

Cette rubrique décrit comment réguler la bande passante entre le Remote Collector et le Local Collector à l'aide du script de shell **set-shovel-transfer-limit.sh**. Elle se compose des sections suivantes :

- L'aide en ligne relative à la commande de script **set-shovel-transfer-limit.sh**.

  Remarque : La valeur du filtre que vous devez définir dépend du taux auquel le collecteur distant de logs envoie les événements au Local Collector.

- Un exemple qui définit le filtre à 4 096 kilobits par seconde.

Aide relative à la ligne de commande pour le script Set Shovel Transfer Limit

Exécutez la commande`-h` pour afficher une aide pour le script de shell `set-shovel-transfer-limit.sh` .

```
cd /opt/netwitness/bin
./set-shovel-transfer-limit.sh
```

Syntaxe :

```
code>set-shovel-transfer-limit.sh -s|-c|-d|[-i interface] [-r rate]
```

où :

- -c = clear existing
- -d = display filter
- -s = set new values
- -i = interface is the name of the network interface. La valeur par défaut est **eth0**
- -r = rate is the bandwidth rate. La valeur par défaut est **256 kbps**

La bande passante et les taux peuvent être spécifiés dans :

- **nolimit**: disables throttling
- **kbit** : Kilobits par seconde
- **mbit** : Mégabits par seconde
- **kbps** : Kilooctets par seconde
- **mbps** : Mégaoctets par seconde
- **bps** : Octets par seconde

Définir le filtre à 4 096 kilobits par seconde

Cet exemple définit le filtre à 4 096 kilobits par seconde.

```
[root@<hostname> bin]#./set-shovel-transfer-limit.sh -s -r 4096kbit
```

```
RATE=4096kbit
 PORTNUMBER=5671
 DEVICE_INTERACE=eth0

iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK
]

Current/new values...

iptables -t mangle -n -v -L
 Chain PREROUTING (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target  prot opt in  out  source
destination

Chain INPUT (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target prot opt in out   source          destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out   source          destination

Chain OUTPUT (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0     0.0.0.0/0
multiport dports 5671 MARK set 0xa
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0    0.0.0.0/0
multiport sports 5671 MARK set 0xa

Chain POSTROUTING (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination

tc -s -d class show dev eth0
 class htb 1:1 root rate 10000Kbit ceil 10000Kbit burst 1600b/8
mpu 0b overhead 0b cburst 1600b/8 mpu 0b overhead 0b level 7
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 20000 ctokens: 20000

class htb 1:2 parent 1:1 prio 0 quantum 51200 rate 4096Kbit ceil
4096Kbit burst 1599b/8 mpu 0b overhead 0b cburst 1599b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 48828 ctokens: 48828
```

Configurer un Lockbox

Cette rubrique vous indique comment configurer les paramètres de sécurité Lockbox.

Définition d'un Lockbox

Un Lockbox est un fichier chiffré permettant de stocker les informations confidentielles d'une application. Le Lockbox NetWitness Suite stocke une clé de chiffrement pour le Log Collector.

La clé de chiffrement est utilisée pour chiffrer tous les mots de passe de la source d'événement et le mot de passe du broker d'événement.

Lorsque vous créez le Lockbox, vous devez lui définir un mot de passe.

Lors de la collecte des données, le Log Collector exploite le Lockbox dans un mode qui ne requiert pas de mot de passe (le Log Collector utilise plutôt l'empreinte numérique sur le système hôte).

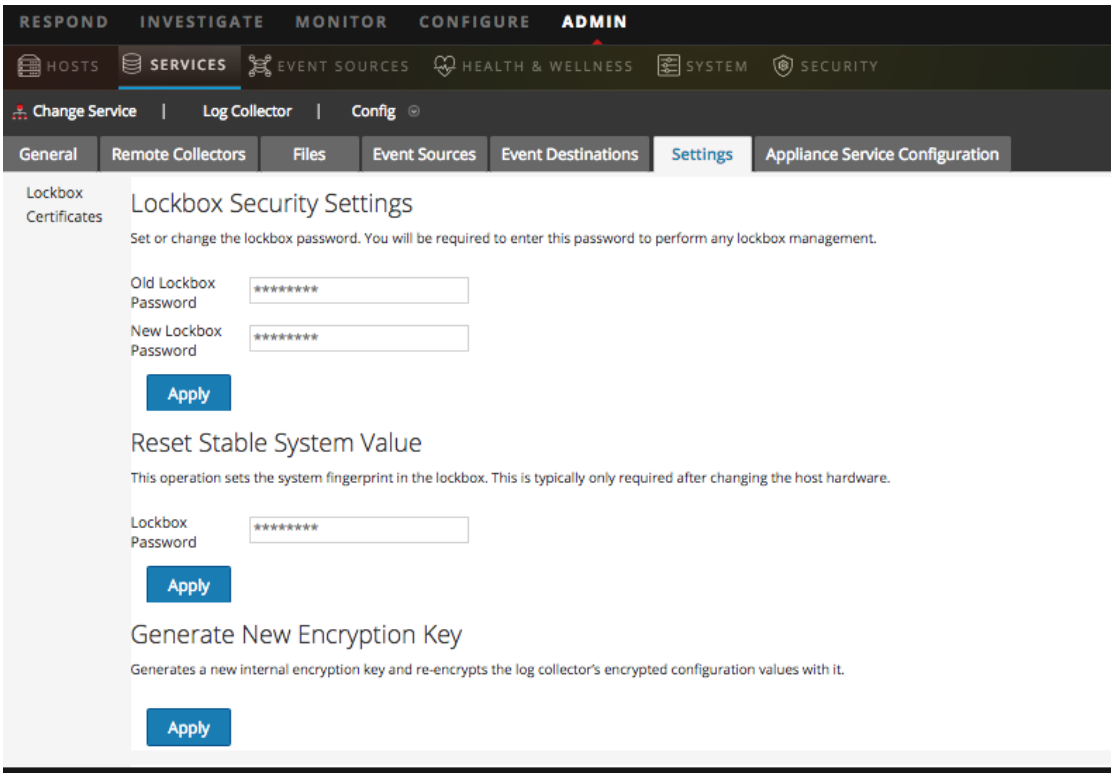
Il s'agit des paramètres de sécurité du lockbox.

Fonctionnalité	Description
Ancien mot de passe Lockbox	Lorsque vous configurez un Lockbox pour la première fois, ce champ est vide. NetWitness Suite renseigne ce champ après avoir saisi un nouveau mot de passe Lockbox, puis cliqué sur Appliquer.
Nouveau mot de passe Lockbox	Mot de passe Lockbox initial ou nouveau. Pour renforcer au maximum la sécurité du Lockbox, spécifiez un mot de passe composé de minimum huit caractères avec au moins un caractère numérique, une lettre majuscule et un caractère non-alphanumérique, par exemple # ou !
Appliquer	Cliquez sur **Appliquer** pour enregistrer le changement du mot de passe Lockbox.

Configurer un Lockbox

Pour configurer un Lockbox, vous devez définir un mot de passe, comme suit :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Paramètres**.



5. Dans le panneau des options, sélectionnez **Lockbox** pour configurer les paramètres Lockbox.
6. Dans **Paramètres de sécurité Lockbox**, saisissez un mot de passe dans le champ **Nouveau mot de passe Lockbox**, puis cliquez sur **Appliquer**.

Démarrer des services de collecte

Si un service de collecte s'arrête, vous devrez peut-être le redémarrer. Vous pouvez aussi activer le démarrage automatique des services de collecte.

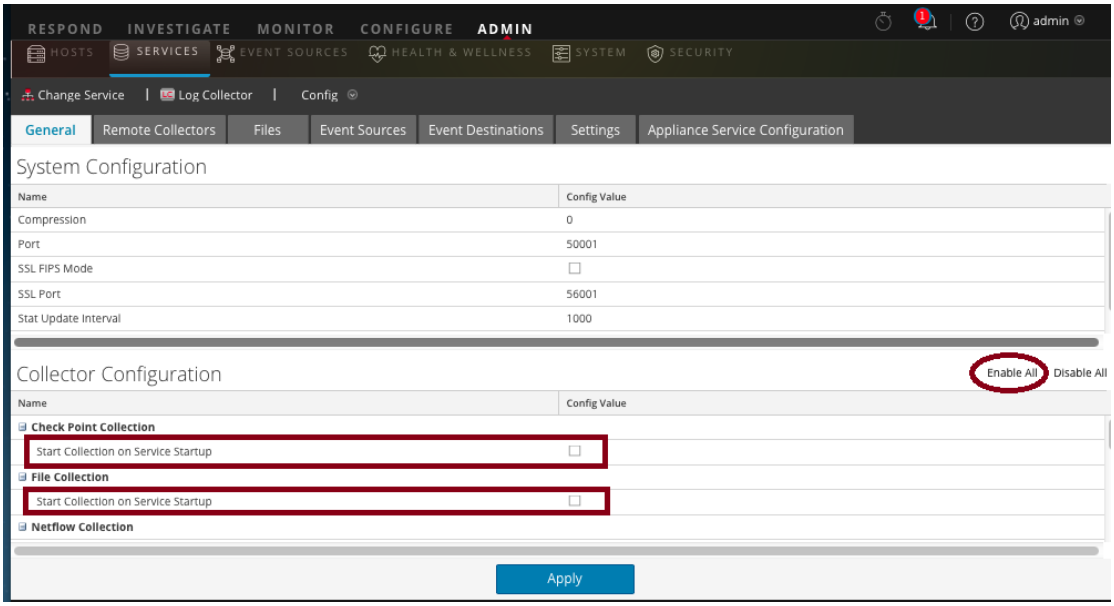
Démarrer un service de collecte

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service Log Collector, puis cliquez sur  sous **Actions**.
3. Cliquez sur **Vue** > **Système**.
4. Cliquez sur **Collecte** > ***service*** (par exemple, **Fichier**) et cliquez sur **Démarrer**.

Activer le démarrage automatique des services de collecte

1. Accédez à **Admin > Services**.
2. Sélectionnez un service Log Collector, puis cliquez sur  sous **Actions**.
3. Cliquez sur **Vue** > **Config**.

   L'onglet Général s'affiche.
4. Dans le panneau Configuration des collecteurs, sélectionnez **Lancer la collecte au démarrage du service** pour les services de collecte individuels que vous voulez lancer automatiquement. Vous pouvez également sélectionner **Activer tout** pour démarrer automatiquement tous les services de collecte.



5. Cliquez sur **Appliquer** pour que vos modifications prennent effet.

Vérifier le fonctionnement de Log Collection

Cette rubrique vous indique comment vérifier que vous avez correctement configuré Log Collection.

Les méthodes suivantes permettent de vérifier que ce Log Collection fonctionne correctement.

- Vérifiez la présence d'une activité d'événement dans l'onglet Surveillance des sources d'événements de la vue **Administration > Intégrité**.
- Pour le protocole de collecte configuré, vérifiez la présence de parsers dans le champ **device.type** de la colonne **Détails** dans la vue **Investigation > Événements**.

Consultez la rubrique de chaque protocole de collecte pour prendre connaissance des étapes de vérification de la configuration du protocole.

Configurer des certificats

Vous gérez les certificats en créant des magasins d'approbations sur le Log Collector. Le Log Collector fait référence à ces magasins d'approbations afin de déterminer si les sources d'événements sont considérées comme fiables.

Ajout d'un certificat

Pour ajouter un certificat :

1. Accédez à **ADMIN > Services**.
2. Dans la grille **Services**, sélectionnez un **Log Collector**service.
3. Cliquez sur  sous **Actions**, puis sélectionnez **Vue > Config**.
4. Cliquez sur l'onglet **Paramètres**.
5. Dans le panneau des options, sélectionnez **Certificats**.
6. Cliquez sur  dans la barre d'outils **Certificats**.

   La boîte de dialogue **Ajouter un certificat** s'affiche.
7. Cliquez sur **Parcourir** et sélectionnez un certificat (***.PEM**) à partir de votre réseau.
8. Spécifiez un mot de passe si nécessaire.
9. Cliquez sur **Enregistrer**.

Panneau Certificats

Le tableau suivant décrit les boutons et les colonnes disponibles dans le panneau Certificats.

Champ	Description
	Ouvre la boîte de dialogue Ajouter un certificat dans laquelle vous pouvez ajouter un certificat et un mot de passe.
	Supprime les certificats sélectionnés.
	Sélectionne les certificats.

Champ	Description
Nom de la zone de stockage fiable	Affiche le nom du magasin d'approbations.
Nom unique de certificat	Pour la source d'événement de point de contrôle uniquement, affiche le nom unique du certificat.
Nom du mot de passe du certificat	Pour la source d'événement de point de contrôle uniquement, affiche le mot de passe du certificat.

Boîte de dialogue Ajouter un certificat

Le tableau suivant décrit les paramètres de la boîte de dialogue **Ajouter un certificat**.

Champ	Description
Nom de la zone de stockage fiable	Saisissez un nom de magasin d'approbations.
Fichier	Cliquez sur Parcourir pour sélectionner un certificat (fichier *.PEM) à partir de votre réseau.
Mot de passe	Spécifie le mot de passe de ce certificat.
Fermer	Ferme la boîte de dialogue sans ajouter de certificat.
Enregistrer	Ajoute le certificat.

Notions de base de log Collection

Fonctionnement de la collecte de logs

Le service Log Collector collecte des logs depuis des sources d'événements dans tout l'environnement IT dans une organisation et transfère les logs à d'autres composants NetWitness Suite. Les logs et le contenu descriptif sont stockés sous forme de métadonnées pour une utilisation dans des procédures d'enquête et des rapports.

Les sources d'événements sont les ressources sur le réseau, telles que des serveurs, des commutateurs réseau, des routeurs, des baies de stockage, des systèmes d'exploitation et des pare-feu. Dans la plupart des cas, votre équipe de technologies de l'information (IT) configure des sources d'événements pour envoyer leurs logs au service Log Collector et l'administrateur NetWitness Suite configure le service Log Collector pour interroger des sources d'événements et récupérer leurs logs. Par conséquent, le Log Collector reçoit tous les logs sous leur forme d'origine.

Protocole de collecte

RSA NetWitness Suite peut collecter des logs à partir d'un large éventail de sources d'événements. Lorsque vous configurez la collecte de logs pour une source d'événement spécifique, vous devez avant tout connaître le protocole utilisé pour collecter les logs.

Protocole de collecte	Description
Check Point	Collecte des événements issus de sources d'événements Check Point à l'aide d'une interface OPSEC LEA. OPSEC LEA est l'APIE Check Point Operations Security Log Export qui facilite l'extraction des fichiers log. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événement Check Point dans NetWitness Suite.
Fichier	Collecte des événements depuis des fichiers logs. Les sources d'événements génèrent des fichiers log qui sont transférés à l'aide d'une méthode de transfert de fichiers sécurisée vers le service Log Collector. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements de fichiers dans NetWitness Suite.
Netflow	Accepte les événements Netflow v5 et Netflow v9. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements Netflow dans NetWitness Suite.

Protocole de collecte	Description
ODBC	Collecte les événements des sources d'événements qui stockent les données d'audit dans une base de données à l'aide de l'interface logicielle ODBC (Open Database Connectivity). Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements ODBC dans NetWitness Suite.
Plug-ins	La collecte de plug-ins est un cadre de collecte générique pour collecter des événements à l'aide de scripts externes écrits dans d'autres langues. RSA effectue actuellement la collecte pour Amazon Web Services (AWS) CloudTrail et Microsoft Azure. • **AWS** : Collecte des événements depuis Amazon Web Services (AWS) CloudTrail. CloudTrail enregistre spécifiquement les appels API AWS pour un compte. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements AWS (CloudTrail) dans NetWitness Suite. • **Azure** : Collecte des événements à partir de Microsoft Azure. Pour plus d'informations, reportez-vous à la rubrique Configurer des Sources d'événements Azure dans NetWitness Suite. Les clients peuvent utiliser ce cadre pour développer leurs propres protocoles de collecte.
SDEE	Collecte les messages IDS (Intrusion Detection System) et IPS (Intrusion Prevention Service). Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements SDEE dans NetWitness Suite.
Trap SNMP	Accepte les traps SNMP. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements SNMP dans NetWitness Suite.
Syslog	Accepte des messages de sources d'événements qui émettent des messages Syslog. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événements Syslog pour le collecteur distant. **Remarque :** Ne configurez pas la collecte Syslog pour les Log Collectors locaux. Vous devez uniquement configurer Syslog Collection pour les Remote Collectors.
VMware	Collecte des événements issus d'une infrastructure virtuelle VMware. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événement VMware dans NetWitness Suite.

Protocole de collecte	Description
Windows	Collecte des événements de machines Windows prenant en charge le modèle Microsoft Windows. Windows 6.0 est un framework de consignation et de suivi des événements compris dans les systèmes d'exploitation à partir de Microsoft Windows Vista et Windows Server 2008. Pour plus d'informations, reportez-vous à la rubrique Configurer des sources d'événement Windows dans NetWitness Suite.
Windows d'ancienne génération	Collecte des événements depuis : • D'anciennes versions de Windows comme Windows 2000 et Windows 2003 et collecte depuis des sources d'événements Windows qui sont déjà configurées pour une collection enVision sans devoir les reconfigurer. • Sources d'événements d'appliances ONTAP NetApp afin que vous puissiez maintenant collecter et analyser des fichiers NetApp evt. • Pour plus d'informations, reportez-vous à la rubrique Guide de configuration de la collecte Windows d'ancienne génération et NetApp. **Remarque :** Installez le collecteur NetWitness SuiteWindows d'ancienne génération sur un serveur physique ou virtuel Windows 2008 R2 SP1 64 bits à l'aide du fichier **SALegacyWindowsCollector-*version-number.exe***.

Procédure de base

La procédure de base est identique pour tous les protocoles de collecte pris en charge.

1. **Définissez votre source d'événement pour la collecte.** Chaque source d'événement prise en charge dispose d'un document de configuration disponible dans l'espace Sources d'événements pris en charge par RSA sur RSA Link.
   a. Accédez à l'espace Sources d'événements pris en charge par RSA sur RSA Link.
   b. Trouvez les Instructions de votre source d'événement.
      La page Overview répertorie toutes les sources d'événements actuellement prises en charge, ainsi que des informations sur la méthode de collecte, les classe du périphérique et les versions prises en charge.

c. Téléchargez les instructions de configuration de votre source d'événement et appliquez-les.

2. **Configurer la collecte sur RSA NetWitness Suite .** Le guide de configuration des sources d'événements contient ces instructions. Toutefois, ce guide fournit également ces instructions, en fonction de la méthode de collecte utilisée par votre source d'événement. Reportez-vous à la rubrique Protocole de collecte pour plus d'informations.
3. **Démarrez le service pour votre méthode de collecte.** Normalement, vous devez uniquement effectuer cette tâche pour la première source d'événement qui utilise cette méthode de collecte. Par exemple, la première fois que vous configurez une source d'événement qui utilise une collecte de fichiers, vous devrez peut-être démarrer le service de fichiers dans NetWitness Suite.
4. **Vérifiez que la collecte fonctionne pour votre source d'événement.**

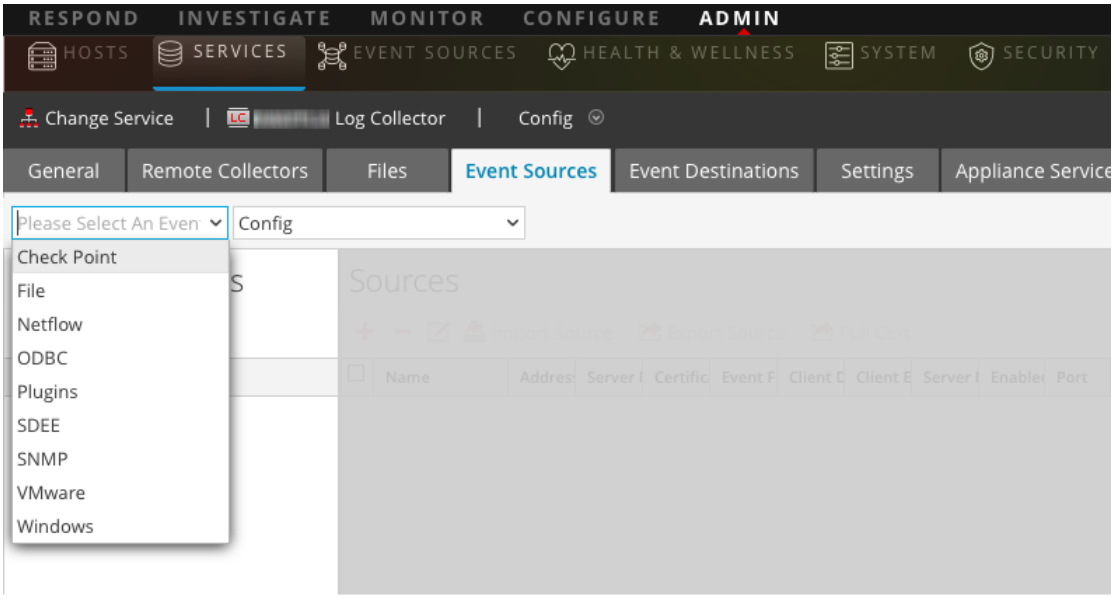
Le reste de cette rubrique décrit les étapes 2, 3 et 4 plus en détails.

Configurer la collecte dans RSA NetWitness Suite.

Le processus de configuration des sources d'événement dépend de la méthode de collecte qu'elles utilisent. Notez toutefois qu'ils sont très similaires. La procédure suivante est générique : plus de détails sur les méthodes de collecte individuelles sont disponibles dans les rubriques qui couvrent les détails pour chaque méthode de collecte spécifique.

1. Accédez à **ADMIN> Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements du Log Collector**, sélectionnez votre méthode de collecte dans le menu déroulant.
6. Dans la barre d'outils du panneau **Catégories d'événements**, cliquez sur +.

   La boîte de dialogue Types de sources d'événements disponibles s'affiche.
7. Sélectionnez un type de source d'événement et cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau Catégories d'événements.
8. Sélectionnez le nouveau type dans le panneau Catégories d'événements, puis cliquez sur **dans la barre d'outils** Sources +.

   La boîte de dialogue **Ajouter une source** s'affiche.
9. Saisissez les valeurs pour les paramètres disponibles.

   Reportez-vous à la rubrique Paramètres de la méthode de collecte spécifique que vous configurez.
10. Cliquez sur **OK**.

Démarrer le service pour votre méthode de collecte

Pour démarrer le service pour votre méthode de collecte, procédez comme suit :

1. Accédez à **Admin > Services**.
2. Sélectionnez un **Log Collector** et sélectionnez ⚙ **> Vue > Système**.

3. Cliquez sur **Collecte > *protocole*> Démarrer**

   où ***protocole*** est le protocole que vous souhaitez démarrer, par exemple **Netflow**.

Vérifier que la collecte fonctionne pour votre source d'événement.

Vous pouvez vérifier le fonctionnement de la méthode de collecte sous l'onglet **Admin > Intégrité > Surveillance des sources d'événements**.

Pour vérifier que la collecte fonctionne pour une source d'événement :

1. Accédez à **ADMIN > Intégrité**
2. Cliquez sur l'onglet **Surveillance des sources d'événements**.
3. Dans la grille, recherchez le **Log Decoder**, la **Source d'événement**et le **Type de source d'événement**.
4. Recherchez toute trace d'activité dans la colonne **Nombre** pour une source d'événement afin de vérifier que la collecte accepte les événements.

Configurer des filtres d'événements pour un Collector

Cette rubrique vous indique comment créer et gérer des filtres d'événements pour tous les protocoles de collecte.

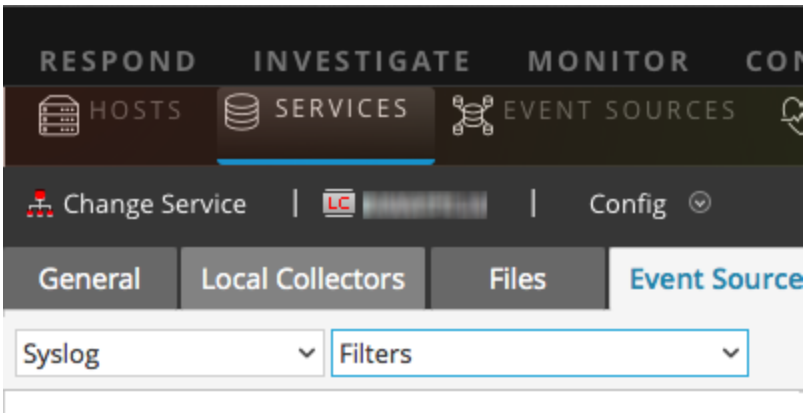
Remarque : Vous ne pouvez pas configurer de collecte Syslog pour les Local Log Collectors. Vous devez uniquement configurer Syslog Collection pour les Remote Collectors. Reportez-vous à la rubrique Configurer des collecteurs locaux et des collecteurs distants pour des informations de configuration supplémentaires.

Configurer un filtre d'événements

Pour configurer une source d'événements :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez **Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.
5. Sous l'onglet **Sources d'événements**, sélectionnez une méthode de collecte/**Filtre** dans les menus déroulants.

   L'écran suivant affiche **Syslog** sélectionné.

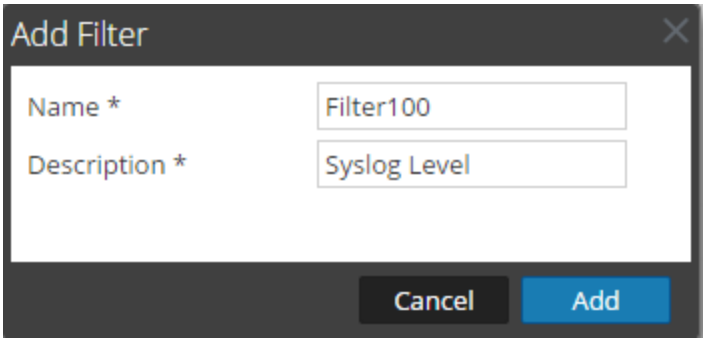


Remarque : La configuration de Syslog est uniquement disponible sur les Remote Collectors : si vous travaillez avec un service de Local Collector, **Syslog** n'est pas disponible dans le menu déroulant.

La vue **Filtres** affiche les filtres configurés pour la méthode de collecte sélectionnée, le cas échéant.

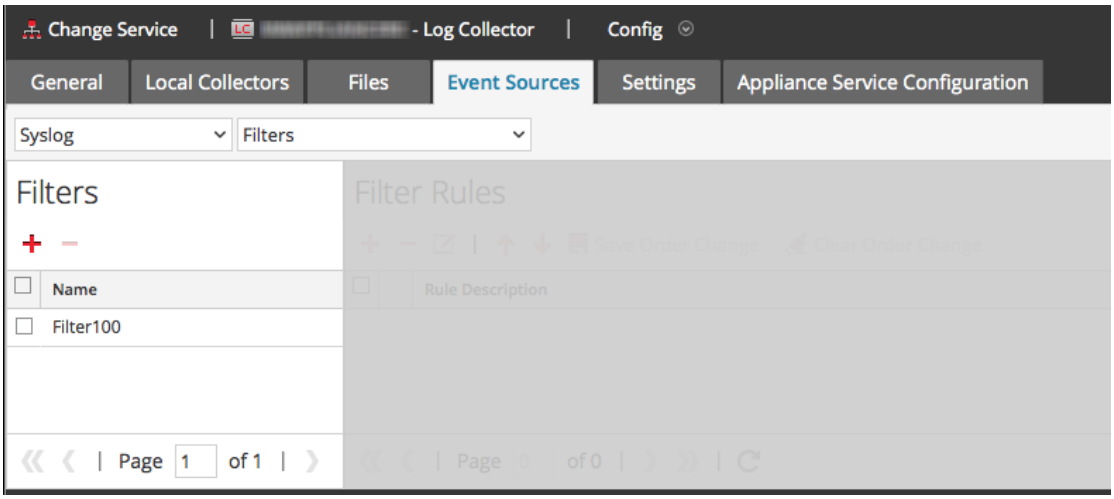
6. Dans la barre d'outils du panneau **Filtres**, cliquez sur +.

   La boîte de dialogue **Ajouter un filtre** s'affiche.



7. Saisissez un nom et une description pour le nouveau filtre et cliquez sur **Ajouter**.

   Le nouveau filtre s'affiche dans le panneau **Filtre**.

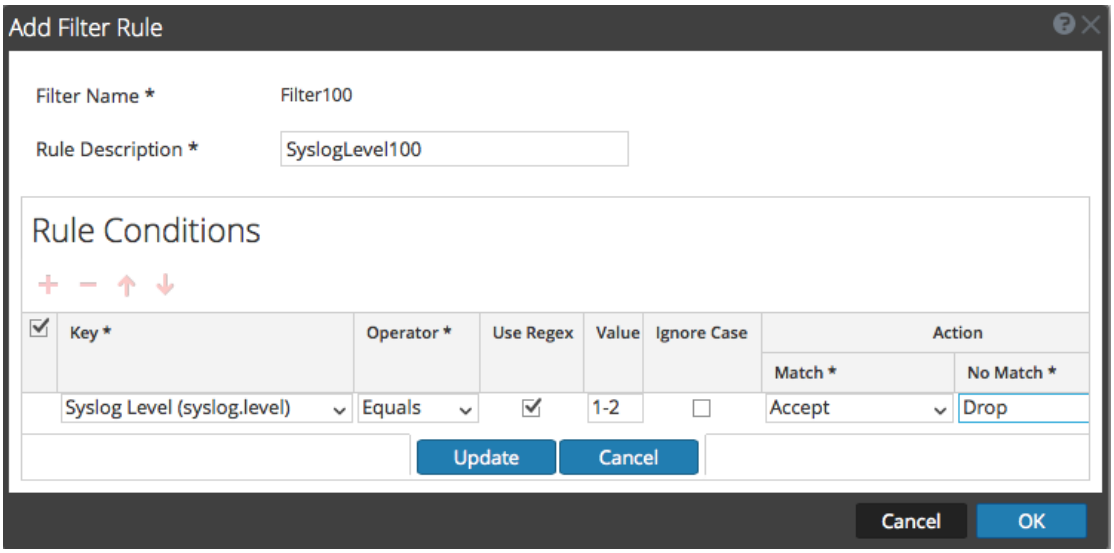


8. Sélectionnez le nouveau filtre dans le panneau **Filtres** et cliquez sur + dans la barre d'outils du panneau **Règles de filtrage**.

   La boîte de dialogue **Ajouter une règle de filtrage** s'affiche.

9. Cliquez sur + sous **Conditions de la règle**.

10. Ajoutez les paramètres pour cette règle et cliquez sur **Mettre à jour > OK**.



NetWitness Suite met à jour le filtre avec la règle que vous avez définie.

Remarque : Les règles sont traitées dans l'ordre du haut vers le bas jusqu'à ce qu'un type d'action abandonne le traitement ou que la règle finale soit vérifiée. Le comportement par défaut est d'accepter la règle si aucune correspondance n'est trouvée.

Les tableaux suivants décrivent les paramètres pour ajouter une règle de filtre.

Paramètre « Clé » d'une règle de filtre d'événement

Les valeurs du champ Clé dépendent de la méthode de collecte à laquelle s'applique le filtre.

Méthode de collecte	Valeurs pour le champ *Clé*
Checkpoint, fichiers, Netflow, Plug-in, SDEE SNMP et VMware	• Tous les champs de données • Type de source d'événement • Nom de la source d'événement • IP source • Événement brut
ODBC	• Tous les champs de données • Type de source d'événement • Nom de la source d'événement • IP source • ID de message • Niveau de message
Syslog	• Tous les champs de données • Type de source d'événement • Nom de la source d'événement • IP source • Niveau Syslog • Événement brut

Méthode de collecte	Valeurs pour le champ *Clé*
Windows	• Tous les champs de données • Type de source d'événement • Nom de la source d'événement • IP source • ID d'événement • Fournisseur • Canal • Ordinateur • UserName • DomainName
Windows d'ancienne génération	• Tous les champs de données • Type de source d'événement • Nom de la source d'événements • IP source • ID d'événement

Autres paramètres de règle de filtre d'événement

Le tableau suivant décrit tous les autres champs disponibles pour créer une règle de filtre d'événement.

Champ	Description
Opérateur	Les valeurs autorisées sont les suivantes : • Contenu • Égal à
Utiliser Regex	Facultatif. Vous pouvez utiliser cette valeur si vous souhaitez utiliser une expression régulière (regex).

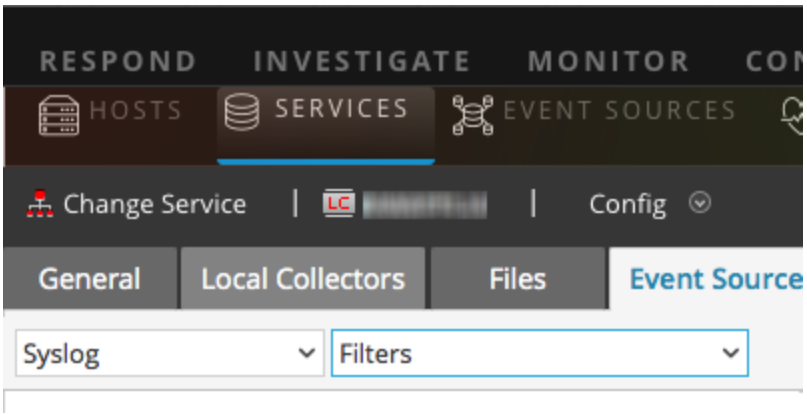
Champ	Description
Valeur	La valeur dépend de la valeur de clé que vous avez sélectionnée. Par exemple, si vous choisissez **Niveau Syslog** en tant que clé, la valeur correspondra à un nombre qui désigne le niveau Syslog.
Ignorer la casse	Facultatif. Sélectionnez cette option pour ignorer le respect de la casse.
Action	En cas de correspondance, vous pouvez choisir une action de type acceptation, refus, condition suivante ou règle suivante : • **Acceptation** : les événements qui correspondent à l'ID fournis sont inclus dans les logs d'événements et s'affichent dans l'interface utilisateur Systems Analytics. • **Refus** : les événements qui correspondent à l'ID fournis ne sont pas inclus dans les logs d'événements et ne s'affichent pas dans l'interface utilisateur. • **Condition suivante** : le filtre ignore les événements aux ID correspondants et passe à la condition de règle suivante. • **Règle suivante** : le filtre ignore les événements aux ID correspondants et passe à la règle suivante. En cas de non-correspondance, vous pouvez choisir une action de type acceptation, refus, condition suivante ou règle suivante.

Modifier les règles de filtrage

Pour modifier une source d'événement :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez **Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.
5. Sous l'onglet **Sources d'événements**, sélectionnez une méthode de collecte/**Filtre** dans les menus déroulants.

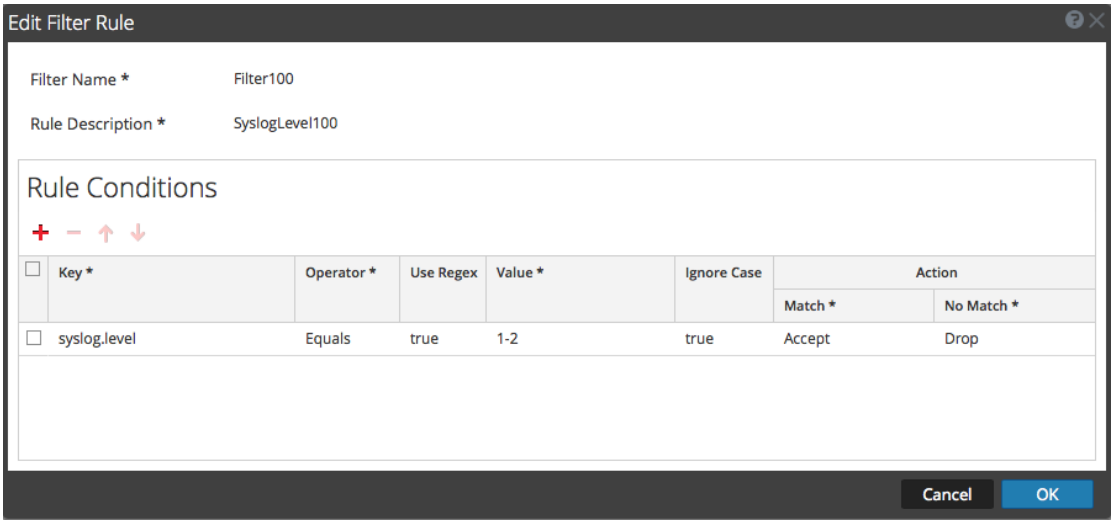
   L'écran suivant affiche **Check Point** sélectionné.



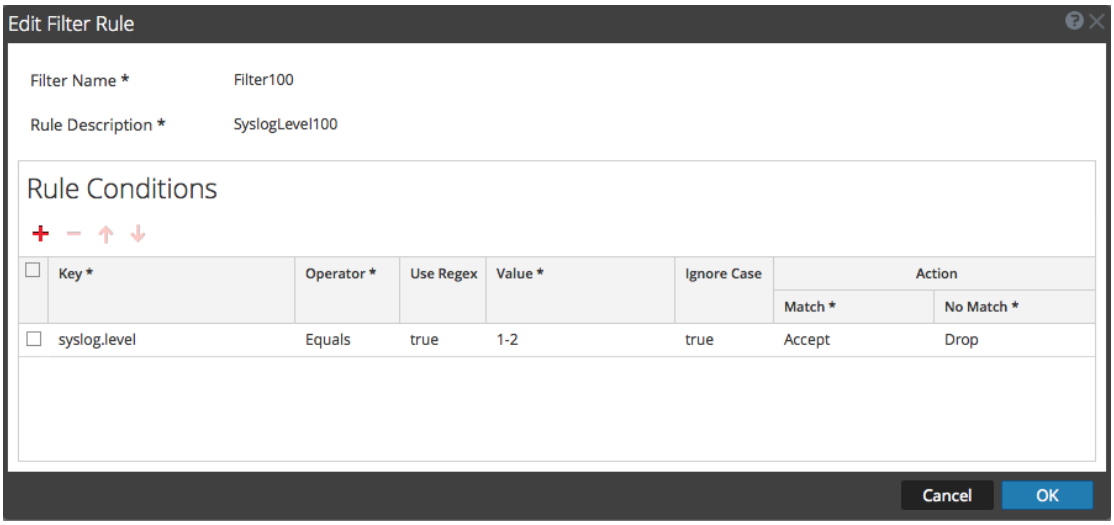
La vue **Filtres** affiche les filtres configurés pour la méthode de collecte sélectionnée, le cas échéant.

