RSA NETWITNESS® SUITE

Guide de configuration de Reporting Engine

pour la version 11.0

Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

février 2018

Sommaire

Mode de fonctionnement du Reporting Engine

Reporting Engine Netwitness est un service sur le serveur d'administration Netwitness et facilite l'extraction de données à partir de différentes sources de données pour générer des rapports de conformité et d'analyse. Reporting Engine stocke les définitions des graphiques, des règles, des rapports et des alertes qui sont utilisées pour générer des rapports, des graphiques et des alertes.

La configuration de Reporting Engine comprend la configuration des sources de données, les définitions des sorties ou des notifications, ainsi que les paramètres pour améliorer les performances de l'extraction des données et la génération de rapports, de graphiques et d'alertes.

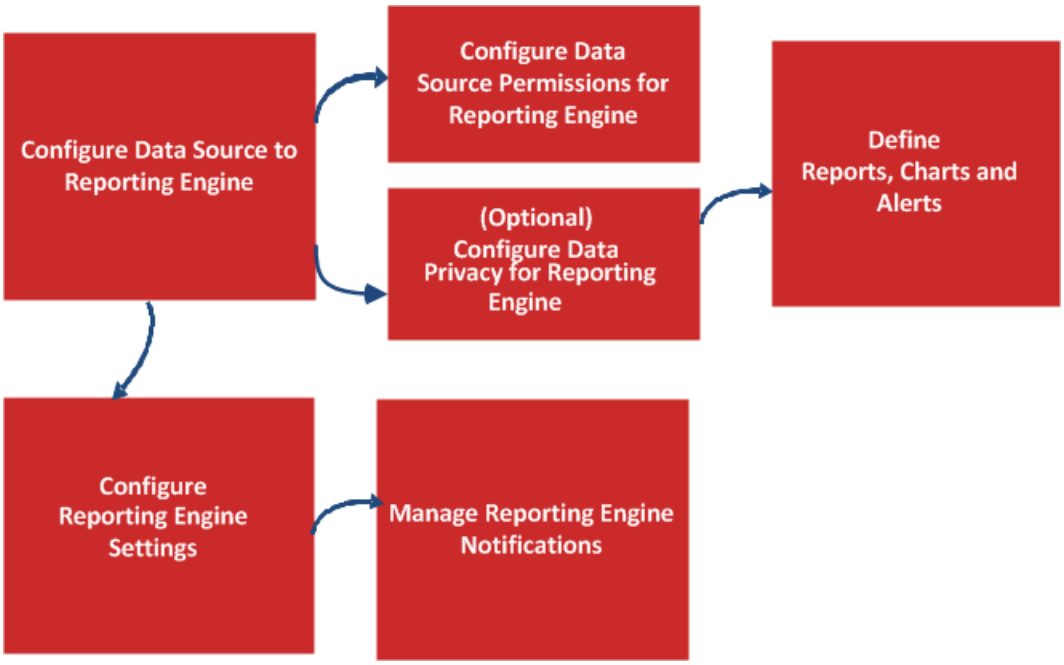
Lorsque vous installez NetWitness Suite, Reporting Engine est automatiquement installé en tant que service. Cela permet à Rapports, aux graphiques, et à Alertes d'être conservées dans NetWitness Suite RSA. Il est également possible de les afficher, de télécharger des rapports au format PDF ou CSV, de télécharger des graphiques au format PDF et de les ajouter en tant que dashlets.

Le Reporting Engine exécute les rapports et alertes en fonction des données issues d'une source de données. Vous devez donc associer une ou plusieurs sources de données à un Reporting Engine. Il existe trois types de sources de données :

- Sources de données NWDB - Les sources de données NetWitness Database (NWDB) sont les composants Decoder, Log Decoder, Broker, Concentrator, Archiver et Collecte. La génération de rapports, d'alertes et de graphiques sur les sources de données NWDB est prise en charge dans Reporting Engine.
- Sources de données Warehouse - Les sources de données Warehouse sont Hortonworks et MapR qui collectent des informations sur le Warehouse Connector et génèrent des rapports et des alertes. Cette source de données génère uniquement des rapports.
- Sources de données Répondre : Répondre est utilisé pour générer des rapports sur les alertes et les incidents. Cette source de données génère uniquement des rapports.

Workflow

Le workflow suivant présente une vue d'ensemble de la configuration Reporting Engine qui permet à l'utilisateur de générer Rapports, des graphiques, et Alertes.


Configure Data Source to Reporting Engine
Configure Data Source Permissions for Reporting Engine
(Optional) Configure Data Privacy for Reporting Engine
Define Reports, Charts and Alerts
Configure Reporting Engine Settings
Manage Reporting Engine Notifications

Configurer le Reporting Engine

Lors de l'installation du serveur Netwitness, le service Reporting Engine est automatiquement disponible et certains paramètres sont pré-remplis avec des valeurs par défaut pour atteindre des résultats optimaux.

Vous devez aussi vous assurer que les sources de données sont déployées et configurées dans NetWitness Suite. Pour plus d'informations, consultez la rubrique « Boîte de dialogue Ajouter un service ou Modifier le service » dans le *Guide de configuration de l'hôte et des services*.

Vous pouvez effectuer les opérations suivantes :

- Recherchez le dernier contenu de source de données dans Live et déployez-le régulièrement. (Pour plus d'informations, reportez-vous à la section « Gérer les ressources Live » dans le *Guide des services Live*.)
- (Facultatif) Ajouter de l'espace supplémentaire pour les rapports volumineux.

Configurer les sources de données

Vous devez configurer des sources de données telles que NWDB, Warehouse, ou Répondre. Vous pouvez configurer NWDB, Warehouse et Répondre pour générer respectivement Rapports, des graphiques, et Alertes. Si vous le souhaitez, vous pouvez également configurer Archiver, la collecte et des sources de données Workbench .

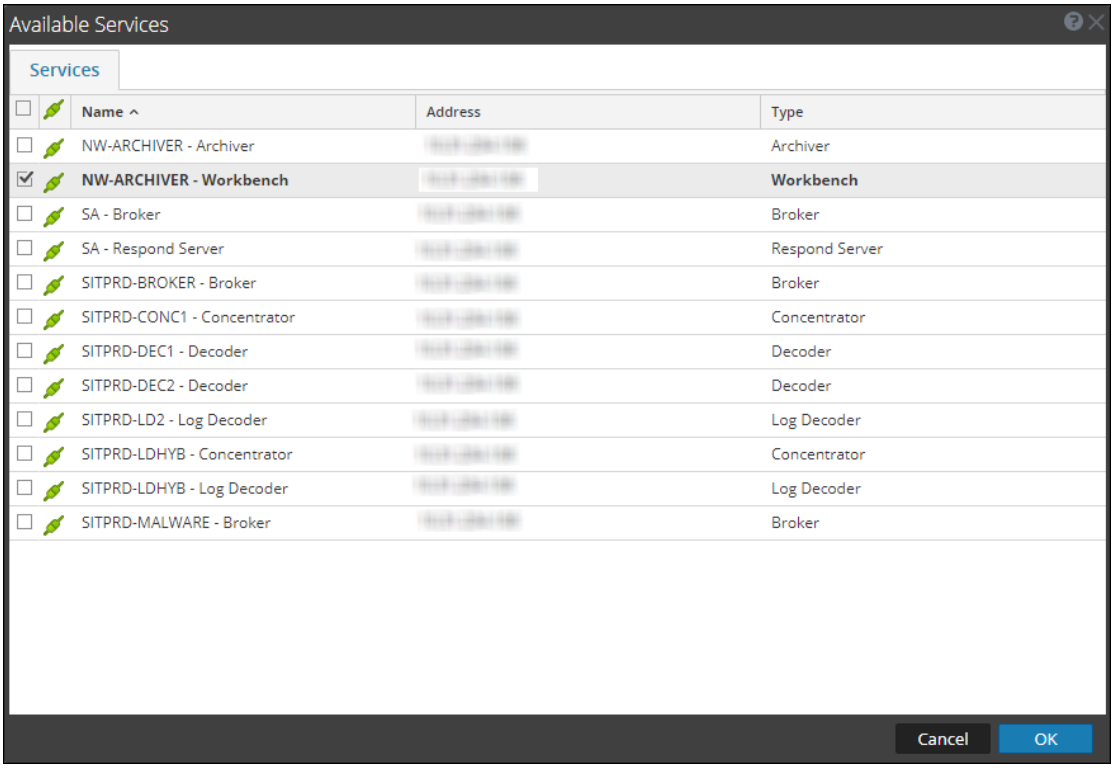
Configurer une source de données NWDB

Pour ajouter une source de données NWDB

1. Accédez à **ADMIN** > **Services**.
2. Dans **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur > **Vue** > **Config**.

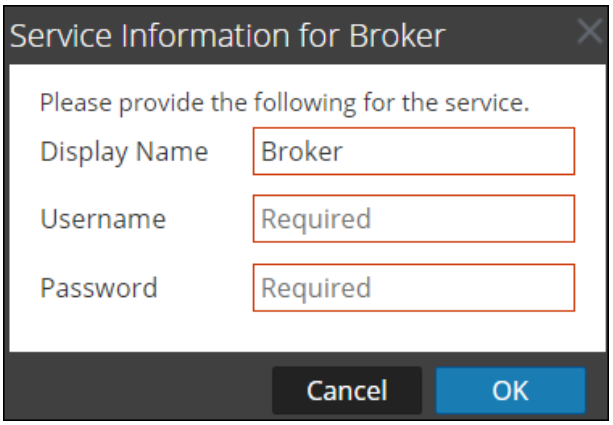
   La vue Configuration des services du Reporting Engine s'affiche.
4. Sur l'onglet **Sources**, cliquez sur > **Services disponibles**.

   La boîte de dialogue **Services disponibles** s'affiche.

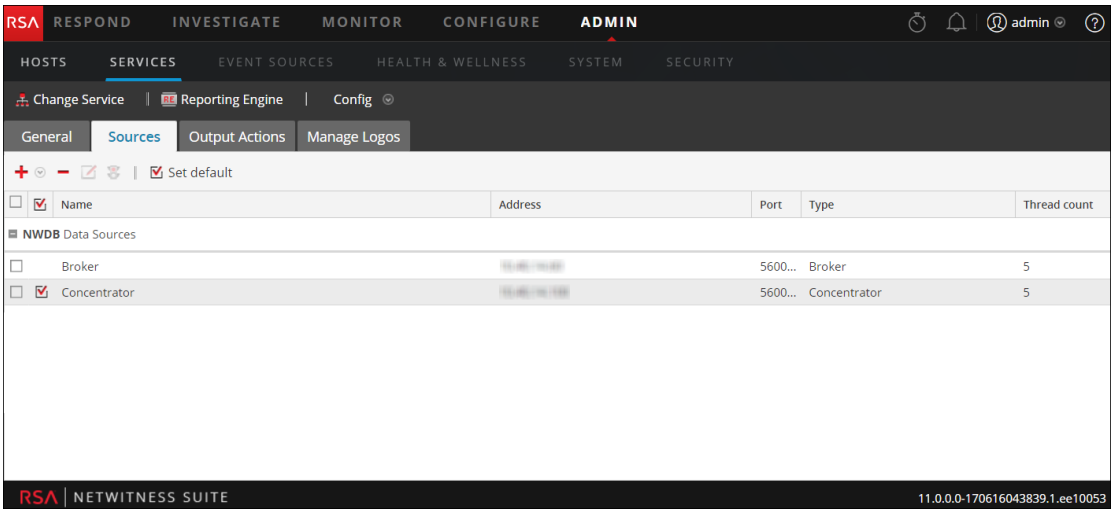


5. Sélectionnez un service NWDB que vous souhaitez ajouter, puis cliquez sur **OK**.

6. Dans les informations de Service pour la boîte de dialogue Broker, saisissez les informations de service pour le service, puis cliquez sur **OK**. Dans cet exemple, nous ajoutons un service Broker.



7. Le service s'affiche sous l'onglet Sources lorsqu'il est ajouté avec succès.



Remarque : Les services dont le Modèle de confiance est activé doivent être ajoutés individuellement. Il vous est demandé de fournir un nom d'utilisateur et un mot de passe pour le service sélectionné.

Configurer une source de données Warehouse

Vous pouvez ajouter la source de données Warehouse à Reporting Engine, afin que vous puissiez extraire les données à partir des services requis, les stocker dans MapR ou Hortonworks et générer Rapports et Alertes. La procédure de configuration de Warehouse comme source de données est différente. Pour extraire des données depuis une source de données Warehouse, vous devez la configurer à l'aide de la procédure suivante.

Remarque : Warehouse Analytics n'est pas pris en charge dans NetWitness Suite 11.0.

Condition préalable

Assurez-vous de :

- Ajouter une source de données Warehouse au Reporting Engine
- Définir une source de données Warehouse en tant que source par défaut
- Vérifier que le serveur Hive est en cours d'exécution sur tous les nœuds Warehouse. Utiliser la commande suivante pour vérifier l'état du serveur Hive :

  ```
  status hive2 (MapR deployments)
   service hive-server2 status (Horton Works deployments)
  ```

- Warehouse Connector est configuré pour écrire des données dans les déploiements de Warehouse.
- Si l'authentification Kerberos est activée pour HiveServer2, vérifiez que le fichier de table de clés est copié dans le répertoire `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/` de l'hôte Reporting Engine.

  Remarque : L'utilisateur **rsasoc** doit bénéficier de droits de lecture pour le fichier de table de clés. Pour plus d'informations, reportez-vous à la rubrique Configurer les autorisations d'accès aux sources de données.

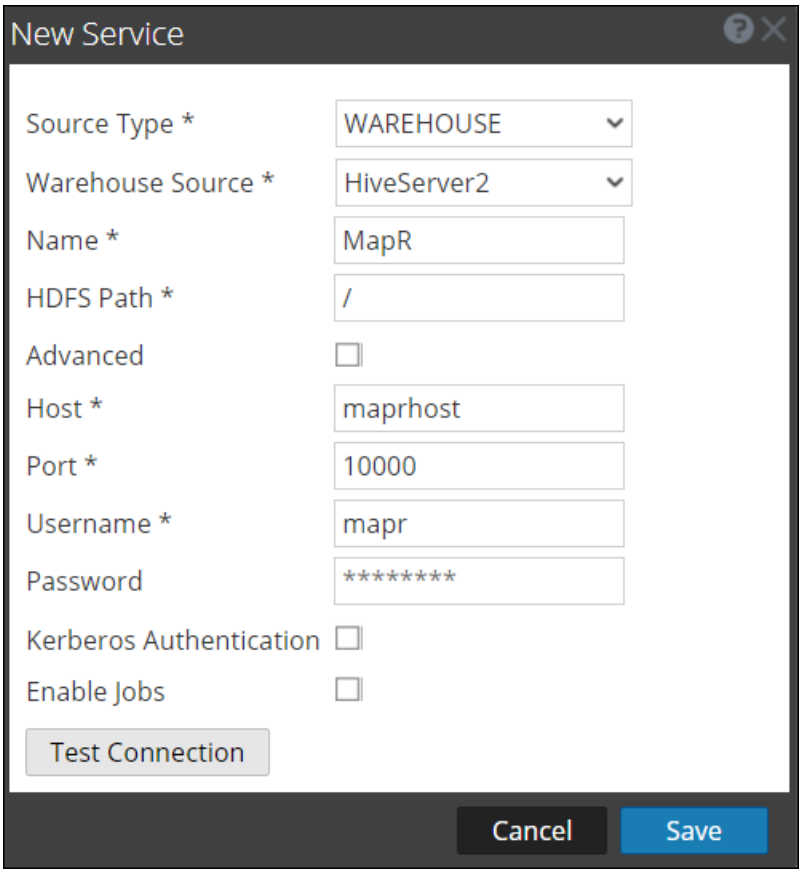
  Veillez également à mettre à jour le chemin d'accès au fichier de table de clés indiqué dans le paramètre **Fichier de table de clés Kerberos** figurant dans la vue Configuration des services du Reporting Engine. Pour plus d'informations, reportez-vous à l'Onglet General.

Pour ajouter la source de données Warehouse pour MapR :

1. Accédez à **Administrateur** > **Services**.
2. Dans la liste **Services**, sélectionnez le service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Config**.
4. Cliquez sur l'onglet **Sources**.

   La vue **Configuration des services** s'affiche avec l'onglet **Sources** Reporting Engine ouvert.
5. Cliquez sur  et sélectionnez **Nouveau service**.

   La boîte de dialogue Nouveau service s'affiche.



6. Dans le menu déroulant **Type de source**, sélectionnez **Warehouse**.
7. Dans le menu déroulant **Source Warehouse**, sélectionnez la source de données Warehouse.
8. Dans le champ **Nom**, saisissez le nom de l'hôte de la source de données Warehouse.
9. Dans le champ **Chemin HDFS**, indiquez le chemin d'accès racine HDFS sur lequel le Warehouse Connector écrit les données.

   Par exemple :
   Si **/saw** est le point de montage local de HDFS que vous avez configuré lors du montage de NFS sur le périphérique. Si vous avez installé le service Warehouse Connector pour écrire dans SAW. Pour plus d'informations, consultez la section Monter Warehouse sur Warehouse Connector dans le *Guide de configuration de RSA Netwitness Warehouse (MapR)*.

   Si vous avez créé un répertoire nommé **Ionsaw01** sous **/saw** et défini le chemin de montage local correspondant sur **/saw/Ionsaw01**, le chemin d'accès racine HDFS correspond à **/Ionsaw01**.

   Le point de montage **/saw** suppose que / est le chemin racine de HDFS. Le service Warehouse Connector écrit les données/ **Ionsaw01** dans HDFS. Si aucune donnée n'est disponible dans ce chemin, le message d'erreur suivant s'affiche :

   ```
   "No data available. Check HDFS path"
   ```

Vérifiez que **/lonsaw01/rsasoc/v1/sessions/meta** contient les fichiers avro des métadonnées avant d'effectuer le test de connexion.

10. Activez la case à cocher **Avancé** pour utiliser les paramètres avancés, puis renseignez le champ **URL de la base de données** avec l'URL JDBC complète pour vous connecter au serveur HiveServer2.

    Par exemple :
    Si Kerberos est activé en mode Hive, l'URL JDBC sera :

    ```
    jdbc:hive2://<host>:<port>/<db>;principal=<Kerberos serverprincipal>
    ```

    Si SSL est activé en mode Hive, l'URL JDBC sera :

    ```
    jdbc:hive2://<host>:<port>/<db>;ssl=true;sslTrustStore=<trust_store_
    path>;trustStorePassword=<trust_store_password>
    ```

    Pour plus d'informations sur les clients du serveur HIVE, consultez https://cwiki.apache.org/confluence/display/Hive/HiveServer2+Clients.

11. Si vous n'utilisez pas les paramètres avancés, indiquez les valeurs pour l'**Hôte** et le **Port**.

    - Dans le champ **Hôte**, saisissez l'adresse IP de l'hôte sur lequel HiveServer2 est hébergé.

      Remarque : Vous pouvez utiliser l'adresse IP virtuelle de MapR uniquement si HiveServer2 est exécuté sur tous les nœuds du cluster.

    - Dans le champ **Port**, saisissez le port HiveServer2 de la source de données Warehouse. Le numéro de port par défaut est **10000**.

12. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification JDBC permettant d'accéder au serveur HiveServer2.

    Remarque : Vous pouvez également utiliser le mode d'authentification LDAP via Active Directory. Pour plus d'instructions sur l'activation du mode d'authentification LDAP, consultez la rubrique Activer l'authentification LDAP.

13. Pour exécuter des rapports Warehouse Analytics, consultez Activer des tâches dans Configuration des sources de données pour Reporting.

14. Activer l'authentification Kerberos : consultez Activer l'authentification Kerberos dans Configuration des sources de données pour Reporting.

15. Si vous souhaitez désigner la source de données Warehouse ajoutée en tant que source par défaut du Reporting Engine, sélectionnez-la, puis cliquez sur Set default.

