RSA NETWITNESS® SUITE

Guía de configuración de Reporting Engine

para la versión 11.0

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de EMC, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por EMC.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

EMC considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

febrero 2018

Contenido

Cómo funciona Reporting Engine

NetWitness Reporting Engine es un servicio en el servidor de Admin de NetWitness, que facilita la extracción de datos de distintos orígenes de datos para generar informes de cumplimiento de normas y análisis. Reporting Engine almacena las definiciones de los gráficos, las reglas, los informes y las alertas que se usan para generar informes, gráficos y alertas.

La configuración de Reporting Engine incluye la configuración de orígenes de datos, definiciones de salidas o notificaciones y parámetros para mejorar el rendimiento de la extracción de datos y la generación de informes, gráficos y alertas.

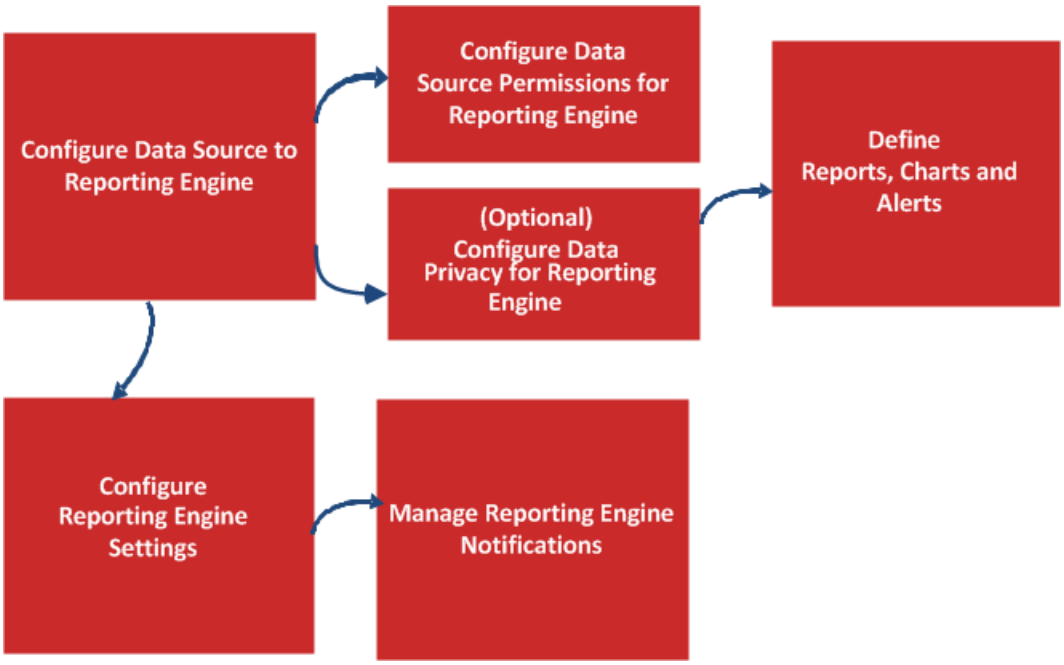
Cuando instala la NetWitness Suite, Reporting Engine se instala automáticamente como un servicio. Esto permite que los Informes, los gráficos y las Alertas se mantengan en RSA NetWitness Suite y que estén disponibles para ver y descargar los informes con formato PDF o CSV, descargar gráficos como archivos PDF y que se agreguen como dashlets.

Para que Reporting Engine ejecute informes y alertas según los datos obtenidos de un origen de datos, debe asociar uno o varios orígenes de datos a un Reporting Engine. Existen tres tipos de orígenes de datos:

- Orígenes de datos de NWDB: los orígenes de datos de NetWitness Database (NWDB) son Decoders, Log Decoders, Brokers, Concentrators, Archiver y Collection. Se admite la generación de informes, alertas y gráficos en los orígenes de datos NWDB en Reporting Engine.
- Orígenes de datos de Warehouse: los orígenes de datos de Warehouse son Horton Works y MapR, que recopila información de Warehouse Connector y genera informes y alertas. Este origen de datos genera informes solamente.
- Orígenes de datos de Respond: Respond se usa para generar informes sobre alertas e incidentes. Este origen de datos genera informes solamente.

Flujo de trabajo

El flujo de trabajo siguiente muestra una descripción general de la configuración de Reporting Engine que permite que el usuario genere Informes, gráficos y Alertas.


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

Configurar Reporting Engine

En la instalación del servidor de NetWitness, el servicio Reporting Engine está disponible automáticamente y algunos parámetros se rellenan previamente con valores predeterminados para alcanzar resultados óptimos.

Debe asegurarse de que los orígenes de datos se implementen y configuren en la NetWitness Suite. Para obtener más información, consulte el tema "Cuadro de diálogo Agregar servicio o Editar servicio" en la *Guía de configuración de hosts y servicios*.

Es posible realizar las siguientes tareas:

- Compruebe Live para obtener el contenido más reciente del origen de datos e implementarlo periódicamente. (Para obtener más información, consulte el tema "Administrar de recursos de Live" en la *Guía de servicios de Live*).
- (Opcional) Agregar espacio adicional para informes grandes.

Configurar los orígenes de datos

Debe configurar los orígenes de datos, como NWDB, Warehouse o Respond. Puede configurar NWDB, Warehouse y Respond para generar Informes, gráficos y Alertas, respectivamente. De manera opcional, también puede configurar los orígenes de datos de Archiver, Collection y Workbench.

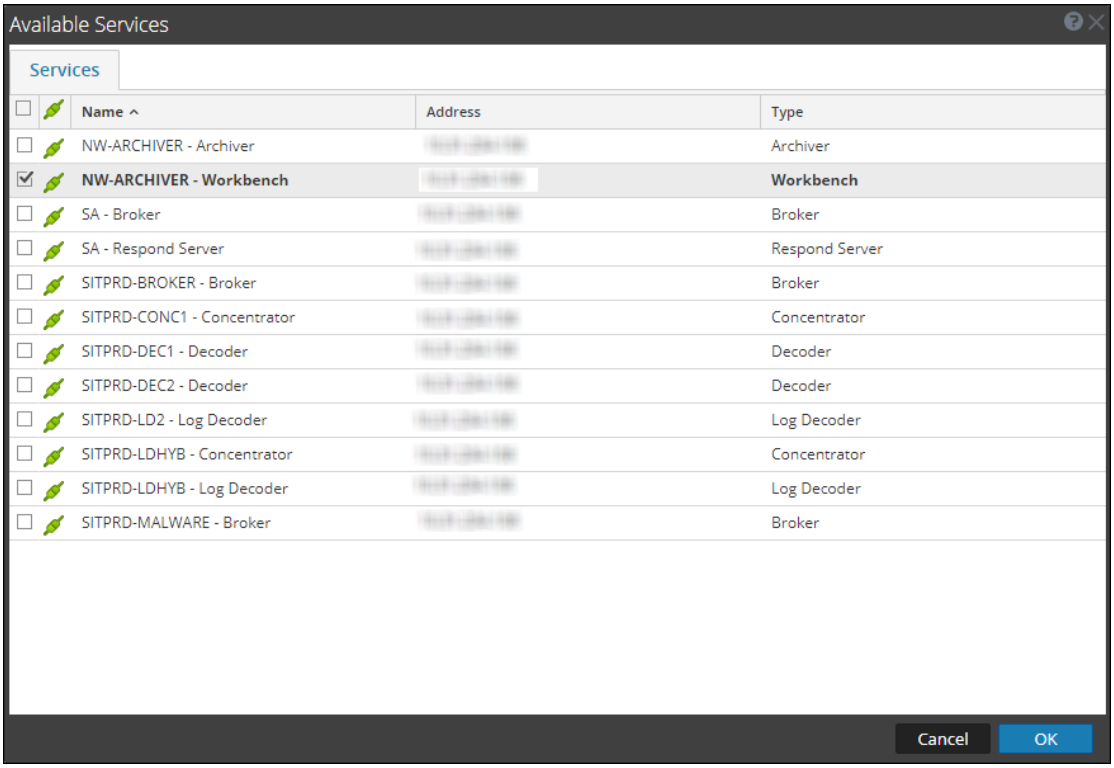
Configurar un origen de datos NWDB

Para agregar un origen de datos NWDB:

1. Vaya a **ADMIN** > **Servicios**.
2. En **Servicios**, seleccione el servicio **Reporting Engine**.
3. Haga clic en > **Ver** > **Configuración**

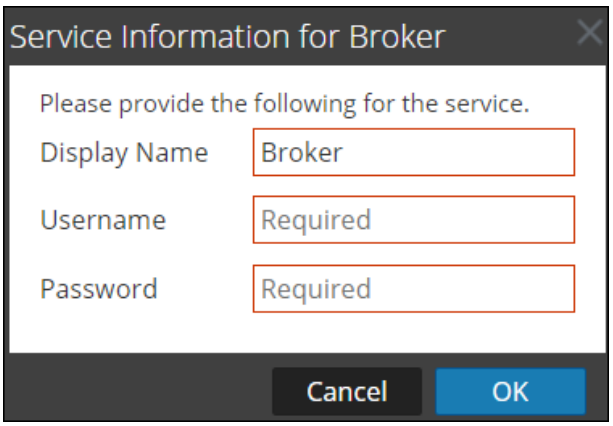
   Se muestra la vista Configuración de servicios de Reporting Engine.
4. En la pestaña **Orígenes**, haga clic en > **Servicios disponibles**.

   Se muestra el cuadro de diálogo **Servicios disponibles**.

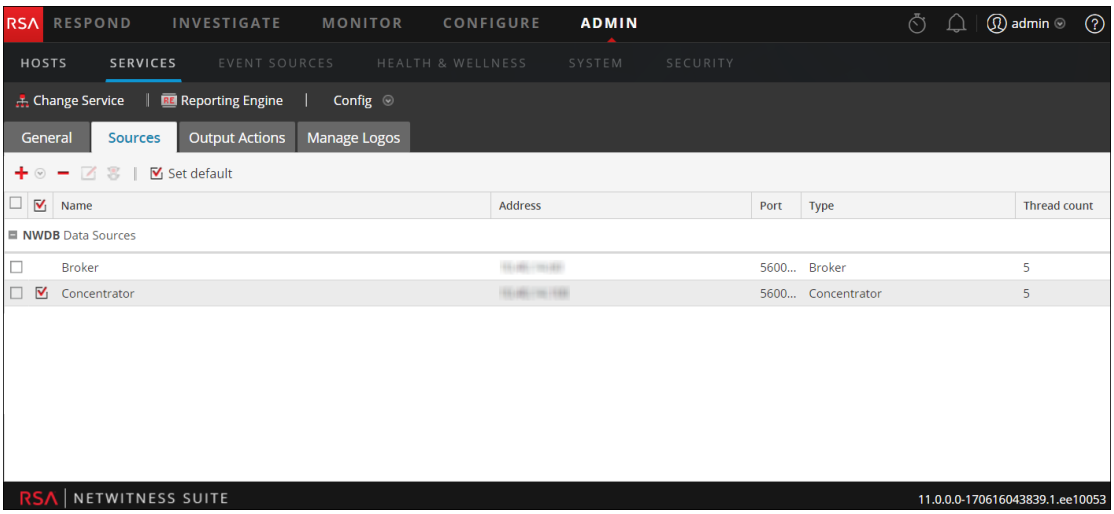


5. Seleccione un servicio NWDB que desee agregar y haga clic en **Aceptar**.

6. En el cuadro de diálogo Información de servicio de Broker, ingrese la información del servicio y haga clic en **Aceptar**. En este ejemplo, estamos agregando un servicio Broker.



7. Cuando se agrega correctamente, el servicio se muestra en la pestaña Orígenes.



Nota: Los servicios en los cuales está activado el modelo de confianza se deben agregar individualmente. Se solicita que proporcione un nombre de usuario y una contraseña para el servicio seleccionado.

Configurar un origen de datos Warehouse

Puede agregar el origen de datos de Warehouse a Reporting Engine, de modo que pueda extraer los datos de los servicios requeridos, almacenarlos en MapR o en Horton Works y generar Informes y Alertas. El procedimiento para configurar Warehouse como origen de datos es diferente. Para extraer datos de un origen de datos Warehouse, primero debe configurarlo mediante el siguiente procedimiento.

Nota: Warehouse Analytics no es compatible con NetWitness Suite versión 11.0.

Requisito previo

Asegúrese de:

- Agregar un origen de datos de Warehouse en Reporting Engine
- Establecer el origen de datos de Warehouse como el origen predeterminado
- Que el servidor de Hive esté en ejecución en todos los nodos de Warehouse. Use el siguiente comando para comprobar el estado del servidor de HIVE:

  ```
  status hive2 (MapR deployments)
   service hive-server2 status (Horton Works deployments)
  ```
- Que Warehouse Connector esté configurado para escribir datos en implementaciones de Warehouse.
- Si la autenticación Kerberos está habilitada para HiveServer2, asegúrese de que el archivo keytab se haya copiado al directorio `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/` en el host de Reporting Engine.

  Nota: El usuario **rsasoc** debe tener permisos de lectura para el archivo keytab. Para obtener más información, consulte Configurar permisos de orígenes de datos.

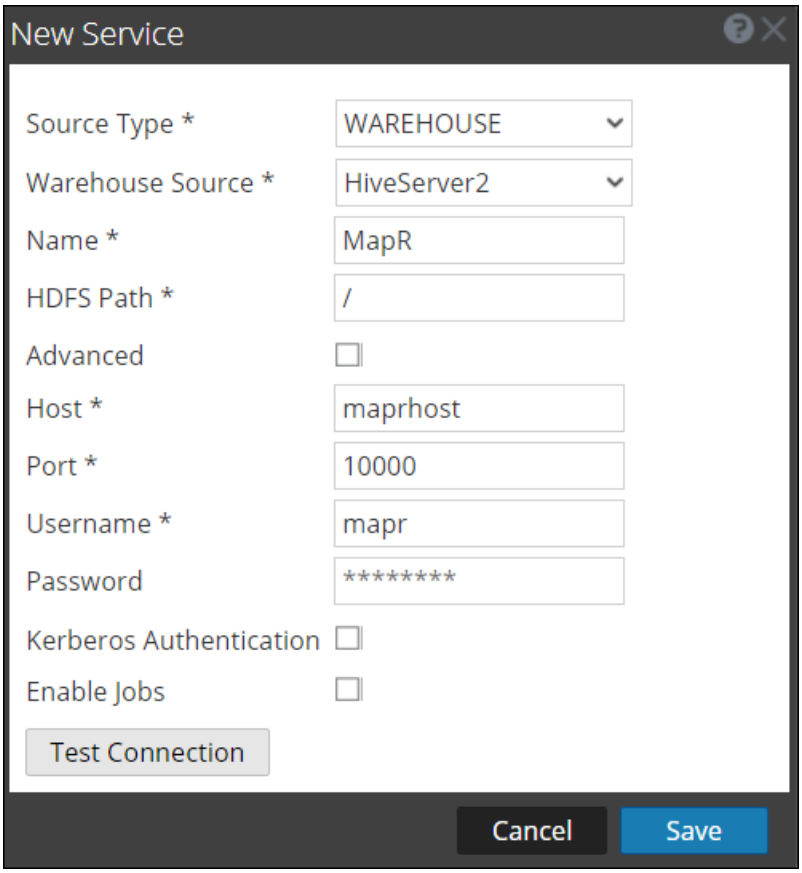
  Además, asegúrese de actualizar la ubicación del archivo keytab en el parámetro **Archivo keytab de Kerberos** de la vista Configuración del servicio de Reporting Engine. Consulte la Pestaña General para obtener más información.

Para agregar el origen de datos de Warehouse para MapR:

1. Vaya a **Admin** > **Servicios**.
2. En la lista **Servicios**, seleccione el servicio **Reporting Engine**.
3. Haga clic en  > **Ver** > **Configuración**.
4. Haga clic en la pestaña **Orígenes**.

   La **vista Configuración del servicio** se muestra con la pestaña **Orígenes** de Reporting Engine abierta.
5. Haga clic en  y seleccione **Nuevo servicio**.

   Se muestra el cuadro de diálogo Nuevo servicio.



6. En el menú desplegable **Tipo de fuente**, seleccione **WAREHOUSE**.
7. En el menú desplegable **Origen de Warehouse**, seleccione el origen de datos de Warehouse.
8. En el campo **Nombre**, ingrese el nombre de host del origen de datos de Warehouse.
9. En el campo **Ruta de HDFS**, ingrese la ruta raíz de HDFS en la cual Warehouse Connector escribe los datos.

   Por ejemplo:
   Si **/saw** es el punto de montaje local para HDFS que configuró durante el montaje de NFS en el dispositivo. Y si instaló el servicio Warehouse Connector para escritura en SAW. Para obtener más información, consulte el tema “Montar Warehouse en Warehouse Connector” de la *Guía de configuración de RSA NetWitness Warehouse (MapR)*.

   Y si creó un directorio denominado **Ionsaw01** bajo **/saw** y proporcionó la ruta de montaje local correspondiente, como **/saw/Ionsaw01**, la ruta raíz de HDFS correspondiente sería **/Ionsaw01**.

   El punto de montaje **/saw** implica a /como la ruta raíz para HDFS. Warehouse Connector escribe los datos / **Ionsaw01** en HDFS. Si no hay datos disponibles en esta ruta, se muestra el siguiente error:

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

Asegúrese de que **/lonsaw01/rsasoc/v1/sessions/meta** contenga archivos avro de los metadatos antes de ejecutar la conexión de prueba.

10. Seleccione la casilla de verificación **Opciones avanzadas** para usar ajustes avanzados y complete la **Dirección URL de base de datos** con la dirección URL de JDBC completa con el fin de conectar HiveServer2.

    Por ejemplo:
    Si Kerberos está habilitado en HIVE, la dirección URL de JDBC será:

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

    Si SSL está habilitado en Hive, la dirección URL de JDBC será:

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

    Para obtener más información sobre los clientes del servidor HIVE, consulte https://cwiki.apache.org/confluence/display/Hive/HiveServer2+Clients.

11. Si no utiliza los ajustes avanzados, ingrese los valores para el **Host** y el **Puerto**.

    - En el campo **Host**, ingrese la dirección IP del host en el cual está alojado HiveServer2.

      Nota: Puede usar la dirección IP virtual de Mapr solo si HiveServer2 se ejecuta en todos los nodos del clúster.

    - En el campo **Puerto**, ingrese el puerto de HiveServer2 del origen de datos de Warehouse. De manera predeterminada, el número de puerto es **10000**.

12. En los campos **Nombre de usuario** y **Contraseña**, ingrese las credenciales de JDBC que se usan para acceder a HiveServer2.

    Nota: también puede utilizar el modo de autenticación LDAP mediante Active Directory. Para obtener instrucciones sobre la habilitación del modo de autenticación LDAP, consulte Habilitar la autenticación LDAP.

13. Para ejecutar informes de Warehouse Analytics, consulte Activar trabajos en Configuración de orígenes de datos para Reporting.

14. Habilite la autenticación Kerberos: consulte Habilitar la autenticación Kerberos en Configuración de orígenes de datos para Reporting.

15. Si desea configurar el origen de datos de Warehouse que agregó como el origen predeterminado para Reporting Engine, selecciónelo y haga clic en 

.

Para agregar el origen de datos de Warehouse para Horton Works (HDP):

Nota: Asegúrese de descargar el archivo `hive-jdbc-1.2.1-with-full-dependencies.jar`. Este jar contiene el archivo del driver de HIVE 1.2.1 que se conecta a Reporting Engine para Hiveserver2 Hive 1.2.1 desde RSA Link (https://community.rsa.com/docs/DOC-67251).

