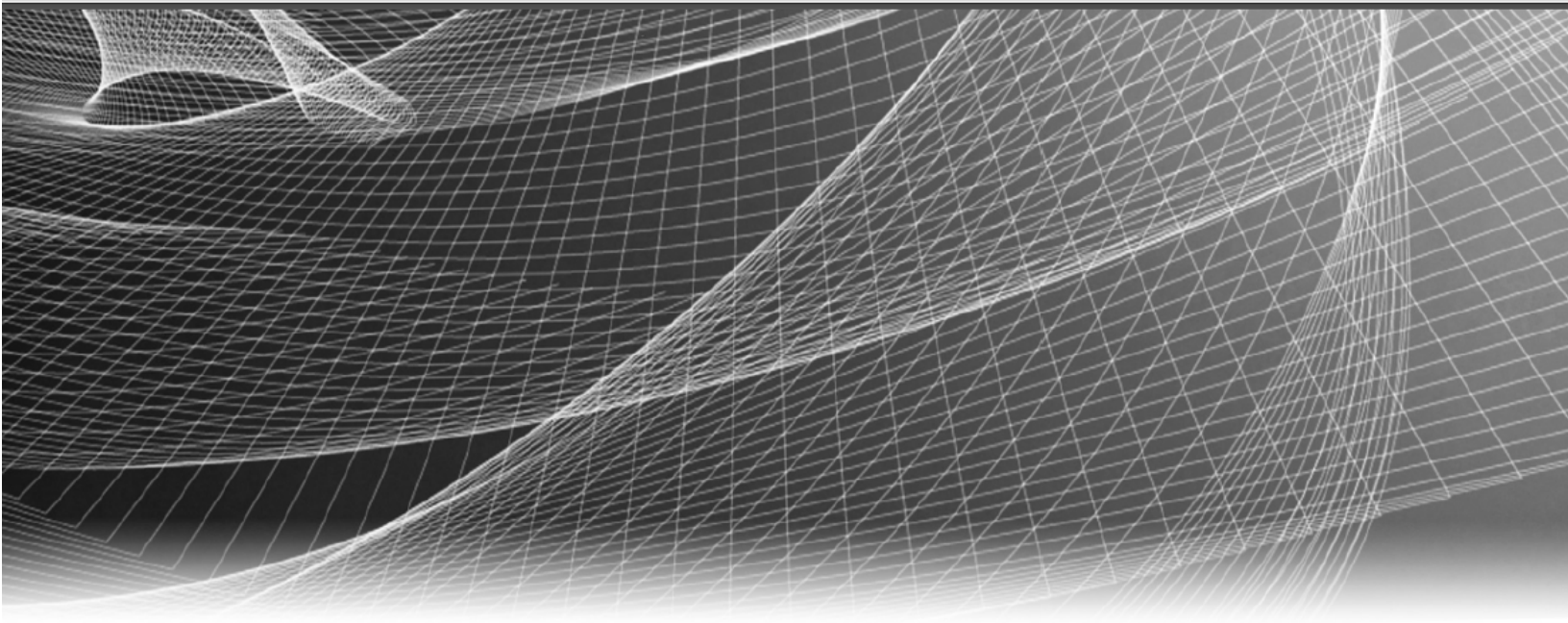


RSA Security Analytics

Guide de configuration de Reporting Engine

pour la version 10.6

RSA EMC²

Marques commerciales

Contrat de licence

Licences tierces

Remarque sur les technologies de chiffrement

Distribution

Sommaire

Présentation du Reporting Engine

Cette rubrique présente le Reporting Engine. Le Reporting Engine prend en charge la définition et la génération des rapports et des alertes que vous gérez dans les vues et les dashlets des modules RSA Security Analytics Reporting et Alerting. Un Reporting Engine :

- Facilite la diffusion des données sélectionnées dans les vues des modules Reporting et Alerting (métadonnées NetWitness et données d'événements IPDB).
- Stocke les définitions des règles qui régissent le mode de représentation des données dans les rapports et les alertes.
- Gère la file d'attente des alertes en vous permettant d'activer ou désactiver les alertes.

  Le Reporting Engine exécute les rapports 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 IPDB : la base de données Internet Protocol Database (IPDB) contient à la fois des messages d'événements normalisés et bruts. Elle stocke tous les messages collectés dans un système de fichiers organisé par source d'événements (périphérique), adresse IP, et indication temporelle (année/mois/jour) avec des fichiers d'index pour faciliter les recherches (rapport et requêtes).
- Sources de données NWDB : les sources de données NetWitness Database (NWDB) sont les composants Decoder, Log Decoder, Broker, Concentrator, Archiver et Collection.
- Sources de données Warehouse : les sources de données Warehouse sont Pivotal et MapR.

Configurer le Reporting Engine

Cette rubrique répertorie les principales tâches de configuration de Reporting Engine pour une source de données. La liste de contrôle suivante répertorie les tâches nécessaires pour configurer un Reporting Engine ainsi qu'une source de données pour l'utiliser avec Reporting Engine. Ces tâches sont répertoriées dans l'ordre dans lequel vous devez les effectuer.

Vous devez vous assurer que les sources de données sont déployées et configurées dans Security Analytics. Reportez-vous à l'étape 2 : ajouter un service à un hôte.

Étape	Description :
1	Étape 1. Ajouter un Reporting Engine à votre déploiement Security Analytics.
2	Étape 2. Configurer les paramètres du Reporting Engine
3	Étape 3. Configurer les sources de données du Reporting Engine et Configurer les autorisations d'accès aux sources de données.
4	Étape 4. Configurer les actions de sortie.
5	Étape 5. Configurer le Planificateur de tâches pour un Reporting Engine

Avec la configuration de base, vous pouvez effectuer ces tâches supplémentaires comme il est nécessaire :

- Recherchez le dernier contenu de source de données dans Live et déployez-le régulièrement. (Voir l'Étape 4 Gérer les ressources Live dans le guide *Gestion des services en direct*).
- (Facultatif) Ajouter de l'espace supplémentaire pour les rapports volumineux.

Topics

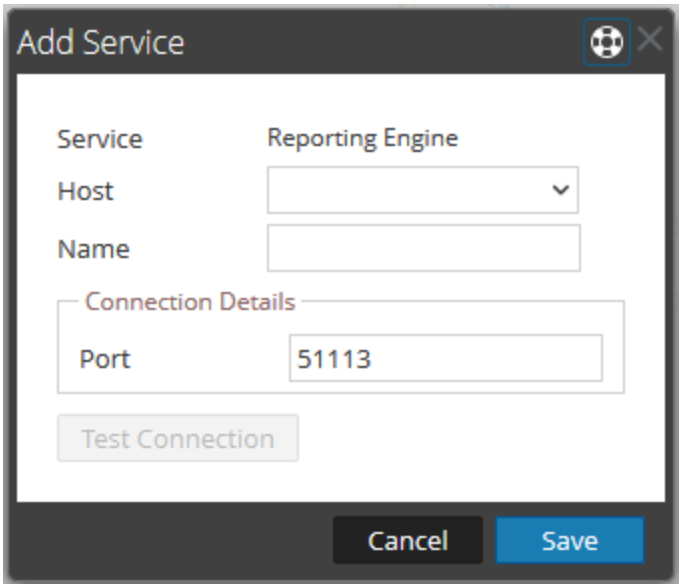
Étape 1. Ajouter un Reporting Engine

Assurez-vous que le service Reporting Engine est déployé sur Security Analytics.

Pour ajouter un Reporting Engine :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** > **Services**.
2. Cliquez sur + > **Reporting Engine**.
3. Dans la boîte de dialogue Ajouter un service, effectuez les opérations suivantes :
   a. Saisissez l'hôte du Reporting Engine.
   b. Saisissez le nom du Reporting Engine.

      L'illustration suivante présente un exemple d'ajout d'un service Reporting Engine à un hôte Broker (par exemple 10.31.205.50).

      Lorsque vous ajoutez un service Reporting Engine, Security Analytics utilise par défaut le port REST correct (**51113**).
   c. Pour utiliser un autre port que le port par défaut, saisissez le numéro de port.
4. Cliquez sur **Tester la connexion** pour vérifier la connexion.

Étapes suivantes

Vous devez spécifier les paramètres généraux, les sources de données et les actions de sortie.

Étape 2. Configurer les paramètres du Reporting Engine

Veillez à ce que le service Reporting Engine soit déployé sur Security Analytics et que le service soit ajouté.

Pour configurer les paramètres de service de Reporting Engine :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans le panneau **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue > Configuration**.

   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 du Reporting Engine, voir Reporting Engine : Onglet General.
4. Modifiez les paramètres de service Reporting Engine et cliquez sur **Appliquer**.

   Les paramètres de service sont configurés sur Reporting Engine.

Étapes suivantes

Étape 3. Configurer les sources de données du Reporting Engine

Étape 3. Configurer les sources de données du Reporting Engine

Cette rubrique vous indique comment :

- Ajouter une source de données au Reporting Engine
- Définir une source de données comme source par défaut

Ajouter une source de données au Reporting Engine

Cette section contient les procédures suivantes :

- Configuration basique
- Activer des tâches
- Activer l'authentification Kerberos

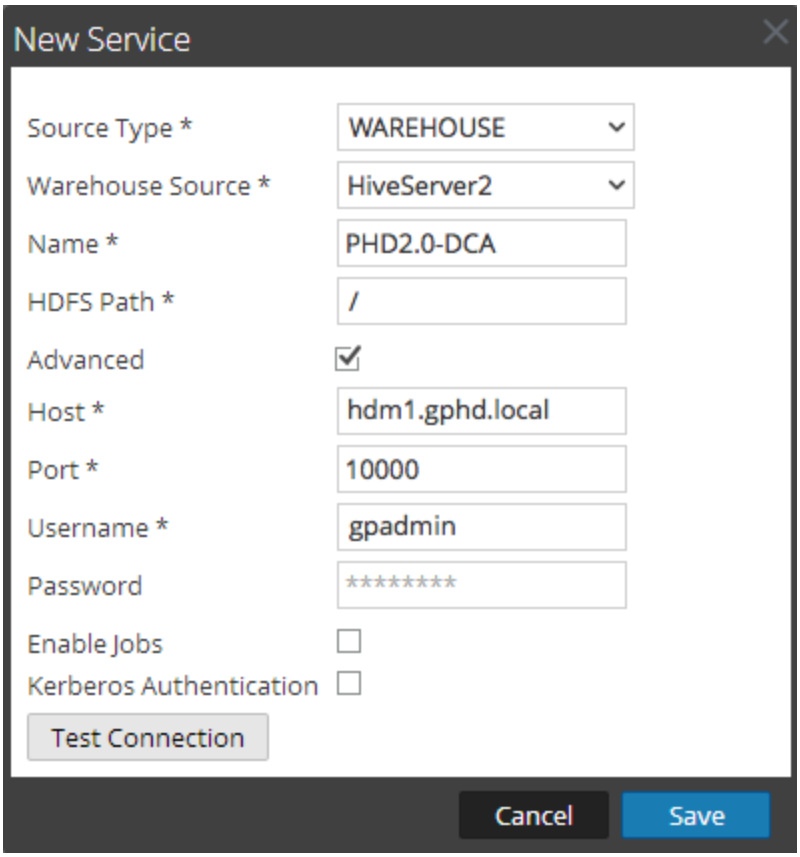
Configuration basique

Pour associer une source de données au Reporting Engine, procédez comme suit :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans la **grille Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  **> Vue > Configuration**.

   La vue Configuration des services du Reporting Engine s'affiche.
4. Sous l'onglet **Sources** , cliquez sur  > **Nouveau service**.

   La boîte de dialogue **Nouveau service** s'affiche.



5. Renseignez les champs comme suit :

   a. Dans le menu déroulant **Type de source**, sélectionnez **Warehouse**.

   b. Dans le menu déroulant **Source Warehouse**, sélectionnez la source de données Warehouse.

   c. Dans le champ **Nom**, saisissez le nom de la source de données Warehouse.

   > **Remarque :** Veillez à ne pas utiliser de caractères spéciaux comme &,' , ", < et > en ajoutant la source de données. Si vous utilisez des caractères spéciaux dans le nom du champ, la mise à jour du Reporting Engine échoue.

   d. Dans le champ **Chemin HDFS**, indiquez le chemin d'accès racine HDFS sur lequel le Warehouse Connector écrit les données.

   Par exemple :
   Supposons que **/saw** correspond au point de montage local de HDFS que vous avez configuré lors du montage de NFS sur le périphérique sur lequel vous avez installé le service Warehouse Connector en vue d'écrire des données sur SAW. Pour plus d'informations, consultez la rubrique **Mount the Warehouse on the Warehouse Connector** dans le *Guide de configuration de RSA Analytics 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.

e. Activez la case à cocher **Avancés** 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.

f. 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**.