6. Dans la liste **Règles de filtrage**, sélectionnez une règle et cliquez sur .

   La boîte de dialogue **Modifier la règle de filtrage** s'affiche.



7. Sélectionnez la condition de règle à modifier.



8. Modifiez les paramètres de condition nécessaires, puis cliquez sur **Mettre à jour> OK**.

NetWitness Suite applique les modifications des paramètres de condition à la règle de filtre sélectionnée.

Importer, exporter, modifier et tester des sources d'événements en bloc

Cette rubrique vous indique comment importer, exporter, modifier et tester des sources d'événements en bloc.

Vous pouvez utiliser l'option d'exportation en bloc pour exporter les détails des sources d'événements de votre configuration actuelle et les stocker. Ces données peuvent être importées en bloc lorsque vous rencontrez un problème avec votre configuration actuelle et que vous avez besoin des données des sources d'événements disponibles.

Vous pouvez utiliser la fonction de modification en bloc lorsque vous avez plusieurs sources d'événements qui requièrent une modification spécifique. Vous pouvez sélectionner toutes les sources et leur appliquer l'option de modification en une seule fois et ainsi éviter d'appliquer la modification à chaque source une par une.

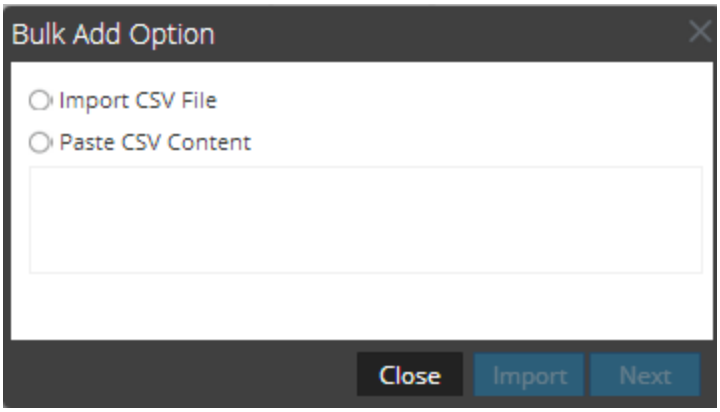
Importer des sources d'événements en bloc

Avertissement : Lorsque vous utilisez un tableur pour modifier un fichier CSV de source événement exporté, certains champs de données comme les numéros et les dates peuvent être reformatés dans des types de champ natif du tableur. Cela peut entraîner des problèmes lors de l'importation de cette information, car certains champs de données peuvent être tronqués ou incorrectement formatés. Cela peut être évité en important le fichier CSV dans le tableur et en spécifiant tous les champs de données en tant que valeurs de texte.

Pour importer plusieurs sources d'événements simultanément :

1. Accédez à **Admin > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.
5. Sélectionnez **Check Point**, **Fichier**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **(Syslog pour les Remote Collectors uniquement)**, **VMware**, **Windows**, ou **Windows d'ancienne génération** (SNMP ne dispose pas d'une fonction d'importation).
6. Dans la barre d'outils du volet **Sources** , cliquez sur **Importer la source**.

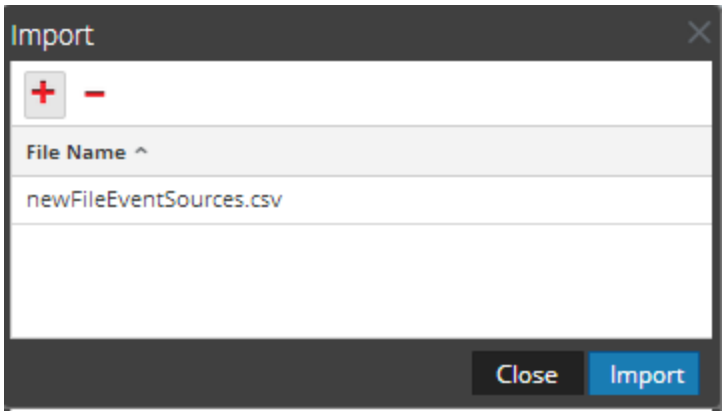
   La boîte de dialogue **Option d'ajout en bloc** s'affiche.



7. Sélectionnez **Importer le fichier CSV** ou **Coller le contenu CSV**. Si vous sélectionnez :
   - Importer le fichier CSV :
     a. Cliquez sur Suivant.

        La boîte de dialogue **Importer** s'affiche.

     b. Cliquez sur **Ajouter**, puis sélectionnez un fichier **.csv** à partir de votre réseau.

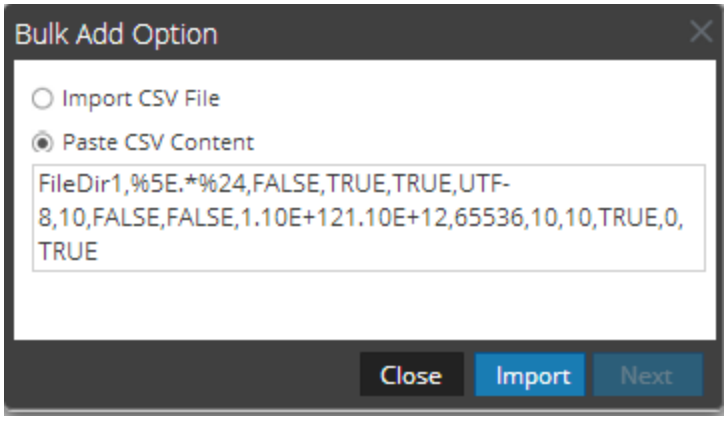


c. Cliquez sur **Importer**.

Les sources d'événements sont ajoutées à la liste **Sources d'événements**.

- Coller le contenu CSV :

a. Copiez le contenu du fichier **.csv** et collez-le dans la boîte de dialogue.



b. Cliquez sur **Importer**.

Les sources d'événements sont ajoutées à la liste **Sources d'événements**.

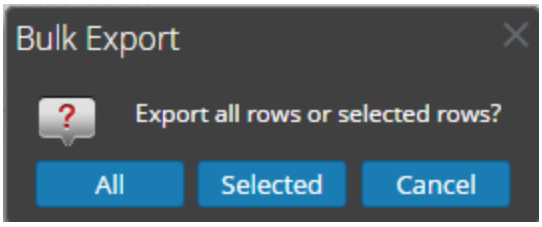
Exporter des sources d'événements en bloc

Avertissement : Lorsque vous utilisez un tableur pour modifier un fichier CSV de source événement exporté, certains champs de données comme les numéros et les dates peuvent être reformatés dans des types de champ natif du tableur. Cela peut entraîner des problèmes lors de l'importation de cette information, car certains champs de données peuvent être tronqués ou incorrectement formatés. Cela peut être évité en important le fichier CSV dans le tableur et en spécifiant tous les champs de données en tant que valeurs de texte.

1. Accédez à **Admin > Services**.
2. Sélectionnez un service de collecte de logs.

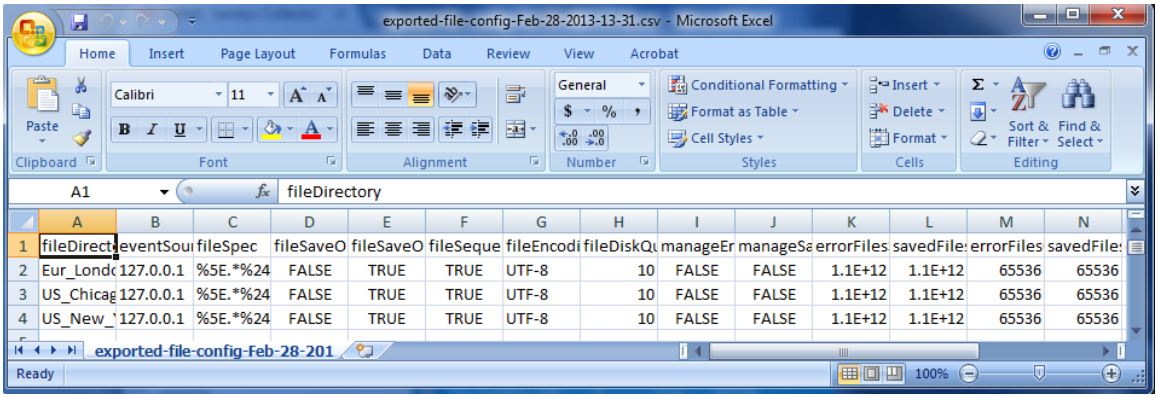
3. Sous Actions, puis sélectionnez  > **Vue** > **Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.
5. Sélectionnez **Check Point**, **Fichier**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **(Syslog pour les Remote Collectors uniquement)**, **VMware**, **Windows**, ou **Windows d'ancienne génération** (SNMP ne dispose pas d'une fonction d'exportation).
6. Dans le volet **Sources**, sélectionnez une ou plusieurs sources d'événements, puis cliquez sur **Exporter la source**.

   La boîte de dialogue **Exporter en bloc** s'affiche.



7. Selon votre sélection :
   - **Tout**, NetWitness Suite exporte toutes les sources d'événements dans un fichier CSV horodaté.
   - **Sélection**, NetWitness Suite exporte la ou les sources d'événements que vous avez sélectionnées dans un fichier CSV horodaté.
   - **Annuler**, NetWitness Suite annule l'exportation.

   Voici un exemple d'un fichier CSV horodaté qui est créé avec les sources d'événements que vous avez sélectionnées dans la liste.

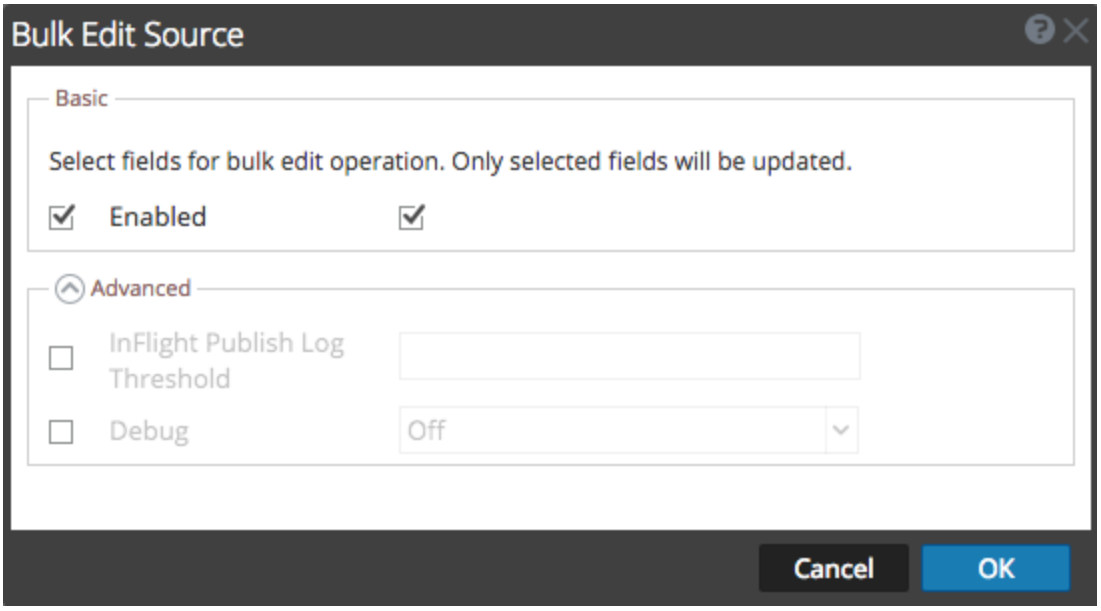


Modifier des sources d'événements en bloc

Pour modifier plusieurs sources d'événements simultanément :

1. Sous l'onglet **Sources d'événements Log Collector**, sélectionnez **Check Point**, **Fichier**, **Netflow**, **ODBC**, **Plug-ins**, **SDEE**, **Syslog**, **VMware**, **Windows** ou **Windows d'ancienne génération** (SNMP ne dispose pas de la fonction Modifier).
2. Dans le panneau **Sources**, sélectionnez plusieurs sources d'événements, puis cliquez sur (icône Modifier).

   La boîte de dialogue **Modifier en bloc** correspondant à la source d'événement s'affiche. La figure suivante illustre la boîte de dialogue **Modifier la source en bloc** en tant que paramètres des sources d'événements Fichiers.



3. Activez la case à cocher située à gauche des champs que vous souhaitez modifier (par exemple, **Debug**).
4. Modifiez les paramètres sélectionnés (par exemple, passez Debug de l'état **Off** à l'état **On**).
5. Cliquez sur **OK**.

   NetWitness Suite applique les mêmes modifications de valeurs de paramètres à toutes les sources d'événements sélectionnées.

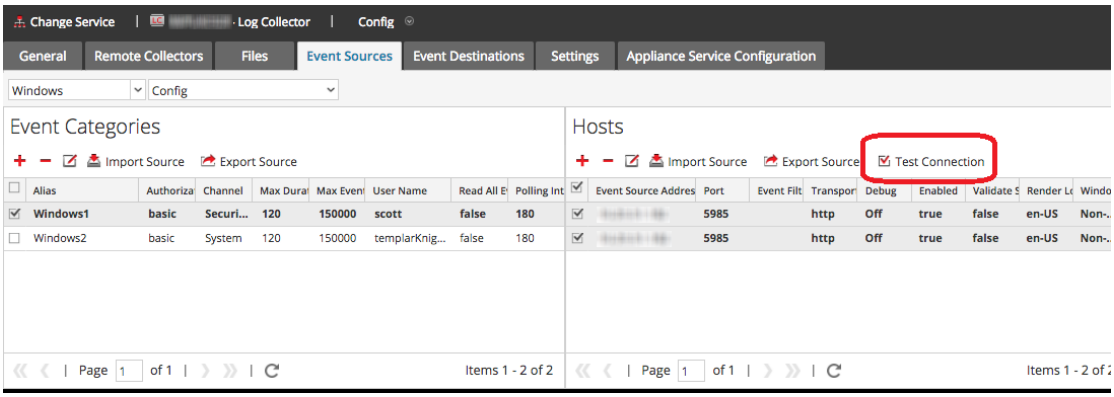
Tester des connexions de sources d'événements en bloc

Pour tester plusieurs connexions de sources d'événements simultanément :

1. Accédez à **Administrateur > Services**.
2. Dans la grille **Services**, sélectionnez un service **Log Collector**.
3. Sous Actions, sélectionnez **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

4. Sélectionnez l'onglet **Sources d'événements**, puis **Plug-ins**, **ODBC**, ou **Windows** (les autres protocoles ne disposent d'aucune fonction de connexion de tests en bloc).
5. Sélectionnez au moins :
   - une source dans le panneau **Sources** pour **Plug-ins** ou **ODBC** ;
   - hôtes à partir du panneau **Hôtes** pour **Windows**

   Le bouton **Tester la connexion** est activé.



6. Cliquez sur Test Connection .

   La boîte de dialogue **Connexions de tests en bloc** qui est affichée indique l'état actuel du test pour chaque source, à savoir en attente, en cours, réussi ou échoué.

   Si vous choisissez d'arrêter le test avant la fin, celui-ci s'arrête et la boîte de dialogue **Connexions de tests en bloc** se ferme.

Une fois le test terminé, les résultats s'affichent dans la boîte de dialogue **Connexions de tests en bloc**.

Voir aussi

Vous pouvez utiliser le module **Sources d'événements** (Administration > Sources d'événements) pour créer des groupes de sources d'événements, généralement importés à partir de CMBD et pour surveiller des sources d'événements basées sur ces groupes. Pour plus d'informations, reportez-vous aux rubriques suivantes dans le *Guide de gestion de la source d'événement* :

- Importer des sources d'événements
- Exporter des sources d'événements
- Modification en bloc de la source d'événement

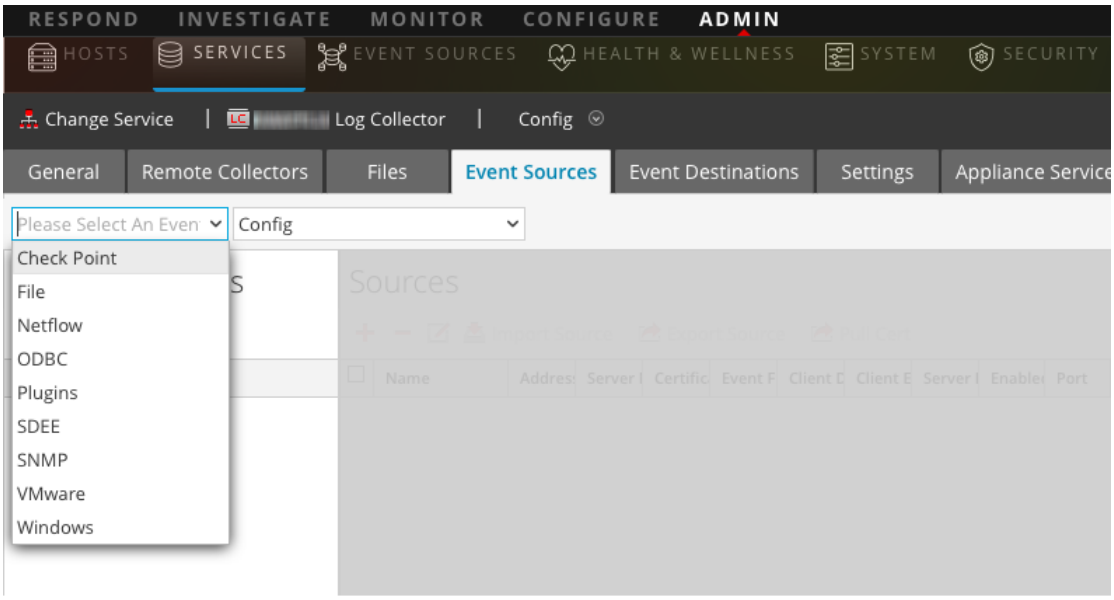
Configurer des protocoles de collecte et des sources d'événements

Cette rubrique vous indique comment configurer des protocoles de collecte et des sources d'événements à l'aide de ces protocoles.

Vous configurez le Log Collector pour collecter des données d'événement à partir de vos sources d'événements sous l'onglet Sources d'événements de la vue des paramètres de la collecte de logs.

Pour configurer un protocole de collecte :

1. Accédez à **ADMIN> Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sélectionnez un protocole de collecte (par exemple, **Fichier**) et sélectionnez **Configuration**.
6. Cliquez sur + et sélectionnez une source d'événement.
7. Sélectionnez la catégorie nouvelle ajoutée, puis cliquez sur +.
8. Spécifiez les paramètres pour la source d'événement. Pour plus d'informations, consultez les rubriques de protocole de collecte individuel.

Les guides ci-dessous fournissent des instructions détaillées sur la configuration des protocoles de collecte et sur leurs sources d'événements associées dans NetWitness Suite. Chaque guide comprend un index pour les instructions de configuration concernant les sources d'événements prises en charge pour ce protocole de collection.

Pour configurer des protocoles de collecte individuels, consultez les rubriques suivantes :

- Configurer des sources d'événements AWS (CloudTrail) dans NetWitness Suite
- Configurer des Sources d'événements Azure dans NetWitness Suite
- Configurer des sources d'événement Check Point dans NetWitness Suite
- Configurer des sources d'événements de fichiers dans NetWitness Suite
- Configurer des sources d'événements Netflow dans NetWitness Suite
- Configurer des sources d'événements ODBC dans NetWitness Suite
  - Configurer des noms de sources de données (DSN)
  - Créer un fichier typespec personnalisé pour la collecte ODBC
  - Paramètres de configuration des sources d'événements ODBC
  - Paramètres de configuration des sources d'événements liées aux DSN ODBC
- Configurer des sources d'événements SDEE dans NetWitness Suite
- Configurer des sources d'événements SNMP dans NetWitness Suite
- Configurer des sources d'événements Syslog pour le collecteur distant
- Configurer des sources d'événement VMware dans NetWitness Suite
- Configurer des sources d'événement Windows dans NetWitness Suite
- Guide de configuration de la collecte Windows d'ancienne génération et NetApp
  - Configurer la collecte Windows d'ancienne génération
  - Configurer des sources d'événements Windows d'ancienne génération et NetApp
  - Dépannage de la collecte Windows d'ancienne génération et NetApp

Configurer des sources d'événements AWS (CloudTrail) dans NetWitness Suite

Cette rubrique vous indique comment configurer le protocole de collecte AWS qui permet de collecter les événements d'Amazon Web Services (AWS) CloudTrail.

Remarque : Le plug-in AWS est destiné uniquement pour la collecte des logs AWS CloudTrail et non pour la collecte des logs arbitraires dans les buckets S3 (sous les répertoires arbitraires). Les logs AWS CloudTrail sont envoyés au format JSON, comme indiqué dans la documentation AWS ici : http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html.

Fonctionnement de la collecte AWS

Le service Log Collector collecte des événements à partir d'Amazon Web Services (AWS) CloudTrail. CloudTrail enregistre les appels API AWS pour un compte. Les événements renferment l'identité de l'appelant API, l'heure de l'appel, l'adresse IP de la source de l'appelant API, les paramètres de demande, et les éléments de réponse renvoyés par le service AWS. L'historique des appels API AWS fourni par les événements CloudTrail vous permet d'analyser la sécurité, de faire le suivi des modifications de ressources et de vérifier la conformité. CloudTrail utilise Amazon S3 pour le stockage de fichiers log et la livraison. NetWitness Suite copie les fichiers log à partir du cloud (bucket S3) et envoie les événements contenus dans les fichiers à Log Collector.

Scénario de déploiement

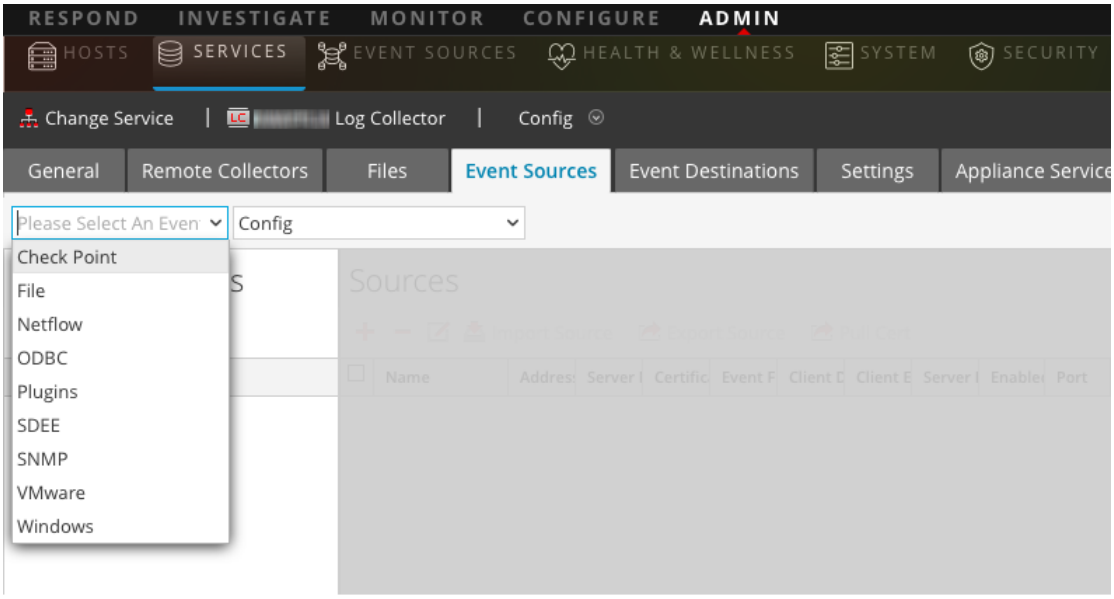
La figure suivante illustre comment déployer le protocole de collecte AWS dans NetWitness Suite.

Configuration

Pour configurer une source d'événements AWS (CloudTrail) :

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **Plug-ins/Config** dans le menu déroulant.
6. Dans la barre d'outils du panneau **Catégories d'événements** , cliquez sur +.

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.
7. Sélectionnez **cloudtrail**, puis cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.
8. Sélectionnez le nouveau type dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils **Sources**.

   La boîte de dialogue **Ajouter une source** s'affiche.
9. Définissez des valeurs de paramètre. Pour plus d'informations, reportez-vous à la section Paramètres AWS ci-dessous.
10. Cliquez sur **Tester la connexion**.

    Le résultat du test s'affiche dans la boîte de dialogue. Si le test échoue, modifiez les informations de l'appareil ou du service et réessayez.

    Le Log Collector prend environ 60 secondes pour renvoyer les résultats du test. Au-delà de ce délai, le test expire et NetWitness Suite affiche un message d'erreur.
11. Si le test aboutit, cliquez sur **OK**.

    La nouvelle source d'événement s'affiche dans le panneau **Sources**.

Paramètres AWS

Le tableau ci-dessous décrit les paramètres de configuration disponibles pour la collecte AWS.

Paramètre	Description
Paramètre	**Description**
	Basique
Nom *	Nom de la source d'événement.
Activé 	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
ID de compte *	Code d'identification de compte du Bucket S3

Paramètre	Description
Nom de compartiment S3 *	Nom de compartiment S3 AWS (CloudTrail). Les noms de Buckets S3 Amazon sont globalement uniques, quelle que soit la région AWS (CloudTrail) dans laquelle vous créez le bucket. Vous spécifiez le nom au moment de la création du bucket. Les noms de buckets doivent se conformer aux conventions de dénomination DNS. Les règles pour les noms de bucket compatibles DNS sont les suivantes : • Les noms de bucket doivent comprendre entre 3 et 63 caractères. • Les noms de bucket doivent être une série d'un ou de plusieurs libellés. Les libellés adjacents sont séparés par un seul point « . ». Les noms de buckets contiennent des lettres minuscules, des chiffres et des tirets. Chaque libellé doit commencer et se terminer par une lettre minuscule ou un chiffre. • Les noms de buckets ne doivent pas être formatés comme une adresse IP (par exemple, 192.168.5.4). Les exemples suivants sont des noms de buckets **valides** : • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** Les exemples suivants sont des noms de buckets **non valides** : • **.myawsbucket** - Un nom de bucket ne doit pas commencer par un point « . ». • **myawsbucket.** - Ne pas terminer un nom de bucket par un point « . ». • **my..examplebucket** - N'utilisez qu'un seul point entre les libellés.
Clé d'accès *	Clé utilisée pour accéder au bucket S3. Les clés d'accès sont utilisées pour garantir la sécurité de requêtes de protocole REST ou Requête sur n'importe quelle API de service AWS. Veuillez vous reporter à Gérer les informations d'identification sur le site de support Amazon Web Services pour plus d'informations sur les clés d'accès.
Clé secrète *	Clé secrète utilisée pour accéder au bucket S3.
Région *	Région du bucket S3. **us-east-1** est la valeur par défaut.

Paramètre	Description
Point de terminaison de la région	Spécifie le nom d'hôte CloudTrail AWS. Par exemple, pour un Cloud public AWS pour la région us-east, le point de terminaison de la région serait s3.amazonaws.com. Pour plus d'informations , vous référez à http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. Ce paramètre est nécessaire pour collecter les logs de CloudTrail à partir de Clouds AWS administratifs ou privés.
Utiliser le proxy	Activer **Utiliser le proxy** pour définir le proxy du serveur AWS. Il est désactivé par défaut,.
Serveur proxy	Saisissez le nom de proxy que vous souhaitez connecter pour accéder au serveur AWS.
Port proxy	Saisissez le numéro de port qui se connecte au serveur proxy pour accéder à serveur AWS.
Utilisateur proxy	Saisissez le nom d'utilisateur permettant de s'authentifier auprès du serveur proxy.
Mot de passe du proxy	Saisissez le mot de passe permettant de s'authentifier auprès du port proxy.
Date de début *	Démarre la collecte AWS (CloudTrail) depuis le nombre de jours spécifié dans le passé, mesuré à partir de l'horodatage actuel. La valeur par défaut est 0, ce qui démarre à partir d'aujourd'hui. La valeur est comprise entre 0 et 89 jours.
Préfixe de fichier log	Le préfixe des fichiers à traiter. **Remarque :** Si vous définissez un préfixe lorsque vous configurez votre service CloudTrail, assurez-vous de saisir le même préfixe dans ce paramètre.
Avancé	

Paramètre	Description
Débogage	**Attention :** n'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).
Arguments de commande	Arguments ajoutés au script.
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est 60. Par exemple, si vous spécifiez 60, le collecteur planifie une interrogation de la source d'événement toutes les 60 secondes. Si le cycle d'interrogation précédent est toujours en cours, il est nécessaire d'attendre qu'il se termine. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 60 secondes avant de démarrer car les threads sont occupés.
SSL activé 	Cochez la case permettant de communiquer en utilisant SSL. La sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL. Cette case à cocher est activée par défaut.

Paramètre	Description
Tester la connexion	Valide que les paramètres de configuration spécifiés dans cette boîte de dialogue sont corrects. Par exemple, ce test valide les points suivants : • NetWitness peut se connecter au Bucket S3 dans AWS en utilisant les informations d'identification spécifiées dans cette boîte de dialogue. • NetWitness peut télécharger un fichier log depuis le bucket (la connexion test échouera s'il n'y a pas de fichiers logs pour l'ensemble du bucket, mais cela est extrêmement improbable).
Annuler	Ferme la boîte de dialogue sans ajouter l'AWS (CloudTrail).
OK	Ajoute les valeurs de paramétrage actuelles en tant que nouvel AWS (CloudTrail).

Configurer des Sources d'événements Azure dans NetWitness Suite

Ce guide indique comment configurer le protocole de collecte Azure. Microsoft Azure est une plate-forme et une infrastructure de Cloud computing permettant la conception, le déploiement et la gestion des applications et services via un réseau global de datacenters gérés par Microsoft.

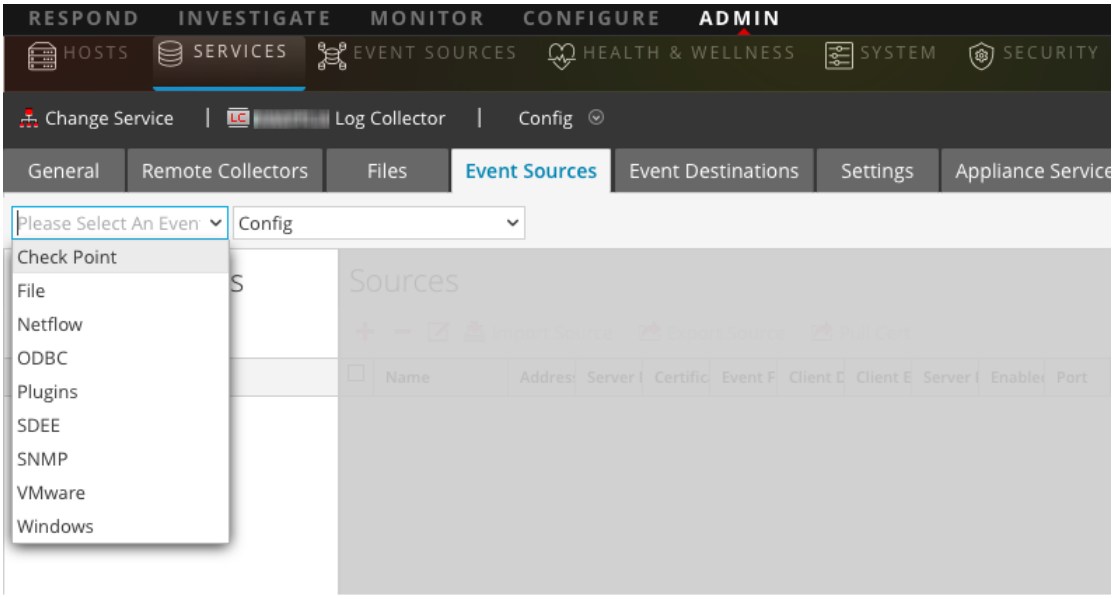
Configuration dans NetWitness Suite

Pour en savoir plus sur la configuration d'Azure comme source d'événement, reportez-vous au Guide de configuration des sources d'événements Azure, disponible sur RSA Link.

Pour configurer une source d'événements Azure :

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **Plug-ins/Config** dans le menu déroulant.
6. Dans la barre d'outils du panneau **Catégories d'événements** , cliquez sur +.

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.
7. Sélectionnez **azureaudit**, puis cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.
8. Sélectionnez le nouveau type dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils **Sources**.

   La boîte de dialogue **Ajouter une source** s'affiche.
9. Définir des valeurs de paramètre Pour plus d'informations, reportez-vous à la section Paramètres Azure ci-dessous.
10. Cliquez sur **Tester la connexion**.

    Le résultat du test s'affiche dans la boîte de dialogue. Si le test échoue, modifiez les informations de l'appareil ou du service et réessayez.

    Log Collector prend environ 60 secondes pour renvoyer les résultats du test. Au-delà de ce délai, le test expire et NetWitness Suite affiche un message d'erreur.
11. Si le test aboutit, cliquez sur **OK**.

    La nouvelle source d'événement s'affiche dans le panneau **Sources**.

Paramètres Azure

Cette section décrit les paramètres de configuration des sources d'événements Azure.

Remarque : Les éléments suivis d'un astérisque (*) sont obligatoires.

Paramètres de base

Nom	Description
Nom *	Saisissez un nom descriptif, alphanumérique pour la source. Cette valeur est uniquement utilisée pour afficher le nom sur cet écran.
Activé	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
ID client *	L'ID client se trouve dans l'onglet Configurer les applications Azure. Faites défiler vers le bas jusqu'à ce qu'il s'affiche.
Code secret client *	Lorsque de la configuration de la source d'événement, le code secret du client s'affiche lorsque vous créez une clé et que vous sélectionnez une durée de validation. Veillez à bien l'enregistrer, car cette information ne sera affichée qu'une seule fois et ne peut pas être récupérée ultérieurement.
URL de base des ressources API *	Saisissez `https://management.azure.com/`. Veillez à inclure la barre oblique de fin (/).
Point de terminaison des métadonnées de fédération *	Dans votre application Azure, cliquez sur le bouton **Afficher les points de terminaison** (au bas du volet). Un grand nombre de liens commencent tous par la même chaîne. Comparez les URL et identifiez la chaîne commune par laquelle commence la plupart d'entre eux. Cette chaîne commune est le point de terminaison que vous devez saisir ici.
ID d'abonnement *	Vous pouvez le trouver dans le tableau de bord Microsoft Azure : cliquez sur Abonnements au bas de la liste sur la gauche.
Domaine du tenant *	Accédez à Active Directory, puis cliquez sur le répertoire. Dans l'URL, le domaine du tenant est la chaîne qui suit directement **manage.windowsazure.com/**. Le domaine du tenant est la chaîne allant jusqu'à **.com**, inclus.
Noms des groupes de ressources *	Dans Azure, sélectionnez Groupes de ressources dans le volet de navigation de gauche, puis sélectionnez votre groupe.

Nom	Description
Date de début *	Choisissez la date du début de la collecte. La date du jour est définie par défaut.
Tester la connexion	Vérifiez les paramètres de configuration spécifiés dans cette boîte de dialogue pour vous assurer qu'ils sont corrects.

Paramètres avancés

Cliquez sur à côté d'**Avancé** pour afficher et modifier les paramètres avancés, si nécessaire.

Nom	Description
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est **180**. Par exemple, si vous spécifiez 180, le collecteur planifie une interrogation de la source d'événement toutes les 180 secondes. Si le cycle d'interrogation précédent est toujours en cours, le collecteur attend la fin de l'opération. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 180 secondes avant de démarrer, car les threads sont occupés.
Nb max. d'interrogations de durées	Durée maximale, en secondes, d'un cycle d'interrogation. La valeur zéro indique aucune limite.
Nb max. d'interrogations d'événements	Nombre maximal d'événements par cycle d'interrogation (nombre d'événements collectés par cycle d'interrogation).
Nb max. d'interrogations liées au délai de mise en veille	Durée maximale, en secondes, d'un cycle d'interrogation. La valeur zéro indique aucune limite.
Arguments de commande	Arguments facultatifs à ajouter à l'appel de script.

Nom	Description
Débogage	**Attention :** n'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. **Attention :** Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire). La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances.

Configurer des sources d'événement Check Point dans NetWitness Suite

Cette rubrique vous indique comment configurer le protocole de collecte Check Point qui permet de collecter les événements de sources d'événements Check Point.

Ce protocole collecte des événements issus des sources d'événements Check Point à l'aide d'une interface OPSEC LEA. OPSEC LEA est l'API Check Point Operations Security Log Export qui facilite l'extraction des fichiers log.

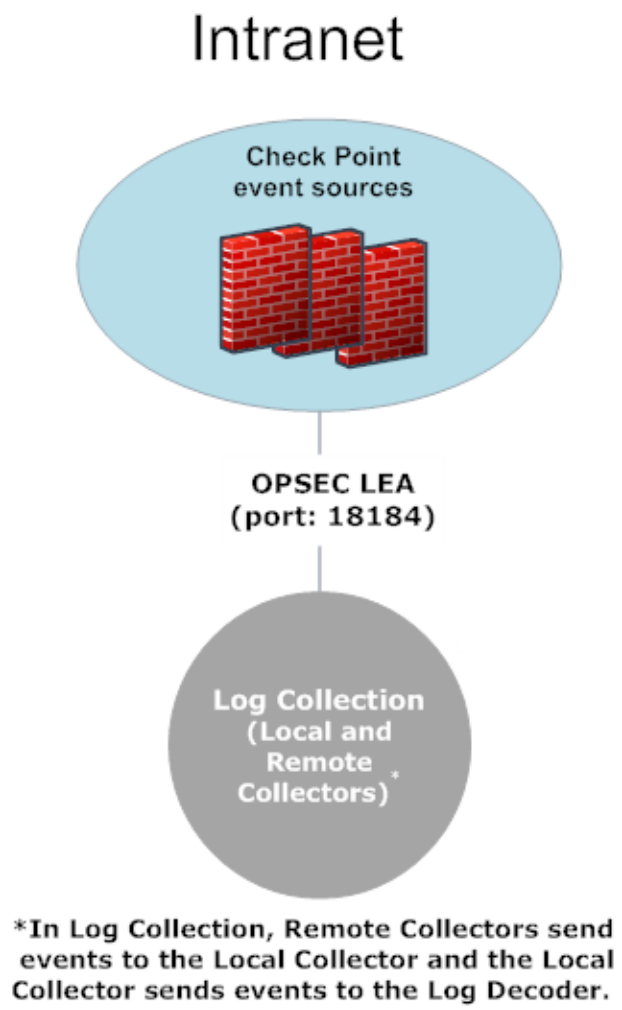
Mode de fonctionnement de la collecte Check Point

Le service Log Collector collecte des événements issus des sources d'événements Check Point à l'aide d'une interface OPSEC LEA. OPSEC LEA est l'API Check Point Operations Security Log Export qui facilite l'extraction des fichiers log.