Pour ajouter une source de données Warehouse pour Hortonworks (HDP) :

Remarque : Assurez-vous de télécharger `hive-jdbc-1.2.1-with-full-dependencies.jar`. Ce fichier jar contient le fichier du pilote de Hive 1.2.1 qui se connecte au Reporting Engine pour Hiveserver2 Hive 1.2.1, à partir de RSA Link (https://community.rsa.com/docs/DOC-67251).

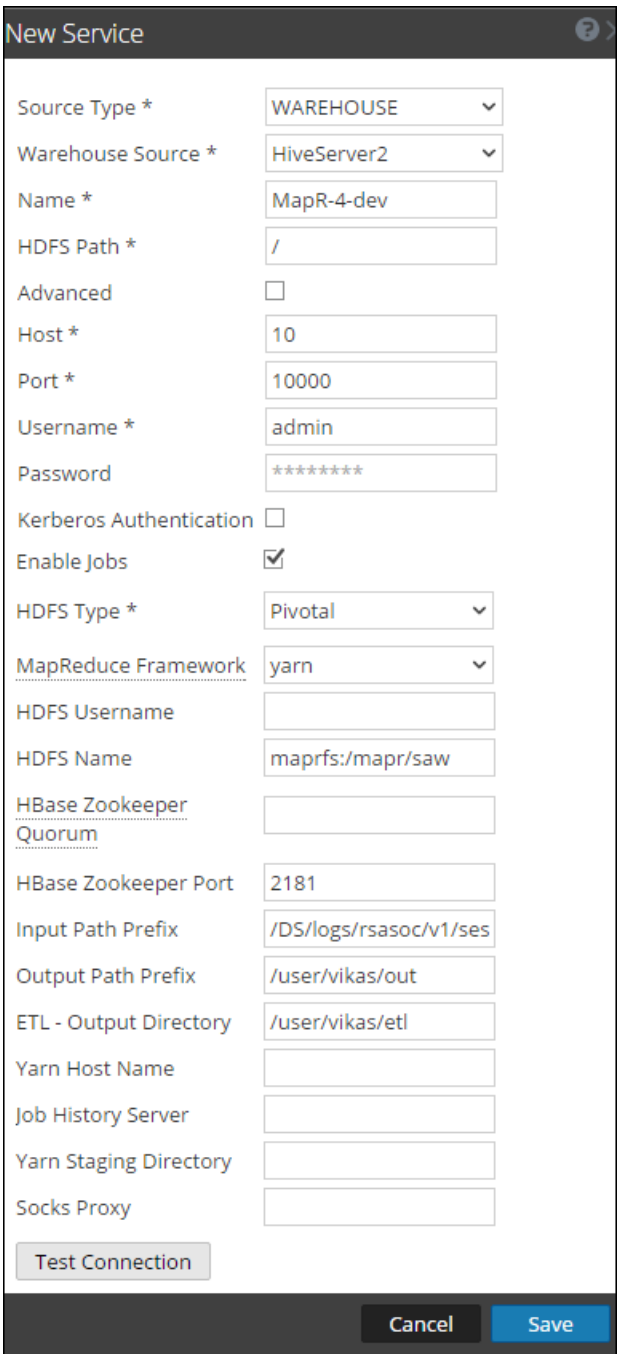
1. Connexion en SSH au serveur Netwitness Suite.
2. Dans le dossier `/opt/rsa/soc/reporting-engine/plugins/`, effectuez la sauvegarde du fichier jar suivant :
   `hive-jdbc-0.12.0-with-full-dependencies.jar` ou`hive-jdbc-1.0.0-mapr-1508-standalone.jar`
3. Supprimer le fichier jar suivant :
   `hive-jdbc-0.12.0-with-full-dependencies.jar` ou `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
4. Dans le dossier /opt/rsa/soc/reporting-engine/plugins, copiez le fichier jar suivant à l'aide de WinSCP :
   `hive-jdbc-1.2.1-with-full-dependencies.jar`
5. Redémarrez le service Reporting Engine.
6. Connectez-vous à l'interface utilisateur NetWitness Suite.
7. Sélectionnez un service **Reporting Engine** et sélectionnez  > **Vue** > **Explorer**.
8. Dans **hiveConfig**, définissez le **paramètre EnableSmallSplitBasedSchemaLiteralCreation** sur **true**.

Activer des tâches

Remarque : Warehouse Analytics n'est pas pris en charge dans NetWitness Suite 11.0.

Pour exécuter des rapports Warehouse Analytics, effectuez cette procédure.

1. Cochez la case **Activer des tâches**.



Remarque : Ne sélectionnez pas Pivotal dans le champ HDFS puisqu'il n'est pas pris en charge dans cette version.

2. Vous pouvez saisir les détails suivants :

a. Dans le menu déroulant **Type de HDFS**, sélectionnez le type de HDFS.

- Si vous sélectionnez le type HDFS Hortonworks, saisissez les informations suivantes :

Champ	Description
Nom d'utilisateur HDFS	Saisissez le nom d'utilisateur que le Reporting Engine doit demander lors de la connexion à Hortonworks. Pour les clusters Hortonworks DCA standard, il s'agit de « gpadmin ».
Nom HDFS	Saisissez l'URL pour accéder à HDFS Par exemple, hdfs://hdm1.gphd.local:8020.
Quorum Zookeeper HBase	Saisissez la liste des noms d'hôte séparés par une virgule sur lesquels les serveurs ZooKeeper s'exécutent.
Port Zookeeper HBase	Saisissez le numéro de port des serveurs ZooKeeper. Le port par défaut est 2181.
Préfixe de chemin d'entrée	Saisissez le chemin de sortie de Warehouse Connector (`/sftp/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) jusqu'au répertoire year. Par exemple, `/sftp/rsasoc/v1/sessions/data/`.
Préfixe de chemin de sortie	Indiquez l'emplacement de stockage des résultats des tâches Data Science sur HDFS.
Nom d'hôte Yarn	Indiquez le nom d'hôte resource-manager Hadoop yarn sur le cluster DCA. Par exemple, **hdm3.gphd.local**.
Serveur d'historique des tâches	Indiquez l'adresse job-history-server Hadoop sur le cluster DCA. Par exemple, **hdm3.gphd.local:10020**.
Répertoire de reclassement Yarn	Indiquez le répertoire de reclassement pour YARN sur le cluster DCA. Par exemple, `/user`.

Champ	Description
Proxy Socks	Si vous utilisez le cluster DCA standard, la plupart des services Hadoop s'exécutent sur un réseau privé local qui n'est pas accessible à partir de Reporting Engine. Vous devez alors exécuter un proxy socks dans le cluster DCA et autoriser l'accès de l'extérieur vers le cluster. Par exemple, **mdw.netwitness.local:1080**.

- Si vous sélectionnez le type HDFS MapR, saisissez les informations suivantes :

Champ	Description
Nom d'hôte MapR	Indiquez éventuellement l'adresse IP publique d'un des hôtes Warehouse MapR.
Utilisateur hôte MapR	Indiquez un nom d'utilisateur UNIX sur l'hôte qui bénéficie d'un accès pour exécuter des tâches map-reduce sur le cluster. La valeur par défaut est « mapr ».
Mot de passe hôte MapR	(Facultatif) Pour autoriser l'authentification sans mot de passe, copiez la clé publique de l'utilisateur « rsasoc » du paramètre **/home/rsasoc/.ssh/id_rsa.pub** dans le fichier « authorized_keys » de l'hôte Warehouse situé dans **/home/mapr/.ssh/authorized_keys**, en partant du principe que « mapr ╗ correspond à l'utilisateur UNIX distant.
Rép travail hôte MapR	Saisissez le chemin d'accès à un emplacement pour lequel l'utilisateur UNIX donné (« mapr », par exemple) dispose d'un accès en écriture. **Remarque :** Le répertoire de travail est utilisé par le Reporting Engine pour copier à distance les fichiers jar de Warehouse Analytics et lancer la tâche à partir du nom d'hôte donné. Il ne faut en aucun cas utiliser « /tmp » car cela saturerait l'espace temporaire du système. Le répertoire de travail sera géré à distance par le Reporting Engine.
Nom HDFS	Saisissez l'URL pour accéder à HDFS Par exemple, pour accéder à un cluster spécifique, maprfs:/mapr/<nom-cluster>.

Champ	Description
Port Zookeeper HBase	Saisissez le numéro de port des serveurs ZooKeeper. Le port par défaut est 5181.
Préfixe de chemin d'entrée	Saisissez le chemin de sortie (`/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) jusqu'au répertoire year. Par exemple, `/rsasoc/v1/sessions/data/`.
Nom de fichier d'entrée	saisissez le filtre de nom de fichier pour les fichiers avro. Par exemple, **sessions-warehouseconnector**.
Préfixe de chemin de sortie	Indiquez l'emplacement de stockage des résultats des tâches Data Science sur HDFS.

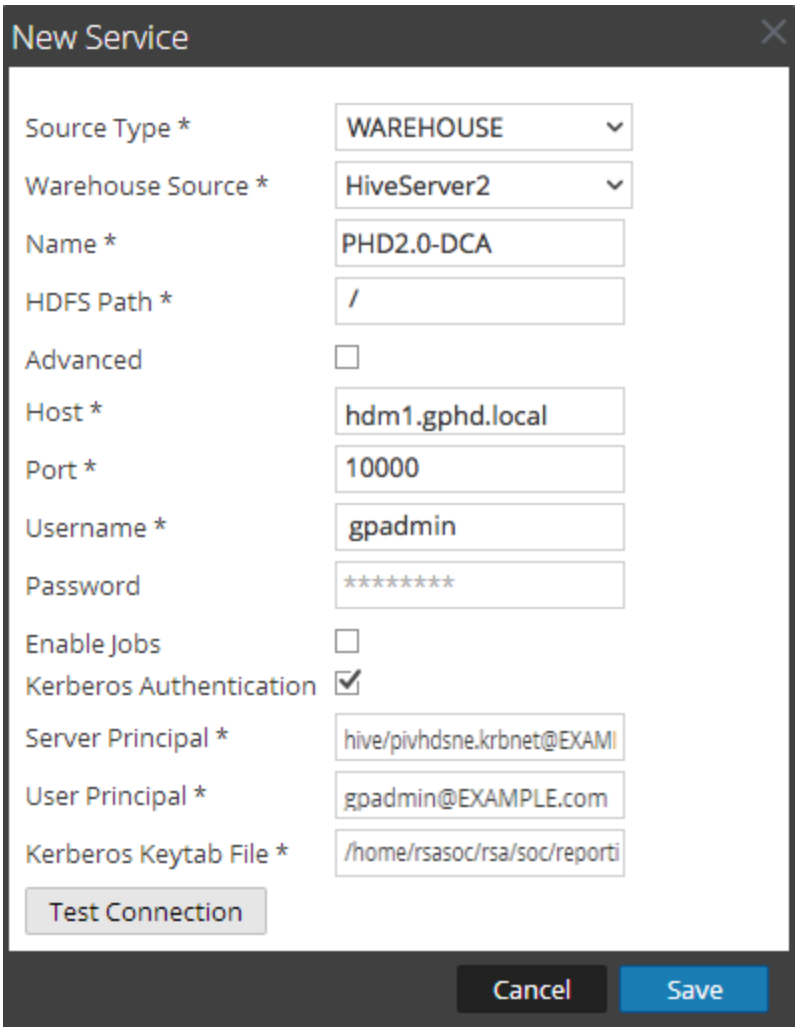
b. Sélectionnez le framework MapReduce en fonction du type HDFS.

Remarque : Pour le type HDFS MapR, sélectionnez Classic pour le framework MapReduce. Pour le type HDFS Hortonworks, sélectionnez Yarn pour le framework MapReduce.

Ensuite, activez l'authentification Kerberos.

Activer l'authentification Kerberos

1. Cochez la case **Authentification Kerberos** si le Warehouse dispose d'un serveur Hive sur lequel Kerberos est activé.



2. Renseignez les champs comme suit :

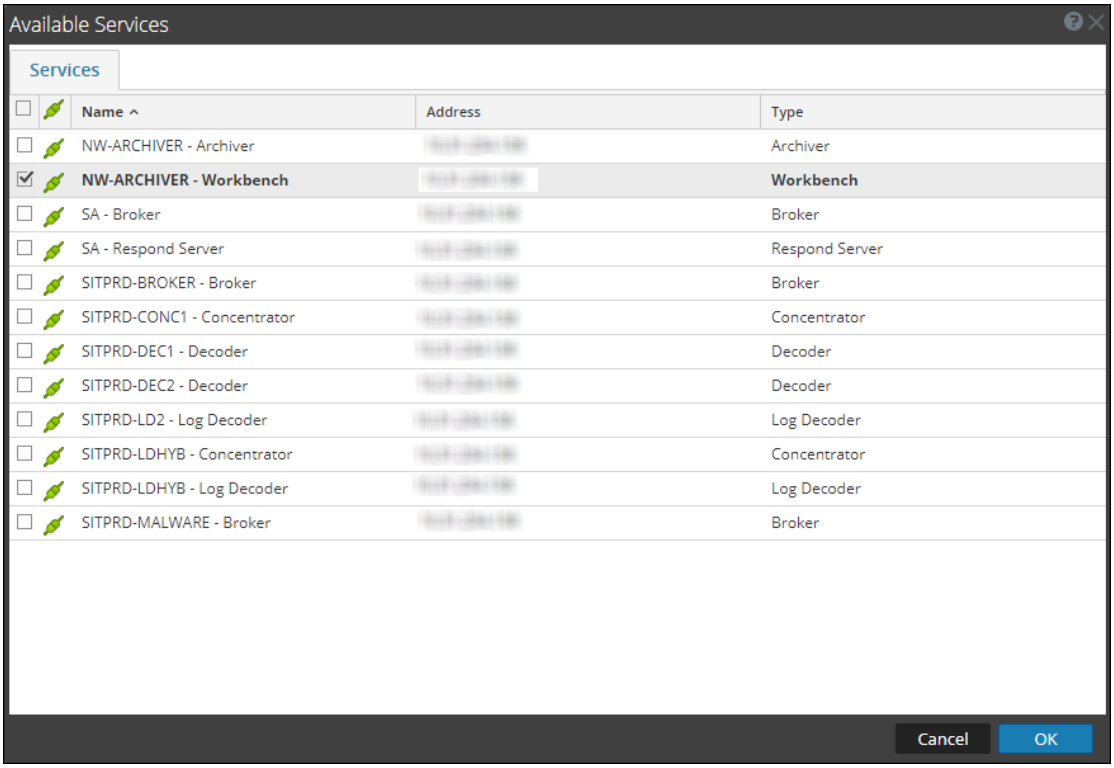
Champ	Description
Entité de sécurité du serveur	Indiquez l'entité de sécurité que le serveur Hive utilise afin de procéder à l'authentification auprès du centre de distribution de clés (KDC) Kerberos.
Entité de sécurité de l'utilisateur	Saisissez l'entité de sécurité que le client JDBC Hive utilise pour s'authentifier auprès du serveur KDC et se connecter au serveur Hive. Par exemple, **gpadmin@EXAMPLE.COM**.

Champ	Description
Fichier de table de clés Kerberos	Affichez le chemin d'accès au fichier de table de clés Kerberos configuré dans le panneau Configuration de Hive dans la rubrique Onglet Général du Reporting Engine. **Remarque :** Le Reporting Engine ne prend en charge que les sources de données configurées avec les mêmes informations d'identification Kerberos, comme l'entité de sécurité de l'utilisateur et le fichier de table de clés.

3. Cliquez sur **Tester la connexion** pour réaliser un test avec les valeurs saisies.
4. Cliquez sur **Enregistrer**.

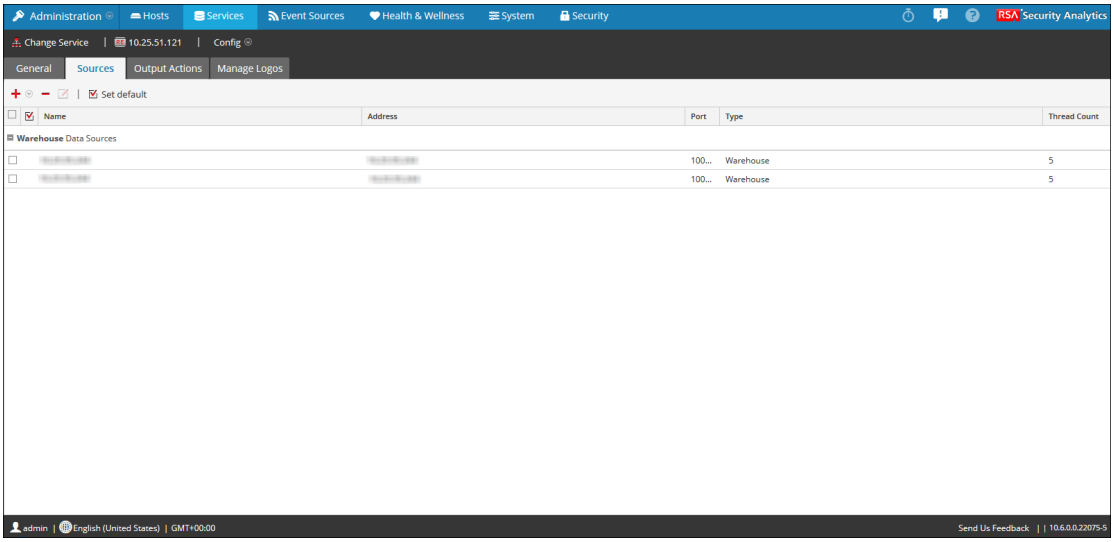
   La source de données Warehouse ajoutée s'affiche sous l'onglet Sources du Reporting Engine.
5. Cliquez sur + > **Services disponibles**.

   La boîte de dialogue Services disponibles s'affiche.



6. Dans la boîte de dialogue Services disponibles, sélectionnez le service que vous souhaitez ajouter comme source de données au Reporting Engine, puis cliquez sur **OK**.

NetWitness Suite ajoute la source de données disponible lors de la génération de rapports et d'alertes dans le cadre de ce Reporting Engine.



Remarque : Cette étape est requise uniquement lorsqu'on utilise un modèle non fiable.

Définir une source de données comme source par défaut

Pour définir une source de données comme source par défaut lors de la génération de rapports et d'alertes :

1. Accédez à **Dashboard** > **Administration** > **Services**.
2. Dans la liste **Services**, sélectionnez un service **Reporting Engine**.
3. Sélectionnez > **Vue** > **Config**.

   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.

   La vue **Configuration des services** s'ouvre sur l'onglet Sources du Reporting Engine.
5. Sélectionnez la source à définir par défaut (Broker, par exemple).
6. Cochez la case **Définir la valeur par défaut**.

   NetWitness Suite est défini sur cette source de données par défaut lorsque vous créez des rapports et des alertes dans le cadre de ce Reporting Engine.

(Facultatif) Ajouter Workbench comme source de données

Vous devez exécuter les configurations Workbench suivantes afin de pouvoir utiliser les données de la source de données Workbench afin de générer Rapports et Alertes : Cette rubrique donne des instructions sur la façon d'ajouter le service Workbench comme source de données au Reporting Engine afin de générer un rapport pour les données collectées par Workbench.

