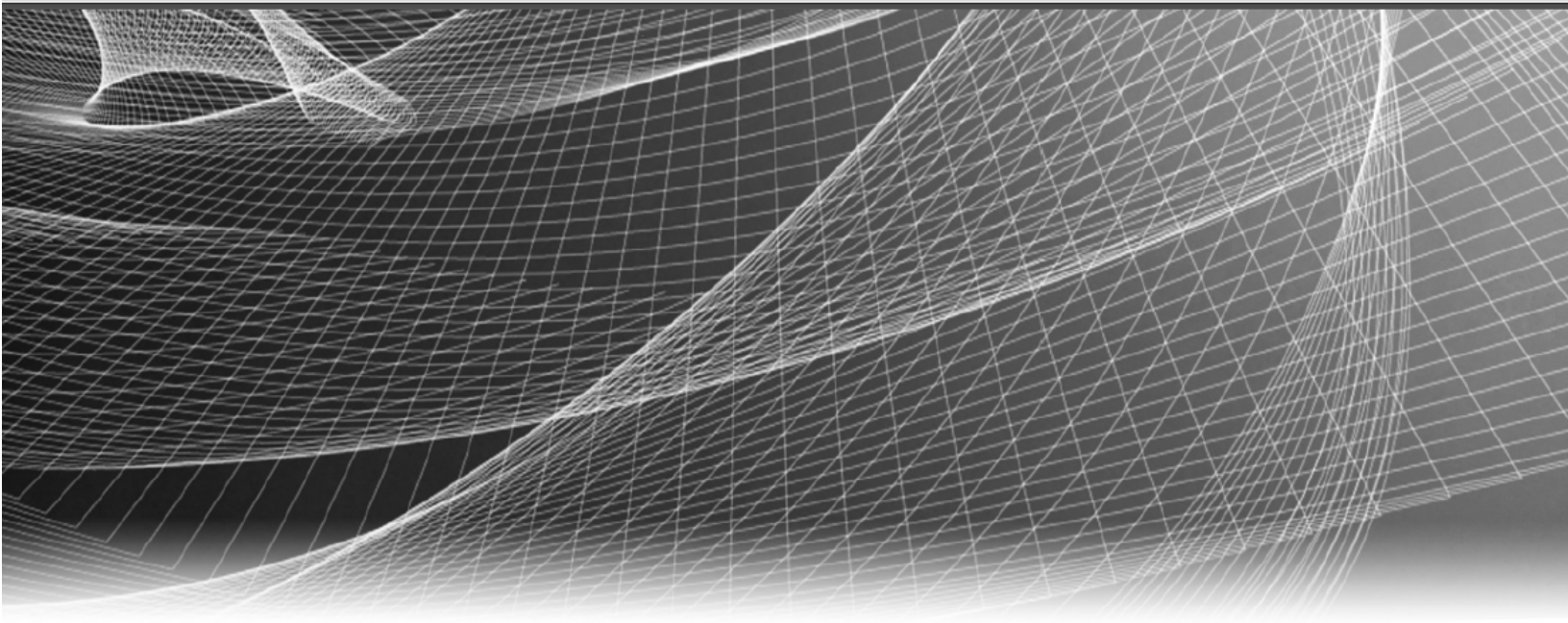


RSA Security Analytics

Warehouse Analytics

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Descripción general de Warehouse Analytics

En este tema se describe la manera en que los analistas de datos pueden analizar e identificar el indicador de riesgo (IOC) mediante el uso de datos de RSA Analytics Warehouse. Puede analizar datos de sesiones y registros en Warehouse con técnicas de ciencia de datos. Como analista de inteligencia de amenazas cibernéticas, puede ver informes de los primeros indicadores de riesgo. Los siguientes modelos de Warehouse Analytics son compatibles para datos de paquete:

- Dominios sospechosos
- Actividad de DNS sospechosa
- Perfil de host

Extraer, transformar y cargar (ETL) trabajos

El trabajo de ETL ejecuta un proceso de back-end en Warehouse y procesa previamente los datos que pueden usar los modelos. Se ejecuta automáticamente a diario a la hora indicada en los datos de paquetes. En esta versión, el módulo maneja los datos de paquetes. La salida del trabajo de ETL se usa como la entrada de los modelos Dominios sospechosos, Actividad de DNS sospechosa y Perfil de host. Debe importar los trabajos más recientes para todos los modelos desde Live.

Cuando se ejecuta por primera vez, el trabajo de ETL procesa datos de los últimos 14 días (en la zona horaria UTC) y, a continuación, datos del día anterior (en la zona horaria UTC). Si desea ejecutar los trabajos de ETL para cualquier otro rango de fechas, puede usar la opción “Trabajo de prueba”.

Nota: No puede usar trabajos de ETL para generar ningún informe visible. Si el trabajo de ETL falla por primera vez, puede utilizar el “trabajo de prueba” para volver a procesar los datos para ese rango de tiempo.

Dominios sospechosos

El modelo Dominios sospechosos identifica dominios maliciosos o sospechosos en función de su comportamiento comunicacional. Utiliza un enfoque automático impulsado por los datos que es reactivo y está diseñado para identificar la actividad de riesgo que es probable que se pierda por otras soluciones, basadas en firmas. Este modelo genera perfiles que describen los comportamientos de los dominios y aplica un método de evaluación de riesgos basado en probabilidades en estos perfiles para revelar los dominios más sospechosos. Con estos puntajes, puede encontrar los dominios que son más susceptibles de utilizarse para actividad maliciosa dentro de la red.

Puede ver un informe con la siguiente información:

- Lista de dominios de destino de alto riesgo y una clasificación de todos los dominios observados según el nivel de anomalía
- Un informe completo que explica por qué cada dominio es de alto riesgo
- Puntaje de riesgo de cada dominio
- Puntaje de riesgo unificado del dominio en relación con todos los dominios y basado en el análisis multidimensional de funciones de la conexión.

De acuerdo con esta información, puede investigar más a fondo, bloquear y recomendar cambios en las políticas de seguridad para evitar futuras apariciones de estas conexiones. También puede generar listas negras de dominios locales propias y utilizarlas en la investigación de incidentes o para definir una nueva política de seguridad que impida que sus activos se conecten a dominios maliciosos similares en el futuro.

Actividad de DNS sospechosa

El modelo Actividad de DNS sospechosa puede identificar dominios maliciosos en función de un patrón de comunicación DNS específico, común a botnets. El módulo utiliza un método automático para identificar los dominios que muestran un patrón de alojamiento, en el cual la dirección IP de los dominios maliciosos está en constante cambio. Este patrón se encuentra en botnets, hosts con balanceo de carga y redes de distribución de contenido (CDN), y este modelo puede diferenciar entre ellos y detectar exclusivamente los dominios maliciosos. Una vez que se identifica el dominio, es posible aislar el host que hace las solicitudes y bloquear el acceso a la red.

Puede ver un informe con la siguiente información:

- Lista de dominios que muestran DNS de flujo rápido sospechoso con un puntaje de riesgo asociado.

- Gráfico de la comunicación de CDN asociada con un puntaje que indica si el dominio muestra o no el patrón de flujo rápido.

Perfil de host

El modelo Perfil de host recopila y resume toda la actividad de HTTP, HTTPS y DNS de cada host interno en los datos de red. El módulo permite una investigación rápida de los diferentes tipos de patrones de uso por parte del host y entrega al analista respuestas a las preguntas que podrían surgir durante una investigación que requiere múltiples consultas o comparaciones manuales.

Puede ver un informe con mapas de riesgos con códigos de colores para identificar el riesgo de tráfico de señalización relacionado con el host. También puede ver gráficos que proporcionan detalles sobre el tráfico.

Después de la generación del informe, puede realizar las siguientes tareas:

- Usar una lista negra para alertar y una lista blanca para no hacer caso de direcciones IP o dominios que son benignos.
- Crear incidentes de seguridad útiles a partir de alertas entrantes.
  - Integrar incidentes con un sistema de help desk de terceros para rastrear el proceso de corrección.
  - Integrarse con RSA Archer eGRC para la administración y corrección de incidentes.
- Usar el módulo Investigation para identificar las causas raíz.

Procedimientos requeridos

En este tema se describen todos los procedimientos requeridos para trabajar con Warehouse Analytics. Se presentan en el orden en que se deben completar.

Temas

Paso 1. Configurar Warehouse Analytics

En este tema se describe un flujo de trabajo general para configurar RSA Analytics Warehouse de modo que pueda realizar analítica avanzada en los datos. Para realizar analítica avanzada en Warehouse, habilite Warehouse en Reporting Engine.

Requisitos previos

Asegúrese de:

- RSA Analytics Warehouse está instalado y en ejecución.
- Warehouse Connector está configurado. Para obtener más información, consulte la *Guía de configuración de Warehouse Connector*.

Tareas

La siguiente tabla proporciona la lista de tareas necesarias para configurar Warehouse Analytics.

Paso	Proceso	Tarea/instrucciones
1	Agregar Warehouse como un origen de datos en Reporting Engine y seleccionar la casilla de verificación Activar trabajos.	Consulte el tema **Agregar orígenes de datos de Warehouse a Reporting Engine** de la *Guía de configuración de hosts y servicios*.
2	Configurar el acceso de los usuarios para Warehouse Analytics.	Consulte Paso 2. Administrar el acceso al módulo Warehouse Analytics.
3	Configurar modelos de Warehouse Analytics.	Consulte Paso 3. Configurar modelos de Warehouse Analytics.
4	Establecer configuraciones de Warehouse Analytics en Reporting Engine.	Consulte las secciones **Configuración de la salida de Warehouse Analytics** y **Configuración del modelo de Warehouse Analytics** en el tema Pestaña General de Reporting Engine de la *Guía de configuración de hosts y servicios*. **Nota:** Debe definir la "Configuración de la salida de Warehouse Analytics" para utilizar Warehouse Analytics. La "Configuración del modelo de Warehouse Analytics" es opcional.

Próximos pasos

Después de configurar RSA Analytics Warehouse, realice las siguientes tareas:

- Analizar los informes de Warehouse Analytics. Para obtener instrucciones, consulte Paso 4. Analizar un informe de Warehouse Analytics.
- Investigar los informes de Warehouse Analytics. Para obtener instrucciones, consulte Paso 5. Investigar un informe de Warehouse Analytics.

Paso 2. Administrar el acceso al módulo Warehouse Analytics

En este tema se describe cómo se puede configurar el acceso y los permisos para administrar el trabajo de Warehouse Analytics. El control de acceso para el módulo Warehouse Analytics se proporciona en el nivel del trabajo. Solo un usuario con el conjunto de permisos correcto puede ejecutar las tareas del módulo Warehouse Analytics. El administrador administra el control de acceso desde la pestaña **Administration > Seguridad > Funciones**.

Como administrador, debe asegurarse de que las funciones creadas para tareas específicas tengan acceso a todos los permisos más altos en la jerarquía de funciones.

Los trabajos están vinculados a un conjunto específico de funciones de usuario de modo que, cuando un usuario inicia sesión en Security Analytics, los únicos trabajos a los que puede acceder son los que le pertenecen. Los usuarios que pertenecen a una función de usuario con el permiso de acceso de “Lectura y escritura” tendrán derechos de acceso completos al trabajo. Además, el acceso se puede reforzar para que solo accedan a los trabajos quienes tengan el acceso de “Solo lectura”.

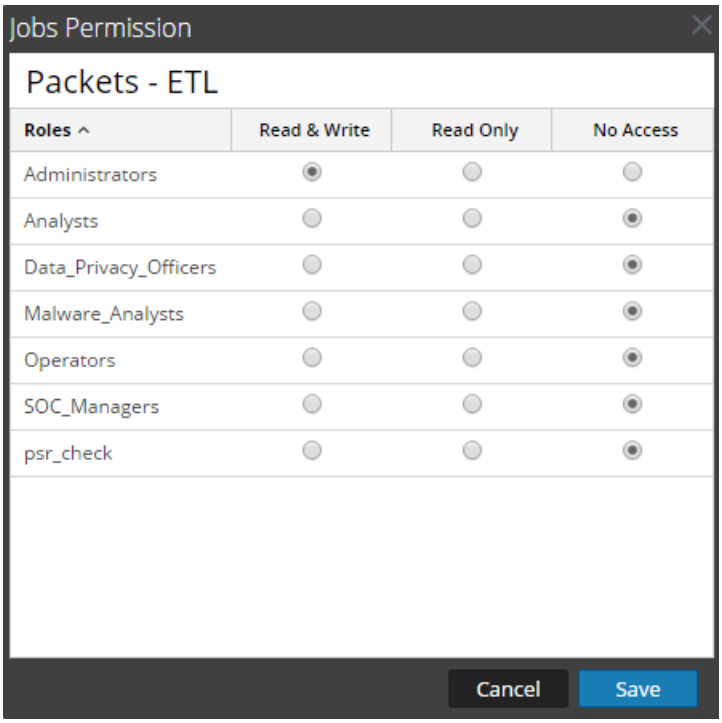
En el nivel del trabajo, puede establecer los siguientes permisos de acceso para las funciones de usuario en Security Analytics:

- Lectura y escritura
- Solo lectura
- Sin acceso

Control de acceso para un módulo de Warehouse Analytics

Cuando desee cambiar los permisos de trabajos, debe seleccionar un trabajo y establecer sus permisos de acceso mediante el panel Permiso de trabajos.