Remarque : L'interface OPSEC LEA (API Log Export) prend en charge l'extraction des fichiers log à partir de sources d'événements Check Point configurés avec un certificat SHA-256 ou SHA-1.

Scénario de déploiement

La figure suivante illustre le déploiement du protocole de collecte Check Point dans NetWitness Suite.

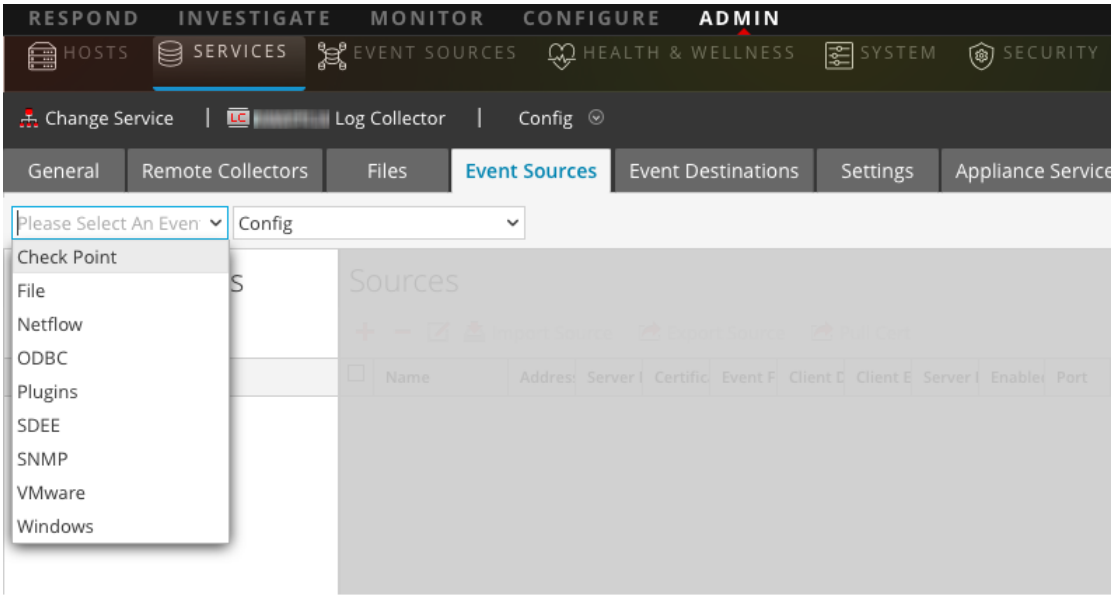


Configuration dans NetWitness Suite

Pour configurer une source d'événement Check Point

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **Check Point/Config** dans le menu déroulant.

6. Dans la barre d'outils du panneau **Catégories d'événements**, cliquez sur + .

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.

7. Sélectionnez un type de source d'événement Check Point et cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.

8. Sélectionnez le nouveau type dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils **Sources**.

   La boîte de dialogue **Ajouter une source** s'affiche.

9. Définissez des valeurs de paramètre. Pour plus d'informations, reportez-vous à la section Paramètres Check Point ci-dessous.

10. Cliquez sur **Tester la connexion**.

    Le résultat du test s'affiche dans la boîte de dialogue. Si le test échoue, modifiez les informations de l'appareil ou du service et réessayez.

    Log Collector prend environ 60 secondes pour renvoyer les résultats du test. Au-delà de ce délai, le test expire et NetWitness Suite affiche un message d'erreur.

11. Si le test aboutit, cliquez sur **OK**.

    La nouvelle source d'événement s'affiche dans le panneau **Sources**.

Paramètres Check Point

Cette section décrit les paramètres de configuration des sources d'événements Check Point.

Paramètres de base

Paramètre	Description
Nom*	Nom de la source d'événement.
Adresse*	Adresse IP du serveur Check Point.
Nom du serveur*	Nom du serveur Check Point.
Nom du certificat	Nom du certificat des connexions sécurité à utiliser lorsque le mode de transport est de type https. S'il est configuré, le certificat doit être présent dans le magasin de certificats de confiance que vous avez créé via l'onglet Paramètres. Sélectionnez un certificat dans la liste déroulante. La convention de dénomination des fichiers pour les certificats de source d'événements Check Point est **checkpoint_*nom-de-la-source-d'événement***.
Client unique	Saisissez le nom unique du client sur le serveur Check Point.
Nom d'entité de client	Saisissez le nom d'entité de client sur le serveur Check Point.
Serveur unique	Saisissez le nom unique du serveur sur le serveur Check Point.
Activé	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
Extraire le certificat	Cochez la case permettant d'extraire un certificat pour la première fois. L'extraction d'un certificat le rend disponible auprès du magasin de certificats de confiance.
Adresse du serveur de certificat	Adresse IP du serveur sur lequel réside le certificat. Par défaut, l'adresse de la source d'événement.

Paramètre	Description
Mot de passe	Actif uniquement lorsque vous cochez la case Extraire le certificat pour la première fois. Mot de passe requis pour extraire le certificat. Le mot de passe est la clé d'activation créée lors de l'ajout d'une application OPSEC à Check Point sur le serveur Check Point.

Déterminer les valeurs des paramètres avancés pour la collecte Check Point

Vous utilisez moins de ressources système lorsque vous configurez une connexion de source d'événements Check Point afin qu'elle reste ouverte pendant une période spécifique et un volume d'événement spécifique (connexion transitoire). RSA NetWitness Suite utilise les paramètres de connexion par défaut suivants pour établir une connexion transitoire :

- Intervalle d'interrogation = **180** (3 minutes)
- Nb max. d'interrogations de durées = **120** (2 minutes)
- Nb max. d'interrogations d'événements = **5 000** (5 000 événements par intervalle d'interrogation)
- Nb max. d'interrogations liées au délai de mise en veille = **0**

Pour les sources d'événements Check Point très actives, nous vous recommandons de configurer une connexion qui reste ouverte jusqu'à ce que vous l'arrêtiez (connexion permanente). Cela garantit que la collecte Check Point maintient le rythme des événements générés par ces sources d'événements actives. La connexion permanente évite les délais de redémarrage et de connexion et empêche que la collecte Check Point soit retardée par la génération d'événements.

Pour établir une connexion permanente pour une source d'événements Check Point, définissez les paramètres de valeurs suivants :

- Intervalle d'interrogation = **-1**
- Nb max. d'interrogations de durées = **0**
- Nb max. d'interrogations d'événements = **0**
- Nb max. d'interrogations liées au délai de mise en veille = **0**

Paramètre	Description
Port	Port du serveur Check Point auquel Log Collector se connecte. La valeur par défaut est 18184.

Paramètre	Description
Type de log de collecte	Type de logs que vous souhaitez collecter. Les valeurs autorisées sont les suivantes : • **Audit** - collecte les événements d'audit. • **Sécurité** - collecte les événements de sécurité. Si vous souhaitez collecter à la fois les événements d'audit et de sécurité, vous devez créer une source d'événements dupliquée. À titre d'exemple, vous créez d'abord une source d'événements avec l'option Audit sélectionnée afin d'extraire un certificat dans le magasin de certificats de confiance pour cette source d'événements. Ensuite, vous créez une autre source d'événements avec les mêmes valeurs, sauf que vous sélectionnez Sécurité comme Type de log de collecte et vous choisissez le même certificat dans le Nom du certificat que celui extrait lors de la configuration des premiers paramètres pour cette source d'événements, et vous vous assurez que Extraire le certificat n'est pas sélectionné.
Collecter les logs de	Lorsque vous configurez une source d'événements Check Point, NetWitness collecte les événements à partir du fichier de log actuel. Les valeurs autorisées sont les suivantes : • **Maintenant** - démarre la collecte des logs maintenant (à un point donné dans le fichier log actuel). • **Début du log** - collecte les logs depuis le début du fichier log actuel. Si vous choisissez « Début du log » pour cette valeur de paramètre, vous risquez de collecter une très grande quantité de données, qui dépend du temps pendant lequel le fichier log actuel a collecté les événements. Notez que cette option est utile uniquement pour la première session de collecte.
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est **180**. Par exemple, si vous spécifiez 180, le collecteur planifie une interrogation de la source d'événement toutes les 180 secondes. Si le cycle d'interrogation précédent est toujours en cours, il est nécessaire d'attendre qu'il se termine. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 180 secondes avant de démarrer car les threads sont occupés.

Paramètre	Description
Nb max. d'interrogations de durées	Durée maximale du cycle d'interrogation en secondes.
Nb max. d'interrogations d'événements	Nombre maximal d'événements par cycle d'interrogation (nombre d'événements collectés par cycle d'interrogation).
Nb max. d'interrogations liées au délai de mise en veille	Délai de mise en veille maximal, en secondes, d'un cycle d'interrogation. 0 indique aucune limite. **> 300** est la valeur par défaut.
Redirecteur	Active ou désactive le serveur Check Point comme un service de transfert. Il est désactivé par défaut.
Type de log (paire Nom-Valeur)	Logs de la source de l'événement au format de la valeur de nom valeur. Il est désactivé par défaut.

Paramètre	Description
Débogage	**Attention :** N'activez le débogage (paramètre défini sur « On » ou « Verbose ») que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active et désactive la consignation du débogage pour la source d'événements. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).

Vérifier le fonctionnement de la collecte Check Point

La procédure suivante illustre comment vérifier que la collecte Check Point fonctionne sous l'onglet **Administration > Intégrité > Surveillance des sources d'événements**.

1. Accédez à l'**onglet Surveillance des sources d'événements** depuis la vue **Administration > Intégrité**.
2. Recherchez **checkpointfw1** dans la colonne **Type de source d'événement** .
3. Recherchez une activité dans la colonne **Nombre** pour vérifier que la collecte Check Point accepte des événements.

La procédure suivante illustre comment vérifier que la collecte Check Point fonctionne à partir de la vue **Investigation > Événements**.

1. Accédez à la vue **Investigation > Événements**.
2. Sélectionnez le Log Decoder (par exemple, **LD1**) qui collecte les événements Check Point dans la boîte de dialogue **Examiner un périphérique**.

3. Recherchez un parser de source d'événements Check Point (par exemple **checkpointfw1**) dans le champ **device.type** de la colonne **Détails** pour vérifier que la collecte Check Point accepte des événements.

Remarque : Si les logs du serveur de pare-feu Check Point VSX sont collectés par le service Check Point Log Collector, pour traduire l'IP VSX dans les logs en méta **ip.orig**, vous devez ajouter le nom d'hôte VSX et l'adresse IP VSX pour le fichier `/etc/hosts` dans Log Collector.

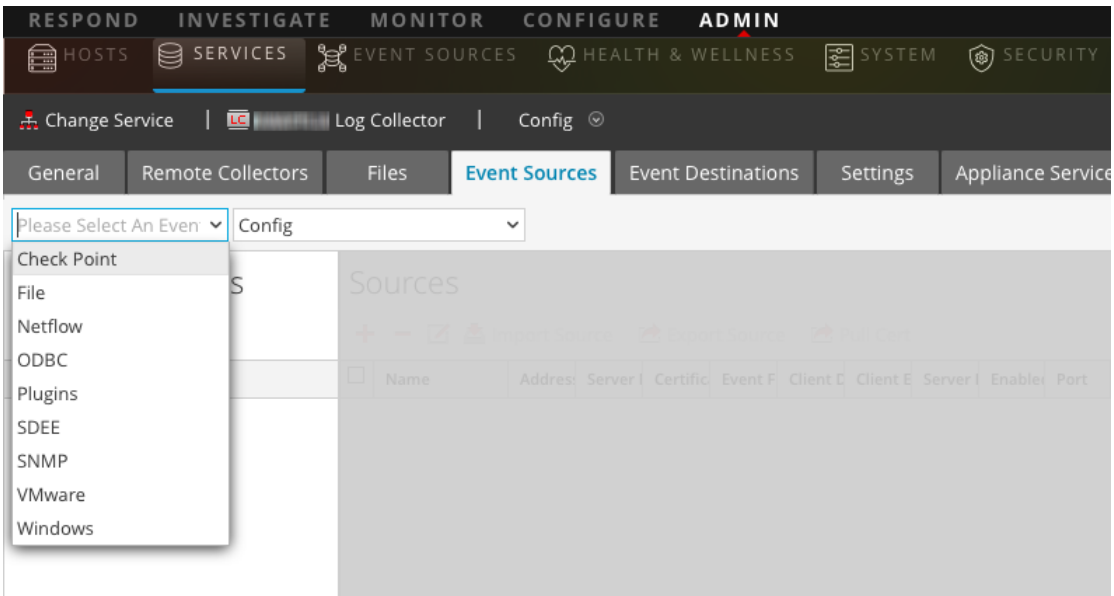
Configurer des sources d'événements de fichiers dans NetWitness Suite

Ce guide indique comment configurer le protocole de collecte des fichiers.

Configurer une source d'événements de fichier

Pour configurer une source d'événements de fichier :

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **Fichier/Configuration** dans le menu déroulant.
6. Dans la barre d'outils du panneau **Catégories d'événements** , cliquez sur + .

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.
7. Sélectionnez un type de source d'événement de fichier, puis cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.
8. Sélectionnez le nouveau type dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils **Sources**.

   La boîte de dialogue **Ajouter une source** s'affiche.
9. Ajoutez un nom de **répertoire de fichiers**, puis modifiez tous les autres paramètres qui requièrent des changements. Pour plus d'informations, reportez-vous à la section Paramètres de collecte de fichiers ci-dessous.
10. Pour obtenir la clé publique et l'entrer dans la boîte de dialogue, procédez comme suit :
    a. Sélectionnez et copiez la clé publique à partir de la source de l'événement en exécutant : **cat ~/.ssh/id_rsa.pub**
    b. Collez la clé publique dans le champ **Clé SSH Eventsource**.
11. Cliquez sur **OK**.

Vous devez redémarrer la collecte de fichiers pour que vos modifications soient appliquées.

Arrêter et redémarrer la collecte de fichier

Après avoir ajouté une nouvelle source d'événement qui utilise la collecte de fichiers, vous devez arrêter et redémarrer le service de collecte de fichier NetWitness Suite. Cette action est nécessaire pour ajouter la clé à une nouvelle source d'événement.

Paramètres de collecte de fichiers

Le tableau suivant fournit des descriptions des paramètres de la source Collecte de fichiers.

Nom	Description
Basique	

Nom	Description
Répertoire de fichiers*	Répertoire de collecte (par exemple **Eur_London100**) dans lequel la source d'événement de fichiers place ses fichiers. Toute chaîne de caractères conforme à l'expression régulière suivante est une valeur valide : **[_a-zA-Z][_a-zA-Z0-9]*** Cela signifie que le répertoire de fichiers doit commencer par une lettre suivie de chiffres, de lettres et de traits de soulignement. Ne modifiez pas ce paramètre après avoir démarré la collecte de données d'événements. Une fois que vous avez créé la collecte, Log Collector crée les sous-répertoires de travail, d'enregistrement et d'erreur dans le répertoire de collecte.
Adresse*	Adresse IP de la source d'événement. La valeur valide est une **adresse IPv4**, une **adresse IPv6** ou un **nom d'hôte** comprenant un nom de domaine complet.
Spéc. fichier	Expression régulière. Par exemple, **^.*$** = tout traiter.
Encodage de fichier	Encodage de fichier pour l'internationalisation. Saisissez la méthode d'encodage de fichier. Les chaînes suivantes sont des exemples de méthodes valides : • UTF-8 (valeur par défaut) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFTJIS • EBCDICUS
Enabled	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
Avancé	

Nom	Description
Ignorer les erreurs de conversion de chiffrement	Activez cette case à cocher pour ignorer les erreurs de conversion de chiffrement et les données non valides. Cette case à cocher est activée par défaut. **Attention :** Cela peut provoquer des erreurs d'analyse et de transformation.
Quota des disques de fichiers	Détermine le moment où l'enregistrement des fichiers doit être arrêté, indépendamment des paramètres **Enregistrer en cas d'erreur** et **Enregistrer en cas de réussite**. Par exemple, la valeur 10 indique que lorsqu'il reste moins de 10 % d'espace disque disponible, Log Collector cesse d'enregistrer les fichiers afin de réserver suffisamment d'espace pour le traitement normal de la collecte. **Attention :** L'espace disque disponible fait référence à une partition de montage du répertoire de collecte de base. Si le serveur Log Decoder a un disque de 10 To, et si 2 To sont alloués au répertoire de collecte de base, l'affectation de la valeur 10 à ce paramètre entraîne l'arrêt de la collecte des logs lorsqu'il reste moins de 0,2 To (10 % de 2 To) d'espace. Cela ne signifie pas 10 % de 10 To. La valeur valide est un nombre compris entre **0** et **100**. **10** est la valeur par défaut.
Traitement séquentiel	Balise de traitement séquentiel : • Activez la case à cocher (par défaut) pour traiter les fichiers de sources d'événements dans l'ordre de collecte. • Désactivez la case à cocher pour traiter les fichiers de sources d'événements en parallèle.
Enregistrer en cas d'erreur	Balise d'enregistrement en cas d'erreur. Activez la case à cocher pour conserver le fichier de **collecte eventsource** lorsque Log Collector rencontre une erreur. Cette case à cocher est activée par défaut.
Enregistrer en cas de réussite	Balise d'enregistrement du fichier de **collecte eventsource** après traitement. Activez la case à cocher pour enregistrer le fichier de collecte eventsource, une fois qu'il a été traité. Par défaut, l'option n'est pas sélectionnée.

Nom	Description
Clé SSH Eventsource	Clé publique SSH utilisée pour télécharger les fichiers de cette source d'événement. Pour obtenir des instructions sur la génération de clés, consultez la section *Générer la paire de clés sur la source de l'événement et importer la clé publique dans Log Collector*, dans le Guide d'installation et de mise à jour d'un agent SFTP. **Remarque :** Si la collecte de fichiers est arrêtée, NetWitness Suite ne met pas à jour le fichier authorized_keys avec la clé publique SSH que vous ajoutez ou modifiez dans ce paramètre. Vous devez redémarrer la collecte de fichiers pour mettre à jour la clé publique. Vous pouvez ajouter ou modifier la valeur de la clé publique dans ce paramètre pour plusieurs sources d'événements de fichiers lorsque la collecte de fichiers n'est pas en cours d'exécution. Toutefois, NetWitness Suite ne met pas à jour le fichier **authorized_keys** tant que la collecte de fichiers n'a pas redémarré.
Gérer les fichiers d'erreurs	Par défaut, Log Collectorutilise le paramètre **Quota des disques de fichiers** pour vérifier que le disque ne dépasse pas sa limite de remplissage avec des fichiers d'erreurs. Si vous affectez **vrai** à ce paramètre, vous pouvez spécifier l'une des valeurs suivantes : • espace maximal alloué aux fichiers d'erreurs dans le paramètre **Taille des fichiers d'erreurs** ; • nombre maximal de fichiers d'erreurs autorisés dans le paramètre **Nombre de fichiers d'erreur**. Un pourcentage de réduction est également spécifié, ce qui indique au système le taux de réduction à appliquer lorsque le seuil maximal est atteint. Activez la case à cocher pour gérer les fichiers d'erreurs. Par défaut, l'option n'est pas sélectionnée.
Taille des fichiers d'erreurs	Valide uniquement si les paramètres **Gérer les fichiers d'erreurs** et **Enregistrer en cas d'erreur** ont la valeur vrai. Spécifie la limite dans laquelle NetWitness Suite enregistre les fichiers d'erreurs. La valeur que vous spécifiez correspond à la taille totale maximale de tous les fichiers dans le répertoire d'erreurs. La valeur valide est un nombre compris entre **0** et **281 474 976 710 655**. Vous devez spécifier ces valeurs en **Kiloœctets**, **Mégaoctets** ou **Gigaoctets**. **100 Mo** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.

Nom	Description
Nombre de fichiers d'erreurs	Valide uniquement si les paramètres **Gérer les fichiers d'erreurs** et **Enregistrer en cas d'erreur** ont la valeur vrai. Nombre maximal de fichiers d'erreurs autorisés dans le répertoire d'erreurs. La valeur valide est un nombre compris entre **0** et **65536**. **65536** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.
% de réduction des fichiers d'erreurs	Valeur en pourcentage de la taille ou du nombre de fichiers d'erreurs que le service Log Collectorsupprime lorsque la taille ou le nombre maximal a été atteint. Le service supprime les anciens fichiers en premier. La valeur valide est un nombre compris entre **0** et **100**. **10** est la valeur par défaut.
Gérer les fichiers enregistrés	Activez la case à cocher pour gérer les fichiers enregistrés. Par défaut, l'option n'est pas sélectionnée. Par défaut, Log Collector utilise le paramètre **Quota des disques de fichiers** pour vérifier que le disque ne dépasse pas sa limite de remplissage avec des fichiers enregistrés. Si vous activez cette case à cocher, vous pouvez spécifier l'une des valeurs suivantes : • espace maximal alloué aux fichiers enregistrés dans le paramètre **Taille des fichiers enregistrés** ; • nombre maximal de fichiers enregistrés autorisés dans le paramètre **Nombre de fichiers enregistrés**. Un pourcentage de réduction est également spécifié, ce qui indique au système le taux de réduction à appliquer lorsque le seuil maximal est atteint.
Taille des fichiers enregistrés	Valide uniquement si les paramètres **Gérer les fichiers enregistrés** et **Enregistrer en cas de réussite** ont la valeur vrai. Taille totale maximale de tous les fichiers dans le répertoire d'enregistrement. La valeur valide est un nombre compris entre **0** et **281474976710655**. Vous devez spécifier ces valeurs en **Kiloœctets**, **Mégaoctets** ou **Gigaoctets**. **100 Mo** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.

Nom	Description
Nombre de fichiers enregistrés	Valide uniquement si les paramètres **Gérer les fichiers enregistrés** et **Enregistrer en cas de réussite** ont la valeur vrai. Nombre maximal de fichiers enregistrés autorisés dans le répertoire d'enregistrement. La valeur valide est un nombre compris entre **0** et **65536**. **65536** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.
% de réduction des fichiers enregistrés	Valeur en pourcentage de la taille ou du nombre de fichiers enregistrés que le service Log Collector supprime lorsque la taille ou le nombre maximal a été atteint. Le service supprime les anciens fichiers en premier. La valeur valide est un nombre compris entre **0** et **100**. **10** est la valeur par défaut.
Débogage	**Attention :** N'activez le débogage (paramètre défini sur **On** ou **Verbose**) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collectorde manière défavorable. Active/désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).
Annuler	Ferme la boîte de dialogue sans ajouter de type de source d'événement.
OK	Ajoute les paramètres de la source d'événement.

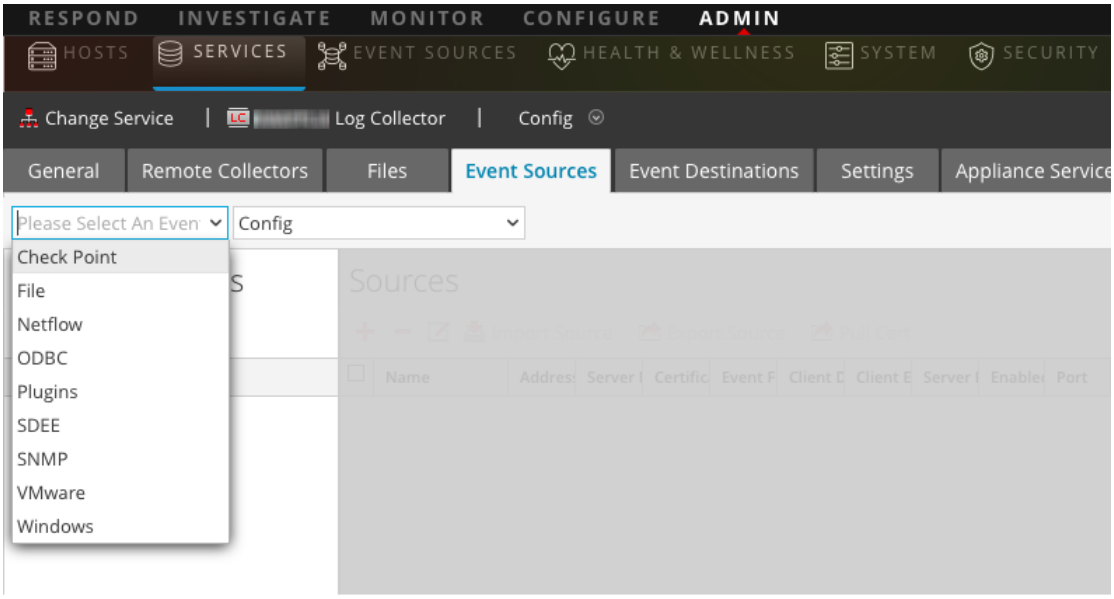
Configurer des sources d'événements Netflow dans NetWitness Suite

Ce guide indique comment configurer le protocole de collecte Netflow.

Configurer une source d'événement Netflow

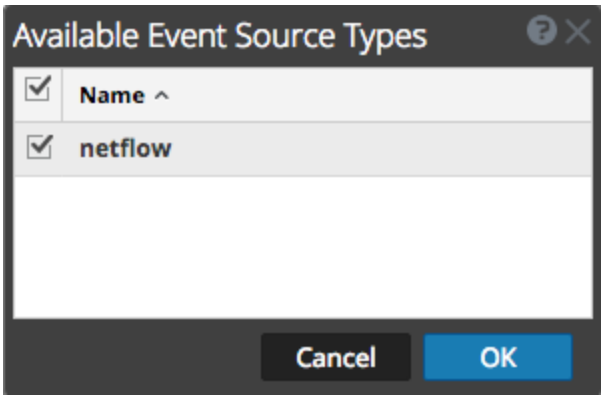
Pour configurer une source d'événement Netflow :

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **Netflow/Configuration** dans le menu déroulant.
6. Dans la barre d'outils du panneau **Catégories d'événements** , cliquez sur  .

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.
7. Sélectionnez le type de source d'événement **netflow** puis cliquez sur **OK**.



Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.

8. Sélectionnez le nouveau type dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils **Sources**.

   La boîte de dialogue **Ajouter une source** s'affiche.

9. Saisissez un numéro de port dans le champ **Port** et assurez-vous que la case Activé est cochée.

   Remarque : NetWitness Suite ouvre les ports 2055, 4739, 6343 et 9995 sur le pare-feu par défaut. Vous pouvez ouvrir d'autres ports pour Netflow, si nécessaire.

   Pour en savoir plus sur d'autres paramètres, reportez-vous à la section Paramètres de collecte Netflow ci-dessous.

10. Cliquez sur **OK**.

La nouvelle source d'événement s'affiche dans la liste.

Paramètres de collecte Netflow

Le tableau suivant fournit les descriptions des paramètres de la source Collecte Netflow.

Nom	Description
	Basique
Port	Spécifiez le numéro de port configuré pour la source d'événement Netflow. NetWitness Suite ouvre les ports 2055, 4739, 6343 et 9995 pour Netflow par défaut. Vous pouvez ouvrir d'autres ports pour Netflow, si nécessaire.
Enabled	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.

Nom	Description
	Avancé
Seuil de logs de publication InFlight	Établit un seuil pour lequel, lorsqu'il est atteint, NetWitness Suite génère un message de log pour vous aider à résoudre des problèmes de flux des événements. Le seuil correspond à la taille des messages d'événements Netflow circulant actuellement entre la source d'événement et NetWitness Suite. Les valeurs autorisées sont les suivantes : • **0 (valeur par défaut)** - désactive le message log. • **100-100000000** - génère un message log lorsque ce Log Collector a traité le nombre spécifié d'événements Netflow. Par exemple, si vous définissez cette valeur sur 100, NetWitness Suite génère un message de log lorsque 100 événements Netflow de la version Netflow spécifique (v5 ou v9) ont été traités.
Débogage	**Attention :** N'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).
Annuler	Ferme la boîte de dialogue sans ajouter de type de source d'événement.
OK	Ajoute les paramètres de la source d'événement.

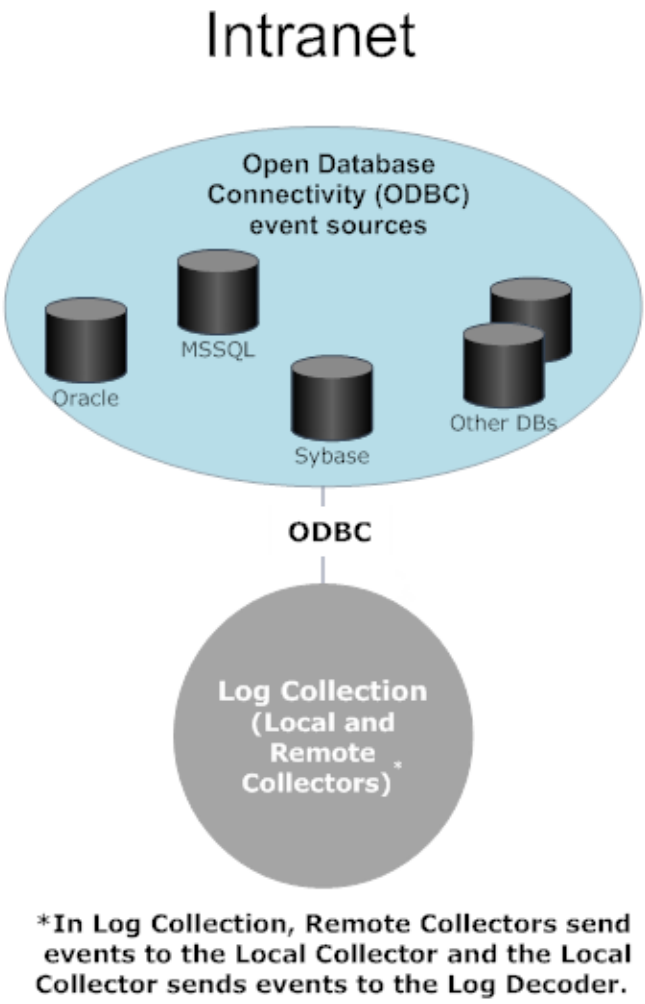
ODBC

Configurer des sources d'événements ODBC dans NetWitness Suite

Cette rubrique vous indique comment configurer le protocole de collecte ODBC permettant de collecter les événements des sources d'événements qui stockent les données d'audit dans une base de données à l'aide de l'interface logicielle ODBC (Open Database Connectivity).

Scénario de déploiement

La figure suivante illustre comment déployer le protocole de collecte ODBC dans NetWitness Suite.



Configurer une source d'événement ODBC

Pour configurer une source d'événement ODBC, vous devez configurer un type de source d'événement et également choisir un modèle DSN.

Configurer un DSN

La procédure suivante explique comment ajouter une source de données à partir d'un modèle DSN existant. Pour les autres procédures liées aux DSN, consultez Configurer des noms de sources de données (DSN).

Configurer un nom de source de données (DSN) :

1. Accédez à **Administration** > **Services**.
2. Dans la grille **Services**, sélectionnez un service **Log Collector**.
3. Cliquez sur  sous **Actions**, puis sélectionnez **Vue** > **Config**.
4. Sous l'onglet **Sources d'événements du Log Collector**, sélectionnez **ODBC/DSN** dans le menu déroulant.
5. Le panneau DSN s'affiche avec les DSN existants, le cas échéant.
6. Cliquez sur + pour ouvrir la boîte de dialogue **Ajouter un DSN**.
7. Choisissez un modèle DSN dans le menu déroulant et saisissez un nom pour le DSN. (Ce nom est utilisé lors de la configuration du type de source d'événement ODBC). Si nécessaire, cliquez sur 

pour ajouter ou supprimer des modèles DSN.
8. Renseignez les paramètres, puis cliquez sur **Enregistrer**.

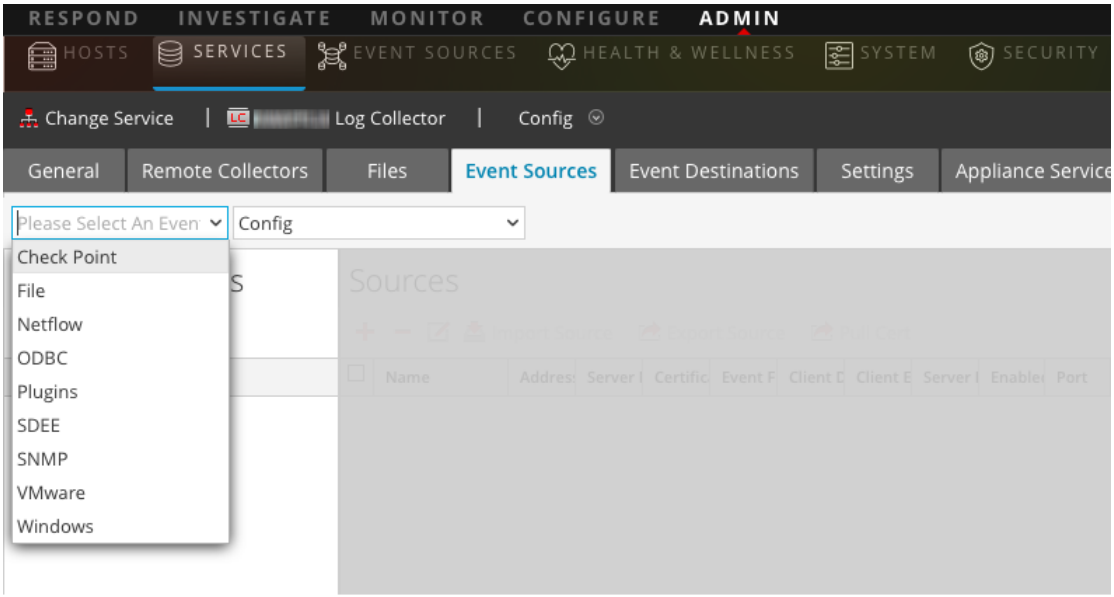
Ajouter un Type de source d'événement

Pour plus d'informations sur les paramètres utilisés dans la procédure suivante, reportez-vous à la section Paramètres de configuration des sources d'événements ODBC.

Pour configurer un type de source d'événement ODBC :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

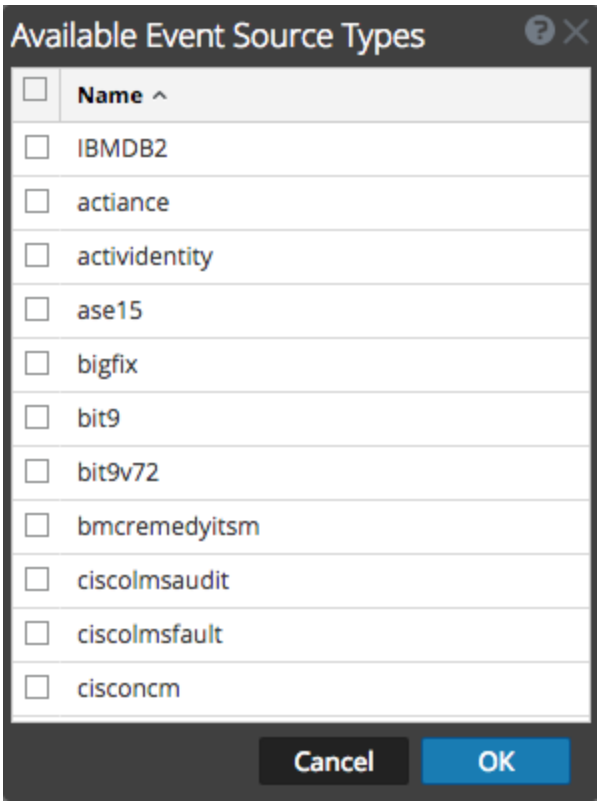
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **ODBC/Config** dans le menu déroulant.

6. Dans la barre d'outils du panneau **Catégories d'événements**, cliquez sur +.

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.

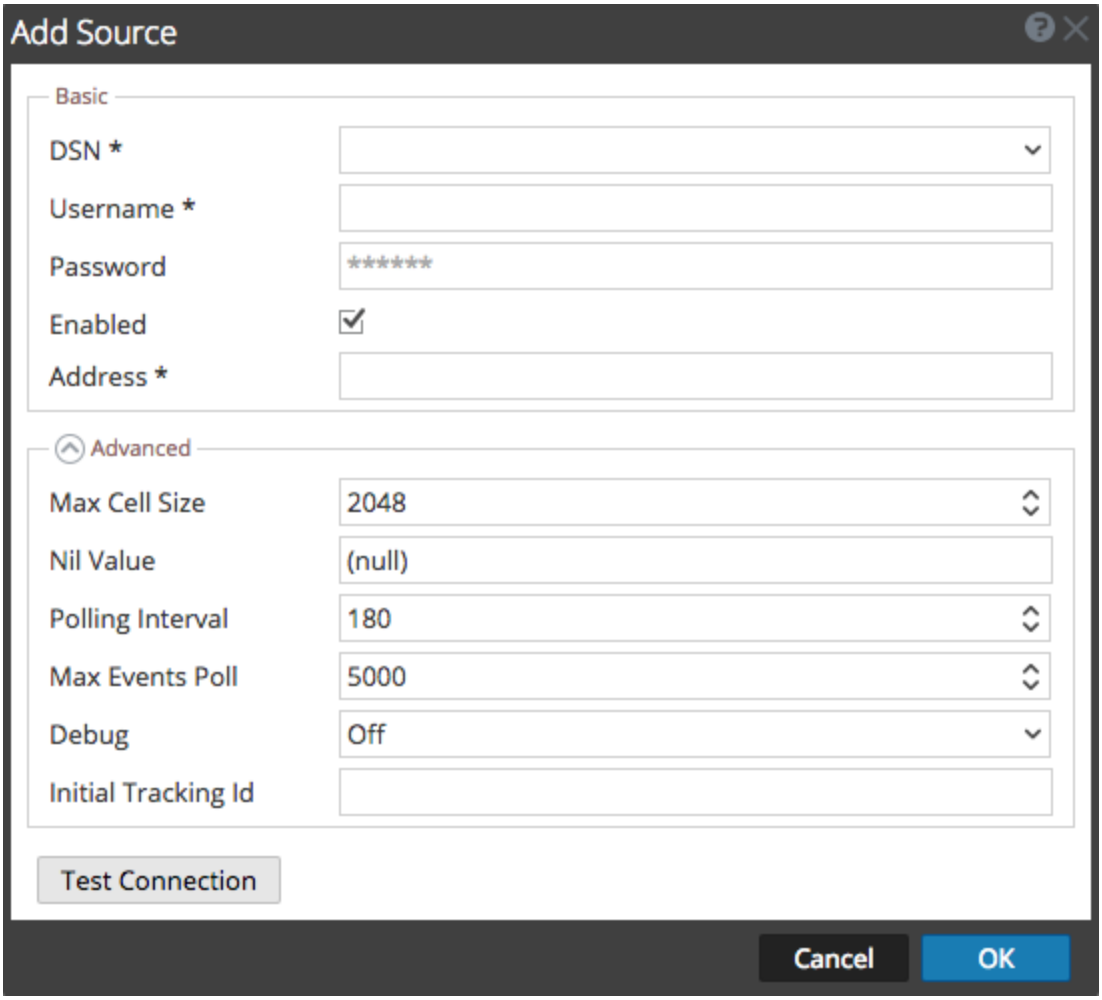


7. Sélectionnez une catégorie de source d'événement (par exemple, **mssql**) et cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.