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

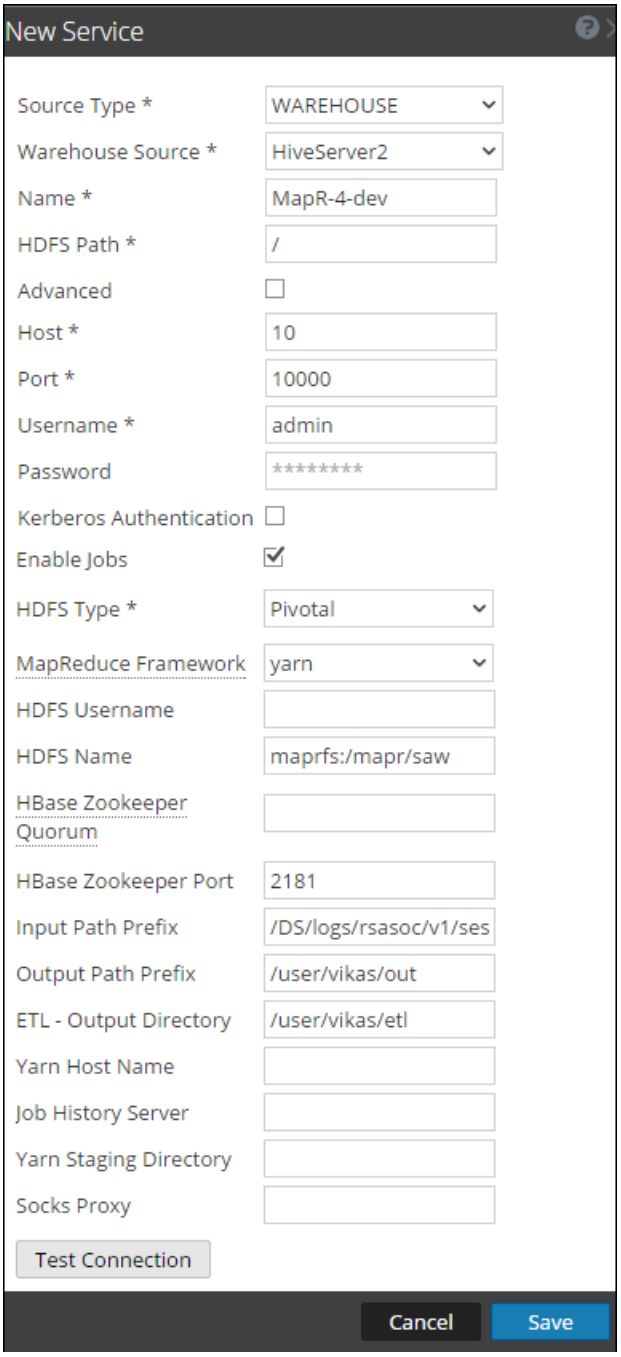
Remarque : Vous pouvez également utiliser le mode d'authentification LDAP via Active Directory. Pour plus d'instructions sur l'activation du mode d'authentification LDAP, consultez la rubrique Activer l'authentification LDAP.

Passez à la section suivante, **Activer des tâches**, si vous souhaitez exécuter des rapports Warehouse Analytics. Si vous ne souhaitez pas exécuter des rapports Warehouse Analytics, passez à **Activer l'authentification Kerberos**.

Activer des tâches

Pour exécuter des rapports Warehouse Analytics, effectuez cette procédure.

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



2. Renseignez les champs comme suit :

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

- Si vous sélectionnez le type HDFS Pivotal, 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 Pivotal. Pour les clusters Pivotal 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.

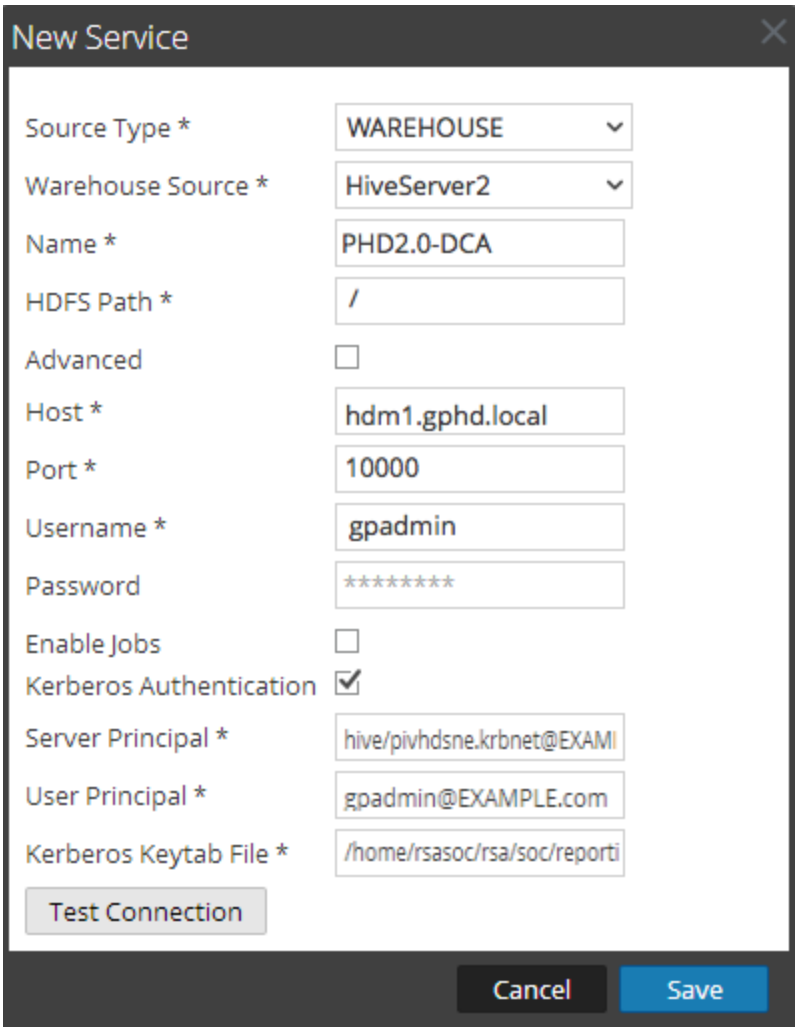
b. Sélectionnez le framework MapReduce en fonction du type HDFS.

Remarque : Pour le type HDFS MapR, sélectionnez Classic pour le framework MapReduce. Pour le type HDFS Pivotal, 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 sur lequel Kerberos est activé.



2. Renseignez les champs comme suit :

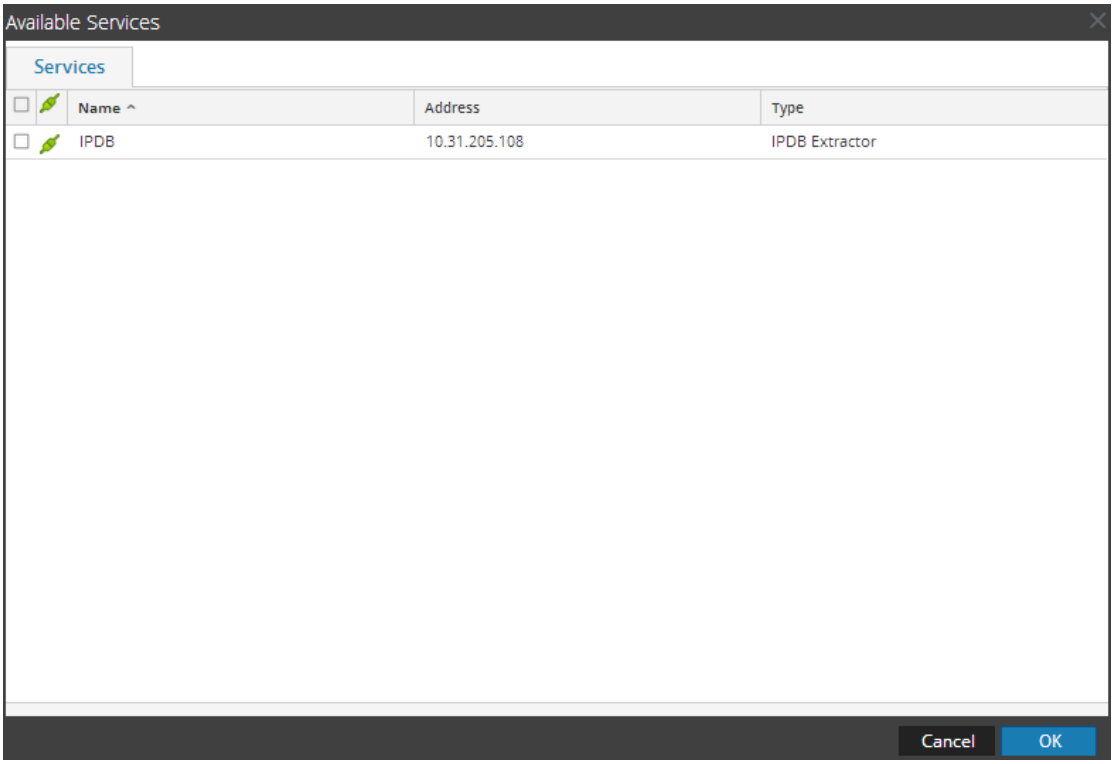
Champ	Description :
Entité de sécurité du serveur	Indiquez l'entité de sécurité que le serveur Hive utilise afin de procéder à l'authentification auprès du centre de distribution de clés (KDC) Kerberos.
Entité de sécurité de l'utilisateur	Saisissez l'entité de sécurité que le client JDBC Hive utilise 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 Reporting Engine : Onglet General. **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 **Save**.

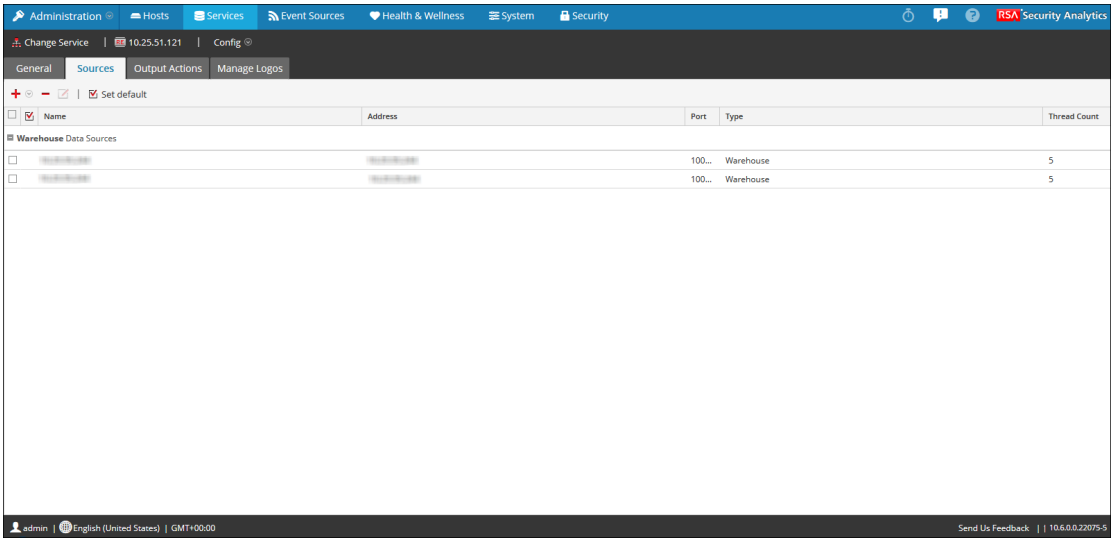
   La source de données Warehouse ajoutée s'affiche sous l'onglet Sources du Reporting Engine.
5. Cliquez sur > **Services disponibles**.

   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**.

Security Analytics 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. Dans le menu **Security Analytics**, sélectionnez **Tableau de bord > Administration > Services**.
2. Dans la **grille 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**.

   Security Analytics est défini sur cette source de données par défaut lorsque vous créez des rapports et des alertes par rapport à ce Reporting Engine.