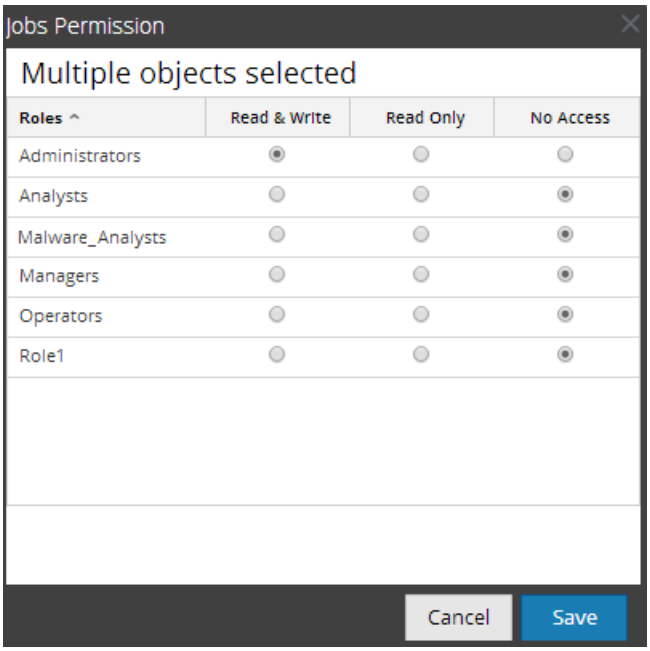
Excepto para los administradores, antes de que se apliquen permisos de trabajos, el conjunto de permisos predeterminado para todas las demás funciones de usuario es “Sin acceso”.



Si desea cambiar el permiso de acceso para una función de usuario específica, debe configurar esto en el nivel del trabajo.

Control de acceso para un trabajo cuando se seleccionan múltiples trabajos

Cuando desea cambiar los permisos de múltiples trabajos, puede seleccionar múltiples trabajos al mismo tiempo y configurar sus permisos de acceso en el panel Permiso de trabajos. El permiso de acceso que selecciona se aplica a todos los trabajos seleccionados.



Lista tabular

La siguiente tabla indica las diversas columnas del panel Permiso de trabajos:

Columna	Descripción
Funciones	La función del usuario que inició sesión en Security Analytics.
Lectura y escritura	El usuario puede acceder, ver, editar y eliminar trabajos en la vista Warehouse Analytics. El usuario también puede cambiar el permiso en el trabajo.
Solo lectura	El usuario solo puede acceder y ver el trabajo en la vista Warehouse Analytics
Sin acceso	El usuario no puede acceder ni ver el trabajo para la que se estableció este permiso.

Temas

- Agregar una función y asignar permisos para Warehouse Analytics
- Establecer el control de acceso para un trabajo de Warehouse Analytics

Agregar una función y asignar permisos para Warehouse Analytics

En este tema se describe cómo agregar una función y cómo asignarle permisos.

Funciones preconfiguradas

Aunque Security Analytics tiene cinco funciones preconfiguradas, puede agregar funciones personalizadas. Por ejemplo, además de la función Analistas preconfigurada, puede agregar las funciones personalizadas AnalystsEurope y AnalystsAsia.

Función	Permiso
Administradores	Acceso completo al sistema
Operadores	Acceso a configuraciones, pero no a datos
Analistas	Acceso a datos, pero no a configuraciones
SOC_Managers	El mismo acceso que poseen los analistas, además del permiso adicional para manejar incidentes
Malware_Analysts	Acceso solo a eventos de malware

Según la función de usuario, puede establecer los siguientes permisos de acceso para acceder al módulo Warehouse Analytics:

- Definir trabajos
- Eliminar trabajos
- Administrar trabajos
- Ver trabajos

Nota: Debe habilitar todos estos permisos para una función de usuario con el fin de poder definir, eliminar, administrar y ver trabajos.

Para obtener más información acerca de la lista de permisos, consulte el tema **Permisos de funciones** de la *Guía de administración de usuarios y de la seguridad del sistema*.

Agregar funciones

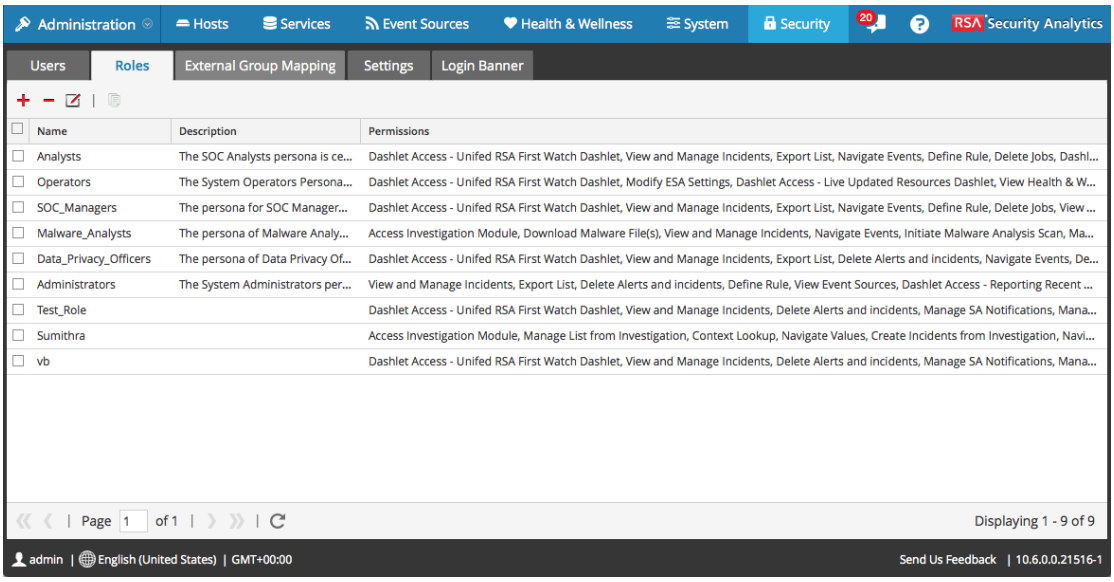
Para agregar funciones y asignar permisos en la pestaña Funciones:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Seguridad**.

   Se muestra la vista Seguridad de Administration.

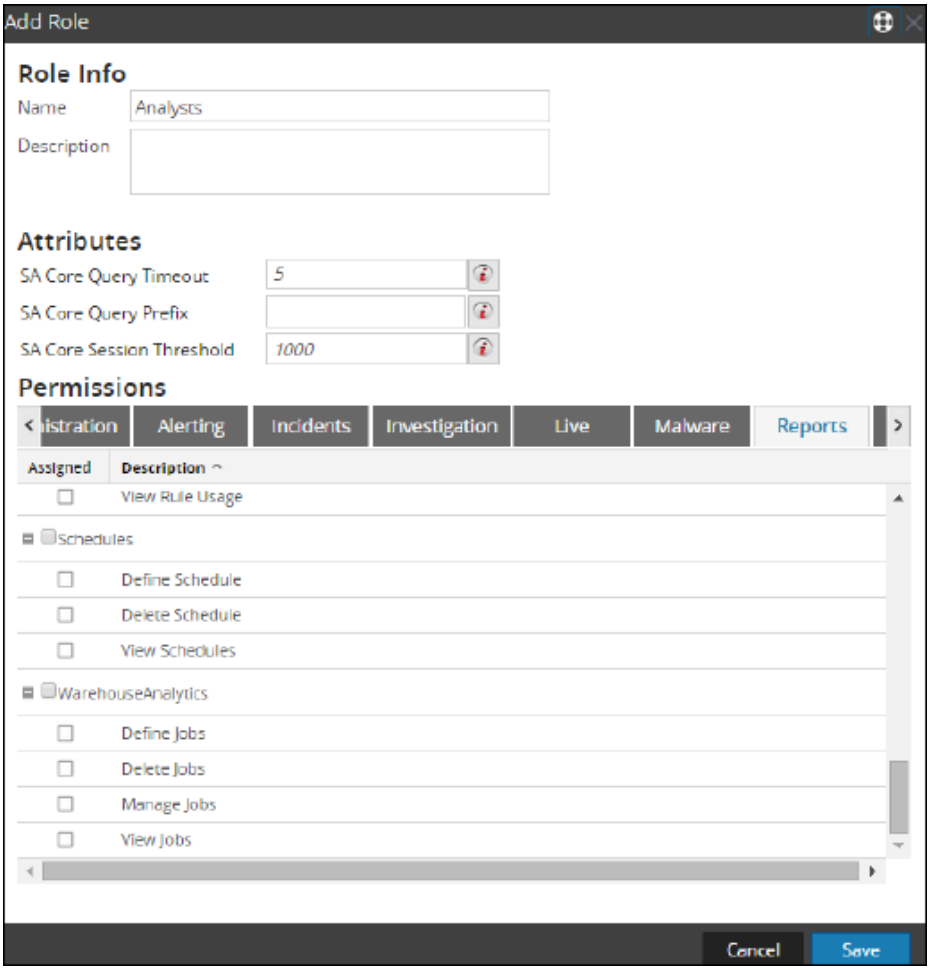
2. Haga clic en la pestaña **Funciones**.

   Se muestra la pestaña **Reglas**.



3. En la pestaña **Funciones**, haga clic en + en la barra de herramientas.

   Se muestra el cuadro de diálogo **Agregar función**.



4. En la sección **Información de función**, ingrese la siguiente información para la función:
    - **Nombre**
    - (Opcional) **Descripción**
5. En la sección **Permisos**, seleccione el módulo Informes al que accederá la función y elija cada permiso que tendrá la función.
6. Repita el paso 5 para seleccionar todos los permisos necesarios para la función.
7. Haga clic en **Guardar**.

Próximos pasos

Ahora puede asignar la nueva función a los usuarios.

Establecer el control de acceso para un trabajo de Warehouse Analytics

En este tema se proporcionan instrucciones para configurar el control de acceso para un trabajo de Warehouse Analytics.

Requisitos previos

Asegúrese de:

- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Comprender los permisos de acceso que tendrá el usuario según la función de usuario. Para obtener más información, consulte Paso 2. Administrar el acceso al módulo Warehouse Analytics.
- Tener un permiso de acceso de Lectura y escritura para configurar el acceso para un trabajo de Warehouse Analytics.

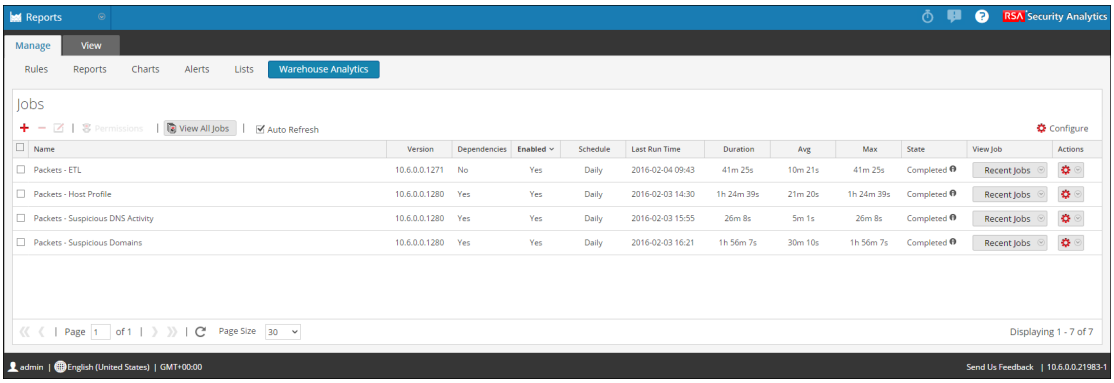
Establecer permisos de acceso

Para establecer permisos de acceso para un trabajo de Warehouse Analytics:

1. En el menú de Security Analytics, haga clic en **Informes**.

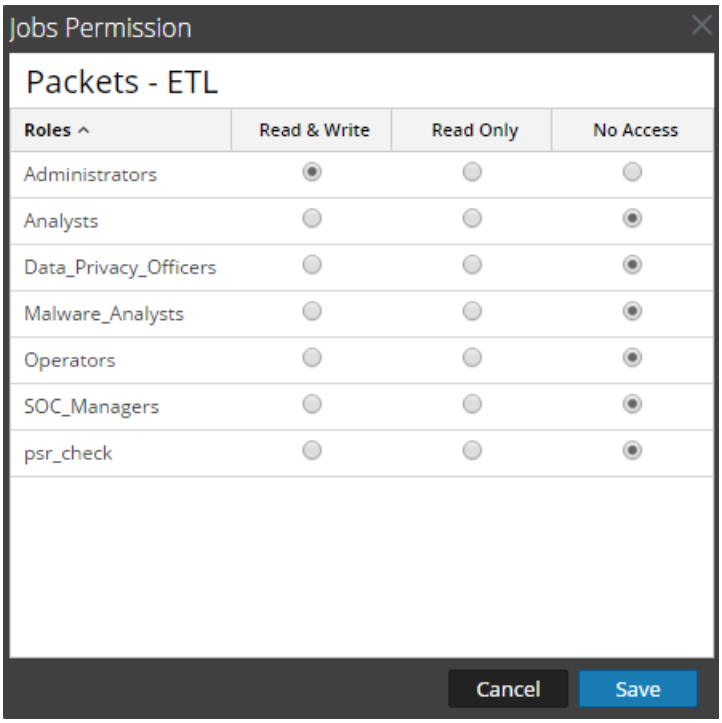
   Se muestra la pestaña Administrar.
2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. Seleccione un trabajo y haga clic en Permissions.