Conditions préalables

Assurez-vous d'avoir :

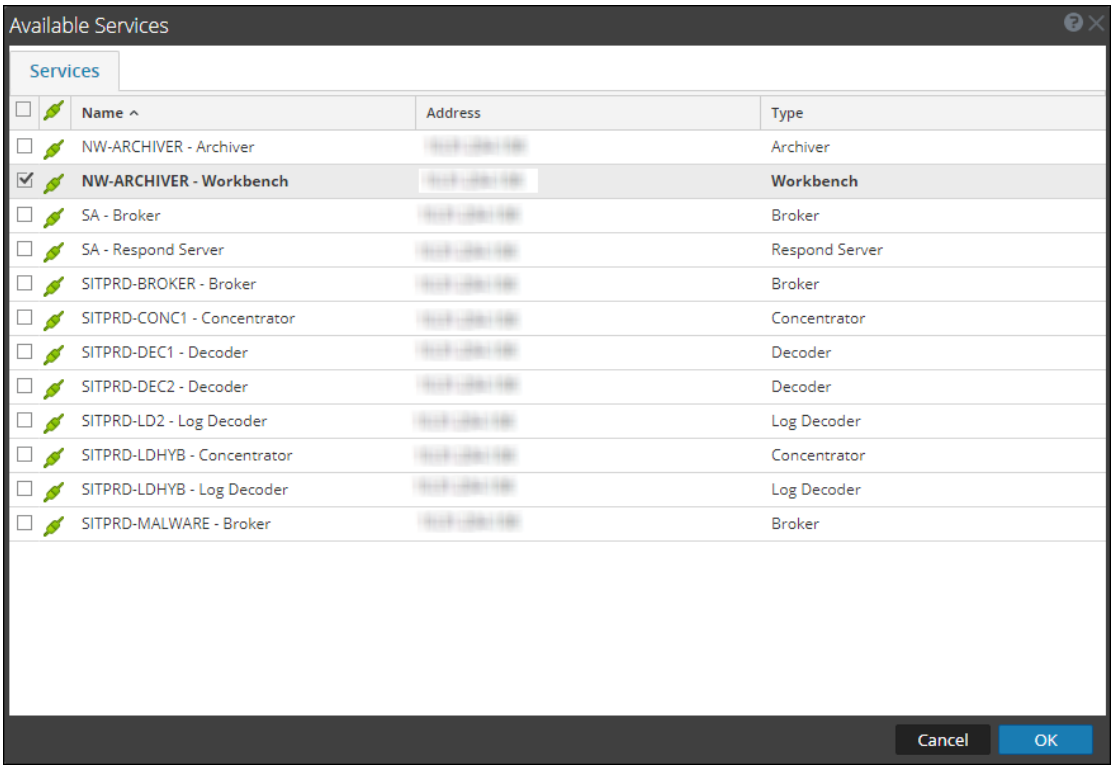
1. Workbench ajouté en tant que service à votre déploiement NetWitness Suite. Pour plus d'informations, consultez le *Guide de configuration d'Archiver*.
2. Ajouté une collection au service Workbench.

Pour ajouter Workbench comme source de données au Reporting Engine

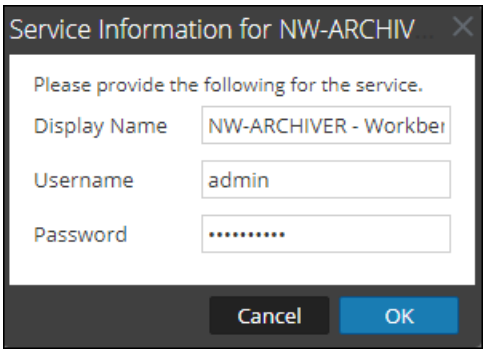
1. Accédez à ADMIN > **Services**.
2. Dans la liste **Services**, sélectionnez un service **Reporting Engine**.
3. Sélectionnez  >**Vue** > **Config**.

   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.
5. Cliquez sur  et sélectionnez **Services disponibles**.

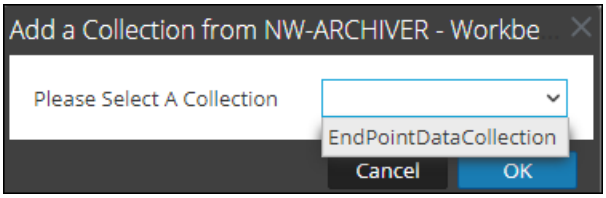
   La boîte de dialogue Services disponibles s'affiche :



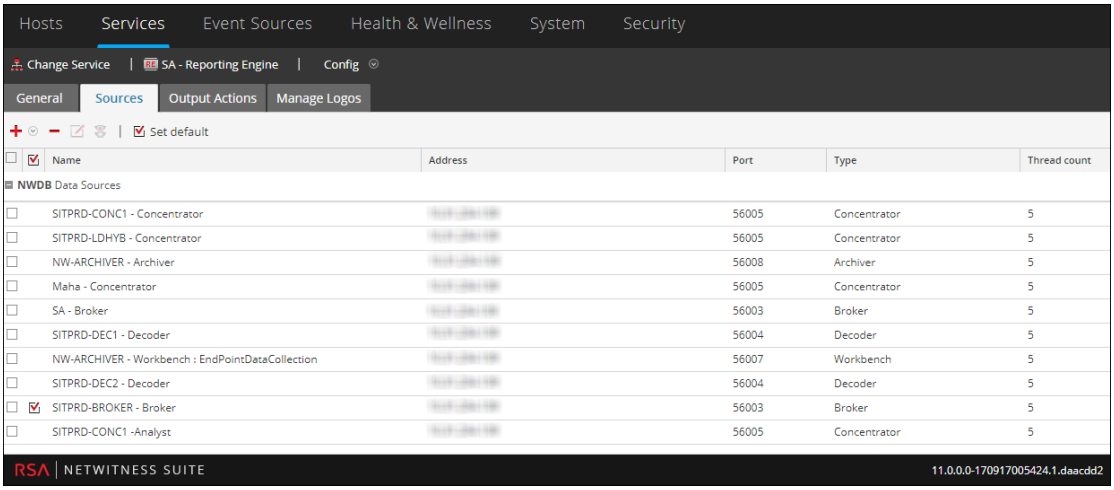
6. Sélectionnez le service Workbench et cliquez sur **OK**.
   Une liste des collections s'affiche.
7. Saisissez les informations de services, puis cliquez sur **OK**



8. Sélectionnez une collection dans la liste déroulante.



9. La source de données s'affiche dans l'onglet Sources.



Le service Workbench est maintenant ajouté comme source de données au Reporting Engine.

Remarque : Les services dont le Modèle de confiance est activé doivent être ajoutés individuellement. Il vous est demandé de fournir un nom d'utilisateur et un mot de passe pour le service sélectionné.

(Facultatif) Ajouter Archiver comme source de données

Vous devez exécuter les configurations Archiver suivantes afin de pouvoir utiliser les données de la source de données Archiver afin de générer Rapports et Alertes :

Conditions préalables

Assurez-vous d'avoir :

1. installé l'hôte Archiver NetWitness Suite dans votre environnement réseau. Pour plus d'informations, reportez-vous au *Guide de mise en route des hôtes et des services*.
2. Log Decoder installé et configuré dans votre environnement réseau. Pour plus d'informations, consultez la section « Ajouter un service Log Decoder en tant que source de données à un service Archiver » dans le *Guide de configuration d'Archiver*.
3. Le Reporting Engine est disponible en tant que service dans votre déploiement NetWitness Suite.
4. Archiver ajouté en tant que service à votre déploiement NetWitness Suite. Pour plus d'informations, consultez la section « Ajouter le service Archiver » dans le *Guide de*

configuration d'Archiver.

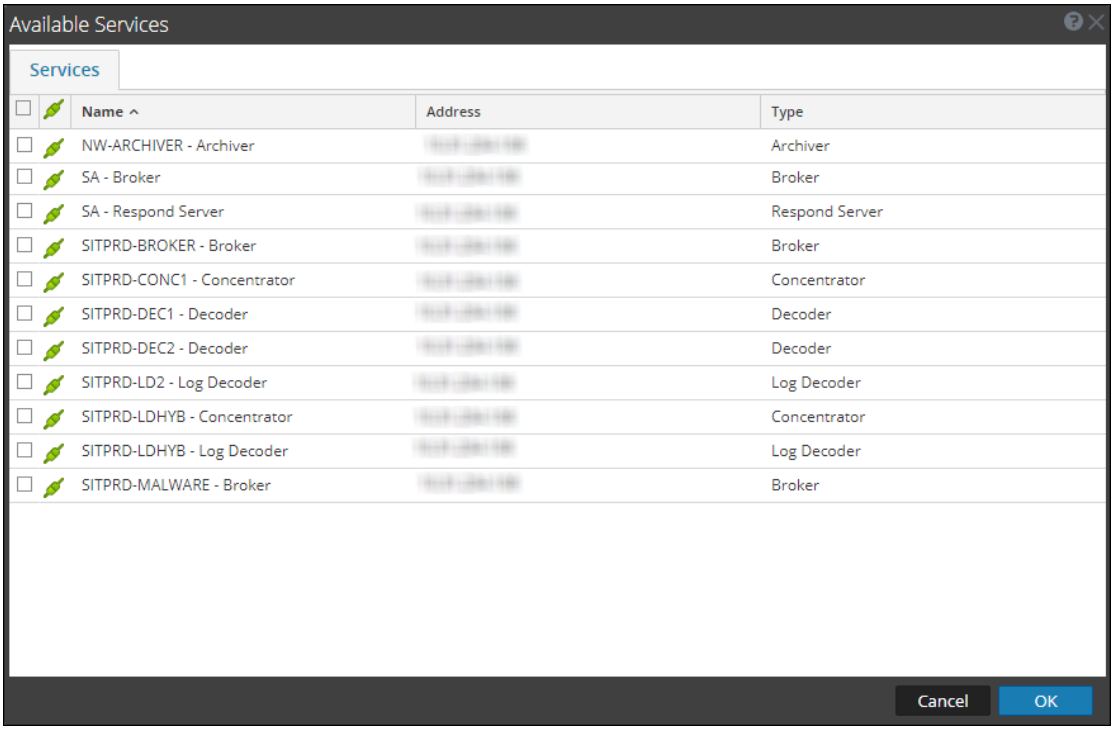
5. Attribué une licence au service Archiver.

Pour ajouter Archiver comme source de données au Reporting Engine :

1. Accédez à **ADMIN** > **Services**.
2. Dans le panneau **Services**, sélectionnez le service **Reporting Engine**.
3. Cliquez sur > **Vue** > **Config**.

   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.
5. Cliquez sur et sélectionnez **Services disponibles**.

   La boîte de dialogue Services disponibles s'affiche.



6. Sélectionnez le service Archiver et cliquez sur **OK**.

   La boîte de dialogue d'authentification du service s'affiche.

   Remarque : Les services dont le Modèle de confiance est activé doivent être ajoutés individuellement. Il vous est demandé de fournir un nom d'utilisateur et un mot de passe pour le service sélectionné.

7. Saisissez le nom d'utilisateur et le mot de passe d'Archiver.

8. Cliquez sur **OK**.

   L'Archiver sélectionné est répertorié dans le panneau Services agrégés.

(Facultatif) Intégrer les informations Endpoint aux Rapports

Vous pouvez utiliser les données Endpoint en utilisant les instructions suivantes et en ajoutant les informations Endpoint dans des rapports. Le *Guide d'intégration de RSA Endpoint* fournit une vue d'ensemble de l'intégration Endpoint dans RSA NetWitness Suite.

Conditions préalables

Vérifiez que :

- Vous avez configuré les alertes Endpoint via syslog dans un Log Decoder. Pour plus d'informations, reportez-vous à la rubrique « Configurer des alertes Endpoint via Syslog dans un Log Decoder » dans le *Guide d'intégration de RSA Endpoint*.

Pour intégrer les informations Endpoint aux Rapports :

1. Dans le **Reporting Engine**> **Vue**> **Config**> **Sources**.
2. Ajoutez le Concentrator qui consomme des données dans le Log Decoder en tant que source de données.

   La méta Endpoint est renseignée dans le Reporting Engine.
3. Exécutez des rapports en sélectionnant l'élément méta approprié.

(Facultatif) Ajouter la collection comme source de données au Reporting Engine

Vous devez exécuter les configurations Collection suivantes afin de pouvoir utiliser les données de la source de données Collection pour générer Rapports et Alertes :

Conditions préalables

Assurez-vous d'avoir :

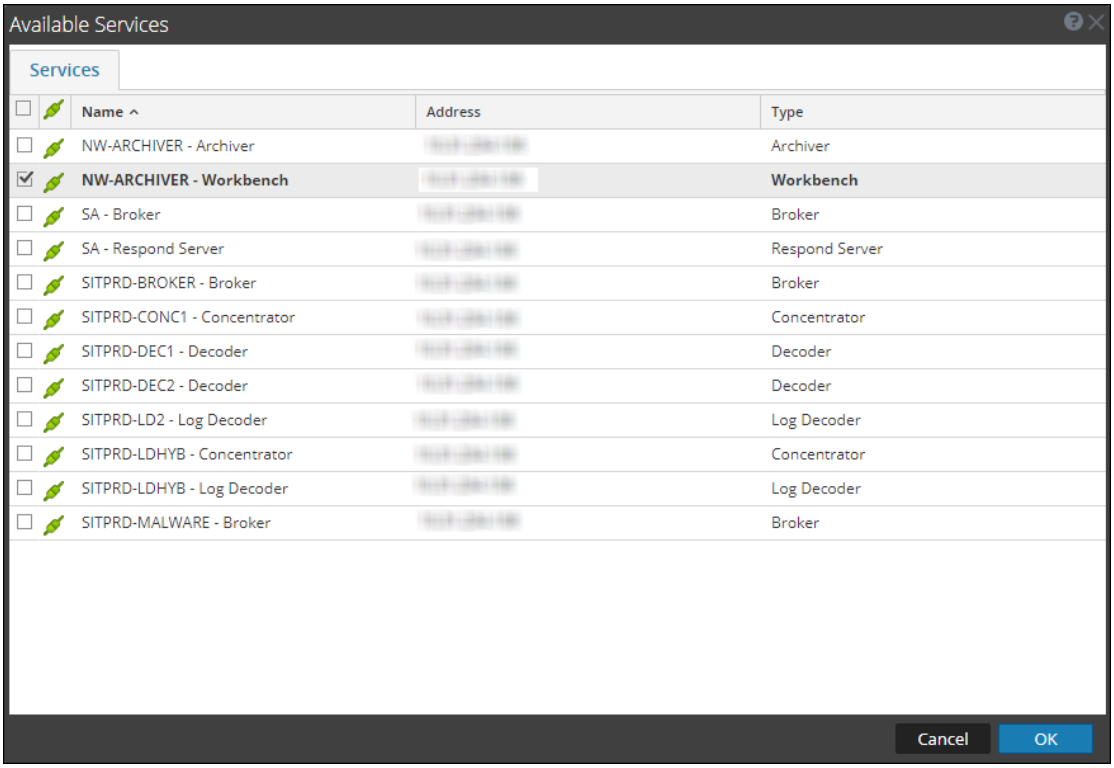
- Installé le service Workbench sur un hôte Reporting Engine.
- Sauvegardé les données dans un emplacement connu sur votre hôte local, si vous ajoutez une collection en utilisant les données restaurées à partir des données sauvegardées.

Pour associer une Collection comme source de données au Reporting Engine :

1. Accédez à **ADMIN** > **Services**.
2. Dans la liste **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur > **Vue** > **Config**.

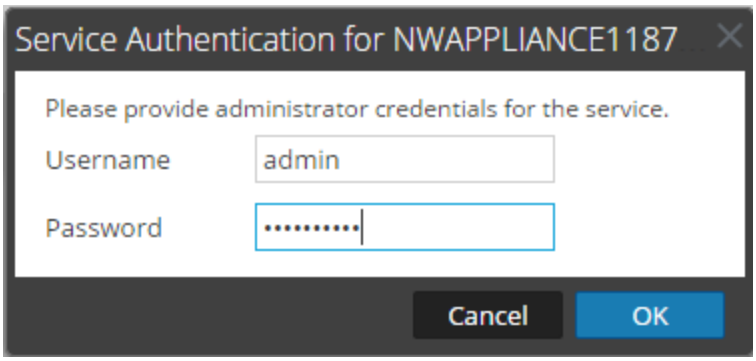
   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.
5. Cliquez sur et sélectionnez **Services disponibles**.

   La boîte de dialogue Services disponibles s'affiche.



6. Sélectionnez le service Workbench et cliquez sur **OK**.

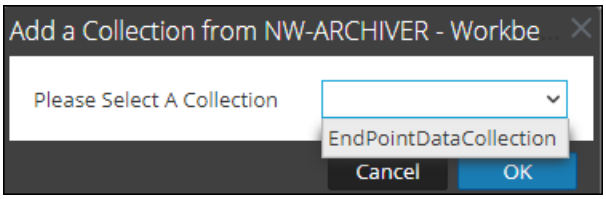
   La boîte de dialogue Authentification du service pour le service sélectionné s'affiche.



Remarque : Les services dont le Modèle de confiance est activé doivent être ajoutés individuellement. Il vous est demandé de fournir un nom d'utilisateur et un mot de passe pour le service sélectionné.

7. Saisissez le nom d'utilisateur et le mot de passe administrateur du service.
8. Cliquez sur **OK**.

   La boîte de dialogue Ajouter une collection s'affiche.



9. Sélectionnez une collection dans la liste déroulante et cliquez sur **OK**.

   Le service Workbench est maintenant ajouté comme source de données au Reporting Engine.

Configurer la confidentialité des données pour le Reporting Engine

Vous pouvez configurer la confidentialité des données pour toutes les sources de données de Reporting Engine à l'aide de l'onglet Sources de Services > Vue > Vue Configuration.

Avec l'ajout de la fonction de confidentialité des données de NetWitness Suite 11.0 et versions ultérieures, l'accès aux métadonnées sensibles dans les services NetWitness Suite Core peut être limité. Cela peut être fait en configurant des sources de données distinctes pour les utilisateurs dotés du rôle de Responsable de la confidentialité des données et pour les autres utilisateurs, et en attribuant les autorisations appropriées.

Dans la vue Configuration des services, vous pouvez ajouter chaque service Core sous la forme de deux sources de données distinctes : l'une avec un compte de service ayant des privilèges équivalents au Responsable de la confidentialité des données, et l'autre avec un compte de service ayant des privilèges équivalents à tout autre utilisateur. Ensuite, pour limiter l'accès à ces sources de données basées sur les rôles, vous pouvez attribuer un accès en lecture ou aucun accès du tout aux rôles individuels. Pour limiter l'accès aux sources de données Warehouse, vous pouvez procéder de la même manière.

Pour plus d'informations, reportez-vous à la rubrique Configurer les autorisations d'accès aux sources de données.

Remarque : Un utilisateur associé au rôle de `Data_Privacy_Officers` (ou autre rôle personnalisé équivalent) peut créer un rapport, un graphique et une alerte. Configurez également un rapport ou des actions de sortie dans le module Reporting. Dans un environnement où les fonctions de confidentialité des données de NetWitness Suite sont activées et une ou plusieurs clés méta sont configurées comme étant protégées, ces actions peuvent donner lieu à ce qui suit :

- Lorsqu'une alerte est créée par un utilisateur responsable de la confidentialité des données, toutes les métadonnées protégées ou sensibles impliquées dans l'alerte sont automatiquement rendues disponibles dans le service Répondre. Par inadvertance, cela risque de permettre à tous les utilisateurs du module Répondre, quels que soient leurs rôles, d'accéder aux métavaleurs sensibles. Pour éviter cela, une option consiste à désactiver la publication sous Répondre, dans Reporting.
- Lorsqu'une action de sortie est configurée par un utilisateur responsable de la confidentialité des données, soit les métavaleurs sensibles, soit les rapports avec des métavaleurs sensibles ou les deux, peuvent devenir disponibles pour cibler les utilisateurs ou les destinations de cette action de sortie, quel que soit le rôle attribué à l'utilisateur cible.

Il est fortement recommandé que les utilisateurs responsables de la confidentialité des données évitent totalement de créer des alertes ou de configurer des actions de sortie sous la forme d'un rapport ou d'une alerte dans le module Reporting. S'ils optent pour une telle configuration, ils doivent examiner avec soin ce que cela implique.