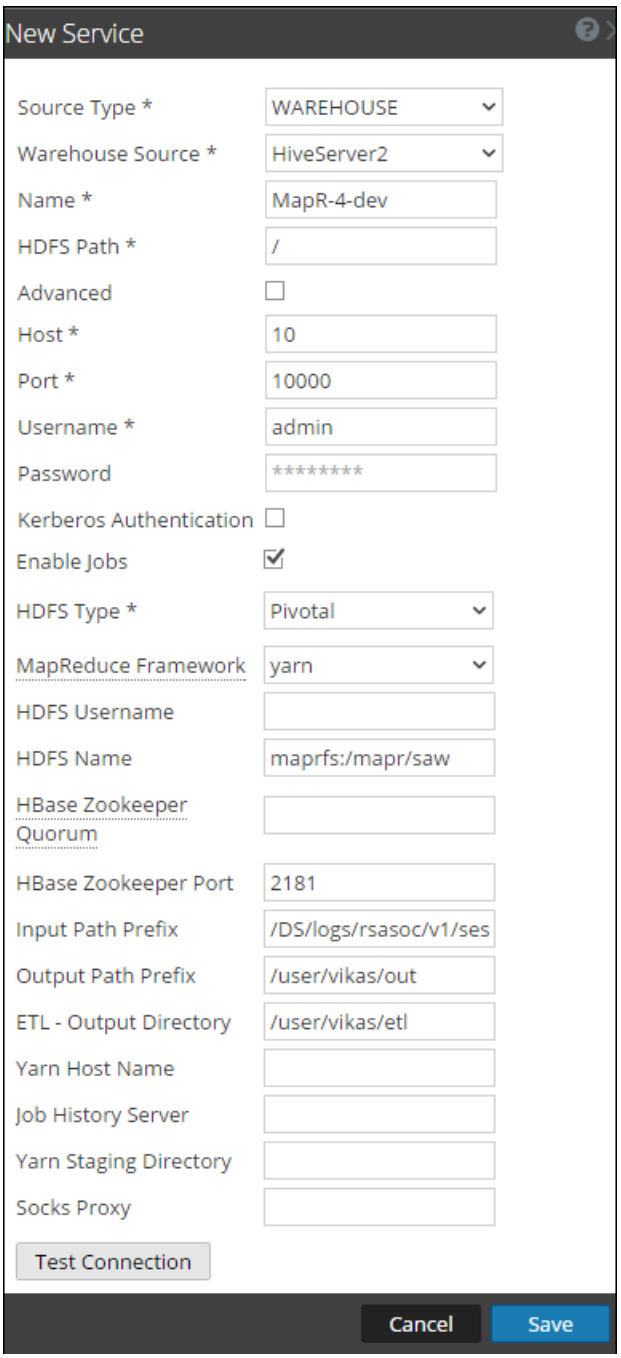
1. Acceda mediante el protocolo SSH al servidor de NetWitness Suite.
2. En la carpeta `/opt/rsa/soc/reporting-engine/plugins/`, respalde el siguiente archivo jar:
   `hive-jdbc-0.12.0-with-full-dependencies.jar` o `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
3. Quite el siguiente archivo jar:
   `hive-jdbc-0.12.0-with-full-dependencies.jar` o `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
4. En la carpeta /opt/rsa/soc/reporting-engine/plugins, copie el siguiente archivo jar mediante WinSCP:
   `hive-jdbc-1.2.1-with-full-dependencies.jar`
5. Reinicie el servicio Reporting Engine.
6. Inicie sesión en la UI NetWitness Suite.
7. Seleccione el servicio **Reporting Engine** y elija > **Ver** > **Explorar**.
8. En **hiveConfig**, configure el **parámetro EnableSmallSplitBasedSchemaLiteralCreation** en **verdadero**.

Activar trabajos

Nota: Warehouse Analytics no es compatible con NetWitness Suite versión 11.0.

Para ejecutar informes de Warehouse Analytics, realice este procedimiento.

1. Seleccione la casilla de verificación **Activar trabajos**.



Nota: No seleccione Pivotal en el campo HDFS, porque no es compatible en esta versión.

2. Ingrese los siguientes detalles:

a. Seleccione el tipo de HDFS en el menú desplegable **Tipo de HDFS**.

- Si selecciona el tipo Horton Works HDFS, ingrese la siguiente información:

Campo	Descripción
Nombre de usuario de HDFS	Ingrese el nombre de usuario que debe presentar Reporting Engine cuando se conecte a Horton Works. Para clústeres de Horton Works DCA estándar, este debe ser “gpadmin”.
Nombre de HDFS	Ingrese la dirección URL para acceder a HDFS. Por ejemplo, hdfs://hdm1.gphd.local:8020.
Quórum HBase Zookeeper	Ingrese la lista de nombres de host separados por comas en los cuales se ejecutan los servidores de ZooKeeper.
Puerto HBase Zookeeper	Ingrese el número de puerto para los servidores de ZooKeeper. El puerto predeterminado es 2181.
Prefijo de ruta de entrada	Ingrese la ruta de salida de Warehouse Connector (`/sftp/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) hasta el directorio year. Por ejemplo, `/sftp/rsasoc/v1/sessions/data/`.
Prefijo de ruta de salida	Ingrese la ubicación donde se almacenan los resultados de los trabajos de ciencia de datos en HDFS.
Nombre de host de Yarn	Ingrese el nombre de host de yarn resource-manager de Hadoop en el clúster de DCA. Por ejemplo, **hdm3.gphd.local**.

Campo	Descripción
Servidor de historial de trabajos	Ingrese la dirección de job-history-server de Hadoop en el clúster de DCA. Por ejemplo, **hdm3.gphd.local:10020**.
Directorio de staging de Yarn	Ingrese el directorio de almacenamiento provisional para YARN en el clúster de DCA. Por ejemplo, `/user`.
Proxy de Socks	Si se usa el clúster de DCA estándar, la mayoría de los servicios de Hadoop se ejecutarán en una red privada local a la cual no se puede acceder desde Reporting Engine. A continuación, debe ejecutar un proxy SOCKS en el clúster de DCA y permitir el acceso desde fuera del clúster. Por ejemplo, **mdw.netwitness.local:1080**.

- Si selecciona el tipo de HDFS MapR, ingrese la siguiente información:

Campo	Descripción
Nombre de host de MapR	El usuario puede completar la dirección IP pública de cualquiera de los hosts de Warehouse de MapR.
Usuario de host de MapR	Ingrese un nombre de usuario de UNIX en el host especificado que tenga acceso para ejecutar trabajos map-reduce en el clúster. El valor predeterminado es “mapr”.
Contraseña de host de MapR	(Opcional) Para configurar la autenticación sin contraseña, copie la clave pública del usuario “rsasoc” desde **/home/rsasoc/.ssh/id_rsa.pub** al archivo “authorized_keys” del host de Warehouse que se encuentra en **/home/mapr/.ssh/authorized_keys**, en el supuesto de que “mapr” es el usuario de UNIX remoto.

Campo	Descripción
Directorio de trabajo de host de MapR	Ingrese una ruta para la cual el usuario de UNIX especificado (por ejemplo, “mapr”) tenga acceso de escritura. **Nota:** Reporting Engine usa el directorio de trabajo para realizar una copia remota de los archivos jar de Warehouse Analytics y dar inicio a los trabajos desde el nombre de host dado. No debe utilizar “/tmp” para evitar llenar el espacio temporal del sistema.Reporting Engine administrará el directorio de trabajo dado de manera remota.
Nombre de HDFS	Ingrese la dirección URL para acceder a HDFS. Por ejemplo, para acceder a un clúster específico, maprfs:/mapr/<cluster-name>.
Puerto HBase Zookeeper	Ingrese el número de puerto para los servidores de ZooKeeper. El puerto predeterminado es 5181.
Prefijo de ruta de entrada	Ingrese la ruta de salida (`/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) hasta el directorio year. Por ejemplo, `/rsasoc/v1/sessions/data/`.
Nombre de archivo de entrada	Ingrese el filtro del nombre de archivo para los archivos avro. Por ejemplo, **sessions-warehouseconnector**.
Prefijo de ruta de salida	Ingrese la ubicación donde se almacenan los resultados de los trabajos de ciencia de datos en HDFS.

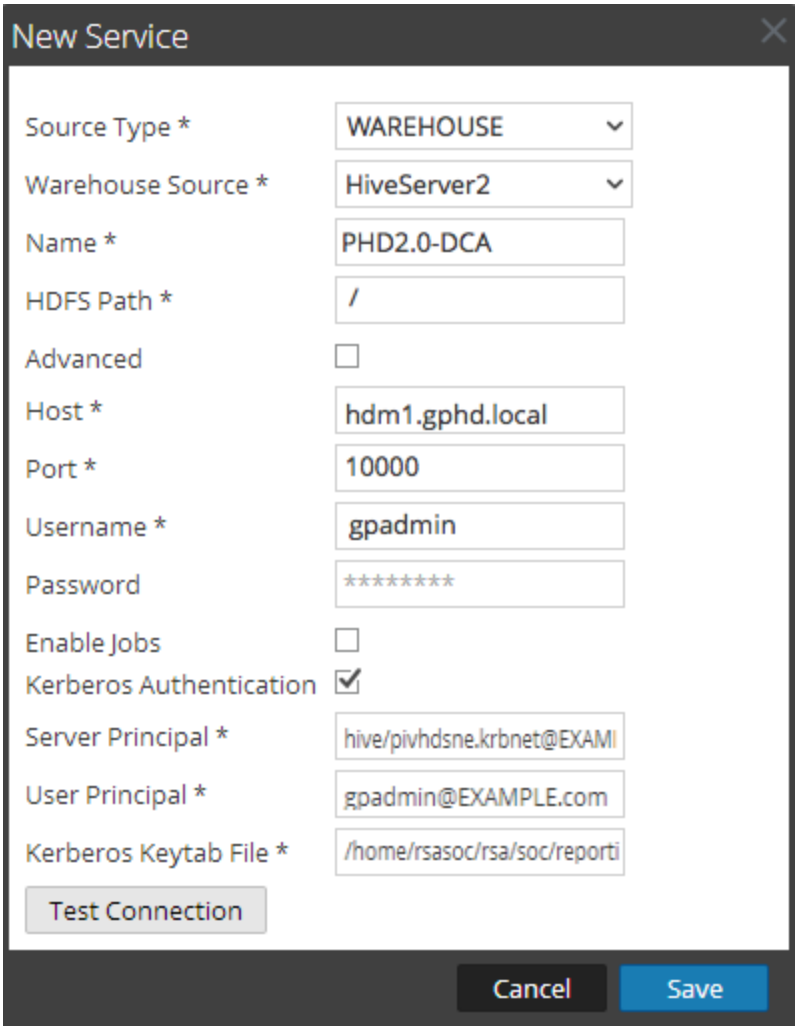
b. Seleccione la infraestructura de MapReduce según el tipo de HDFS.

Nota: Para MapR como tipo de HDFS, seleccione Clásica como la infraestructura de MapReduce. Para Horton Works como tipo de HDFS, seleccione Yarn como la infraestructura de MapReduce.

A continuación, habilite la autenticación Kerberos.

Habilitar la autenticación Kerberos

1. Seleccione la casilla de verificación **Autenticación Kerberos** si Warehouse tiene un servidor Hive activado para Kerberos.



2. Complete los campos de la siguiente manera:

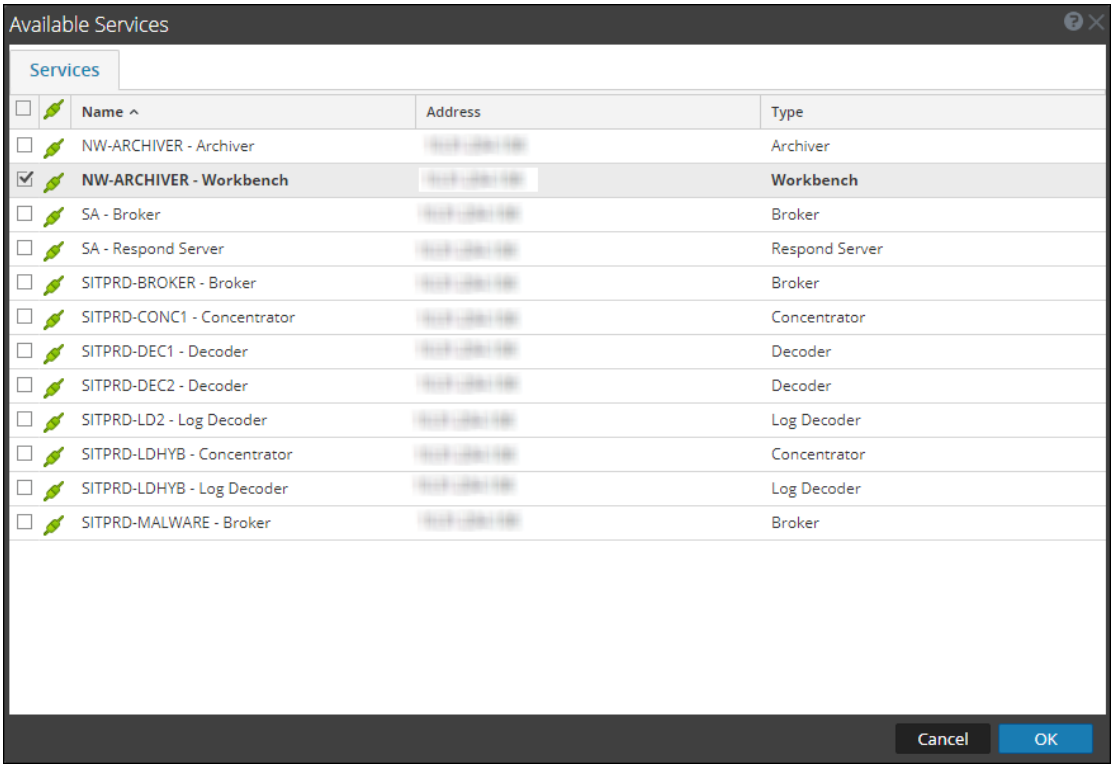
Campo	Descripción
Principal del servidor	Ingrese el principio que usa el servidor Hive para autenticarse en el servidor del centro de distribución de claves (KDC) de Kerberos.
Principal de usuario	Ingrese el principio que usa el cliente de JDBC de HIVE para autenticarse en el servidor de KDC con el fin de conectarse al servidor de Hive. Por ejemplo, **gpadmin@EXAMPLE.COM**.

Campo	Descripción
Archivo keytab de Kerberos	Vea la ubicación del archivo keytab de Kerberos configurada en el panel Configuración de HIVE en la pestaña General de Reporting Engine. **Nota:** Reporting Engine solo es compatible con los orígenes de datos configurados con las mismas credenciales de Kerberos, como el principal del usuario y el archivo keytab.

3. Haga clic en **Probar conexión** para probar la conexión con los valores ingresados.
4. Haga clic en **Guardar**.

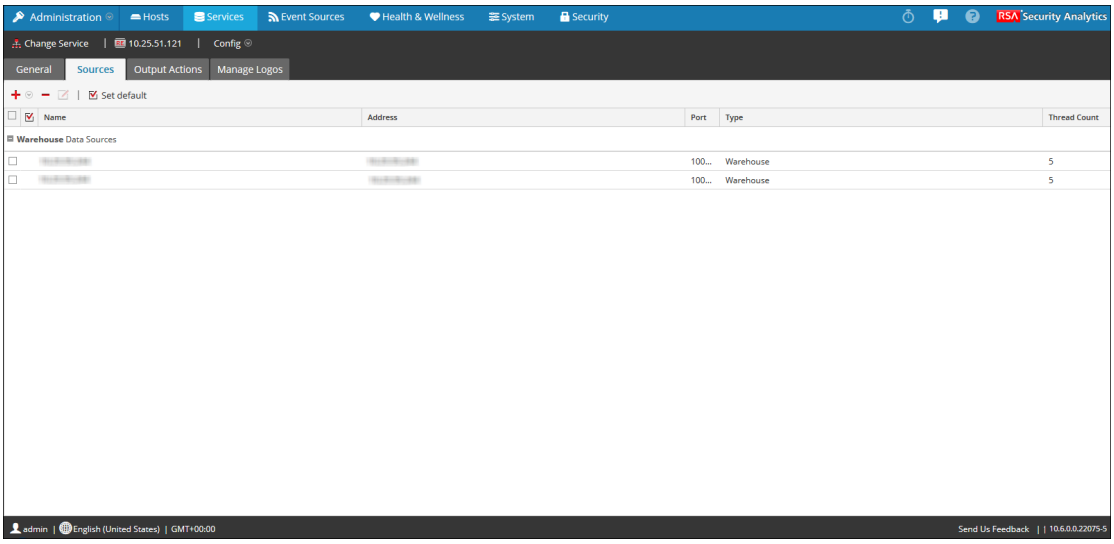
   El origen de datos de Warehouse agregado se muestra en la pestaña Orígenes de Reporting Engine.
5. Haga clic en + > **Servicios disponibles**.

   Se muestra el cuadro de diálogo Servicios disponibles.



6. En el cuadro de diálogo Servicios disponibles, seleccione el servicio que desea agregar como origen de datos en Reporting Engine y haga clic en **Aceptar**.

   NetWitness Suite agrega esto como un origen de datos disponible para informes y alertas relacionados con este Reporting Engine.



Nota: Este paso es importante solo para un modelo no confiable.

Definir un origen de datos como el origen predeterminado

Para definir un origen de datos como el origen de datos predeterminado cuando cree informes y alertas:

1. Vaya a **Dashboard** > **Administración** > **Servicios**.
2. En la lista **Servicios**, seleccione un servicio **Reporting Engine**.
3. Seleccione > **Ver**> **Configuración**.

   Se muestra la vista Configuración de servicios de Reporting Engine.
4. Seleccione la pestaña **Orígenes**.

   Se muestra la **vista Configuración de servicios** con la pestaña Orígenes de Reporting Engine abierta.
5. Seleccione el origen que desea establecer como predeterminado (por ejemplo, Broker).
6. Haga clic en la casilla de verificación **Establecer valor predeterminado**.

   NetWitness Suite configura este origen de datos como predeterminado cuando crea informes y alertas relacionados con este Reporting Engine.

(Opcional) Agregar Workbench como un origen de datos

Debe realizar las siguientes configuraciones de Workbench para que pueda usar los datos del origen de datos de Workbench para generar Informes y Alertas. En este tema se proporcionan instrucciones para agregar el servicio Workbench como un origen de datos en Reporting Engine con el fin de generar un informe de los datos que recopila Workbench.