   Se muestra el cuadro de diálogo Permiso de trabajos.



4. Según la función de usuario, seleccione los botones de opción que correspondan.
5. Haga clic en **Guardar**.

   Se muestra un mensaje de confirmación que indica que el permiso se estableció correctamente para el trabajo seleccionado.

Paso 3. Configurar modelos de Warehouse Analytics

En este tema se proporcionan instrucciones para importar y definir modelos de Warehouse Analytics y calendarizarlos para ejecución. La vista Warehouse Analytics permite programar un trabajo para el modelo de Warehouse Analytics.

Requisitos previos

Asegúrese de:

- Haber comprendido los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Haber comprendido los componentes de la vista Definición de trabajo. Para obtener más información, consulte Vista Definición de trabajo.

Procedimiento

Para configurar modelos de Warehouse Analytics:

Paso	Proceso	Tarea/instrucciones
1	Descargar los modelos de Warehouse Analytics desde Live.	Consulte Implementar modelos de Warehouse Analytics
2	Definir el trabajo de Warehouse Analytics	Consulte Implementar modelos de Warehouse Analytics

Temas

- Implementar modelos de Warehouse Analytics
- Definir un trabajo de Warehouse Analytics
- Usar una lista blanca en un trabajo de Warehouse Analytics

Implementar modelos de Warehouse Analytics

En este tema se describe un flujo de trabajo general para descargar un modelo de Warehouse Analytics desde el servidor de RSA Live.

Requisito previo

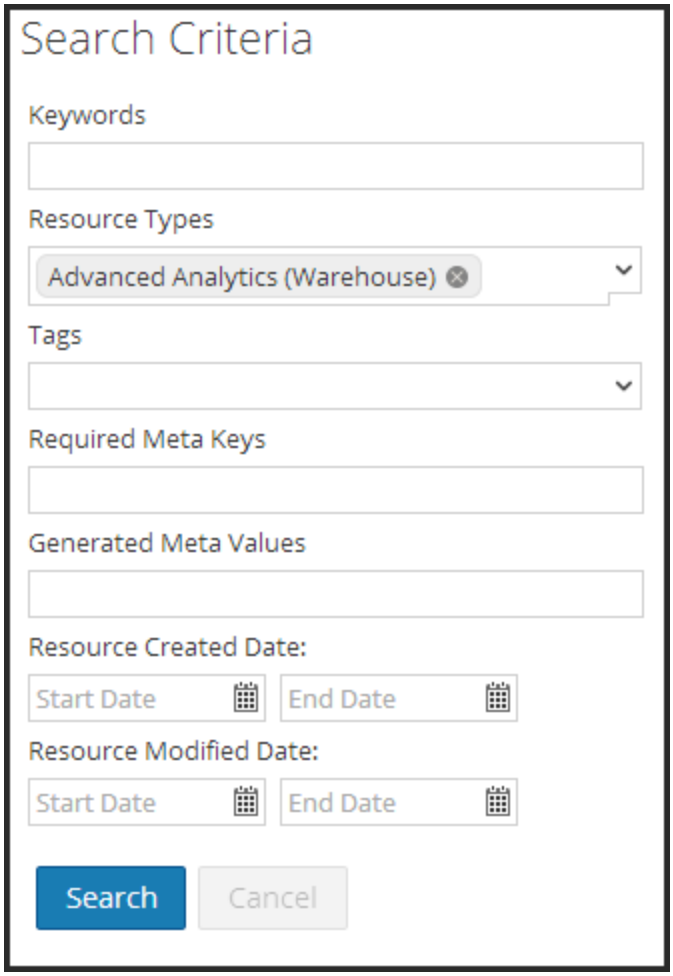
Asegúrese de haber realizado lo siguiente:

- Haber creado una cuenta de Live. Para obtener más información, consulte **Paso 1. Crear una cuenta de Live** en la *Guía de administración de servicios de Live*.
- Haber configurado la conexión y la sincronización entre el servidor de CMS y Security Analytics. Para obtener más información, consulte **Paso 2. Configurar Live en Security Analytics** en la *Guía de administración de servicios de Live*.

Implementar un modelo de Warehouse Analytics

Para implementar un modelo de Warehouse Analytics:

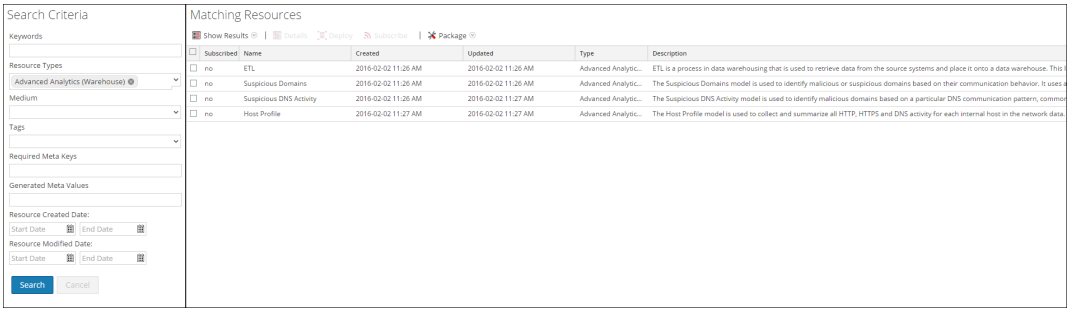
1. Busque un modelo de Warehouse Analytics.
   a. En el menú de Security Analytics, seleccione **Live > Buscar**.
   b. En el panel **Criterios de búsqueda**, especifique los criterios de búsqueda. En **Tipos de recursos**, seleccione **Analítica avanzada (Warehouse)**.



   c. Haga clic en **Buscar**.

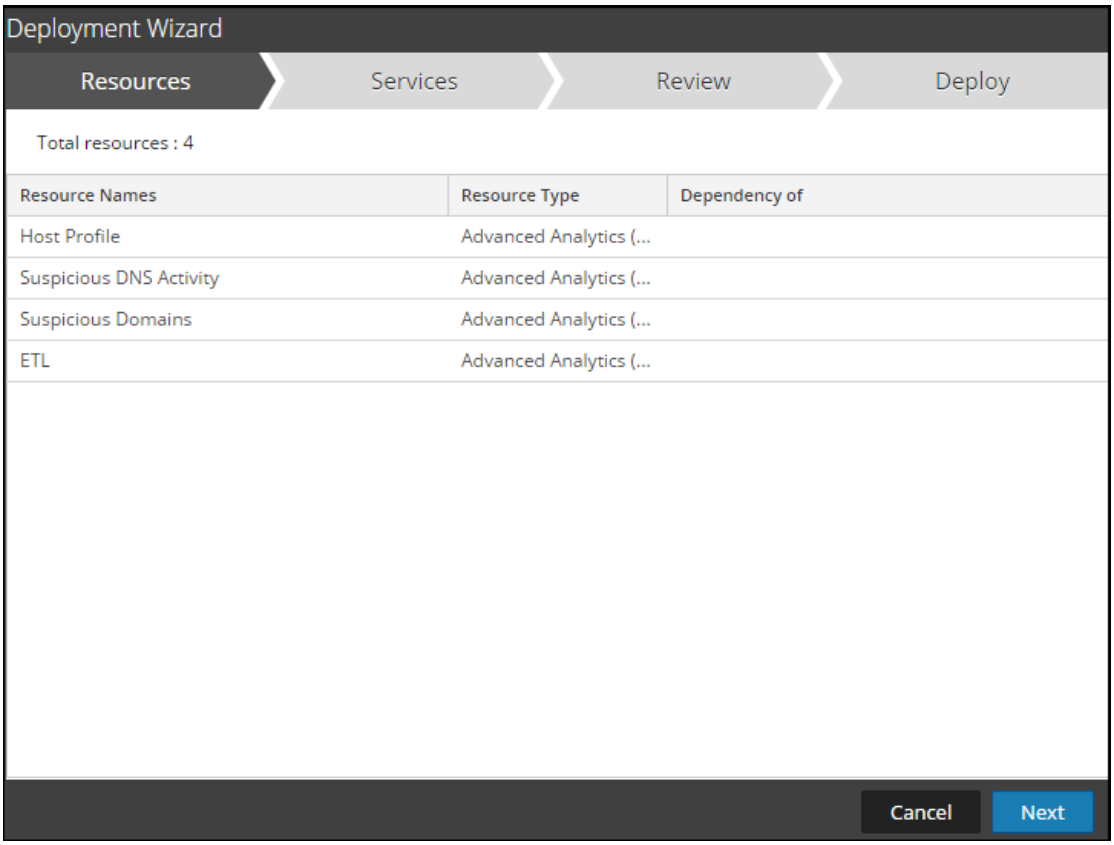
      Los modelos de Warehouse Analytics se enumeran como se muestra en el panel

Coincidencias de recursos.



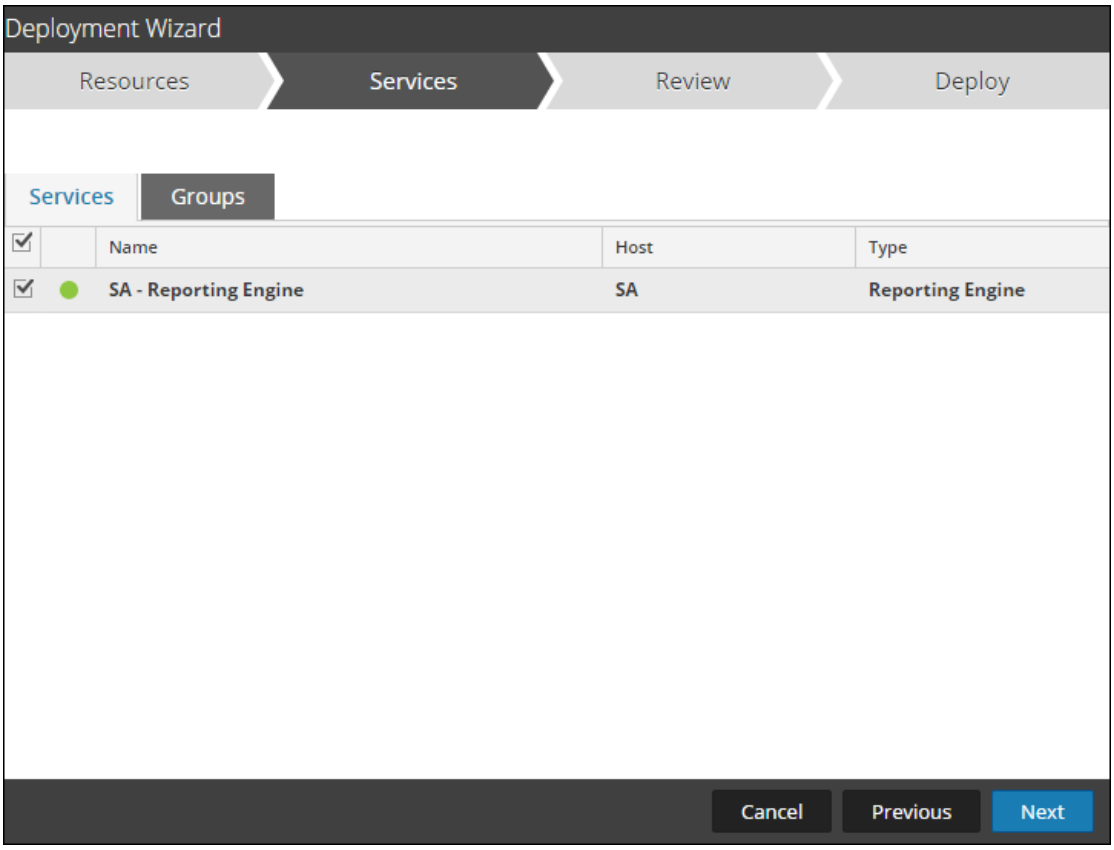
2. Seleccione el recurso deseado y haga clic en Deploy.