Les services NetWitness Suite Core (par exemple, Concentrator, Broker ou Archiver) ont la possibilité de restreindre les métadonnées basées sur le rôle d'utilisateur configuré. Pour utiliser la fonction de confidentialité des données pour le Reporting Engine, vous pouvez configurer deux comptes de service distincts par rapport à Core. Un compte de service pour le reporting général ne contenant pas de données sensibles et un autre compte pour les utilisateurs privilégiés avec un accès à toutes les données y compris les données sensibles. L'accès aux métadonnées restreintes pour les deux comptes de service est configuré dans le cadre du plan de confidentialité des données sur chaque service Core.

Dans Reporting Engine, vous pouvez ajouter chaque service Core sous la forme de deux sources de données distinctes (une pour la source de données standard et l'autre pour la source de données privilégiée) à l'aide des deux comptes de service distincts. Vous pouvez configurer Reporting Engine pour autoriser uniquement les utilisateurs dotés des rôles privilégiés à accéder à la source de données sensibles. Par conséquent, Reporting Engine peut se connecter à une source de données NWDB de deux manières possibles :

- Utilisation d'un compte de service avec le rôle de Responsable de la confidentialité des données.
- Utilisation d'un compte de service sans le rôle de Responsable de la confidentialité des données.

Remarque : Vous pouvez également ajouter au moins deux sources de données pour le même service Core.

Après l'ajout des deux sources de données avec différents comptes de service pour le même service Core, vous pouvez configurer des autorisations d'accès aux sources de données qu'il est possible de gérer. Pour plus d'informations, reportez-vous à la rubrique Configurer les autorisations d'accès aux sources de données.

Remarque : Si le contenu est modifié pour utiliser la clé méta, la valeur de hachage du méta d'origine s'affiche à la place lors de la consultation des rapports, des graphiques et des alertes.

Ajouter une source de données NWDB avec différents comptes de service

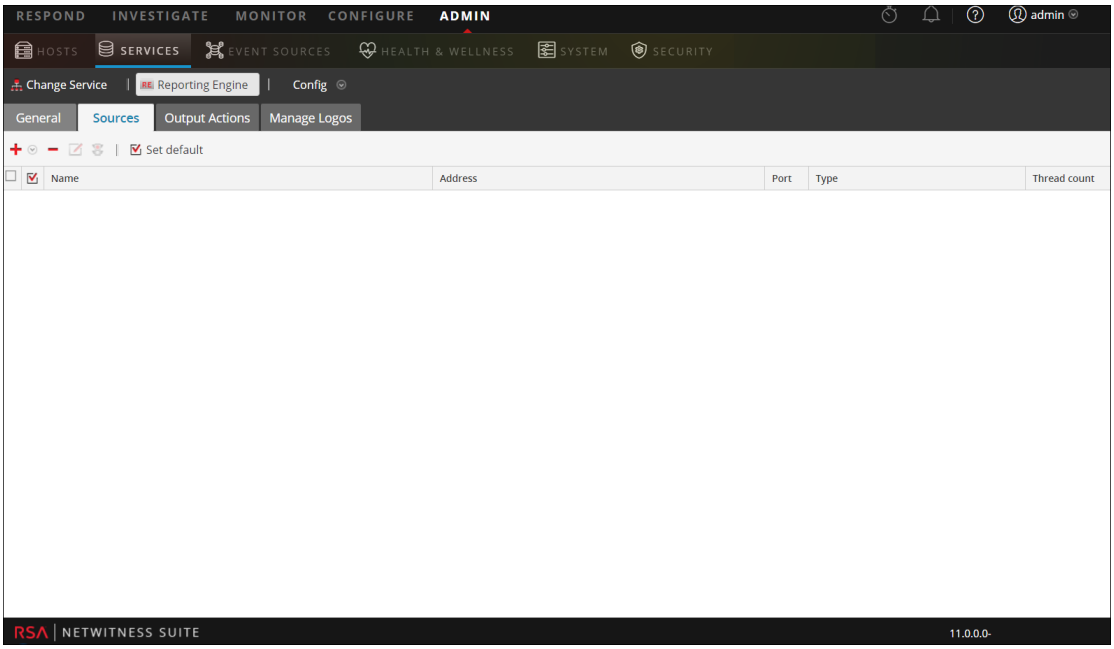
Pour ajouter une source de données NWDB :

1. Accédez à **ADMIN** > **Services**.
2. Dans la liste **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  **Vue** > **Config**.

   La vue Configuration des services du Reporting Engine s'affiche.

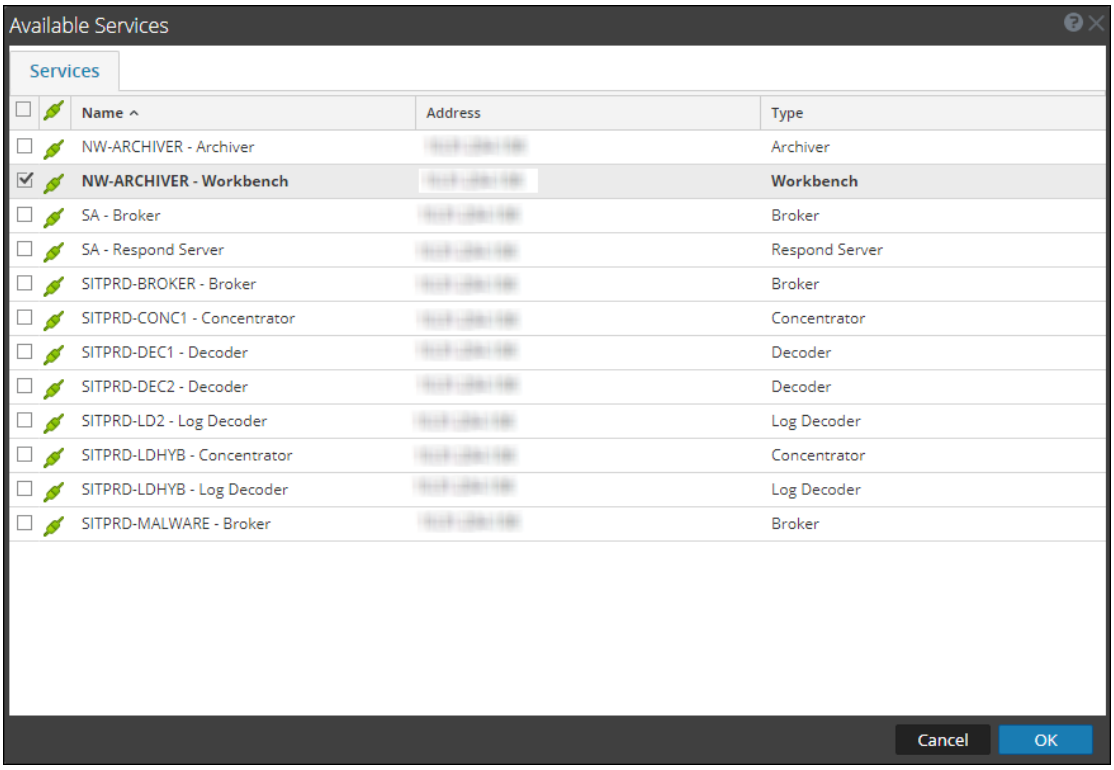
4. Sélectionnez l'onglet **Sources**.

   La vue Configuration des services s'affiche.



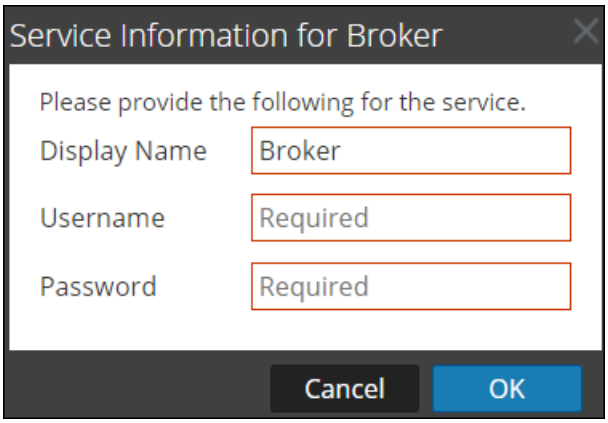
5. Cliquez sur + et sélectionnez Services disponibles.

   La boîte de dialogue Services disponibles s'affiche. Tous les services apparaissent, y compris ceux qui ont déjà été ajoutés au Reporting Engine.



6. Sélectionnez la case à cocher à côté du service, puis cliquez sur **OK**.

   La boîte de dialogue Informations de service du service sélectionné s'affiche.

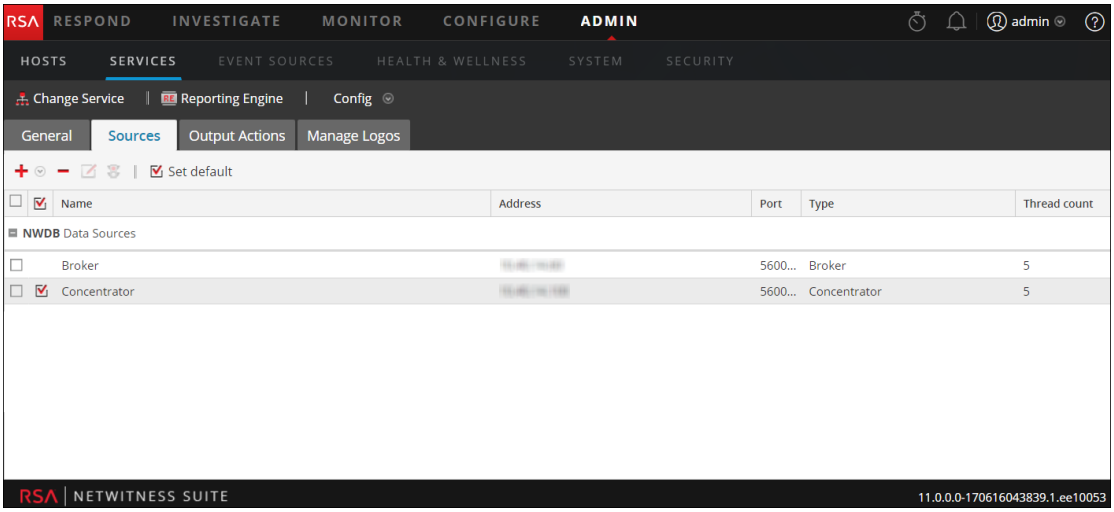


Remarque : NetWitness Suite vous demande de fournir un nom d'utilisateur et un mot de passe pour le service sélectionné. Pour limiter l'accès aux données sensibles, les utilisateurs responsables de la confidentialité des données doivent utiliser leurs informations d'identification, tout en ajoutant la source au lieu d'utiliser les informations d'identification d'administrateur. Ces informations d'identification doivent être appliquées à l'hôte, même en cas d'utilisation de connexions fiables entre le serveur NetWitness Suite et les hôtes NetWitness Suite Core.

Répétez la procédure pour la source de données non soumise à la confidentialité des données

7. Saisissez le nom d'utilisateur et le mot de passe du compte de service requis.
8. Cliquez sur **OK**.

   Le service requis est ajouté comme source de données au Reporting Engine. Deux sources de données sont ajoutées au Reporting Engine pour le même périphérique Core.



Configurer les autorisations d'accès aux sources de données

Vous pouvez configurer des autorisations de sources de données en utilisant l'onglet Sources de la vue Configuration des services pour le Reporting Engine. Cela permet de gérer le contrôle d'accès aux sources de données en définissant les autorisations de source de données. Désormais, avec la capacité d'ajouter plusieurs sources de données pour le même service Core, vous pouvez configurer différentes autorisations pour chaque source de données du même service Core. Par exemple, les Responsables de la confidentialité des données (DPO) peuvent créer une source Warehouse en utilisant leurs informations d'identification. Cela leur permet d'exécuter des rapports avec Warehouse tout en restreignant l'utilisation de cette source pour toute autre personne.

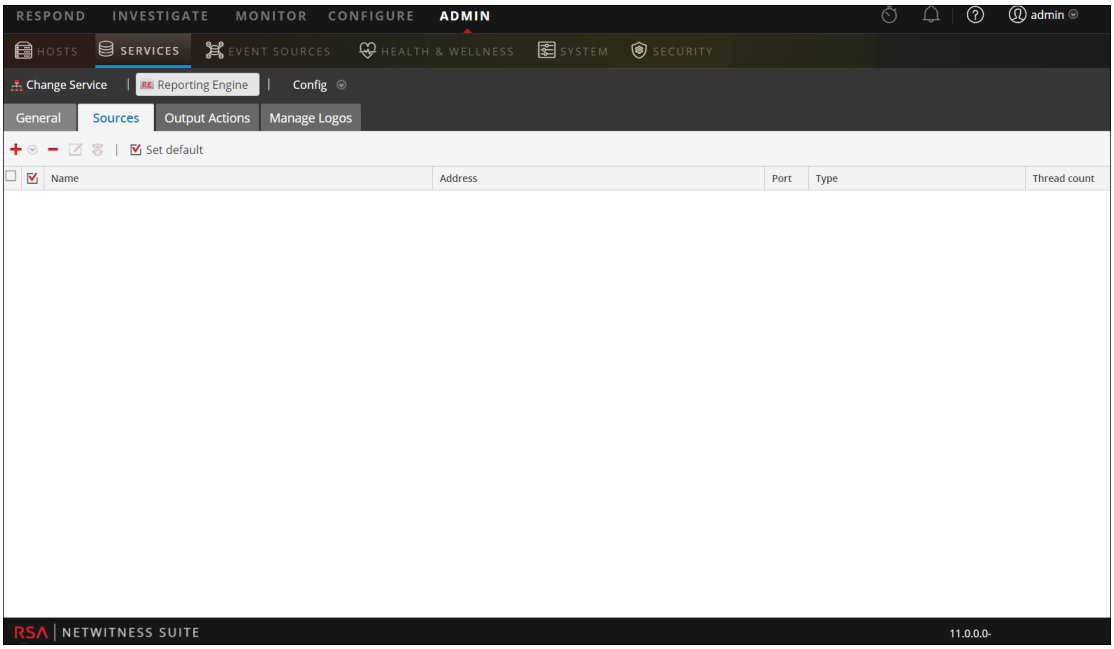
Remarque : Dans la version 11.0, les autorisations de NWDB et des sources de données Warehouse sont automatiquement définies d'après les autorisations des objets de reporting. Par exemple, si le rôle avait des autorisations définies en **Lecture seule**/**Lecture et écriture** pour tout objet de reporting dans la version 10.5, ce rôle se voit automatiquement attribué l'autorisation de lecture seule pour toutes les sources de données qui existaient dans la version 10.5. Si aucune autorisation n'est définie pour le rôle, l'autorisation de source de données est automatiquement définie sur Aucun accès.

Pour configurer les autorisations d'accès aux sources de données :

1. Accédez à **Administrateur** > **Services**.
2. Dans la liste **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Config**.

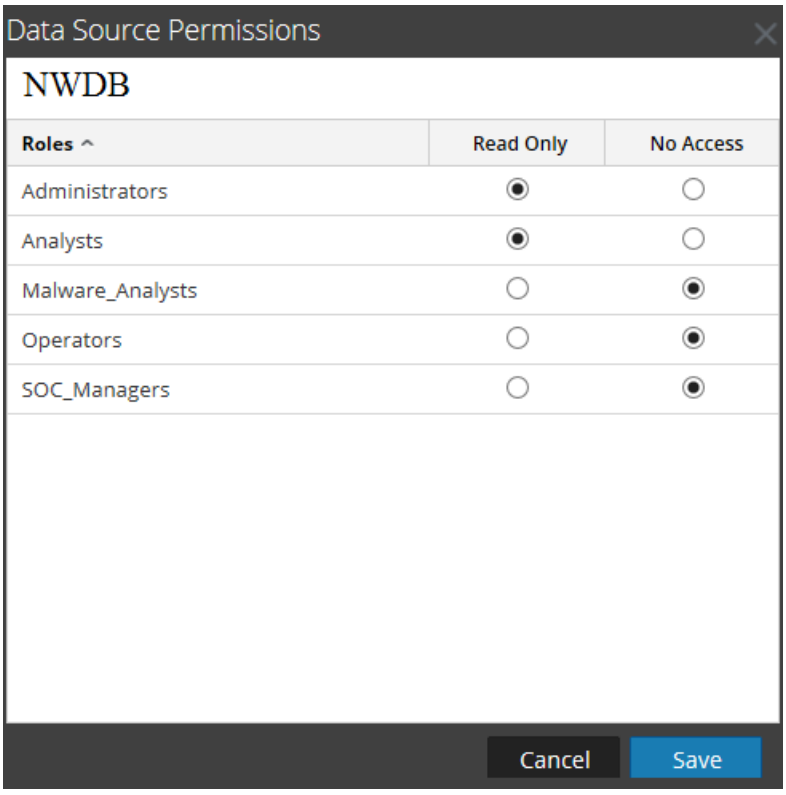
   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.

   La vue Configuration des services affiche l'onglet Sources.



5. Sélectionnez la source de données pour laquelle vous souhaitez configurer des autorisations en cochant la case.
6. Cliquez sur .

   La boîte de dialogue Autorisations de source de données s'affiche.



7. Modifiez l'autorisation d'accès pour différents utilisateurs d'après le type de compte de service de la source de données. L'autorisation peut être **En lecture seule** ou **Aucun accès**.
8. Cliquez sur **Enregistrer**.

   Les autorisations requises sont configurées pour la source de données.

Pour plus d'informations, consultez le *Guide de Reporting*.

Configurer les paramètres du Reporting Engine

Après avoir configuré Reporting Engine et les sources de données requises en fonction de vos besoins, vous pouvez modifier certaines des configurations pour personnaliser vos graphiques, Rapports et Alertes.

Pour configurer les paramètres :

1. Accédez à **Administrateur** > **Services**.
2. Dans la liste **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Config**.

   La vue Configuration des services de Reporting Engine s'ouvre avec l'onglet Général mis en évidence. Pour plus d'informations sur l'onglet Général de Reporting Engine, consultez l'Onglet General.
4. Modifiez les paramètres de service Reporting Engine et cliquez sur **Appliquer**.

   Les paramètres de service sont configurés sur Reporting Engine.

Activer l'authentification LDAP

Pour activer le mode d'authentification LDAP à l'aide d'Active Directory pour HiveServer2 pour la source de données Warehouse, procédez comme suit.

1. Connectez-vous à l'appliance RSA Analytics Warehouse en tant qu'utilisateur root.
2. Accédez au répertoire `/opt/mapr/hive/hive-0.11/conf.new/` . Saisissez la commande suivante et appuyez sur ENTRÉE :

   ```
   cd /opt/mapr/hive/hive-0.11/conf.new/
   ```
3. Modifiez le fichier `hive-site.xml`. Saisissez la commande suivante et appuyez sur ENTRÉE :

   ```
   vi hive-site.xml
   ```
4. Ajoutez les propriétés suivantes sous la balise `<Configuration>` :

   ```
   <property>
       <name>hive.server2.authentication</name>
       <value>LDAP</value>
   </property>
   <property>
       <name>hive.server2.authentication.ldap.url</name>
   ```

```
    <value>LDAP_URL</value>
</property>
```

Où `LDAP_URL` est l'URL du serveur LDAP.

5. Redémarrez HiveServer2.

Ajouter de l'espace supplémentaire pour les rapports volumineux

Pour ajouter de l'espace disque supplémentaire à Reporting Engine pour les rapports volumineux, suivez les étapes ci-dessous. Si vous devez générer des rapports de conformité volumineux pour ou Warehouse, l'espace disque de Reporting Engine risque d'être utilisé plus rapidement que prévu. Dans ce cas, vous pouvez monter un stockage externe comme un système SAN ou NAS pour stocker les rapports.

Les répertoires qui ont tendance à occuper l'espace disque sont `resultstore` et `formattedReports`. Ils se trouvent dans le répertoire de base de Reporting Engine. Il est recommandé de déplacer uniquement ces deux répertoires sur des systèmes SAN ou NAS et de remplacer les emplacements initiaux par des liens symboliques pointant vers les nouveaux emplacements. Il est également recommandé de laisser les autres répertoires sur le disque local pour maintenir des performances d'E/S fiables et élevées.