Requisitos previos

Asegúrese de haber:

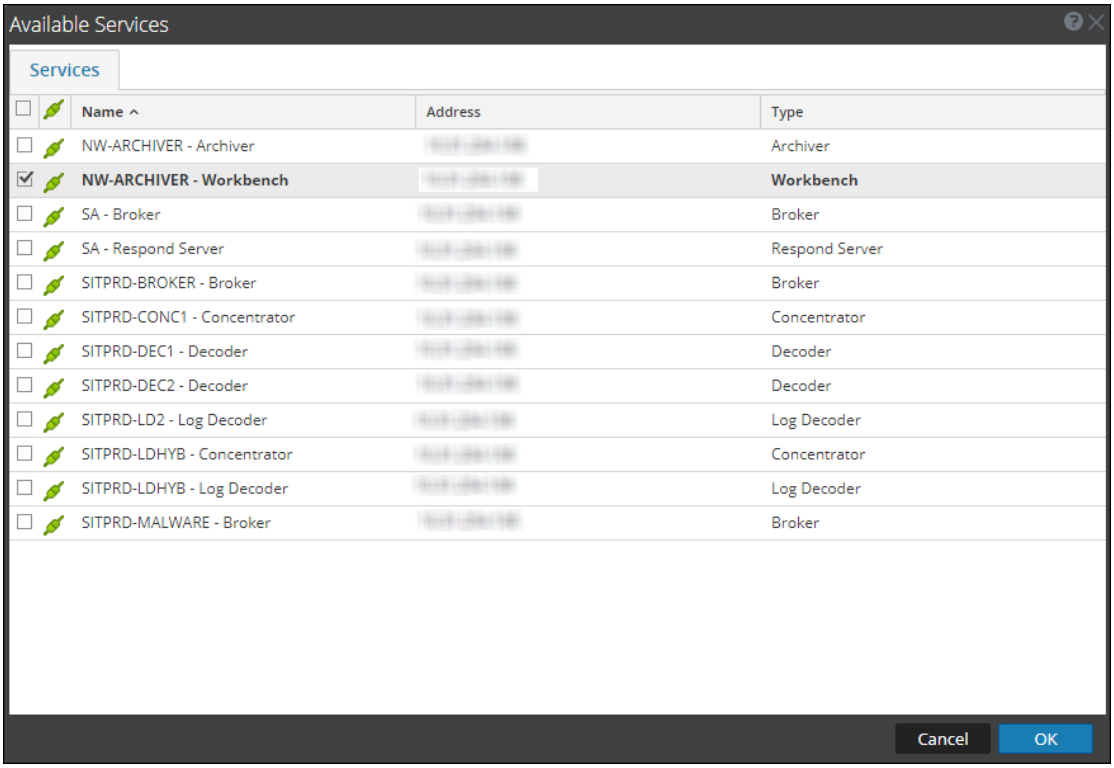
1. Agregado Workbench como un servicio a la implementación de NetWitness Suite. Para obtener más información, consulte la *Guía de configuración de Archiver*.
2. Agregado una recopilación en el servicio Workbench.

Para agregar Workbench como un origen de datos en Reporting Engine:

1. Vaya a ADMIN > **Servicios**.
2. En la lista **Servicios**, seleccione un servicio **Reporting Engine**.
3. Seleccione > **Ver** > **Configuración**.

   Se muestra la vista Configuración de servicios de Reporting Engine.
4. Seleccione la pestaña **Orígenes**.
5. Haga clic en y seleccione **Servicios disponibles**.

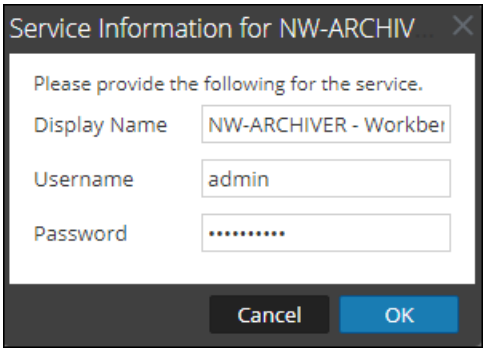
   Se muestra el cuadro de diálogo Servicios disponibles:



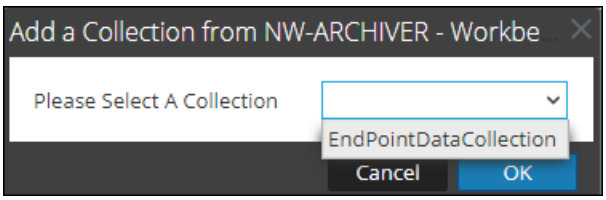
6. Seleccione el servicio Workbench y haga clic en **Aceptar**.

   Se muestra una lista de recopilaciones.

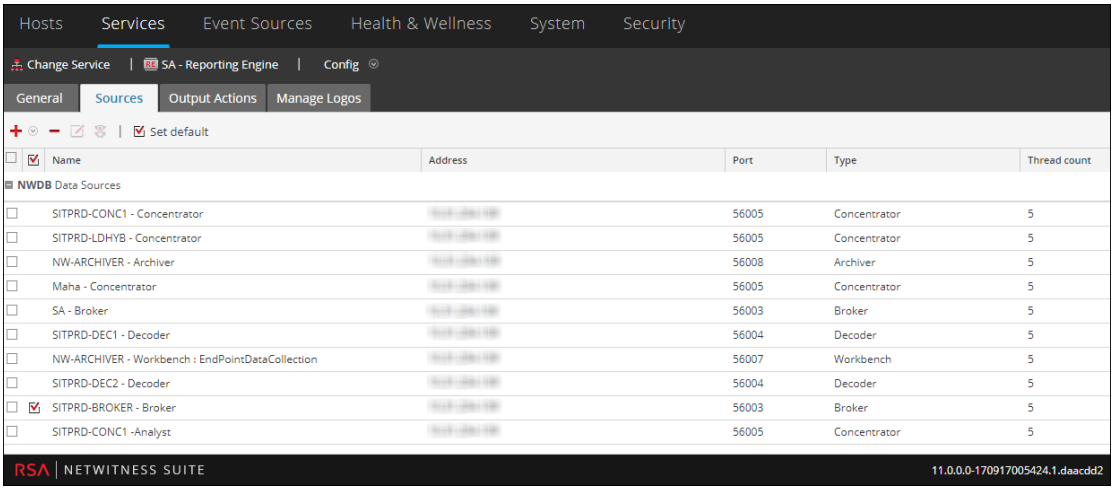
7. Ingrese la información del servicio y haga clic en **Aceptar**



8. Seleccione una recopilación en el menú desplegable.



9. El origen de datos se muestra en la pestaña Orígenes.



El servicio Workbench se agrega como un origen de datos en Reporting Engine.

Nota: Los servicios en los cuales está activado el modelo de confianza se deben agregar individualmente. Se solicita que proporcione un nombre de usuario y una contraseña para el servicio seleccionado.

(Opcional) Agregar Archiver como un origen de datos

Debe realizar las siguientes configuraciones de Archiver para que pueda usar los datos del origen de datos de Archiver para generar Informes y Alertas:

Requisitos previos

Asegúrese de haber:

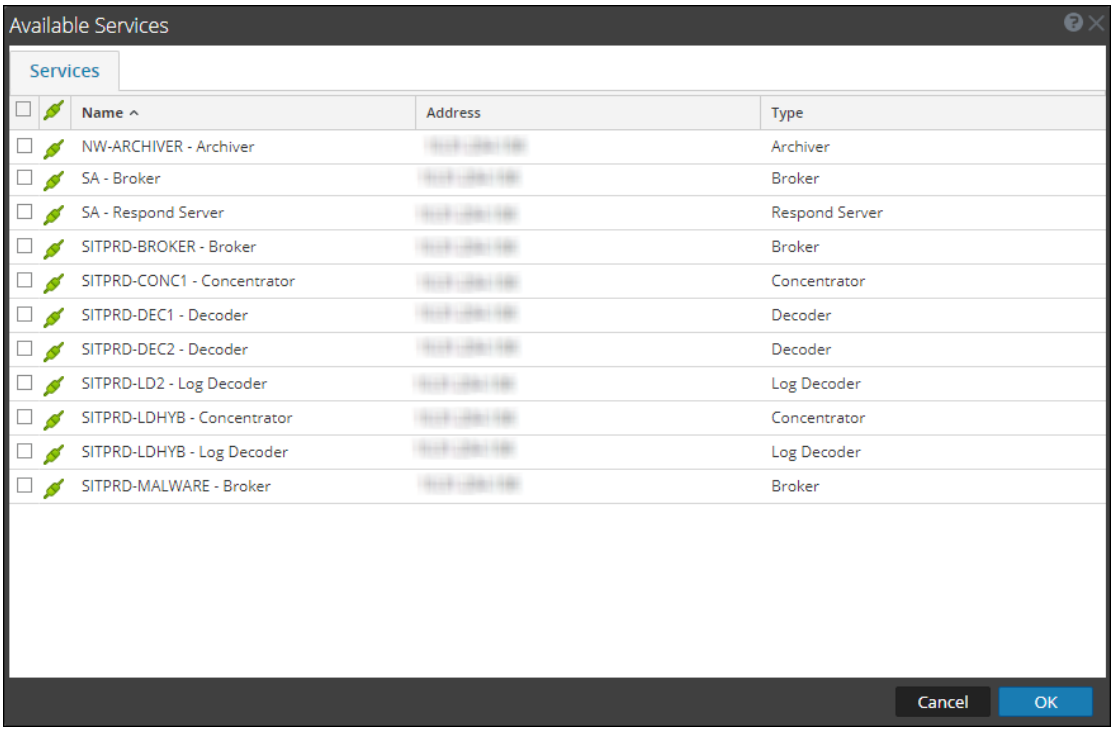
1. Instalado el host de NetWitness Suite Archiver en el ambiente de red. Para obtener más información, consulte la *Guía de introducción de hosts y servicios*.
2. Instalado y configurado Log Decoder en el ambiente de red. Para obtener más información, consulte "Agregar Log Decoder como un origen de datos en Archiver" en la *Guía de configuración de Archiver*.
3. Reporting Engine como un servicio está disponible en la implementación de NetWitness Suite.
4. Agregado Archiver como un servicio a la implementación de NetWitness Suite. Para obtener más información, consulte "Agregar el servicio Archiver" en la *Guía de configuración de Archiver*.
5. Aplicado una licencia al servicio Archiver.

Para agregar el origen de datos Archiver en Reporting Engine:

1. Vaya a **ADMIN** > **Servicios**.
2. En la lista **Servicios**, seleccione el servicio **Reporting Engine**.
3. Haga clic en  > **Ver** > **Configuración**.

   Se muestra la vista Configuración de servicios de Reporting Engine.
4. Seleccione la pestaña **Orígenes**.
5. Haga clic en  y seleccione **Servicios disponibles**.

   Se muestra el cuadro de diálogo Servicios disponibles.



6. Seleccione el servicio Archiver y haga clic en **Aceptar**.

   Se muestra el cuadro de diálogo Autenticación del servicio.

   Nota: Los servicios en los cuales está activado el modelo de confianza se deben agregar individualmente. Se solicita que proporcione un nombre de usuario y una contraseña para el servicio seleccionado.

7. Escriba el nombre de usuario y la contraseña de Archiver.
8. Haga clic en **Aceptar**.

   El Archiver seleccionado se muestra en el panel Servicios agregados.

(Opcional) Integrar información de Endpoint en Reports

Puede usar los datos de Endpoint mediante las siguientes instrucciones y agregar la información de Endpoint en los informes. La *Guía de integración de RSA Endpoint* proporciona una descripción general de la integración de Endpoint en RSA NetWitness Suite.

Requisitos previos

Asegúrese de:

- Debe haber configurado las alertas de Endpoint mediante syslog en un Log Decoder. Para obtener más información, consulte el tema "Configurar alertas de Endpoint mediante syslog en un Log Decoder" de la *Guía de integración de RSA Endpoint*).

Para integrar la información de Endpoint en los informes:

1. En **Reporting Engine**> **Ver**> **Configuración**> **Orígenes**.
2. Agregue el Concentrator que está consumiendo datos desde el Log Decoder como un origen de datos.
   Los metadatos de Endpoint se completan en Reporting Engine.
3. Ejecute informes mediante la selección de los metadatos apropiados.

(Opcional) Agregar la recopilación como un origen de datos en Reporting Engine

Debe realizar las siguientes configuraciones de Collection para que pueda usar los datos del origen de datos de Collection para generar Informes, gráficos y Alertas:

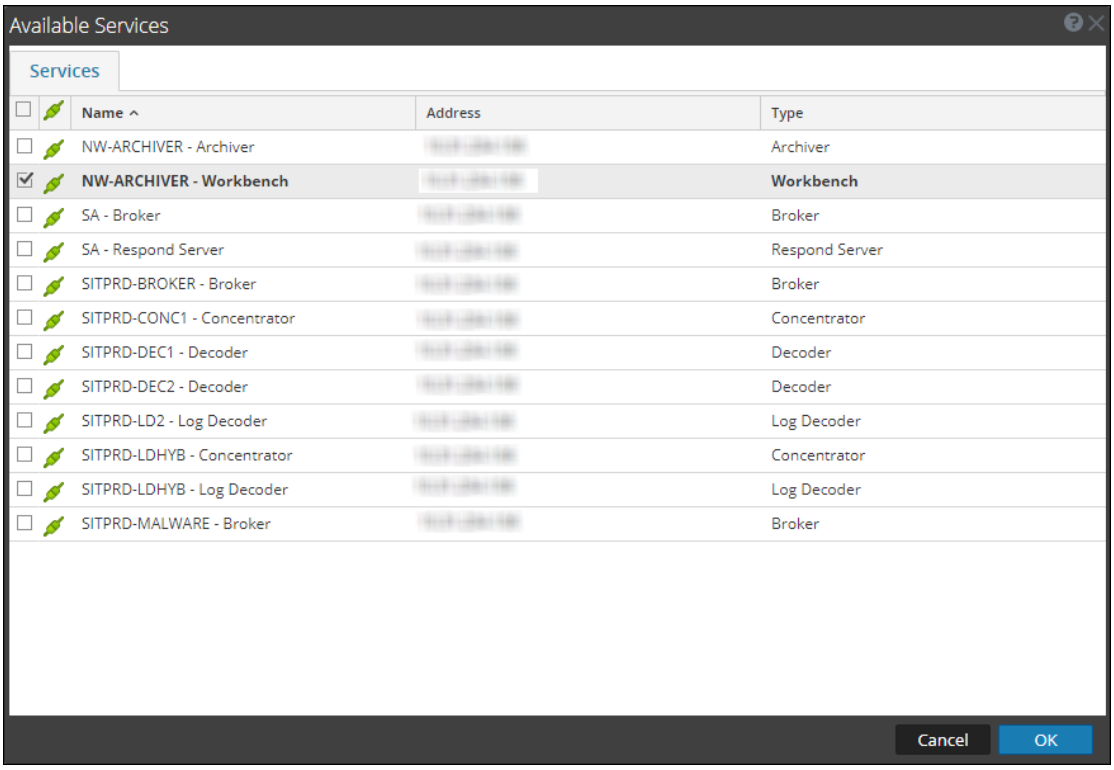
Requisitos previos

Asegúrese de haber:

- Instalado un servicio Workbench en un host de Reporting Engine.
- Respaldado datos en una ubicación conocida en el host local, si va a agregar una recopilación mediante el uso de los datos restaurados a partir de los datos respaldados.

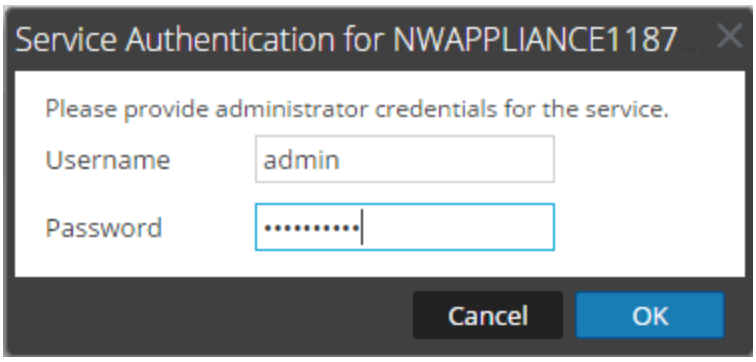
Para asociar una recopilación con un origen de datos con Reporting Engine:

1. Vaya a **ADMIN** > **Servicios**.
2. En la lista **Servicios**, seleccione un servicio **Reporting Engine**.
3. Haga clic en  > **Ver** > **Configuración**.
   Se muestra la vista Configuración de servicios de Reporting Engine.
4. Seleccione la pestaña **Orígenes**.
5. Haga clic en  y seleccione **Servicios disponibles**.
   Se muestra el cuadro de diálogo Servicios disponibles.



6. Seleccione el servicio Workbench y haga clic en **Aceptar**.

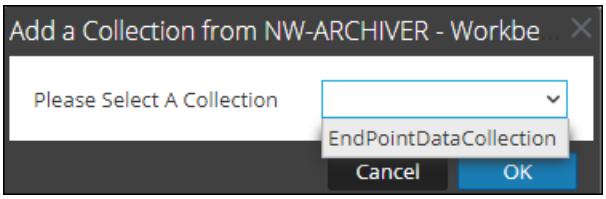
   Se muestra el cuadro de diálogo Autenticación del servicio correspondiente al servicio seleccionado.



Nota: Los servicios en los cuales está activado el modelo de confianza se deben agregar individualmente. Se solicita que proporcione un nombre de usuario y una contraseña para el servicio seleccionado.

7. Escriba el nombre de usuario y la contraseña de las credenciales de administrador correspondientes al servicio.
8. Haga clic en **Aceptar**.

   Se muestra el cuadro de diálogo Agregar recopilación.



9. Seleccione una recopilación en la lista desplegable y haga clic en **Aceptar**.

   El servicio Workbench se agrega como un origen de datos en Reporting Engine.

Configurar la privacidad de datos para Reporting Engine

Puede configurar la privacidad de datos para todos los orígenes de datos de Reporting Engine mediante la pestaña Orígenes de la vista Servicios > Ver > Configuración.

Con la adición de la función Privacidad de datos de NetWitness Suite 11.0 y superior, el acceso a metadatos confidenciales en los servicios de NetWitness Suite Core se puede restringir mediante la configuración de orígenes de datos por separado para los usuarios del perfil de Encargado de la privacidad de datos (DPO) y los usuarios no DPO, y a través de la limitación del acceso a aquellos orígenes de datos con la asignación de los permisos apropiados.

En la vista Configuración de servicios, puede agregar cada servicio principal como dos orígenes de datos por separado: uno con una cuenta de servicio que tiene privilegios equivalentes a un DPO y el otro con una cuenta de servicio que tiene privilegios equivalentes a cualquier otro usuario. Posteriormente, para limitar el acceso a esos orígenes de datos según las funciones, puede asignar acceso de lectura o impedir el acceso a esos orígenes de datos para funciones individuales. Para limitar el acceso a orígenes de datos de Warehouse, puede hacer lo mismo.

Para obtener más información, consulte Configurar permisos de orígenes de datos.

Nota: Un usuario asignado a la función `Data_Privacy_Officers` (o una función personalizada equivalente), puede crear un informe, un gráfico y una alerta. Además, se debe configurar un informe o acciones de salida de alerta en el módulo Reporting. En un ambiente donde hay funciones de privacidad de datos de NetWitness Suite habilitadas y una o más claves de metadatos están configuradas como protegidas, estas acciones pueden dar lugar a lo siguiente:

- Cuando un usuario DPO crea una alerta, los metadatos protegidos o confidenciales relacionados con ella están disponibles automáticamente en Respond. Esto puede proporcionar involuntariamente acceso a los valores de metadatos confidenciales a todos los usuarios del módulo Respond, sin importar sus funciones. Una opción para impedir esto es deshabilitar la publicación en Respond desde Reporting.
- Cuando un usuario DPO configura una acción de salida, valores de metadatos confidenciales, informes con valores de metadatos confidenciales o ambos pueden quedar a disposición de destinos o usuarios objetivo de esa acción de salida, sin importar la función asignada al usuario objetivo.

Se recomienda enfáticamente que los usuarios DPO eviten por completo la creación de alertas o la configuración de acciones de salida para un informe o una alerta en el módulo Reporting. Si realizan tal configuración, las implicaciones antes mencionadas se deben considerar cuidadosamente.