   Se muestra la página **Asistente de implementación**.



3. Haga clic en **Siguiente**.

   Se muestra la página **Servicios**.

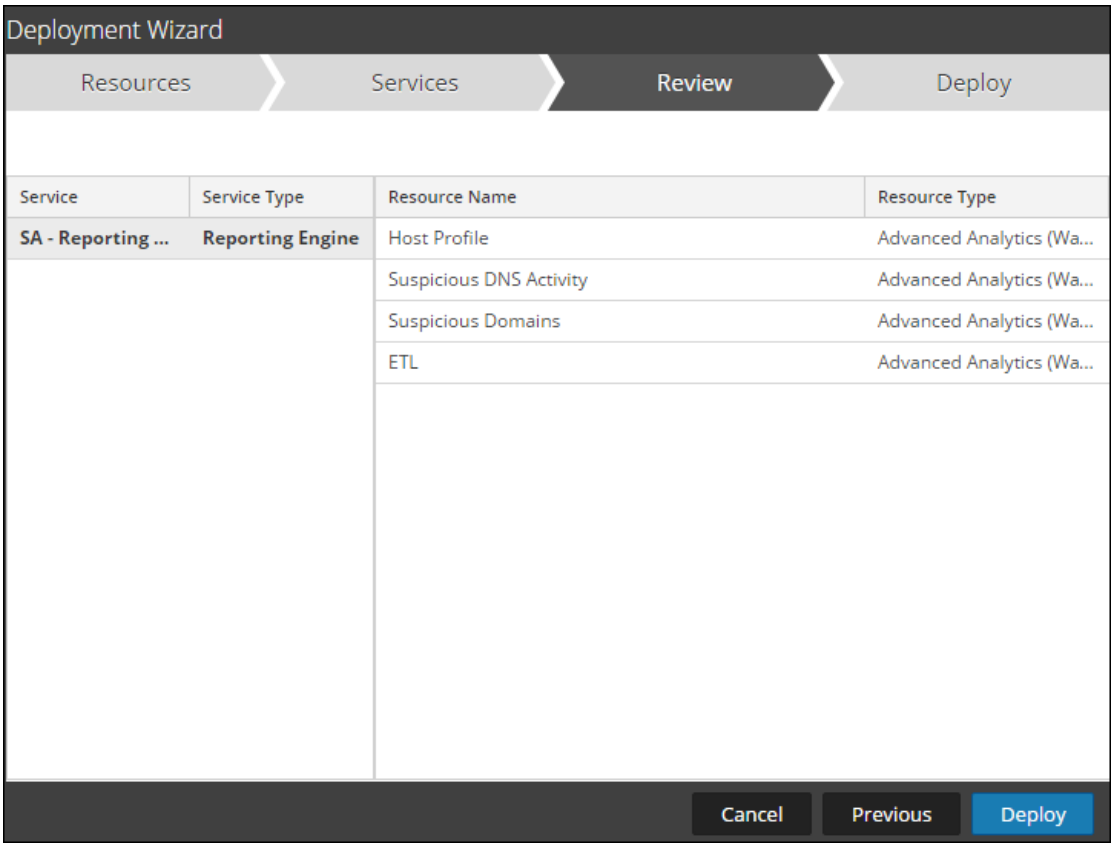


La página **Servicios** contiene dos pestañas, **Servicios** y **Grupos**. Estas pestañas proporcionan una lista de servicios y grupos de servicios que se configuran en la vista **Administration > Servicios**. Las columnas son un subconjunto de las columnas disponibles en la vista Servicios. Puede seleccionar una combinación de servicios y grupos de servicios, como se explica a continuación:

- Use la pestaña **Servicios** para seleccionar servicios individuales, la lista de servicios y grupos de servicios que se configuran en la vista Servicios de Administration.
- Use la pestaña **Grupos** para seleccionar grupos de servicios.

4. Haga clic en **Siguiente**.

   Se muestra la pestaña **Revisar**.



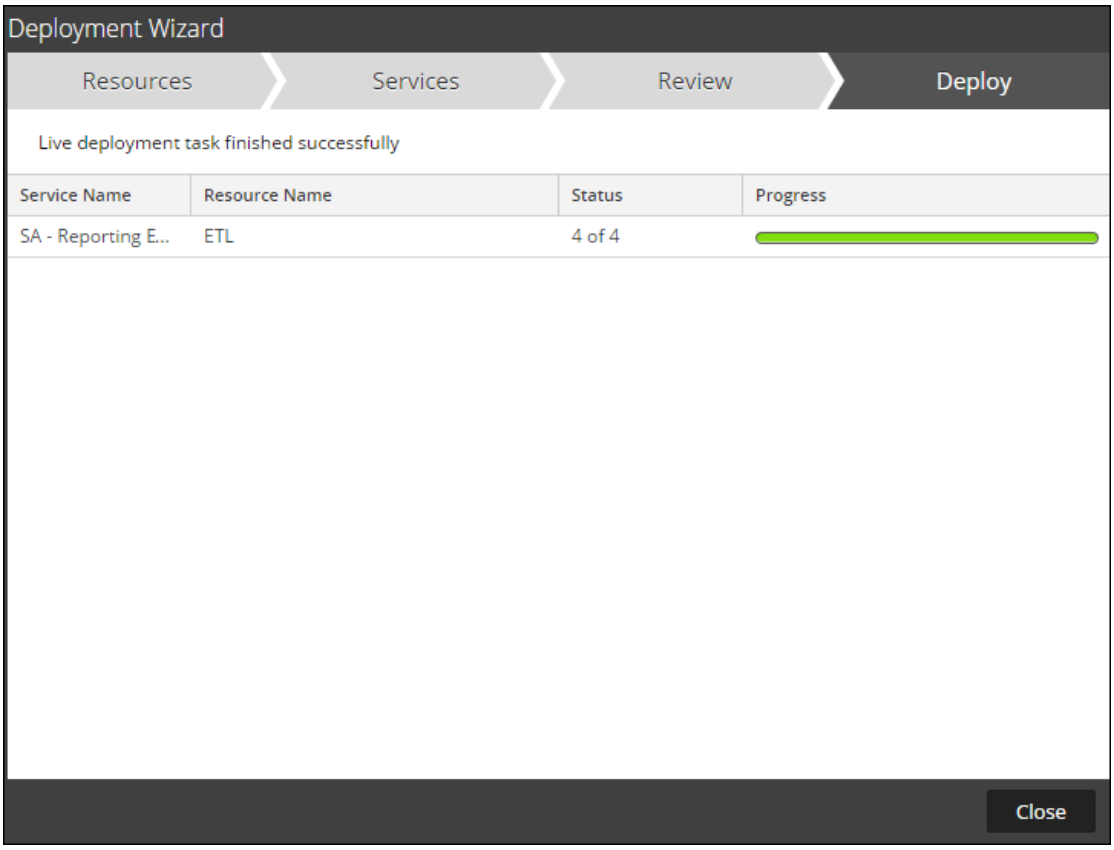
Nota: Asegúrese de haber seleccionado los recursos correctos y los servicios en los cuales desea implementarlos.

5. Haga clic en **Implementar** para iniciar la implementación de Live.

   La pestaña **Implementar** se muestra con la barra de progreso que indica el estado de la implementación de Live.

   Si intenta implementar recursos y servicios que no son compatibles, Security Analytics muestra los botones Errors y Retry en los cuales puede hacer clic para revisar los errores y volver a intentar la implementación.

   Cuando se completa la implementación, se muestra el siguiente mensaje y la barra se vuelve verde: "**La tarea de implementación de Live finalizó correctamente**".



6. Haga clic en **Close**.

Definir un trabajo de Warehouse Analytics

En este tema se proporcionan instrucciones para definir y programar un trabajo. Para definir un trabajo de Warehouse Analytics, primero debe importar el modelo de Warehouse Analytics desde RSA Live y, a continuación, programar el trabajo.

Requisitos previos

Asegúrese de haber comprendido lo siguiente:

- Implementación de modelos de Warehouse Analytics desde Live. Para obtener más información, consulte Implementar un modelo de Warehouse Analytics.

  Nota: Se recomienda implementar siempre los modelos de Warehouse Analytics desde Live.

- Los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.

- Los componentes de la vista Definición de trabajo. Para obtener más información, consulte Vista Definición de trabajo.

Agregar y programar un trabajo

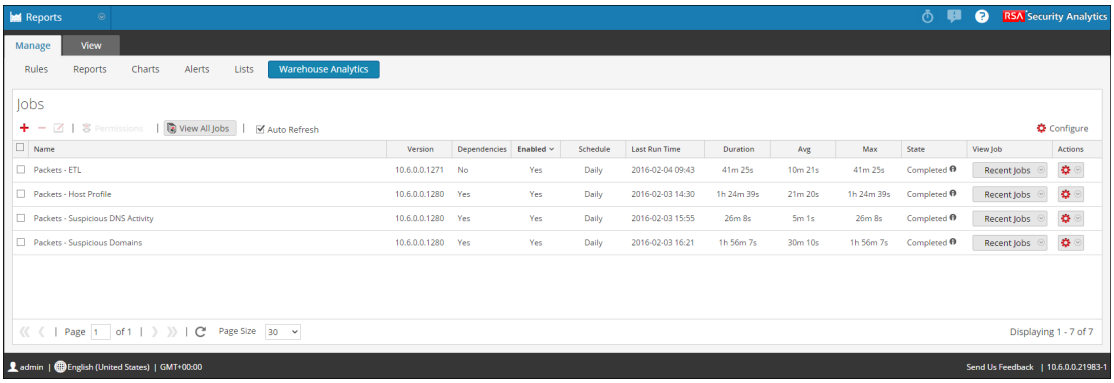
Para agregar y programar un trabajo:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En la barra de herramientas de Warehouse Analytics, haga clic en +.

   Se muestra la pestaña Definición de trabajo.

4. Para ejecutar los trabajos según el calendario, seleccione la casilla de verificación **Activar**.
5. En el campo **Nombre**, escriba un nombre para la configuración del trabajo.
6. En el campo **Modelo**, haga clic en **Navegar** para seleccionar el archivo jar que importará.

   Security Analytics proporciona una vista del sistema de archivos.

7. Busque el archivo jar y haga clic en **Abrir**.

   El archivo se agrega a la vista Definición de trabajo.

8. En el campo **Warehouse**, seleccione el origen de datos que se creó en la página de configuración de Reporting Engine. (Por ejemplo, Pivotal o MapR).
9. Realice una de las siguientes acciones

   - Para una cantidad específica de días, seleccione el rango de fechas para ejecutar la consulta de acuerdo con la opción **Pasado**

- Para un intervalo de tiempo específico, especifique las fechas **De** y **Hasta** en el calendario

Nota: Cuando actualiza a 10.6, los trabajos para los modelos Dominios sospechosos, Actividad de DNS sospechosa y Perfil de host están obsoletos e inhabilitados. Estos aparecen en la pestaña **Administrar > Warehouse Analytics** como trabajos "OBSOLETOS" y se pueden usar como referencia para crear nuevos trabajos.

10. En el campo **Opciones avanzadas** , realice lo siguiente:
    - En el campo **Parámetros de modelo**, escriba los parámetros de modelo o trabajo de DS de la ventana Selección de lista. Para obtener más información sobre el uso de una lista blanca, consulte Usar una lista blanca en un trabajo de Warehouse Analytics
    - En el campo **Parámetros de HDFS**, escriba los parámetros de configuración de HDFS.
    - En el campo **Parámetros de MapReduce**, escriba los parámetros de configuración de Hadoop o MapR.
    - En el campo **Parámetros de SandBox JVM**, escriba los parámetros de JVM o del sistema "-D" para que JVM ejecute el modelo DS.

    Nota: Al cargar el trabajo, varios parámetros importantes se completan automáticamente. Si no se especifican parámetros, el trabajo se ejecuta con los valores predeterminados.
11. Haga clic en **Guardar**.