Remarque : Les étapes suivantes partent du principe que le répertoire de base du Reporting Engine se trouve dans le répertoire `/var/netwitness/re-server/rsa/soc/reporting-engine/` et que le stockage externe est monté dans `/externalStorage/`. En outre, l'utilisateur 'rsasoc' doit accéder en lecture/écriture au chemin spécifié de stockage externe.

Pour déplacer l'espace disque pour le Reporting Engine vers le stockage externe :

1. Arrêtez le service Reporting Engine en tant qu'utilisateur root.

   ```
   service rsasoc_re stop
   ```

2. Passez à l'utilisateur `rsasoc`.

   ```
   su rsasoc
   ```

3. Basculez dans le répertoire personnel RE.

   ```
   cd /var/netwitness/re-server/rsa/soc/reporting-engine/
   ```

4. Déplacez le répertoire resultstore sur un stockage externe monté. Saisissez la commande suivante et appuyez sur ENTRÉE :

   ```
   mv resultstore /externalStorage
   ```

5. Déplacez le répertoire formattedReports sur un stockage externe monté. Saisissez la commande suivante et appuyez sur ENTRÉE :

   ```
   mv formattedReports /externalStorage
   ```

6. Créez un lien symbolique pour resultstore. Saisissez la commande suivante et appuyez sur

ENTRÉE :

```
ln -s /externalStorage/resultstore /var/netwitness/re-server/rsa/soc/reporting-engine/resultstore
```

7. Créez un lien symbolique pour formattedReports. Saisissez la commande suivante et appuyez sur ENTRÉE :

   ```
   ln -s /externalStorage/formattedReports /var/netwitness/re-server/rsa/soc/reporting-engine/formattedReports
   ```

8. Quittez l'utilisateur `rsasoc`.

   ```
   exit
   ```

9. Démarrez le service Reporting Engine en tant qu'utilisateur root.

   ```
   service rsasoc_re start
   ```

   Remarque : Si le stockage externe est hors ligne, vous ne pouvez pas effectuer les tâches suivantes :
   1) Exécuter des rapports ou des alertes Reporting
   2) Consulter les rapports ou les alertes Reporting existants
   Cependant, vous pouvez créer de nouveaux objets Reporting comme des rapports et des graphiques, et accéder à ces graphiques et au tableau de bord Live créés pour ces derniers. Vous devez donc vous assurer que le stockage externe est fiable et dispose de l'espace requis.

   Par ailleurs, pour pouvoir stocker des rapports pendant plus de 100 jours, modifiez en conséquence la configuration de rétention dans Configurer les paramètres du Reporting Engine.

Accès aux fichiers log de Reporting Engine

Vous pouvez accéder aux fichiers log de Reporting Engine qui sont stockés dans le répertoire de logs suivant `/var/netwitness/re-server/rsa/soc/reporting-engine/logs/`

- Log actuels du fichier `reporting-engine.log`.
- Sauvegardez des copies des logs précédents dans le fichier `reporting-engine.log.*`.
- Tous les logs de script UNIX dans les fichiers ayant la syntaxe suivante : `reporting-engine.sh_timestamp.log` (par exemple, `reporting-engine.sh_20120921.log`)

Reporting Engine écrit rarement des messages d'erreur de ligne de commande dans le fichier **rsasoc/nohup.out**.

Reporting Engine ajoute les messages et la sortie de log écrits par le système systemd et les commandes utilisées pour démarrer Reporting Engine dans le répertoire `/var/log/messages`. Un fichier log `/var/log/messages` est un fichier log système. Seul l'utilisateur root peut donc le lire.

Configurer le Planificateur de tâches pour un Reporting Engine

Vous pouvez configurer des files d'attente et des pools dans Reporting Engine afin de planifier des rapports NWDB ou Warehouse. Pour plus d'informations sur les planificateurs de tâches, reportez-vous à la rubrique Planificateur de tâches pour Warehouse Reporting dans le *Guide de reporting de RSA NetWitness Suite*.

Conditions préalables

Veillez à bien identifier les éléments suivants :

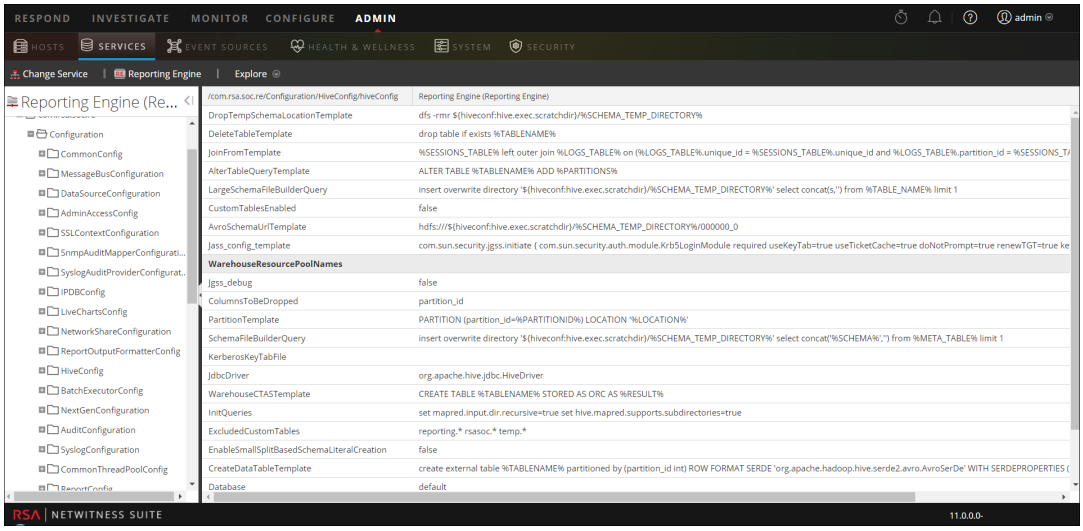
- Type de planificateur et pools ou files d'attente à utiliser. Vous ne pouvez configurer qu'un seul planificateur pour Reporting Engine. Le planificateur Fair est configuré par défaut.
- Noms des pools ou files d'attente, et ressources attribuées à chacune et chacun d'entre eux.
- NetWitness Suite n'accepte qu'une file d'attente ou pool par cluster. RSA recommande d'utiliser des noms de file d'attente ou de pool uniques dans tous les clusters ou le même nom de file d'attente ou de pool dans les deux clusters. Si le cluster est très volumineux, vous pouvez utiliser plus de trois files d'attente ou pools.
- Si vous utilisez un planificateur non pris en charge, Reporting Engine ne définit aucune propriété pour les tâches qu'il lance.
- Si le nom de la file d'attente ou du pool n'existe pas dans le cluster, le Planificateur de capacité utilise la file d'attente par défaut pour le rapport. Il se peut que le Planificateur de capacité n'exécute pas les règles ou crée un pool avec le partage le plus réduit. Cela dépend de la valeur spécifiée pour la propriété du Planificateur Fair `mapred.fairscheduler.allow.undeclared.pools`.
- Si vous ne spécifiez aucune file d'attente ou aucun pool, la tâche lancée par la règle de test se trouve dans le pool `mapr` ou dans la file d'attente par défaut. RSA vous recommande de configurer un pool mapr avec un partage réduit (environ 1/10 de la capacité totale) avec `maxRunningJobs = 2` pour que ces règles n'interrompent pas la génération des rapports. Veillez à ne spécifier ce nom de pool pour aucun rapport.

Spécifier les pools et les files d’attente

Pour spécifier les pools et les files d’attente :

1. Accédez à **ADMIN** > **Services**.
2. Sélectionnez **Reporting Engine** et cliquez sur  > **Vue** > **Explorer**.

3. Sélectionnez **com.rsa.soc.re** > **Configuration** > **HiveConfig** > **hiveconfig** > **WarehouseResourcePoolNames**.
4. Dans le champ **NomsPoolsRessourcesWarehouse**, saisissez les noms des files d'attente et des pools en les séparant par un espace. Par exemple, pour configurer quatre files d'attente ou pools avec les noms pool1, pool2, erreur et par défaut, saisissez ces noms en les séparant par un espace.



Définir les rapports, graphiques et alertes

Une fois le Reporting Engine et les sources de données requises configurés selon vos besoins, vous pouvez générer des rapports, des graphiques et des alertes.

Définir les rapports, graphiques et alertes

Comment définir Rapports

Après avoir créé les sources de données et configuré les autorisations utilisateur à partir de ces sources de données, vous pouvez désormais utiliser ces sources de données pour effectuer les tâches suivantes pour le module Reporting :

- **Définir une règle**
- **Tester une règle**
- **Planifier des rapports**
- **Ajouter une alerte**
- **Ajouter un graphique**
- **Tester un graphique**

Pour plus d'informations, reportez-vous aux sections ci-dessus dans le *RSA Netwitness Reporting Reports Guide*.

Comment définir des graphiques

Après avoir créé les sources de données et configuré les autorisations utilisateur à partir de ces sources de données, vous pouvez désormais utiliser ces sources de données pour effectuer les tâches suivantes pour le module Reporting :

- **Définir les graphiques et les groupes de graphiques**
- **Tester un graphique**
- **Rechercher des graphiques**
- **Gestions des graphiques**

Pour plus d'informations, reportez-vous aux sections ci-dessus dans le *RSA Netwitness Reporting Reports Guide*.

Comment définir des alertes

Après avoir créé les sources de données et configuré les autorisations utilisateur à partir de ces sources de données, vous pouvez désormais utiliser ces sources de données pour effectuer les tâches suivantes pour le module Alerting :

- **Configurer Alertes**
- **Générer Alertes**
- **Ajouter une alerte**
- **Afficher une alerte**
- **Afficher la planification des alertes**
- **Analyser une alerte**

Pour plus d'informations, reportez-vous aux sections ci-dessus dans le *RSA Netwitness Reporting Alerting Guide*.

Configurer les paramètres généraux du Reporting Engine

En ajoutant et en configurant le service Reporting Engine, les paramètres du système sont pré-remplis avec des valeurs par défaut pour atteindre des résultats optimaux. Toutefois, vous pouvez modifier et personnaliser les notifications du Reporting Engine en fonction de vos besoins en accédant à l'onglet Général dans la vue Configuration des Services pour un Reporting Engine.

Pour accéder à l'onglet Général :

Vous devez ouvrir l'onglet Général pour configurer les paramètres généraux du Reporting Engine.

Pour accéder à cette vue :

1. Accédez à **Administrateur** > **Services**.
2. Dans la liste Services disponibles, sélectionnez un service **Reporting Engine**.
3. Cliquez sur**Vue** > **Config**.
4. Cliquez sur l'onglet **Général**.
5. Cliquez sur **Appliquer** après avoir modifié les paramètres.

Une fois que vous accédez à l'onglet Général, vous pouvez modifier les paramètres suivants.

- Configuration système
- Configuration de la consignation
- Configuration de sortie Warehouse Analytics
- Configuration de modèle Warehouse Analytics
- Configuration Warehouse Kerberos

Pour plus d'informations sur les paramètres de configuration, consultez l'onglet Général.

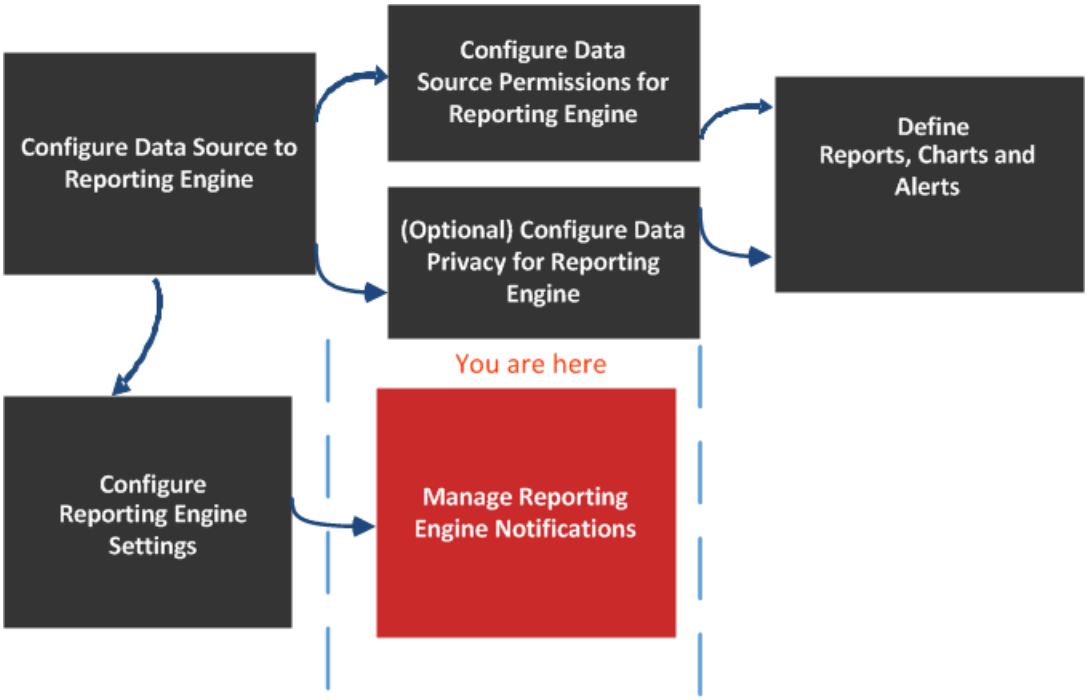
Références

Pour pouvoir personnaliser et optimiser l'utilisation du service, vous pouvez modifier les paramètres Reporting Engine dans la vue Configuration des services, qui contient des paramètres spécifiques au Reporting Engine.

Onglet General

L'onglet Général du service Reporting Engine permet de contrôler plusieurs paramètres en vue d'optimiser les performances d'un service et de spécifier les informations d'identification. Accédez à Services > Vue > Config > Reporting Engine > Général. Ces paramètres sont utilisés exclusivement pour le service Reporting Engine.

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



Que voulez-vous faire ?

Rôle	Je souhaite...	Consultez...
Administrateur	Configurer la source de données du Reporting Engine	Configurer les sources de données

Rôle	Je souhaite...	Consultez...
Administrateur	Configurer les autorisations d'accès aux sources de données pour le Reporting Engine	Configurer les autorisations d'accès aux sources de données
Administrateur	Configurer la confidentialité des données pour le Reporting Engine	Configurer la confidentialité des données pour le Reporting Engine
Administrateur	Définir les rapports, graphiques et alertes	Définir les rapports, graphiques et alertes
Administrateur	Configurer les paramètres du Reporting Engine	Configurer les paramètres du Reporting Engine
Administrateur/responsable du SOC	Configurer les paramètres du système*	Configurer les paramètres généraux du Reporting Engine
Administrateur/responsable du SOC	Configurer la consignation *	Configurer les paramètres généraux du Reporting Engine
Administrateur/responsable du SOC	Configurer la sortie de Warehouse Analytics *	Configurer les paramètres généraux du Reporting Engine
Administrateur/responsable du SOC	Configurer le modèle Warehouse Analytics *	Configurer les paramètres généraux du Reporting Engine
Administrateur/responsable du SOC	Configurer Warehouse Kerberos *	Configurer les paramètres généraux du Reporting Engine

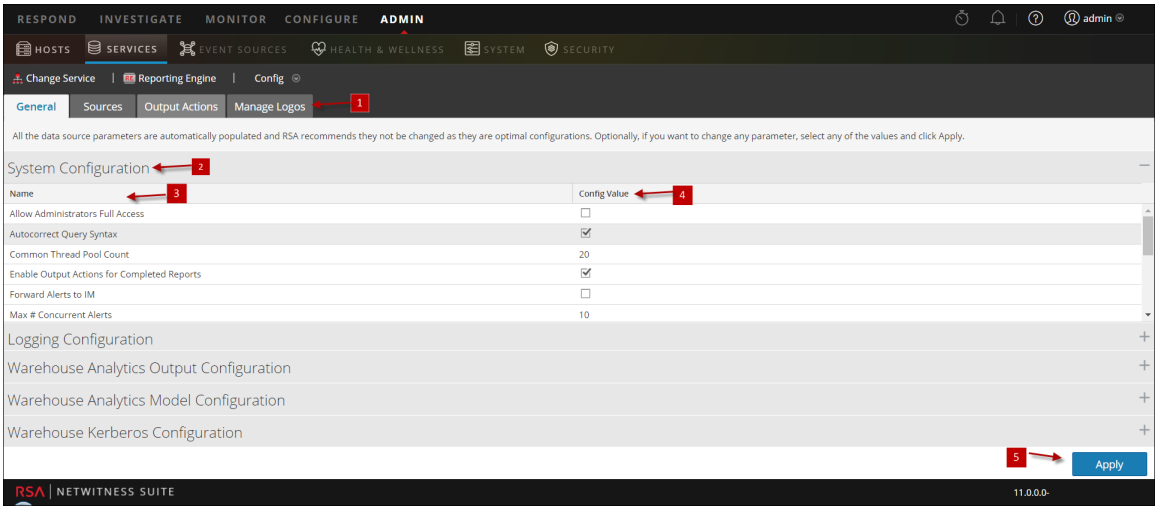
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Mode de fonctionnement du Reporting Engine

Aperçu rapide

Voici un exemple de l'onglet Général dans lequel les configurations de service sont affichées.



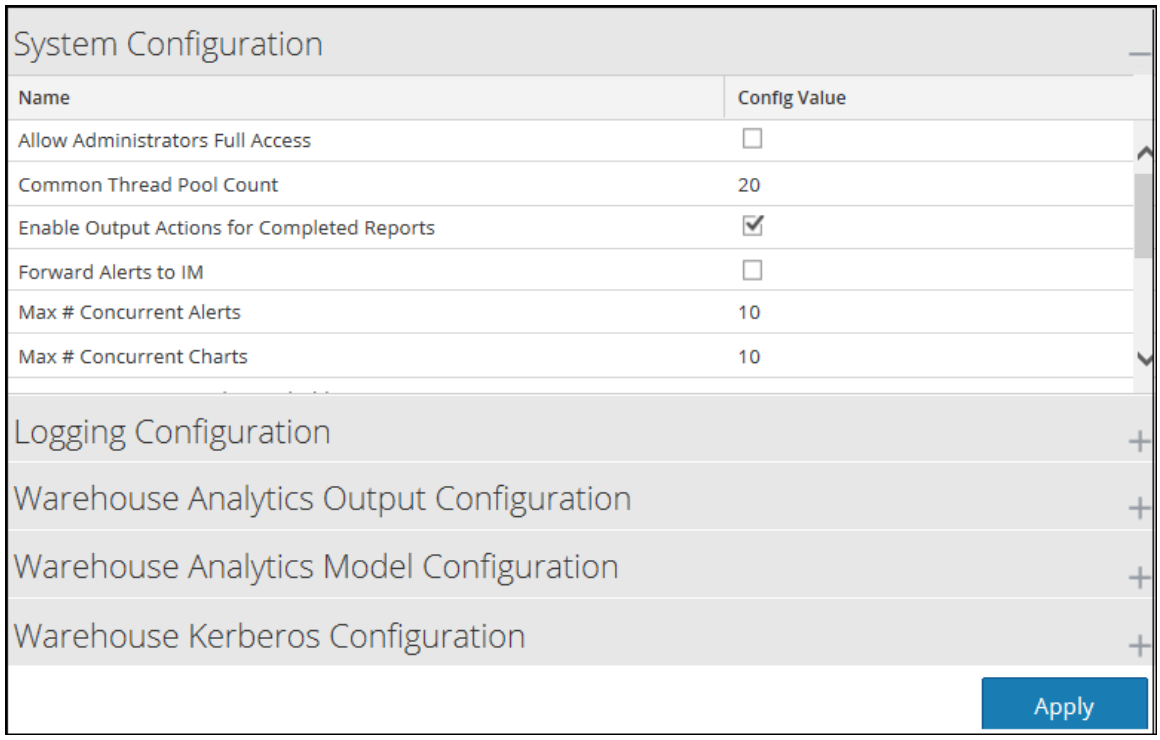
1	Affiche tous les onglets configurables disponibles.
2	Affiche les paramètres de configuration disponibles pour le système.
3	Affiche le nom du paramètre.
4	Affiche les valeurs définies pour chaque paramètre.
5	Applique les modifications.