Los servicios principales de NetWitness Suite (por ejemplo, Concentrator, Broker o Archiver) son compatibles con la capacidad de restringir los metadatos según la función del usuario configurada. Para usar la función de privacidad de datos en Reporting Engine, puede configurar dos cuentas de servicio por separado para Core. Una cuenta de servicio para creación de informes de uso general que no incluye datos confidenciales y la otra cuenta para usuarios con privilegios que tienen acceso a todos los datos, incluidos los datos confidenciales. El acceso a los metadatos restringidos para las dos cuentas de servicio se configura como parte del plan de privacidad de datos en cada servicio Core.

En Reporting Engine, puede agregar cada servicio Core como dos orígenes de datos por separado (uno es el origen de datos corriente y el otro, un origen de datos con privilegios) mediante las dos cuentas de servicio por separado. Puede configurar Reporting Engine para permitir que solo los usuarios con funciones con privilegios accedan al origen de datos confidencial. Por lo tanto, Reporting Engine puede conectarse a un origen de datos de NWDB de dos maneras:

- Mediante una cuenta de servicio con función DPO.
- Mediante una cuenta de servicio sin función DPO.

Nota: También puede agregar dos o varios orígenes de datos para el mismo servicio Core.

Después de agregar dos orígenes de datos con distintas cuentas de servicio para el mismo servicio Core, puede configurar permisos de orígenes de datos para administrar el acceso a estos orígenes de datos. Para obtener más información, consulte Configurar permisos de orígenes de datos.

Nota: si el contenido se cambia para utilizar la clave de metadatos transformada, el valor de hash de los metadatos originales se muestra en su lugar cuando se ven informes, gráficos y alertas.

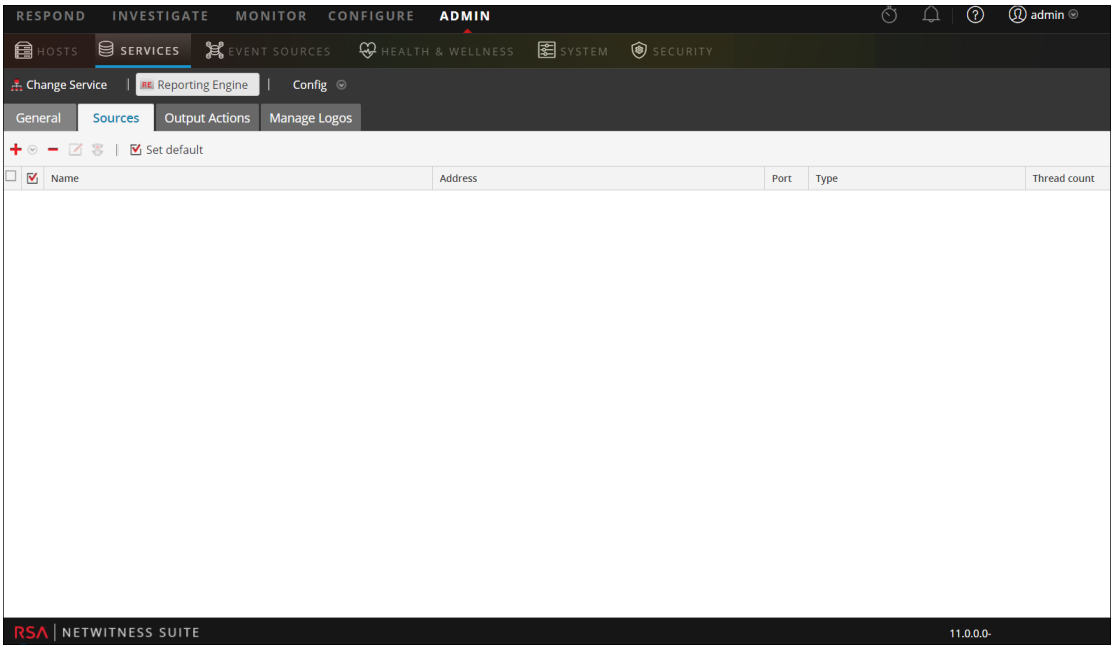
Agregar un origen de datos de NWDB con distintas cuentas de servicio

Para agregar un origen de datos NWDB:

1. Vaya a **ADMIN** > **Servicios**.
2. En la lista **Servicios**, seleccione un servicio **Reporting Engine**.
3. Haga clic en  **Ver** > **Configuración**.

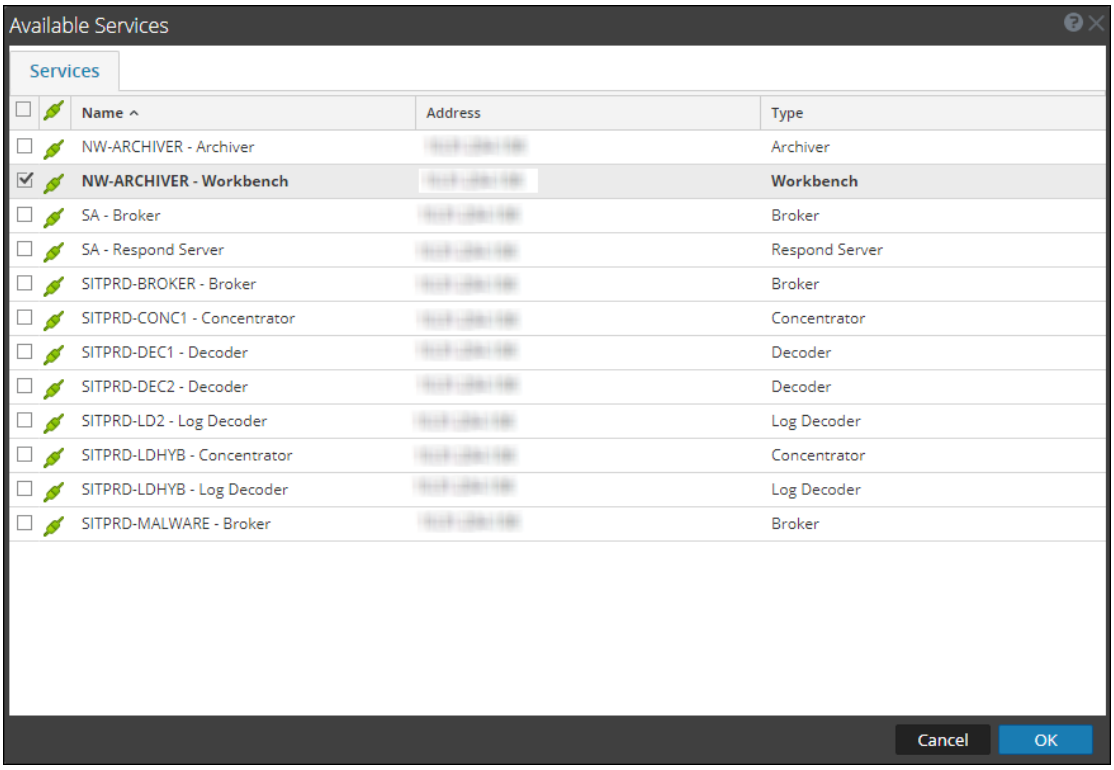
   Se muestra la vista Configuración de servicios de Reporting Engine.
4. Seleccione la pestaña **Orígenes**.

   Se muestra la vista Configuración de servicios.



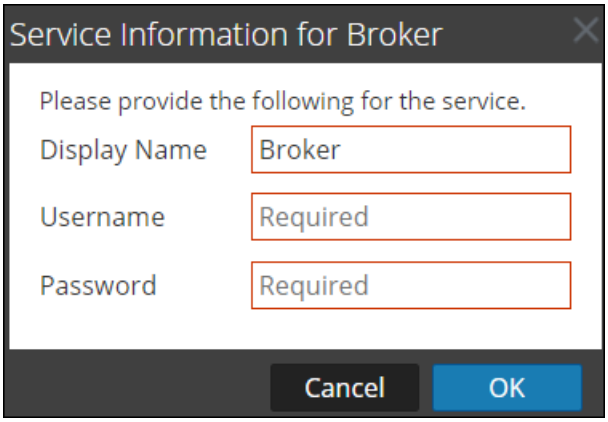
5. Haga clic en + y seleccione Servicios disponibles.

   Se muestra el cuadro de diálogo Servicios disponibles. Se enumeran todos los servicios, incluso aquellos que ya se agregaron a Reporting Engine.



6. Seleccione la casilla de verificación situada junto al servicio y haga clic en **Aceptar**.

Se muestra el cuadro de diálogo Información de servicio del servicio seleccionado.

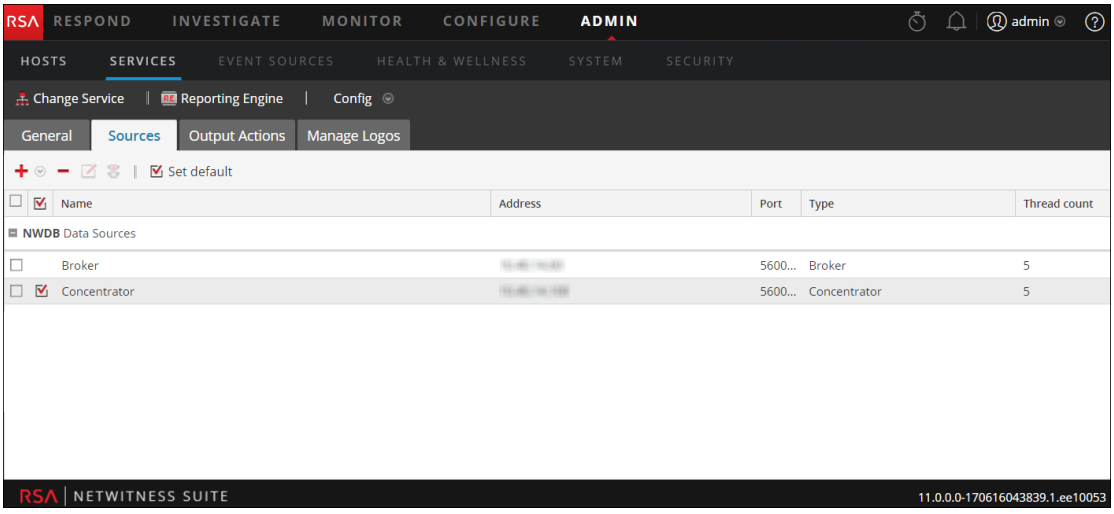


Nota: NetWitness Suite solicita que proporcione un nombre de usuario y una contraseña para el servicio seleccionado. Para limitar el acceso a datos confidenciales, los usuarios DPO deben usar sus credenciales mientras agregan el origen en lugar de usar las credenciales de administrador. Estas credenciales se deben aplicar al host, incluso si se usan conexiones de confianza entre el servidor de NetWitness Suite y los hosts de NetWitness Suite Core.

Repita el paso para el origen de datos no DPO.

7. Escriba el nombre de usuario y la contraseña para la cuenta de servicio requerida.
8. Haga clic en **Aceptar**.

   El servicio requerido se agrega como un origen de datos en Reporting Engine. Se agregan dos orígenes de datos en Reporting Engine para el mismo dispositivo Core.



Configurar permisos de orígenes de datos

Puede configurar permisos de orígenes de datos mediante la pestaña Orígenes de la vista Configuración de servicios de Reporting Engine. Esto ayuda a administrar el control de acceso a los orígenes de datos mediante la configuración de permisos de orígenes de datos. Ahora, con la capacidad de agregar más de un origen de datos para el mismo servicio principal, puede configurar distintos permisos para cada uno de ellos en el mismo servicio principal. Por ejemplo, los encargados de la privacidad de datos (DPO) pueden crear un origen de Warehouse con sus credenciales, lo que les permitirá ejecutar informes relacionados con Warehouse, a la vez que se impide que los demás usen ese origen.

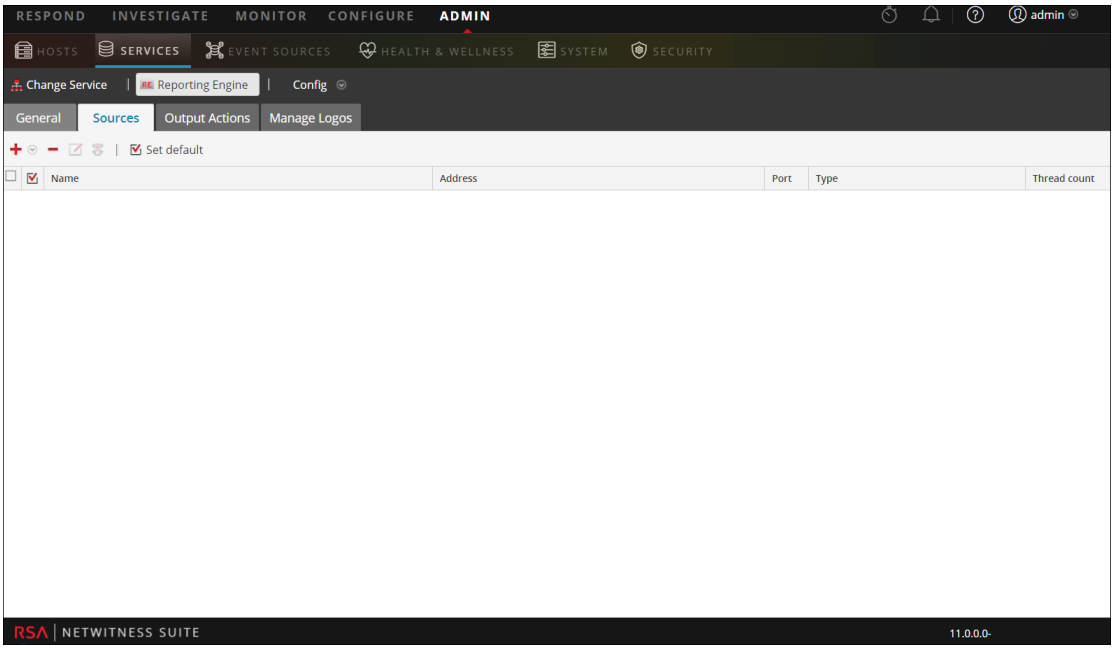
Nota: En 11.0, los permisos para los orígenes de datos de NWDB y Warehouse se configuran automáticamente en función de los permisos de los objetos de creación de informes. Por ejemplo, si los permisos de la función estaban configurados como de **Solo lectura**/**Lectura y escritura** para cualquier objeto de creación de informes en 10.5, se asigna automáticamente el permiso de solo lectura a esa función para todos los orígenes de datos que existían en 10.5. Si no se configura ningún permiso para la función, el permiso del origen de datos se configura automáticamente en Sin acceso.

Para configurar permisos para orígenes de datos:

1. Vaya a **ADMIN** > **Servicios**.
2. En la lista **Servicios**, seleccione un servicio **Reporting Engine**.
3. Haga clic en  > **Ver** > **Configuración**.

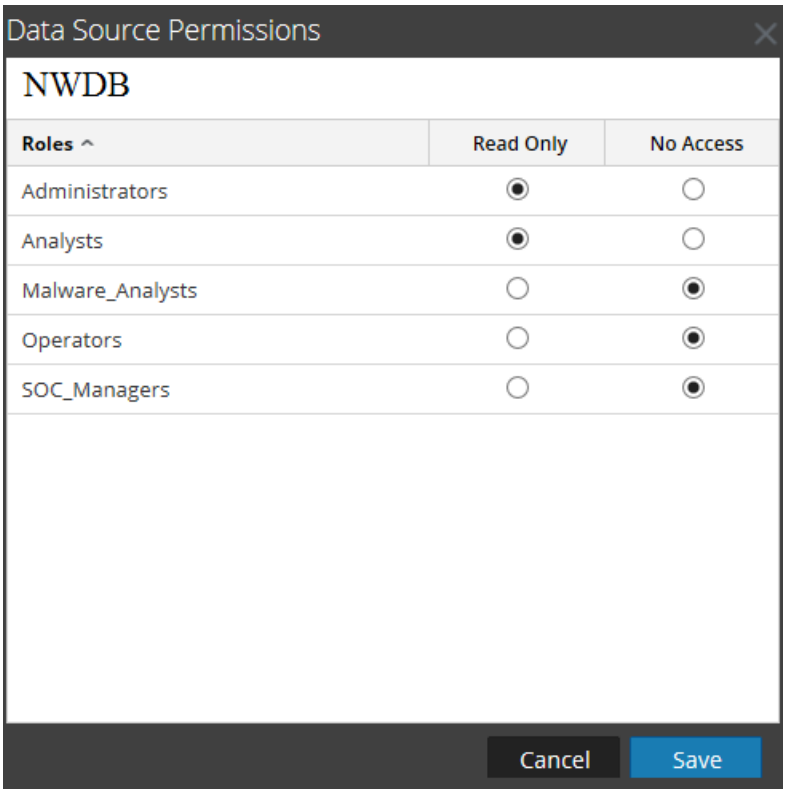
   Se muestra la vista Configuración de servicios de Reporting Engine.
4. Seleccione la pestaña **Orígenes**.

   La vista Configuración de servicios se muestra con la pestaña Orígenes.



5. Seleccione la casilla de verificación para elegir el origen de datos cuyos permisos desea configurar.
6. Haga clic en .

   Se muestra el cuadro de diálogo Permisos de origen de datos.



7. Modifique el permiso de acceso para distintos usuarios en función del tipo de cuenta de servicio del origen de datos. El permiso puede ser **Solo lectura** o **Sin acceso**.
8. Haga clic en **Guardar**.

   Los permisos requeridos se configuran para el origen de datos.

Para obtener más información, consulte la *Guía de Reporting*.

Configurar ajustes de Reporting Engine

Después de configurar el Reporting Engine y los orígenes de datos requeridos según sus requisitos, puede modificar algunas de las configuraciones para personalizar sus Informes, gráficos y Alertas.

Para configurar los ajustes:

1. Vaya a **ADMIN** > **Servicios**.
2. En la lista **Servicios**, seleccione un servicio **Reporting Engine**.
3. Haga clic en  > **Ver** > **Configuración**.

   La vista Configuración de servicios de Reporting Engine se muestra con la pestaña General resaltada. Para obtener más información sobre la pestaña General de Reporting Engine, consulte la Pestaña General.
4. Edite la configuración del servicio Reporting Engine y haga clic en **Aplicar**.

   Los ajustes de servicio se configuran en Reporting Engine.

Activar la autenticación LDAP

Para habilitar el modo de autenticación LDAP mediante Active Directory para HiveServer2 para el origen de datos de Warehouse, siga estos pasos.

1. Inicie sesión en el dispositivo de RSA Analytics Warehouse como usuario raíz.
2. Navegue al directorio `/opt/mapr/hive/hive-0.11/conf.new/` . Escriba el siguiente comando y presione INTRO:

   ```
   cd /opt/mapr/hive/hive-0.11/conf.new/
   ```
3. Edite el archivo `hive-site.xml`. Escriba el siguiente comando y presione INTRO:

   ```
   vi hive-site.xml
   ```
4. Agregue las siguientes propiedades bajo la etiqueta `<Configuration>`:

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

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

Donde `LDAP_URL` es la URL del servidor LDAP.

5. Reinicie HiveServer2.

Agregar espacio adicional para informes grandes

Para agregar espacio adicional en disco al Reporting Engine para informes grandes, siga los siguientes pasos. Si se debe generar informes de cumplimiento de normas grandes para , el espacio de disco de Reporting Engine se puede consumir más rápido de lo esperado. Si es este el caso, puede montar cualquier almacenamiento externo como SAN o NAS para almacenar informes.