    Warehouse Analytics ejecuta el trabajo según lo programado y proporciona las salidas configuradas.

Próximos pasos

Puede ver el trabajo programado en la vista Warehouse Analytics.

Usar una lista blanca en un trabajo de Warehouse Analytics

En este tema se proporcionan instrucciones para usar listas blancas en un trabajo de Warehouse Analytics. Puede usar una lista blanca en un trabajo de Warehouse Analytics, de modo que los dominios que no son sospechosos se puedan omitir durante el procesamiento. Puede usar listas blancas solo en los informes Dominios sospechosos y Actividad de DNS sospechosa.

Requisitos previos

Asegúrese de:

- Haber creado la lista blanca. Por ejemplo, una lista de dominios confirmados como no sospechosos o una lista blanca de dominios en los cuales no ocurren actividades de DNS.

Para obtener más información acerca de la creación de una lista, consulte el tema Agregar una lista en la *Guía de Reporting*.

- Haber descargado los trabajos de Warehouse Analytics del servidor de Live. Para obtener más información, consulte Implementar modelos de Warehouse Analytics.

- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.

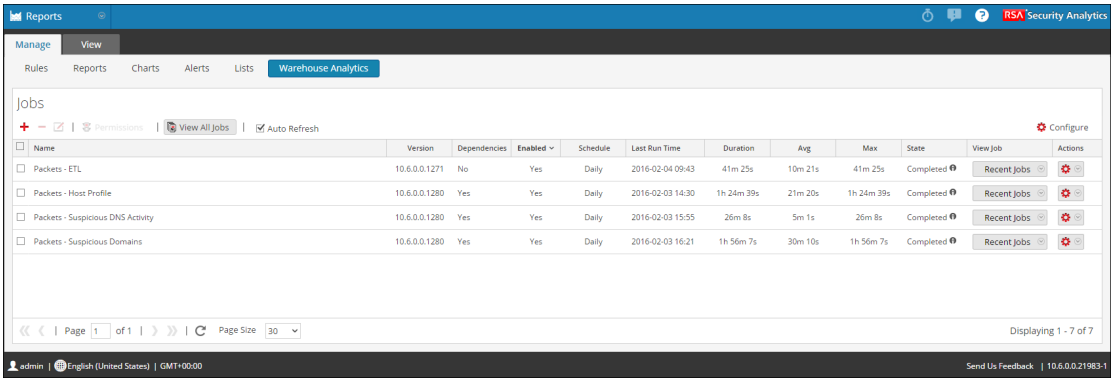
- Comprender los componentes de la vista Definición de trabajo. Para obtener más información, consulte Vista Definición de trabajo.

Procedimiento

Realice los siguientes pasos para agregar y programar un trabajo para ejecución:

1. En el menú de Security Analytics, haga clic en **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.
   Aparece la vista Warehouse Analytics.



3. En la barra de herramientas de Warehouse Analytics, haga clic en +.
   Se muestra la pestaña Definición de trabajo.

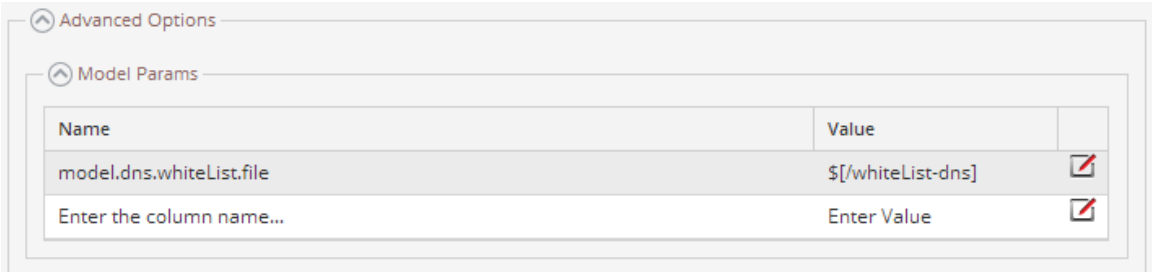
4. Definir el trabajo y el calendario. Para obtener más información, consulte Paso 3. Configurar modelos de Warehouse Analytics.

5. En **Opciones avanzadas:**

    1. En el campo **Parámetros de modelo**, ingrese los parámetros que desea incluir en la lista blanca.

    - Para el modelo Dominios sospechosos, ingrese el nombre del parámetro como **model.suspiciousDomains**.whiteList.file y seleccione la lista mediante . Para obtener más información, consulte Analizar un informe de dominios sospechoso.

    - Para el modelo Actividad de DNS sospechosa, ingrese el nombre del parámetro como **model.dns.whiteList.file** y seleccione la lista mediante . Para obtener más información, consulte Analizar un informe Actividad de DNS sospechosa.



6. Haga clic en **Guardar**.
   Warehouse Analytics ejecuta el trabajo programado y proporciona las salidas configuradas.

Paso 4. Analizar un informe de Warehouse Analytics

En este tema se abordan todas las instancias de análisis de un informe de Warehouse Analytics. Los módulos Warehouse Analytics ofrecen a los analistas informes de los primeros indicadores de riesgo. Los siguientes informes de Warehouse Analytics se pueden analizar en Security Analytics:

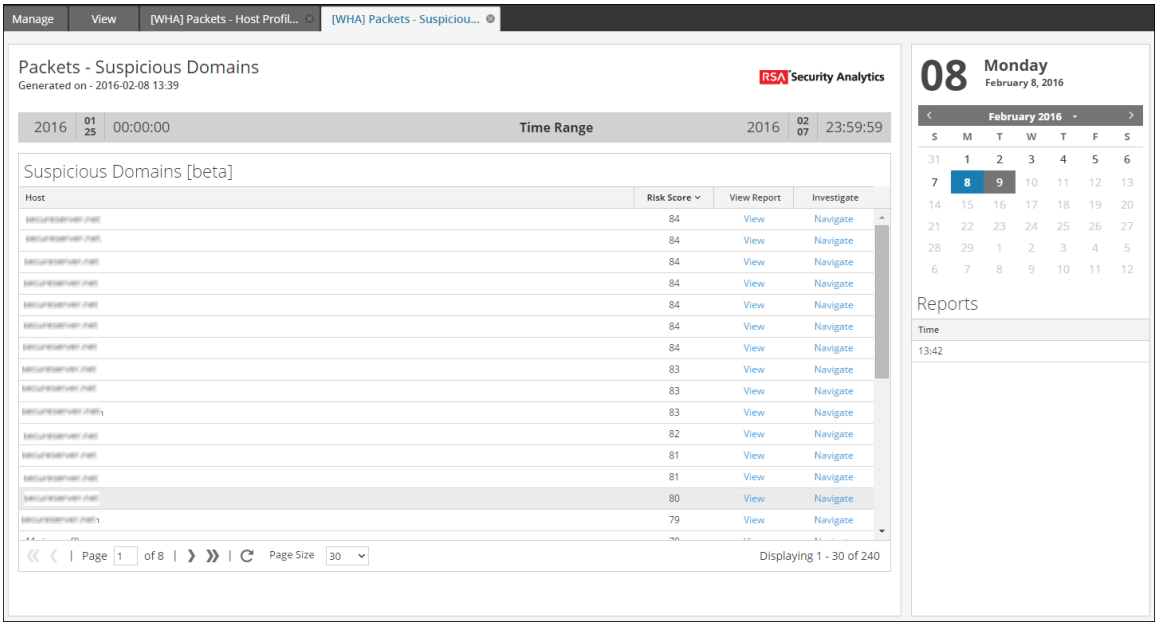
- Informe Dominios sospechosos. Para obtener más información, consulte Analizar un informe de dominios sospechoso.
- Informe Actividad de DNS sospechosa. Para obtener más información, consulte Analizar un informe Actividad de DNS sospechosa.
- Informe Perfil de host. Para obtener más información, consulte Analizar un informe Perfil de host.

Temas

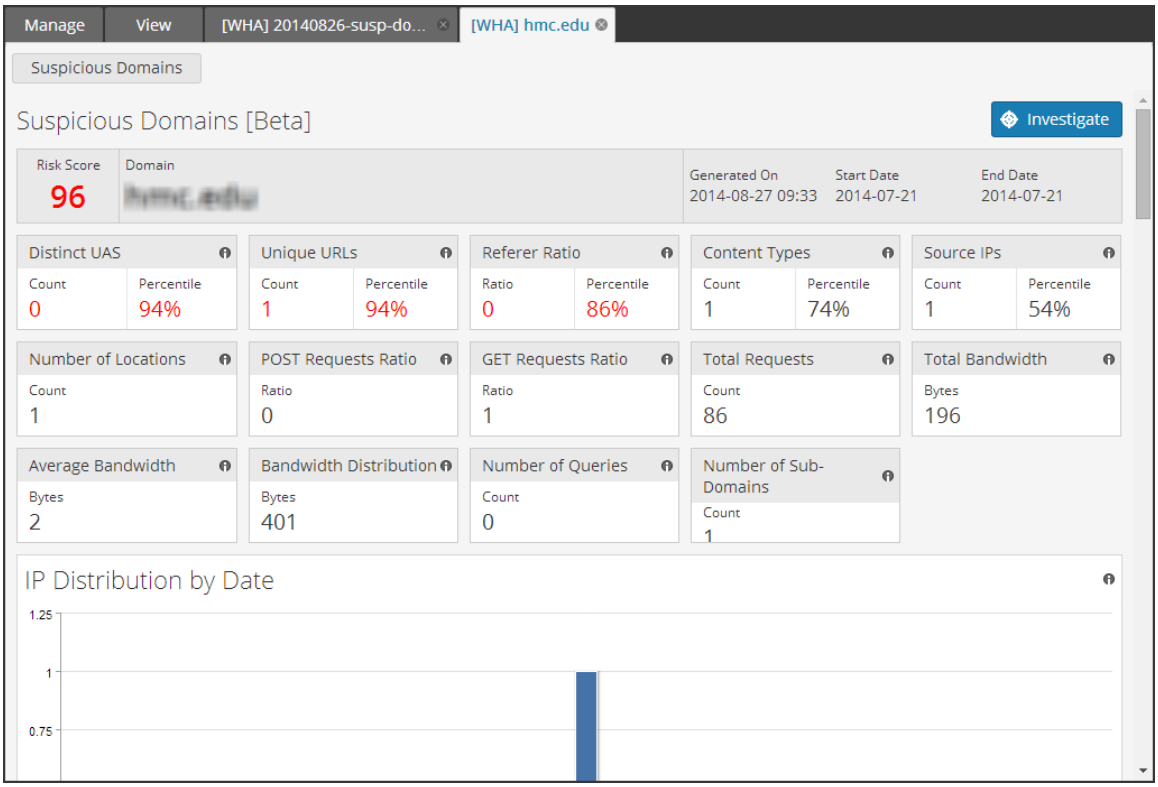
- Analizar un informe de dominios sospechoso
- Analizar un informe Actividad de DNS sospechosa
- Analizar un informe Perfil de host

Analizar un informe de dominios sospechoso

En este tema se describe el informe Dominios sospechosos. En la siguiente figura se muestra el informe Dominios sospechosos que enumera todos los dominios sospechosos potenciales y el puntaje de riesgo de cada uno.



En la siguiente figura se muestran los diferentes paneles de esta vista.



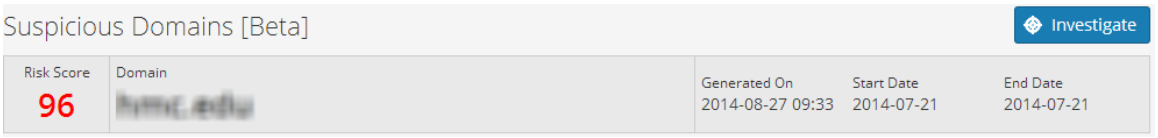
El informe Dominios sospechosos incluye los siguientes paneles:

1. Encabezado de dominio
2. Campos de dominio
3. Histogramas de dominio
4. Listas de dominios

Panel Encabezado de dominio

El panel Encabezado de dominio permite ver el puntaje de riesgo, el nombre del dominio (ejemplo, hmc.edu), la hora en que se genera el informe y las fechas de inicio y de finalización en que se ejecuta el informe.