8. Sélectionnez le nouveau type dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils **Sources**.

   La boîte de dialogue **Ajouter une source** s'affiche.



9. Sélectionnez un DSN dans la liste déroulante, spécifiez ou modifiez les autres paramètres selon le besoin, puis cliquez sur **OK**.

10. Cliquez sur **Tester la connexion**.

    Le résultat du test s'affiche dans la boîte de dialogue. Si le test échoue, modifiez les informations DSN et réessayez.

Remarque : Log Collector prend environ 60 secondes pour renvoyer les résultats du test. Au-delà de ce délai, le test expire et le serveur NetWitness Suite affiche un message d'erreur.

11. Si le test aboutit, cliquez sur **OK**.

La nouvelle source DSN définie s'affiche dans le panneau **Sources**.

Configurer des noms de sources de données (DSN)

Cette rubrique vous indique comment créer et gérer les DSN pour la collecte ODBC.

Contexte

Les sources d'événements ODBC (Open Database Connectivity) requièrent des noms de sources de données (DSN), donc vous devez définir les DSN avec leurs paires de valeurs associées pour la configuration des sources d'événements ODBC.

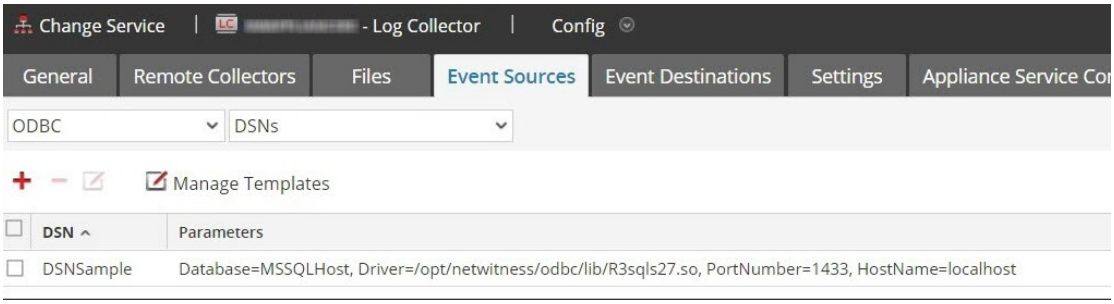
Accéder au panneau DSN

Pour ajouter ou modifier des DSN ou des modèles DSN, commencez par accéder à l'écran approprié.

Pour accéder au panneau Modèles DSN :

1. Accédez à **ADMIN > Services**.
2. Dans la grille **Services**, sélectionnez un **Log Collector**service.
3. Cliquez sur  sous **Actions**, puis sélectionnez **Vue > Config**.
4. Sous l'onglet **Log CollectorSources d'événements**, sélectionnez **ODBC/DSNs** dans le menu déroulant.

   Le panneau **DSN** s'affiche avec les DSN qui sont ajoutés, le cas échéant.



Depuis cet écran, vous pouvez effectuer les opérations suivantes :

- Ajouter un modèle DSN
- Ajouter une source de données à partir d'un modèle existant

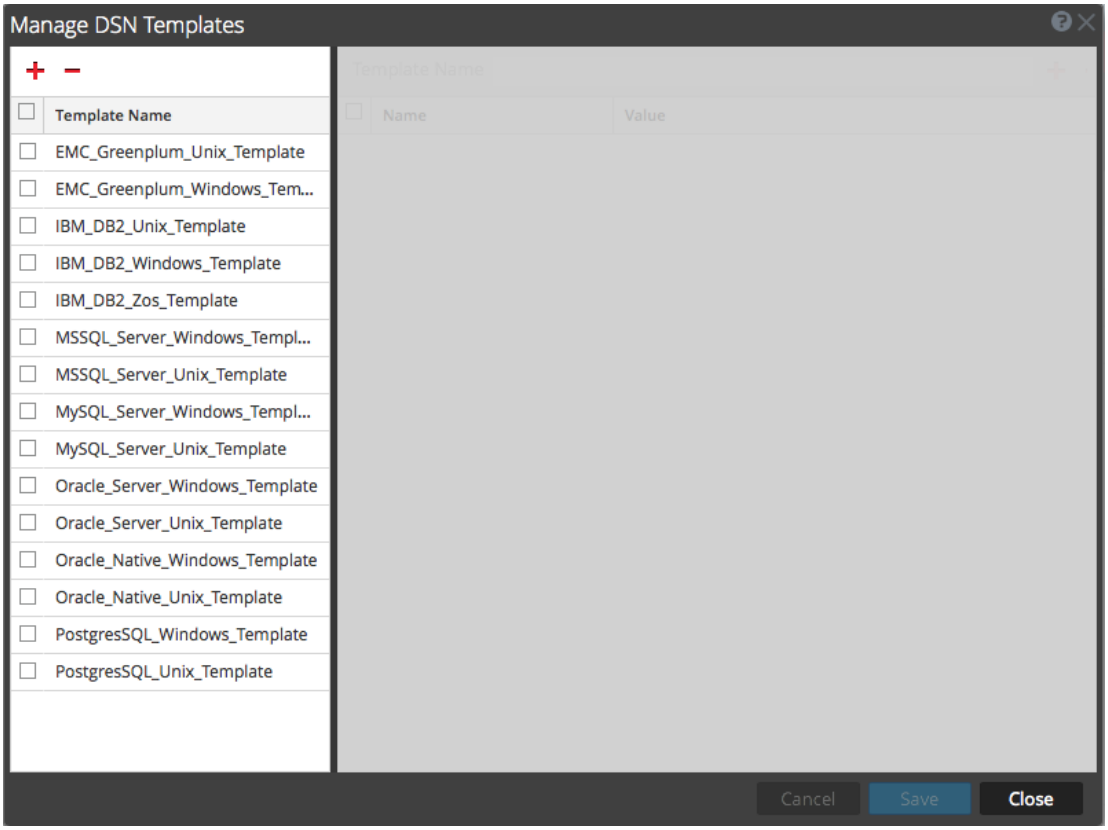
- Ajouter une source de données en modifiant un modèle DSN existant
- Supprimer une source de données ou un modèle DSN

Ajouter un modèle DSN

Si aucun des modèles DSN prédéfinis ne répond à vos besoins, utilisez cette procédure pour ajouter un modèle DSN.

1. Dans le panneau DSN, cliquez sur Manage Templates.

   La boîte de dialogue **Gérer les modèles DSN** s'affiche.



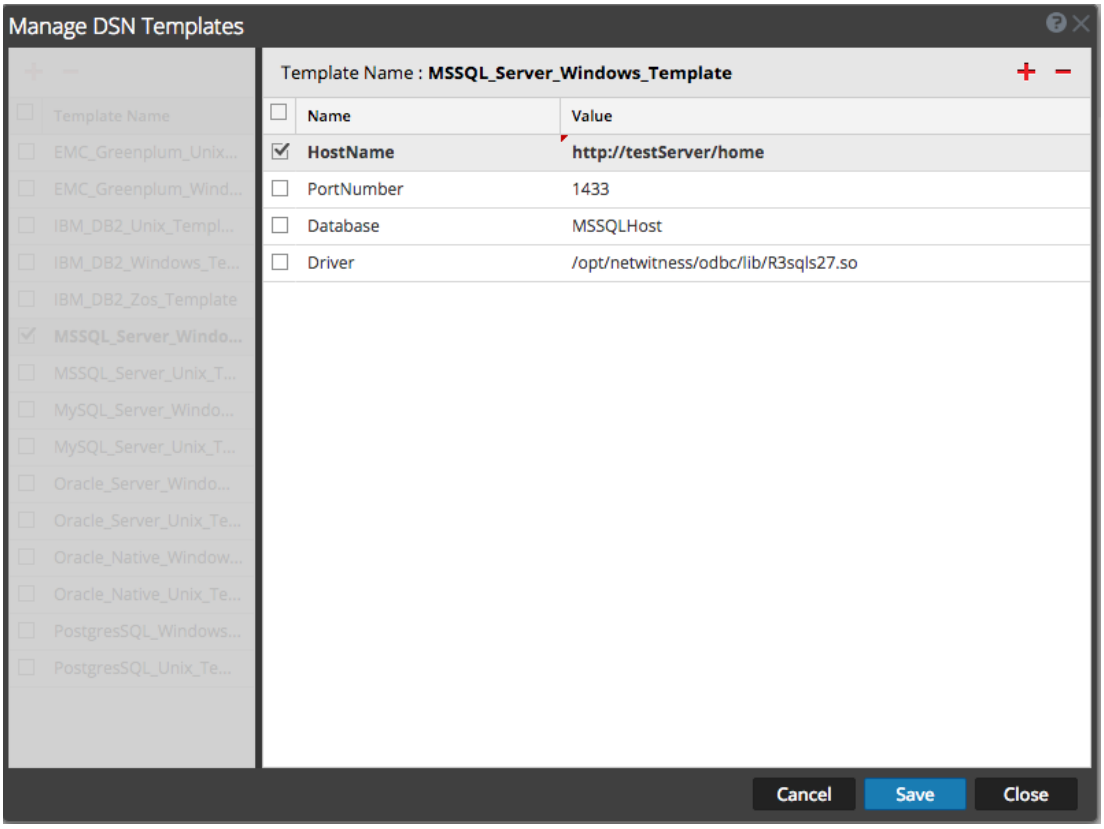
   Remarque : RSA fournit des modèles par défaut sur le panneau gauche, que vous pouvez utiliser lors de l'ajout d'un nouveau DSN.

2. Cliquez sur +.

   Le panneau droit est activé.

3. Spécifiez un nom de modèle et cliquez sur + sur le panneau droit pour ajouter des paramètres.

4. Spécifiez les paramètres. Cliquez sur **Enregistrer**.



Le nouveau modèle DSN est ajouté dans la liste **Gérer les modèles DSN**.

Ajouter une source de données à partir d'un modèle existant

Vous pouvez sélectionner un modèle existant et renseigner les paramètres selon vos besoins.

1. Dans le panneau DSN, cliquez sur + pour ouvrir la boîte de dialogue Ajouter un DSN.

   La boîte de dialogue **Ajouter un DSN** s'affiche avec les sources de données existantes, le cas échéant

2. Choisissez un modèle DSN dans le menu déroulant et saisissez un nom pour le DSN. (Ce nom est utilisé lorsque vous configurez le type de source d'événement ODBC.)

3. Renseignez les paramètres, puis cliquez sur **Enregistrer**.

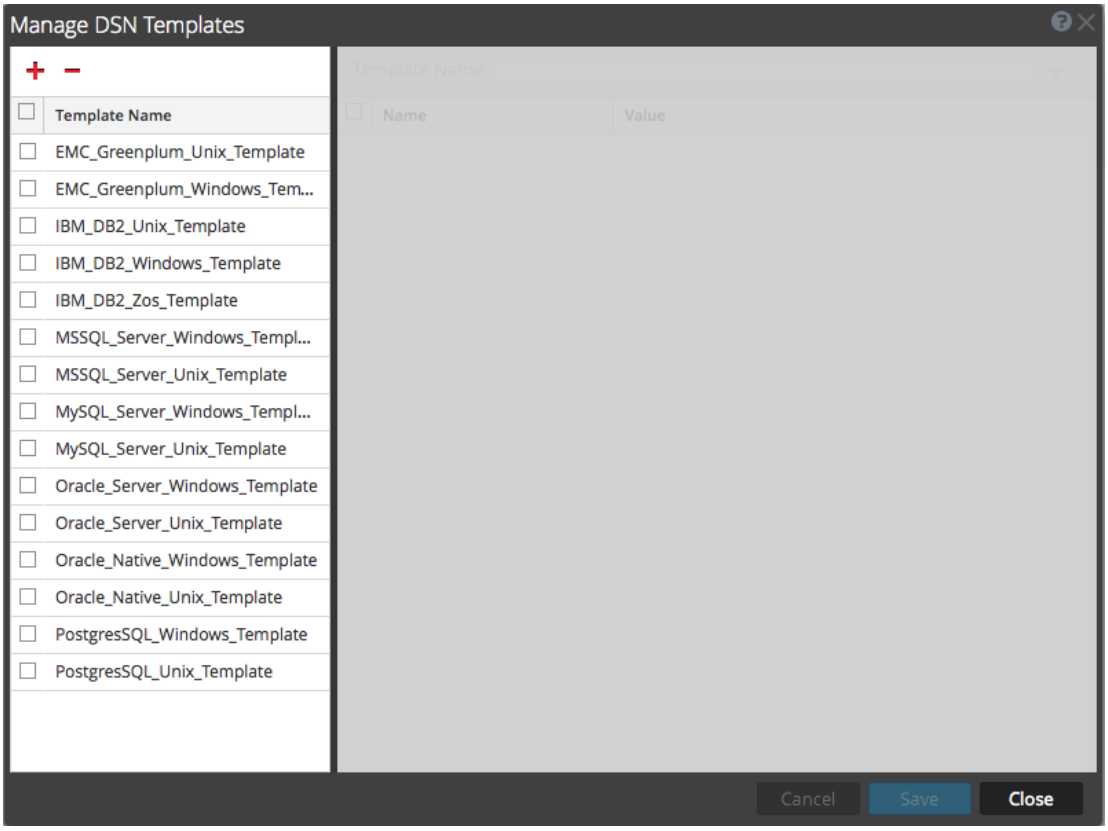
Votre DSN est ajouté à la liste des sources de données.

Ajouter une nouvelle source de données en modifiant un modèle DSN existant

Vous pouvez ajouter une source de données en mettant à jour un modèle DSN existant selon vos besoins.

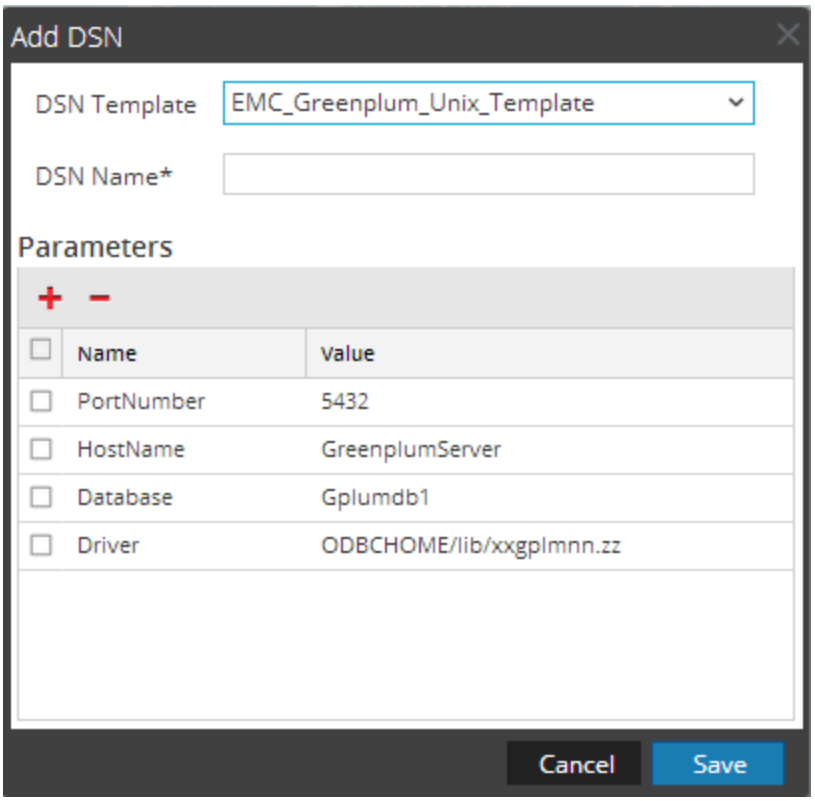
1. Dans le panneau DSN, cliquez sur Manage Templates.

   La boîte de dialogue **Gérer les modèles DSN** s'affiche.



2. Sélectionnez le modèle à modifier :

   Le volet de droite est activé et les paramètres par défaut pour le modèle sélectionné s'affichent.



3. Saisissez un nom dans le champ **Nom DSN**.
4. Ajoutez, supprimez ou modifiez les paramètres par défaut.
5. Une fois que vous avez appliqué l'ensemble des paramètres requis, cliquez sur **Enregistrer**, puis **Fermer**.
6. Sélectionnez le modèle DSN mis à jour dans le menu déroulant et saisissez un nom pour la source de données. (Ce nom est utilisé lorsque vous configurez le type de source d'événement ODBC.)
7. Renseignez les paramètres, puis cliquez sur **Enregistrer**.

Votre DSN est ajouté à la liste des sources de données.

Supprimer une source de données ou un modèle DSN

Si vous n'utilisez plus un DSN ou un modèle DSN, vous pouvez le supprimer à partir du système.

Pour supprimer une source de données existante :

1. Dans le panneau DSN, sélectionnez une source de données existante.
2. Cliquez sur —.

Un message d'avertissement s'affiche vous demandant si vous êtes sûr de vouloir supprimer la source de données.

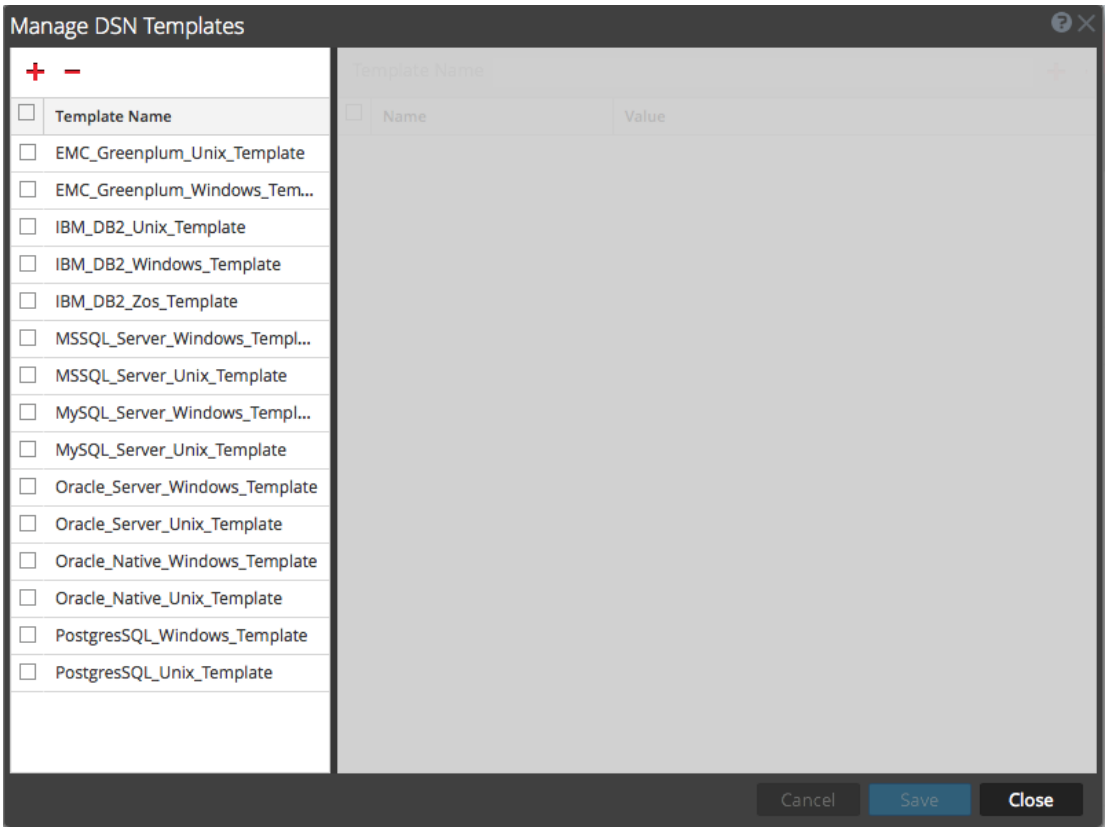
3. Pour supprimer la source de données, cliquez sur **Oui**. Sinon, pour annuler la suppression, cliquez sur **Non**.

Si vous avez confirmé la suppression, la source de données sélectionnée est supprimée du système.

Pour supprimer un modèle DSN existant :

1. Dans le panneau DSN, cliquez sur Manage Templates.

   La boîte de dialogue **Gérer les modèles DSN** s'affiche.



2. Dans le panneau DSN, sélectionnez un modèle DSN existant.
3. Cliquez sur −.

   Un message d'avertissement s'affiche vous demandant si vous êtes sûr de vouloir supprimer le modèle DSN.

4. Pour supprimer le modèle DSN, cliquez sur **Oui** . Sinon, pour annuler la suppression, cliquez sur **Non**.

Si vous avez confirmé la suppression, le modèle DSN sélectionné est retiré du système.

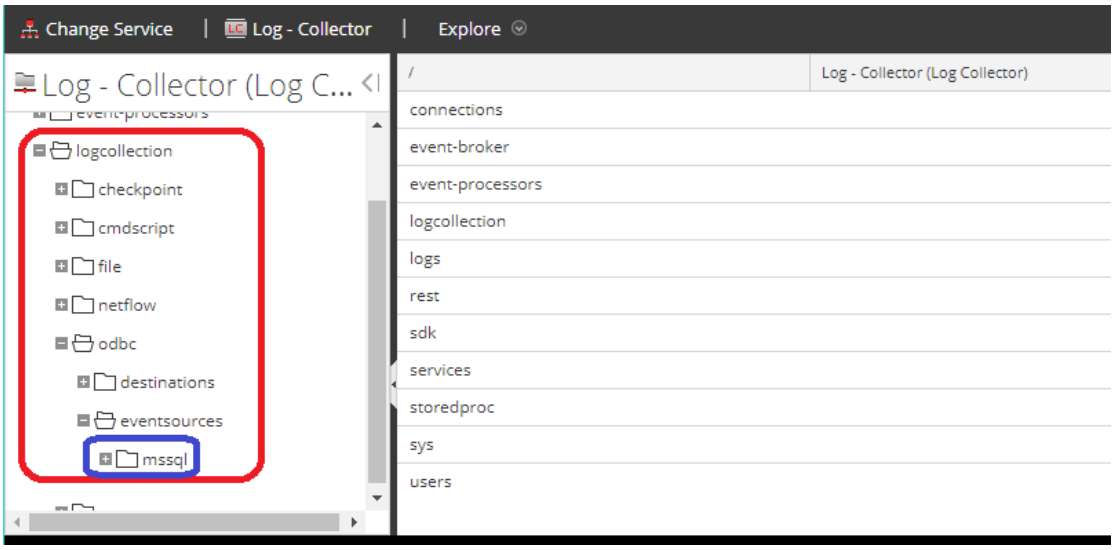
Configurer la méta device.ip pour la source de données ODBC

Pour toute source d'événement ODBC, vous pouvez choisir que le collecteur ODBC renseigne la métavaleur **device.ip** avec l'adresse IP de la source événements ou l'adresse IP source réelle sur laquelle les logs sont collectés.

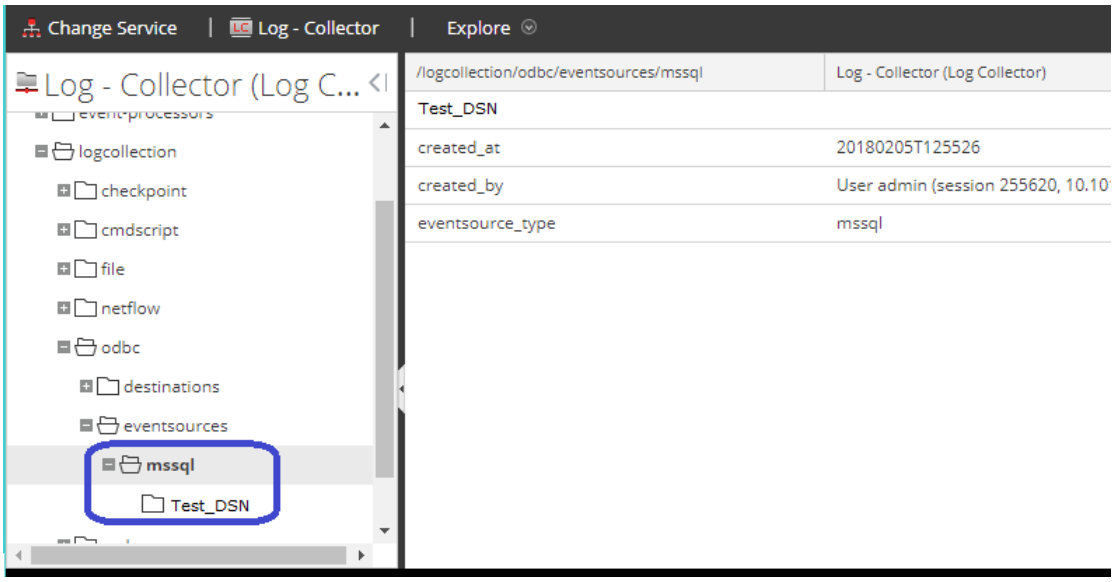
Pour afficher ou définir ce paramètre :

1. Accédez à **ADMIN > Services**.
2. Dans la grille **Services**, sélectionnez un **Log Collector**service.
3. Cliquez sur  sous **Actions** et sélectionnez **Vue > Explorer**.
4. Accédez à **logcollection > odbc > eventsources**.

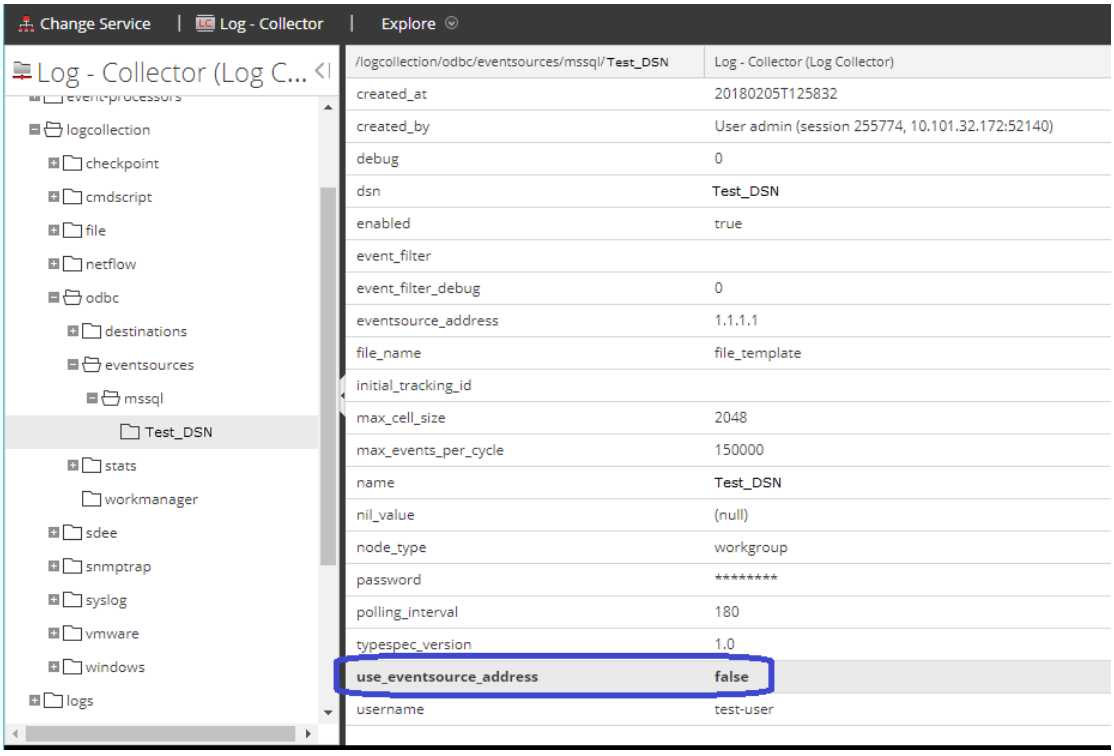
   Il existe des entrées pour chaque source d'événement ODBC que vous avez configuré dans NetWitness. Par exemple, pour cette installation, la seule source d'événement ODBC actuellement configurée est MS SQL :



5. Cliquez sur + en regard d'une source d'événement pour la développer et afficher son entrée DSN.



6. Cliquez sur l'entrée DSN (dans cet exemple **Test_DSN**) pour afficher les paramètres.
7. Le paramètre **use_eventsource_address** est répertorié.



- **False** : l'adresse IP source réelle est utilisée. Il s'agit de la valeur par défaut.
- **True** : l'adresse IP de la source d'événement est utilisée.

8. Cliquez sur la valeur (dans ce cas **False**), saisissez la nouvelle valeur.

Remarque : Si vous saisissez une valeur autre que **true** ou **false** (peu importe la casse), vous recevez une erreur indiquant que la valeur que vous avez saisie ne peut pas être définie.

Les modifications que vous apportez prennent effet immédiatement.

Créer un fichier typespec personnalisé pour la collecte ODBC

Cette rubrique explique comment créer un fichier typespec personnalisé pour le Log Collector. Cette rubrique comprend :

- Créer une procédure typespec personnalisée
- Syntaxe typespec pour la collecte ODBC
- Exemple de fichiers Typespec pour la collecte ODBC

Créer un fichier Typespec personnalisé

Pour créer un fichier typespec personnalisé :

1. Ouvrez un client SFTP (par exemple, WinSCP) et connectez-vous à un Log Collector ou un Remote Log Collector.
2. Accédez à **/etc/netwitness/ng/logcollection/content/collection/odbc**, puis copiez un fichier existant, par exemple **bit9.xml**.
3. Modifiez le fichier en fonction de vos exigences. Reportez-vous à la section Syntaxe typespec pour la collecte ODBC pour plus d'informations.
4. Renommez et enregistrez le fichier sur le même répertoire.
5. Redémarrez le Log Collector.

Remarque : Vous ne pourrez pas voir le nouveau type de source d'événement NetWitness Suite tant que vous ne redémarrez pas le Log Collector.

Syntaxe typespec pour la collecte ODBC

Le tableau suivant décrit les paramètres typespec.

Paramètre	Description
nom	Le nom d'affichage de votre source d'événement ODBC (par exemple, **activeidentity**). NetWitness Suite affiche ce nom dans le panneau **Sources** de **Vue > Config > onglet Sources d'événements**. Utilisez une chaîne alphanumérique comme valeur. Vous ne pouvez pas utiliser de tiret (-), de tiret bas (_) ni d'espace. Le nom doit être unique parmi tous les fichiers typespec du dossier.
type	Type de source d'événement : **odbc**. Ne modifiez pas cette ligne.
prettyName	Nom défini par l'utilisateur pour la source d'événement. Vous pouvez utiliser la même valeur que le nom (par exemple, apache) ou utiliser un nom plus descriptif.
version	Version de ce fichier typespec. La valeur par défaut est 1.0.
auteur	Auteur du fichier typespec. Remplacez author-name par votre nom.
description	Description formelle de la source d'événement. Remplacez formal-description par votre description de la source d'événements.
	Section <périphérique>
parser	Ce paramètre facultatif contient le nom de l'analyseur de log. Cette valeur impose au Log Decoder d'utiliser l'analyseur de log spécifié lors de l'analyse des logs à partir de cette source d'événement. **Remarque :** Veuillez laisser ce champ vide lorsque vous n'êtes pas sûr de l'analyseur de log à utiliser.
nom	Nom de votre source d'événement ODBC (par exemple, **ActivIdentity ActivCard AAA Server**).
maxVersion	Numéro de version de la source d'événement (par exemple, **6.4.1**).
description	Description de la source d'événement.
	Section <collection>
odbc	La syntaxe sous `<odbc>` est utilisée pour la collecte et le traitement des événements. Vous pouvez fournir plusieurs requêtes pour le même type de source d'événements en ajoutant des balises `<query>`.
query	Cette section contient les détails de la requête utilisée pour collecter des informations à partir de la source d'événement.

Paramètre	Description
tag	Balise de préfixe que vous souhaitez ajouter aux événements durant la transformation (par exemple, **ActivIdentity**).
outputDelimiter	Précisez le délimiteur à utiliser pour séparer les champs. Spécifiez l'une des valeurs suivantes : • || (double barre verticale) • ^ (accent circonflexe) • **,** (virgule) • **:** (deux-points) • **0x20** (pour représenter un espace)
interval	Spécifiez le nombre de secondes entre les événements. La valeur par défaut est **60**.
dataQuery	Spécifiez la requête pour récupérer les données de la base de données de source d'événements ODBC pour SQL-syntax. Par exemple : `SELECT acceptedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate`
maxTrackingQuery	Requête utilisée lors de l'extraction initiale des événements afin d'identifier le point de départ dans le jeu de données pour commencer l'extraction des logs. Après l'extraction initiale, cette requête n'est plus utilisée, sauf si la valeur **maxTracking** a été réinitialisée ou modifiée. Par exemple : `SELECT MAX(Event_Id) from ExEvents`
trackingColumn	Valeur de la colonne de suivi utilisée lorsque le collecteur ODBC extrait un nouveau jeu d'événements.