Los directorios que tienden a llenar el espacio en disco son `resultstore` y `formattedReports` en el directorio principal de Reporting Engine. Se recomienda transferir solo estos dos directorios a SAN o NAS y reemplazar las ubicaciones originales por vínculos simbólicos que lleven a las nuevas ubicaciones. También se recomienda dejar los directorios restantes en el disco local para un rendimiento de I/O confiable y alto.

Nota: En los siguientes pasos, se supone que el directorio principal de Reporting Engine se encuentra en `/var/netwitness/re-server/rsa/soc/reporting-engine/` y que el almacenamiento externo está montado en `/externalStorage/`. Además, el usuario "rsasoc" debe tener acceso de lectura y escritura a la ruta de almacenamiento externo especificado.

Para transferir el espacio en disco del Reporting Engine a almacenamiento externo:

1. Detenga el servicio Reporting Engine como usuario raíz.

   ```
   service rsasoc_re stop
   ```

2. Cambie al usuario `rsasoc`.

   ```
   su rsasoc
   ```

3. Cambie al directorio de inicio de RE.

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

4. Mueva el directorio resultstore a un almacenamiento externo montado. Escriba el siguiente comando y presione INTRO:

   ```
   mv resultstore /externalStorage
   ```

5. Mueva el directorio Informes formateados a un almacenamiento externo montado. Escriba el siguiente comando y presione INTRO:

   ```
   mv formattedReports /externalStorage
   ```

6. Cree un vínculo simbólico para resultstore. Escriba el siguiente comando y presione INTRO:

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

7. Crear un vínculo simbólico para formattedReports. Escriba el siguiente comando y presione INTRO:

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

8. Salga del usuario `rsasoc`.

   ```
   exit
   ```

9. Iniciar el servicio Reporting Engine como usuario raíz.

   ```
   service rsasoc_re start
   ```

   Nota: Si el almacenamiento externo está offline, no puede realizar las siguientes tareas:
   1) Ejecutar informes o alertas de Reporting
   2) Ver informes o alertas de Reporting existentes
   Sin embargo, puede crear nuevos objetos de Reporting, como informes y gráficos, y acceder a gráficos y al tablero de Live creado para los gráficos. Por lo tanto, debe asegurarse de que el almacenamiento externo sea confiable y que tenga el espacio requerido.

   Además, si desea almacenar informes durante más de 100 días, cambie la configuración de la retención según corresponda en Configurar ajustes de Reporting Engine.

Acceso a archivos de registro de Reporting Engine

Puede acceder a los archivos de registro de Reporting Engine que se almacenan en el siguiente directorio de registros `/var/netwitness/re-server/rsa/soc/reporting-engine/logs/`

- Los registros actuales en el archivo `reporting-engine.log`.
- Copia de respaldo de registros anteriores en el archivo `reporting-engine.log.*`.
- Todos los registros de script de UNIX en los archivos que tienen la siguiente sintaxis: `reporting-engine.sh_timestamp.log` (por ejemplo, `reporting-engine.sh_20120921.log`)

Es poco frecuente que Reporting Engine escriba mensajes de error de la línea de comandos en el archivo **rsasoc/nohup.out**.

Reporting Engine anexa la salida y los mensajes de registro que escribe el sistema systemd, así como los comandos que se usan para iniciar el motor de creación de informes, en el directorio `/var/log/messages`. Un archivo de registro `/var/log/messages` es un archivo de registro del sistema que solo puede leer el usuario raíz.

Configurar el programador de tareas para un Reporting Engine

Puede configurar líneas de espera y pools en Reporting Engine para programar informes de NWSB o Warehouse. Para obtener más información acerca de los programadores de tareas, consulte “Programador de tareas para Warehouse Reporting” en la *Guía de Reporting de RSA NetWitness Suite*

Requisitos previos

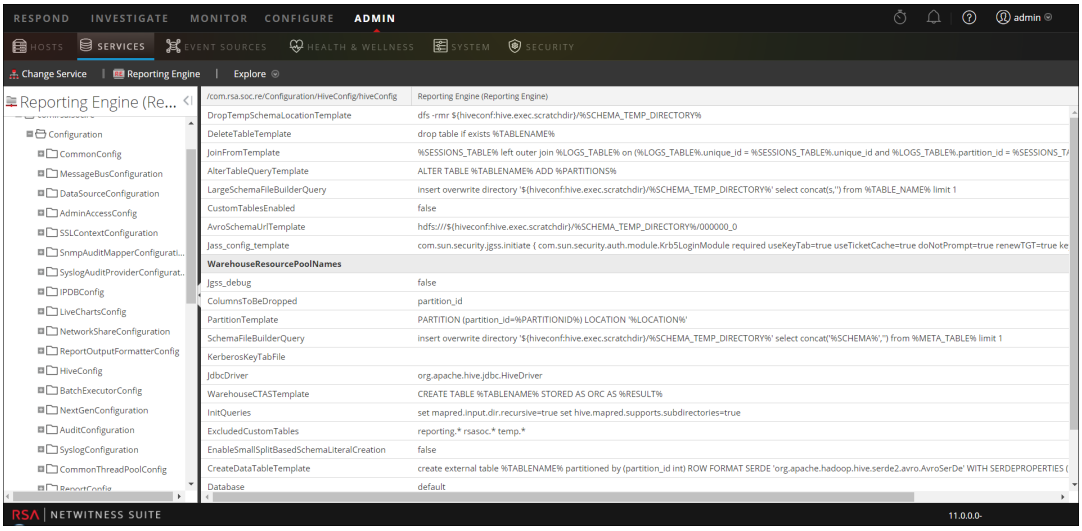
Asegúrese de haber identificado lo siguiente:

- Tipo de analizador y pools o líneas de espera que desea usar. Puede configurar solo un programador para Reporting Engine. De manera predeterminada, se configura el analizador justo.
- Nombres de las líneas de espera o pools, y los recursos proporcionados para cada línea de espera y pool.
- NetWitness Suite no es compatible con múltiples líneas de espera o pools por clúster. RSA recomienda que proporcione nombres únicos a las líneas de espera o pools en todos los clústeres, o que use los mismos nombres de línea de espera o pool en ambos clústeres. Si el tamaño del clúster es grande, es posible que haya más de tres pools o líneas de espera.
- Si usa un programador no compatible, Reporting Engine no configura ninguna propiedad para los trabajos que inicia.
- Si el nombre del pool o la línea de espera no existen en el clúster, el analizador de capacidad usará la línea de espera predeterminada para el informe. Es posible que el analizador justo no pueda ejecutar la regla o creará un nuevo pool con el recurso compartido más bajo. Esto se basa en el valor especificado para la propiedad del programador justo `mapred.fairscheduler.allow.undeclared.pools`.
- Si no especifica un pool o una línea de espera, el trabajo que inició la regla de prueba está en el pool `mapr` o en la línea de espera predeterminada. RSA recomienda configurar un pool mapr con un recurso compartido bajo (alrededor de 1/10 de la capacidad total) con `maxRunningJobs = 2` de modo que estas reglas no interrumpan los informes en ejecución. Asegúrese de no especificar este nombre de pool para ningún informe.

Especificar los pools y las líneas de espera

Para especificar los pools y las líneas de espera:

1. Vaya a **ADMIN** > **Servicios**.
2. Seleccione **Reporting Engine** y haga clic en  > **Ver** > **Explorar**.
3. Seleccione **com.rsa.soc.re** > **Configuración** > **HiveConfig** > **hiveconfig** > **WarehouseResourcePoolNames**.
4. En el campo **WarehouseResourcePoolNames**, ingrese los nombres de pool o línea de espera separados por espacios. Por ejemplo, para configurar cuatro pools o líneas de espera con los nombres pool1, pool2, incorrecto y predeterminado, ingrese los nombres separados por un espacio.



Definir informes, gráficos y alertas

Después de configurar Reporting Engine y el origen de datos requerido según sus requisitos, puede generar informes, gráficos y alertas.

Definir informes, gráficos y alertas

Cómo definir Informes

Después de crear los orígenes de datos y de configurar los permisos de usuario para ellos, puede usarlos con el fin de realizar las siguientes tareas para el módulo Reporting:

- **Definir una regla**
- **Probar una regla**
- **Calendarizar informes**
- **Agregar una alerta**
- **Agregar un gráfico**
- **Probar un gráfico**

Para obtener más información, consulte los temas anteriores en la *Guía de informes de RSA NetWitness Reporting*.

Cómo definir gráficos

Después de crear los orígenes de datos y de configurar los permisos de usuario para ellos, puede usarlos con el fin de realizar las siguientes tareas para el módulo Reporting:

- **Definir un gráfico y grupos de gráficos**
- **Probar un gráfico**
- **Investigar gráficos**
- **Administrar gráficos**

Para obtener más información, consulte los temas anteriores en la *Guía de informes de RSA NetWitness Reporting*.

Cómo definir alertas

Después de crear los orígenes de datos y de configurar los permisos de usuario para ellos, puede usarlos con el fin de realizar las siguientes tareas para el módulo Alerting:

- **Configurar Alertas**
- **Generar Alertas**

- **Agregar una alerta**
- **Ver una alerta**
- **Ver programa de alertas**
- **Investigar una alerta**

Para obtener más información, consulte los temas anteriores en la *Guía de alertas de RSA NetWitness Reporting*.

Configurar ajustes generales de Reporting Engine

Al agregar y configurar el servicio Reporting Engine, la configuración del sistema se define con valores predeterminados para alcanzar resultados óptimos. Sin embargo, puede modificar y personalizar las notificaciones de Reporting Engine en función de sus requisitos, para ello vaya a la pestaña General en la vista Configuración de servicios para un Reporting Engine.

Acceder a la pestaña General

Debe abrir la pestaña General para configurar los parámetros generales para Reporting Engine.

Para acceder a esta vista:

1. Vaya a **ADMIN** > **Servicios**.
2. En la lista Servicios disponibles, seleccione un servicio **Reporting Engine**.
3. Haga clic en **Ver** > **Configuración**.
4. Seleccione la pestaña **General**.
5. Haga clic en **Aplicar** después de editar los parámetros.

Después de que navega a la pestaña General, puede modificar los siguientes parámetros.

- Configuración del sistema
- Configuración de registro
- Configuración de la salida de Warehouse Analytics
- Configuración del modelo de Warehouse Analytics
- Configuración de Kerberos de Warehouse

Para obtener más información, consulte la pestaña General para obtener detalles sobre los parámetros de configuración.

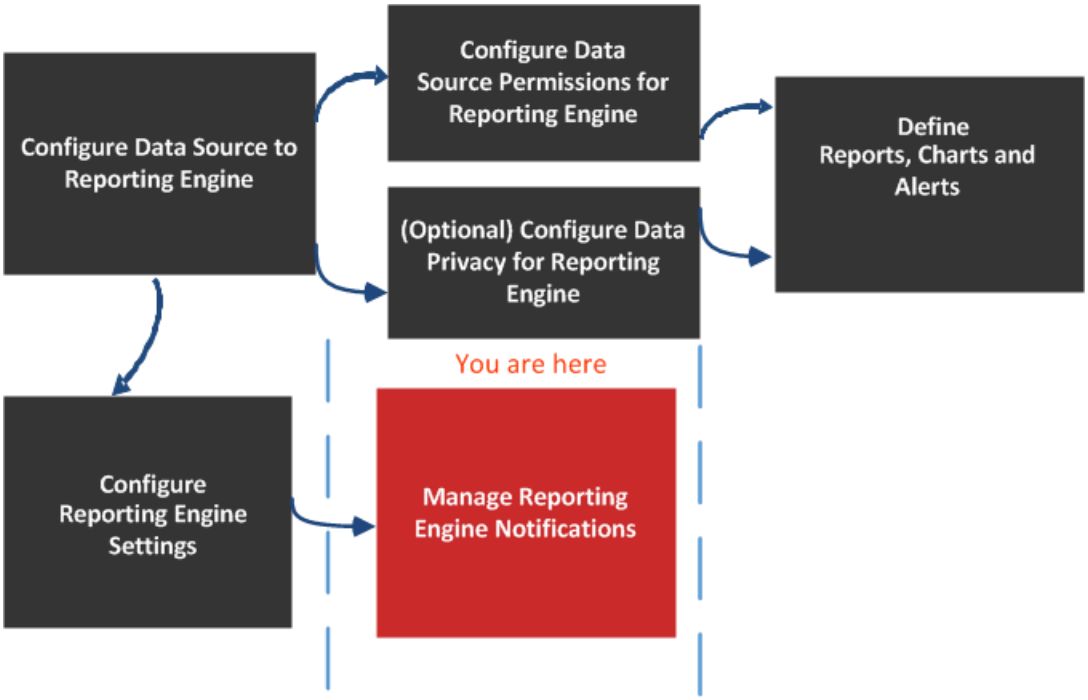
Referencias

Para poder personalizar y optimizar el uso del servicio, puede modificar los ajustes de Reporting Engine en la vista Configuración de servicios, lo cual tiene parámetros que se relacionan específicamente con Reporting Engine.

Pestaña General

La pestaña General del servicio Reporting Engine controla diversos ajustes que pueden optimizar el rendimiento de un servicio y especificar los parámetros de conexión del usuario para el servicio. Navegue a Servicios > Ver > Configuración > Reporting Engine > General. Estos ajustes se usan exclusivamente para el servicio Reporting Engine.

El permiso requerido para acceder a esta vista es Administrar servicios.



¿Qué desea hacer?

Función	Deseo…	Consulte...
Administrador	Configurar orígenes de datos en Reporting Engine	Configurar los orígenes de datos
Administrador	Configurar permisos de orígenes de datos para Reporting Engine	Configurar permisos de orígenes de datos

Función	Deseo…	Consulte...
Administrador	Configurar la privacidad de datos para Reporting Engine	Configurar la privacidad de datos para Reporting Engine
Administrador	Definir informes, gráficos y alertas	Definir informes, gráficos y alertas
Administrador	Configurar ajustes de Reporting Engine	Configurar ajustes de Reporting Engine
Administrador/administrador del SOC	Configurar los ajustes del sistema*	Configurar ajustes generales de Reporting Engine
Administrador/administrador del SOC	Configurar el registro *	Configurar ajustes generales de Reporting Engine
Administrador/administrador del SOC	Configurar la salida de Warehouse Analytics *	Configurar ajustes generales de Reporting Engine
Administrador/administrador del SOC	Configurar modelos de Warehouse Analytics *	Configurar ajustes generales de Reporting Engine
Administrador/administrador del SOC	Configurar Kerberos de Warehouse *	Configurar ajustes generales de Reporting Engine

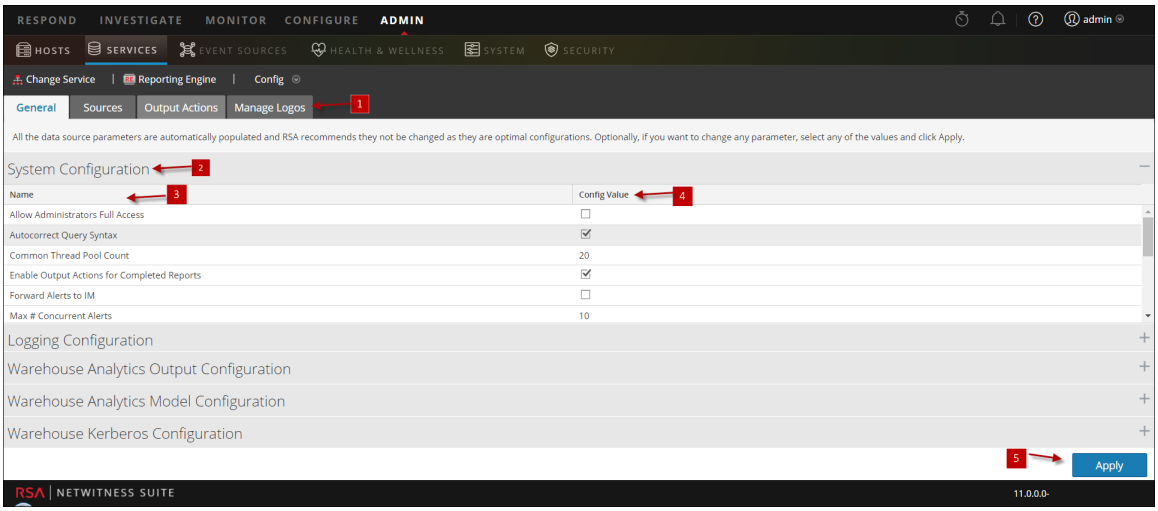
*Puede realizar estas tareas aquí.

Temas relacionados

- Cómo funciona Reporting Engine

Vista rápida

Este es un ejemplo de la pestaña General, en la cual se muestran configuraciones de servicios.



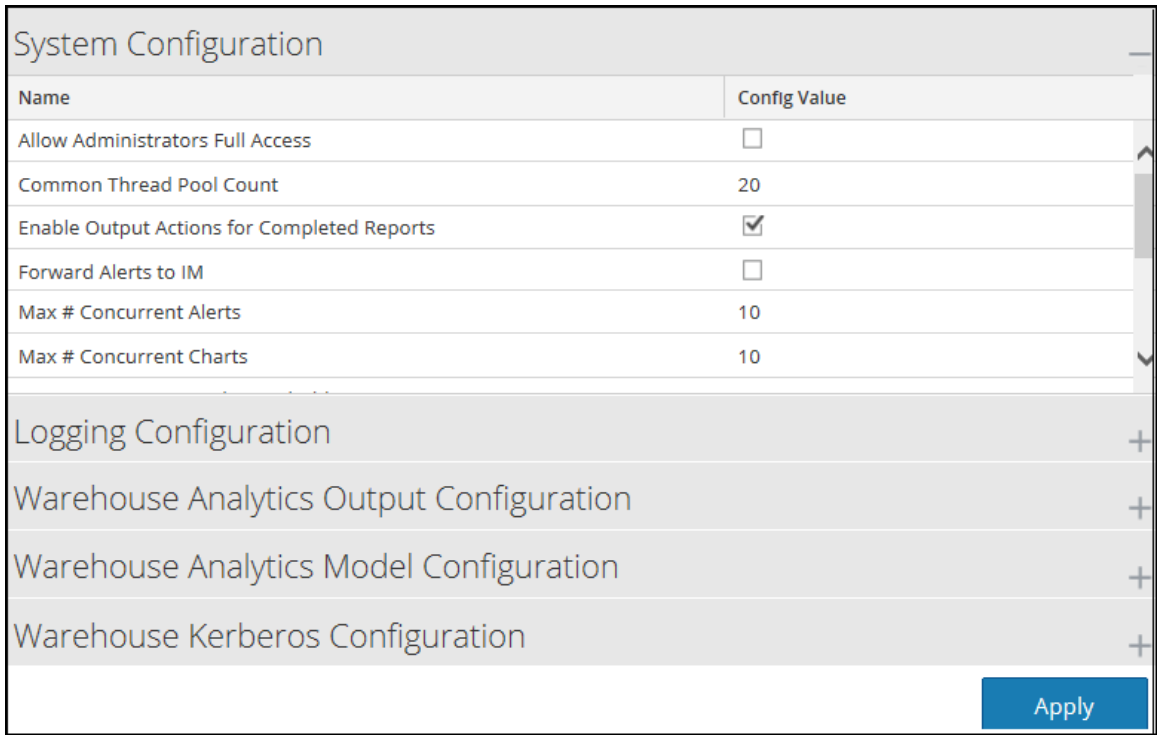
1. Muestra todas las pestañas configurables disponibles.
2. Muestra los parámetros de configuración disponibles para el sistema.
3. Muestra el nombre del parámetro.
4. Muestra los valores configurados para cada parámetro.
5. Aplica los cambios.

Nota: Warehouse Analytics no es compatible con NetWitness Suite versión 11.0.