Étapes suivantes

Ajouter Warehouse comme source de données au Reporting Engine

Cette rubrique fournit les instructions à suivre pour réaliser les opérations ci-après :

- Ajouter une source de données Warehouse au Reporting Engine
- Définir une source de données Warehouse en tant que source par défaut

Conditions préalables

Vérifiez que :

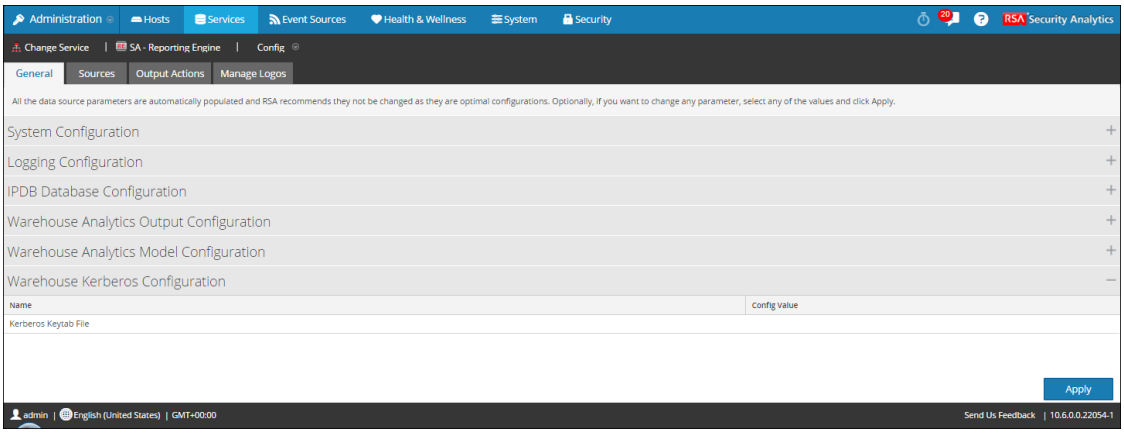
- Le serveur Hive est en cours d'exécution sur tous les nœuds Warehouse. Vous pouvez utiliser la commande suivante pour vérifier l'état du serveur hive :

  ```
  status hive2 (MapR deployments)
  service hive-server2 status (Pivotal HD 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 `/home/rsasoc/rsa/soc/reporting-engine/conf/` de l'hôte Reporting Engine.

  Remarque : Vérifiez que le rôle d'utilisateur **rsasoc** dispose d'autorisations de lecture en vue de lire le fichier de table de clés.

  Veillez également à mettre à jour le chemin d'accès indiqué dans le paramètre **Fichier de table de clés Kerberos** figurant dans la vue Configuration des services du Reporting Engine, comme indiqué ci-après.



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

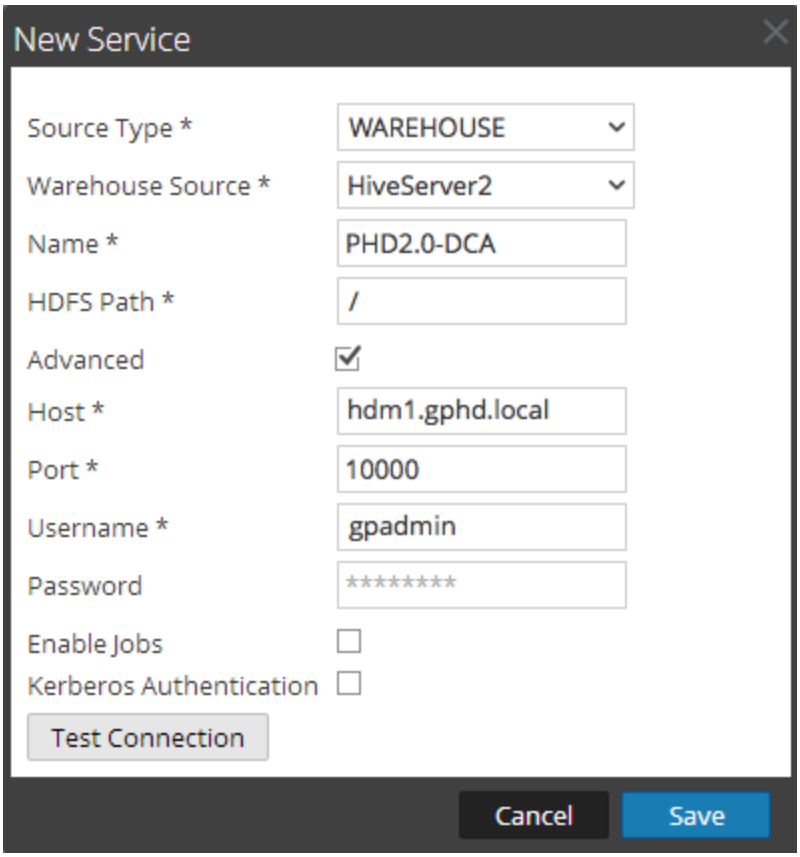
Procédure

Suivez les étapes ci-après pour associer une source de données Warehouse au Reporting Engine :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans la grille des **Services**, sélectionnez **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 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 :
   Supposons que **/saw** correspond au point de montage local de HDFS que vous avez configuré lors du montage de NFS sur le périphérique sur lequel vous avez installé le service Warehouse Connector en vue d'écrire des données sur SAW. Pour plus d'informations, consultez la rubrique **Mount the Warehouse on the Warehouse Connector** dans le *Guide de configuration de RSA Analytics 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 **Avancés** 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, reportez-vous à la section Activer des tâches à l'Étape 3. Configurer les sources de données du Reporting Engine.

14. Activez l'authentification Kerberos : reportez-vous à la section Activer l'authentification Kerberos à l'Étape 3. Configurer les sources de données du Reporting Engine.

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.

Résultat

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

Activer l'authentification LDAP

Cette rubrique donne des instructions sur la façon d'activer le mode LDAP pour l'authentification via Active Directory pour HiveServer2.

Procédure

Effectuez les étapes suivantes pour activer l'authentification LDAP de HiveServer2 :

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.

Résultat

Vous pouvez désormais vous connecter à HiveServer2 à l'aide des informations d'identification LDAP.

(Facultatif) Ajouter Archiver comme source de données au Reporting Engine

Cette rubrique donne des instructions sur la façon d'ajouter Archiver comme source de données au Reporting Engine afin de générer un rapport pour les données collectées par Archiver.

Conditions préalables

Assurez-vous d'avoir :

1. Installé l'hôte Security Analytics Archiver dans votre environnement réseau. Pour plus d'informations, reportez-vous à l'**Étape 1. Ajouter ou mettre à jour des hôtes** dans le *Guide de mise en route de l'hôte et des services*.
2. Log Decoder installé et configuré dans votre environnement réseau. Pour plus d'informations, voir l'**Étape 2. Ajouter un service Log Decoder en tant que source de données à un service Archiver** dans le *Guide de configuration d'Archiver*.
3. Ajouté Reporting Engine en tant que service à votre déploiement de l'Security Analytics. Pour plus d'informations, reportez-vous à la section. Pour plus d'informations, voir Étape 1. Ajouter un Reporting Engine.
4. Ajouté Archiver en tant que service à votre déploiement de l'Security Analytics. Pour plus d'informations, reportez-vous à la section. Pour plus d'informations, voir l'**Étape 1. Ajouter le service Archiver** dans le *Guide de configuration Archiver*.
5. Attribué une licence au service Archiver.

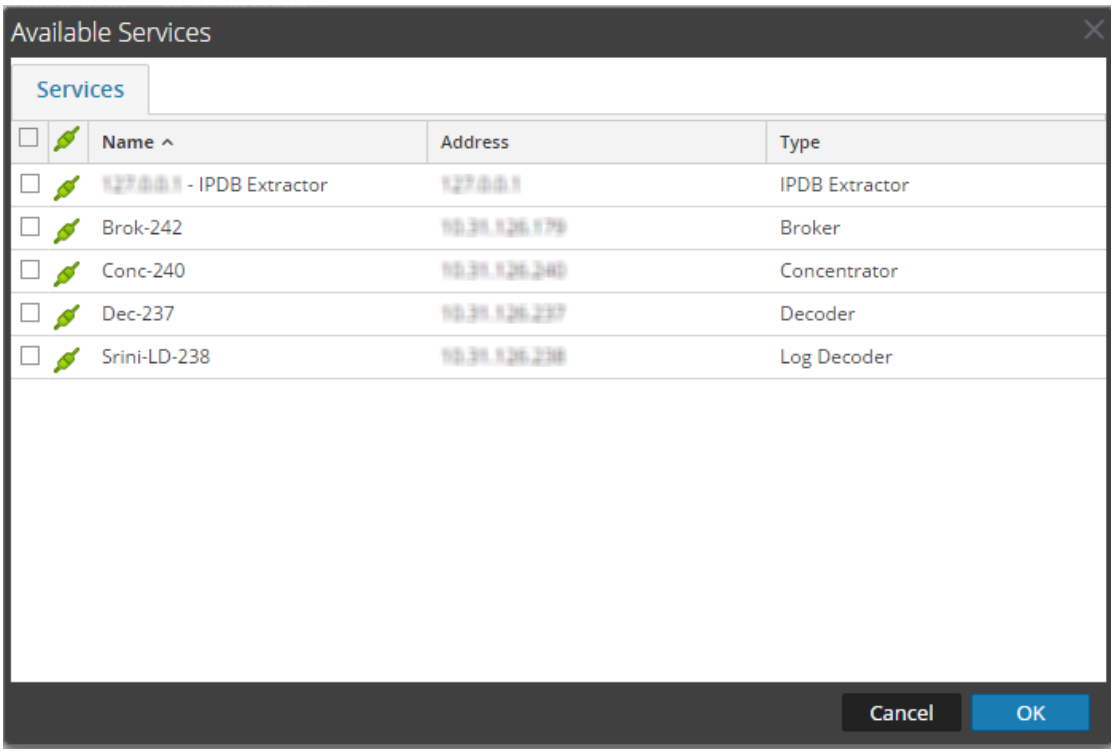
Associer une source de données Archiver au Reporting Engine

Pour associer une source de données Archiver au Reporting Engine, procédez comme suit :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans le panneau **Services**, sélectionnez le service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Configuration**.

   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**.

Résultat

Vous pouvez maintenant créer des rapports sur les données collectées par Archiver.

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

Cette rubrique donne des informations sur l'ajout d'une collection comme source de données au Reporting Engine.

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.

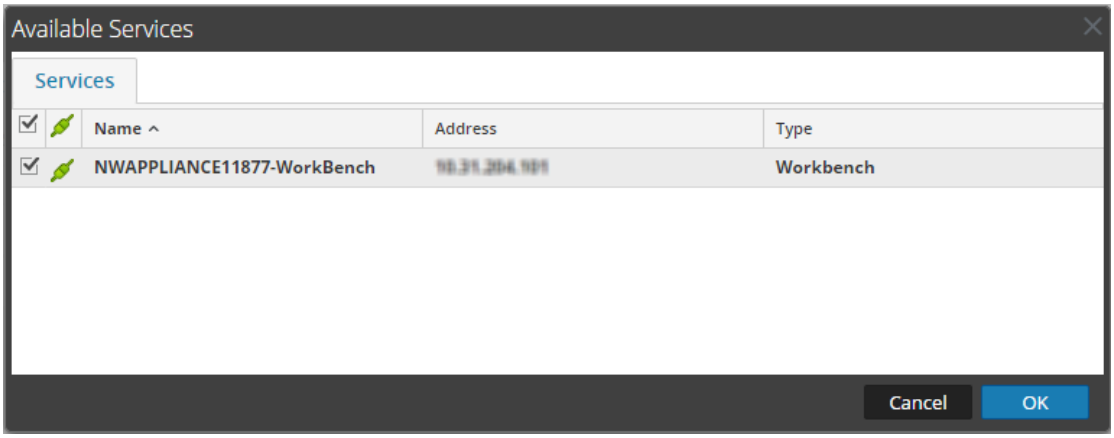
Procédure

Suivez les étapes ci-après pour associer une Collection en tant que source de doonnées au Reporting Engine :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** >**Services**.
2. Dans le panneau **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Config**.

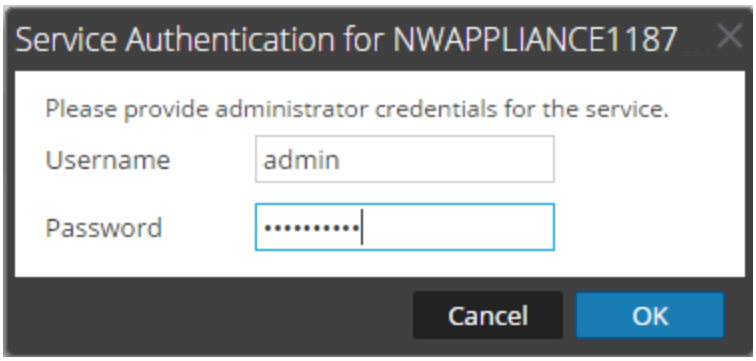
   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.
5. Cliquez sur + et sélectionnez **Services disponibles**.

   La boîte de dialogue Services disponibles s'affiche.



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

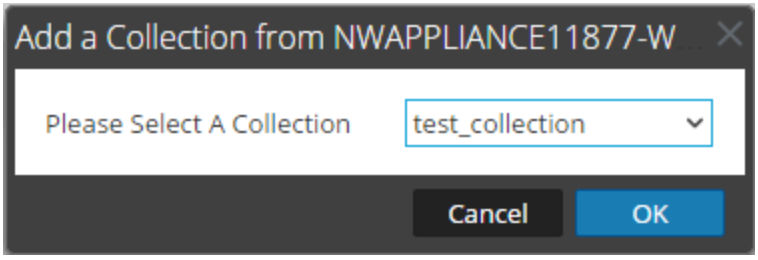
   La boîte de dialogue Authentification du service pour le service sélectionné s'affiche.



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.

Résultat

Vous pouvez maintenant créer des rapports sur les données collectées par la collection.

(Facultatif) Ajouter Workbench comme source de données au Reporting Engine

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. Ajouté Workbench en tant que service à votre déploiement de l'Security Analytics. Pour plus d'informations, reportez-vous à la section. Pour plus d'informations, voir l'**Étape 1. Ajouter le service Workbench** dans le *Guide de configuration Archiver*.
2. Ajouté une collection au service Workbench.

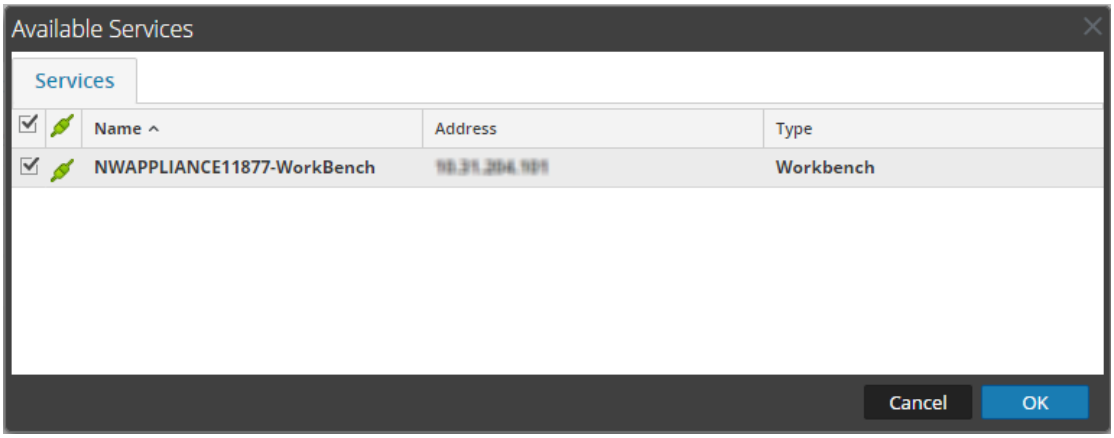
Procédure

Effectuez les étapes suivantes pour ajouter Workbench comme source de données au Reporting Engine :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** >**Services**.
2. Dans le panneau **Services**, sélectionnez un service **Reporting Engine**.
3. Sélectionnez  > **Vue** > **Configuration**.