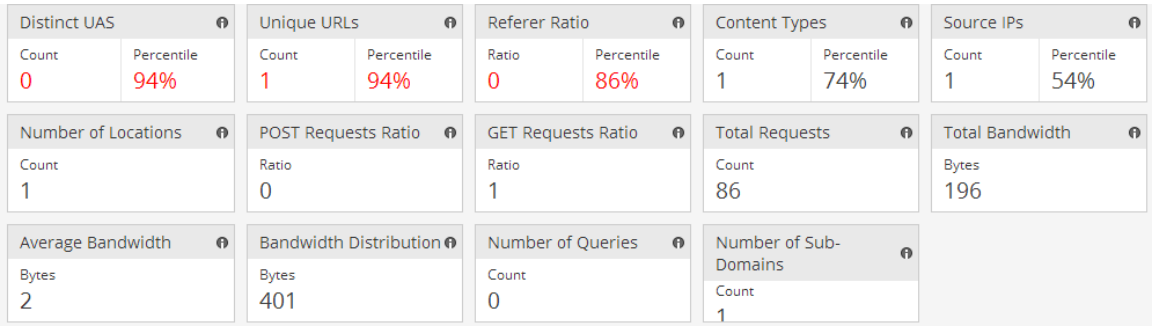
Nota: Si el puntaje de riesgo es mayor o igual que 50, la codificación en colores se muestra en rojo o, de lo contrario, en verde.



Panel Campos de dominio

En el panel Campos de dominio se muestran los siguientes campos de la base de datos Mongo DB.

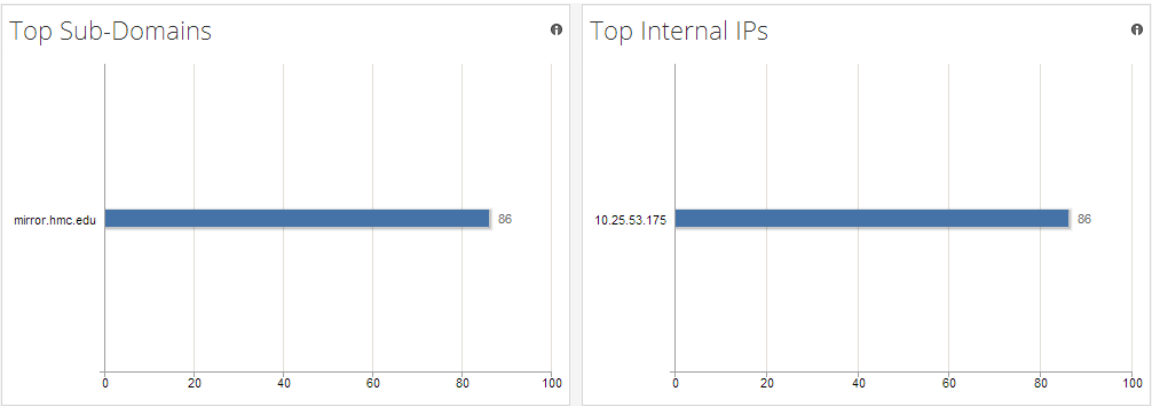
Nota: Los valores de los campos se basan en el dominio sospechoso seleccionado. Todos los campos se completan con valores en el tiempo de ejecución.



Panel Histogramas de dominio

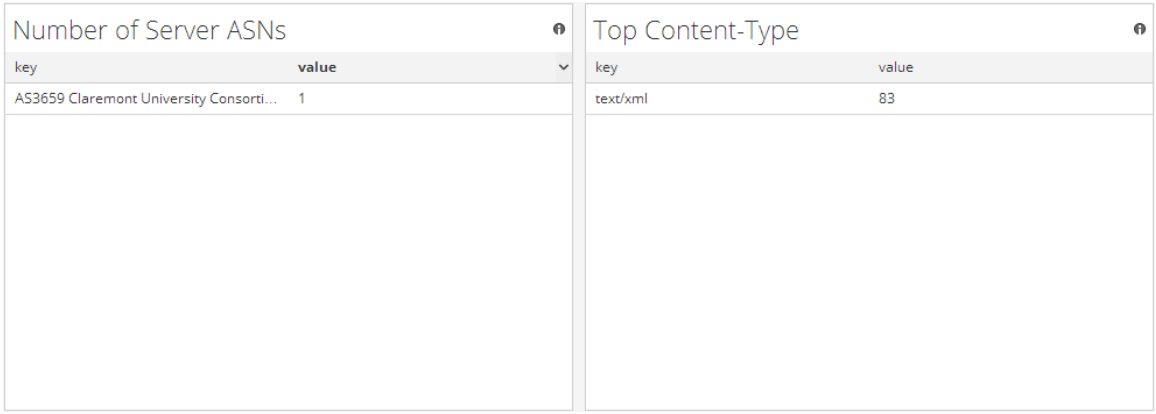
En el panel Histogramas de dominio se muestra el histograma vertical que representa las direcciones IP internas o los subdominios sospechosos de color azul oscuro.

Histograma vertical



Panel Lista de dominios

En el panel Lista de dominios se muestra el número de sistema autónomo (ASN) del servidor y tipos de contenido superior.



Ver el informe Dominios sospechosos

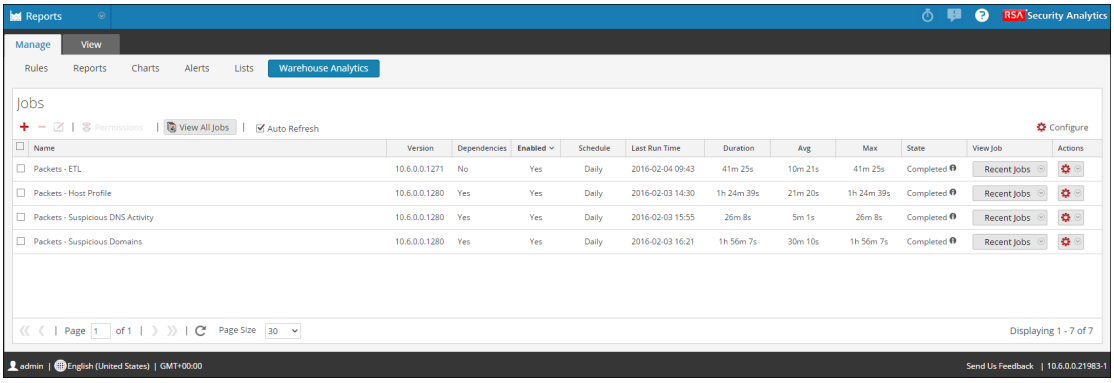
Realice los siguientes pasos para ver el informe Dominios sospechosos:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En la barra de herramientas de Warehouse Analytics, haga clic en **Ver todas las tareas**.

   En la pestaña Ver se muestra una lista de trabajos junto con el nombre del calendario y la hora.

   Nota: Si no se muestra ninguna lista, seleccione una fecha del calendario para ver una lista de trabajos.

4. Haga doble clic en una ejecución de acuerdo con el dominio sospechoso.

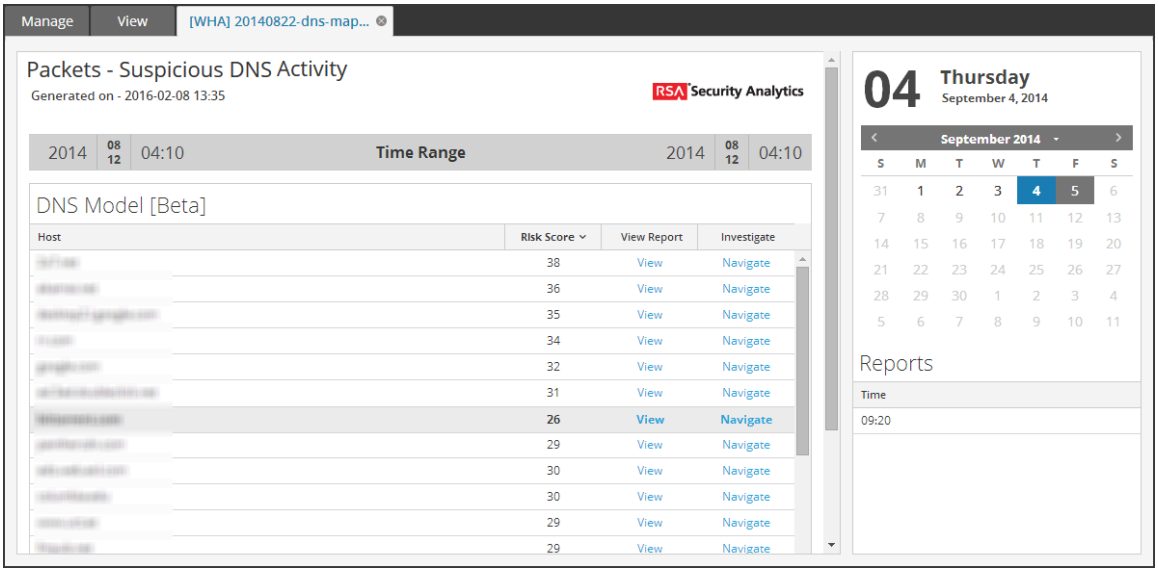
   Se muestra el informe Dominios sospechosos.

Próximos pasos

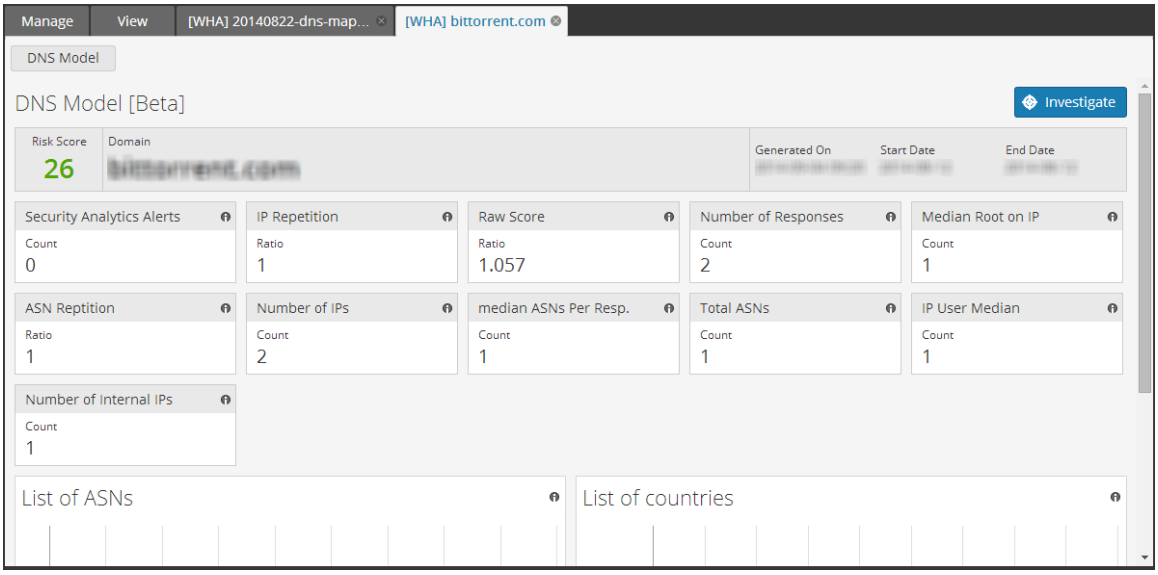
Realice la siguiente tarea: Haga clic en el botón **Navegar** para investigar un dominio sospechoso.

Analizar un informe Actividad de DNS sospechosa

En este tema se describe el informe Actividad de DNS sospechosa. En la siguiente figura se muestra el informe Actividad de DNS sospechosa que enumera todos los dominios sospechosos y el puntaje de riesgo de cada uno.



En la siguiente figura se muestran los diferentes paneles de esta vista.



Contexto

El informe Actividad de DNS sospechosa incluye los siguientes paneles:

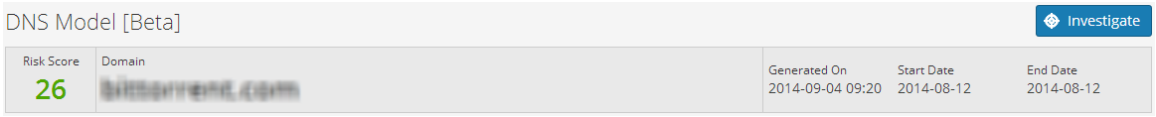
- Encabezado de dominio
- Campos de dominio

- Histogramas de dominio

Panel Encabezado de dominio

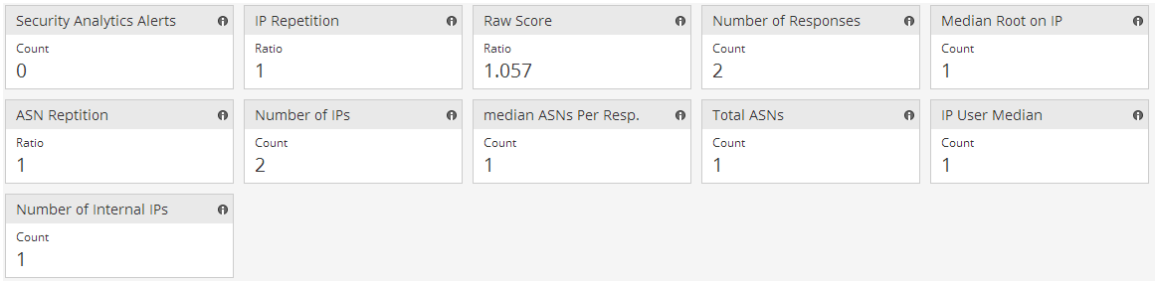
El panel Encabezado de dominio permite ver el puntaje de riesgo, el nombre del dominio (ejemplo, bitminter.com), la hora en que se generó el informe y las fechas de inicio y de finalización en que se ejecutó el informe.