Exemple de fichiers Typespec pour la collecte ODBC

L'exemple suivant est le fichier typespec pour la source d'événement IBM ISS SiteProtector.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>siteprotector4_x</name>
   <type>odbc</type>
```

```
   <prettyName>SITEPROTECTOR4_X</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Collects events from SiteProtector</description>

   <device>
      <name>Internet Security Systems, Inc. RealSecure SiteProtector v 2.0</name>
      <maxVersion>2.0</maxVersion>
      <description></description>
      <parser>iss</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag></tag>
            <outputDelimiter></outputDelimiter>
            <interval></interval>
            <dataQuery></dataQuery>
            <maxTrackingQuery></maxTrackingQuery>
            <trackingColumn></trackingColumn>
            <levelColumn></levelColumn>
            <eventIdColumn></eventIdColumn>
            <addressColumn></addressColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

L'exemple suivant est le fichier typespec pour la source d'événement Bit9 Security Platform.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>bit9</name>
   <type>odbc</type>
   <prettyName>BIT9</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
```

```
   <description>Bit9 Events</description>

   <device>
      <name>Bit9</name>
      <parser>bit9</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag>BIT9</tag>
            <outputDelimiter>||</outputDelimiter>
            <interval>10</interval>
            <dataQuery>
            SELECT
            Timestamp,
            Event_Id,
            Computer_Id,
            File_Catalog_Id,
            Root_File_Catalog_Id,
            Priority,
            Type,
            Subtype,
            IP_Address,
            User_Name,
            Process,
            Description
            FROM
            ExEvents
            WHERE
            Event_Id > '%TRACKING%'
            </dataQuery>
            <trackingColumn>Event_Id</trackingColumn>
            <maxTrackingQuery>SELECT MAX(Event_Id) from
ExEvents</maxTrackingQuery>
            <eventIdColumn></eventIdColumn>
         </query>
      </odbc>
```

```
   </collection>
</typespec>
```

Résoudre les problèmes liés à la collecte ODBC

Vous pouvez résoudre les problèmes et surveiller la collecte ODBC en examinant les messages d'erreur, d'avertissement et d'information du log ODBC, lors de l'exécution de la collecte.

Chaque message du log ODBC inclut les éléments suivants :

- Horodatage
- Catégorie : `debug`, `info`, `warning` ou `failure`
- Méthode de collecte = `OdbcCollection`
- Type de source d'événement ODBC (nom-GOTS) = Nom de la spécification du type ODBC générique que vous avez configuré pour la source d'événement.
- Fonction de collecte terminée ou tentée (par exemple, `[processing]`)
- Nom de la source d'événement ODBC (nom-DSN) = Nom de la source de données que vous avez configuré pour la source d'événement.
- Description (par exemple, le nombre d'événements collectés par Log Collector)
- ID de suivi = la position Log Collector dans le tableau de la base de données cible.

L'exemple suivant illustre le message que vous recevrez en cas de collecte réussie d'un événement ODBC :