   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**.

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.

Résultat

Vous pouvez maintenant créer des rapports sur les données collectées par Workbench.

(Facultatif) Intégrer les informations ECAT aux Rapports

Cette section fournit des instructions pour ajouter des informations ECAT aux rapports. Le *Guide d'intégration de RSA ECAT* fournit une vue d'ensemble de l'intégration d'ECAT dans RSA Security Analytics.

Conditions préalables

Vous devez avoir configuré les alertes ECAT via syslog dans un Log Decoder (reportez-vous à la rubrique Configurer des alertes ECAT via Syslog dans un Log Decoder dans le *Guide d'intégration de RSA ECAT*).

Intégrer les informations ECAT aux Rapports

Pour intégrer les informations ECAT aux Rapports :

1. Dans **Reporting Engine**>**Vue**>**Configuration**>**Sources**, ajoutez le Concentrator qui consomme des données dans le Log Decoder en tant que source de données.

   L'élément ECAT est renseigné dans Reporting Engine.

2. Exécutez des rapports en sélectionnant l'élément méta approprié.

Étape 4. Configurer les actions de sortie

Cette rubrique décrit comment configurer les actions de sortie pour un Reporting Engine.Elle fournit des informations sur la configuration des actions de sortie.

Pour configurer les actions de sortie pour un Reporting Engine :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans la **grille Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue**> **Configuration**.

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

4. Sous l'onglet **Actions de sortie**, modifiez les paramètres d'action de sortie pour chacune des configurations :
   - SMTP
   - SNMP
   - Syslog
   - SFTP
   - URL

- Partage réseau

  Pour plus d'informations sur chacune des configurations, consultez Actions de sortie du Reporting Engine.

5. Cliquez sur **Apply**.

Les actions de sortie sont configurées sur Reporting Engine.

Étape 5. 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 Warehouse. Pour plus d'informations sur les planificateurs de tâches, reportez-vous à la rubrique **Planificateur de tâches pour Warehouse Reporting** dans le *Reporting Guide*.

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.

  Notez les points suivants :

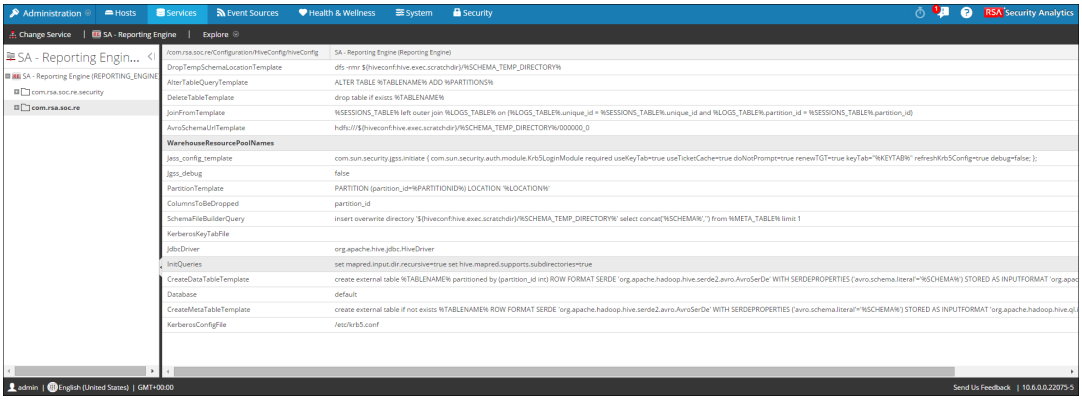
- SA n'accepte qu'une file d'attente ou pool par cluster. RSA recommande d'utiliser des noms de file d'attente ou de pool uniques dans tous les clusters ou le même nom de file d'attente ou de pool dans les deux clusters. Si le cluster est très volumineux, vous pouvez utiliser plus de trois files d'attente 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. Ce comportement repose sur la valeur spécifiée pour la propriété **mapred.fairscheduler.allow.undeclared.pools** du planificateur Fair.
- 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. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Sélectionnez **Moteur de reporting** et cliquez sur  > **Vue > Explorer**.
3. Accédez à **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.



Procédures supplémentaires

Cette rubrique regroupe des procédures supplémentaires pour le Reporting Engine. Consultez cette section pour obtenir des instructions sur une tâche spécifique après la configuration initiale du Reporting Engine.

Topics

Ajouter de l'espace supplémentaire pour les rapports volumineux

Cette rubrique donne des instructions pour ajouter de l'espace supplémentaire au Reporting Engine pour les rapports volumineux. Si vous devez générer des rapports de conformité volumineux pour IPDB ou Warehouse, l'espace disque de Reporting Engine risque d'être consommé 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 personnel 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.

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

Remarque : Les étapes ci-dessous partent du principe que le répertoire d'accueil de Reporting Engine se trouve dans le répertoire **/home/rsasoc/rsa/soc/reporting-engine/** et que le stockage externe est monté dans **/externalStorage/**.

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

   ```
   stop rsasoc_re
   ```

2. Passez à l'utilisateur `rsasoc`.

   ```
   su rsasoc
   ```

3. Basculez dans le répertoire personnel RE.

   ```
   cd /home/rsasoc/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 /home/rsasoc/rsa/soc/reporting-engine/resultstore
   ```

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

   ```
   ln -s /externalStorage/formattedReports /home/rsasoc/rsa/soc/reporting-engine/formattedReports
   ```

8. Quittez l'utilisateur `rsasoc`.

   ```
   exit
   ```

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

   ```
   start rsasoc_re
   ```

Remarque : Si le stockage externe est hors ligne, vous ne pouvez par effectuer les tâches suivantes :
(1) Exécuter des rapports ou des alertes de reporting
(2) Afficher les rapports existants ou les alertes de reporting
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 à l' Étape 2. Configurer les paramètres du Reporting Engine.

Configurer la confidentialité des données pour le Reporting Engine

Cette rubrique fournit des informations sur la configuration des sources de données pour Reporting Engine à l'aide de l'onglet **Sources** de la vue **Services > Vue > Config**.

Avec la fonction de confidentialité des données de Security Analytics 10.6 et version supérieure, l'accès aux métadonnées sensibles dans les services SA Core peut être limité par la configuration de sources de données distinctes pour les utilisateurs dotés du rôle de Responsable de la confidentialité des données et pour les autres utilisateurs, 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, voir le Configurer les autorisations d'accès aux sources de données.

Remarque : Un utilisateur dont le rôle est Responsable de la confidentialité des données (ou avec un rôle personnalisé équivalent), peut créer une alerte et configurer des actions de sortie sous la forme d'un rapport ou d'une alerte dans le module Reporting. Dans un environnement où les fonctions de confidentialité des données de Security Analytics 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, tous les méta protégés ou sensibles impliqués dans l'alerte sont automatiquement disponibles dans le service Gestion des incidents. Il se peut que par inadvertance l'accès au module Incident Management permettent à tous les utilisateurs d'accéder aux métavaleurs sensibles, quels que soient leurs rôles. Une option permet d'éviter cela en désactivant la publication sous Incident Management 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 Security Analytics 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, voir le 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.