Nota: Si el puntaje de riesgo es mayor o igual que 50, la codificación en colores se muestra en rojo o, de lo contrario, en verde.



Panel Campos de dominio

En el panel Campos de dominio se muestran los siguientes campos de la base de datos Mongo DB.



Nota: En todos los campos completados del panel Campos de dominio se muestran valores de acuerdo con la hora de ejecución.

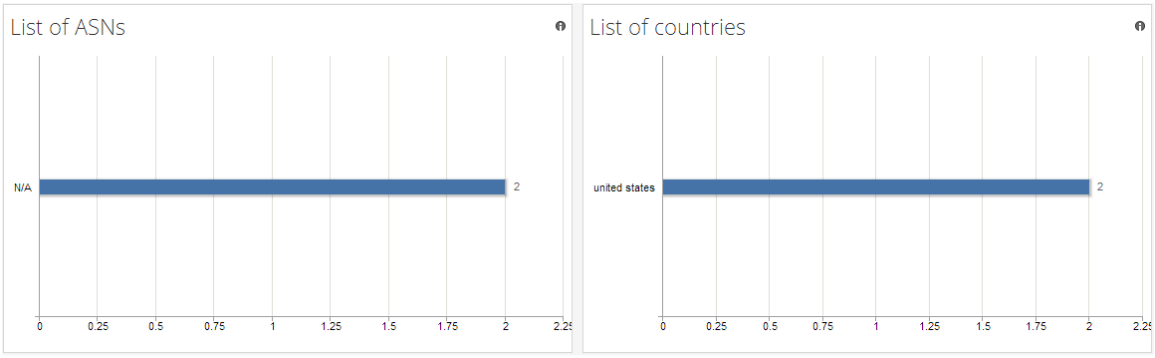
Campo	Descripción
Alertas de Security Analytics	La cantidad de alertas de Security Analytics por respuesta.
Repetición de IP	El número de pares distintos para la dirección IP y la fecha dividido por el número total de direcciones IP en el dominio.
Puntaje crudo	El puntaje crudo.
Número de respuestas	El número de respuestas DNS (con las solicitudes omitidas).

Campo	Descripción
Raíz de mediana en IP	La mediana del número de raíces distintas por IP devuelta.
Repetición de ASN	El porcentaje de ASN que se ve todos los días del total de direcciones IP vistas en el dominio.
Número de direcciones IP	El número total de direcciones IP.
ASN de mediana por respuesta	La mediana del número de ASN por respuesta.
Total de ASN	El número total de ASN.
Mediana de usuario de dirección IP	La mediana de las direcciones IP internas en las IP del dominio.
Número de direcciones IP internas	El número de direcciones IP de origen desde las cuales se abordó el dominio.

Panel Histogramas de dominio

El panel Histogramas de dominio muestra el histograma vertical que representa los ASN o los países sospechosos en color azul oscuro.

Histograma vertical



Ver un informe Actividad de DNS sospechosa

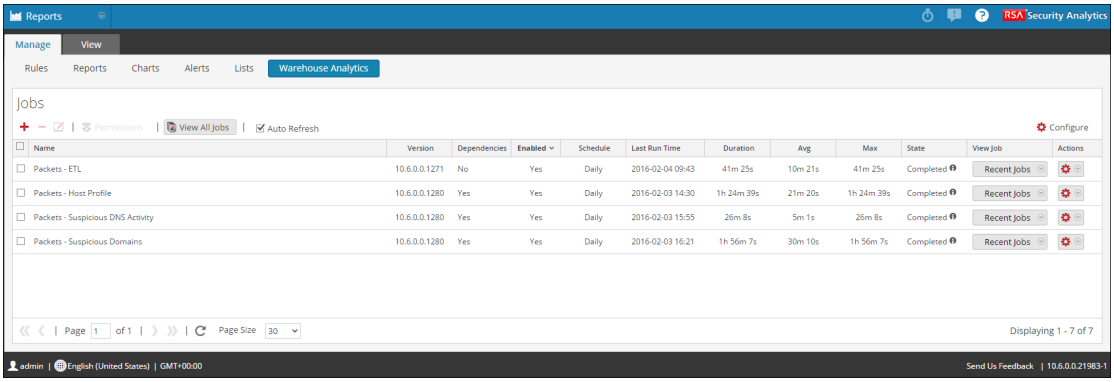
Para ver un informe Actividad de DNS sospechosa:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En la barra de herramientas de Warehouse Analytics, haga clic en **Ver todas las tareas**.

   En la pestaña Ver se muestra una lista de trabajos junto con el nombre del calendario y la hora.

   Nota: Si no se muestra ninguna lista, seleccione una fecha del calendario para ver una lista de trabajos.

4. Haga doble clic en una ejecución de acuerdo con la Actividad de DNS sospechosa.

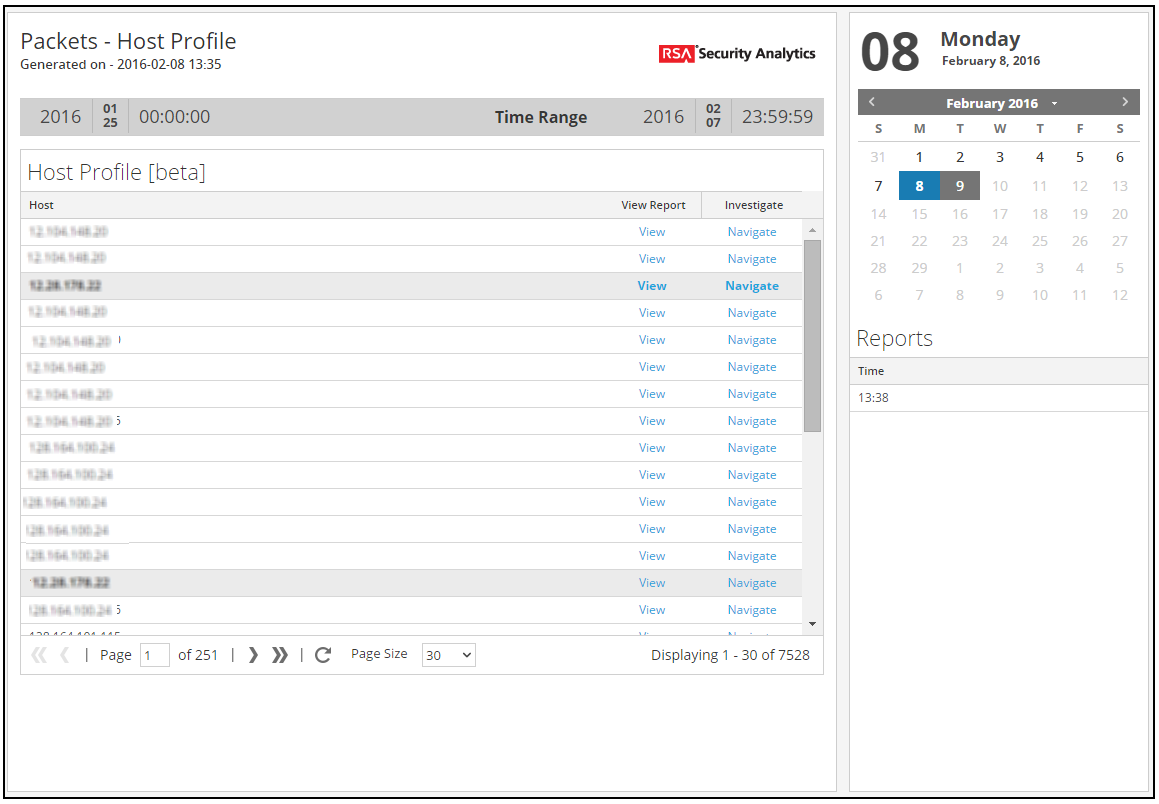
   Se muestra el informe Actividad de DNS sospechosa del dominio.

Próximos pasos

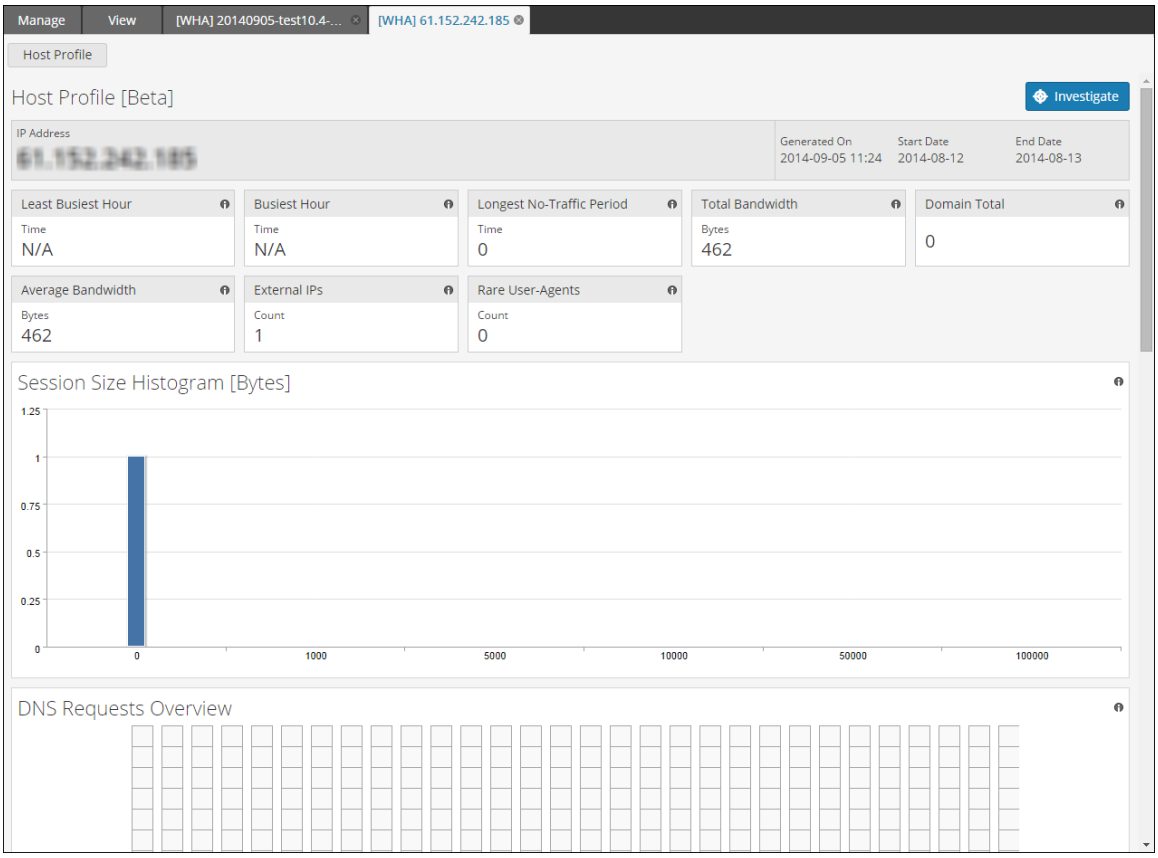
Realice la siguiente tarea: Haga clic en el botón **Investigar** para revisar la actividad de DNS sospechosa.

Analizar un informe Perfil de host

En este tema se describe el informe Perfil de host. En la siguiente figura se muestra el informe Perfil de host, el cual enumera todos los hosts sospechosos.



En la siguiente figura se muestran los diferentes paneles de esta vista.

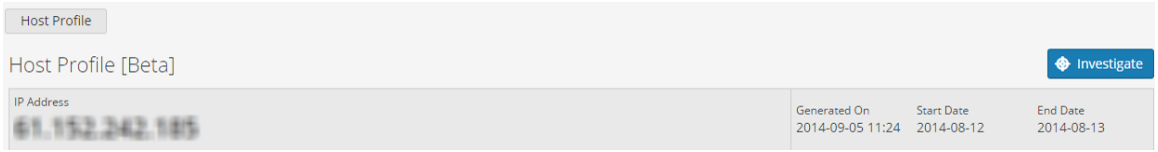


El informe Perfil de host tiene los siguientes paneles:

- Encabezado de actividad
- Campos de actividad
- Histogramas de actividad
- Mapas de riesgos de actividad
- Lista de actividades

Panel Encabezado de actividad

El panel Encabezado de actividad permite ver el nombre de la actividad, la dirección IP, la hora de generación del informe y las fechas de inicio y de finalización.