Remarque : Warehouse Analytics n'est pas pris en charge dans NetWitness Suite 11.0.

Configuration système

Les paramètres du panneau Configuration de la consignation du Reporting Engine définissent la configuration d'un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, les valeurs par défaut s'appliquent. Les valeurs par défaut sont conçues pour s'adapter à la plupart des environnements et il est recommandé de ne pas modifier ces valeurs car cela pourrait avoir un impact négatif sur les performances.

La figure suivante présente les champs qu'il est possible de renseigner dans le panneau Configuration système :



Le tableau suivant décrit les fonctions du panneau Configuration système.

Nom	Valeur de configuration
Autoriser un accès complet aux administrateurs	Activez cette case à cocher si vous souhaitez accéder à tous les objets Reporting Engine (rapports, règles, graphiques, plannings et listes) créés par d'autres utilisateurs (non administrateurs). Par défaut, cette case n'est pas cochée. **Remarque :** si vous désactivez cette case à cocher après l'avoir activée, tous les objets Reporting Engine concernés ne sont plus accessibles. En revanche, si vous avez défini l'accès à des objets spécifiques dans la fenêtre Autorisations (**Rapports > Gérer > Objet RE >** > **Autorisations**), le fait d'activer ou de désactiver cette case à cocher n'a aucun impact sur ces objets.
Nombre de pools de threads communs	Nombre de pools de threads alloués pour exécuter des tâches courantes dans le Reporting Engine. Pour être valide, la valeur doit être un nombre entier (**20** par défaut).

Nom	Valeur de configuration
Activer les opérations de sortie pour les rapports exécutés	Activez la case à cocher pour traiter les opérations de sortie uniquement pour les rapports dont toutes les exécutions de règle ont abouti. Cette option est activée par défaut. Si elle est désactivée, les opérations de sortie sont traitées pour tous les scénarios (complet, partiel ou échec).
Transférer les alertes au service Respond	Activez la case à cocher pour transférer toutes les alertes à Respond. Par défaut, cette case n'est pas cochée.
Nbre max. d'alertes simultanées	Nombre maximal d'alertes pouvant s'exécuter simultanément. Cela a un impact direct sur le service RSA sur lequel les alertes sont exécutés, étant donné que chaque alerte utilise un thread de requête sur le service RSA. Pour être valide, la valeur doit être un nombre entier (**10** par défaut).
Nbre max. de graphiques simultanés	Nombre maximal de graphiques pouvant s'exécuter simultanément. Pour être valide, la valeur doit être un nombre entier (**10** par défaut).
Nbre max. de requêtes LookupAndAdd simultanées	Nombre maximal de requêtes LookupAndAdd parallèles pouvant s'exécuter par règle NWDB Pour être valide, la valeur doit être un nombre entier (**2** par défaut). Si vous augmentez cette valeur, il faut vérifier que la source de données NWDB est configurée pour gérer les requêtes parallèles en vue d'optimiser les performances.
Nbre max. de rapports de listes de valeurs simultanés	Nombre maximal de rapports de listes de valeurs par planning pouvant être générés en parallèle. Pour être valide, la valeur doit être un nombre entier (**1** par défaut).

Nom	Valeur de configuration
Nbre max. de rapports de listes de valeurs	Nombre maximal de rapports de listes de valeurs générés indépendamment du nombre de valeurs dans la liste. Pour être valide, la valeur doit être un nombre entier (**10 000** par défaut).
Max. lignes stockées par règle (Milliards)	Nombre maximal de lignes qu'une règle peut extraire lors d'une requête. Pour être valide, la valeur doit être un nombre entier (**100** par défaut).
Seuil maximal d'espace disque	Seuil d'espace disque maximal en gigaoctets alloué pour exécuter les rapports, les alertes et les graphiques. La valeur initiale est configurée en fonction de l'espace disponible du système.
Seuil minimal d'espace disque	Seuil d'espace disque minimal en pourcentage alloué pour exécuter les rapports, les graphiques et les alertes. Par défaut, la valeur est définie sur 5. **Remarque :** Remarque : si le seuil est atteint, l'exécution de rapports, graphiques et des alertes s'arrête même si le service est en cours d'exécution.
Délai d'expiration des requêtes d'information NWDB	Délai d'expiration des requêtes d'information en quelques secondes sur le serveur NWDB. Pour être valide, la valeur doit être un nombre entier (**0** par défaut).
Nbre maximal de lignes agrégées NWDB	Nombre maximal de lignes renvoyées lorsque l'agrégation est utilisée dans la règle NWDB. Pour être valide, la valeur doit être un nombre entier (**1000** par défaut).

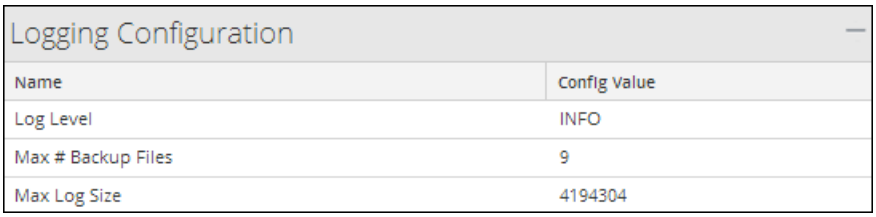
Nom	Valeur de configuration
Délai d'expiration des requêtes NWDB	Délai (exprimé en secondes) au terme duquel le serveur NWDB considère que l'exécution de la règle a expiré s'il ne parvient pas à traiter le résultat dans le délai configuré. La valeur par défaut est fixée à 0, ce qui signifie qu'il n'y a pas de délai d'expiration. Pour être valide, la valeur doit être un nombre entier.
Traiter les opérations de sortie uniquement pour les rapports réussis	Activez cette case à cocher pour traiter les opérations de sortie uniquement pour les rapports dont les exécutions de règle ont abouti. Si vous désactivez cette case à cocher, les opérations de sortie seront déclenchées pour les rapports partiels, terminés et en échec. **Remarque :** Cette option s'applique à toutes les opérations de sortie, à l'exception des listes dynamiques.
Conserver l'historique des alertes pendant (nombre) jours	Nombre maximal de jours durant lesquels conserver l'historique et l'état des alertes. Pour être valide, la valeur doit être un nombre entier (**100** par défaut).
Conserver l'historique des graphiques pendant (nombre) jours	Nombre maximal de jours durant lesquels conserver l'historique et l'état des graphiques. Pour être valide, la valeur doit être un nombre entier (**30** par défaut).
Conserver l'historique des rapports pendant (nombre) jours	Nombre maximal de jours durant lesquels le système conserve l'historique et l'état des rapports. Pour être valide, la valeur doit être un nombre entier (**100** par défaut).

Nom	Valeur de configuration
Nombre de pools de threads planifiés	Nombre de pools de threads alloués aux tâches planifiées (suppression de l'historique, par exemple) sur le Reporting Engine. Pour être valide, la valeur doit être un nombre entier (**5** par défaut).

Configuration de la consignation

Les paramètres du panneau Configuration de la consignation du Reporting Engine gèrent la configuration de consignation d'un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, les valeurs par défaut s'appliquent. Les valeurs par défaut proposées par RSA s'adaptent à la plupart des environnements et il est recommandé de ne pas modifier ces valeurs car cela pourrait avoir un impact négatif sur les performances du Reporting Engine.

La figure suivante présente les champs qu'il est possible de renseigner dans le panneau Configuration de la consignation.



Le tableau suivant décrit les fonctions du panneau Configuration de la consignation.

Nom	Valeur de configuration
Log Level	Le niveau de consignation détermine l'étendue des informations incluses dans les fichiers log. Les valeurs possibles sont les suivantes : • `ERROR` • `WARN` • `INFO (par défaut)` • `DEBUG` • `ALL`
Nbre max. de fichiers de sauvegarde	Nombre maximal de fichiers log de sauvegarde que le système conserve. Pour être valide, la valeur doit être un nombre entier (**9** par défaut).

Nom	Valeur de configuration
Taille de log max.	Taille maximale (en octets) du fichier log principal. Pour être valide, la valeur doit être un nombre entier (**4194304** par défaut).

Pour plus d'informations sur la consignation du Reporting Engine, consultez la rubrique Accès aux fichiers log de Reporting Engine.

Configuration de sortie Warehouse Analytics

Remarque : Warehouse Analytics n'est pas pris en charge dans NetWitness Suite 11.0.

Le panneau Configuration de sortie Warehouse Analytics permet de configurer la sortie Warehouse Analytics sur ce Reporting Engine.

La figure suivante présente les champs qu'il est possible de renseigner dans le panneau Configuration de sortie Warehouse Analytics :

Après une mise à niveau, veillez à mettre à jour les détails de **Mongodb** centralisés afin d'être en mesure d'utiliser Warehouse Analytics.

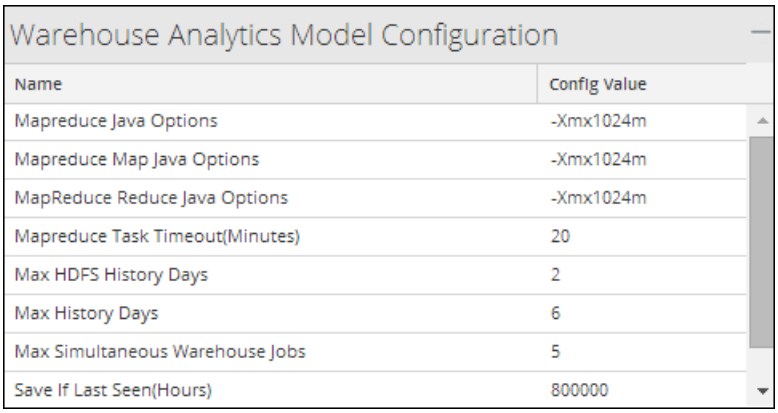
Le tableau suivant décrit les fonctions du panneau Configuration de sortie Warehouse Analytics.

Nom	Valeur de configuration
Nom	**Valeur de configuration**
Nom d'utilisateur	Nom de l'utilisateur de Warehouse Analytics.
Port	Port de la base de données Mongo utilisée par Warehouse Analytics.
Hôte	Hôte de la base de données Mongo utilisée par Warehouse Analytics.
Mot de passe	Mot de passe de l'utilisateur de Warehouse Analytics.

Configuration de modèle Warehouse Analytics

Le panneau Configuration de modèle Warehouse Analytics permet de configurer le modèle Warehouse Analytics sur ce Reporting Engine.

La figure suivante présente les champs qu'il est possible de renseigner dans le panneau Configuration de modèle Warehouse Analytics :



Le tableau suivant décrit les fonctions du panneau Configuration de modèle Warehouse Analytics.

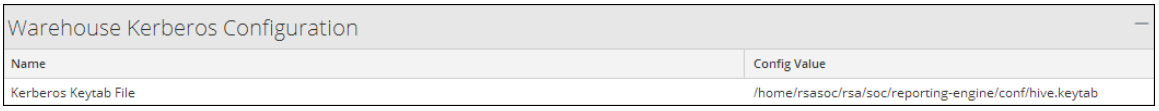
Nom	Valeur de configuration
Options Java MapReduce	Paramètres JVM définissant la machine virtuelle Java enfant de suivi de tâches Hadoop MapReduce. Par défaut, la valeur est **-Xmx1024m**.
Options Java de mappage MapReduce	Contrôle les paramètres JVM pour mapper les tâches dans le cluster Hadoop. Par défaut, la valeur est **-Xmx1024m**.
Options Java de réduction MapReduce	Contrôle les paramètres JVM pour réduire les tâches dans le cluster Hadoop. Par défaut, la valeur est **-Xmx1024m**.
Expiration du délai de la tâche MapReduce (minutes)	Délai (en minutes) avant qu'une tâche ne soit terminée si le framework MapReduce estime qu'elle ne répond pas ou est inactive. Pour être valide, la valeur doit être un nombre entier (**20** par défaut).
Jours d'historique HDFS max.	Durée maximale (en jours) de conservation des fichiers temporaires et de sortie de tâche dans HDFS. Une valeur valide doit être un nombre entier (**2** par défaut).
Jours max. historique	Durée maximale (en jours) de conservation de la sortie de tâche dans MongoDB. Une valeur valide doit être un nombre entier (**6** par défaut).

Nom	Valeur de configuration
Tâches Warehouse simultanées max.	Contrôle le nombre maximal de tâches exécutées en parallèle dans le framework Warehouse Analytics. Une valeur valide doit être un nombre entier (**1** par défaut).
Enregistrer si vu pour la dernière fois (heures)	Permet d'enregistrer les clés de la sortie de tâche si elles n'ont pas été vues au cours des N dernières heures. Une valeur valide doit être un nombre entier (**800 000** par défaut).
Score de seuil	Permet d'enregistrer les clés de la sortie de tâche dans les listes de surveillance en vue de leur utilisation par ESA uniquement si le score est supérieur à N. Une valeur valide doit être un nombre entier (**55** par défaut).

Configuration Warehouse Kerberos

Le panneau Configuration Warehouse Kerberos permet de spécifier le fichier de table de clés Kerberos sur ce Reporting Engine.

La figure suivante présente les champs qu'il est possible de renseigner dans le panneau Configuration Warehouse Kerberos :



Le tableau suivant décrit les fonctions du panneau Configuration Warehouse Kerberos.

Nom	Valeur de configuration
Fichier de table de clés Kerberos	Chemin d'accès au fichier de table de clés Kerberos. Par exemple, `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/hive.keytab`.

Le fichier de configuration par défaut de Kerberos est stocké sous `/etc/kbr5.conf` dans le Reporting Engine. Vous pouvez modifier le fichier de configuration afin de fournir des détails sur les realms Kerberos et d'autres paramètres associés.

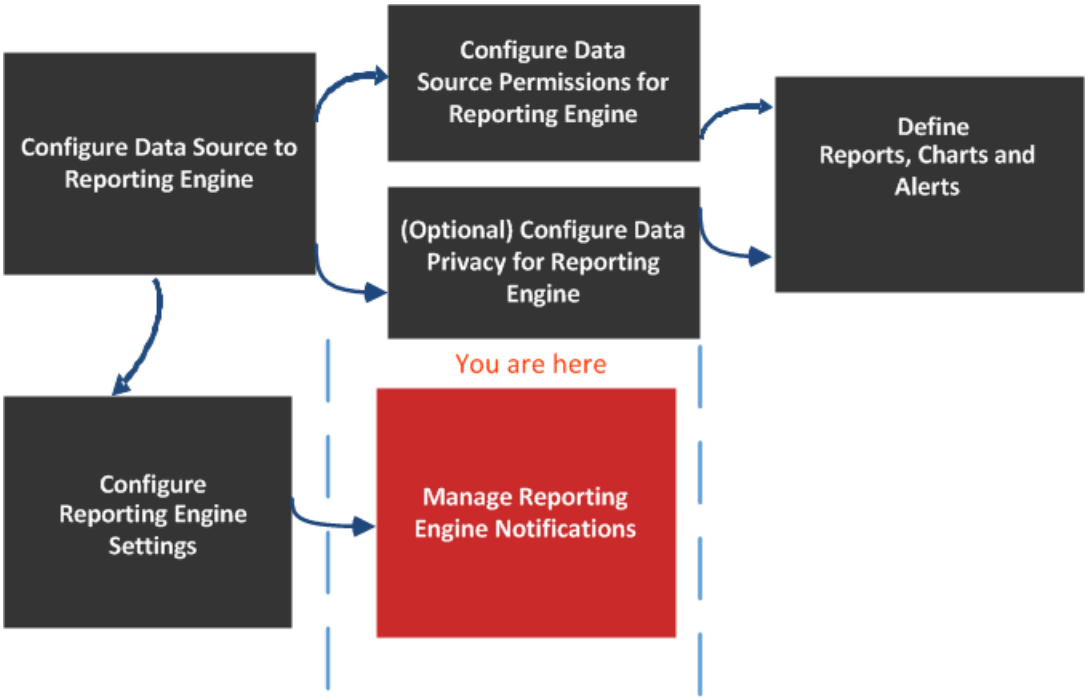
Vous avez ajouté le nom d'hôte (ou nom de domaine complet, FQDN) ainsi que l'adresse IP des nœuds Horton Works et du Warehouse Connector sur le serveur DNS. Si le serveur DNS n'est pas configuré, ajoutez le nom d'hôte (ou le nom de domaine complet), ainsi que l'adresse IP des

nœuds Horton Works et du service Warehouse Connector dans le fichier `/etc/hosts` sur l'hôte sur lequel le service Warehouse Connector est installé.

Onglet Sources

Les paramètres de configuration des services sont disponibles sous l'onglet Sources de la vue Configuration des services pour le Reporting Engine. L'onglet Sources du service Reporting Engine dans la vue Configuration des services contrôle les sources de données associées à un Reporting Engine. L'onglet Source se compose d'un panneau unique avec une barre d'outils et une grille qui répertorie les sources de données associées au Reporting Engine.

Workflow



Rôle	Je souhaite...	Consultez...
Administrateur	Configurer la source de données dans le Reporting Engine	Configurer les sources de données
Administrateur	Configurer les autorisations d'accès aux sources de données pour le Reporting Engine	Configurer les autorisations d'accès aux sources de données

Rôle	Je souhaite...	Consultez...
Administrateur	Configurer la confidentialité des données pour le Reporting Engine	Configurer la confidentialité des données pour le Reporting Engine
Administrateur	Définir les rapports, graphiques et alertes	Définir les rapports, graphiques et alertes
Administrateur	Configurer les paramètres du Reporting Engine	Configurer les paramètres du Reporting Engine
Administrateur	Ajouter, supprimer ou modifier un service nouvelle ou disponibles*	Configurer les sources de données
Administrateur	Définir une source de données comme source par défaut*	Configurer les sources de données
Administrateur	Configurer les autorisations d'accès aux sources de données*	Configurer les autorisations d'accès aux sources de données

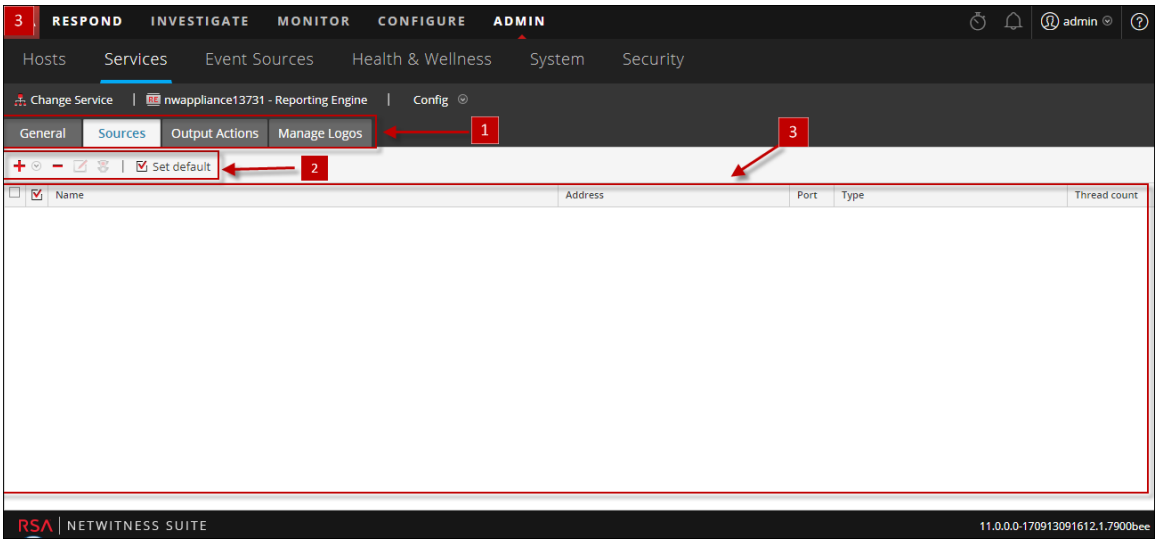
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Mode de fonctionnement du Reporting Engine

Aperçu rapide

Voici un exemple de l'onglet Sources dans lequel les services disponibles sont affichés.