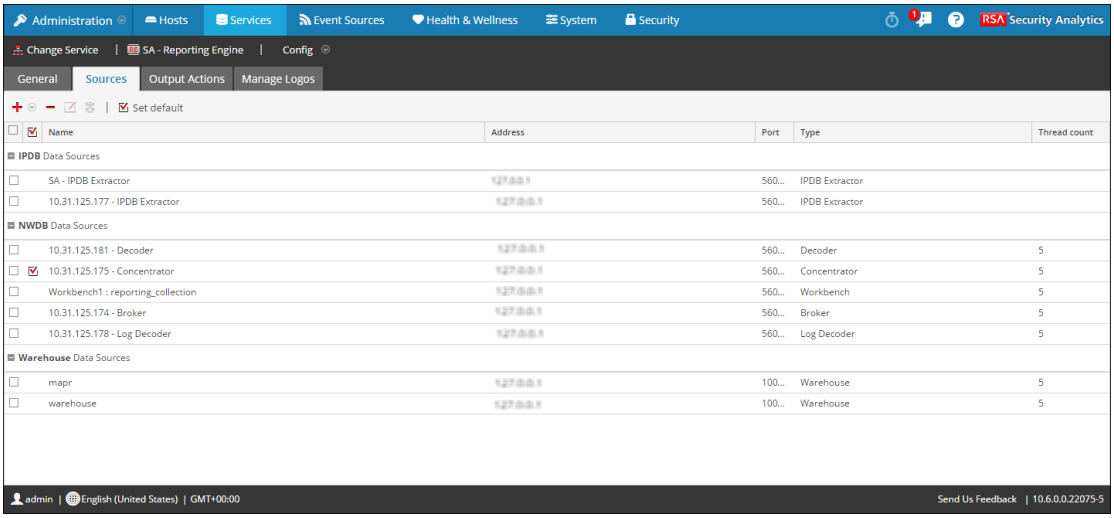
Ajouter une source de données NWDB avec différents comptes de service

Pour ajouter une source de données NWDB avec différents comptes de service :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans le panneau **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  **> Vue > Configuration**.

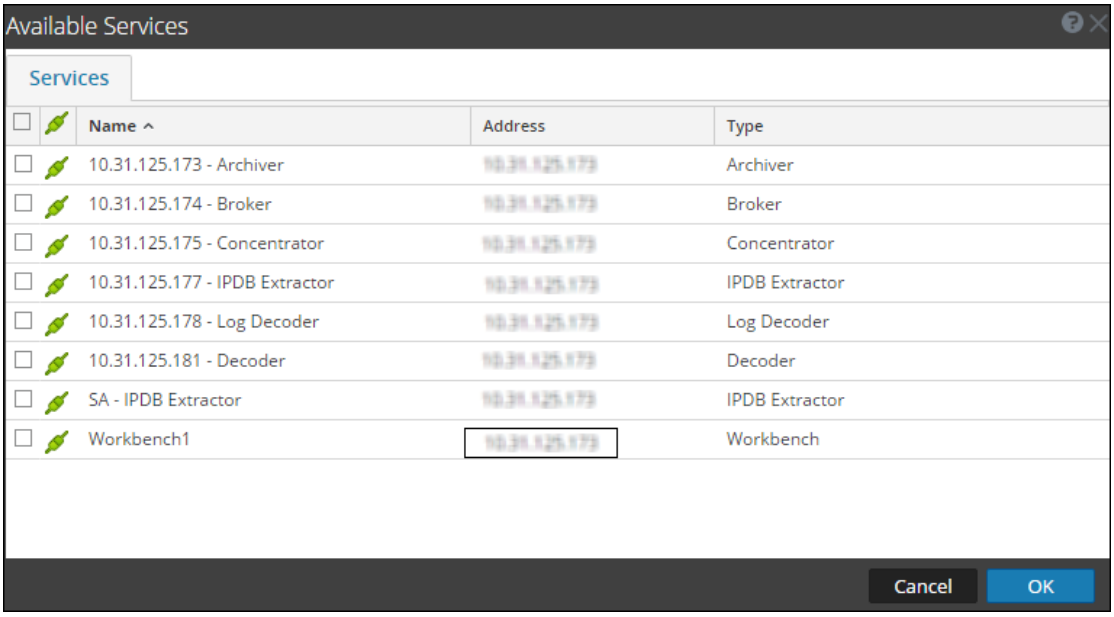
   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.

   La vue Configuration des services s'ouvre sur l'onglet Sources du Reporting Engine.



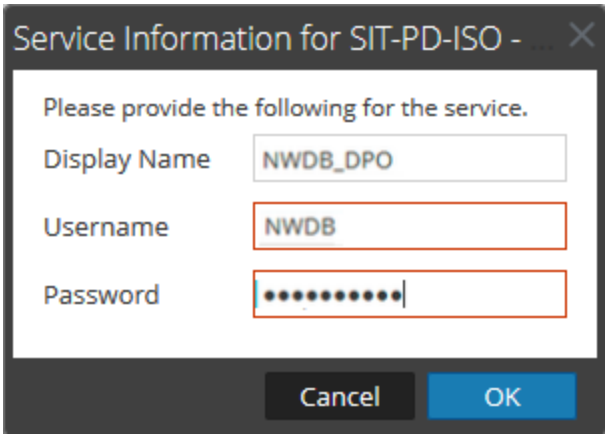
5. Cliquez sur + et sélectionnez Services disponibles.

   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 le service requis et cliquez sur **OK**.

   La boîte de dialogue Informations de gestion pour le service sélectionné s'affiche.

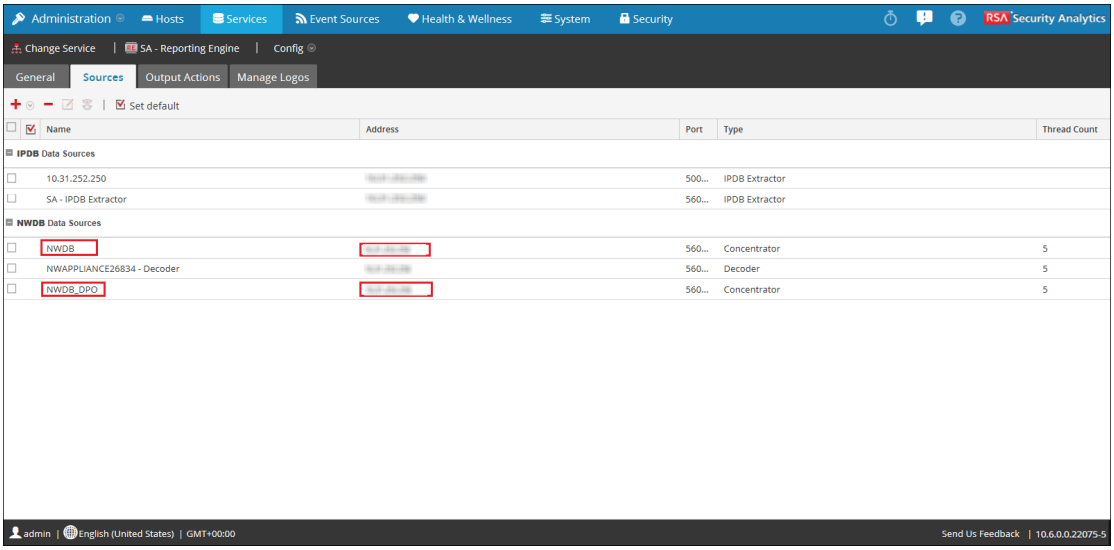


Remarque : Security Analytics vous demande de fournir un nom d'utilisateur et un mot de passe pour le service sélectionné. Pour limiter l'accès aux données sensibles, les utilisateurs responsables de la confidentialité des données doivent utiliser leurs informations d'identification, tout en ajoutant 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 Security Analytics et les hôtes Security Analytics 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.



Étapes suivantes

Après l'ajout de plusieurs sources de données avec différents comptes de service pour le même périphérique Core, vous pouvez configurer des autorisations d'accès aux sources de données qu'il est possible de gérer.

Configurer les autorisations d'accès aux sources de données

Cette rubrique donne des informations sur la configuration des autorisations de sources de données en utilisant l'onglet Sources de la vue Configuration des services pour le Reporting Engine. Vous pouvez gérer le contrôle d'accès aux sources de données en définissant les autorisations de source de données. Désormais, avec la capacité à 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 permettra d'exécuter des rapports avec Warehouse tout en restreignant l'utilisation de cette source pour toute autre personne.

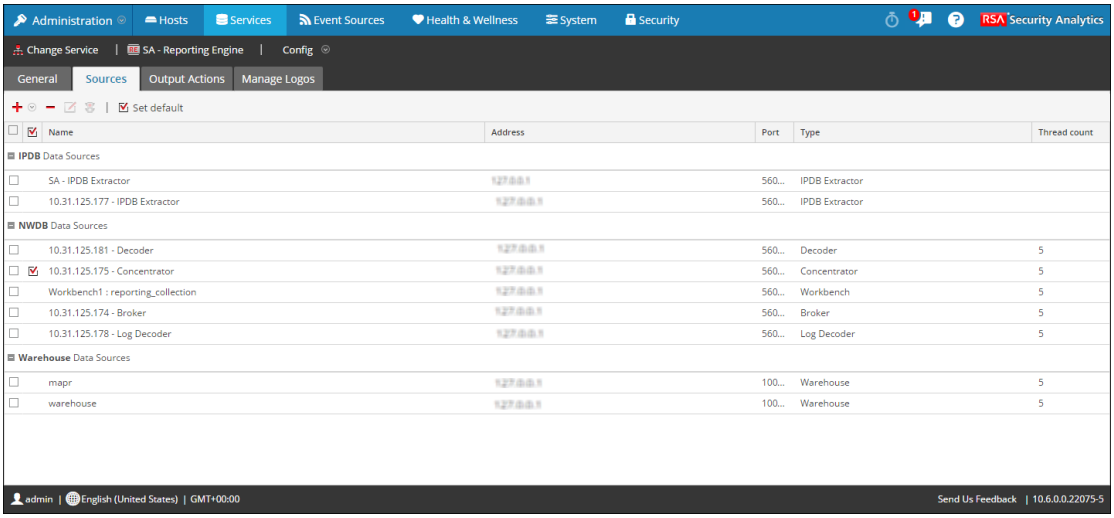
Remarque : Lorsque vous effectuez la mise à niveau de la version 10.5 à la version 10.6, les autorisations de NWDB et des sources de données Warehouse sont automatiquement définies d'après les autorisations des objets de reporting. Par exemple, si le rôle avait des autorisations définies en **Lecture seule**/**Lecture et écriture** pour tout objet de reporting dans la version 10.5, ce rôle se voit automatiquement attribuer 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. Les autorisations ne sont pas applicables pour les sources de données IPDB.

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

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans le panneau **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Configuration**.

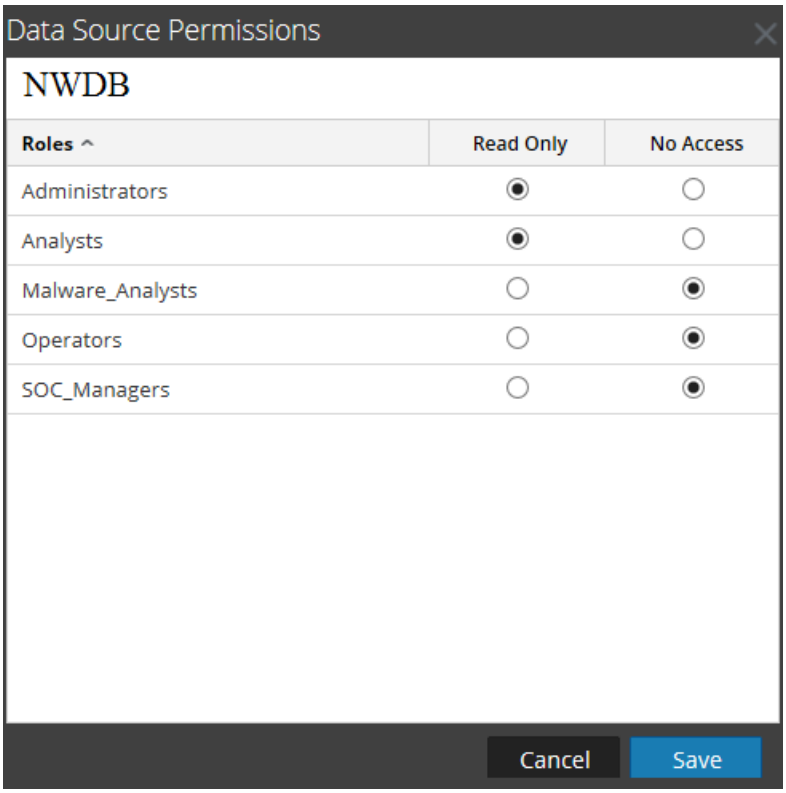
   La vue Configuration des services du Reporting Engine s'affiche.
4. Sélectionnez l'onglet **Sources**.

   La vue Configuration des services s'affiche avec l'onglet Sources Reporting Engine ouvert.



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 **Save**.

   Les autorisations requises sont configurées pour la source de données.

Étapes suivantes

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 *Reporting Guide*.

Configurer Workbench

Cette rubrique décrit les tâches générales permettant de configurer Security Analytics Workbench.

Conditions préalables

Assurez-vous d'avoir :

- Installé le service Security Analytics Workbench dans votre environnement réseau.
- Ajouté une collection au service Workbench.

Procédure

Reportez-vous au tableau suivant pour configurer Workbench :

Tâches	Référence
1. Ajouter un hôte RSA Archiver avec un service Reporting Engine.	Reportez-vous à l'**étape 1 : Ajouter ou mettre à jour des hôtes** dans le *Guide de mise en route de l'hôte et des services*.
2. Ajouter le service Workbench sur un Reporting Engine dans votre déploiement Security Analytics.	Reportez-vous à **Ajouter le service Workbench** ci-dessous.
3. Ajoutez Workbench comme source de données au Reporting Engine.	Reportez-vous à l'**Étape 3 : Ajouter Workbench comme source de données au Reporting Engine.** dans le *Guide de configuration d'Archiver*.

Ajouter le service Workbench

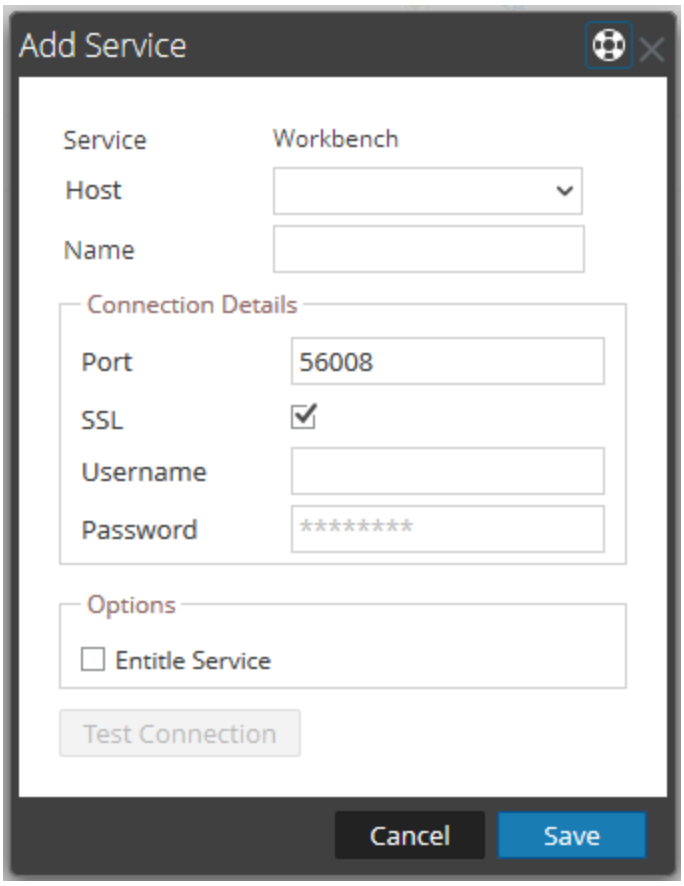
Le service Workbench est installé sur un Reporting Engine. Les données à restaurer doivent être restaurées sur le service Workbench.

Remarque : Vérifiez que vous avez ajouté un service Reporting Engine et que vous lui avez appliqué une licence.

Pour ajouter le service Workbench :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans le panneau Services, cliquez sur + > **Workbench**.

   La boîte de dialogue Ajouter un service s'affiche.



3. Fournissez les informations suivantes :

Champ	Description :
Hôte	Sélectionnez un hôte de Reporting Engine.
Name	Saisissez le nom du service.
Port	Le port par défaut est 50007

Champ	Description :
SSL	Sélectionnez **SSL** si vous souhaitez que Security Analytics communique avec le service via SSL. La sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL. **Remarque :** Si vous sélectionnez SSL, assurez-vous que SSL est activé dans le panneau Configuration système.
Username	Saisissez le nom d'utilisateur pour le service.
Mot de passe	Saisissez le mot de passe pour le service.

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

   Le service ajouté s'affiche désormais dans le panneau Services.

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

Références

Cette rubrique présente la vue Configuration des services pour le Reporting Engine qui dispose de paramètres spécifiques au Reporting Engine.

Vous pouvez spécifier les configurations suivantes pour le Reporting Engine :

- Configurations générales
- Sources
- Actions de sortie
- Gérer les logos

Remarque : Dans une version précédente de Security Analytics, la configuration des audits pour Reporting Engine était effectuée à l'aide de l'onglet Configuration des audits de la vue Configuration des services (**Administration > Services > Reporting Engine** > **Vue > Config > Configuration des audits**).