Configuración del sistema

Los parámetros del panel Configuración del sistema de Reporting Engine administran la configuración de un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, se aplican valores predeterminados. Los valores predeterminados se diseñaron para adecuarse a la mayoría de los ambientes y se recomienda no editarlos, dado que esto podría afectar negativamente el rendimiento.

En la siguiente figura se muestran los campos que se pueden configurar en el panel Configuración del sistema:



La siguiente tabla describe las funcionalidades del panel Configuración del sistema.

Nombre	Valor de configuración
Permitir acceso completo a los administradores	Seleccione la casilla de verificación si desea acceder a todos los objetos de Reporting Engine (informes, regla, gráficos, calendario y lista) que crean otros usuarios (no administrativos). De forma predeterminada, esta opción no está habilitada. **Nota:** Si habilita la casilla de verificación y después la deshabilita, el acceso en todos los objetos de Reporting Engine que se habilitó cuando se seleccionó la casilla no estará disponible. Sin embargo, si definió el acceso en objetos específicos a través de la ventana Permisos (**Informes > Administrar > Objeto de RE > > Permisos**), la habilitación/deshabilitación de esta casilla de verificación no afectará a estos objetos.
Conteo de pools de hilos de ejecución comunes	La cantidad de pools de hilos de ejecución asignados a la ejecución de tareas comunes en Reporting Engine. Un valor válido es un entero (el valor predeterminado es **20**).

Nombre	Valor de configuración
Activar acciones de salida para informes finalizados	Seleccione la casilla de verificación para procesar acciones de salida solo para informes con todas las ejecuciones de reglas correctas. De forma predeterminada, está habilitada. Si está deshabilitada, las acciones de salida se procesan para todos los escenarios (completados, parciales y fallidos).
Reenviar alertas a Respond	Seleccione la casilla de verificación para reenviar todas las alertas a Respond. De forma predeterminada, esta opción no está habilitada.
Cantidad máx. de alertas simultáneas	El número máximo de alertas que se pueden ejecutar de manera simultánea. Esto afecta directamente al servicio de RSA contra el cual se ejecutan las alertas, debido a que cada alerta consume un subproceso de consulta en el servicio de RSA. Un valor válido es un entero (el valor predeterminado es **10**).
Cantidad máx. de gráficos simultáneos	La cantidad máxima de gráficos que se pueden ejecutar de manera simultánea. Un valor válido es un entero (el valor predeterminado es **10**).
Cantidad máx. de consultas LookupAndAdd simultáneas	La cantidad máxima de consultas LookupAndAdd paralelas que se pueden ejecutar por regla NWDB. Un valor válido es un entero (el valor predeterminado es **2**). Cuando aumenta este valor, para un mejor rendimiento, debe asegurarse de que el origen de datos NWDB esté configurado para manejar las consultas paralelas.
Cantidad máx. de informes de valores de lista simultáneos	La cantidad máxima de informes de valores de lista por programa que se pueden generar en paralelo. Un valor válido es un entero (el valor predeterminado es **1**).

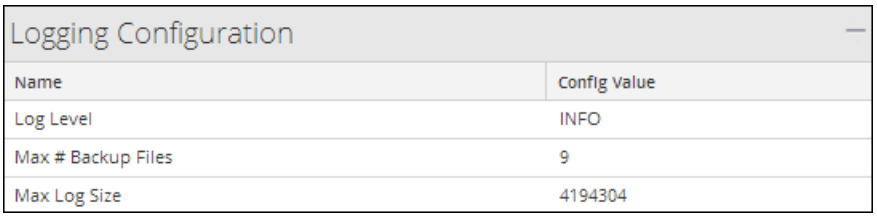
Nombre	Valor de configuración
Cantidad máx. de informes de valores de lista	La cantidad máxima de informes de valores de lista generados, independientemente del número de valores en la lista. Un valor válido es un entero (el valor predeterminado es **10000**).
Máximo de filas almacenadas por regla (mil millones)	La cantidad máxima de filas que puede buscar una regla cuando se consulta. Un valor válido es un entero (el valor predeterminado es **100**).
Umbral máximo de espacio en disco	Este es el umbral máximo de espacio en disco asignado (en GB) para ejecutar informes, alertas y gráficos. El valor inicial se configura en función del espacio disponible en el sistema.
Umbral mínimo de espacio en disco	Este es el umbral mínimo de espacio en disco asignado (en porcentaje) necesario para ejecutar informes, gráficos y alertas. De forma predeterminada, este valor está configurado en 5. **Nota:** Nota: Si se alcanza el umbral mínimo, la ejecución de informes, gráficos y alertas se detendrá incluso si el servicio está en ejecución.
Tiempo de espera agotado de consultas de información de NWDB	El tiempo de espera de consultas de información en segundos para el servidor de NWDB. Un valor válido es un entero (el valor predeterminado es **0**).
Máximo de filas agregadas de NWDB	La cantidad máxima de filas que se devuelve cuando se usa agregación en la regla NWDB. Un valor válido es un entero (el valor predeterminado es **1,000**).

Nombre	Valor de configuración
Tiempo de espera agotado de consulta de NWDB	El tiempo de espera en segundos para que el servidor NWDB de por agotado el tiempo de espera para la ejecución de la regla, si no puede procesar el resultado en el tiempo configurado. El valor predeterminado se establece en 0, lo que significa que no hay tiempo de espera agotado. Un valor válido es un número entero.
Procesar acciones de salida solo para informes correctos	Seleccione esta casilla de verificación para procesar acciones de salida solo para informes cuyas reglas se ejecutan correctamente. Cuando deselecciona esta casilla de verificación, la acción se salida se activa para los informes parciales, finalizados y fallidos. **Nota:** Esto se aplica a todas las acciones de salida, excepto a las acciones de salida de lista dinámica.
Conservar historial de alertas durante N días	La cantidad máxima de días que se conserva el historial de alertas y el estado de alertas. Un valor válido es un entero (el valor predeterminado es **100**).
Conservar historial de gráficos durante N días	La cantidad máxima de días que se conserva el historial de gráficos y el estado de gráficos. Un valor válido es un entero (el valor predeterminado es **30**).
Conservar historial de informes durante N días	La cantidad máxima de días que el sistema conserva el historial de informes y el estado de informes. Un valor válido es un entero (el valor predeterminado es **100**).
Conteo de pools de hilos de ejecución calendarizados	La cantidad de pools de subproceso asignados para las tareas programadas (por ejemplo, borrar el historial) en Reporting Engine. Un valor válido es un entero (el valor predeterminado es **5**).

Configuración de registro

Los parámetros del panel Configuración de registro de Reporting Engine administran la configuración de registro de un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, se aplican valores predeterminados. RSA diseñó los valores predeterminados para adecuarse a la mayoría de los ambientes y recomienda no editarlos, dado que esto podría afectar negativamente el rendimiento de Reporting Engine.

En la siguiente figura se muestran los campos que se pueden configurar en el panel Configuración de registro.



La siguiente tabla describe las funcionalidades del panel Configuración de registro.

Nombre	Valor de configuración
Log Level	El nivel de registro que determina el alcance de la información que se incluye en los archivos de registro. Los valores posibles son: • ERROR • WARN • INFO (valor predeterminado) • DEBUG • ALL
Cantidad máx. de archivos de respaldo	La cantidad máxima de archivos de registro de respaldo que el sistema conserva. Un valor válido es un entero (el valor predeterminado es **9**).
Tamaño máximo de registro	El tamaño máximo (en bytes) del archivo de registro primario. Un valor válido es un entero (el valor predeterminado es **4194304**).

Para obtener más información sobre el registro de Reporting Engine, consulte Acceso a archivos de registro de Reporting Engine.

Configuración de la salida de Warehouse Analytics

Nota: Warehouse Analytics no es compatible con NetWitness Suite versión 11.0.

El panel Configuración de la salida de Warehouse Analytics proporciona una forma de especificar la configuración de la salida de Warehouse Analytics en este Reporting Engine.

En la siguiente figura se muestran los campos que se pueden configurar en el panel Configuración de la salida de Warehouse Analytics:

Después de una actualización, asegúrese de actualizar los detalles de **Mongo DB** centralizada para poder usar Warehouse Analytics.

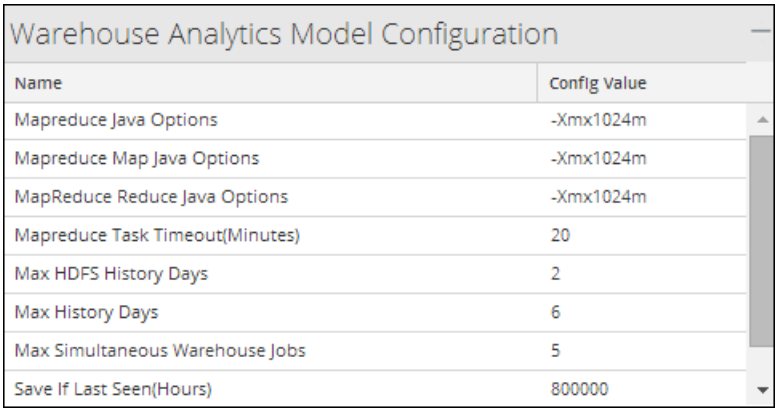
En la siguiente tabla se describen las funciones del panel Configuración de la salida de Warehouse Analytics.

Nombre	Valor de configuración
Nombre	**Valor de configuración**
Nombre de usuario	El nombre de usuario del usuario de Warehouse Analytics.
Puerto	El puerto de Mongo DB que usa Warehouse Analytics.
Host	El host de Mongo DB que usa Warehouse Analytics.
Contraseña	La contraseña del usuario de Warehouse Analytics.

Configuración del modelo de Warehouse Analytics

En el panel Configuración del modelo de Warehouse Analytics se proporciona una forma de especificar la configuración del modelo de Warehouse Analytics en este Reporting Engine.

En la siguiente figura se muestran los campos que se pueden configurar en el panel Configuración del modelo de Warehouse Analytics:



En la siguiente tabla se describen las funciones del panel Configuración del modelo de Warehouse Analytics:

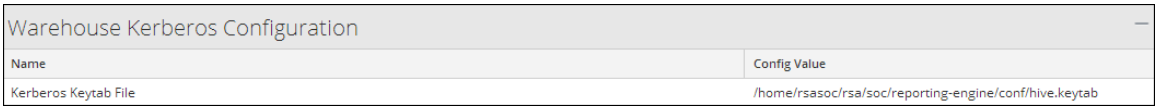
Nombre	Valor de configuración
Opciones de Mapreduce Java	Los parámetros de JVM para JVM secundario del tracker de la tarea MapReduce de Hadoop. De forma predeterminada, el valor es **-Xmx1024m**.
Opciones de Mapreduce Map Java	El parámetro que controla los parámetros de JVM para los trabajos de mapeo dentro del clúster de Hadoop. De manera predeterminada, el valor es **-Xmx1024m**.
Opciones de MapReduce Reduce Java	El parámetro que controla los parámetros de JVM para los trabajos de reducción dentro del clúster de Hadoop. De manera predeterminada, el valor es **-Xmx1024m**.
Tiempo de espera agotado de la tarea de Mapreduce (minutos)	La cantidad de minutos antes de que finalice una tarea cuando una infraestructura de MapReduce la titula como sin respuesta o inactiva. Un valor válido es un entero (el valor predeterminado es **20**).
Máximo de días de historial de HDFS	La cantidad máxima de días que se conservan los archivos temporales y de salida del trabajo en HDFS. Un valor válido es un entero (el valor predeterminado es **2**).
Máximo de días de historial	La cantidad máxima de días que se conserva la salida del trabajo en Mongo DB. Un valor válido es un entero (el valor predeterminado es **6**).
Máximo de trabajos simultáneos de Warehouse	El parámetro que controla la cantidad máxima de trabajos paralelos ejecutados a través de la infraestructura Warehouse Analytics. Un valor válido es un entero (el valor predeterminado es **1**).
Guardar si se vieron por última vez (horas)	El parámetro para guardar las claves de la salida del trabajo si no se vieron en las últimas “n” horas. Un valor válido es un entero (el valor predeterminado es **800000**).

Nombre	Valor de configuración
Puntaje de umbral	El parámetro para guardar las claves de la salida del trabajo en listas de seguimiento para que ESA las use solo si el puntaje es mayor que "n". Un valor válido es un entero (el valor predeterminado es **55**).

Configuración de Kerberos de Warehouse

En el panel Configuración de Kerberos de Warehouse se proporciona una forma de especificar el archivo keytab de Kerberos en este Reporting Engine.

En la siguiente figura se muestra el campo que se puede configurar en el panel Configuración de Kerberos de Warehouse:



En la siguiente tabla se describen las funciones del panel Configuración de Kerberos:

Nombre	Valor de configuración
Archivo keytab de Kerberos	Ubicación del archivo keytab de Kerberos. Por ejemplo, `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/hive.keytab`.

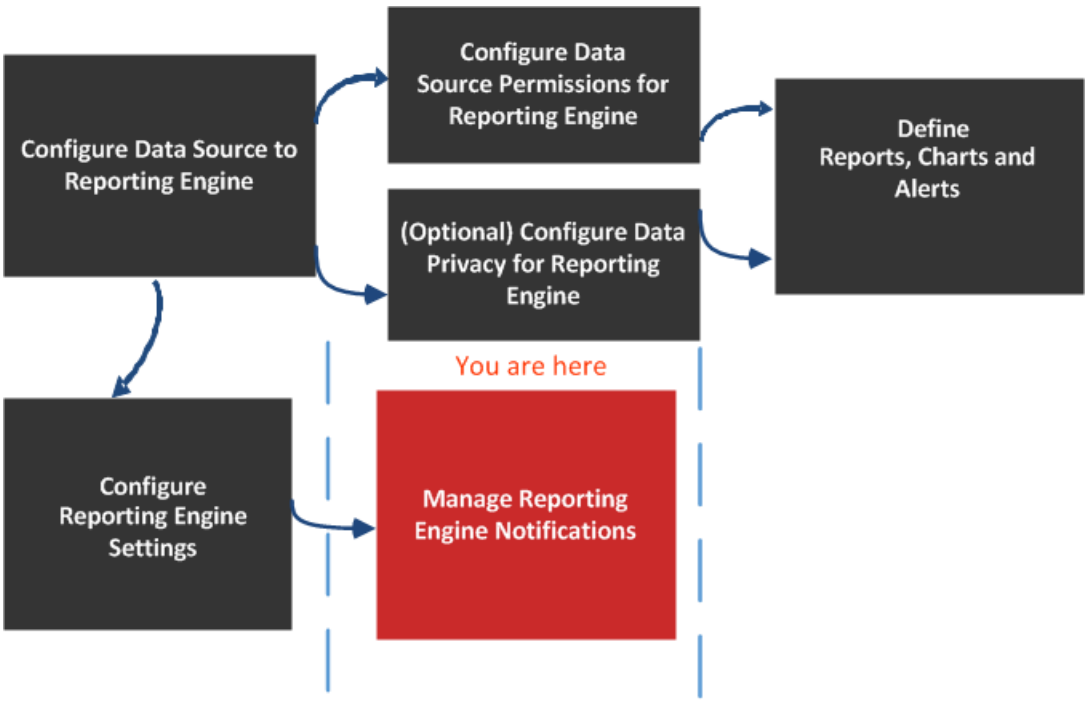
Que el archivo de configuración predeterminado de Kerberos se encuentre en `/etc/kbr5.conf` en Reporting Engine. Puede modificarlo para proporcionar detalles de dominios de Kerberos y otros parámetros relacionados con Kerberos.

Que se haya agregado el nombre de host (o el nombre de dominio calificado) y la dirección IP de los nodos de Horton Works y de Warehouse Connector al servidor DNS. Si el servidor DNS no está configurado, agregue el nombre de host (o nombre de dominio calificado) y la dirección IP de los nodos de Horton Works y Warehouse Connector al archivo `/etc/hosts` en el host en el cual está instalado el servicio Warehouse Connector.

Pestaña Orígenes

Los parámetros de configuración de servicios están disponibles en la pestaña Orígenes de la vista Configuración de servicios de Reporting Engine. La pestaña Orígenes del servicio Reporting Engine en la vista Configuración de servicios controla los orígenes de datos asociados con un Reporting Engine. La pestaña Origen consta de un único panel con una barra de herramientas y una cuadrícula que enumera los orígenes de datos asociados con Reporting Engine.

Flujo de trabajo



Función	Deseo…	Consulte…
Administrador	Configurar orígenes de datos en Reporting Engine	Configurar los orígenes de datos
Administrador	Configurar permisos de orígenes de datos para Reporting Engine	Configurar permisos de orígenes de datos

Función	Deseo…	Consulte…
Administrador	Configurar la privacidad de datos para Reporting Engine	Configurar la privacidad de datos para Reporting Engine
Administrador	Definir informes, gráficos y alertas	Definir informes, gráficos y alertas
Administrador	Configurar ajustes de Reporting Engine	Configurar ajustes de Reporting Engine
Administrador	Agregar, eliminar o editar un servicio nuevo o disponible*	Configurar los orígenes de datos
Administrador	Configurar un origen de datos como el valor predeterminado*	Configurar los orígenes de datos
Administrador	Configurar permisos de orígenes de datos*	Configurar permisos de orígenes de datos

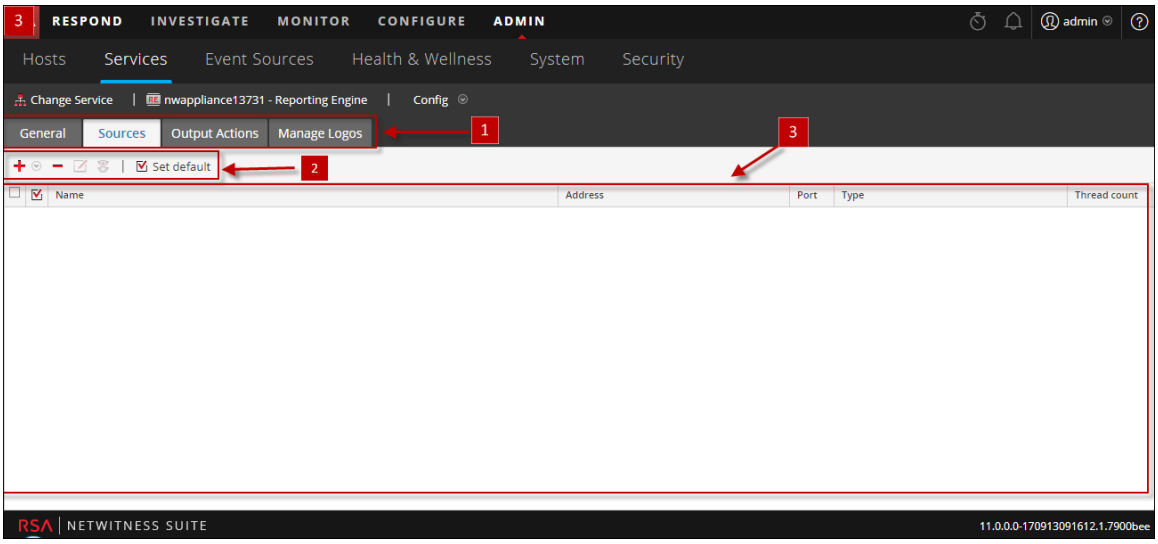
*Puede realizar estas tareas aquí.

Temas relacionados

- Cómo funciona Reporting Engine

Vista rápida

Este es un ejemplo de la pestaña Orígenes, en la cual se muestran los servicios disponibles.