1 Affiche tous les onglets configurables disponibles.

2 Affiche les paramètres de configuration disponibles pour le service sélectionné.

3 Affiche les paramètres du champ disponibles pour le service sélectionné.

Les sources de données disponibles dans le Reporting Engine pour lequel vous définissez des rapports, des graphiques et des alertes sont les suivantes :

- **Sources de données NWDB** - Les sources de données NetWitness Database (NWDB) sont les composants Decoder, Log Decoder, Broker, Concentrator, Archiver et Collection.

  Remarque : lorsqu'un plan de protection des données a été mis en œuvre pour limiter l'accès aux données sensibles sur une source de données, vous devez configurer différents comptes de service dans Reporting Engine pour les utilisateurs privilégiés et non privilégiés. Pour configurer différents comptes de service pour la confidentialité des données, vous pouvez ajouter plusieurs sources de données NWDB. Cette procédure est disponible sous Configurer les paramètres du Reporting Engine.

- **Sources de données Warehouse** - Les sources de données Warehouse sont Horton Works et MapR.

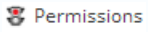
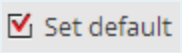
- **Sources de données Respond** - Respond est utilisé pour générer des rapports sur les alertes et les incidents. Les sources de données Respond sont Reporting Engine, ESA, Malware, EndPoint et Web Threat Detection. Respond est utilisé pour stocker les rapports d'alertes et d'incidents.

Si vous définissez une source comme source de données par défaut, NetWitness Suite utilise cette source lorsque vous créez des rapports et des alertes, sauf si vous choisissez de la remplacer par une autre des sources contenues dans cet onglet.

Remarque : vous pouvez gérer le contrôle d'accès aux sources de données NWDB et Warehouse. Pour plus d'informations, consultez la rubrique Configurer les paramètres du Reporting Engine.

Fonctions

Vous pouvez effectuer les actions suivantes sous l'onglet Sources :

Icône	Actions
	Cette option permet d'ajouter de nouveaux services en tant que sources de données pour Reporting Engine. Ajouter des services existants (Archiver, Workbench et Collecte) en tant que sources de données pour Reporting Engine.
	Cette option permet de supprimer des sources de données à partir d'un Reporting Engine.
	Cette option configure les autorisations de sources de données. Ce paramètre n'est activé que pour les sources de données NWDB et Warehouse. Pour plus d'informations, consultez la rubrique Configurer les autorisations d'accès aux sources de données.
	Cette option permet de définir les sources de données par défaut pour un Reporting Engine. Il s'agit de la source à laquelle NetWitness Suite applique les paramètres par défaut dans le champ **Source de données** des vues suivantes : • Vue Définition de règle. • Vue Créer ou modifier une alerte

Les sources de données NetWitness Suite s'affichent sous les différentes catégories suivantes :

- Catégorie Sources de données NWDB affiche les sources de données NetWitness.
- Catégorie Sources de données Warehouse affiche les sources de données Warehouse.

Colonne	Description
	Activer la case à cocher permet de sélectionner la source de données. Après l'avoir sélectionnée, vous pouvez utiliser la barre d'outils pour supprimer la source ou la définir comme source par défaut.
Nom	Affiche le nom de la source de données.
Adresse	Affiche l'adresse IP de la source de données.
Port	Affiche le port de la source de données.
Type	Affiche le type de service de la source de données.
Nombre de threads	Affiche la taille du pool de threads utilisé pour exécuter les règles sur la source de données.

Onglet Actions de sortie

Vous pouvez configurer les actions de sortie pour un Reporting Engine afin de déterminer le format dans lequel vous souhaitez recevoir les données en fonction de vos besoins. Les paramètres de configuration du service sont disponibles dans l'onglet Actions de sortie de la vue Configuration des services configurée pour un rapport ou une exécution d'alerte. Cet onglet comprend les panneaux suivants :

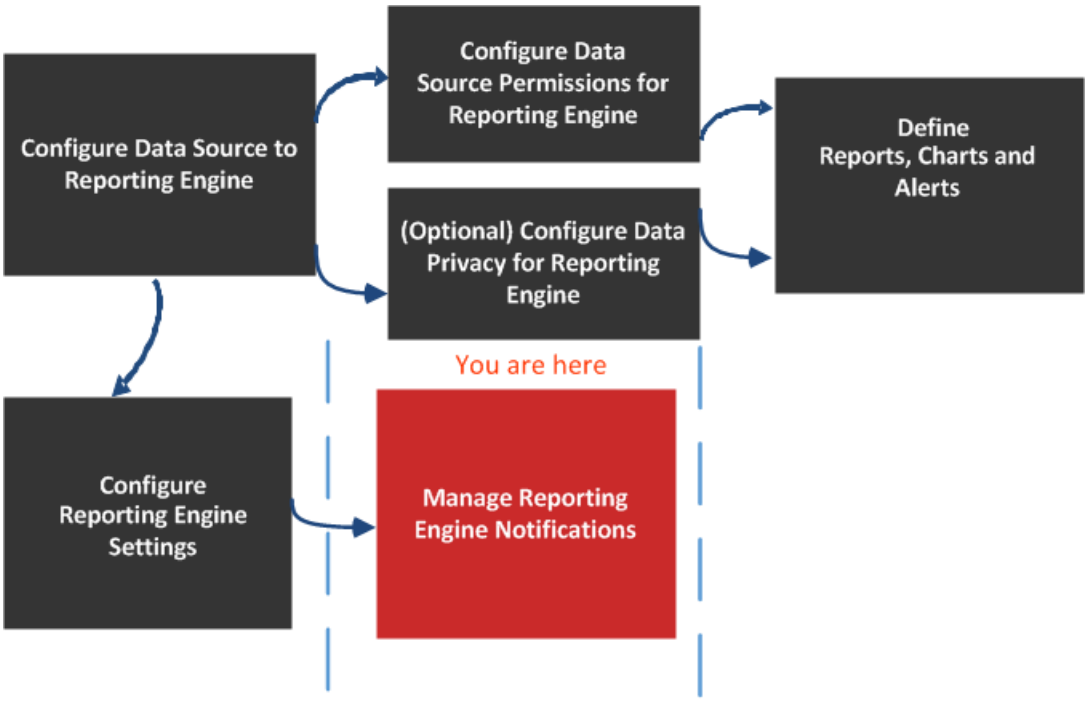
- NetWitness Suite Configuration
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- Syslog
- SFTP (Simple Mail Transfer Protocol)
- URL (Uniform Resource Locator)
- Partage réseau

Par exemple, l'action de sortie Syslog est utilisée spécifiquement pour les alertes Reporting Engine, alors que les actions de sortie SFTP, URL et Partage réseau sont utilisées spécifiquement pour les rapports Reporting Engine.

Vous pouvez configurer l'autorisation requise pour accéder à cette vue dans Gérer les services.

Vous devez vous assurer que le Reporting Engine est en cours d'exécution et que la source de données à partir de laquelle vous souhaitez générer un rapport est configurée dans NetWitness Suite.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Consultez...
Administrateur	Configurer la source de données vers le Reporting Engine	Configurer les sources de données
Administrateur	Configurer les autorisations d'accès aux sources de données pour le Reporting Engine	Configurer les autorisations d'accès aux sources de données
Administrateur	Configurer la confidentialité des données pour le Reporting Engine	Configurer la confidentialité des données pour le Reporting Engine

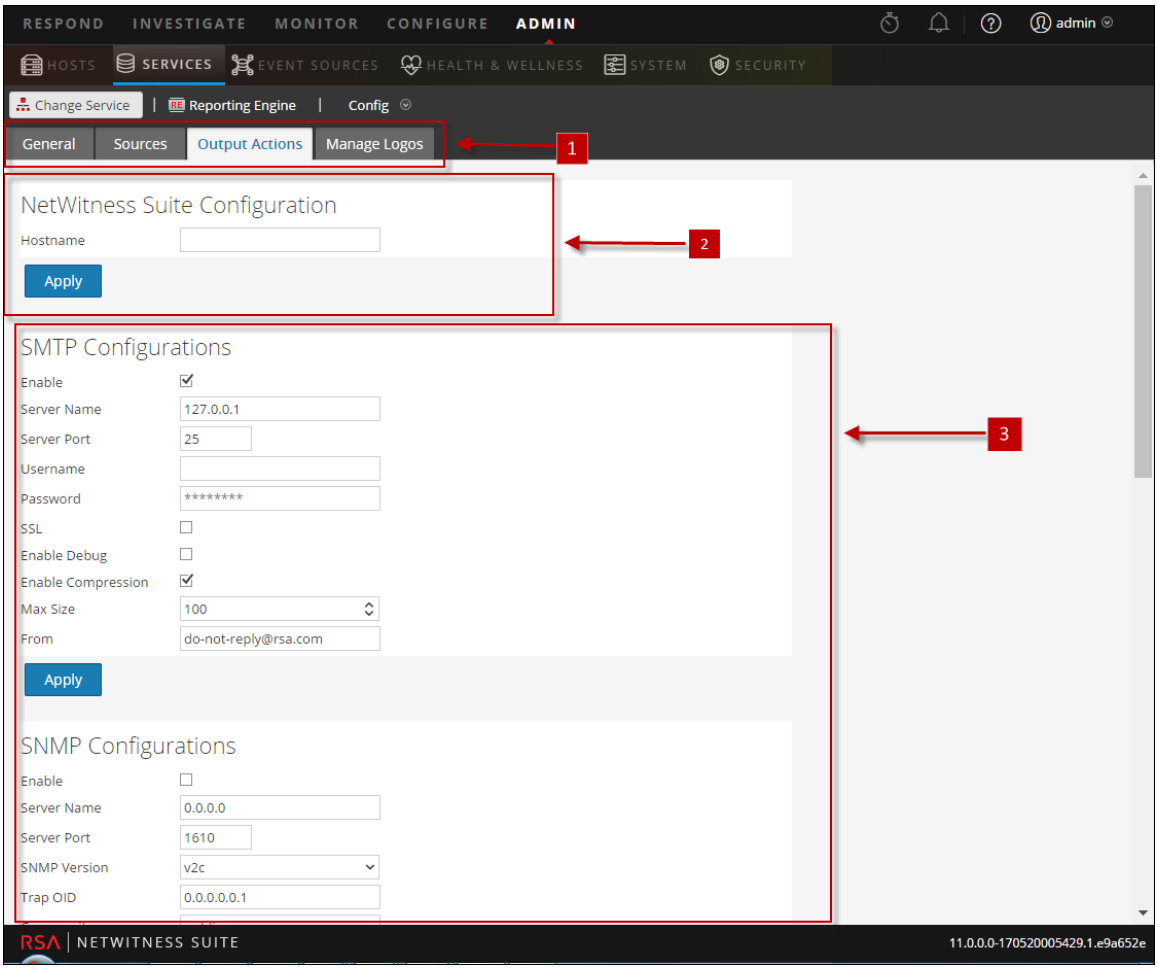
Rôle	Je souhaite...	Consultez...
Administrateur	Définir les rapports, graphiques et alertes	Définir les rapports, graphiques et alertes
Administrateur	Configurer les paramètres du Reporting Engine	Configurer les paramètres du Reporting Engine
Administrateur	Procéder à la configuration de NetWitness Suite*	Configurer les paramètres généraux du Reporting Engine
Administrateur	Procéder à la configuration SMTP*	Configurer les paramètres généraux du Reporting Engine
Administrateur	Procéder à la configuration SNMP*	Configurer les paramètres généraux du Reporting Engine
Administrateur	Procéder à la configuration Syslog*	Configurer les paramètres généraux du Reporting Engine
Administrateur	Procéder à la configuration SFTP*	Configurer les paramètres généraux du Reporting Engine
Administrateur	Procéder à la configuration URL*	Configurer les paramètres généraux du Reporting Engine
Administrateur	Procéder à la configuration du Partage réseau*	Configurer les paramètres généraux du Reporting Engine

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Mode de fonctionnement du Reporting Engine

Aperçu rapide



1	Affiche tous les onglets configurables disponibles.
2	Affiche l'hôte pour la configuration de NetWitness Suite.
3	Affiche tous les types d'action de sortie qui peuvent être configurés.

NetWitness Suite Configuration

La figure suivante montre la configuration NetWitness Suite sous l'onglet Actions de sortie.

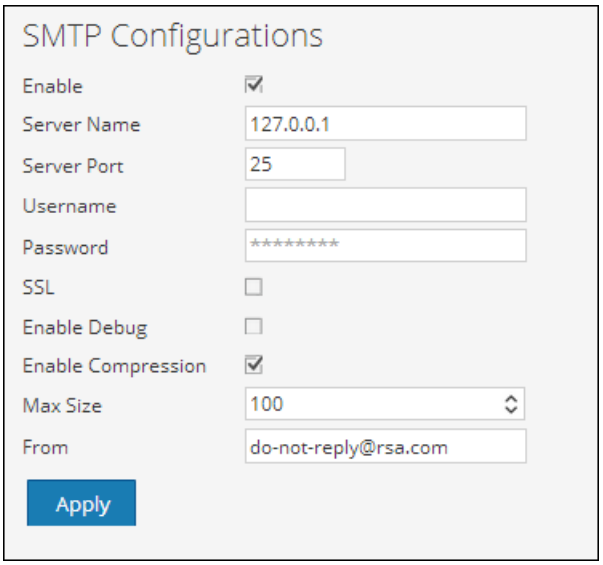
Les paramètres suivants identifient l'hôte NetWitness Suite associé au Reporting Engine.

Nom	Valeur de configuration
Nom d'hôte	Adresse IP ou nom d'hôte du serveur NetWitness Suite. Vous devez spécifier ce paramètre pour tous les types de déploiements. Ainsi, vous pouvez vous référer à cette adresse pour créer des liaisons de procédure d'enquête vers NetWitness Suite à partir des rapports, alertes, etc. NetWitness Suite utilise ce paramètre pour générer correctement les éléments suivants : • Action de sortie SMTP • Action de sortie SNMP • Action de sortie Syslog • Action de sortie SFTP • Action de sortie URL • Action de sortie de partage réseau • Liens hypertexte des métavaleurs dans les PDF de rapport
Appliquer	Mettez à jour la configuration.

SMTP

Une fois l'exécution terminée, une notification par e-mail est envoyée à l'utilisateur en fonction de la configuration SMTP.

La figure suivante montre la configuration SMTP sous l'onglet Actions de sortie.



Les paramètres suivants gèrent la configuration de l'action de sortie SMTP (e-mail) pour un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, les valeurs par défaut s'appliquent. Vous devez modifier les **Valeurs de configuration** de ces paramètres selon les exigences de votre entreprise.

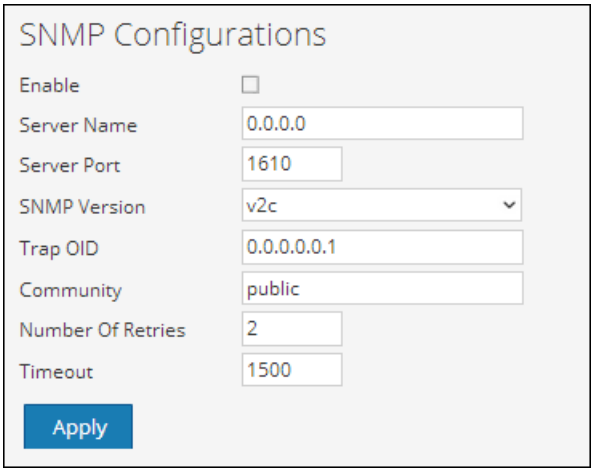
Nom	Valeur de configuration
Activer	Activez cette case à cocher pour activer l'action de sortie SMTP des alertes et des rapports à partir de ce Reporting Engine. Cette valeur est activée par défaut.
Nom du serveur	Spécifiez le nom d'hôte ou l'adresse IP du serveur sur lequel s'exécute le serveur SMTP cible. La valeur par défaut est 0.0.0.0.
Port de serveur	Spécifiez le numéro de port du serveur SMTP. La valeur par défaut est 25.
Nom d'utilisateur	Spécifiez le nom d'utilisateur de votre compte SMTP. La valeur par défaut est vide. Spécifier le mot de passe
Mot de passe	Spécifiez le mot de passe de votre compte SMTP.

Nom	Valeur de configuration
SSL	Activez cette case à cocher pour utiliser le protocole SSL (Secure Socket Layer) et communiquer avec le serveur SMTP. La valeur par défaut consiste à ne pas utiliser le protocole SSL.
Activer le débogage	Activez cette case à cocher pour activer le débogage. La valeur par défaut consiste à ne pas activer le débogage.
Activer la compression	Activez cette case à cocher pour activer la compression. La valeur par défaut est Activer la compression. Si cette valeur est activée, les fichiers de sortie présentent l'extension `.zip`.
Taille maximale	Spécifiez la taille maximale des pièces jointes pouvant être envoyées. La valeur par défaut est 100.
From	Spécifiez l'adresse email à partir de laquelle Security Analytics envoie tous les messages. La valeur par défaut est `do-not-reply@rsa.com`.
Appliquer	Mettez à jour la configuration.

SNMP

Une fois l'exécution terminée, une notification trap est envoyée à l'utilisateur en fonction de la configuration SNMP.

La figure suivante montre la configuration SNMP sous l'onglet Actions de sortie.



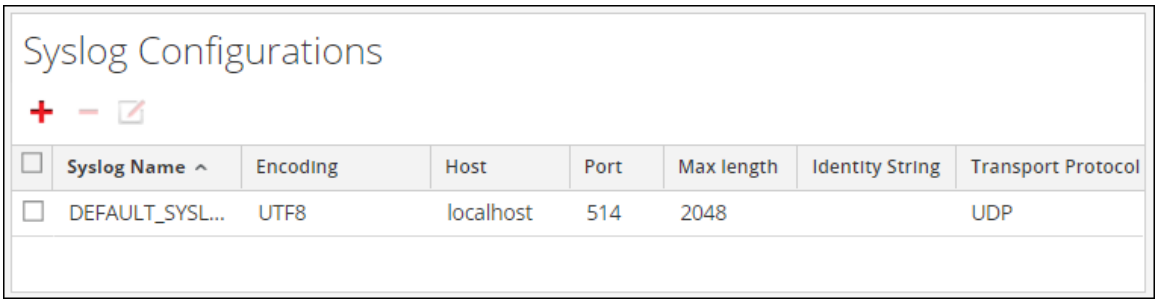
Les paramètres suivants gèrent la configuration de l'action de sortie SNMP (messages aux services rattachés au réseau) pour un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, les valeurs par défaut s'appliquent. Vous devez modifier les **Valeurs de configuration** de ces paramètres selon les exigences de votre entreprise.

Nom	Valeur de configuration
Activer	Activez cette case à cocher pour activer l'action de sortie SNMP des messages d'alerte du Reporting Engine. La valeur par défaut est Désactiver.
Nom du serveur	Spécifiez le nom d'hôte ou l'adresse IP du serveur sur lequel s'exécute le serveur SNMP. La valeur par défaut est **0.0.0.0**.
Port de serveur	Spécifiez le numéro de port du serveur sur lequel le serveur SNMP cible écoute les défaillances et les exceptions. La valeur par défaut est **1610**.
Version SNMP	Spécifiez le numéro de version du protocole SNMP que NetWitness Suite utilise pour envoyer des traps SNMP.
ID d'objet de trap	Spécifiez le numéro d'identification d'objet qui identifie le type de traps à envoyer. La valeur par défaut est **0.0.0.0.0.1**.
Communauté	Spécifiez le groupe SNMP auquel NetWitness Suite appartient. La valeur par défaut est **public**.
Nombre de tentatives	Spécifiez le nombre maximal de tentatives que NetWitness Suite effectue pour renvoyer le message d'alerte via SNMP. La valeur par défaut est **2**.
Expiration du délai	Spécifiez le délai d'expiration de NetWitness Suite en secondes (arrêt des tentatives d'envoi d'alertes SNMP). La valeur par défaut est **1 500**.
Appliquer	Mettez à jour la configuration.