La fonction Configuration de l'audit est désormais disponible dans le panneau de configuration de l'audit global (**Administration > Système > Audit global**). Pour plus d'informations, reportez-vous à la rubrique **Configurer la consignation globale des audits** et **Panneau Configurations de consignation d'audit globale** dans le *Guide de configuration système*.

Topics

Reporting Engine : Onglet General

Cette rubrique présente la vue Configuration des services > onglet Général pour le Reporting Engine. L'onglet Général du service Reporting Engine figurant dans la vue Configuration des services permet de contrôler plusieurs paramètres en vue d'optimiser les performances d'un service et de spécifier les informations d'identification. Ces paramètres s'appliquent exclusivement au service Reporting Engine.

Procédure

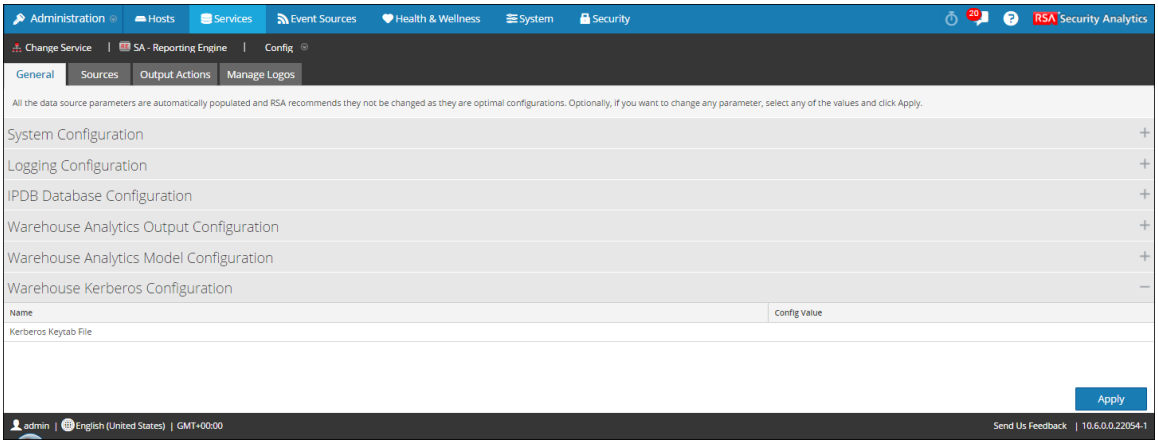
L'autorisation requise pour accéder à cette vue est **Gérer les services**.

Pour accéder à cette vue :

1. Dans le menu **Security Analytics**, cliquez sur **Administration** > **Services**.
2. Dans la grille **Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Configuration**.

   La vue Configuration des services s'ouvre sur l'onglet **Général** du Reporting Engine.

Un exemple de l'onglet Général du service IPDB Extractor s'affiche.



Fonctions

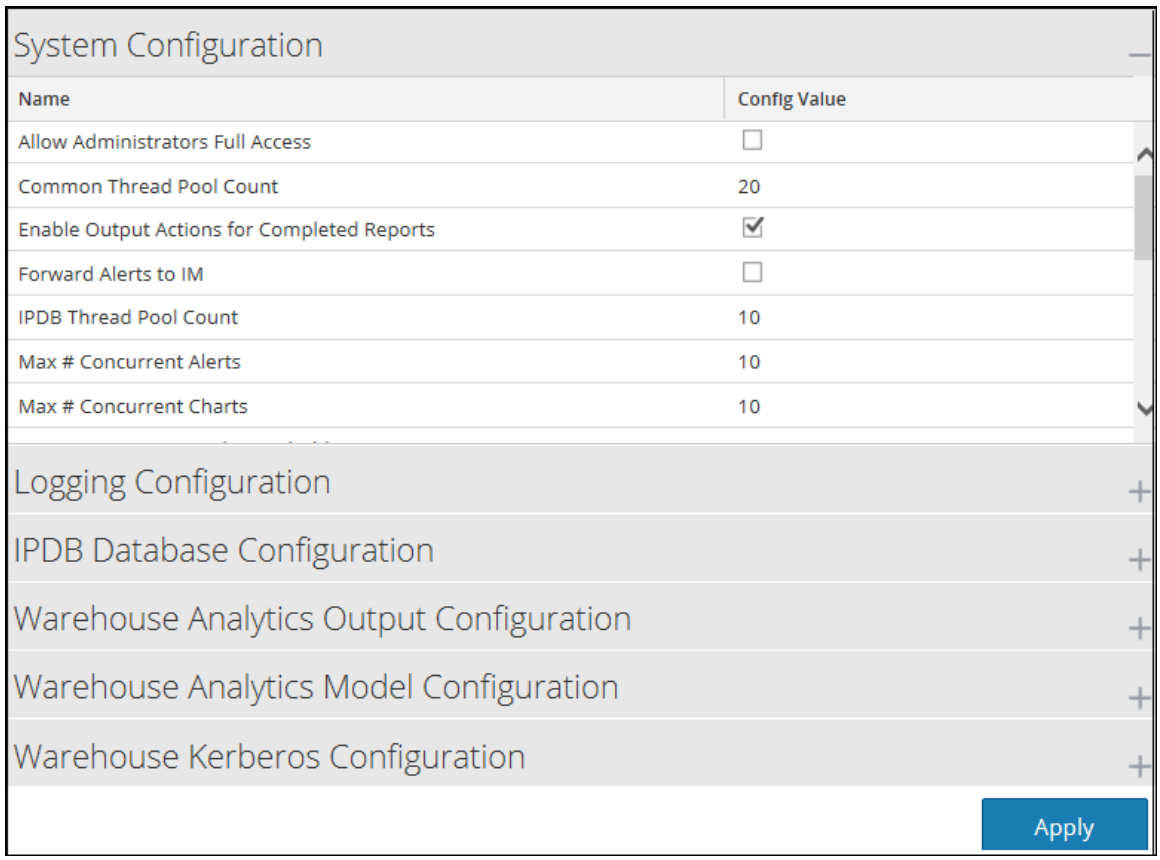
L'onglet **Général** du Reporting Engine contient six panneaux :

- Configuration système
- Configuration de la consignation
- Configuration de la base de données IPDB
- Configuration de sortie Warehouse Analytics
- Configuration de modèle Warehouse Analytics
- Configuration Warehouse Kerberos

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 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.

La capture d'écran 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.

Name	Valeur de configuration
Autoriser un accès complet aux administrateurs	Activez cette case à cocher si vous souhaitez accéder à tous les objets RE (rapports, règles, graphiques, plannings et listes) créés par d'autres utilisateurs (non administrateur). Par défaut, cette case n'est pas cochée. **Remarque :** Si vous désactivez cette case à cocher après l'avoir activée, l'intégralité des objets RE 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).
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 des alertes vers IM	Activez cette case à cocher pour transférer toutes les alertes vers Incident Management. Par défaut, cette case n'est pas cochée.
Nombre de pools de threads IPDB	Nombre de pools de threads alloués pour exécuter des tâches IPDB dans le Reporting Engine. Pour être valide, la valeur doit être un nombre entier (**10** par défaut).
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).

Name	Valeur de configuration
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).
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).
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).

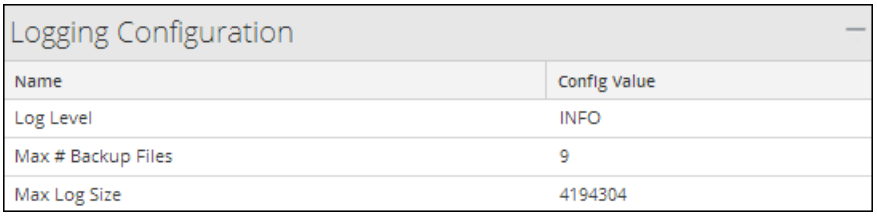
Name	Valeur de configuration
Nbre maximal de lignes agrégées NWDB	Nombre maximal de lignes renvoyées lorsque l'agrégation est utilisée dans la règle NWDB. Pour être valide, la valeur doit être un nombre entier (**1000** par défaut).
Délai d'expiration des requêtes NWDB	Délai (exprimé en secondes) au 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).

Name	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 système 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 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.

La capture d'écran 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.

Name	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).

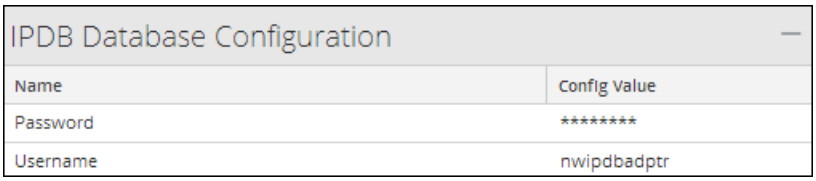
Name	Valeur de configuration
Taille de log max.	Taille maximale (en octets) du fichier log principal. Pour être valide, la valeur doit être un nombre entier (**4194304** par défaut).

Pour plus d'informations sur la consignation du Reporting Engine, voir Paramètres des fichiers log Reporting Engine.

Configuration de la base de données IPDB

Le panneau Configuration de la base de données IPDB permet de spécifier le mot de passe IPDB lors de la mise en œuvre d'IPDB sur ce Reporting Engine.

La capture d'écran suivante présente les champs qu'il est possible de renseigner dans le panneau Configuration de la base de données IPDB :



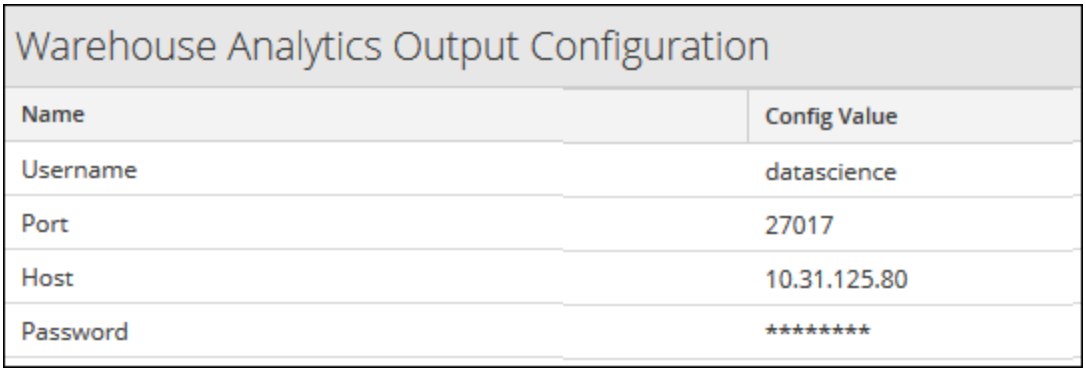
Le tableau suivant décrit les fonctions du panneau Configuration de la base de données IPDB.

Name	Valeur de configuration
Mot de passe	Mot de passe de l'utilisateur **nwipdbadptr**. RSA insère un mot de passe temporaire qu'il faut impérativement remplacer par le mot de passe IPDB réel lors de l'implémentation d'IPDB sur ce Reporting Engine.
Nom d'utilisateur	**nwipdbadptr** Vous ne pouvez pas modifier ce champ.

Configuration de sortie Warehouse Analytics

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

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



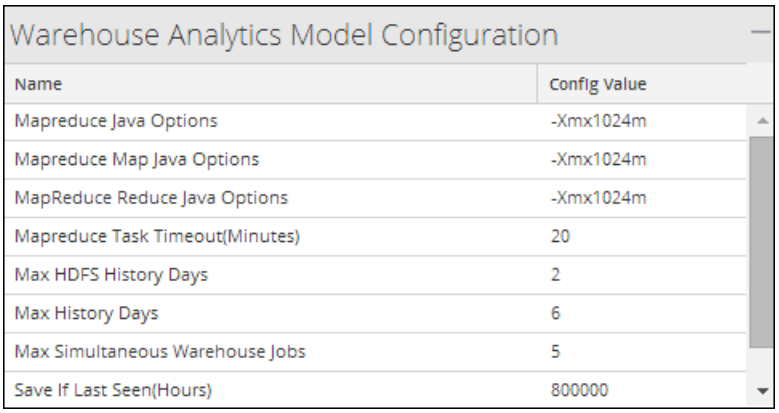
Le tableau suivant décrit les fonctions du panneau Configuration de sortie Warehouse Analytics.

Name	Valeur de configuration
Name	**Valeur de configuration**
Username	Nom de l'utilisateur de Warehouse Analytics.
Port	Port de la sortie MongoDB utilisée par Warehouse Analytics.
Hôte	Hôte de la sortie MongoDB 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 capture d'écran 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.

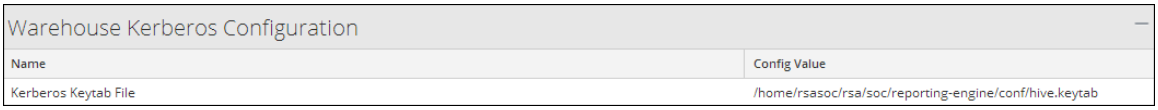
Name	Valeur de configuration
Options Java MapReduce	Paramètres JVM définissant la machine virtuelle Java enfant de suivi de tâches Hadoop MapReduce. Par défaut, la valeur est **-Xmx1024m**.
Options Java de mappage MapReduce	Contrôle les paramètres JVM pour mapper les tâches dans le cluster Hadoop. Par 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).
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).

Name	Valeur de configuration
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 capture d'écran 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.

Name	Valeur de configuration
Fichier de table de clés Kerberos	Chemin d'accès au fichier de table de clés Kerberos. Exemple : /home/rsasoc/rsa/soc/reporting-engine/conf/hive.keytab.

Onglet Gérer les logos du Reporting Engine

Cette rubrique présente les tâches de configuration de logo disponibles dans la vue Configuration des services > onglet Gérer les logos pour le Reporting Engine. L'onglet Gérer les logos de la vue de configuration des services permet de gérer les logos associés à Reporting Engine. Il 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 pouvez utiliser dans le 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, reportez-vous à la rubrique Sélectionner un logo.