1 Muestra todas las pestañas configurables disponibles.

2 Muestra los parámetros de configuración disponibles para el servicio seleccionado.

3 Muestra los parámetros de campos para el servicio seleccionado.

Los orígenes de datos disponibles en Reporting Engine para los cuales define informes, gráficos y alertas son los siguientes:

- **Orígenes de datos de NWDB**: los orígenes de datos de NetWitness Database (NWDB) son Decoders, Log Decoders, Brokers, Concentrators, Archiver y Collection.

  Nota: Cuando se implementa un plan de privacidad de datos para limitar el acceso a datos confidenciales en un origen de datos, debe configurar distintas cuentas de servicio en Reporting Engine para usuarios con privilegios y sin ellos. Para configurar distintas cuentas de servicio para la privacidad de datos, puede agregar más de un origen de datos NWDB. Este procedimiento está disponible en Configurar ajustes de Reporting Engine.

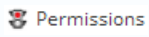
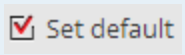
- **Orígenes de datos de Warehouse**: Los orígenes de datos de Warehouse son Horton Works y MapR.
- **Orígenes de datos de Respond**: Respond se usa para generar informes sobre alertas e incidentes. Los orígenes de datos de Respond son Reporting Engine, ESA, Malware, Endpoint y Web Threat Detection. Respond se utiliza para almacenar las alertas y los informes de incidentes.

Si define un origen como el origen de datos predeterminado, NetWitness Suite lo utiliza cuando usted crea informes y alertas, a menos que decida reemplazarlo por uno de los otros orígenes que aparecen en esta pestaña.

Nota: puede administrar el control de acceso a los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte Configurar ajustes de Reporting Engine.

Funciones

Puede realizar las siguientes acciones en la pestaña Orígenes:

Ícono	Acciones
	Esta opción agrega servicios nuevos como orígenes de datos para Reporting Engine. Agregue servicios existentes (Archiver, Workbench y Collection) como orígenes de datos para Reporting Engine.
	Esta opción quita los orígenes de datos de un Reporting Engine.
	Esta opción configura los permisos de orígenes de datos. Esto se habilita únicamente para los orígenes de datos NWDB y Warehouse. Para obtener más información, consulte Configurar permisos de orígenes de datos.
	Esta opción configura los orígenes de datos predeterminados para un Reporting Engine. Este es el origen que NetWitness Suite usa como valor predeterminado en el campo **Origen de datos** de las siguientes vistas: • Vista Definición de reglas. • Vista Crear/modificar alerta.

Los orígenes de datos de NetWitness Suite se enumeran bajo las distintas categorías como se indica a continuación:

- La categoría Orígenes de datos de NWDB muestra los orígenes de datos de NetWitness.
- La categoría Orígenes de datos de Warehouse muestra los orígenes de datos de Warehouse.

Columna	Descripción
	Si se hace clic en la casilla de verificación, se selecciona el origen de datos. Después de seleccionarlo, puede usar la barra de herramientas para quitar el origen o definirlo como predeterminado.
Nombre	Muestra el nombre del origen de datos.
Dirección	Muestra la dirección IP del origen de datos.
Puerto	Muestra el puerto del origen de datos.
Tipo	Muestra el tipo de servicio del origen de datos.
Conteo de hilos de ejecución	Muestra el tamaño del pool de subprocesos que se usa para ejecutar reglas en el origen de datos.

Pestaña Acciones de salida

Puede configurar acciones de salida para un Reporting Engine a fin de determinar el formato en que desea que se presenten los datos al usuario en función de sus requisitos. Los parámetros de configuración de servicios están disponibles en la pestaña Acciones de salida de la vista Configuración de servicios configurada para un informe o una ejecución de alerta. Esta pestaña consta de los siguientes paneles:

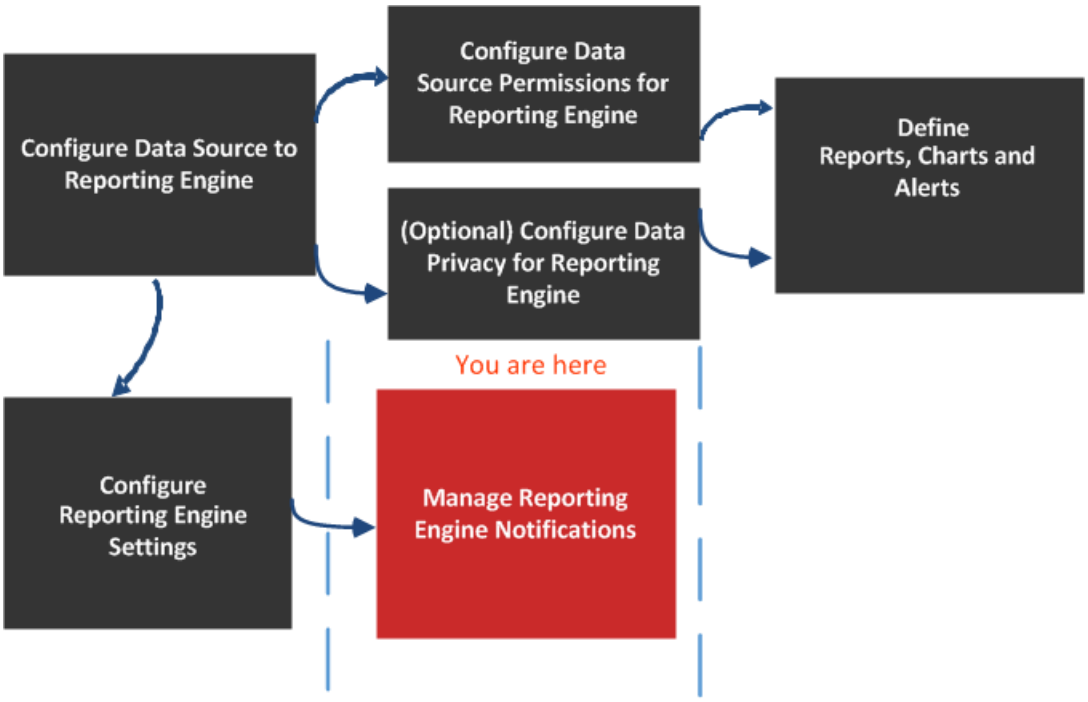
- Configuración de NetWitness Suite
- Protocolo simple de transferencia de correo (SMTP)
- Protocolo de administración de redes (SNMP)
- Syslog
- Protocolo simple de transferencia de archivos (SFTP)
- Localizador uniforme de recursos (URL)
- Recurso compartido de red

Por ejemplo, la acción de salida de syslog se usa específicamente para alertas de Reporting Engine, mientras que la acción de salida de SFTP, URL y recurso compartido de red, para informes de Reporting Engine.

Puede configurar el permiso requerido para acceder a esta vista en Administrar servicios.

Debe asegurarse de que el Reporting Engine esté en funcionamiento y que el origen de datos desde el cual desea generar un informe esté configurado en NetWitness Suite.

Flujo de trabajo



¿Qué desea hacer?

Función	Deseo…	Consulte...
Administrador	Configurar orígenes de datos en Reporting Engine	Configurar los orígenes de datos
Administrador	Configurar permisos de orígenes de datos para Reporting Engine	Configurar permisos de orígenes de datos
Administrador	Configurar la privacidad de datos para Reporting Engine	Configurar la privacidad de datos para Reporting Engine
Administrador	Definir informes, gráficos y alertas	Definir informes, gráficos y alertas

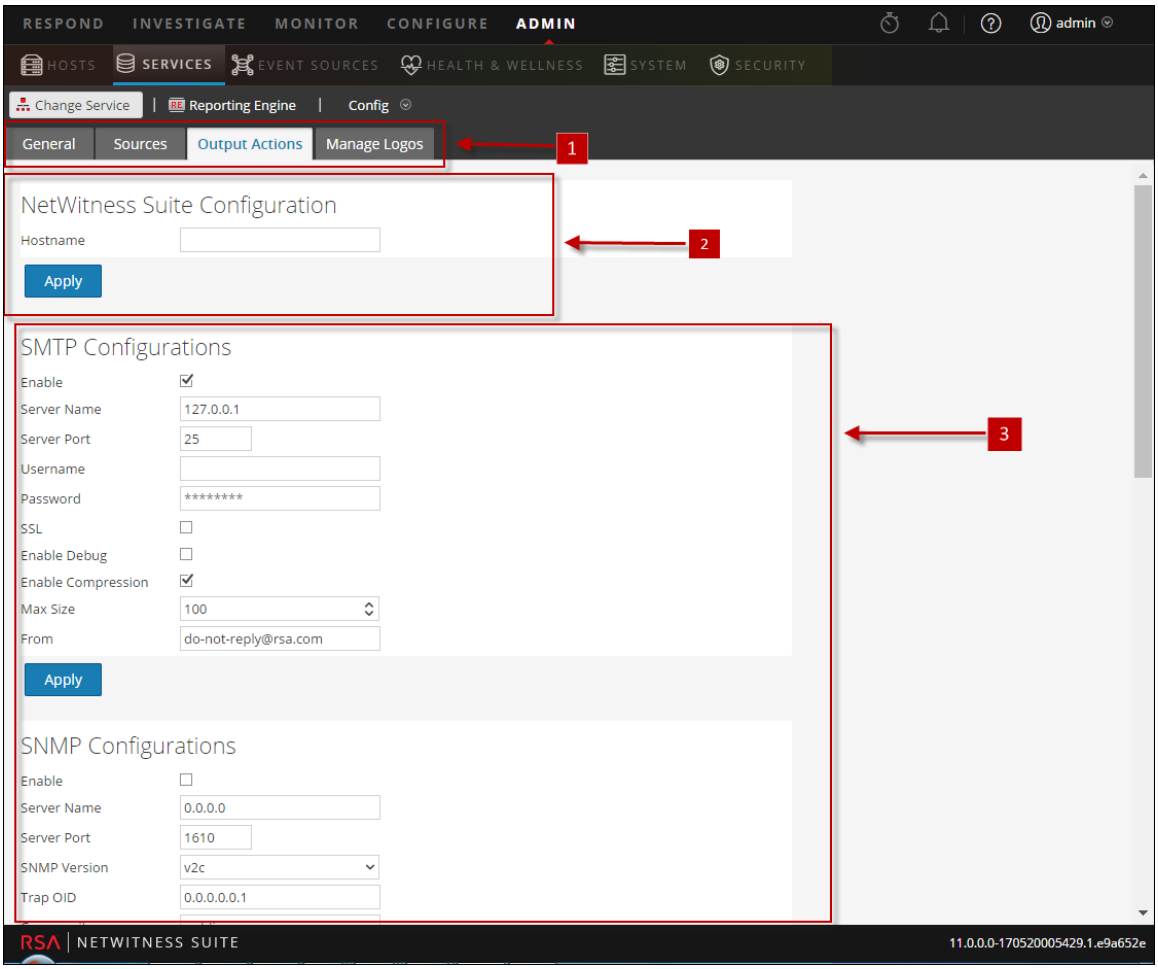
Función	Deseo…	Consulte...
Administrador	Configurar ajustes de Reporting Engine	Configurar ajustes de Reporting Engine
Administrador	Establecer la configuración de NetWitness Suite *	Configurar ajustes generales de Reporting Engine
Administrador	Establecer la configuración de SMTP*	Configurar ajustes generales de Reporting Engine
Administrador	Establecer la configuración de SNMP*	Configurar ajustes generales de Reporting Engine
Administrador	Establecer la configuración de syslog*	Configurar ajustes generales de Reporting Engine
Administrador	Establecer la configuración de SFTP*	Configurar ajustes generales de Reporting Engine
Administrador	Establecer la configuración de URL*	Configurar ajustes generales de Reporting Engine
Administrador	Establecer la configuración de recurso compartido de red*	Configurar ajustes generales de Reporting Engine

*Puede realizar estas tareas aquí.

Temas relacionados

- Cómo funciona Reporting Engine

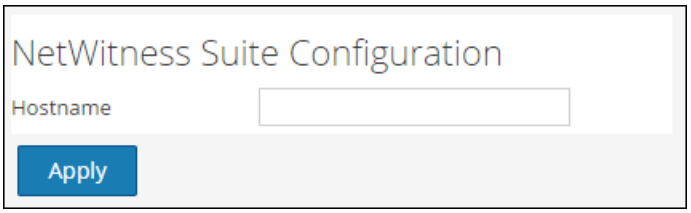
Vista rápida



1	Muestra todas las pestañas configurables disponibles.
2	Muestra el host de configuración de NetWitness Suite.
3	Muestra todos los tipos de acción de salida que se pueden configurar.

Configuración de NetWitness Suite

En la siguiente figura se muestra la configuración de NetWitness Suite en la pestaña Acciones de salida.



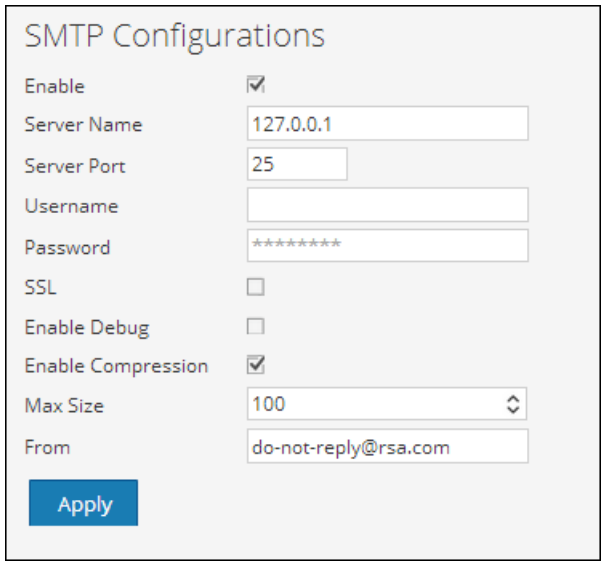
Los siguientes parámetros identifican el host de NetWitness Suite que está asociado con Reporting Engine.

Nombre	Valor de configuración
Nombre del host	Dirección IP o nombre del host del servidor de NetWitness Suite. Debe especificar este parámetro para todos los tipos de implementaciones, de modo que pueda hacer referencia a esta dirección con el fin de crear vínculos de investigación a NetWitness Suite desde informes, alertas, etc. NetWitness Suite utiliza este parámetro para generar correctamente: • Acción de salida de SMTP • Acción de salida de SNMP • Acción de salida de syslog • Acción de salida de SFTP • Acción de salida de URL • Acción de salida de recurso compartido de red • Hipervínculos para valores de metadatos en PDF de informes
Aplicar	Actualice la configuración.

SMTP

Cuando finaliza una ejecución, se envía una notificación por correo electrónico al usuario de acuerdo con la configuración de SMTP.

En la siguiente figura se muestra la configuración de SMTP en la pestaña Acciones de salida.



Los siguientes parámetros administran la configuración de las acciones de salida de SMTP (correo electrónico) para un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, se aplican valores predeterminados. Debe modificar los **valores de configuración** de estos parámetros según los requisitos de la empresa.

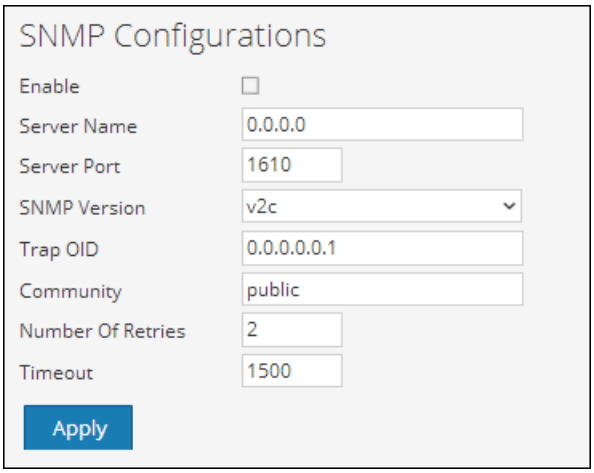
Nombre	Valor de configuración
Habilitar	Seleccione esta casilla para habilitar SMTP como una acción de salida para alertas e informes de este Reporting Engine. De forma predeterminada, este valor está habilitado.
Nombre del servidor	Especifique el nombre de host o la dirección IP del servidor donde se ejecuta el servidor SMTP de destino. El valor predeterminado es 0.0.0.0.
Puerto del servidor	Especifique el número de puerto del servidor SMTP. El valor predeterminado es 25.
Nombre de usuario	Especifique el nombre de usuario de la cuenta SMTP. El valor predeterminado es en blanco. Especificación de contraseña
Contraseña	Especifique la contraseña de la cuenta SMTP.
SSL	Seleccione esta casilla para usar la capa de conexión segura (SSL) para comunicarse con el servidor SMTP. El valor predeterminado es no usar SSL.

Nombre	Valor de configuración
Activar depuración	Seleccione esta casilla para habilitar la depuración. El valor predeterminado es no habilitar la depuración.
Activar compresión	Seleccione esta casilla para habilitar la compresión. La compresión está habilitada de forma predeterminada. Si se habilita este valor, los archivos de salida tendrán la extensión `.zip`.
Tamaño máximo	Especifique el tamaño máximo de los archivos adjuntos que se pueden enviar. El valor predeterminado es 100.
De	Especifique la dirección de correo electrónico desde la cual Security Analytics envía todos los mensajes. El valor predeterminado es `do-not-reply@rsa.com`.
Aplicar	Actualice la configuración.

SNMP

Cuando finaliza una ejecución, se envía una notificación trap al usuario de acuerdo con la configuración de SNMP.

En la siguiente figura se muestra la configuración de SNMP en la pestaña Acciones de salida.



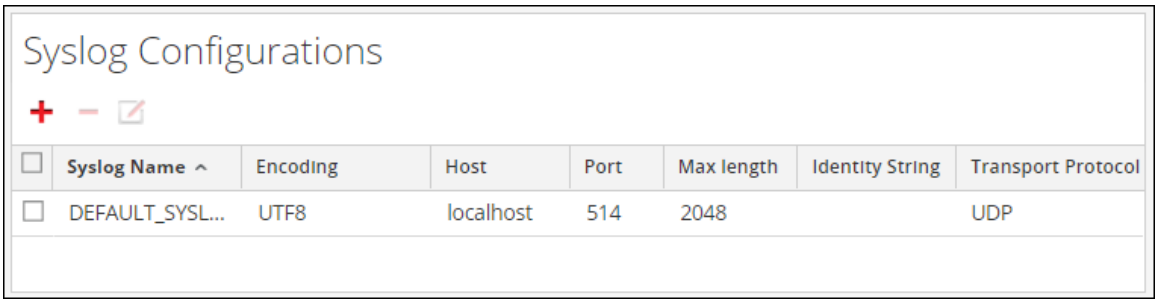
Los siguientes parámetros administran la configuración de las acciones de salida de SNMP (mensajes a servicios conectados en red) para un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, se aplican valores predeterminados. Debe modificar los **valores de configuración** de estos parámetros según los requisitos de la empresa.

Nombre	Valor de configuración
Habilitar	Seleccione esta casilla para habilitar la acción de salida de SNMP como salida para mensajes de alerta de este Reporting Engine. El valor predeterminado es Desactivar.
Nombre del servidor	Especifique el nombre de host o la dirección IP del servidor donde se ejecuta el servidor SNMP de destino. El valor predeterminado es **0.0.0.0**.
Puerto del servidor	Especifique el número de puerto del servidor en el cual el servidor SNMP de destino escucha las fallas y las excepciones. El valor predeterminado es **1610**.
Versión SNMP	Especifique el número de versión del protocolo SNMP que usa NetWitness Suite para enviar SNMP traps.
OID de traps	Especifique el número de identificación de objeto que identifica el tipo de trap que se envía. El valor predeterminado es **0.0.0.0.0.1**.
Comunidad	Especifique el grupo de SNMP al cual pertenece NetWitness Suite. El valor predeterminado es **público**.
Número de reintentos	Especifique la cantidad máxima de veces que NetWitness Suite intenta reenviar el mensaje de alerta a través de SNMP. El valor predeterminado es **2**.
Timeout	Especifique la cantidad de segundos después de los cuales se agota el tiempo de espera de NetWitness Suite (deja de intentar enviar alertas de SNMP). El valor predeterminado es **1,500**.
Aplicar	Actualice la configuración.