```
2014-July-25 17:21:25 info (OdbcCollection) : [event-source]
[processing] [event-source] Published 100 ODBC events: last tracking
id: 2014-July-25 13:22:00.280
```

L'exemple suivant illustre le message que vous pourrez recevoir en cas de collecte réussie d'un événement ODBC :

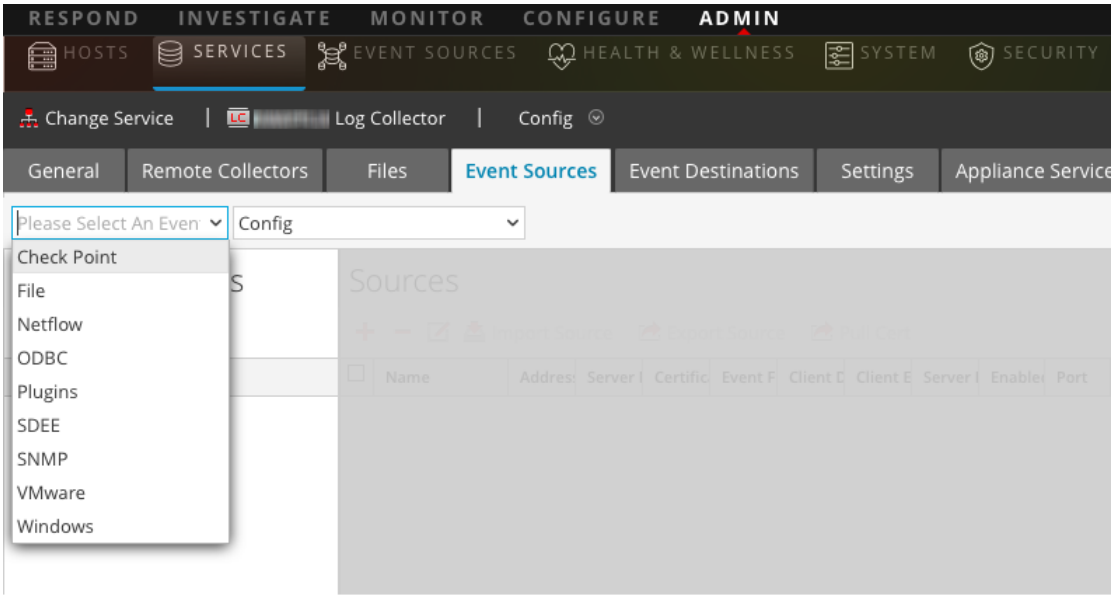
Message log	`timestamp failure (OdbcCollection: [event-source] [processing][event-source-type] Failed during doWork: Unable to prepare statement: state: S0002; error-code:208; description: [RSA] [ODBC-driver][event-source-type]Invalid object name 'object-name'.`
Cause probable	La collecte ODBC a échoué lors de l'accès au pilote ODBC ou à la base de données cible.
Solutions	Validez les paires de valeurs DSN pour la source d'événements.

Configurer des sources d'événements SDEE dans NetWitness Suite

Cette rubrique indique comment configurer le protocole de collecte SDEE.

Pour ajouter une source d'événement SDEE :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez > **Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **SDEE/Config** dans le menu déroulant.

   Le panneau Catégories d'événements affiche les sources d'événements SDEE qui sont configurées, le cas échéant.

6. Dans la barre d'outils du panneau **Catégories d'événements** , cliquez sur .

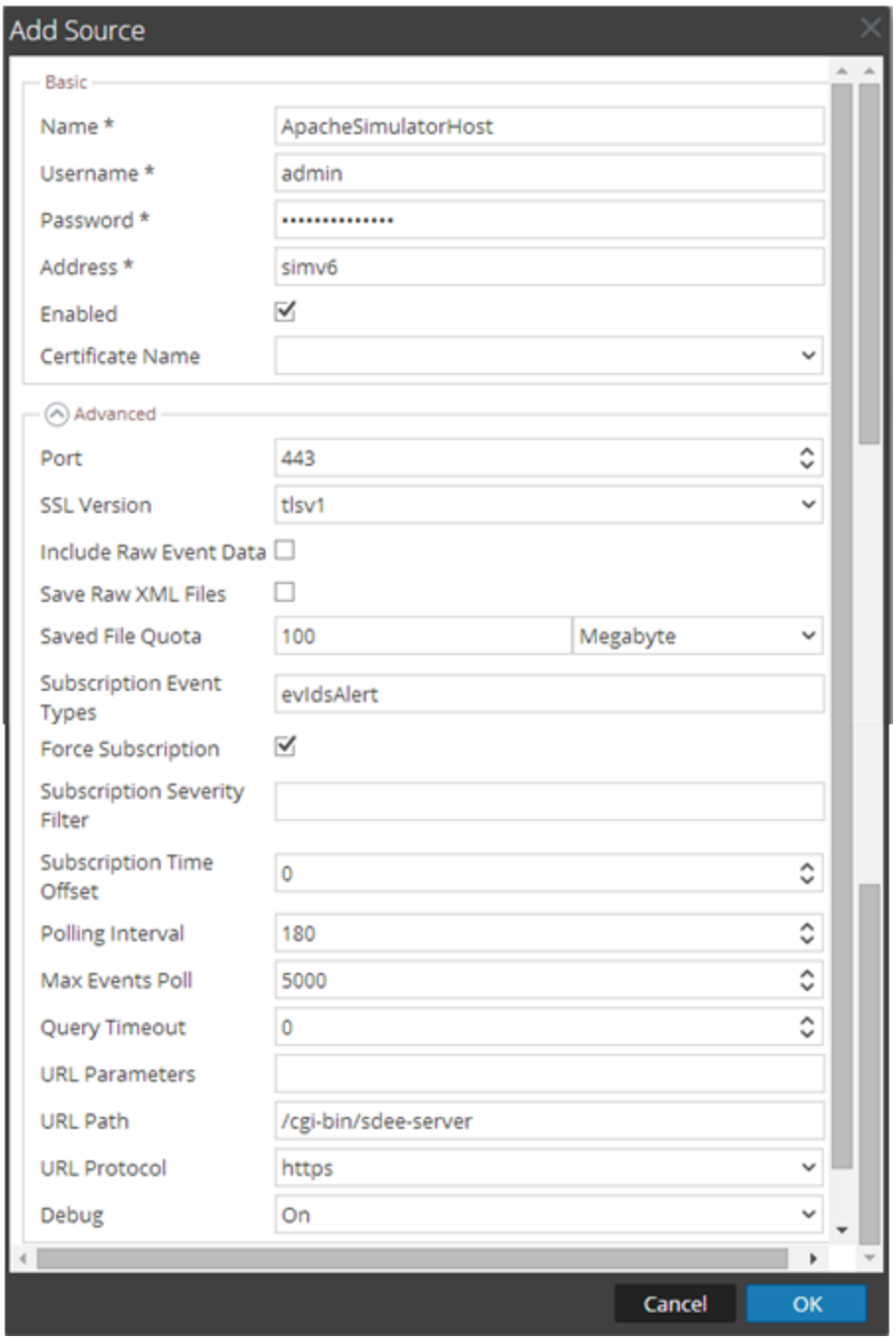
   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.

7. Sélectionnez un type de source d'événement et cliquez sur **OK**.

   Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.

8. Sélectionnez le nouveau type dans le panneau Catégories d'événements, puis cliquez sur + dans la barre d'outils du panneau Sources.

   La boîte de dialogue Ajouter une source s'affiche.



9. Ajoutez un nom, un nom d'utilisateur, une adresse et un mot de passe, modifiez les autres paramètres qui nécessitent des modifications, puis cliquez sur **OK**.

Configurer des sources d'événements SNMP dans NetWitness Suite

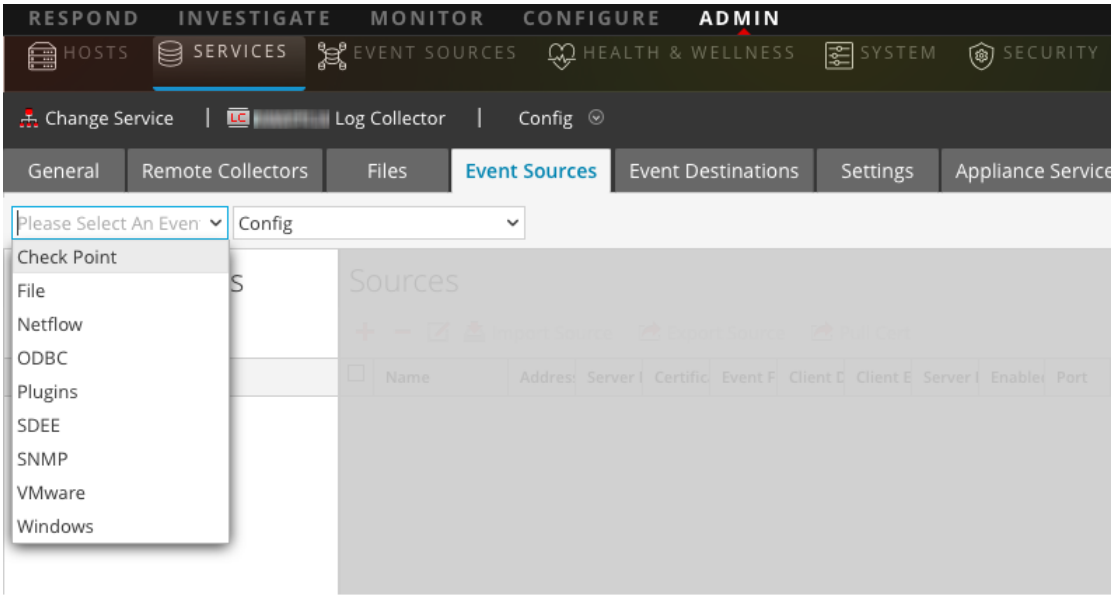
Cette rubrique indique comment configurer le protocole de collecte SNMP.

Configurer une source d'événements Trap SNMP

Pour ajouter la source d'événement SNMP :

Remarque : Si vous avez ajouté précédemment le type **snmptrap**, vous ne pouvez pas l'ajouter de nouveau. Vous pouvez le modifier ou gérer les utilisateurs.

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez > **Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements**, sélectionnez **SNMP/Config** dans le menu déroulant.
6. Dans la barre d'outils du panneau **Catégories d'événements**, cliquez sur +.

   La boîte de dialogue **Types de sources d'événements disponibles** s'affiche.
7. Sélectionnez le type de source d'événement **snmptrap**, puis cliquez sur **OK**.

Le type de source d'événement nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.

8. Sélectionnez **snmptrap** dans le panneau Catégories d'événements.
9. Sélectionnez **snmptrap** dans le panneau Sources, puis cliquez sur l'icône Modifier, , pour modifier les paramètres.
10. Mettez à jour les paramètres que vous souhaitez modifier, puis cliquez sur **OK**.

(Facultatif) Configurer des utilisateurs SNMP

Si vous utilisez SNMP v3, suivez cette procédure pour mettre à jour et maintenir en conditions opérationnelles les utilisateurs SNMP v3.

Configurer des utilisateurs SNMP v3

1. Accédez à **Administrateur** > **Services**.
2. Dans la grille **Services**, sélectionnez un service **Log Collector**.
3. Cliquez sur sous **Actions**, puis sélectionnez **Vue** > **Config**.
4. Sous l'onglet **Sources d'événements** du Log Collector, sélectionnez **Gestionnaire des utilisateurs SNMP V3/SNMP** dans le menu déroulant.

   Le panneau d'utilisateur SNMP v3 s'affiche avec les utilisateurs existants, le cas échéant.
5. Cliquez sur pour ouvrir la boîte de dialogue **Ajouter un utilisateur SNMP**.
6. Renseignez la boîte de dialogue avec les paramètres nécessaires. Les paramètres disponibles sont décrits ci-dessous.

Paramètres des utilisateurs SNMP

Le tableau suivant décrit les paramètres que vous devez saisir lorsque vous créez un utilisateur SNMP v3.

Paramètre	Description
Nom d'utilisateur *	Le nom d'utilisateur (ou plus précisément, dans la terminologie SNMP, le nom de sécurité). NetWitness Suite utilise ce paramètre et le paramètre **ID du moteur** pour créer une entrée utilisateur dans le moteur SNMP du service de collecte. L'association **Nom d'utilisateur** et **ID du moteur** doivent être uniques (par exemple, **logcollector**).

Paramètre	Description
ID du moteur	(Facultatif) ID du moteur de la source d'événement. Pour toutes les sources d'événements envoyant des traps SNMP v3 à ce service de collecte, vous devez ajouter le nom d'utilisateur et l'ID du moteur de la source d'événement expéditrice. Pour toutes les sources d'événements envoyant des informations SNMP v3, vous devez simplement ajouter le nom d'utilisateur avec un ID de moteur vierge.
Type d'authentification	(Facultatif) Protocole d'authentification. Les valeurs valides sont les suivantes : • **Aucun** (valeur par défaut) - seul le niveau de sécurité de **noAuthNoPriv** peut être utilisé pour les traps envoyés à ce service. • **SHA** - Algorithme de hachage • **MD5** - Algorithme Message Digest **Ne pas utiliser : ne sélectionnez pas MD5, cela entre en conflit avec le Log Collector en cours d'exécution en mode FIPS.**
Phrase de passe d'authentification	Facultatif, si vous n'avez pas défini le **Type d'authentification**. Phrase de passe d'authentification.
Type de confidentialité	(Facultatif) Protocole de confidentialité. Vous ne pouvez définir ce paramètre que si le Type d'authentification l'est. Les valeurs valides sont les suivantes : • **None** (valeur par défaut) • **AES -** Advanced Encryption Standard • **DES** -Data Encryption Standard **Ne pas utiliser : ne sélectionnez pas DES, cela entre en conflit avec le Log Collector en cours d'exécution en mode FIPS.**
Phrase de passe de confidentialité	Facultatif si vous n'avez pas défini le **Type de confidentialité**. Phrase de passe de confidentialité
Fermer	Ferme la boîte de dialogue sans ajouter l'utilisateur SNMP v3, ni enregistrer les modifications apportées aux paramètres.
Enregistrer	Ajoute les paramètres d'utilisateur SNMP v3 ou enregistre les modifications apportées aux paramètres.

Configurer des sources d'événements Syslog pour le collecteur distant

Cette rubrique vous indique comment configurer des sources d'événements Syslog pour le Log Collector.

Ne configurez pas la collecte Syslog pour les Local Log Collectors. Vous devez uniquement configurer la collecte Syslog pour les Remote Collectors.

Configurer une source d'événements Syslog

Les écouteurs Syslog pour UDP sur le port 514, TCP sur le port 514 et SSL sur le port 6514 sont créés par défaut. Vous ne devez pas modifier les paramètres SSL sur les écouteurs TCP et SSL. Si vous devez vérifier le certificat SSL, créez un nouveau type de source d'événement à écouter sur un port différent. Veuillez noter que **iptables** doit être configuré pour ouvrir ce port.

Pour configurer le Remote Log Collector pour la collecte Syslog :

1. Accédez à **ADMIN > Services**.
2. Dans la grille Services, sélectionnez un Remote Log Collector et dans le menu Actions, choisissez  **> Vue > Config**.
3. Sélectionnez l'onglet **Sources d'événements**.
4. Sélectionnez **Syslog/Configuration** dans le menu déroulant.

   Le panneau Catégories d'événements affiche les sources d'événements Syslog qui sont configurées, le cas échéant.

   Remarque : Pour RSA NetWitness Suite, certaines sources d'événements Syslog sont disponibles par défaut. Dans ce cas, vous pouvez passer à l'étape 6.

5. Dans la barre d'outils du panneau Catégories d'événements, cliquez sur  .

   La boîte de dialogue Types de sources d'événements disponibles s'affiche.

6. Sélectionnez **syslog-tcp** ou **syslog-udp**. Vous pouvez configurer l'un ou les deux, selon les besoins de votre organisation.
7. Sélectionnez le nouveau type dans le panneau Catégories d'événements, puis cliquez sur  dans la barre d'outils du panneau Sources.

   La boîte de dialogue Ajouter une source s'affiche.

8. Saisissez le numéro du port et sélectionnez **Activé**. Si vous le souhaitez, vous pouvez également configurer les paramètres avancés selon vos besoins.

   Cliquez sur **OK** pour accepter vos modifications et fermer la boîte de dialogue.

Une fois que vous configurez un ou les deux types Syslog, le Log Decoder ou le Remote Log Collector collecte ces types de messages à partir de toutes les sources d'événements disponibles. Par conséquent, vous pouvez continuer à ajouter des sources d'événements Syslog à votre système sans avoir à effectuer de configuration supplémentaire dans RSA NetWitness Suite.

Paramètres Syslog

Les tableaux suivants décrivent les paramètres de base et avancés disponibles pour la configuration de Syslog.

Paramètres de base

Nom	Description
Port*	Le port par défaut est **514**.
Enabled	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
Destinataire SSL	**Remarque :** Ce paramètre s'applique aux versions RSA NetWitness® Suite 11.1 ou supérieure. Il est disponible uniquement pour la catégorie d'événement **syslog-tcp**. Si vous activez la case à cocher, la source d'événement accepte uniquement les connexions SSL/TLS. En outre, si vous modifiez ce paramètre, vous devez arrêter et redémarrer la collecte Syslog pour que la modification soit effective.

Paramètres avancés

Nom	Description
Seuil des logs de publications en vol	Établit un seuil pour lequel, lorsqu'il est atteint, NetWitness génère un message de log pour vous aider à résoudre des problèmes de flux des événements. Le seuil correspond à la taille des messages d'événements Syslog circulant actuellement entre la source d'événement et NetWitness. Les valeurs autorisées sont les suivantes : • **0** (valeur par défaut) - désactive le message log • **100-100000000** - génère le message log lorsque les messages d'événements Syslog passant de la source d'événement à NetWitness sont compris dans une plage d'octets entre 100 et 100 000 000.

Nom	Description
Nombre maximal de récepteurs	Nombre maximum de ressources récepteur utilisées pour traiter les événements syslog collectés. La valeur par défaut est **2**.
Filtre d'événements	Sélectionnez un filtre. Reportez-vous à Configurer des filtres d'événements pour un Collector pour obtenir des instructions sur la manière de définir des filtres.
Débogage	**Attention :** N'activez le débogage (paramètre défini sur « On » ou « Verbose ») que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).

Nom	Description
Mode de vérification SSL	**Remarque :** Ce paramètre s'applique aux versions RSA NetWitness® Suite 11.1 ou supérieure. Il est disponible uniquement pour la catégorie d'événement **syslog-tcp**. Ce paramètre s'applique uniquement si le paramètre **Destinataire SSL** est sélectionné. Si vous modifiez le mode de vérification SSL, vous devez arrêter et redémarrer la collecte Syslog pour que la modification soit effective. Options disponibles : • **verify-none** : (par défaut) le serveur ne vérifie pas le certificat du client, si existant. Un client peut se connecter sans présenter de certificat. • **verify-peer**: Le serveur vérifie le certificat du client, si existant. Un client peut se connecter sans présenter de certificat. **Remarque :** Si la vérification échoue, un message d'avertissement est consigné mais les messages continueront d'être acceptés. • **verify-peer-fail-if-no-cert** : Le client doit présenter un certificat pour qu'il soit vérifié par le serveur. **Remarque :** Si vous utilisez ce mode, le certificat d'autorité de certification du client ***doit*** être téléchargé dans le magasin d'approbations du Log Collector à l'aide de l'API REST à l'adresse `http://LC-ip-address:50101/sys/caupload`

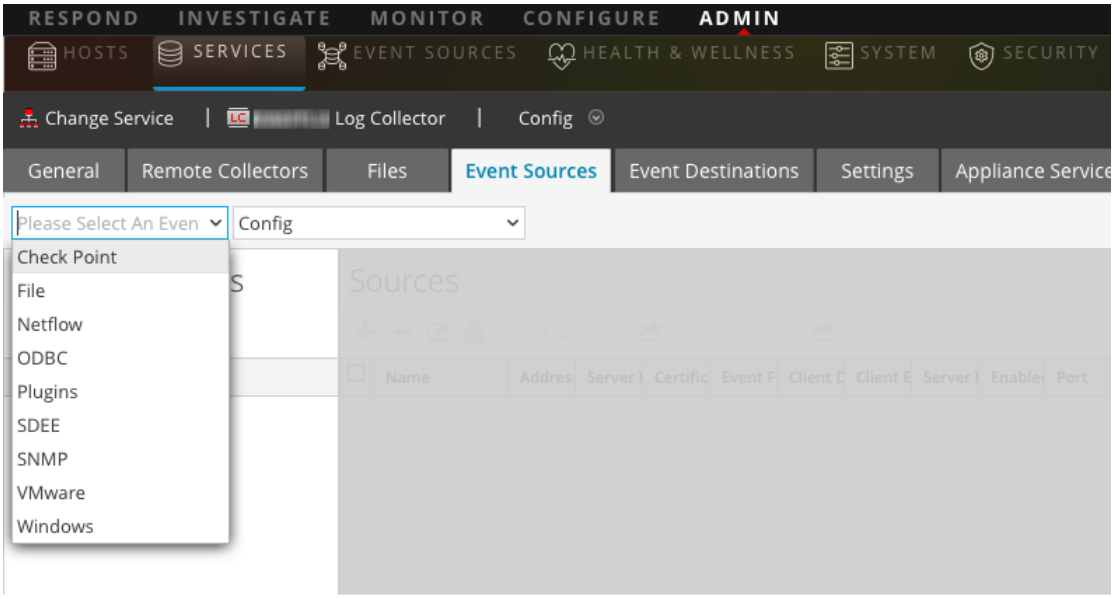
Configurer des sources d'événement VMware dans NetWitness Suite

Ce guide indique comment configurer le protocole de collecte VMware.

Pour ajouter une source d'événement VMware :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

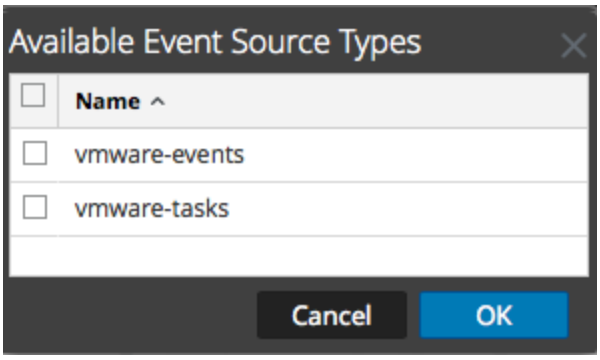
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sous l'onglet **Sources d'événements** du Log Collector, sélectionnez **VMware/Config** dans le menu déroulant.

   Le panneau Catégories d'événements affiche les sources d'événements VMware qui sont configurées, le cas échéant.

6. Cliquez sur + pour ouvrir la boîte de dialogue **Types de sources d'événements disponibles**.



7. Sélectionnez **vmware-events** ou **vmware-tasks** à partir de la boîte de dialogue Types de sources d'événements disponibles, puis cliquez sur **OK**.

   Les types de sources d'événements disponibles VMware sont les suivants :

   - **vmware-events :** Configurez vmware-events pour collecter des événements issus des serveurs vCenter et des serveurs ESX/ESXi.

- **vmware-tasks :** (Facultatif) Configurez vmware-tasks pour collecter des tâches issues des serveurs vCenter.

8. Sélectionnez le nouveau type dans le panneau Catégories d'événements, puis cliquez sur + dans la barre d'outils Sources.
9. Ajoutez un nom, un nom d'utilisateur et un mot de passe, puis modifiez les autres paramètres qui nécessitent des modifications.

   Attention : Si vous devez saisir le nom de domaine en tant que partie du Nom d'utilisateur, vous devez utiliser une double barre oblique comme séparateur. Par exemple, si le nom de domaine | nom d'utilisateur est corp\smithj, vous devez spécifier **corp\\smithj**.

10. Cliquez sur **OK** pour enregistrer vos modifications.

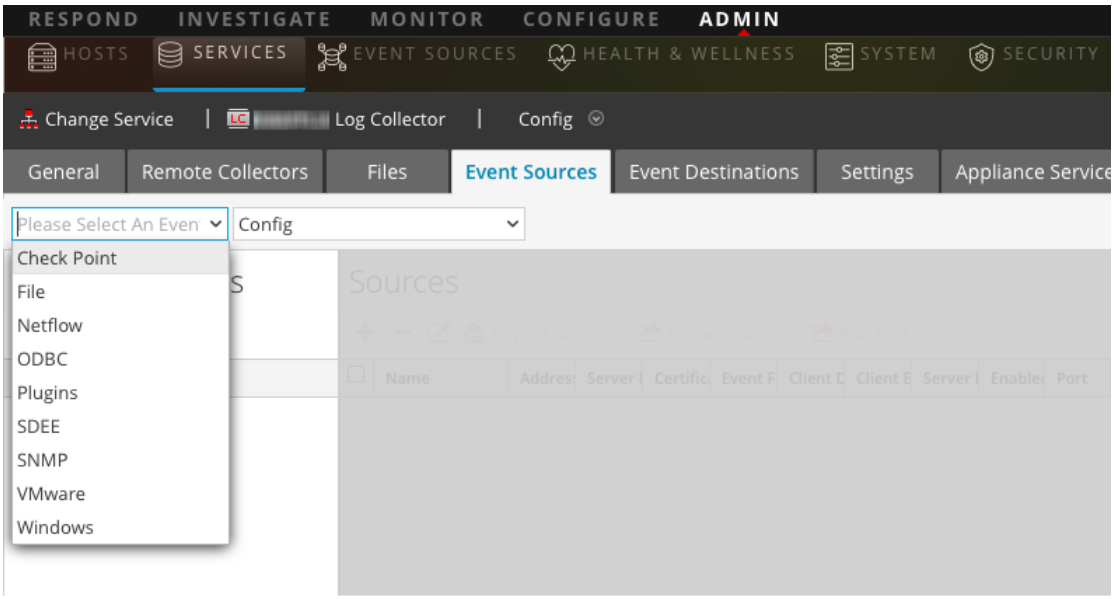
Configurer des sources d'événement Windows dans NetWitness Suite

Ce guide indique comment configurer le protocole de collecte Windows.

Dans RSA NetWitness Suite, vous devez configurer le realm Kerberos, puis ajouter le type de source d'événement Windows.

Pour configurer le realm Kerberos pour la collecte Windows :

1. Accédez à **ADMIN > Services.**
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.



5. Sélectionnez **Realm Kerberos/Windows** dans le menu déroulant.
6. Dans la barre d'outils du panneau de Configuration du realm Kerberos, cliquez sur + pour ajouter un nouveau realm.

   La boîte de dialogue Ajouter un domaine Kerberos s'affiche.
7. Renseignez les paramètres, en suivant les instructions ci-dessous.

Paramètre	Détails
Nom du realm Kerberos	Saisissez le nom de realm, tout en majuscules. Par exemple, DSNETWORKING.COM. Notez que le paramètre Mappages est automatiquement rempli avec des variantes du nom de realm.
Nom de l'hôte KDC	Saisissez le nom du contrôleur de domaine. ***N'utilisez pas*** de nom complet ici, simplement le nom d'hôte du contrôleur de domaine. **Remarque :** Assurez-vous que le Log Collector est configuré comme client DNS pour le serveur DNS d'entreprise. Dans le cas contraire, le Log Collector ne saura pas comment rechercher le realm Kerberos.
Serveur d'administration	(Facultatif) Nom du serveur d'administration Kerberos au format FQDN.

8. Cliquez sur **Enregistrer** pour ajouter le domaine Kerberos.

Pour ajouter une source d'événements Windows

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.

3. Sous Actions, sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.
5. Sous l'onglet **Sources d'événements** du Log Collector, sélectionnez **Windows/Config** dans le menu déroulant.

   Le panneau Catégories d'événements affiche les sources d'événements VMware qui sont configurées, le cas échéant.

Ensuite, poursuivez à partir de l'écran actuel pour ajouter une catégorie et un type d'événements Windows.

Pour configurer un type d'événement Windows :

1. Sélectionnez **Windows/Configuration** dans le menu déroulant.
2. Dans la barre d'outils du panneau Catégories d'événements , cliquez sur  pour ajouter une source.

   La boîte de dialogue Ajouter une source s'affiche.
3. Renseignez les paramètres, en suivant les instructions ci-dessous.

Paramètre	Détails
Alias	Saisissez un nom descriptif.
Méthode d'authentification	Choisissez **Négocier**.
Canal	Pour la plupart des sources d'événements qui utilisent la collecte Windows, il est souhaitable de collecter les canaux **Sécurité**, **Système**, et **Application**.
Nom d'utilisateur	Saisissez le nom du compte pour le compte utilisateur Windows que vous avez configuré précédemment pour la communication avec NetWitness. Notez que vous devez saisir le nom complet du compte, qui inclut le domaine. Par exemple, **rsalog@DSNETWORKING.COM**.
Mot de passe	Saisissez le mot de passe du compte utilisateur.
Nbre max. d'événements par cycle	(Facultatif). RSA recommande de définir cette valeur sur 0, ce qui permet de collecter tous les éléments.
Intervalle d'interrogation	(Facultatif). Pour la plupart des utilisateurs, la valeur **60** devrait fonctionner correctement.

4. Cliquez sur **OK** pour ajouter la source.

   La source d'événement Windows nouvellement ajoutée s'affiche dans le panneau Catégories d'événements.

5. Sélectionnez la nouvelle source d'événement dans le panneau Catégories d'événements.

   Le panneau **Hôtes** est activé.

6. Cliquez sur + dans la barre d'outils du panneau Hôtes.

7. Renseignez les paramètres, en suivant les instructions ci-dessous.

Paramètre	Détails
Adresse de la source d'événement	Saisissez l'adresse IP de l'hôte Windows.
Port	Acceptez la valeur par défaut, **5985**.
Mode de transport	Saisissez **http**.
Activé	Assurez-vous que la case à cocher est activée.

8. Cliquez sur **Tester la connexion**.

   Remarque : Vous devriez pouvoir tester la connexion même si le service de Windows n'est pas en cours d'exécution.

Pour plus d'informations sur l'une des étapes précédentes, consultez les rubriques d'aide suivantes dans le Guide d'utilisation NetWitness Suite :

- Configurer la collecte de Windows : https://community.rsa.com/docs/DOC-43410
- Guide de Configuration de Microsoft WinRM : https://community.rsa.com/docs/DOC-58163
- Guide de test et de résolution des problèmes de Microsoft WinRM : https://community.rsa.com/docs/DOC-58164

Guide de configuration de la collecte Windows d'ancienne génération et NetApp

Ce protocole **Windows d'ancienne génération** collecte des événements Windows d'ancienne génération (sources d'événements Windows 2003 ou versions antérieures) et des événements d'audit CIFS issus des sources d'événements ONTAP NetApp.

Vous devez déployer Log Collection, un ensemble composé d'un Local Collector et d'un Remote Collector Windows d'ancienne génération, avant de pouvoir configurer le protocole de collecte Windows d'ancienne génération.

Mode de fonctionnement de la collecte Windows d'ancienne génération et NetApp

Utilisez le protocole de collecte Windows d'ancienne génération pour configurer NetWitness Suite afin qu'il collecte les événements issus de :

- Sources d'événements Microsoft Windows d'ancienne génération (Sources d'événements Windows 2003 et de version antérieure)
- Sources d'événements NetApp

Sources d'événements Windows 2003 et de version antérieure

Les sources d'événements Windows d'ancienne génération sont antérieures aux versions Windows (telles que Windows 2000 et Windows 2003). Le protocole de collecte de l'ancienne génération de Windows collecte les sources d'événements de Windows qui sont déjà configurées pour une collecte enVision pour éviter d'avoir à les reconfigurer. Configurez ces sources d'événements sous le type de source d'événement windows.

Sources d'événements NetApp

Les appliances NetApp exécutant Data ONTAP prennent en charge un framework d'audit natif qui est similaire aux serveurs Windows. Une fois configuré, ce framework d'audit génère et enregistre les événements d'audit au format de fichier Windows .evt. Le protocole de collecte Windows d'ancienne génération prend en charge la collecte des événements tels que les fichiers NetApp.evt. Configurez ces sources d'événements sous le type de source d'événement netapp_evt.

L'appliance NetApp Data ONTAP est configurée pour générer des événements d'audit CIFS et les enregistrer périodiquement au format de fichiers as.evt incluant l'horodatage dans le nom de fichier. Pour plus d'informations, reportez-vous au Guide de configuration des sources d'événement de Network Appliance Data ONTAP sur RSA Link. Le protocole de collecte enregistre l'horodatage du dernier nom de fichier au format .evt traité pour suivre l'état de la collecte.

Paramètres spécifiques à NetApp

La plupart des paramètres gérés dans la boîte de dialogue Ajouter ou modifier la source s'appliquent à la fois aux sources d'événements Windows d'ancienne génération et NetApp.

Les deux paramètres suivants sont propres aux sources d'événements NetApp.

- **Chemin d'accès au répertoire d'événements** - L'appliance NetApp génère des données d'événements et les enregistre dans des fichiers .evt au sein d'un répertoire qu'il est possible de partager sur l'appliance NetApp. NetWitness Suite nécessite que vous renseigniez ce chemin d'accès au répertoire dans les paramètres de Chemin d'accès au répertoire d'événements.

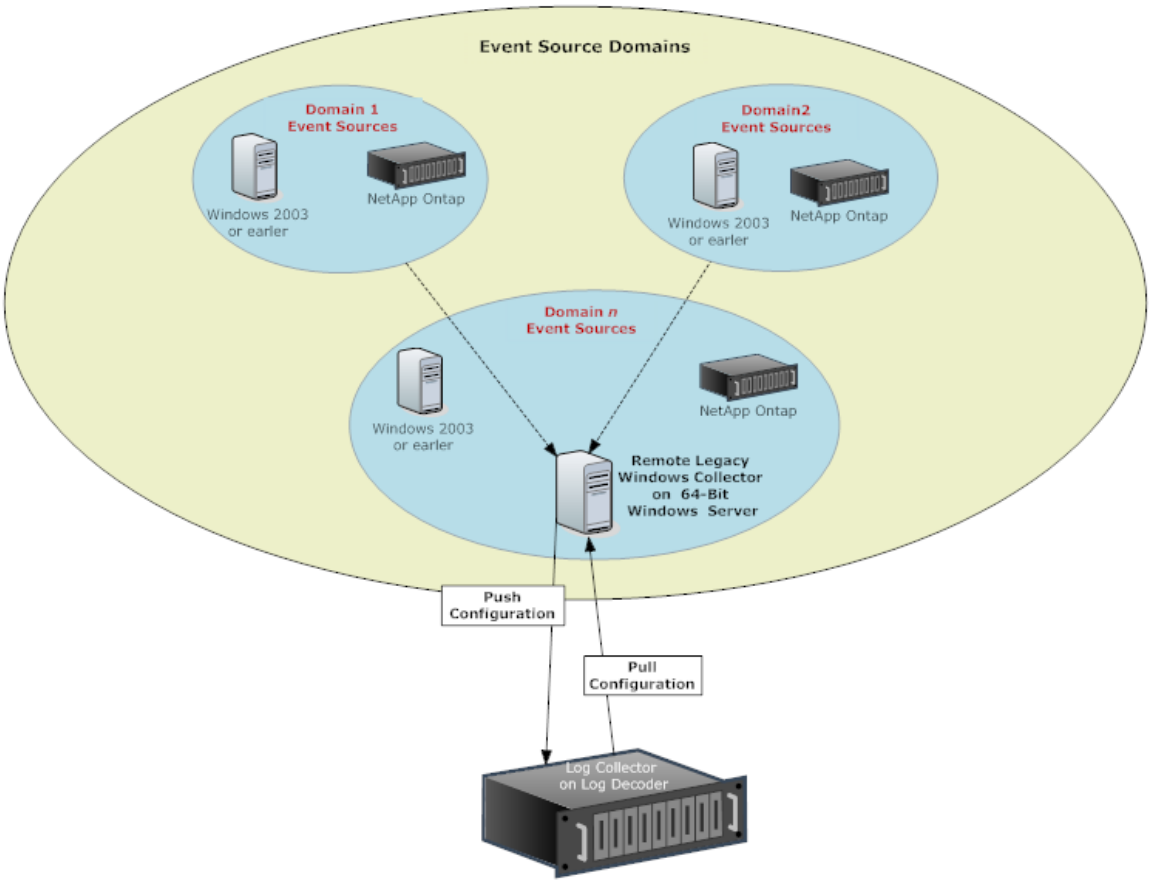
- **Préfixe des fichiers d'événements** - Similaire au Chemin d'accès au répertoire d'événements, NetWitness Suite requiert que vous spécifiiez le préfixe (par exemple, adtlog.) des fichiers .evt de données d'événements afin que NetWitness Suite puisse traiter ces données.

Lors de chaque cycle d'interrogation, NetWitness Suite parcourt le chemin partagé NetApp qui a été configuré pour les fichiers **.evt** identifiés dans les paramètres Chemin d'accès au répertoire d'événements et Préfixe des fichiers d'événements. NetWitness Suite :

- Trie les fichiers correspondants au format event-file-prefix.AAMMJJhhmmss.evt dans l'ordre ascendant.
- Utilise l'horodatage du dernier fichier traité pour déterminer les fichiers qui doivent encore être traités. Si NetWitness Suite trouve un fichier traité partiellement, il ignore les événements déjà traités.

Scénario de déploiement

Le protocole de collecte de l'ancienne génération de Windows collecte les événements de données issus des sources d'événements Windows 2003 ou version antérieure, et de l'appliance NetApp ONTAP. Le collecteur distant de l'ancienne génération de Windows correspond au SA Legacy Windows Collector installé sur un serveur 64 bits physique ou virtuel doté de Windows 2008 dans votre domaine de source d'événement.



Configurer la collecte Windows d'ancienne génération

Cette rubrique vous indique comment rechercher les fichiers exécutables et les instructions nécessaires pour installer ou mettre à niveau le collecteur Windows d'ancienne génération dans vos domaines Windows d'ancienne génération.

Installez le collecteur Windows d'ancienne génération NetWitness Suite sur un serveur physique ou virtuel Windows 2008 R2 SP1 64 bits à l'aide du fichier **NWLegacyWindowsCollector-11.*numéro-version.exe***. Vous téléchargez le fichier **NWLegacyWindowsCollector-11.*numéro-version.exe*** à partir du lien de RSA. Consultez la page *Instructions d'installation et de mise à niveau de la collecte Windows d'ancienne génération pour NetWitness 11* pour obtenir un complément d'informations sur l'installation ou la mise à niveau de la collecte Windows d'ancienne génération.

Remarque : La console MMC (Microsoft Management Console) doit être fermée durant le processus d'installation.

Configurer des sources d'événements Windows d'ancienne génération et NetApp

Cette rubrique vous indique comment configurer des sources d'événements Windows d'ancienne génération dans NetWitness Suite.

Le protocole de collecte Windows d'ancienne génération collecte les données d'événements des sources d'événements Windows 2003 ou antérieures et NetApp.

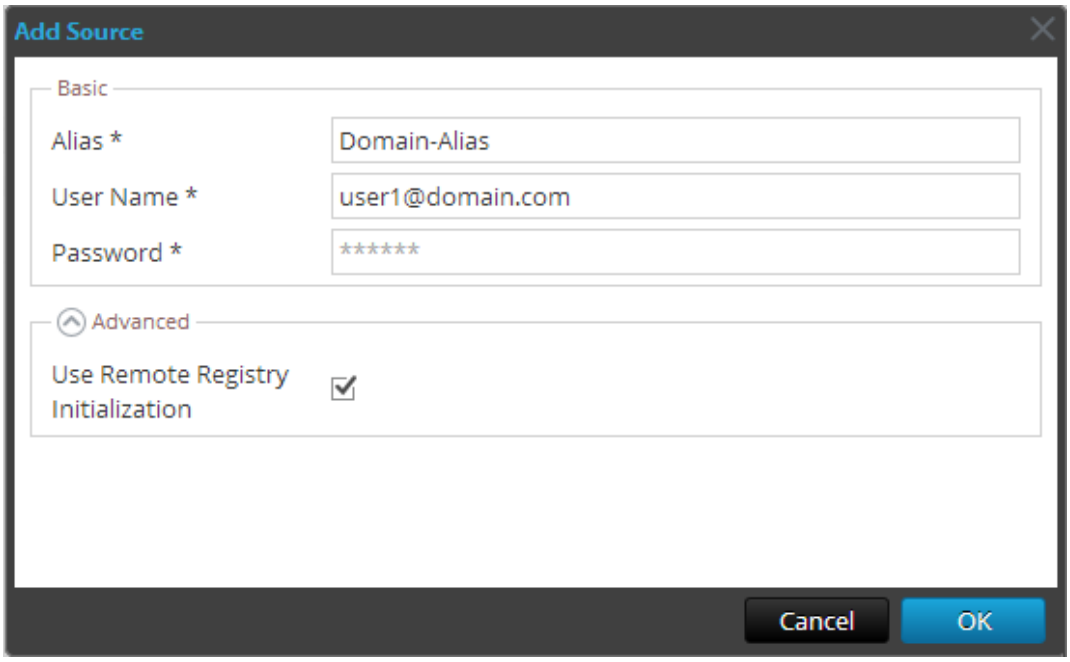
Conditions préalables

Avant de configurer une source d'événement Windows d'ancienne génération, vérifiez les points suivants :

1. Le collecteur distant Windows d'ancienne génération de NetWitness Suite est installé sur un serveur physique ou virtuel Windows 2008 64 bits.
2. Le collecteur distant Windows d'ancienne génération a été ajouté à NetWitness Suite.

Ajouter une source d'événements Windows d'ancienne génération.

1. Pour accéder à la vue Services, cliquez sur le menu NetWitness Suite et sélectionnez **Admin > Services**.
2. Dans la grille **Services**, sélectionnez le service **Windows d'ancienne génération Log Decoder**.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. Cliquez sur l'onglet **Sources d'événements**.
5. Sous l'onglet **Sources d'événements**, sélectionnez l'une des options suivantes dans le menu déroulant.
   - Windows d'ancienne génération/Windows.
   - Windows d'ancienne génération/NetApp.
6. Configurer l'alias :
   a. Cliquez sur  dans la barre d'outils du panneau **Catégories d'événements**.
   La boîte de dialogue **Ajouter une source** s'affiche.
   b. Spécifiez des valeurs de paramétrage, puis cliquez sur **OK**.



Remarque : Par défaut, l'**Initialisation de registre à distance** est sélectionnée. Pour plus d'informations, reportez-vous à la section Service de registre à distance ci-dessous.

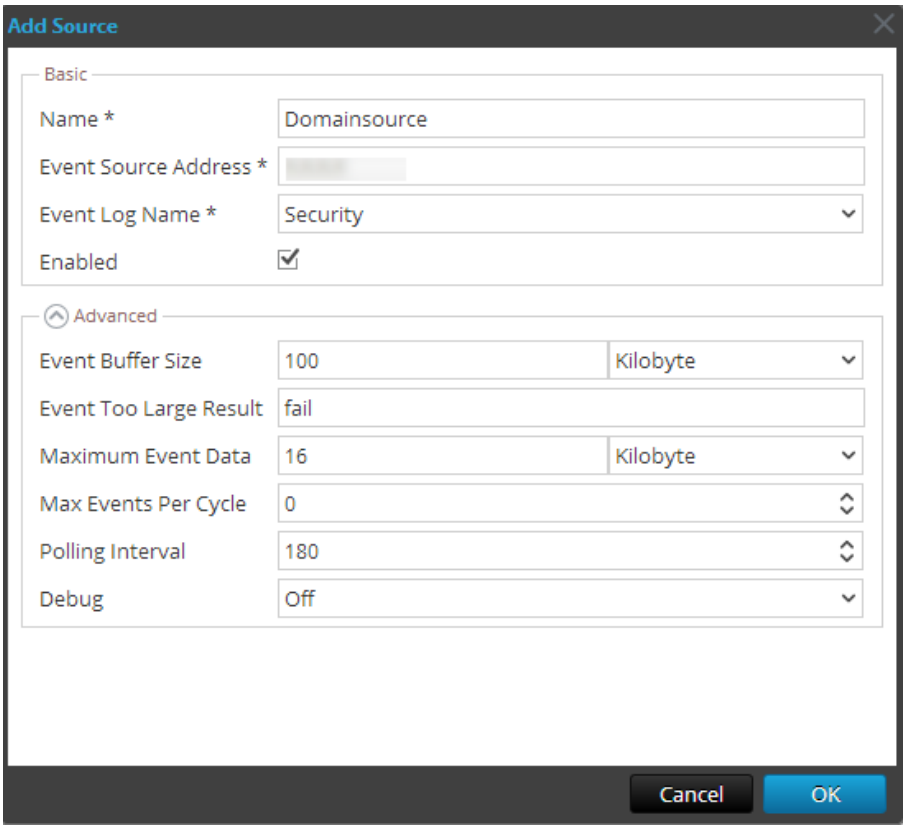
Le type de source d'événement Windows nouvellement ajouté s'affiche dans le panneau **Catégories d'événements**.

7. Ajouter la source de l'événement :

   a. Sélectionnez le nouvel alias dans le panneau **Catégories d'événements**, puis cliquez sur + dans la barre d'outils du panneau **Sources**.

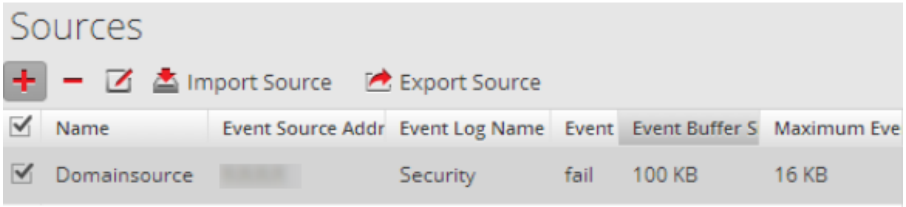
   La boîte de dialogue **Ajouter une source** s'affiche.

   b. Spécifiez les paramètres de la source d'événement, puis cliquez sur **OK**.



Pour plus d'informations, reportez-vous à la section Paramètres de Configuration de Windows d'ancienne génération ci-dessous.

La source d'événement Windows nouvellement ajoutée s'affiche dans le panneau **Catégories d'événements**.



Service de registre à distance

Le service Collector Windows d'ancienne génération effectue une vérification initiale de la source d'événement avant de collecter les données. Par défaut, le service Collector Windows d'ancienne génération utilise la méthode Windows Management Instrumentation (WMI) pour effectuer cette vérification initiale. Si vous activez la méthode Remote Registry Access, le service Collector Windows d'ancienne génération exécute une requête de registre distant pour vérifier la source d'événement.

Configurer la transmission ou l'extraction entre Log Collector et le collecteur Windows d'ancienne génération

Vous pouvez configurer le collecteur Windows d'ancienne génération pour transmettre les données d'événements à un collecteur local, ou vous pouvez configurer un collecteur local pour extraire les données d'événements du collecteur Windows d'ancienne génération.

Pour configurer un collecteur local ou le collecteur Windows d'ancienne génération :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez un collecteur local ou le service de collecte Windows d'ancienne génération.
3. Sous Actions, sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.
4. En fonction de votre sélection à l'étape 2 :
   - Si vous avez sélectionné un collecteur local, l'onglet **Collecteurs distants** s'affiche. Sélectionnez le collecteur Windows d'ancienne génération à partir duquel le collecteur local extrait les événements dans cet onglet.
   - Si vous sélectionnez un collecteur Windows d'ancienne génération, les **Collecteurs locaux** s'affichent. Sélectionnez les collecteurs locaux vers lesquels le collecteur Windows d'ancienne génération envoie des événements dans cet onglet.

Paramètres de Configuration de Windows d'ancienne génération

Le tableau suivant décrit les paramètres pour une source d'événement Windows d'ancienne génération.

Fonctionnalité	Description
	Basique
Nom*	Nom de la source de l'événement. La valeur valide est un nom compris dans la plage **[_a-zA-Z] [_a-zA-Z0-9]***. Vous pouvez utiliser un trait « **-** » comme partie du nom.
Adresse de la source d'événement*	Adresse IP de la source d'événement. Une valeur valide peut être une adresse IPv4, une adresse IPv6 ou un nom d'hôte comprenant un nom de domaine complet. NetWitness Suite par défaut est **127.0.0.1**. Log Collector convertit le nom d'hôte en lettres minuscules pour éviter les doublons.

Fonctionnalité	Description
Nom du log d'événements	Nom du log des événements à partir duquel collecter les données d'événements (par exemple, **Système**, **Application**, or **Sécurité**). Voici quelques exemples de canaux : • **Système** - applications qui s'exécutent sous des comptes de service système (services système installés), des pilotes, des composants ou des applications avec des événements liés à l'intégrité du système. • **Application** - toutes les applications de niveau utilisateur. Ce canal est non-sécurisé et reste ouvert à n'importe quelle application. Si une application comporte des informations détaillées, vous devez lui définir un canal qui lui est spécifique. • **Sécurité** - le journal d'audit Windows (log d'événements) utilisé exclusivement pour l'Autorité de sécurité locale de Windows.
Activé	Cochez cette case pour effectuer une collecte à partir de cette source d'événement. Si vous ne cochez pas cette case, le Log Collector ne collectera pas les événements de cette source d'événements.

Fonctionnalité	Description

Chemin d'accès au répertoire d'événements	Chemin du répertoire de fichiers NetApp **.evt ou .evtx**. Ce doit être le chemin UNC.
	NetApp génère des données d'événements et les enregistre dans des fichiers .evt ou .evtx au sein d'un répertoire qu'il est possible de partager sur l'appliance NetApp.
	• Lors de chaque cycle d'interrogation, Log Collector parcourt le chemin partagé NetApp qui a été configuré pour les fichiers .evt identifiés dans les paramètres **Chemin d'accès au répertoire d'événements** et **Préfixe des fichiers d'événements**. Log Collector :
	  ◦ trie les fichiers qui correspondent au format **event-file-prefix.YYMMDDhhmmss.evt**, par ordre croissant.
	  ◦ utilise l'horodatage du dernier fichier traité pour déterminer les fichiers qui doivent encore être traités. Si Log Collector trouve un fichier traité partiellement, il ignore les événements déjà traités.
	• Lors de chaque cycle d'interrogation, Log Collector parcourt le chemin partagé NetApp qui a été configuré jusqu'aux fichiers **.evtx** identifiés dans les paramètres **Chemin d'accès au répertoire d'événements** et **Préfixe des fichiers d'événements**. Log Collector :
	  ◦ trie les fichiers qui correspondent au format **event-file-prefix.AAMMJJhhmmss.evtx**, par ordre croissant.
	  ◦ utilise l'horodatage du dernier fichier traité pour déterminer les fichiers qui doivent encore être traités. Si Log Collector trouve un fichier traité partiellement, il ignore les événements déjà traités.

Préfixe des fichiers d'événements	Préfixe des fichiers **.evt** (par exemple, **adtlog.**) enregistrés au **Chemin d'accès au répertoire d'événements**.
Avancé	
Taille du tampon d'événement	Taille maximale des données que Log Collector extrait de la source d'événement pour chaque requête. La valeur valide est un nombre compris entre **0** et **511 kilo-octets**. Vous spécifiez cette valeur en **kilo-octets**.

Fonctionnalité	Description
Résultats des événements trop volumineux	Indique à Log Collector ce qu'il doit faire si un événement est trop volumineux pour le tampon d'événement.
Nombre maximal de données d'événements	Taille maximum des données d'événement à inclure dans la sortie. La valeur valide est un nombre compris entre **0** et **511 kilo-octets**. Vous spécifiez cette valeur en **kilo-octet**s ou **mégaoctets**. • 1 kilo-octet - 100 mégaoctets • 0 = n'inclut pas les données d'événements dans la sortie.
Nbre max. d'événements par cycle	Nombre maximal d'événements par cycle d'interrogation (nombre d'événements collectés par cycle d'interrogation).
Intervalle d'interrogation :	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est **180**. Par exemple, si vous spécifiez 180, le collecteur planifie une interrogation de la source d'événement toutes les 180 secondes. Si le cycle d'interrogation précédent est toujours en cours, il est nécessaire d'attendre qu'il se termine. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 180 secondes avant de démarrer, car les threads sont occupés.

Fonctionnalité	Description
Débogage	**Attention :** n'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire). Limitez le nombre de sources d'événements pour lesquelles vous utilisez le débogage Verbose pour réduire l'impact sur les performances.
Annuler	Ferme la boîte de dialogue sans ajouter la source d'événement Windows d'ancienne génération.
OK	Ajoute les valeurs de paramétrage actuelles en tant que nouvelle source d'événement

Dépannage de la collecte Windows d'ancienne génération et NetApp

Cette rubrique présente les problèmes potentiels que vous pouvez rencontrer lors de la collecte Windows d'ancienne génération (LWC) et propose des solutions à ces problèmes.

Remarque : En général, vous recevez davantage de messages log en désactivant le protocole SSL.

Problèmes de redémarrage du protocole

Problème	Causes possibles	Solutions
Vous redémarrez le protocole de collecte Windows d'ancienne génération, mais NetWitness Suite ne reçoit pas les événements.	Le service logcollector est arrêté.	Redémarrez le service **logcollector**. 1. Connectez-vous au **collecteur distant Windows d'ancienne génération**. 2. Accédez à **Démarrer > Outils d'administration > Planificateur de tâches**, puis cliquez sur **Bibliothèque du Planificateur de tâches**. 3. Dans le panneau de droite, recherchez la tâche **restartnwlogcollector** et assurez-vous qu'elle est en cours d'exécution. 4. Si ce n'est pas le cas, cliquez avec le bouton droit de la souris sur **restartnwlogcollector**, puis sélectionnez **Exécuter**.

Problèmes d'installation

Si vous voyez l'un des messages suivants dans le fichier **MessageBroker.log**, vous pouvez avoir des problèmes.

Messages de log	Tout message qui contient « rabbitmq »
Cause probable	Le service RabbitMQ peut ne pas être en cours d'exécution. Le port **5671** ne doit pas être ouvert.
Solutions	Assurez-vous que le service RabbitMQ est en cours d'exécution. Vérifiez que le port **5671** est ouvert.

Messages de log	Erreur : Ajout d'un compte utilisateur logcollector. Erreur : Ajout d'une balise administrateur au compte logcollector. Erreur : Ajout d'un vhost logcollection. Erreur : Définition des autorisations pour le compte logcollector dans tous les vhosts.
Cause probable	**rabbitmq-server** n'était pas en cours d'exécution lorsque le programme d'installation a tenté de créer des utilisateurs et des hôtes virtuels (vhosts).

Solutions	Assurez-vous que le service **RabbitMQ** est en cours d'exécution et exécutez les commandes ci-dessous manuellement.
	`rabbitmqctl -q add_user logcollector netwitness`
	`rabbitmqctl -q set_user_tags logcollector administrator`
	`rabbitmqctl -q add_vhost logcollection`
	`rabbitmqctl -q set_permissions -p / logcollector ".*" ".*" ".*"`
	`rabbitmqctl -q set_permissions -p logcollection logcollector ".*" ".*" ".*"`

Problèmes liés au script Federation sous Windows d'ancienne génération

Si l'un des messages suivants contenus dans le log de script Federation apparaît, c'est que vous rencontrez des problèmes.

Problème	Symptômes possibles	Solutions
Le script Federation a démarré, mais le service LWC est en panne.	Le log NetWitness Suite affiche des exceptions liées aux échecs de connexion avec le Collector Windows d'ancienne génération.	Ce problème se résout automatiquement au redémarrage du service Windows d'ancienne génération.

Problème	Symptômes possibles	Solutions

LWC est en cours d'exécution, mais le service RabbitMQ est en panne ou redémarre.	Le fichier log Federation côté Windows d'ancienne génération affiche un message d'erreur relatif à la panne du service RabbitMQ.
	Le fichier log à consulter est : **C:\NetWitness\ng\logcollector**
	Le message d'erreur suivant est consigné en cas d'exécution du service RabbitMQ :
	`"Unable to connect to node logcollector@localhost: nodedown"`
	Les messages de diagnostics suivants s'affichent :
	`attempted to contact: [logcollector@localhost]`
	`logcollector@localhost: * connected to epmd (port 4369) on localhost * epmd reports: node 'logcollector' not running at all other nodes on localhost: ['rabbitmqctl-4084'] * suggestion: start the node`
		Exécutez le script **federation.bat** manuellement sur LWC.
		Pour exécuter le script **federate.bat**, procédez comme suit :
		1. Accédez au dossier **C:\Program Files\NwLogCollector** où l'instance de Windows d'ancienne génération est installée.
		2. Recherchez le fichier **federate.bat** dans ce dossier. Sélectionnez le fichier, puis cliquez avec le bouton droit.
		3. Sélectionnez **Exécuter en tant qu'administrateur**.
		4. Pour surveiller le fichier log, accédez au fichier **C:\NetWitness\ng\logcollector\federate.log** lors de l'exécution du script **federate.bat**.
		Remarque : Vérifiez que le fichier log ne contient pas d'erreurs lors de l'exécution du script.

Le service RabbitMQ est en panne du côté NetWitness Suite.	Les pages de l'interface utilisateur de NetWitness Suite ne fonctionnent pas.	Redémarrez le service RabbitMQ.

Problème	Symptômes possibles	Solutions
Le client reçoit une notification d'intégrité, ou l'alarme d'intégrité suivante s'affiche : « Échec de communication entre l'hôte NetWitness Suite principal et un hôte distant » avec l'hôte LWC en tant qu'adresse IP distante.	Le script **Federate.bat** n'a pas pu être exécuté correctement.	Si le script **federate.bat** ne s'est pas exécuté correctement, exécutez-le manuellement comme décrit précédemment.

Windows Log Collection pour les agents Endpoint

Dans la version 11.1, la collecte des fichiers log Windows peut être réalisée à l'aide de l'agent RSA® NetWitness Endpoint Insights. Lorsque l'agent est activé pour la collecte des fichiers log, un fichier de configuration des logs est fourni avec le Packager d'agent permettant d'activer la collecte et le transfert des fichiers log Windows en plus des données Endpoint. Le fichier de configuration généré contient des informations sur les canaux à partir desquels les logs doivent être collectés (source et destination) (Log Decoder ou Remote Log Collector) pour transférer les événements Windows définis. Le packager d'agent généré est en mesure de collecter à la fois les données des fichiers log Endpoint et Windows à partir des hôtes. Le packager d'agent Endpoint est extrait localement sur une machine Windows pour créer le fichier d'installation de l'agent. Le fichier du programme d'installation est ensuite déployé via un outil de distribution de logiciels tiers pour tous les points de terminaison de votre réseau.

Il existe trois scénarios pour la collecte de fichiers log Windows :

- **Générer l'agent avec Log Collection**: si l'option **Activer Windows Log Collection** est activée et que vous cliquez sur **Générer un agent** après avoir fourni les informations

requises. Le fichier AgentPackager.zip généré contient le fichier de collecte de logs. Pour plus d'informations, consultez la section « Génération d'un packager d'agent avec Windows Log Collection » dans le *Guide d'installation de l'agent Endpoint Insights*.

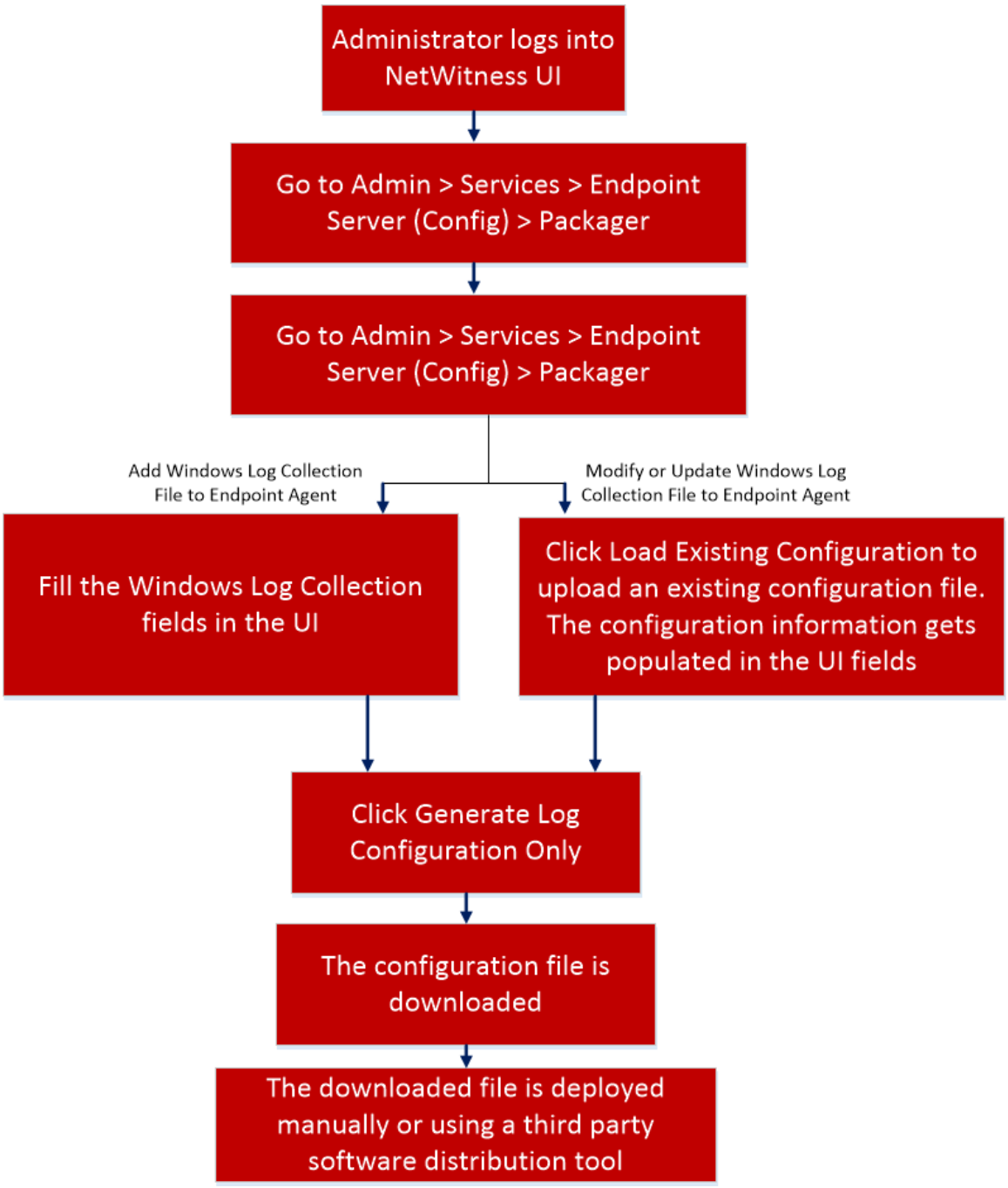
- **Générer le fichier Agent uniquement sans collecte de fichiers log** : Si l'option **Activer Windows Log Collection** est désactivée et que vous cliquez sur **Générer l'agent**, alors seul le fichier zip est créé sans le fichier de collecte de logs. Pour plus d'informations, consultez la section « Générer un packager d'agent Endpoint » dans le *Guide d'installation de l'agent Endpoint Insights*.
- Si vous cliquez sur **Générer uniquement la configuration du journal**, alors seule la configuration du log est créée. Cela peut permettre de mettre à jour le fichier de configuration de log dans un déploiement d'agent Endpoint existant pour la collecte de logs ou pour ajouter la configuration de log à un déploiement d'agent Endpoint. Pour plus d'informations, reportez-vous à la section « Ajouter la configuration de Windows Log Collection à un agent Endpoint installé ou la mettre à jour ».

Ajouter la configuration de Windows Log Collection à un agent Endpoint installé ou la mettre à jour

Vous pouvez ajouter un fichier de configuration de Windows Log Collection à un agent Endpoint, mais aussi modifier un fichier de configuration existant. Si une modification est requise dans la configuration de la collecte de logs pour les agents Endpoint, les agents n'ont pas besoin d'être réinstallés. Le fichier de configuration du log (`nwelcfg file`) peut être généré à partir de l'interface utilisateur du Packager et modifié.

Workflow

Ce workflow montre la procédure d'ajout ou de mise à jour d'un fichier de configuration de Windows Log Collection.



Voici quelques exemples de raisons qui nécessiteraient une modification de la configuration :

- La destination vers laquelle les fenêtres doivent être transférées doit être modifiée pour une meilleure gestion de la charge du côté destination.

- Le point de terminaison est déplacé vers un nouveau groupe défini par un système de gestion des points de terminaison tiers nécessitant une modification de la destination ou de la liste des ID d'événement à transférer.
- Il existe des conditions requises pour modifier la liste des ID d'événement utilisés du côté destination.

Un nouveau fichier de configuration peut être généré en entrant les nouvelles valeurs dans l'écran Packager, ou en chargeant un fichier de configuration existant.

Remarque : L'agent Endpoint est conçu pour lire le fichier `nwelcfg` avec le dernier horodatage sous le dossier config. Par conséquent, assurez-vous que l'outil de gestion des points de terminaison tiers actualise l'horodatage du fichier en fonction de l'heure du point de terminaison tout en transmettant le fichier de configuration.

Suivez ces étapes pour ajouter un fichier de configuration de Windows Log Collection à un agent Endpoint existant, ou le mettre à jour :

1. Dans l'interface utilisateur du Packager, effectuez l'une des opérations suivantes :
   a. Pour ajouter la configuration de Windows Log Collection : Fournissez les informations requises mentionnées dans la section « Génération d'un packager d'agent avec Windows Log Collection » dans le *Guide d'installation de l'agent Endpoint Insights*.
   b. Pour mettre à jour la configuration de Windows Log Collection : cliquez sur **Charger la configuration existante** et modifiez les champs prévus mentionnés sous « Génération d'un packager d'agent avec Windows Log Collection » dans le *Guide d'installation de l'agent Endpoint Insights*.
2. Cliquez sur **Générer uniquement la configuration du journal** pour générer le fichier `nwelcfg`.
3. Copiez le fichier `nwelcfg` téléchargé dans l'agent Endpoint à partir duquel les fichiers log doivent être transférés. Le fichier de configuration doit être copié dans le dossier %ProgramData%\NWEAgent. Pour déployer le fichier de configuration sur plusieurs agents, utilisez l'outil de distribution de logiciels tiers.

L'agent est conçu pour sélectionner le fichier de configuration de log contenant le dernier horodatage. S'il existe une différence de fuseau horaire, vérifiez que le fichier de configuration est mis à jour en fonction de l'horodatage de l'agent après la copie. Pour cela, exécutez la commande sur l'agent : `copy /b <filename.nwelcfg> +,,` dans le dossier %programdata%\NWEAgent\ à l'emplacement du fichier nwelcfg.

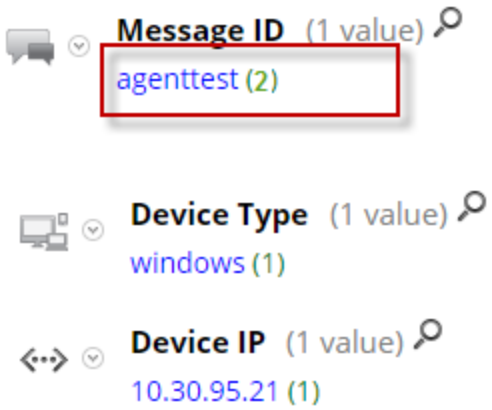
Vérifier Windows Log Collection

Pour vérifier que le déploiement de Windows Log Collection s'est effectué correctement sur un agent Endpoint, procédez comme suit :

1. Accédez à **ADMIN** > **Intégrité** > **Surveillance des sources d'événements**.
2. Dans le champ Période, sélectionnez **5 dernières minutes** ou **10 dernières minutes** en fonction du moment où les agents ont été installés.
3. Cliquez sur **Appliquer**.
4. Dans la liste affichée, l'adresse IP de l'agent doit être définie dans la colonne Source d'événement avec le Type de source d'événement Windows. Cela confirme que l'agent a été installé avec succès.

Pour vérifier que Windows Log Collection a été mis à jour avec succès, procédez comme suit :

1. Accédez à **ENQUÊTER** > **Naviguer**. Patientez 2 à 3 minutes pour que ce fichier de configuration soit sélectionné par l'agent Endpoint.
2. Sélectionnez le service **Concentrator** dans **Investigate**.
3. Changez la chronologie en sélectionnant **5 dernières minutes**, ou ce qui vous semblera approprié.
4. Cliquez sur **Charger les valeurs**.
5. Recherchez la clé méta de l'ID de message.
6. Elle doit contenir une valeur agent.test. Une augmentation du nombre d'événements signifie que la mise à jour s'est déroulée correctement.



Activer le transfert de logs et configurer Log Decoder

Vous pouvez activer la fonction de transfert de logs et configurer Log Decoder dans Endpoint Hybrid en tant que destination dans l'interface utilisateur du Packager. Ensuite, vous devez ajouter les ports TCP/UDP 514 dans le fichier iptables dans Endpoint Hybrid.

Suivez ces étapes pour ajouter les ports :

1. Pour le protocole TCP, vous devez ajouter le port « 514 » à la liste des ports du fichier `/etc/sysconfig/iptables` dans Endpoint Hybrid :

   ```
   INPUT -p tcp -m tcp -m multiport --dports 514,
   6514,50002,50102,50202,56002,56202 -m comment --comment
   "nwlogdecoderPorts" -m conntrack --ctstate NEW -j ACCEPT -
   ```

2. Pour le protocole UDP, vous devez ajouter le contenu ci-dessous dans le fichier `/etc/sysconfig/iptables` dans Endpoint Hybrid :

   ```
   -A INPUT -p udp -m udp -m multiport --dports 514 -m comment --comment
   "nwlogcollectorUdpPorts" -m conntrack --ctstate NEW -j ACCEPT
   ```

3. Redémarrez le service iptables pour que les nouvelles configurations ci-dessus prennent effet : `service iptables restart`.

Rubriques connexes

Résolution des problèmes - Windows Log Collection utilisant un agent Endpoint

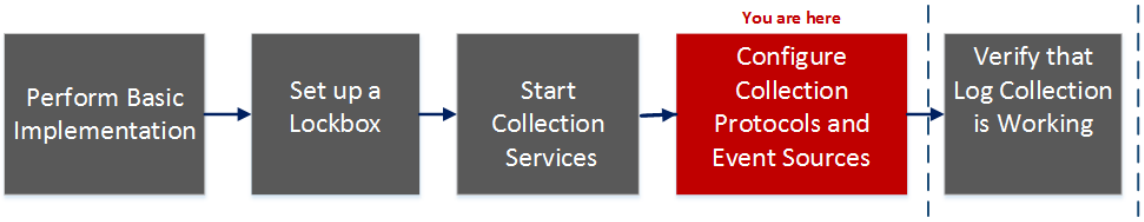
Référence

Paramètres AWS

Cette rubrique fournit une vue d'ensemble de paramètres de configuration de la collecte AWS pour le déploiement d'un service de collecte de logs à distance (VLC) dans un environnement Amazon Web Services (AWS).

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Configurer des sources d'événements AWS (CloudTrail) dans NetWitness Suite

Le tableau ci-dessous décrit les paramètres de configuration disponibles pour la collecte AWS.

Paramètre	Description
Paramètre	**Description**
	Basique
Nom *	Nom de la source d'événement.
Activé	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
ID de compte *	Code d'identification de compte du Bucket S3

Paramètre	Description
Nom de compartiment S3 *	Nom de compartiment S3 AWS (CloudTrail). Les noms de Buckets S3 Amazon sont globalement uniques, quelle que soit la région AWS (CloudTrail) dans laquelle vous créez le bucket. Vous spécifiez le nom au moment de la création du bucket. Les noms de buckets doivent se conformer aux conventions de dénomination DNS. Les règles pour les noms de bucket compatibles DNS sont les suivantes : • Les noms de bucket doivent comprendre entre 3 et 63 caractères. • Les noms de bucket doivent être une série d'un ou de plusieurs libellés. Les libellés adjacents sont séparés par un seul point « . ». Les noms de buckets contiennent des lettres minuscules, des chiffres et des tirets. Chaque libellé doit commencer et se terminer par une lettre minuscule ou un chiffre. • Les noms de buckets ne doivent pas être formatés comme une adresse IP (par exemple, 192.168.5.4). Les exemples suivants sont des noms de buckets **valides** : • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** Les exemples suivants sont des noms de buckets **non valides** : • **.myawsbucket** - Un nom de bucket ne doit pas commencer par un point « . ». • **myawsbucket.** - Ne pas terminer un nom de bucket par un point « . ». • **my..examplebucket** - N'utilisez qu'un seul point entre les libellés.
Clé d'accès *	Clé utilisée pour accéder au bucket S3. Les clés d'accès sont utilisées pour garantir la sécurité de requêtes de protocole REST ou Requête sur n'importe quelle API de service AWS. Veuillez vous reporter à Gérer les informations d'identification sur le site de support Amazon Web Services pour plus d'informations sur les clés d'accès.
Clé secrète *	Clé secrète utilisée pour accéder au bucket S3.
Région *	Région du bucket S3. **us-east-1** est la valeur par défaut.

Paramètre	Description
Point de terminaison de la région	Spécifie le nom d'hôte CloudTrail AWS. Par exemple, pour un Cloud public AWS pour la région us-east, le point de terminaison de la région serait s3.amazonaws.com. Pour plus d'informations , vous référez à http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. Ce paramètre est nécessaire pour collecter les logs de CloudTrail à partir de Clouds AWS administratifs ou privés.
Utiliser le proxy	Activer **Utiliser le proxy** pour définir le proxy du serveur AWS. Il est désactivé par défaut,.
Serveur proxy	Saisissez le nom de proxy que vous souhaitez connecter pour accéder au serveur AWS.
Port proxy	Saisissez le numéro de port qui se connecte au serveur proxy pour accéder à serveur AWS.
Utilisateur proxy	Saisissez le nom d'utilisateur permettant de s'authentifier auprès du serveur proxy.
Mot de passe du proxy	Saisissez le mot de passe permettant de s'authentifier auprès du port proxy.
Date de début *	Démarre la collecte AWS (CloudTrail) depuis le nombre de jours spécifié dans le passé, mesuré à partir de l'horodatage actuel. La valeur par défaut est 0, ce qui démarre à partir d'aujourd'hui. La valeur est comprise entre 0 et 89 jours.
Préfixe de fichier log	Le préfixe des fichiers à traiter. **Remarque :** Si vous définissez un préfixe lorsque vous configurez votre service CloudTrail, assurez-vous de saisir le même préfixe dans ce paramètre.
Avancé	

Paramètre	Description
Débogage	**Attention :** n'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).
Arguments de commande	Arguments ajoutés au script.
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est 60. Par exemple, si vous spécifiez 60, le collecteur planifie une interrogation de la source d'événement toutes les 60 secondes. Si le cycle d'interrogation précédent est toujours en cours, il est nécessaire d'attendre qu'il se termine. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 60 secondes avant de démarrer car les threads sont occupés.
SSL activé 	Cochez la case permettant de communiquer en utilisant SSL. La sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL. Cette case à cocher est activée par défaut.

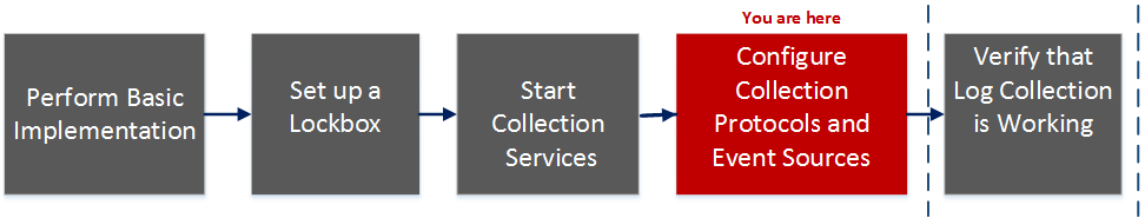
Paramètre	Description
Tester la connexion	Valide que les paramètres de configuration spécifiés dans cette boîte de dialogue sont corrects. Par exemple, ce test valide les points suivants : • NetWitness peut se connecter au Bucket S3 dans AWS en utilisant les informations d'identification spécifiées dans cette boîte de dialogue. • NetWitness peut télécharger un fichier log depuis le bucket (la connexion test échouera s'il n'y a pas de fichiers logs pour l'ensemble du bucket, mais cela est extrêmement improbable).
Annuler	Ferme la boîte de dialogue sans ajouter l'AWS (CloudTrail).
OK	Ajoute les valeurs de paramétrage actuelles en tant que nouvel AWS (CloudTrail).

Paramètres Azure

Microsoft Azure est une plateforme et une infrastructure de Cloud computing permettant la conception, le déploiement et la gestion des applications et services via un réseau global de datacenters gérés par Microsoft.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Configurer des Sources d'événements Azure dans NetWitness Suite

Paramètres de configuration des sources d'événements Azure

Cette rubrique décrit les paramètres de configuration des sources d'événements Azure.

Remarque : Les éléments suivis d'un astérisque (*) sont obligatoires.

Paramètres de base

Nom	Description
Nom *	Saisissez un nom descriptif, alphanumérique pour la source. Cette valeur est uniquement utilisée pour afficher le nom sur cet écran.
Activé	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
ID client *	L'ID client se trouve dans l'onglet Configurer les applications Azure. Faites défiler vers le bas jusqu'à ce qu'il s'affiche.
Code secret client *	Lorsque de la configuration de la source d'événement, le code secret du client s'affiche lorsque vous créez une clé et que vous sélectionnez une durée de validation. Veillez à bien l'enregistrer, car cette information ne sera affichée qu'une seule fois et ne peut pas être récupérée ultérieurement.
URL de base des ressources API *	Saisissez `https://management.azure.com/`. Veillez à inclure la barre oblique de fin (/).
Point de terminaison des métadonnées de fédération *	Dans votre application Azure, cliquez sur le bouton **Afficher les points de terminaison** (au bas du volet). Un grand nombre de liens commencent tous par la même chaîne. Comparez les URL et identifiez la chaîne commune par laquelle commence la plupart d'entre eux. Cette chaîne commune est le point de terminaison que vous devez saisir ici.
ID d'abonnement *	Vous pouvez le trouver dans le tableau de bord Microsoft Azure : cliquez sur Abonnements au bas de la liste sur la gauche.
Domaine du tenant *	Accédez à Active Directory, puis cliquez sur le répertoire. Dans l'URL, le domaine du tenant est la chaîne qui suit directement **manage.windowsazure.com/**. Le domaine du tenant est la chaîne allant jusqu'à **.com**, inclus.

Nom	Description
Noms des groupes de ressources *	Dans Azure, sélectionnez Groupes de ressources dans le volet de navigation de gauche, puis sélectionnez votre groupe.
Date de début *	Choisissez la date du début de la collecte. La date du jour est définie par défaut.
Tester la connexion	Vérifiez les paramètres de configuration spécifiés dans cette boîte de dialogue pour vous assurer qu'ils sont corrects.