Les formats d'images pris en charge sont :

- .jpg
- .png

- .gif

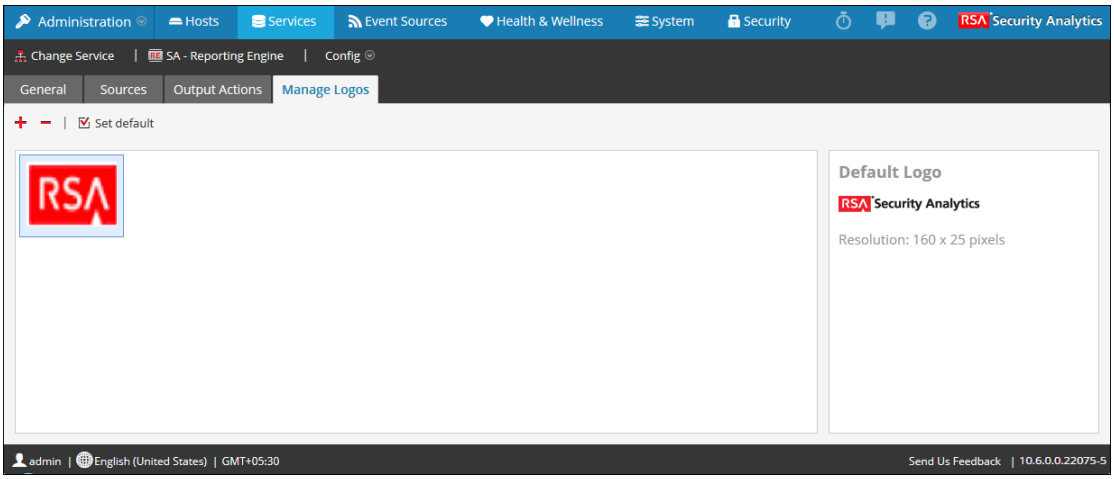
Remarque : Le logo à télécharger ne doit pas dépasser 500 Ko.

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

Pour accéder à cette vue :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans la **grille Services**, sélectionnez un service **Reporting Engine**.
3. Sélectionnez  > **Vue** > **Config**.
4. Sélectionnez l'onglet **Gérer les logos**.

   La **vue Configuration des services** s'ouvre sur l'onglet **Gérer les logos** de Reporting Engine.



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

Icône	Actions
	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 Security Analytics dans le panneau **Logo** de la vue Planifier un rapport. **Remarque :** Si aucun logo par défaut n'est sélectionné, le logo RSA s'affiche.

Actions de sortie du Reporting Engine

Cette rubrique présente les paramètres de configuration de services disponibles sous l'onglet Actions de sortie de la vue Configuration des services pour le Reporting Engine. L'action de sortie est l'action configurée pour un rapport ou l'exécution d'une alerte. Vous pouvez configurer l'action de sortie sous l'onglet Actions de sortie dans la vue Configuration des services de Reporting Engine. Cet onglet comprend les panneaux suivants :

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

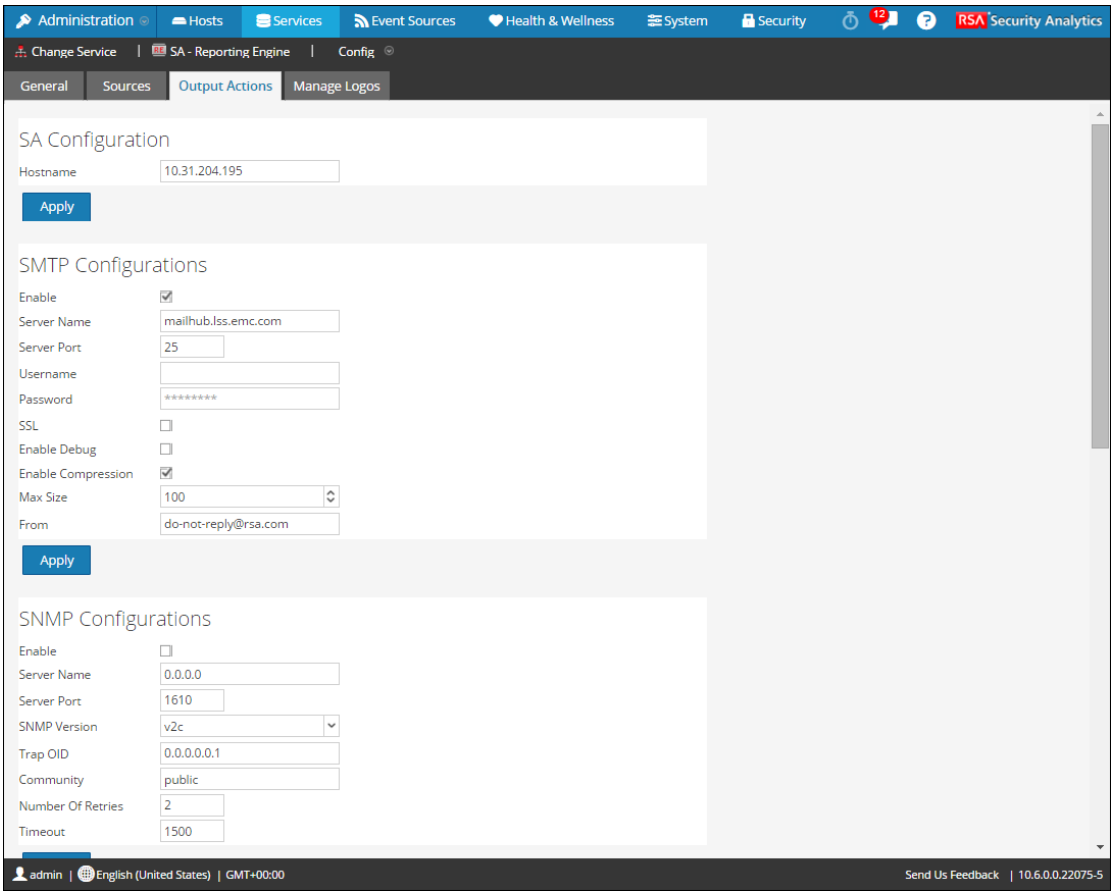
Chacune de ces actions de sortie répond à une finalité particulière. Par exemple, l'action de sortie Syslog est utilisée spécifiquement pour les alertes Reporting Engine, alors que les actions de sortie SFTP, URL et Partage réseau sont utilisées spécifiquement pour les rapports Reporting Engine.

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

Pour accéder à cette vue :

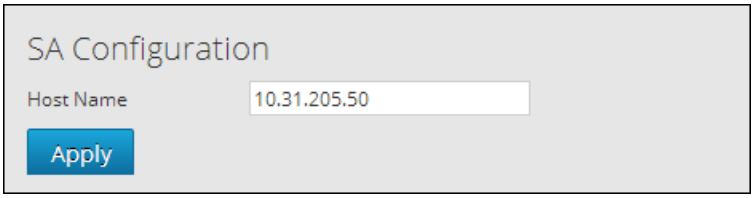
1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services.**
2. Dans la **grille Services**, sélectionnez un service **Reporting Engine**.
3. Click  > **Vue** > **Config**.
4. Cliquez sur l'onglet **Actions de sortie**.

   La vue **Configuration des services** s'ouvre sur l'onglet **Actions de sortie** du Reporting Engine.



Configuration SA

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



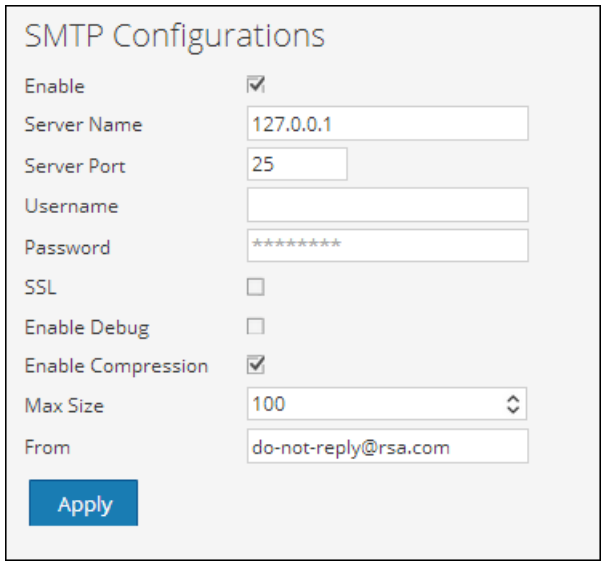
Les paramètres suivants identifient l'hôte Security Analytics associé à Reporting Engine.

Name	Valeur de configuration
Nom d'hôte	Adresse IP ou nom d'hôte du serveur Security Analytics. 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 Security Analytics à partir des rapports, alertes, etc. Security Analytics 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
Apply	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.

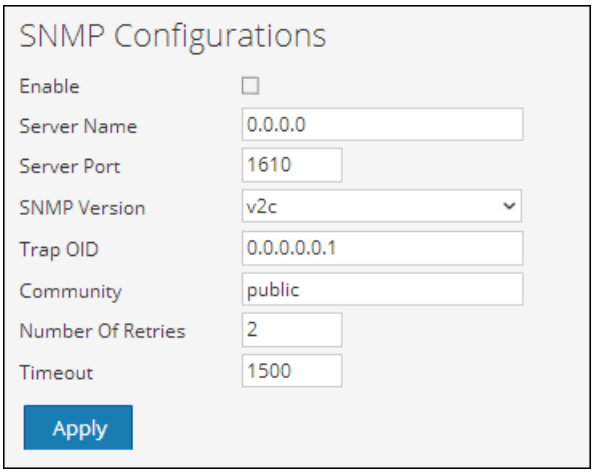
Name	Valeur de configuration
Activer	Activez cette case à cocher pour activer l'action de sortie SMTP des alertes et des rapports à partir de ce Reporting Engine. La valeur par défaut est Activer.
Nom du serveur	Spécifiez le nom d'hôte ou l'adresse IP du serveur sur lequel s'exécute le serveur SMTP cible. La valeur par défaut est **0.0.0.0**.
Port de serveur	Spécifiez le numéro de port du serveur SMTP. Valeur par défaut est**25**.
Username	Spécifiez le nom d'utilisateur de votre compte SMTP. Par défaut, la valeur n'est pas renseignée.
Mot de passe	Spécifiez le mot de passe de votre compte SMTP.
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	Cochez cette case pour activer le débogage. Valeur par défaut est 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 la 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 e-mail à partir de laquelle Security Analytics envoie tous les messages. La valeur par défaut est do-not-reply@rsa.com.

Name	Valeur de configuration
Apply	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.

Name	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**.
SNMP Version	Spécifiez le numéro de version du protocole SNMP que Security Analytics utilise pour envoyer des traps SNMP.

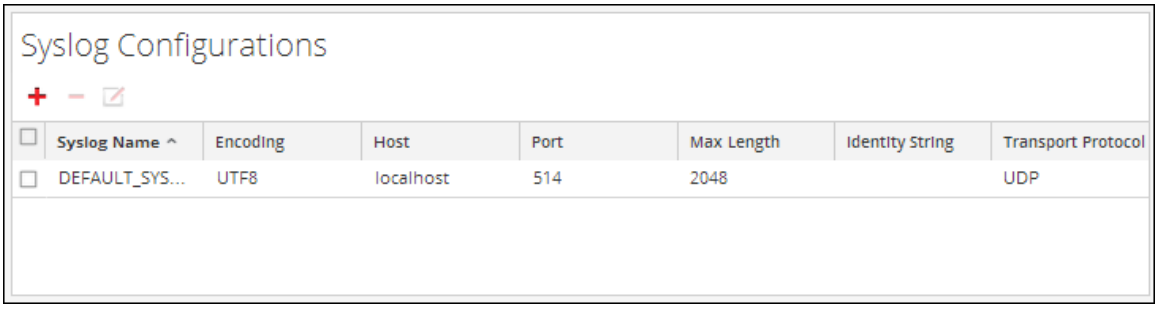
Name	Valeur de configuration
ID d'objet de trap	Spécifiez le numéro d'identification d'objet qui identifie le type de traps à envoyer. La valeur par défaut est **0.0.0.0.0.1**.
Communauté	Spécifiez le groupe SNMP auquel appartient Security Analytics. La valeur par défaut est **public**.
Nombre de tentatives	Spécifiez le nombre maximal de tentatives que Security Analytics effectue pour renvoyer le message d'alerte via SNMP. La valeur par défaut est **2**.
Timeout	Spécifiez le délai d'expiration de Security Analytics en secondes (arrêt des tentatives d'envoi d'alertes SNMP). La valeur par défaut est **1 500**.
Apply	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.

Remarque : Après la mise à niveau vers la version 10.4, la configuration Syslog des versions précédentes est migrée et enregistrée en tant que « DEFAULT_SYSLOG ».

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



Le tableau suivant répertorie les opérations de la section Configuration Syslog.

Opération	Description :
+	Créez une configuration Syslog.

Opération	Description :
	Supprimez une configuration Syslog.
	Modifiez une configuration Syslog.

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.

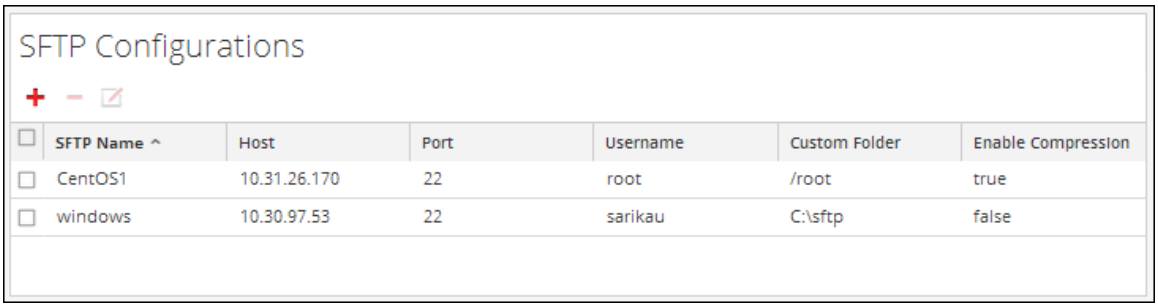
Name	Valeur de configuration
Nom Syslog	Nom de la configuration Syslog. **Remarque :** Vous ne pouvez pas créer de configuration Syslog avec un nom qui existe déjà dans la liste de configurations Syslog de Reporting Engine.
Encoding	Spécifiez l'encodage d'internationalisation des messages Syslog. La 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 Security Analytics insère au début de tous les messages d'alerte Syslog. Par défaut, la valeur n'est pas renseignée.
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.

Name	Valeur de configuration
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, 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.
Save	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.



Le tableau suivant répertorie les opérations de la section Configuration SFTP.

Opération	Description :
+	Créez une configuration SFTP.
−	Supprimez une configuration SFTP.
✎	Modifiez une configuration SFTP.

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.

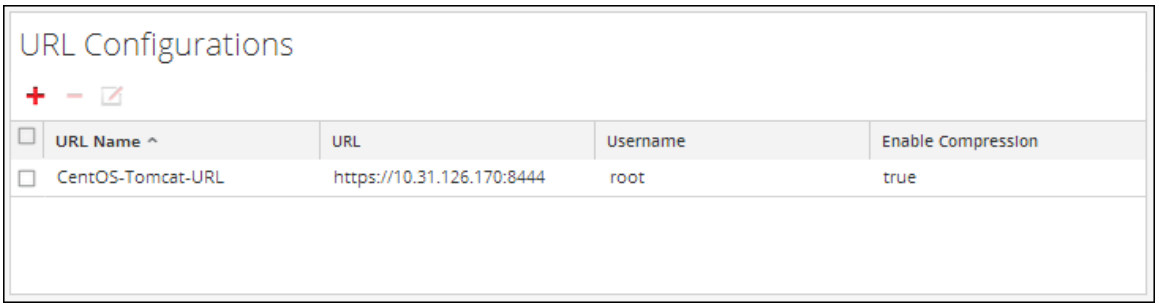
Name	Valeur de configuration
Nom SFTP	Nom de la configuration SFTP. **Remarque :** Vous ne pouvez pas créer de configuration SFTP avec un nom qui existe déjà dans la liste de configurations SFTP de Reporting Engine.