Syslog

Cuando finaliza una ejecución, todas las notificaciones se envían a través de mensajes de syslog a un host específico de acuerdo con la configuración de syslog. Es posible configurar múltiples servidores de syslog en el panel Configuración de syslog.

En la siguiente figura se muestra la configuración de syslog en la pestaña Acciones de salida.



Los siguientes parámetros administran la configuración de las acciones de salida de syslog para un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, puede definir valores para esta configuración de salida, ya que no hay valores predeterminados disponibles para esta configuración. Debe modificar los **valores de configuración** de estos parámetros según los requisitos de la empresa.

Nombre	Valor de configuración
Nombre de syslog	Nombre de la configuración de syslog. **Nota:** No puede crear una configuración de syslog con un nombre que ya exista en la lista de configuraciones de syslog de Reporting Engine.
Codificación	Especifique la codificación de internacionalización de los mensajes de syslog. El valor predeterminado es **UTF8**.
Nombre del servidor	Especifique el nombre de host o la dirección IP del servidor donde se ejecuta el proceso de syslog de destino. El valor predeterminado es en blanco.
Puerto del servidor	Especifique el número de puerto del servidor en el cual el servidor de syslog de destino escucha las fallas y las excepciones. El valor predeterminado es **514**.
Longitud máxima	Especifique el tamaño máximo (en bytes) de cada mensaje de alerta de syslog. El valor predeterminado es **2048**. Si **UDP** es el tipo de transporte y el tamaño de los mensajes de syslog es mayor de 1024 bytes, debe configurar un servidor de syslog que sea compatible con tamaños de mensaje mayores de 1024 bytes.

Nombre	Valor de configuración
Cadena de identidad	Especifique la cadena que NetWitness Suite inserta como prefijo en todos los mensajes de alerta de Syslog. El valor predeterminado es en blanco.
Incluir nombre de host local	Seleccione esta casilla para incluir el nombre de host local en todos los mensajes de alerta de Syslog. El valor predeterminado es no incluir el nombre de host local.
Truncar mensaje	Seleccione esta casilla para truncar todos los mensajes de alerta de syslog. El valor predeterminado es no truncar los mensajes de syslog.
Usar identidad	Seleccione esta casilla para usar el protocolo IDENT. El valor predeterminado es no usar este protocolo.
Incluir registro de fecha y hora local	Seleccione esta casilla para incluir el registro de fecha y hora local en todos los mensajes de alerta de Syslog. El valor predeterminado es no incluir registro de fecha y hora local.
Protocolo de transporte	Especifique el tipo de transporte para la entrega de mensajes de syslog. El tipo de transporte de syslog tiene tres partes: UDP, TCP y SECURE_TCP. El valor predeterminado es **UDP**.
Delimitador de mensaje de syslog	Especifique el delimitador para el mensaje de syslog. Hay tres delimitadores: CR, LF y CRLF. El valor predeterminado es **CR**. **Nota:** Este campose completa cuando selecciona TCP o SECURE_TCP como el protocolo de transporte.
Contraseña del área de almacenamiento de confianza	Especifique la contraseña del área de almacenamiento de confianza. **Nota:** este campo se completa cuando selecciona SECURE_TCP como el protocolo de transporte.

Nombre	Valor de configuración
Contraseña de área de almacenamiento de claves	Especifique la contraseña del área de almacenamiento de claves. **Nota:** este campo se completa cuando selecciona SECURE_TCP como el protocolo de transporte.
Aplicar	Guarde la configuración.

SFTP

Cuando finaliza una ejecución, puede enviar o transferir archivos a una ubicación remota de acuerdo con la configuración de SFTP.

En la siguiente figura se muestra la configuración de SFTP en la pestaña Acciones de salida.

Los siguientes parámetros administran la configuración de las acciones de salida de SFTP (transferencia de archivos a una unidad local) para un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, puede definir valores para esta configuración de salida, ya que no hay valores predeterminados disponibles para esta configuración. Debe modificar los **valores de configuración** de estos parámetros según los requisitos de la empresa.

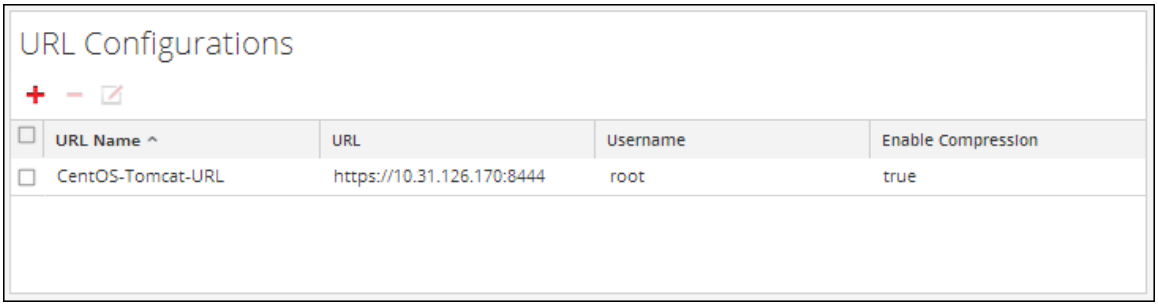
Nombre	Valor de configuración
Nombre de SFTP	Nombre de la configuración de SFTP. **Nota:** No puede crear una configuración de SFTP con un nombre que ya exista en la lista de configuraciones de SFTP de Reporting Engine.
Host	La dirección IP o el nombre de host del servidor de Reporting Engine asociado con la transferencia de archivos.
Puerto	Si desea usar un puerto distinto al predeterminado, ingrese un número de puerto. El valor predeterminado es **22**.

Nombre	Valor de configuración
Nombre de usuario	Especifique el nombre de usuario para la configuración de SFTP.
Contraseña	Especifique la contraseña para la configuración de SFTP.
Carpeta personalizada	Seleccione una ubicación de SFTP a la cual desea transferir el archivo. Puede usar la estructura de directorios predefinida de Windows o Linux en la ruta de carpetas personalizada. Por ejemplo, **/root/Downloaded_Files**. **Nota:** si el directorio no existe, RE lo creará en la ruta de carpetas personalizada y copiará los archivos en él.
Activar compresión	Seleccione esta casilla de verificación para activar la compresión. La compresión está habilitada de forma predeterminada. Si se habilita, los archivos de salida tendrán la extensión ".zip".

URL

Cuando finaliza una ejecución, los archivos de salida se publican en una dirección URL de acuerdo con la configuración de URL.

En la siguiente figura se muestra la configuración de URL en la pestaña Acciones de salida.



Los siguientes parámetros administran la configuración de las acciones de salida de URL (transferencia de archivos a una dirección URL) para un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, puede definir valores para esta configuración de salida, ya que no hay valores predeterminados disponibles para esta configuración. Debe modificar los valores de configuración de estos parámetros según los requisitos de la empresa.

Nombre	Valor de configuración
Nombre de URL	Nombre de la configuración de URL. **Nota:** No puede crear una configuración de URL con un nombre que ya exista en la lista de configuraciones de URL de Reporting Engine.
URL	Dirección URL asociada a la transferencia de archivos.
Nombre de usuario	Especifique el nombre de usuario para la configuración de URL.
Contraseña	Especifique la contraseña para la configuración de URL.
Activar compresión	Seleccione esta casilla de verificación para activar la compresión. La compresión está habilitada de forma predeterminada. Si se habilita, los archivos de salida tendrán la extensión ".zip".

Una vez configurada la dirección URL, los archivos se copiarán al directorio "URL_OUTPUT_ACTION" y los siguientes parámetros se enviarán al servidor junto con el archivo comprimido.

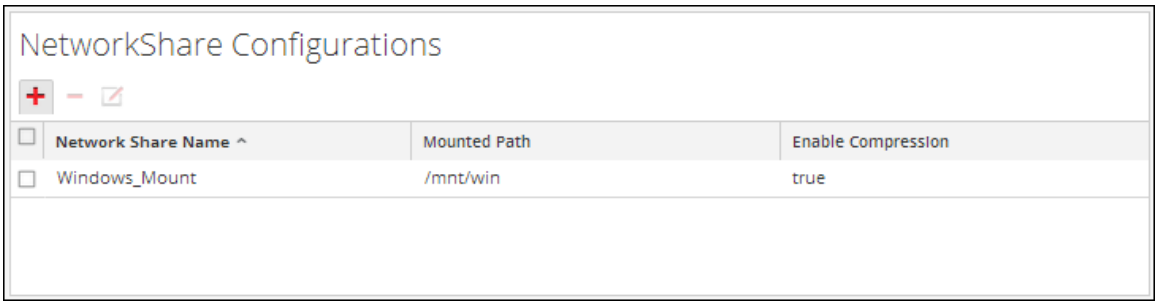
Nombre	Valor de configuración
filename	El nombre del archivo.
filesize	El tamaño del archivo en bytes.
filetype	El tipo de archivo asociado al archivo.
filechecksum	El número calculado a partir de un archivo que se puede usar para comprobar que es el que se espera y que se ha descargado y almacenado correctamente.
hashingalgorithm	El algoritmo hash que se usa para calcular la suma de verificación del archivo.
reportname	El nombre del informe descargado.
executionid	El ID de ejecución asociado con la ejecución del informe.
reportexecutionstarttime	La hora de inicio en que se ejecutó el informe.

Nombre	Valor de configuración
status	El estado de creación del informe.
status description	La descripción del estado.

Recurso compartido de red

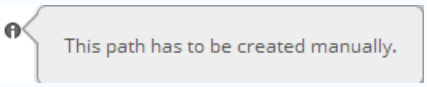
Cuando finaliza una ejecución, puede transferir los archivos de salida a una ruta montada o una ubicación compartida de acuerdo con la configuración del recurso compartido de red.

En la siguiente figura se muestra la configuración del recurso compartido de red en la pestaña Acciones de salida.



Los siguientes parámetros administran la configuración de las acciones de salida del recurso compartido de red (transferencia de archivos a una ubicación compartida en la red) para un servicio Reporting Engine. Cuando agrega un servicio Reporting Engine, puede definir valores para esta configuración de salida, ya que no hay valores predeterminados disponibles para esta configuración. Debe modificar los **valores de configuración** de estos parámetros según los requisitos de la empresa.

Nombre	Valor de configuración
Nombre de recurso compartido de red	El nombre del recurso compartido de red. **Nota:** No puede crear una configuración del recurso compartido de red con un nombre que ya exista en la lista de configuraciones del recurso compartido de red de Reporting Engine.

Nombre	Valor de configuración
Ruta montada	La ruta (ubicación) asociada a la transferencia de archivos. Puede usar la estructura de directorios predefinida de Linux en la ruta montada. Por ejemplo, **/mnt/win**. **Nota:** el usuario "rsasoc" debe tener acceso de lectura y escritura a la ruta montada del recurso compartido de red especificado.
	Haga clic para ver cómo se crea la ruta montada. Este cuadro emergente informa que debe crear manualmente la ruta montada.
Activar compresión	Seleccione esta casilla de verificación para activar la compresión. La compresión está habilitada de forma predeterminada. Si se habilita, los archivos de salida tendrán la extensión ".zip".

En la siguiente tabla se indican las operaciones comunes que se puede realizar en las secciones Syslog, SFTP, URL y Recurso compartido de red.

Operación	Descripción
	Crear una configuración de Syslog, SFTP, URL y Recurso compartido de red.
	Eliminar una configuración de Syslog, SFTP, URL y Recurso compartido de red.
	Editar una configuración de Syslog, SFTP, URL y Recurso compartido de red.

Pestaña Administrar logotipos

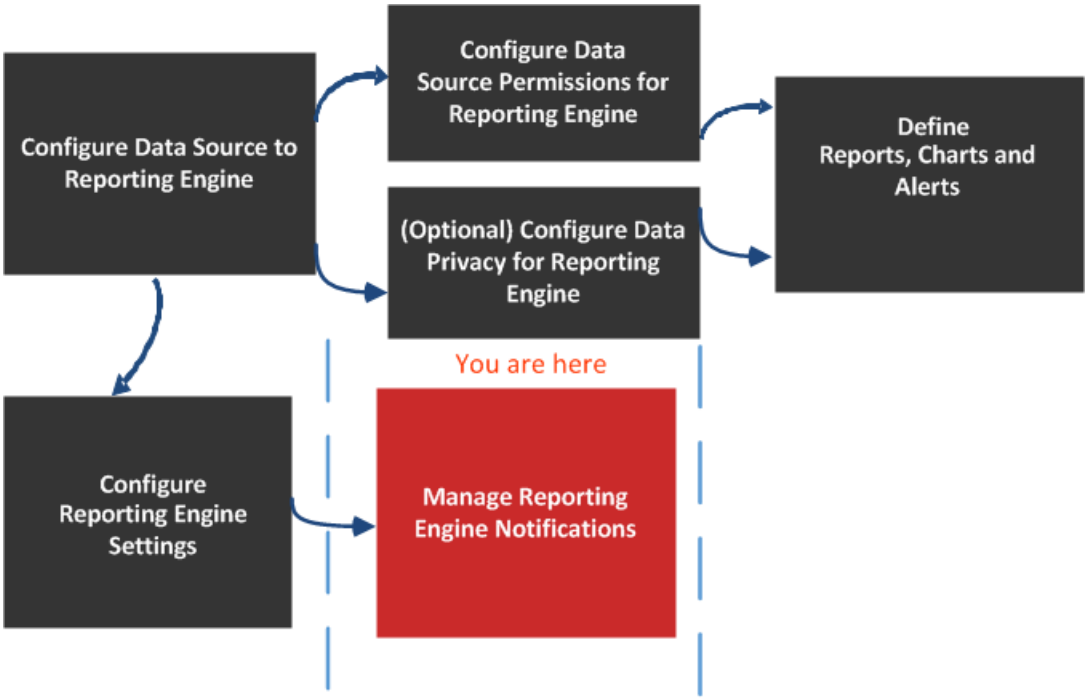
La opción Administrar logotipos disponible en la **vista Configuración de servicios** > pestaña **Administrar logotipos** permite administrar los logotipos asociados con el Reporting Engine. Esta pestaña consta de un único panel con una barra de herramientas y una cuadrícula que enumera los logotipos.

Puede cargar los logotipos que desea usar en el informe. Después de cargar el logotipo, puede establecer cualquier logotipo como logotipo predeterminado, el que se utilizará automáticamente en todos los informes programados. Cuando programa un informe, puede optar por reemplazar el logotipo predeterminado por cualquier otro enumerado en esta pestaña. Para obtener más información, consulte el tema “Cuadro de diálogo Seleccionar un logotipo” de la *Guía de Reporting*.

Los formatos de imagen compatibles son:

- .jpg
- .png
- .gif

Flujo de trabajo



¿Qué desea hacer?

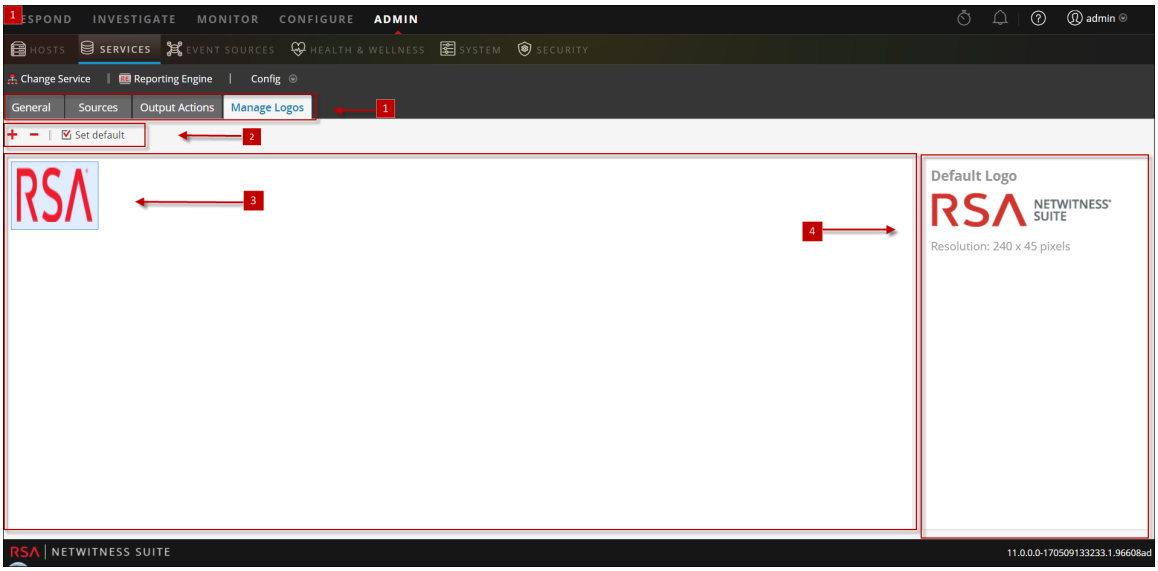
Función	Deseo…	Consulte…
Administrador	Configurar orígenes de datos en Reporting Engine	Configurar los orígenes de datos
Administrador	Configurar permisos de orígenes de datos para Reporting Engine	Configurar permisos de orígenes de datos
Administrador	Configurar la privacidad de datos para Reporting Engine	Configurar la privacidad de datos para Reporting Engine
Administrador	Definir informes, gráficos y alertas	Definir informes, gráficos y alertas
Administrador	Configurar ajustes de Reporting Engine	Configurar ajustes de Reporting Engine
Administrador/administrador del SOC	Agregar o eliminar logotipos*	Configurar ajustes generales de Reporting Engine
Administrador/administrador del SOC	Ver la lista de logotipos*	Configurar ajustes generales de Reporting Engine
Administrador/administrador del SOC	Configurar un logotipo como el valor predeterminado*	Configurar ajustes generales de Reporting Engine

*Puede realizar estas tareas aquí.

Temas relacionados

- Cómo funciona Reporting Engine

Vista rápida



Nota: El logotipo que se cargará no debe exceder los 500 KB. El permiso necesario para acceder a esta vista es Administrar servicios.

1. Muestra todas las pestañas configurables disponibles.
2. Muestra las acciones de edición.
3. Muestra todos los logotipos que se han utilizado.
4. Muestra el logotipo predeterminado utilizado.

Puede realizar las siguientes acciones en la pestaña Administrar logotipos.

Ícono	Acciones
+	Agregue nuevos logotipos desde el directorio local del sistema al Reporting Engine. **Nota:** El tamaño del logotipo no puede exceder los 500 KB. Los logotipos escogidos deben ser de los siguientes tipos de archivo: *.jpg *.gif *.png

Ícono	Acciones
	Elimina logotipos desde el Reporting Engine. **Nota:** Al realizar (Ctrl+clic), puede seleccionar múltiples logotipos para su eliminación.
	Establece el logotipo predeterminado para un Reporting Engine. Este es el logotipo que NetWitness Suite establece como predeterminado en el panel **Logotipo** de la vista Programar un informe. **Nota:** Si no se selecciona un logotipo predeterminado, se muestra el logotipo de RSA.