Paramètres avancés

Cliquez sur  à côté d'**Avancé** pour afficher et modifier les paramètres avancés, si nécessaire.

Nom	Description
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est **180**. Par exemple, si vous spécifiez 180, le collecteur planifie une interrogation de la source d'événement toutes les 180 secondes. Si le cycle d'interrogation précédent est toujours en cours, le collecteur attend la fin de l'opération. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 180 secondes avant de démarrer, car les threads sont occupés.
Nb max. d'interrogations de durées	Durée maximale, en secondes, d'un cycle d'interrogation. La valeur zéro indique aucune limite.
Nb max. d'interrogations d'événements	Nombre maximal d'événements par cycle d'interrogation (nombre d'événements collectés par cycle d'interrogation).
Nb max. d'interrogations liées au délai de mise en veille	Durée maximale, en secondes, d'un cycle d'interrogation. La valeur zéro indique aucune limite.
Arguments de commande	Arguments facultatifs à ajouter à l'appel de script.

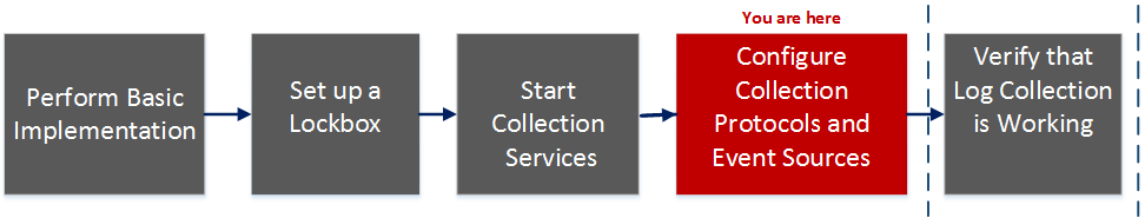
Nom	Description
Débogage	**Attention :** n'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. **Attention :** Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire). La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances.

Paramètres Check Point

Le protocole de collecte Check Point collecte des événements issus des sources d'événements Check Point à l'aide d'OPSEC LEA. OPSEC LEA est l'API Check Point Operations Security Log Export qui facilite l'extraction des fichiers log.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Configurer des sources d'événement Check Point dans NetWitness Suite

Paramètres de configuration de collecte Check Point

Paramètres de base

Paramètre	Description
Nom*	Nom de la source d'événement.
Adresse*	Adresse IP du serveur Check Point.
Nom du serveur*	Nom du serveur Check Point.
Nom du certificat	Nom du certificat des connexions sécurité à utiliser lorsque le mode de transport est de type https. S'il est configuré, le certificat doit être présent dans le magasin de certificats de confiance que vous avez créé via l'onglet Paramètres. Sélectionnez un certificat dans la liste déroulante. La convention de dénomination des fichiers pour les certificats de source d'événements Check Point est **checkpoint_*nom-de-la-source-d'événement***.
Client unique	Saisissez le nom unique du client sur le serveur Check Point.
Nom d'entité de client	Saisissez le nom d'entité de client sur le serveur Check Point.
Serveur unique	Saisissez le nom unique du serveur sur le serveur Check Point.
Activé	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
Extraire le certificat	Cochez la case permettant d'extraire un certificat pour la première fois. L'extraction d'un certificat le rend disponible auprès du magasin de certificats de confiance.

Paramètre	Description
Adresse du serveur de certificat	Adresse IP du serveur sur lequel réside le certificat. Par défaut, l'adresse de la source d'événement.
Mot de passe	Actif uniquement lorsque vous cochez la case Extraire le certificat pour la première fois. Mot de passe requis pour extraire le certificat. Le mot de passe est la clé d'activation créée lors de l'ajout d'une application OPSEC à Check Point sur le serveur Check Point.

Déterminer les valeurs des paramètres avancés pour la collecte Check Point

Vous utilisez moins de ressources système lorsque vous configurez une connexion de source d'événements Check Point afin qu'elle reste ouverte pendant une période spécifique et un volume d'événement spécifique (connexion transitoire). RSA NetWitness Suite utilise les paramètres de connexion par défaut suivants pour établir une connexion transitoire :

- Intervalle d'interrogation = **180** (3 minutes)
- Nb max. d'interrogations de durées = **120** (2 minutes)
- Nb max. d'interrogations d'événements = **5 000** (5 000 événements par intervalle d'interrogation)
- Nb max. d'interrogations liées au délai de mise en veille = **0**

Pour les sources d'événements Check Point très actives, nous vous recommandons de configurer une connexion qui reste ouverte jusqu'à ce que vous l'arrêtiez (connexion permanente). Cela garantit que la collecte Check Point maintient le rythme des événements générés par ces sources d'événements actives. La connexion permanente évite les délais de redémarrage et de connexion et empêche que la collecte Check Point soit retardée par la génération d'événements.

Pour établir une connexion permanente pour une source d'événements Check Point, définissez les paramètres de valeurs suivants :

- Intervalle d'interrogation = **-1**
- Nb max. d'interrogations de durées = **0**
- Nb max. d'interrogations d'événements = **0**
- Nb max. d'interrogations liées au délai de mise en veille = **0**

Paramètre	Description
Port	Port du serveur Check Point auquel Log Collector se connecte. La valeur par défaut est 18184.
Type de log de collecte	Type de logs que vous souhaitez collecter. Les valeurs autorisées sont les suivantes : • **Audit** - collecte les événements d'audit. • **Sécurité** - collecte les événements de sécurité. Si vous souhaitez collecter à la fois les événements d'audit et de sécurité, vous devez créer une source d'événements dupliquée. À titre d'exemple, vous créez d'abord une source d'événements avec l'option Audit sélectionnée afin d'extraire un certificat dans le magasin de certificats de confiance pour cette source d'événements. Ensuite, vous créez une autre source d'événements avec les mêmes valeurs, sauf que vous sélectionnez Sécurité comme Type de log de collecte et vous choisissez le même certificat dans le Nom du certificat que celui extrait lors de la configuration des premiers paramètres pour cette source d'événements, et vous vous assurez que Extraire le certificat n'est pas sélectionné.
Collecter les logs de	Lorsque vous configurez une source d'événements Check Point, NetWitness collecte les événements à partir du fichier de log actuel. Les valeurs autorisées sont les suivantes : • **Maintenant** - démarre la collecte des logs maintenant (à un point donné dans le fichier log actuel). • **Début du log** - collecte les logs depuis le début du fichier log actuel. Si vous choisissez « Début du log » pour cette valeur de paramètre, vous risquez de collecter une très grande quantité de données, qui dépend du temps pendant lequel le fichier log actuel a collecté les événements. Notez que cette option est utile uniquement pour la première session de collecte.
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est **180**. Par exemple, si vous spécifiez 180, le collecteur planifie une interrogation de la source d'événement toutes les 180 secondes. Si le cycle d'interrogation précédent est toujours en cours, il est nécessaire d'attendre qu'il se termine. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 180 secondes avant de démarrer car les threads sont occupés.

Paramètre	Description
Nb max. d'interrogations de durées	Durée maximale du cycle d'interrogation en secondes.
Nb max. d'interrogations d'événements	Nombre maximal d'événements par cycle d'interrogation (nombre d'événements collectés par cycle d'interrogation).
Nb max. d'interrogations liées au délai de mise en veille	Délai de mise en veille maximal, en secondes, d'un cycle d'interrogation. 0 indique aucune limite. **> 300** est la valeur par défaut.
Redirecteur	Active ou désactive le serveur Check Point comme un service de transfert. Il est désactivé par défaut.
Type de log (paire Nom-Valeur)	Logs de la source de l'événement au format de la valeur de nom valeur. Il est désactivé par défaut.

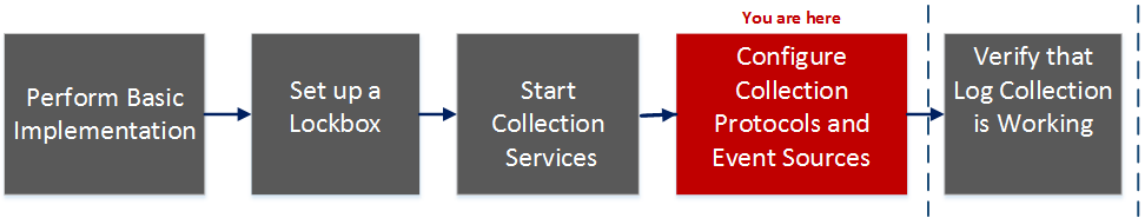
Paramètre	Description
Débogage	**Attention :** N'activez le débogage (paramètre défini sur « On » ou « Verbose ») que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active et désactive la consignation du débogage pour la source d'événements. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).

Paramètres du fichier

Cette rubrique décrit les paramètres de configuration de la collecte de fichiers.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Configurer des sources d'événements de fichiers dans NetWitness Suite

Paramètres de source d'événements de collecte de fichiers

Le tableau suivant fournit des descriptions des paramètres de la source de collecte de fichiers.

Nom	Description
	Basique
Répertoire de fichiers*	Répertoire de collecte (par exemple **Eur_London100**) dans lequel la source d'événement de fichiers place ses fichiers. Toute chaîne de caractères conforme à l'expression régulière suivante est une valeur valide : **[_a-zA-Z][_a-zA-Z0-9]*** Cela signifie que le répertoire de fichiers doit commencer par une lettre suivie de chiffres, de lettres et de traits de soulignement. Ne modifiez pas ce paramètre après avoir démarré la collecte de données d'événements. Une fois que vous avez créé la collecte, Log Collector crée les sous-répertoires de travail, d'enregistrement et d'erreur dans le répertoire de collecte.
Adresse*	Adresse IP de la source d'événement. La valeur valide est une **adresse IPv4**, une **adresse IPv6** ou un **nom d'hôte** comprenant un nom de domaine complet.
Spéc. fichier	Expression régulière. Par exemple, **^.*$** = tout traiter.
Encodage de fichier	Encodage de fichier pour l'internationalisation. Saisissez la méthode d'encodage de fichier. Les chaînes suivantes sont des exemples de méthodes valides : • UTF-8 (valeur par défaut) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFTJIS • EBCDICUS
Enabled	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
	Avancé

Nom	Description
Ignorer les erreurs de conversion de chiffrement	Activez cette case à cocher pour ignorer les erreurs de conversion de chiffrement et les données non valides. Cette case à cocher est activée par défaut. **Attention :** Cela peut provoquer des erreurs d'analyse et de transformation.
Quota des disques de fichiers	Détermine le moment où l'enregistrement des fichiers doit être arrêté, indépendamment des paramètres **Enregistrer en cas d'erreur** et **Enregistrer en cas de réussite**. Par exemple, la valeur 10 indique que lorsqu'il reste moins de 10 % d'espace disque disponible, Log Collector cesse d'enregistrer les fichiers afin de réserver suffisamment d'espace pour le traitement normal de la collecte. **Attention :** L'espace disque disponible fait référence à une partition de montage du répertoire de collecte de base. Si le serveur Log Decoder a un disque de 10 To, et si 2 To sont alloués au répertoire de collecte de base, l'affectation de la valeur 10 à ce paramètre entraîne l'arrêt de la collecte des logs lorsqu'il reste moins de 0,2 To (10 % de 2 To) d'espace. Cela ne signifie pas 10 % de 10 To. La valeur valide est un nombre compris entre **0** et **100**. **10** est la valeur par défaut.
Traitement séquentiel	Balise de traitement séquentiel : • Activez la case à cocher (par défaut) pour traiter les fichiers de sources d'événements dans l'ordre de collecte. • Désactivez la case à cocher pour traiter les fichiers de sources d'événements en parallèle.
Enregistrer en cas d'erreur	Balise d'enregistrement en cas d'erreur. Activez la case à cocher pour conserver le fichier de **collecte eventsource** lorsque Log Collector rencontre une erreur. Cette case à cocher est activée par défaut.
Enregistrer en cas de réussite	Balise d'enregistrement du fichier de **collecte eventsource** après traitement. Activez la case à cocher pour enregistrer le fichier de collecte eventsource, une fois qu'il a été traité. Par défaut, l'option n'est pas sélectionnée.

Nom	Description
Clé SSH Eventsource	Clé publique SSH utilisée pour télécharger les fichiers de cette source d'événement. Pour obtenir des instructions sur la génération de clés, consultez la section *Générer la paire de clés sur la source de l'événement et importer la clé publique dans Log Collector*, dans le Guide d'installation et de mise à jour d'un agent SFTP. **Remarque :** Si la collecte de fichiers est arrêtée, NetWitness Suite ne met pas à jour le fichier authorized_keys avec la clé publique SSH que vous ajoutez ou modifiez dans ce paramètre. Vous devez redémarrer la collecte de fichiers pour mettre à jour la clé publique. Vous pouvez ajouter ou modifier la valeur de la clé publique dans ce paramètre pour plusieurs sources d'événements de fichiers lorsque la collecte de fichiers n'est pas en cours d'exécution. Toutefois, NetWitness Suite ne met pas à jour le fichier **authorized_keys** tant que la collecte de fichiers n'a pas redémarré.
Gérer les fichiers d'erreurs	Par défaut, Log Collectorutilise le paramètre **Quota des disques de fichiers** pour vérifier que le disque ne dépasse pas sa limite de remplissage avec des fichiers d'erreurs. Si vous affectez **vrai** à ce paramètre, vous pouvez spécifier l'une des valeurs suivantes : • espace maximal alloué aux fichiers d'erreurs dans le paramètre **Taille des fichiers d'erreurs** ; • nombre maximal de fichiers d'erreurs autorisés dans le paramètre **Nombre de fichiers d'erreur**. Un pourcentage de réduction est également spécifié, ce qui indique au système le taux de réduction à appliquer lorsque le seuil maximal est atteint. Activez la case à cocher pour gérer les fichiers d'erreurs. Par défaut, l'option n'est pas sélectionnée.
Taille des fichiers d'erreurs	Valide uniquement si les paramètres **Gérer les fichiers d'erreurs** et **Enregistrer en cas d'erreur** ont la valeur vrai. Spécifie la limite dans laquelle NetWitness Suite enregistre les fichiers d'erreurs. La valeur que vous spécifiez correspond à la taille totale maximale de tous les fichiers dans le répertoire d'erreurs. La valeur valide est un nombre compris entre **0** et **281 474 976 710 655**. Vous devez spécifier ces valeurs en **Kiloœctets**, **Mégaoctets** ou **Gigaoctets**. **100 Mo** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.

Nom	Description
Nombre de fichiers d'erreurs	Valide uniquement si les paramètres **Gérer les fichiers d'erreurs** et **Enregistrer en cas d'erreur** ont la valeur vrai. Nombre maximal de fichiers d'erreurs autorisés dans le répertoire d'erreurs. La valeur valide est un nombre compris entre **0** et **65536**. **65536** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.
% de réduction des fichiers d'erreurs	Valeur en pourcentage de la taille ou du nombre de fichiers d'erreurs que le service Log Collectorsupprime lorsque la taille ou le nombre maximal a été atteint. Le service supprime les anciens fichiers en premier. La valeur valide est un nombre compris entre **0** et **100**. **10** est la valeur par défaut.
Gérer les fichiers enregistrés	Activez la case à cocher pour gérer les fichiers enregistrés. Par défaut, l'option n'est pas sélectionnée. Par défaut, Log Collector utilise le paramètre **Quota des disques de fichiers** pour vérifier que le disque ne dépasse pas sa limite de remplissage avec des fichiers enregistrés. Si vous activez cette case à cocher, vous pouvez spécifier l'une des valeurs suivantes : • espace maximal alloué aux fichiers enregistrés dans le paramètre **Taille des fichiers enregistrés** ; • nombre maximal de fichiers enregistrés autorisés dans le paramètre **Nombre de fichiers enregistrés**. Un pourcentage de réduction est également spécifié, ce qui indique au système le taux de réduction à appliquer lorsque le seuil maximal est atteint.
Taille des fichiers enregistrés	Valide uniquement si les paramètres **Gérer les fichiers enregistrés** et **Enregistrer en cas de réussite** ont la valeur vrai. Taille totale maximale de tous les fichiers dans le répertoire d'enregistrement. La valeur valide est un nombre compris entre **0** et **281474976710655**. Vous devez spécifier ces valeurs en **Kiloœctets**, **Mégaoctets** ou **Gigaoctets**. **100 Mo** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.

Nom	Description
Nombre de fichiers enregistrés	Valide uniquement si les paramètres **Gérer les fichiers enregistrés** et **Enregistrer en cas de réussite** ont la valeur vrai. Nombre maximal de fichiers enregistrés autorisés dans le répertoire d'enregistrement. La valeur valide est un nombre compris entre **0** et **65536**. **65536** est la valeur par défaut. Si vous modifiez ce paramètre, le changement ne prendra effet qu'au redémarrage de la collecte ou du service Log Collector.
% de réduction des fichiers enregistrés	Valeur en pourcentage de la taille ou du nombre de fichiers enregistrés que le service Log Collector supprime lorsque la taille ou le nombre maximal a été atteint. Le service supprime les anciens fichiers en premier. La valeur valide est un nombre compris entre **0** et **100**. **10** est la valeur par défaut.
Débogage	**Attention :** N'activez le débogage (paramètre défini sur **On** ou **Verbose**) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collectorde manière défavorable. Active/désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire).
Annuler	Ferme la boîte de dialogue sans ajouter de type de source d'événement.
OK	Ajoute les paramètres de la source d'événement.

Vue Log Collection Service System

Un Log Collector est un service qui s'exécute sur un hôte Log Decoder (appelé Local Collector) ou envoie des événements depuis un Remote Collector vers un Local Collector. Il est configuré et géré de la même façon qu'un Log Decoder.

Pour accéder à la vue Log Collection Service System, accédez à ADMIN > Services, puis sélectionnez un service Log Collector, puis sélectionnez Vue > Système.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.

Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox	Configurer un Lockbox
Administrateur	*Démarrer les services Log Collection	Démarrer des services de collecte
Administrateur	Configurer les protocoles et les sources d'événements Log Collection.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

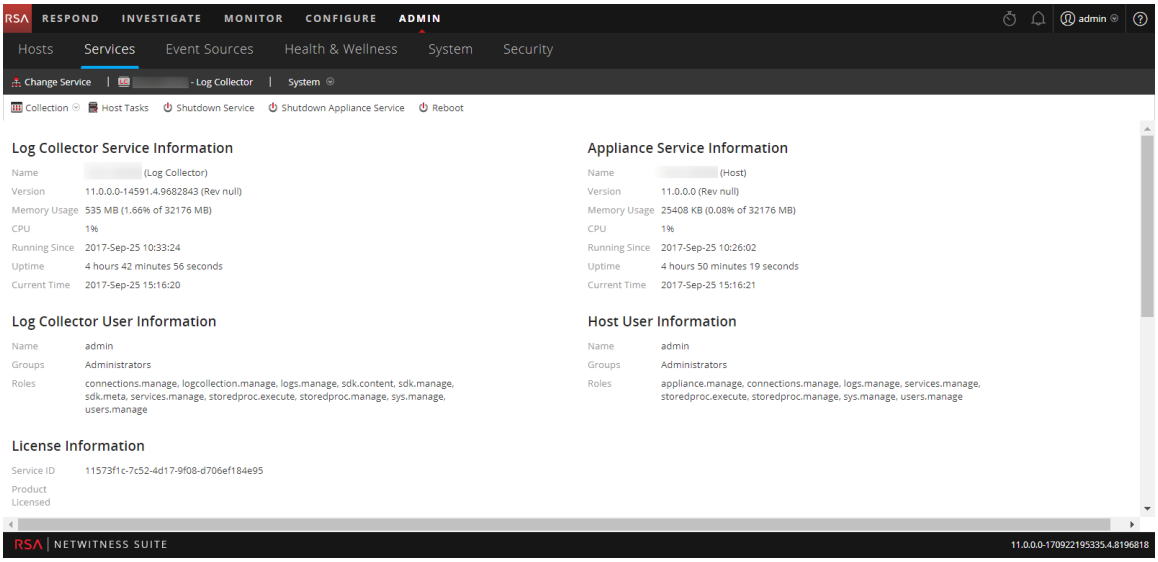
*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

Implémentation de base

Aperçu rapide

Dans la barre d'outils d'informations du service Log Collector, vous pouvez gérer les données d'événements à l'aide de l'icône Collecte pour lancer la collecte des données d'événements à partir d'un protocole arrêté ou arrêter la collecte des données à partir d'un protocole démarré. À partir de l'icône Tâches de l'hôte, vous pouvez sélectionner les tâches que vous souhaitez exécuter. Vous pouvez également arrêter et redémarrer votre service à partir de la barre d'outils d'informations du service.



Paramètres de configuration des sources d'événements ODBC

Cette rubrique vous indique comment configurer le protocole de collecte ODBC permettant de collecter les événements des sources d'événements qui stockent les données d'audit dans une base de données à l'aide de l'interface logicielle ODBC (Open Database Connectivity).

Accéder aux paramètres de configuration ODBC

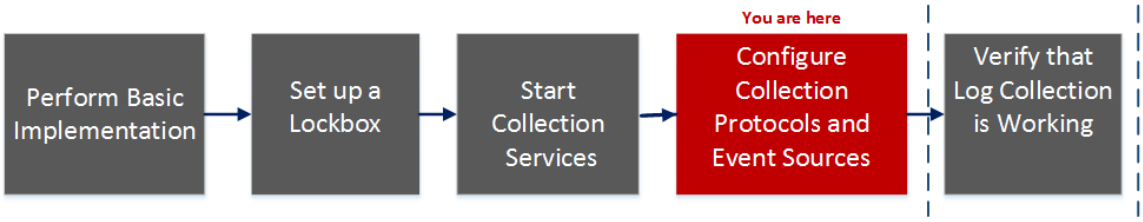
Pour accéder aux paramètres de configuration des sources d'événements ODBC :

1. Accédez à **Administration> Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez **Vue > Config** pour afficher les onglets des paramètres de configuration de la collecte de logs.

   La vue **Configuration des services** s'affiche avec l'onglet **Général** de Log Collector ouvert.
4. Cliquez sur l'onglet **Sources d'événements** et sélectionnez **ODBC/Config** dans le menu déroulant.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte

Rôle	Je souhaite...	Documentation
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Configurer des sources d'événements ODBC dans NetWitness Suite
- Configurer des noms de sources de données (DSN)
- Résoudre les problèmes liés à la collecte ODBC
- Créer un fichier typespec personnalisé pour la collecte ODBC

Paramètres de nom de source de données (DSN)

Utilisez le panneau Sources pour passer en revue, ajouter, modifier et supprimer des paramètres DSN (Data Source Name).

Panneau Sources

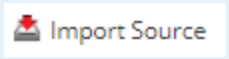
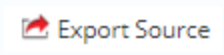
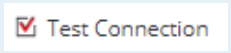
Le DSN ODBC indique au Log Collector comment atteindre un point d'extrémité ODBC. Vous faites référence à un DSN ODBC lorsque vous configurez un nom de source de données avec des informations comme le pilote ODBC à utiliser ou le nom d'hôte et le port du point d'extrémité ODBC.

Un DSN ODBC est une séquence de paires nom-valeur. Pour obtenir des informations sur les noms valides pour un type de source de données ODBC, comme Sybase, Microsoft SQL Server ou Oracle, téléchargez le *Guide de l'utilisateur DataDirect Connect Series pour ODBC* et le *Guide de l'utilisateur DataDirect Connect Series pour ODBC* figurant dans la bibliothèque de documentation Progress DataDirect.

Barre d'outils

Le tableau ci-dessous fournit la description des options contenues dans les barres d'outils.

Option	Description
+	Ouvre la boîte de dialogue Ajouter un DSN dans laquelle vous ajoutez une source d'événement pour le type de source d'événement que vous avez sélectionné dans le panneau Catégories d'événements.

Option	Description
	Supprime les sources d'événements sélectionnées.
	Ouvre la boîte de dialogue Modifier un DSN permettant de modifier les paramètres de configuration de la source d'événement sélectionnée. Si vous sélectionnez plusieurs sources d'événements, cette option ouvre la boîte de dialogue Modifier la source en bloc permettant de modifier les valeurs de paramétrage des répertoires de fichiers sélectionnés.
	Ouvre la boîte de dialogue Option d'ajout en bloc permettant d'importer en bloc les paramètres DSN contenus dans un fichier CSV. La boîte de dialogue Option d'ajout en bloc contient les deux options suivantes : • Importer le fichier CSV • Coller le contenu CSV
	Crée un fichier **.csv** contenant les paramètres des DSN sélectionnées.
	Valide les paramètres de configuration pour la base de données ODBC sélectionnée.

Boîte de dialogue Ajouter ou modifier un DSN

Dans cette boîte de dialogue, ajoutez ou modifiez une source d'événement pour la source d'événement sélectionnée.

Paramètres de base

Nom	Description
DSN*	DSN (nom de source de données) définissant la base de données à partir de laquelle collecter des événements. Sélectionnez un DSN existant dans la liste déroulante. Pour plus d'informations, consultez la rubrique Paramètres de configuration des sources d'événements liées aux DSN ODBC.
Nom d'utilisateur*	Nom d'utilisateur utilisé par le nom de source de données pour se connecter à la base de données. Vous devez spécifier un nom d'utilisateur lorsque vous créez la source d'événement.

Nom	Description
Mot de passe	Mot de passe utilisé par le nom de source de données pour se connecter à la base de données. **Attention :** le mot de passe est chiffré en interne et s'affiche dans sa forme chiffrée.
Activé	Cochez la case pour activer la configuration de la source d'événement et démarrer la collecte. Cette case à cocher est activée par défaut.
Adresse*	Pour ODBC, ce champ n'est pas utilisé. Le Log Collector utilise l'adresse figurant dans le fichier **ODBC.ini**.

Paramètres avancés

Nom	Description
Taille de cellule max.	Taille maximale des données (en octets) que le Log Collector peut extraire d'une cellule de la base de données. La valeur par défaut est **2048**.
Valeur nulle	Chaîne de caractères que le Log Collector affiche lorsque NIL est renvoyé pour une cellule de la base de données. Valeur par défaut : “” (null).
Intervalle d'interrogation	Intervalle (durée en secondes) entre chaque interrogation. La valeur par défaut est **180**. Par exemple, si vous spécifiez 180, le collecteur planifie une interrogation de la source d'événement toutes les 180 secondes. Si le cycle d'interrogation précédent est toujours en cours, le collecteur attend la fin de l'opération. Si vous avez un grand nombre de sources d'événements à interroger, il se peut que l'opération d'interrogation mette plus de 180 secondes avant de démarrer, car les threads sont occupés.
Nb max. d'interrogations d'événements	Nombre maximal d'événements par cycle d'interrogation (nombre d'événements collectés par cycle d'interrogation).

Nom	Description
Débogage	**Attention :** Attention : n'activez le débogage (paramètre défini sur On ou Verbose) que si vous rencontrez un problème avec cette source d'événement et que vous recherchez une solution pour corriger le problème. L'activation du débogage risque d'affecter les performances du Log Collector de manière défavorable. Active ou désactive la consignation du débogage pour la source d'événement. Les valeurs autorisées sont les suivantes : • **Off** = (valeur par défaut) désactivée • **On** = activée • **Verbose** = activée en mode détaillé. Ajoute aux messages des informations liées aux threads et au contexte de la source. Ce paramètre est conçu pour déboguer et analyser les problèmes de collecte des sources d'événements isolés. Si vous modifiez cette valeur, la modification prendra effet immédiatement (aucun redémarrage nécessaire). La consignation du débogage s'effectue en mode détaillé, donc limitez le nombre de sources d'événements afin de réduire tout impact sur les performances.
ID de suivi initial	Code d'identification initial que le Log Collector assigne à cette source d'événement si la collecte n'a pas commencé. S'il n'y a pas de valeur pour ce paramètre, le Log Collector commence en bas du tableau et n'extrait que les lignes après la fin du tableau au fur et à mesure de leur ajout. La valeur par défaut est “” (null).
Nom du fichier	Pour les sources d'événements Microsoft SQL Server uniquement, emplacement du répertoire des fichiers de suivi (par exemple, **C:\MyTraceFiles**). Consultez le Guide de configuration RSA Microsoft SQL Server Event Source, disponible sur RSA Link ici : https://community.rsa.com/docs/DOC-40241.
Tester la connexion	Vérifiez les paramètres de configuration spécifiés dans cette boîte de dialogue pour vous assurer qu'ils sont corrects.
Annuler	Ferme la boîte de dialogue sans ajouter ou modifier les paramètres DSN.
OK	Ajoute ou modifie les paramètres du DSN.

Paramètres de configuration des sources d'événements liées aux DSN ODBC

Les sources d'événements ODBC (Open Database Connectivity) requièrent des noms de sources de données (DSN), donc vous devez définir les DSN avec leurs paires de valeurs associées pour la configuration des sources d'événements ODBC.

Accéder aux paramètres de configuration ODBC

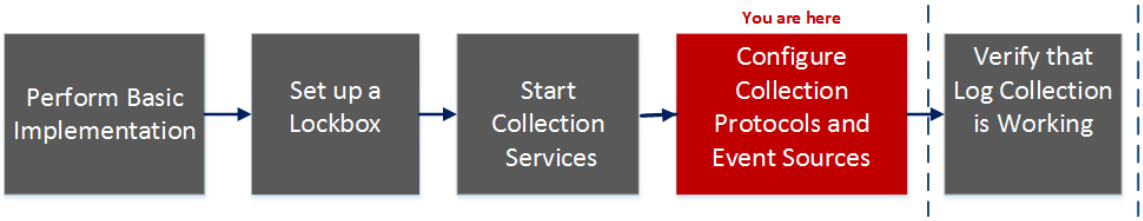
Pour accéder aux paramètres de configuration des sources d'événements ODBC :

1. Pour accéder à la vue Services, cliquez sur le menu NetWitness Suite et sélectionnez **Admin > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez **Vue > Config** pour afficher les onglets des paramètres de configuration de la collecte de logs.

   La vue **Configuration des services** s'affiche avec l'onglet **Général** de Log Collector ouvert.
4. Cliquez sur l'onglet **Sources d'événements** et sélectionnez **ODBC/DSN** dans le menu déroulant.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base

Rôle	Je souhaite...	Documentation
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Configurer des sources d'événements ODBC dans NetWitness Suite
- Configurer des noms de sources de données (DSN)

Paramètres de configuration des DSN ODBC

Cette rubrique décrit les paramètres de configuration des noms des sources de données (DSN).

Panneau DSN

Dans le panneau DSN, vous pouvez ajouter, supprimer ou modifier les paires nom-valeur DSN pour les sources d'événements ODBC.

Fonctionnalité	Description
	Affiche la boîte de dialogue Ajouter un DSN qui vous permet de définir un DSN et ses paramètres.
	Supprime les DSN sélectionnés.
	Affiche la boîte de dialogue Modifier un DSN qui vous permet de modifier les paires nom-valeur pour le DSN sélectionné.

Fonctionnalité	Description
Manage Templates	Affiche la boîte de dialogue Gérer les modèles DSN qui vous permet d'ajouter ou de supprimer les modèles de paires nom-valeur DSN.
	Sélectionne les DSN.
DSN	Nom du DSN que vous avez ajouté.
Paramètres	**<nom-valeur pour="" p="" paires="" le=""> </nom-valeur>**

Boîte de dialogue Ajouter ou modifier un DSN

Dans cette boîte de dialogue, ajoutez ou modifiez un répertoire de fichiers pour la source d'événement sélectionnée.

Fonctionnalité	Description
Modèle de DSN	Sélectionnez un modèle de paires nom-valeur DSN prédéfini pour le DSN.
Nom DSN*	Ajoutez le nom du DSN. Vous ne pouvez pas modifier un nom DSN après l'avoir ajouté. Cette valeur doit correspondre à une entrée DSN dans le fichier ODBC.ini. La valeur valide est une chaîne de caractères qui est restreinte aux caractères suivants : `[_a-zA-Z][_a-zA-Z0-9]*` Cela signifie que le répertoire du fichier doit commencer par une lettre suivie de chiffres, lettres et caractères de soulignement (par exemple, **rémunération_dirigeants_oracle**).
Paramètres	 Ajoute une ligne qui vous permet de définir une paire de paramètres nom-valeur. Supprime la paire de paramètres nom-valeur sélectionnée.  Sélectionne la paire de paramètres nom-valeur. Nom - Saisissez ou modifiez le nom du paramètre. Valeur - Saisissez ou modifiez la valeur associée au nom du paramètre.

Fonctionnalité	Description
Annuler	Ferme la boîte de dialogue sans ajouter le DSN et ses paires nom-valeur ni enregistrer les modifications appliquées aux paires nom-valeur.
Enregistrer	Ajoute le DSN et ses paires nom-valeur ou enregistre les modifications appliquées aux paires nom-valeur.

Boîte de dialogue Gérer les modèles DSN

Cette boîte de dialogue vous permet d'ajouter ou de supprimer les modèles de paires nom-valeur DSN.

Fonctionnalité	Description
	Panneau Sélection d'un modèle
	Ouvre le panneau Ajouter un modèle qui vous permet d'ajouter un modèle de paire nom-valeur DSN.
	Supprime le modèle sélectionné.
	Sélectionne un modèle pour la suppression ou la modification.
	Panneau Ajouter un modèle
	Ajoute une ligne de paire de valeurs
	Supprime une ligne de paire de valeurs
	Sélectionne une ligne de paire de valeurs
Nom	Saisissez le nom du paramètre.
Valeur	Saisissez la valeur associée au nom du paramètre.
Annuler	Annule les modifications que vous avez effectuées dans la boîte de dialogue.

Fonctionnalité	Description
Enregistrer	Ajoute le DSN et ses paires nom-valeur ou enregistre les modifications appliquées aux paires nom-valeur.
Fermer	Ferme la boîte de dialogue sans ajouter le DSN et ses paires nom-valeur ni enregistrer les modifications appliquées aux paires nom-valeur.

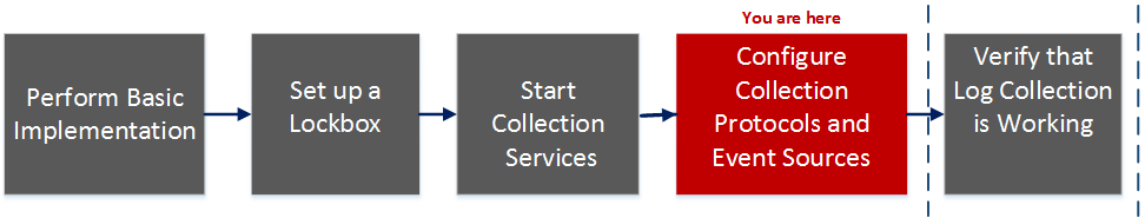
Paramètres de configuration du collecteur distant et du collecteur local

Lorsque vous déployez Log Collection, vous devez configurer les Log Collectors pour qu'ils collectent les événements de log auprès des diverses sources d'événements, puis pour qu'ils fournissent de manière fiable et sécurisée ces événements à l'hôte Log Decoder, dans lequel ils sont décryptés et stockés pour analyse ultérieure.

Cette rubrique présente les fonctionnalités de la vue Configuration des services > onglets Collecteurs distants/Collecteurs locaux.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Provisionner des collecteurs locaux et des collecteurs distants
- Configurer des collecteurs locaux et des collecteurs distants

Vue Configuration des Services

La vue Configuration des services vous permet de gérer tous les paramètres Log Collection. Les onglets sous lesquels vous gérez les paramètres de déploiement et auxquels il est fait référence dans ce guide sont les onglets **Collecteurs distants/Collecteurs locaux** :

- Si vous configurez un Local Collector, NetWitness Suite affiche l'onglet **Collecteurs distants** pour que vous puissiez configurer le Local Collector afin qu'il extraie les événements des collecteurs distants.
- Si vous configurez un Remote Collector, NetWitness Suite affiche l'onglet **Collecteurs locaux** pour que vous puissiez configurer le Remote Collector afin qu'il transmette des événements à un Local Collector.

Onglets Collecteurs distants

Sur un Local Collector, le panneau Collecteurs distants offre un moyen d'ajouter ou de supprimer des collecteurs distants à partir desquels le Local Collector extrait les événements.

Colonne	Description
	Affiche la boîte de dialogue **Ajouter une source** permettant de sélectionner les collecteurs distants à partir desquels vous souhaitez que le Local Collector extraie les événements.
	Supprime le Remote Collector à partir de la Local Collector panneau Collecteurs distants.
	Affiche la boîte de dialogue **Modifier la source** pour le Remote Collector sélectionné.
	Sélectionne des collecteurs distants.

Colonne	Description
Nom	Noms des collecteurs distants à partir desquels le Local Collector extrait actuellement les événements.
Adresse	Adresses IP des collecteurs distants à partir desquels le Local Collector extrait actuellement les événements.
Collecte	Choisissez les protocoles de collecte que le Remote Collector transmet à un Local Collector. Vous pouvez sélectionner n'importe quelle combinaison de protocoles. Si vous ne définissez aucun protocole, NetWitness Suite sélectionnera alors tous les protocoles.

Onglet Local Collector

Sur un Remote Collector, le panneau Local Collector permet d'ajouter ou de supprimer des Collecteurs locaux vers lesquels vous souhaitez que le Remote Collector transmette des événements.

Sélectionnez la **Destination** ou la **Source** dans la liste déroulante **Sélectionner une configuration**.

- **Destination** affiche la boîte de dialogue **Ajouter une destination distante**.
- Source affiche la boîte de dialogue **Ajouter une source**.

Le tableau suivant décrit la boîte de dialogue Ajouter une source.

Colonne	Description
	Affiche la boîte de dialogue **Ajouter une source** permettant de sélectionner les collecteurs distants à partir desquels vous souhaitez que le Local Collector extraie les événements.
	Supprime le Remote Collector à partir de la Local Collector panneau Collecteurs distants.
	Affiche la boîte de dialogue **Modifier la source** pour le Remote Collector sélectionné.
	Sélectionne des collecteurs distants.

Colonne	Description
Nom	Noms des collecteurs distants à partir desquels le Local Collector extrait actuellement les événements.
Adresse	Adresses IP des collecteurs distants à partir desquels le Local Collector extrait actuellement les événements.

Le tableau suivant décrit le panneau Local Collectors.

Colonne	Description
	Affiche la boîte de dialogue **Ajouter une destination distante** pour le groupe que vous avez sélectionné. Pour ce groupe, vous ajoutez des Local Collectors de destination auxquels vous souhaitez que le Remote Collector transmette des événements.
	Supprime le Log Collector de destination du groupe.
	Affiche la boîte de dialogue **Modifier la destination distante** pour le Local Collector de destination sélectionné.
	Sélectionnez une destination Local Collector.
Nom de la destination	Affiche le nom du Local Collector de destination.
Adresse	Affiche l'adresse IP du Local Collector de destination.
Collecte	Choisissez les protocoles de collecte que le Local Collector extraie d'un collecteur distant. Vous pouvez sélectionner n'importe quelle combinaison de protocoles. Si vous ne définissez aucun protocole, NetWitness Suite sélectionnera alors tous les protocoles.

Onglets Collecte de logs

Cette rubrique décrit les onglets disponibles dans la vue Collecte de logs.

Accéder à la vue Collecte de logs

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, sélectionnez **Vue > Config** pour afficher les onglets des paramètres de configuration de la collecte de logs.

   La vue **Configuration des services** s'affiche avec l'onglet **Général** Log Collector ouvert.
4. Sélectionnez l'un des onglets disponibles pour afficher ou mettre à jour les paramètres correspondants.

Onglets disponibles

Utilisez la vue Admin > Services pour mettre à jour les paramètres de collecte des logs. Il comprend les onglets suivants :

- **Général** : contient les paramètres de haut niveau qui gèrent le fonctionnement du service Log Collector et chaque protocole de collecte. Reportez-vous à l'Onglet Général de Log Collection pour plus d'informations.
- **Remote Collectors** : utilisez cet onglet pour configurer des remote collectors. Reportez-vous à la rubrique Configurer des collecteurs locaux et des collecteurs distants pour plus d'informations.
- **Fichiers** : fournit une interface de modification des fichiers de configuration de Log Collector.
- **Sources d'événements** : utilisez cet onglet pour configurer la collecte de vos sources d'événements. Reportez-vous à l'Onglet Sources d'événements de Log Collection pour plus d'informations.
- **Destinations d'événements** : utilisez l'onglet Destinations d'événements de la vue Configurer le service de collecte de logs pour configurer la destination des données d'événements collectées par le Log Collector. Reportez-vous à l'Onglet Destinations des événements de Log Collection pour plus d'informations.
- **Paramètres** : contient les paramètres de configuration de la sécurité Lockbox et de gestion des certificats.
- **Configuration du service Appliance** : contient les paramètres de configuration pour le service Appliance de RSA NetWitness Suite Core.

Reportez-vous aux onglets **Fichiers** et **Configuration du service Appliance** dans le *Guide de configuration de l'hôte et des services* pour obtenir des informations sur les paramètres de configuration de ces onglets.

Onglet Général de Log Collection

Cette rubrique présente les fonctions de la vue Configuration des services> onglet Général liées spécifiquement à Log Collector.

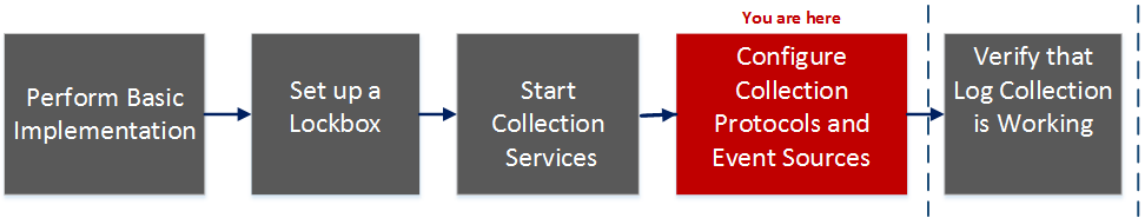
Pour accéder à l'onglet Général de Log Collection :

1. Accédez à **ADMIN > Services** à partir du menu NetWitness Suite.
2. Sélectionnez un service de collecte de logs.
3. Cliquez sur  sous Actions, puis sélectionnez **Vue > Config**.

   La vue **Configuration des services** s'affiche avec l'onglet **Général** de Log Collector ouvert.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	Configurer les protocoles et les sources d'événements Log Collection.	Configurer des protocoles de collecte et des sources d'événements

Rôle	Je souhaite...	Documentation
Administrateur	*Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

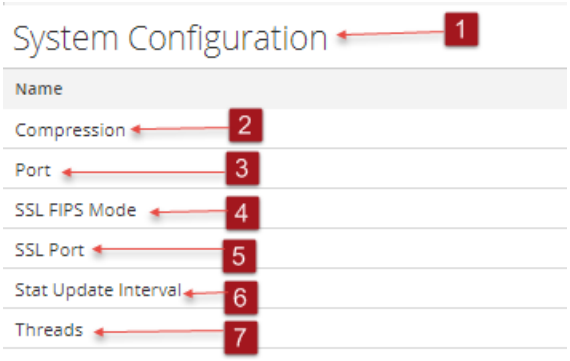
- Configurer des sources d'événements AWS (CloudTrail) dans NetWitness Suite
- Configurer des sources d'événement Check Point dans NetWitness Suite
- Configurer des sources d'événements de fichiers dans NetWitness Suite
- Configurer des sources d'événements Netflow dans NetWitness Suite
- Configurer des sources d'événements ODBC dans NetWitness Suite
- Configurer des sources d'événements SDEE dans NetWitness Suite
- Configurer des sources d'événements SNMP dans NetWitness Suite
- Configurer des sources d'événements Syslog pour le collecteur distant
- Configurer des sources d'événement VMware dans NetWitness Suite
- Configurer des sources d'événement Windows dans NetWitness Suite
- Guide de configuration de la collecte Windows d'ancienne génération et NetApp

Aperçu rapide

L'administrateur de RSA NetWitness Suite doit configurer des sources d'événements pour envoyer les logs aux collecteurs. Lorsque des sources d'événements sont configurées, les collecteurs interrogent des sources d'événements, récupèrent les logs et envoient les données d'événement à NetWitness Suite).

Panneau Configuration système

Le panneau Configuration système gère la configuration des services pour un service NetWitness Suite. lorsqu'un service est ajouté pour la première fois, les valeurs par défaut s'appliquent. Vous pouvez modifier ces valeurs pour optimiser les performances. Reportez-vous à l'onglet **Général** pour une description de ces paramètres.



1	Le panneau Configuration système gère la configuration des services pour un service NetWitness Suite.
2	Compression : Le nombre minimum d'octets devant être transmis par réponse avant la compression. Le paramètre 0 désactive la compression. La valeur par défaut est **0**. La modification d'une valeur prend effet immédiatement pour toutes les connexions suivantes.
3	Port : Port sur lequel le service écoute. Les ports sont : • 50001 pour les Log Collectors • 50002 pour les Log Decoders • 50003 pour les Brokers • 50004 pour les Decoders • 50005 pour les Concentrators • 50007 pour les autres services
4	Mode FIPS SSL : En cas d'activation (**on**), la sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL. La valeur par défaut est **off**.
5	Port SSL : Port SSL de base NetWitness Suite sur lequel le service écoute. Les ports sont : • 56001 pour les Log Collectors • 56002 pour les Log Decoders • 56003 pour les Brokers • 56004 pour les Decoders • 56005 pour les Concentrators

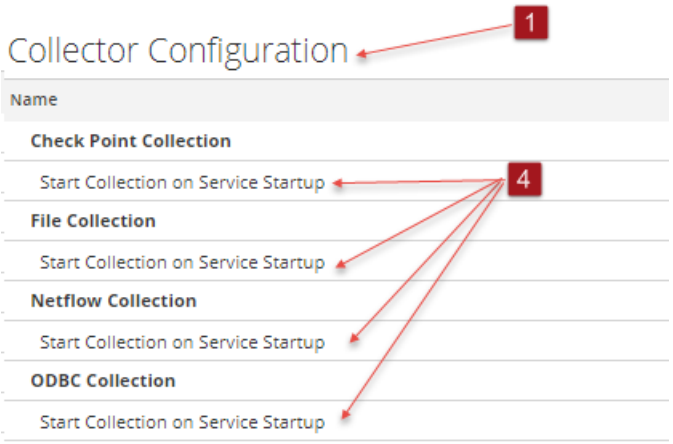
- 56007 pour les autres services

6 Intervalle de mise à jour des statistiques : Nombre de millisecondes entre les mises à jour statistiques sur le système. Les petites valeurs engendrent des mises à jour plus fréquentes et peuvent ralentir d'autres processus. La valeur par défaut est **1 000**.
La modification de la valeur prend effet immédiatement.

7 Threads : Nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. Le paramètre 0 laisse le système décider. La valeur par défaut est 15.
Les modifications prendront effet au redémarrage du service.

Panneau Configuration des collecteurs

Le panneau Configuration des collecteurs permet d'activer le démarrage automatique de la collecte des logs en fonction du type de source d'événement :



1 Le panneau Configuration des collecteurs permet d'activer le démarrage automatique de la collecte des logs en fonction du type de source d'événement.

2 Activer tout active la collecte automatique pour tous les types d'événements.
Activer tout = commence la réception des événements et la collecte des logs pour tous les types d'événements lorsque le service Log Collector démarre.

3 Désactiver tout désactive la collecte automatique pour tous les types d'événements.
Désactiver tout = (paramètre par défaut) ne reçoit pas de données d'événements pour tous les types d'événements tant que vous ne démarrez pas explicitement la collecte.

4 Démarrer la collecte au démarrage du service active le démarrage automatique, par type de source d'événement, de collecte de logs lorsque le service Log Collector démarre. Les valeurs autorisées sont les suivantes :

- Sélectionné = démarre la collecte des logs lorsque le service Log Collector démarre.

- Non sélectionné = (paramètre par défaut) ne collecte aucun événement tant que vous ne démarrez pas explicitement la collecte.

5 **Appliquer** : Cliquez sur **Appliquer** pour enregistrer les changements appliqués aux valeurs de paramètres.

Onglet Destinations des événements de Log Collection

Utilisez l'onglet Destinations d'événements de la vue Config du service Log Collection pour configurer la destination des données d'événements collectées par le Log Collector :

- Log Decoders
- Identity Feed

Conditions préalables

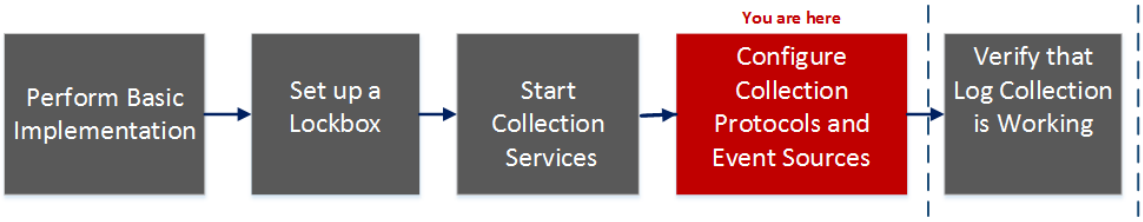
Vous devez implémenter la configuration suivante pour créer un Identity Feed.

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

Remarque : pour plus d'informations sur le mode de création et d'examen d'un Identity Feed, reportez-vous à la rubrique « Créer un IdentityFeed » dans le *Guide de gestion des ressources Live*.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte

Rôle	Je souhaite...	Documentation
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

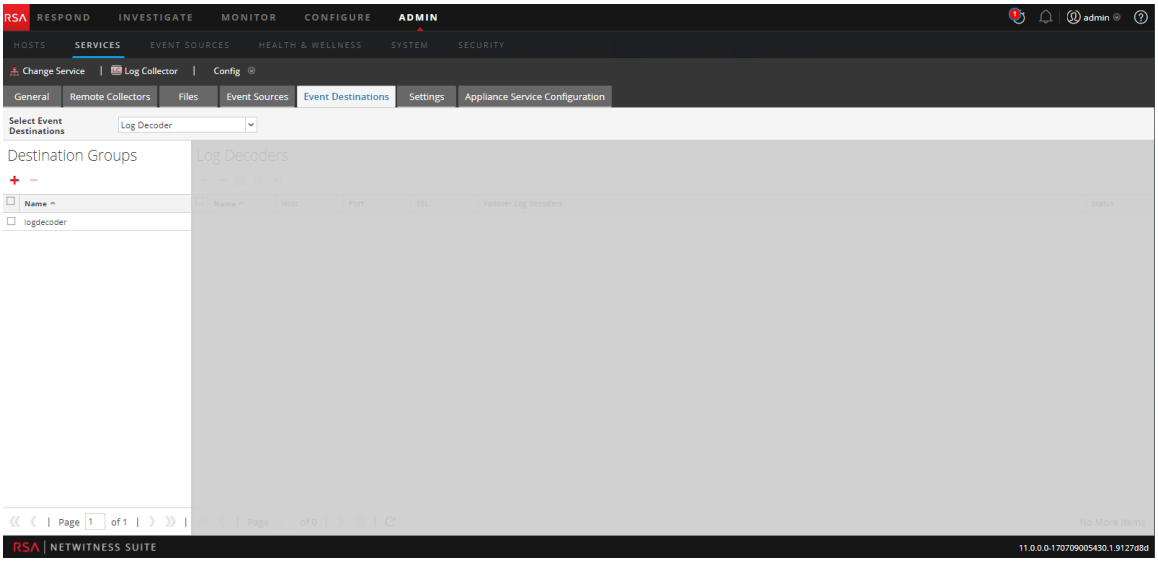
*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Reportez-vous à la rubrique **Créer un Identity Feed** dans le *Guide de gestion des ressources Live*.

Aperçu rapide

L'onglet Destinations d'événements de la vue Config du service Log Collection vous permet de configurer la destination des données d'événements collectées par le Log Collector.



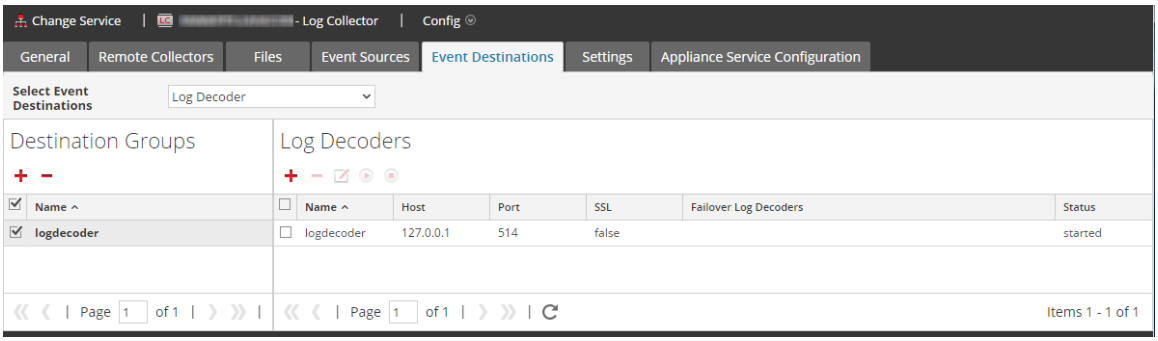
L'autorisation requise pour accéder à cette vue est Gérer les services.

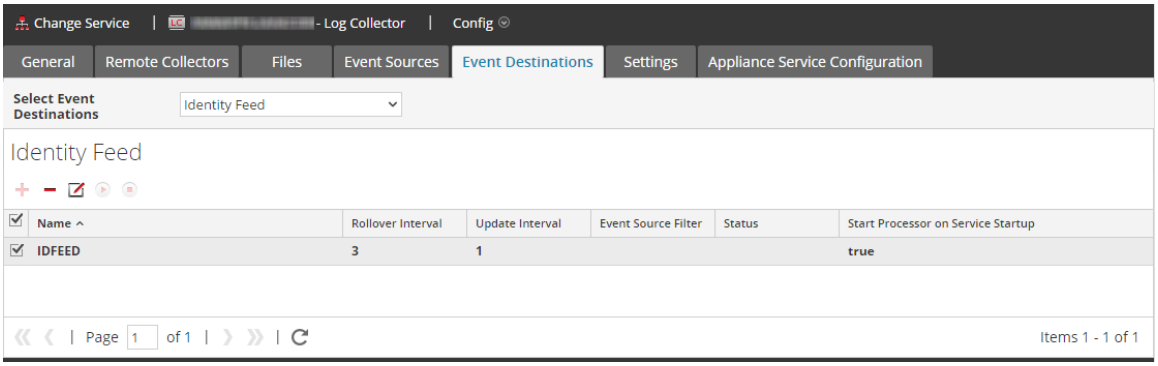
1. Accédez à **ADMIN > Services**.
2. Sélectionnez un service de collecte de logs.
3. Sous Actions, puis sélectionnez  **> Vue > Config** pour afficher les onglets des paramètres de configuration de collecte de logs.

4. Cliquez sur l'onglet **Destinations d'événements**.
5. Dans le menu déroulant **Sélectionner des destinations d'événements** :
   - Sélectionnez **Log Decoder** pour configurer les destinations de Log Decoder pour les données d'événements collectées par le Log Collector.

     Remarque : vous devez sélectionner un service Log Decoder dans la boîte de dialogue Ajouter une destination Log Decoder, mais le reste de la configuration s'effectue automatiquement.

   - Sélectionnez **Identity Feed** pour configurer une destination de flux d'identité pour les données d'événements collectées par le Log CollectorLog Collector.





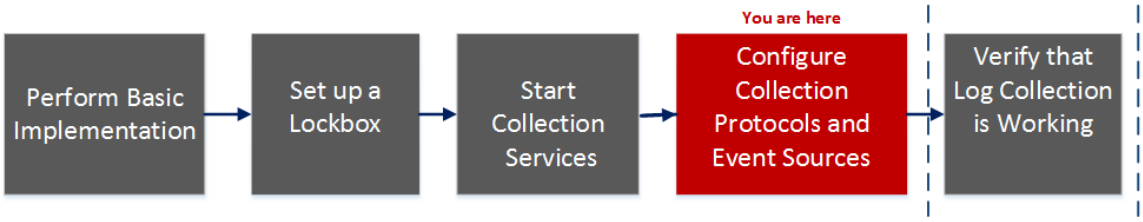
Onglet Sources d'événements de Log Collection

Utilisez l'onglet Sources d'événements pour configurer les sources d'événements AWS (CloudTrail), Check Point, File, ODBC, SDEE, SNMP, Syslog, SNMP, VMware, Windows et Windows Legacy.

Pour accéder à l'onglet Sources d'événements, allez à ADMIN > Services > sélectionnez Service Log Collection > Vue > Configurer > Sources d'événements).

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte
Administrateur	*Configurer des protocoles Log Collection et des sources d'événements.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

*Vous pouvez effectuer cette tâche ici.

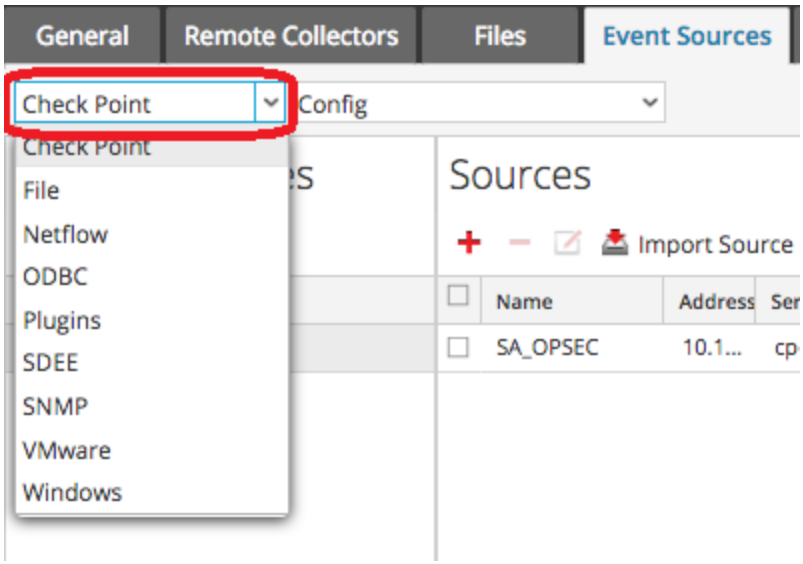
Rubriques connexes

- Configurer des sources d'événements AWS (CloudTrail) dans NetWitness Suite
- Configurer des sources d'événement Check Point dans NetWitness Suite
- Configurer des sources d'événements de fichiers dans NetWitness Suite
- Configurer des sources d'événements ODBC dans NetWitness Suite
- Configurer des sources d'événements SDEE dans NetWitness Suite
- Configurer des sources d'événements SNMP dans NetWitness Suite
- Configurer des sources d'événements Syslog pour le collecteur distant
- Configurer des sources d'événement VMware dans NetWitness Suite
- Configurer des sources d'événement Windows dans NetWitness Suite
- Guide de configuration de la collecte Windows d'ancienne génération et NetApp

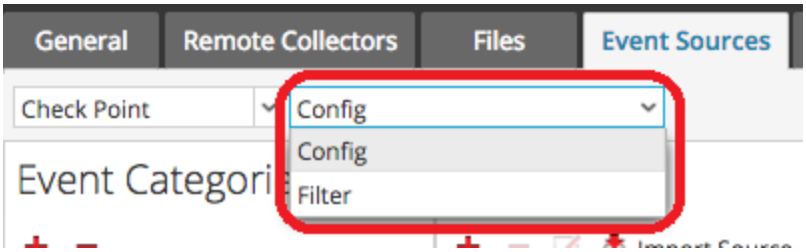
Aperçu rapide

La vue Configuration possède deux menus déroulants :

- Le menu de gauche répertorie tous les protocoles de collecte disponibles.



- Le menu de droite contient deux options : **Config** et **Filtrer**.



La vue Configuration de l'onglet Sources d'événements contient deux panneaux : Catégories et sources d'événements

Remarque : pour plus d'informations sur l'élément de menu Filtrer, consultez la rubrique Configurer des filtres d'événements pour un Collector.

Menu Types de sources d'événements

L'onglet Sources d'événements Log Collector contient un menu déroulant à deux zones dans lequel vous pouvez sélectionner le protocole de collecte et les paramètres de prise en charge correspondant.

Dans la zones de gauche, sélectionnez l'un des protocoles suivants : Check Point, File, ODBC, Plugins, SDEE, SNMP, SNMP, VMware, Windows et Windows Legacy.

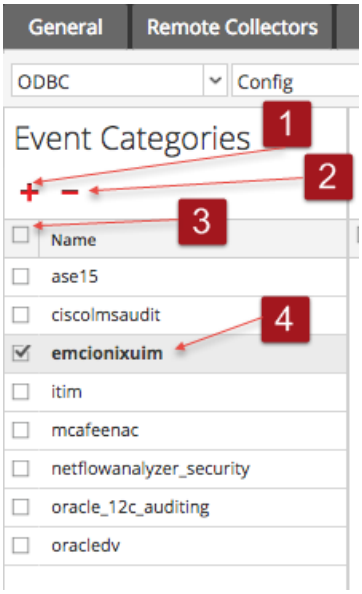
Dans la zone de droite, sélectionnez :

- Config pour configurer les paramètres des sources d'événements génériques pour le type que vous avez sélectionné dans la zone déroulante située à gauche. Tous les panneaux de configuration génériques contiennent une barre d'outils comportant les options suivantes :
  - Ajouter, Modifier et Supprimer
  - Importer (également Importer la source, Importer un DSN)
  - Exporter (également Exporter la source, Exporter un DSN)
- Pour ODBC, SNMP et Windows uniquement :
  - Pour ODBC, DSN à configurer
  - Pour SNMP, Gestionnaire des utilisateurs SNMP V3
  - Pour Windows, Configuration du realm Kerberos

Si vous sélectionnez une option, un panneau de configuration s'affiche. Vous pouvez y configurer les paramètres de collecte de la source d'événements. Les panneaux de configuration sont légèrement différents d'une source d'événements à l'autre et sont décrits séparément.

Panneau Catégories d'événements

Une fois que vous avez sélectionné un protocole de collecte, le panneau Catégories d'événements est rempli avec toutes les sources d'événements que vous avez configurées pour ce protocole de collecte. Par exemple, l'image suivante illustre les sources d'événements ODBC qui ont été configurées :



Le panneau Catégories d'événements permet d'ajouter ou de supprimer des types de source d'événement.

1	Affiche la boîte de dialogue Types de sources d'événements disponibles qui permet de sélectionner le type de source d'événement pour lequel vous souhaitez définir les paramètres.
2	Supprime les types de sources d'événements sélectionnés à partir du panneau Catégories d'événements.
3	Sélectionne les types de sources d'événements.
4	Affiche le nom des types de sources d'événements que vous avez ajoutés.

Panneau Sources

Le panneau Sources répertorie les valeurs des paramètres pour le type de source d'événement sélectionné. Pour plus d'informations, consultez les rubriques de protocole de collecte individuel.

Onglet Paramètres de Log Collection

Vous utilisez l'onglet Paramètres pour :

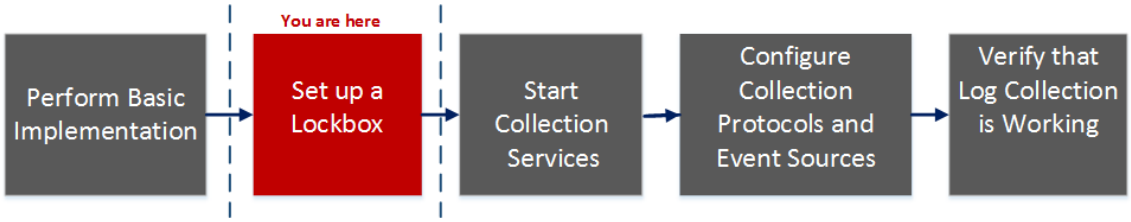
- Configurer un lockbox
- Réinitialiser la valeur du système stable
- Gérer des certificats

Attention : Si le nom d'hôte sur lequel le Log Collector est installé est modifié après l'installation, le Log Collector ne parviendra pas à collecter des événements à partir de sources. Vous devez réinitialiser les valeurs de système stable si le nom d'hôte change.

Pour accéder à l'onglet Paramètres de Log Collection, allez à ADMIN > Services. Dans la grille Services, sélectionnez un service Log Collector. Cliquez sur Menu Actions détouré sous Actions, puis sélectionnez Vue > Config.

Workflow

Ce workflow illustre les tâches de base qui vous permettent de commencer la collecte d'événements via Log Collection.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Effectuer l'implémentation Log Collection de base.	Implémentation de base
Administrateur	*Configurer un lockbox pour conserver les paramètres lockbox.	Configurer un Lockbox
Administrateur	Démarrer les services Log Collection.	Démarrer des services de collecte

Rôle	Je souhaite...	Documentation
Administrateur	Configurer les protocoles et les sources d'événements Log Collection.	Configurer des protocoles de collecte et des sources d'événements
Administrateur	Vérifier le fonctionnement de Log Collection.	Vérifier le fonctionnement de Log Collection

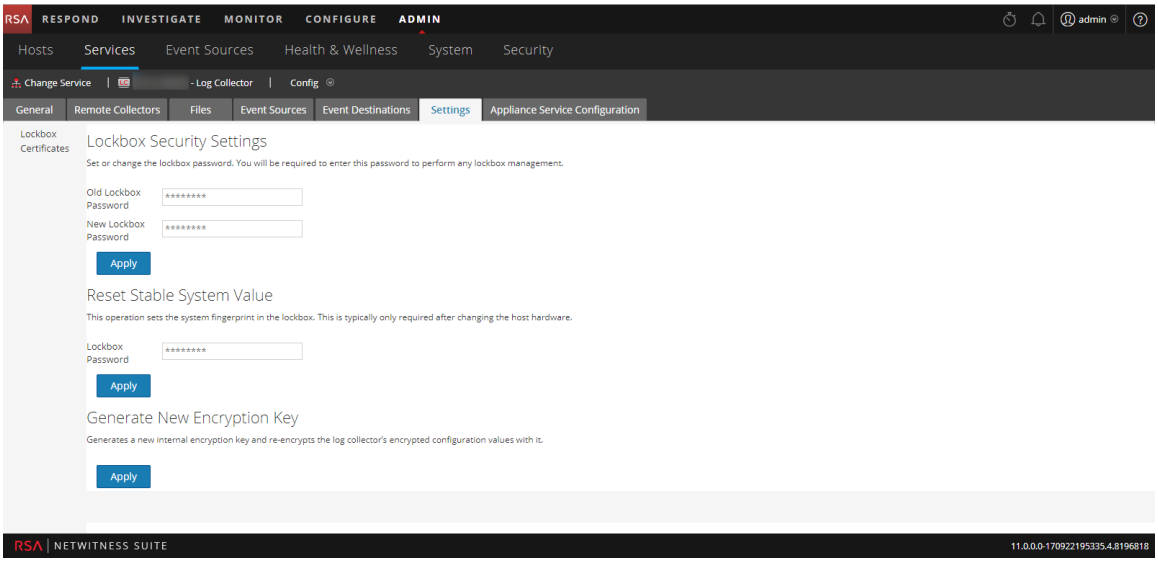
*Vous pouvez effectuer cette tâche ici.

Rubriques connexes

- Reportez-vous à la rubrique « Créer un Identity Feed » dans le *Guide de gestion des ressources Live*.

Aperçu rapide

Il s'agit d'un exemple de l'onglet Paramètres.



Résoudre les problèmes liés à Log Collection

Cette rubrique décrit le format et le contenu de la résolution des problèmes de collecte de logs. NetWitness Suite vous informe des problèmes de Log Collector ou des problèmes potentiels dans le code suivant deux façons.

- Fichiers log.
- Vues Contrôle de l'intégrité.

Fichiers log

Si vous rencontrez un problème avec un protocole de collecte de sources d'événements, vous pouvez consulter les logs de débogage pour analyser les solutions à ce problème. Chaque source d'événement comporte un paramètre Debug que vous pouvez activer (définissez le paramètre sur On ou Verbose) pour capturer ces logs.

Attention : N'activez le débogage que si vous rencontrez un problème avec cette source d'événement et que vous devez analyser ce problème. Si vous activez le paramètre Debug en permanence, les performances du Log Collector risquent d'être affectées de manière défavorable.

Contrôle de l'intégrité

Le Contrôle de l'intégrité vous fait prendre conscience des problèmes matériels et logiciels potentiels en temps opportun de sorte que vous puissiez éviter les pannes. RSA recommande de surveiller les champs statistiques du Log Collector afin de vérifier que le service fonctionne efficacement et qu'il ne se rapproche pas des valeurs maximales que vous avez configurées au point de les atteindre. Vous pouvez surveiller les statistiques suivantes décrites dans la vue **Admin > Intégrité**.

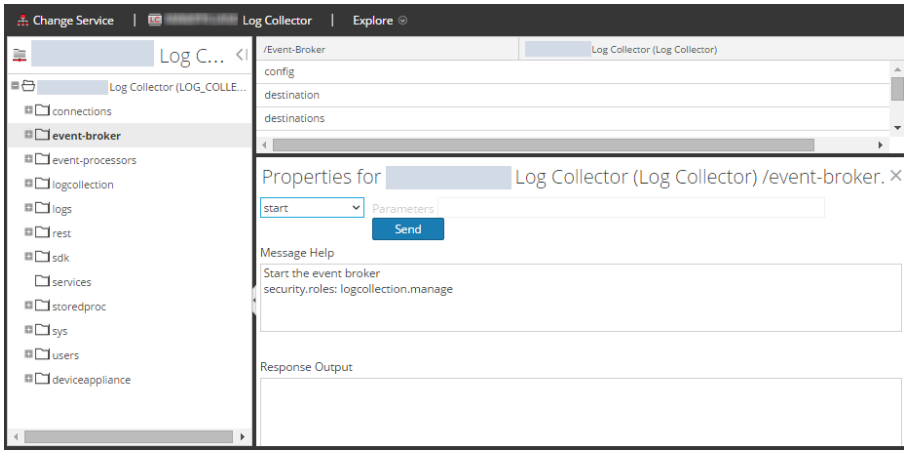
Exemple de format d'échantillon

RSA NetWitness Suite renvoie les types de messages d'erreur suivants dans les fichiers log.

Messages de log	`timestamp failure (LogCollection) Message-Broker Statistics:...`
	`timestamp failure (AMQPClientBaseLogCollection):...`
	`timestamp failure (MessageBrokerLogReceiver):...`

Cause	Le Log Collector ne réussit pas à contacter le courtier de messages, car ce dernier :

probable	• s'est arrêté de fonctionner ; • comporte des paramètres de connexion incorrects.

Solutions	1. <use the="the" systemctl="systemctl" command="command" on="on" console="console" to="to" check="check" status="status" of="of" message="message" broker="broker" shell="shell" console.="console.">returns the following if the message broker is not running:</use>
	`prompt$ systemctl status rabbitmq-server`
	`rabbitmq start/running, process 10916`
	2. Lancez le courtier de messages RabbitMQ sur le nœud event-broker dans la vue Explorer :
	 

Résolution des problèmes - Windows Log Collection utilisant un agent Endpoint

Les sections suivantes vous aident à résoudre les problèmes que vous pouvez rencontrer lors de l'utilisation du fichier Windows Log Collection sur l'agent Endpoint Insights.

Explication du format de fichier de configuration Windows Log

Attention : Ne modifiez pas le fichier de configuration généré. Si des modifications sont apportées, l'agent ne lit pas les informations à partir du fichier.

Le fichier de configuration de log contient des informations utiles pour l'analyse des logs d'événements. Vous trouverez ci-dessous un exemple :