Hôte	Adresse IP ou nom d'hôte du serveur Reporting Engine associé au transfert de fichiers.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

Name	Valeur de configuration
Username	Spécifiez le nom d'utilisateur de la configuration SFTP.
Mot de passe	Spécifiez le mot de passe de la configuration SFTP.
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.



Le tableau suivant répertorie les opérations de la section Configuration URL.

Opération	Description :
+	Créez une configuration URL.
−	Supprimez une configuration URL.
✎	Modifiez une configuration URL.

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.

Name	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.
Username	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.

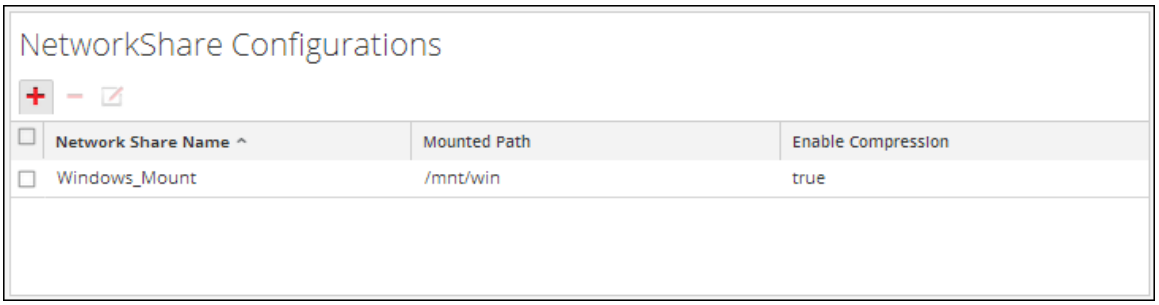
Name	Valeur de configuration
filename	Le nom du fichier.
filesize	Taille du fichier en octets.
filetype	Type de fichiers associé au fichier.
filechecksum	Nombre calculé à partir d'un fichier pour confirmer qu'il s'agit bien du fichier attendu, et qu'il a été téléchargé et stocké correctement.
hashingalgorithm	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.

Name	Valeur de configuration
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.

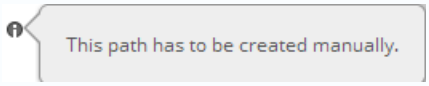
La figure suivante montre la configuration de partage réseau sous l'onglet Actions de sortie.



Le tableau suivant répertorie les opérations de la section Configuration de partage réseau.

Opération	Description :
+	Créez une configuration de partage réseau.
−	Supprimez une configuration de partage réseau.
✎	Modifiez une configuration de partage réseau.

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.

Name	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 pré-définie 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.

Onglet Sources du Reporting Engine

Cette rubrique présente les paramètres de configuration des services 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.

Toutes les procédures associées à cet onglet sont disponibles dans Configurer le Reporting Engine ou Procédures supplémentaires.

À propos des sources de données

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

- **Sources de données IPDB** - La base de données Internet Protocol Database (IPDB) contient à la fois des messages d'événements normalisés et bruts. Elle stocke tous les messages collectés dans un système de fichiers organisé par source d'événement (service), adresse IP, et indication temporelle (année/mois/jour) avec des fichiers d'index pour faciliter les recherches (rapport et requêtes).
- **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 Procédures supplémentaires.
- **Sources de données Warehouse** - Les sources de données Warehouse sont Pivotal et MapR.

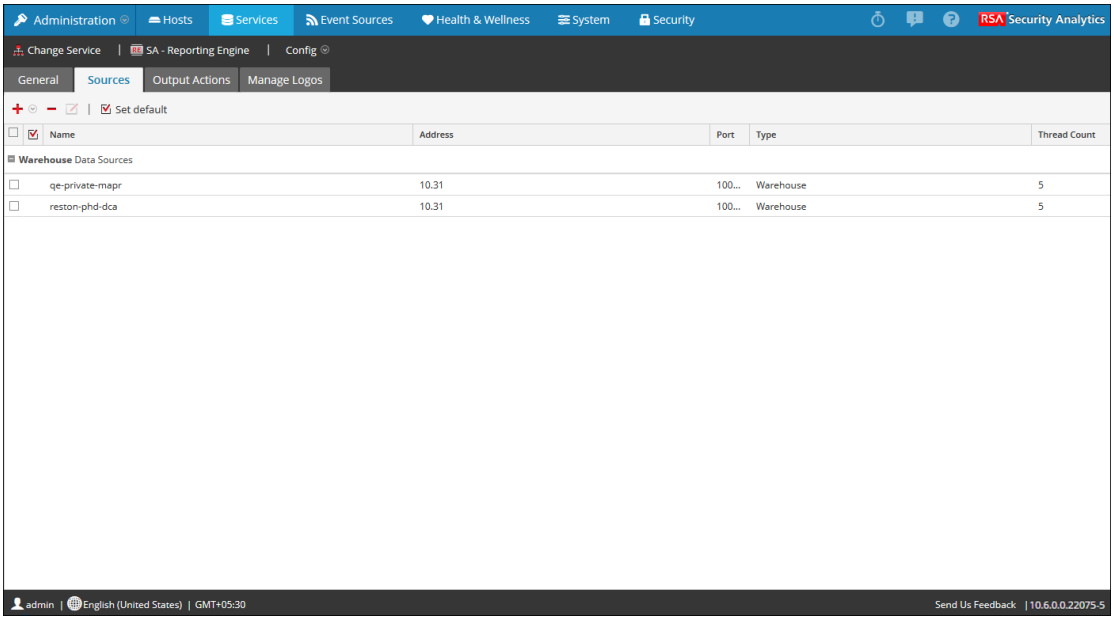
Si vous définissez une source comme source de données par défaut, Security Analytics utilise cette source lorsque vous créez des rapports et des alertes, sauf si vous choisissez de la remplacer par une autre des sources contenues dans cet onglet.

Remarque : Vous pouvez gérer le contrôle d'accès aux sources de données NWDB et Warehouse. Pour plus d'informations, voir le Procédures supplémentaires.

Pour accéder à cette vue :

1. Dans le **menu Security Analytics**, sélectionnez **Administration** > **Services**.
2. Dans la **grille Services**, sélectionnez un service **Reporting Engine**.
3. Cliquez sur  > **Vue** > **Config**.
4. Sélectionnez l'onglet **Sources**.

La **vue Configuration des services** s'affiche avec l'onglet **Sources** Reporting Engine ouvert.



Fonctions

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

Icône	Actions
	Ajoute de nouveaux services en tant que sources de données pour Reporting Engine. Pour ajouter un Warehouse comme source de données, reportez-vous à Ajouter Warehouse comme source de données au Reporting Engine. Ajouter des services existants ((Facultatif) Ajouter Archiver comme source de données au Reporting Engine, (Facultatif) Ajouter Workbench comme source de données au Reporting Engine, (Facultatif) Ajouter la collection comme source de données au Reporting Engine) en tant que sources de données pour Reporting Engine.
	Supprime les sources de données à partir d'un Reporting Engine.
	Configure les autorisations de source de données. Ce paramètre n'est activé que pour les sources de données NWDB et Warehouse. Pour plus d'informations, voir le Configurer les autorisations d'accès aux sources de données.

Icône	Actions
Set default	Définit les sources de données par défaut pour un Reporting Engine. Il s'agit de la source à laquelle Security Analytics applique les paramètres par défaut dans le champ **Source de données** des vues suivantes : • Vue Définition de règle. • Vue Créer/modifier une alerte.

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

- Catégorie Sources de données IPDB : Security Analytics affiche les sources de données du service IPDB Extractor.
- Catégorie Sources de données NWDB, Security Analytics affiche les sources de données NetWitness.
- Catégorie Sources de données Warehouse : Security Analytics 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.
Name	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. Pour la source de données IPDB, cette colonne est vide, la taille du pool de threads s'affiche à la place sous l'onglet **Général**, à l'aide du paramètre **Nombre de pools de threads IPDB**.

Paramètres des fichiers log Reporting Engine

Cette rubrique présente la procédure à suivre pour accéder aux fichiers log du Reporting Engine. Le Reporting Engine stocke les fichiers log suivants dans le répertoire **rsasoc/rsa/soc/reporting-engine/log** :

- Fichiers log actuels du fichier **reporting-engine.log**.
- Copies de sauvegarde des fichiers log précédents du fichier **reporting-engine.log.***.
- Tous les fichiers log de script UNIX dans les fichiers ayant la syntaxe suivante : **reporting-engine.sh_*timestamp*.log** (par exemple, **reporting-engine.sh_20120921.log**)

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

Le Reporting Engine ajoute les messages log, la sortie de log écrits par upstart daemon et les commandes utilisées pour démarrer le Reporting Engine dans le répertoire **/var/log/secure**.

Le fichier log upstart est un fichier log système. Seul l'utilisateur root peut donc le lire. Le Reporting Engine génère les fichiers log, conserve des copies de sauvegarde des fichiers log précédents, stocke les fichiers log de script UNIX et ajoute les fichiers log upstart à un autre répertoire.