Syslog

Une fois l'exécution terminée, toutes les notifications sont envoyées via des messages Syslog à un hôte particulier en fonction de la configuration Syslog. Vous pouvez configurer plusieurs serveurs Syslog dans le panneau Configuration Syslog.

La figure suivante montre la configuration Syslog sous l'onglet Actions de sortie.



Les paramètres suivants gèrent la configuration de l'action de sortie syslog pour un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, vous pouvez définir des valeurs pour cette configuration de sortie, car aucune valeur par défaut n'est disponible pour cette configuration. Vous devez modifier les **valeurs de configuration** de ces paramètres selon les exigences de votre entreprise.

Nom	Valeur de configuration
Nom Syslog	Nom de la configuration Syslog. **Remarque :** Vous ne pouvez pas créer de configuration Syslog avec un nom qui existe déjà dans la liste de configurations Syslog de Reporting Engine.
Encoding	Spécifiez l'encodage d'internationalisation des messages Syslog. La valeur par défaut est **UTF8**.
Nom du serveur	Spécifiez le nom d'hôte ou l'adresse IP du serveur sur lequel s'exécute le processus Syslog cible. Par défaut, la valeur n'est pas renseignée.
Port de serveur	Spécifiez le numéro de port du serveur sur lequel le serveur Syslog cible écoute les défaillances et les exceptions. La valeur par défaut est **514**.
Longueur max.	Spécifiez la taille maximale (en octets) de chaque message d'alerte Syslog. La valeur par défaut est **2048**. Si **UDP** est le type de transports et si la taille du message Syslog est supérieure à 1 024 octets, vous devez configurer un serveur Syslog qui prend en charge les messages dont la taille est supérieure à 1 024 octets.
Identifier la chaîne	Spécifiez la chaîne que NetWitness Suite insère au début de tous les messages d'alerte Syslog. Par défaut, la valeur n'est pas renseignée.

Nom	Valeur de configuration
Inclure le nom d'hôte local	Activez cette case à cocher pour inclure le nom d'hôte local dans tous les messages d'alerte Syslog. La valeur par défaut consiste à ne pas inclure de nom d'hôte local.
Tronquer le message	Activez cette case à cocher pour tronquer tous les messages d'alerte Syslog. La valeur par défaut consiste à ne pas tronquer les messages Syslog.
Utiliser l'identité	Activez cette case à cocher pour utiliser le protocole IDENT. La valeur par défaut consiste à ne pas utiliser ce protocole.
Inclure l'horodatage local	Activez cette case à cocher pour inclure l'horodatage local dans tous les messages d'alerte Syslog. La valeur par défaut consiste à ne pas inclure d'horodatage local.
Protocole de transport	Spécifiez le type de transports pour la remise des messages Syslog. Il existe trois parties pour le type de transport Syslog : UDP, TCP et SECURE_TCP. La valeur par défaut est **UDP**.
Délimiteur de message Syslog	Spécifiez le délimiteur du message Syslog. Il existe trois délimiteurs : CR, LF et CRLF. La valeur par défaut est **CR**. **Remarque :** Ce champ est renseigné lorsque vous sélectionnez TCP ou SECURE_TCP en tant que protocole de transport.
Mot de passe de la zone de stockage fiable	Spécifiez le mot de passe du magasin d'approbations. **Remarque :** Ce champ est renseigné lorsque vous sélectionnez SECURE_TCP en tant que protocole de transport.
Mot de passe du magasin de clés	Spécifiez le mot de passe du magasin de clés. **Remarque :** Ce champ est renseigné lorsque vous sélectionnez SECURE_TCP en tant que protocole de transport.
Appliquer	Enregistrez la configuration.

SFTP

Une fois l'exécution terminée, vous pouvez envoyer ou transférer des fichiers vers un site distant en fonction de la configuration SFTP.

La figure suivante montre la configuration SFTP sous l'onglet Actions de sortie.

Les paramètres suivants gèrent la configuration de l'action de sortie SFTP (transfert de fichiers vers un disque local) pour un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, vous pouvez définir des valeurs pour la configuration de cette sortie, car aucune valeur par défaut n'est disponible pour cette configuration. Vous devez modifier les **Valeurs de configuration** de ces paramètres selon les exigences de votre entreprise.

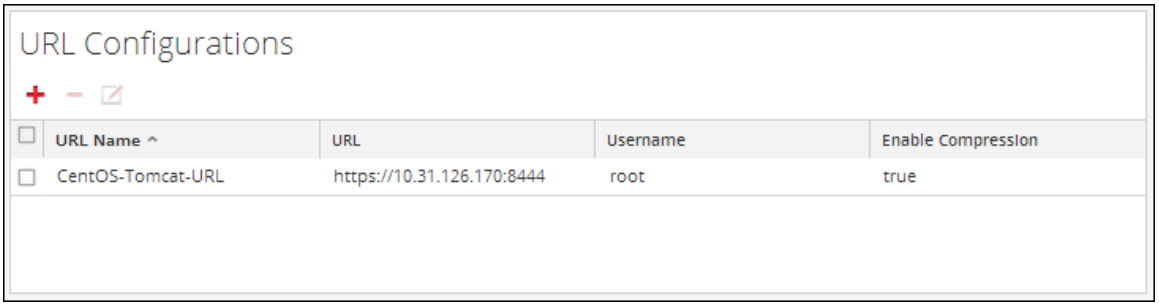
Nom	Valeur de configuration
Nom SFTP	Nom de la configuration SFTP. **Remarque :** Vous ne pouvez pas créer de configuration SFTP avec un nom qui existe déjà dans la liste de configurations SFTP de Reporting Engine.
Hôte	Adresse IP ou nom d'hôte du serveur Reporting Engine associé au transfert de fichiers.
Port	Si vous souhaitez utiliser un autre port que le port par défaut, saisissez un numéro de port. La valeur par défaut est **22**.
Nom d'utilisateur	Spécifiez le nom d'utilisateur de la configuration SFTP.
Mot de passe	Spécifiez le mot de passe de la configuration SFTP.

Nom	Valeur de configuration
Dossier personnalisé	Sélectionnez un emplacement SFTP auquel vous souhaitez transférer le fichier. Vous pouvez utiliser la structure de répertoire Windows ou Linux prédéfinie dans le chemin de dossier personnalisé. Par exemple, **/root/Downloaded_Files**. **Remarque :** Si le répertoire n'existe pas, RE le crée dans le chemin de dossier personnalisé, puis copie les fichiers dans ce répertoire.
Activer la compression	Cochez cette case pour activer la compression. La valeur par défaut est Activer la compression. Si la valeur est activée, les fichiers de sortie présentent l'extension .zip.

URL

Une fois l'exécution terminée, les fichiers de sortie sont publiés vers une URL en fonction de la configuration URL.

La figure suivante montre la configuration URL sous l'onglet Actions de sortie.



Les paramètres suivants gèrent la configuration de l'action de sortie URL (transfert de fichiers vers une URL) pour un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, vous pouvez définir des valeurs pour cette configuration de sortie, car aucune valeur par défaut n'est disponible pour cette configuration. Vous devez modifier les valeurs de configuration de ces paramètres selon les exigences de votre entreprise.

Nom	Valeur de configuration
Nom de l'URL	Nom de la configuration URL. **Remarque :** Vous ne pouvez pas créer de configuration URL avec un nom qui existe déjà dans la liste des configurations URL de Reporting Engine.
URL	Adresse URL associée au transfert de fichiers.

Nom	Valeur de configuration
Nom d'utilisateur	Spécifiez le nom d'utilisateur de la configuration URL.
Mot de passe	Spécifiez le mot de passe de la configuration URL.
Activer la compression	Cochez cette case pour activer la compression. La valeur par défaut est Activer la compression. Si la valeur est activée, les fichiers de sortie présentent l'extension .zip.

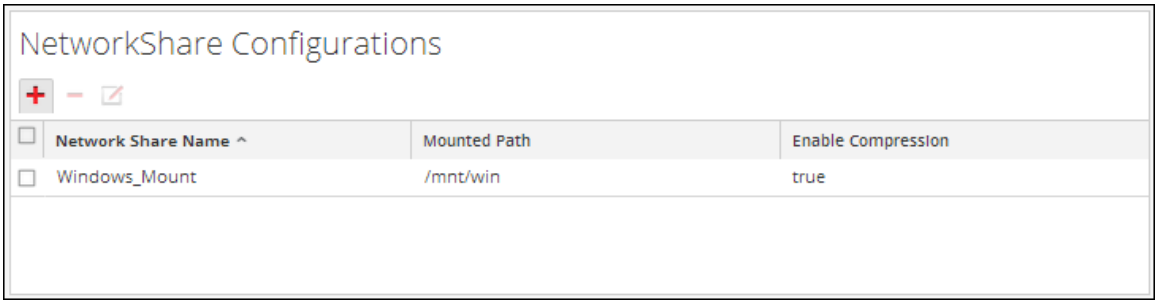
Une fois l'URL configurée, les fichiers sont copiés dans le répertoire « URL_OUTPUT_ ACTION », et les paramètres suivants sont envoyés au serveur avec le fichier compressé.

Nom	Valeur de configuration
filename	Le nom du fichier.
filesize	Taille du fichier en octets.
filetype	Type de fichiers associé au fichier.
filechecksum	Nombre calculé à partir d'un fichier pour confirmer qu'il s'agit bien du fichier attendu, et qu'il a été téléchargé et stocké correctement.
hashingalgorithm	Algorithme de hachage utilisé pour calculer le cheksum du fichier.
reportname	Nom du rapport téléchargé.
executionid	ID d'exécution associé à l'exécution du rapport.
reportexecutionstarttime	Heure de début de l'exécution du rapport.
état	État de création du rapport.
description d'état	Description de l'état.

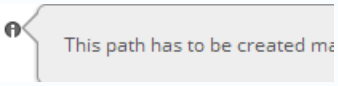
Partage réseau

Une fois l'exécution terminée, vous pouvez transférer les fichiers de sortie vers un chemin monté ou un emplacement partagé en fonction de la configuration de partage réseau.

La figure suivante montre la configuration de partage réseau sous l'onglet Actions de sortie.



Les paramètres suivants gèrent la configuration de l'action de sortie Partage réseau (transfert de fichiers vers un emplacement partagé sur le réseau) pour un service Reporting Engine. Lorsque vous ajoutez un service Reporting Engine, vous pouvez définir des valeurs pour cette configuration de sortie, car aucune valeur par défaut n'est disponible pour cette configuration. Vous devez modifier les **valeurs de configuration** de ces paramètres selon les exigences de votre entreprise.

Nom	Valeur de configuration
Nom du partage réseau	Nom du partage de réseau. **Remarque :** Vous ne pouvez pas créer de configuration Partage réseau avec un nom qui existe déjà dans la liste de configurations Partage réseau de Reporting Engine.
Chemin d'accès monté	Chemin (emplacement) associé au transfert de fichiers. Vous pouvez utiliser la structure de répertoire Linux prédéfinie dans le chemin monté. Par exemple **/mnt/win**. **Remarque :** L'utilisateur « rsasoc » doit disposer d'un accès en lecture/écriture au chemin monté du partage réseau spécifié.
	Cliquez pour visualiser la façon dont le chemin monté est créé. Cette fenêtre popup vous avertit que vous devez créer manuellement le chemin monté.
Activer la compression	Cochez cette case pour activer la compression. La valeur par défaut est Activer la compression. Si la valeur est activée, les fichiers de sortie présentent l'extension .zip.

Le tableau suivant répertorie les opérations courantes que vous pouvez effectuer dans les sections Syslog, SFTP, URL et de Partage réseau.

Opération	Description
	Créer une configuration Syslog, SFTP, URL et de Partage réseau.
	Supprimer une configuration Syslog, SFTP, URL et de Partage réseau.
	Modifier une configuration Syslog, SFTP, URL et de Partage réseau.

Onglet Gérer les Logos

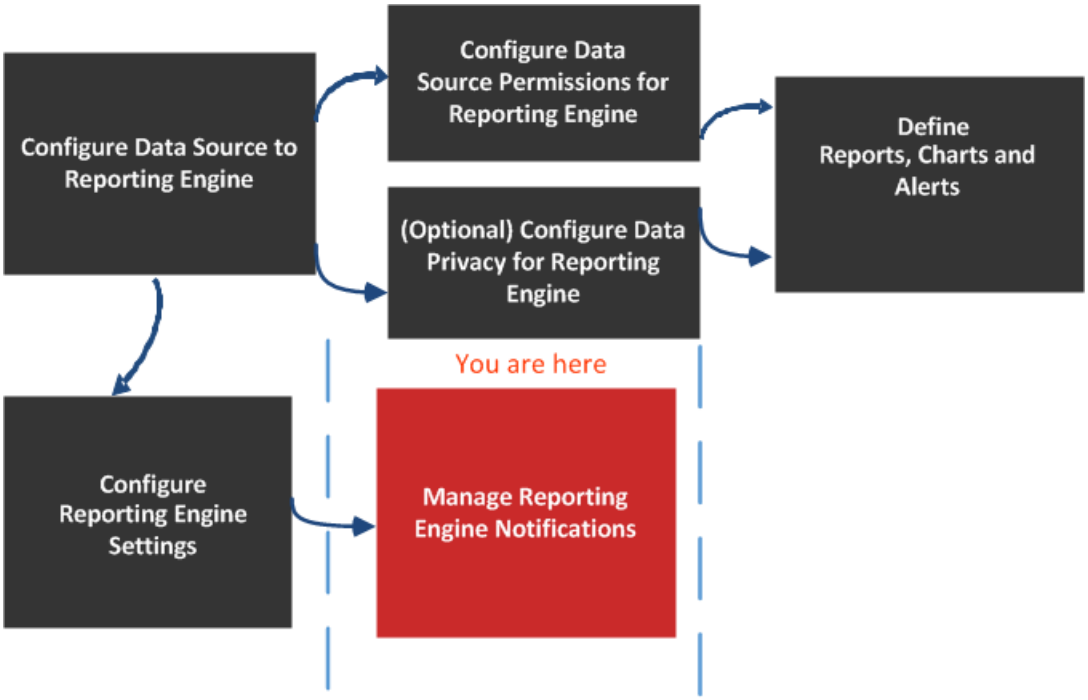
Les options de Gérer les logos disponibles dans la **Vue Configuration des services** > onglet **Gérer les logos** vous aident à gérer les logos associés à Reporting Engine. L'onglet Gérer les logos est composé d'un panneau unique avec une barre d'outils et une grille qui répertorie les logos.

Vous pouvez télécharger les logos que vous voulez utiliser dans votre rapport. Après avoir téléchargé le logo, vous pouvez définir tout logo comme logo par défaut qui sera utilisé automatiquement dans tous les rapports planifiés. Vous pouvez choisir de remplacer le logo par défaut avec un autre logo figurant dans cet onglet lorsque vous planifiez un rapport. Pour plus d'informations, consultez la rubrique « Boîte de dialogue Sélectionner un logo » dans le *Guide de Reporting*.

Les formats d'images pris en charge sont :

- .jpg
- .png
- .gif

Workflow



Que voulez-vous faire ?

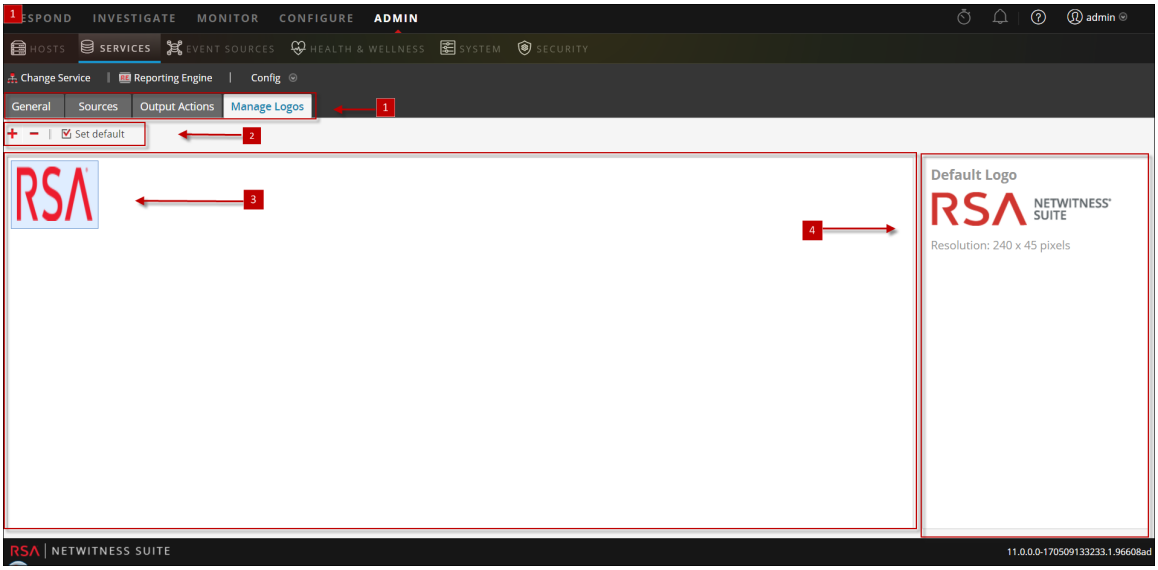
Rôle	Je souhaite...	Consultez...
Administrateur	Configurer la source de données dans le Reporting Engine	Configurer les sources de données
Administrateur	Configurer les autorisations d'accès aux sources de données pour le Reporting Engine	Configurer les autorisations d'accès aux sources de données
Administrateur	Configurer la confidentialité des données pour le Reporting Engine	Configurer la confidentialité des données pour le Reporting Engine
Administrateur	Définir les rapports, graphiques et alertes	Définir les rapports, graphiques et alertes
Administrateur	Configurer les paramètres du Reporting Engine	Configurer les paramètres du Reporting Engine
Administrateur/responsable du SOC	Ajouter ou supprimer des logos*	Configurer les paramètres généraux du Reporting Engine
Administrateur/responsable du SOC	Afficher la liste des logos*	Configurer les paramètres généraux du Reporting Engine
Administrateur/responsable du SOC	Définir un logo comme valeur par défaut*	Configurer les paramètres généraux du Reporting Engine

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Mode de fonctionnement du Reporting Engine

Aperçu rapide



Remarque : le logo à télécharger ne doit pas dépasser 500 Ko. L'autorisation requise pour accéder à cette vue est gérer les services.

1. Affiche tous les onglets configurables disponibles.
2. Affiche les actions de modification.
3. Affiche tous les logos qui ont été utilisés.
4. Affiche le logo par défaut utilisé.

L'onglet Gérer les logos vous permet d'effectuer les actions suivantes :

Icône	Actions
	Ajoutez de nouveaux logos à partir du répertoire local sur Reporting Engine. **Remarque :** la taille du logo ne peut pas dépasser 500 Ko. Les logos choisis doivent être les types de fichiers suivants : * .jpg * .gif * .png
	Supprime les logos de Reporting Engine. **Remarque :** en effectuant (Ctrl + clic), vous pouvez sélectionner plusieurs logos à supprimer.
	Définit le logo par défaut pour Reporting Engine. Il s'agit du logo par défaut de NetWitness Suite dans le panneau **Logo** de la vue Planifier un rapport. **Remarque :** si aucun logo par défaut n'est sélectionné, le logo RSA s'affiche.