```
#### Warning: Do not modify this system generated file.
{
  "enabled" : true,
  "configName" : "FE",
  "servers" : [ "tcp://[redacted]" ],
  "filter" : "<QueryList><Query Id='0'> <Select
  Path='ForwardedEvents'>*</Select> </Query></QueryList>",
  "testLogOnLoad" : true
}

q5yrOSY6qkdediE9XUI361926LOF2ZyU7JU2sklntgMWeV3KWFekwqJqhZ8XmPr6vbeOTK6wiYb
uW6zDL0WB/PPo+x5bErzvjoALA7zwAu61HVk4R4sYP4MRgGCsuiikC2pMB667P5bFg0+sUESsxZ
eFN91cjFPUjIIujuUdd0uMhnyur4tt+4F/WGJsBl57pTow2D8NRHvb9hKBjE1lo7/nZ0WpSO0Fq
yHx90NuS42d0OhjrC3oDyucwdAjqKkxm7VtsAJQwwxZT1wUbmDRPoiIyTG7egERVDDyqGcu2Ii+
fkijkFhuxTta8kWIeleQiBts1BAk+JZNfDSNYdYqUg==
```

Le fichier de configuration généré contient les éléments suivants :

- **configName** : nom du fichier de configuration.
- **servers** : baie d'URL de serveurs, décrivant à la fois leur adresse et le protocole à utiliser lors du transfert des logs. L'agent tente de les contacter dans l'ordre.
- **filter** : format XML compatible avec Windows Event Viewer qui décrit les canaux à surveiller et les exclusions d'ID d'événement. Filtre XML standard pour collecter à partir de l'application et du système de canaux. Lorsqu'un ID d'événement unique est utilisé pour les deux, cela ressemblerait à ceci :

```
<QueryList>
    <Query Id="0" Path="Application">
        <Select Path="Application">*</Select>
        <Select Path="System">*</Select>
        <Suppress Path="Application">*[System[(EventID=3366)]]</Suppress>
        <Suppress Path="System">*[System[(EventID=3366)]]</Suppress>
    </Query>
</QueryList>
```

- **Enabled** : permet de désactiver la collecte, mais d'envoyer quand même un log de test s'il est activé.
- **TestLogOnLoad** : envoie un message de log lorsqu'une configuration est chargée, même si le transfert d'événements n'est pas activé. Cela permet aux analystes de tester une configuration avant d'activer la collecte. Ce message n'est pas consigné en local dans le Journal des événements Windows.

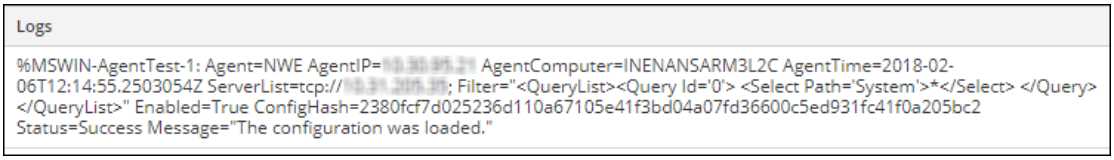
Comment lire un log de test

Message de log de test est envoyé chaque fois qu'un agent Endpoint avec un fichier Windows Log Collection est installé pour la première fois sur un agent Endpoint ou lorsqu'un fichier de configuration de log est mis à jour. Lors d'une installation ou mise à jour réussie de Windows Log Collection, 3 sections s'affichent dans le fichier log de test.

1	Type de message de log de test, adresse IP de l'agent, nom d'hôte de l'agent et heure de génération du log de test
2	Configuration fournie lors de la création de l'agent
3	État et message associé

Il existe trois scénarios.

1. Déploiement réussi d'une configuration Log Collection - Le type de message de log de test sera -1 et l'état indique Success (réussite).



2. Lorsque le fichier de configuration Log Collection est falsifié : le message de test de l'agent indique -2 et un message indiquant que le fichier de configuration a été falsifié s'affiche. Si vous souhaitez appliquer de nouveau les modifications, regénérez le fichier Log Collection.

3. Lorsque le nom du canal personnalisé est incorrect, le message « Status Failure » indiquant l'état d'échec s'affiche. Générez Log Collection de nouveau avec le canal approprié.