Nota: El informe Perfil de host no muestra un puntaje en el panel Encabezado de actividad.

Panel Campos de actividad

En el panel Campos de actividad se muestran los siguientes campos de la base de datos de Mongo DB.

Campo	Descripción
Hora menos ocupada	La hora con el menor número de solicitudes.
Hora más ocupada	La hora con el mayor número de solicitudes.
Mayor período sin tráfico (horas)	La mayor pausa sin tráfico para este IP.
Total bandwidth	El ancho de banda total consumido para envío y recepción.
Dominio total	El número total de dominios a los que accede esta dirección IP.
Ancho de banda promedio	El ancho de banda promedio para envío o recepción por sesión.
Direcciones IP externas	El número de direcciones IP externas a las que se accede.
Agentes de usuario poco frecuentes	El número de cadenas de agente de usuario poco frecuentes que se ven desde esta dirección IP.

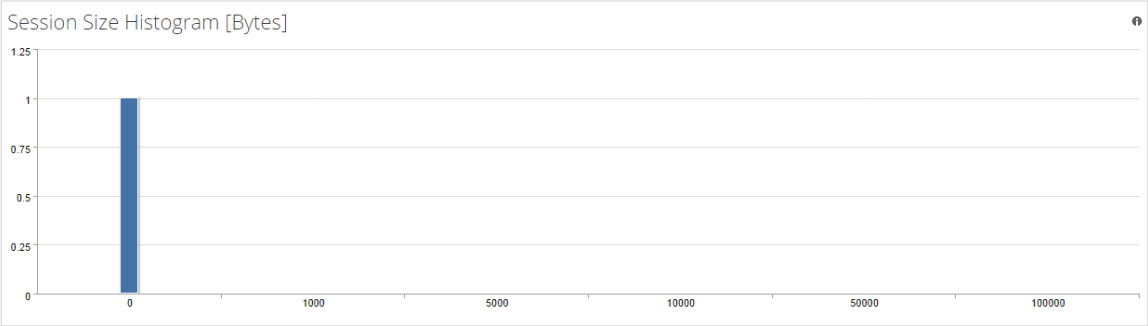
Panel Histogramas de actividad

En el panel Histogramas de actividad se muestra el histograma del tamaño de la sesión. Este es un histograma vertical que muestra la actividad del host en azul.

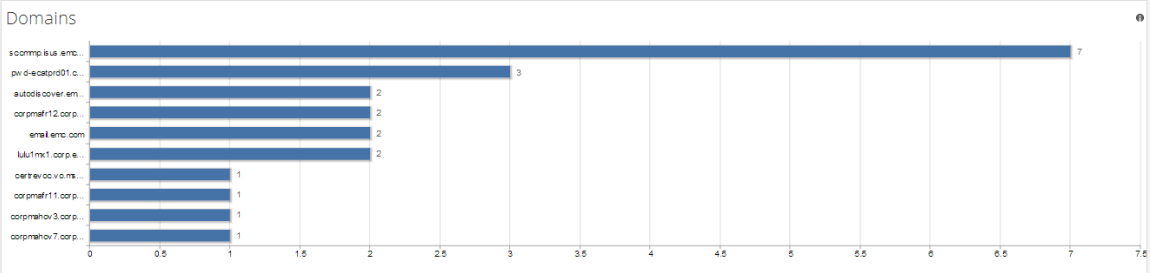
Existen dos tipos de histogramas:

- Histograma vertical: los datos se representan en forma de un histograma vertical en caso de un histograma de horas o de tamaño de sesión.
- Histograma horizontal: Los datos se representan en forma de un histograma horizontal en el caso de un histograma de dominios.

Histograma vertical



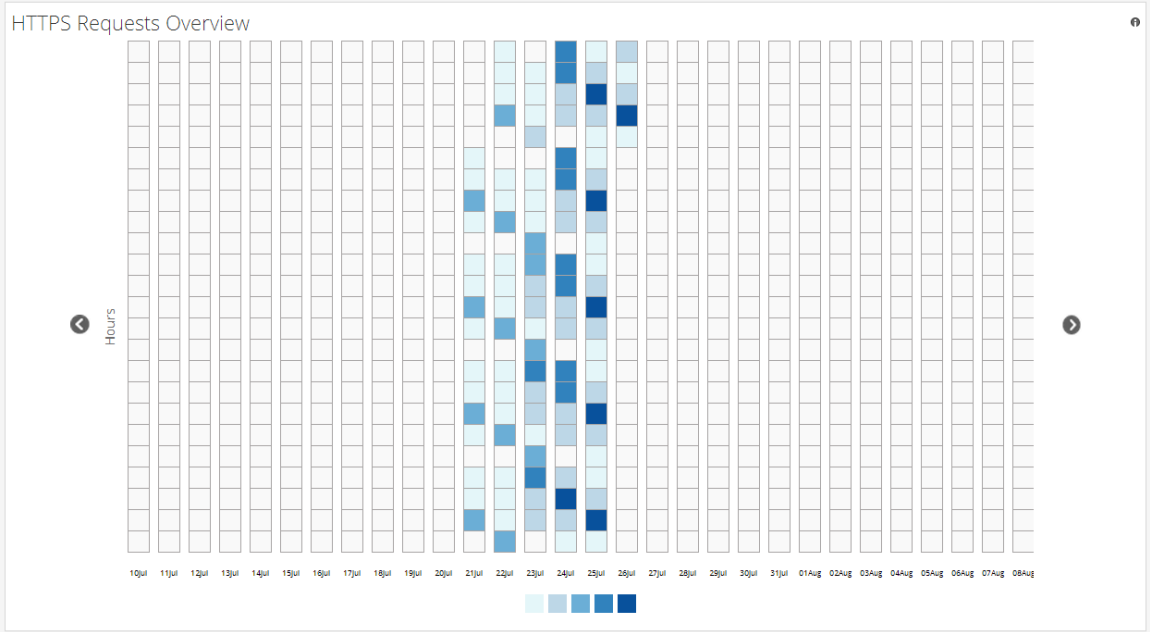
Histograma horizontal



Panel Mapas de riesgos de actividad

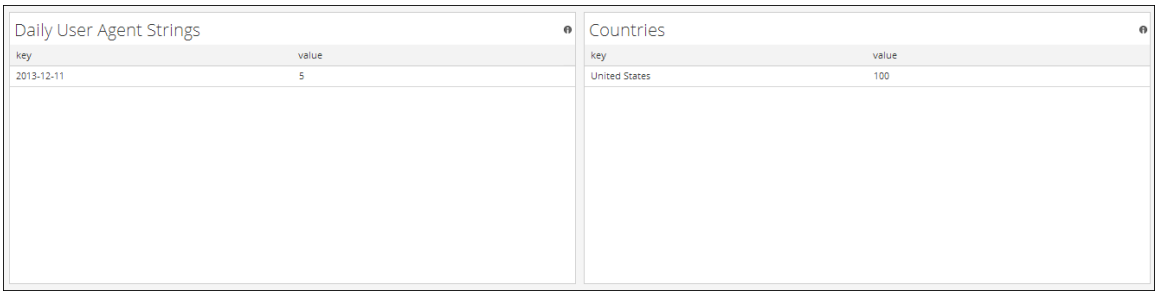
El panel Mapas de riesgos de actividad muestra el mapa de riesgos de Descripción general de solicitudes HTTPS. El mapa de riesgos se representa basándose en días (eje X) y horas (eje Y). El conteo de las actividades se calcula según el promedio de varias actividades. Los códigos de colores que se muestran para las actividades varían ya que son dinámicos. El mapa de riesgos se muestra a partir de la fecha inicial del informe, la cual aparece sobre el panel Encabezado. Por ejemplo, en un día particular en la hora 23, si la actividad es alta, entonces el código de color azul oscuro se muestra en el mapa de riesgos.

Nota: el alto índice de actividades durante un periodo específico no es un indicador de que hay actividad sospechosa en el host. Los códigos de colores solo representan el índice de actividades durante un período.



Panel Lista de actividades

El panel Lista de actividades se muestra en función del porcentaje de tráfico en el campo al cual accedió. Por ejemplo, Configuración diaria de agente de usuario y Países.



Ver un informe Perfil de host

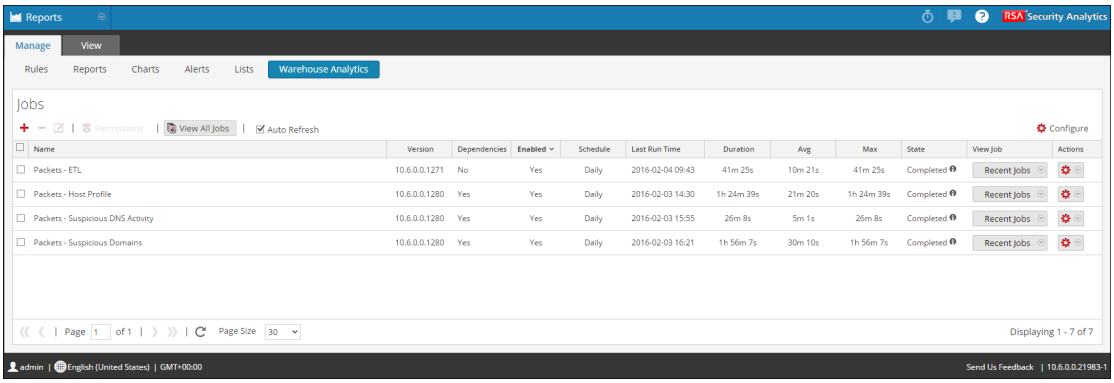
Para ver un informe Perfil de host:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En la barra de herramientas de Warehouse Analytics, haga clic en **Ver todas las tareas**.

   En la pestaña Ver se muestra una lista de trabajos junto con el nombre del calendario y la hora.

   Nota: Si no se muestra ninguna lista, seleccione una fecha del calendario para ver una lista de trabajos.

   Haga doble clic en una ejecución de acuerdo con el modelo de perfil de host.

   Se muestra el informe Perfil de host.

Próximos pasos Los próximos pasos

Puede investigar un informe Perfil de host.

Paso 5. Investigar un informe de Warehouse Analytics

En este tema se proporcionan instrucciones para investigar desde un informe de Warehouse Analytics. Puede investigar desde un informe de Warehouse Analytics, para lo cual debe navegar directamente hacia el módulo Investigation desde el informe. Puede hacer lo siguiente para investigar desde el informe o los detalles del informe:

- Usar la opción Navegar en la vista Ver trabajo para investigar el trabajo.
- Usar la opción Investigar para investigar el dominio o la actividad.

Requisitos previos

Asegúrese de:

- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Comprender los componentes del panel Ver todas las tareas. Para obtener más información, consulte Panel Ver todas las tareas.

Investigar un informe de Warehouse Analytics

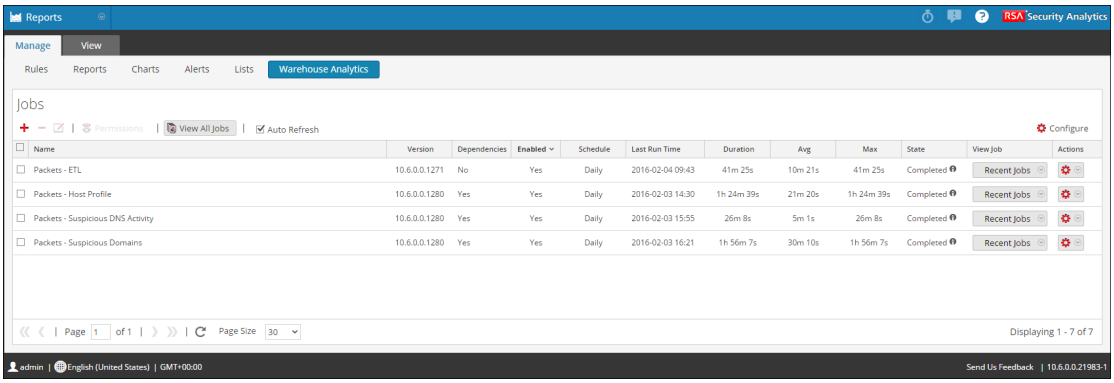
Para investigar a partir de un informe de Warehouse Analytics:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.

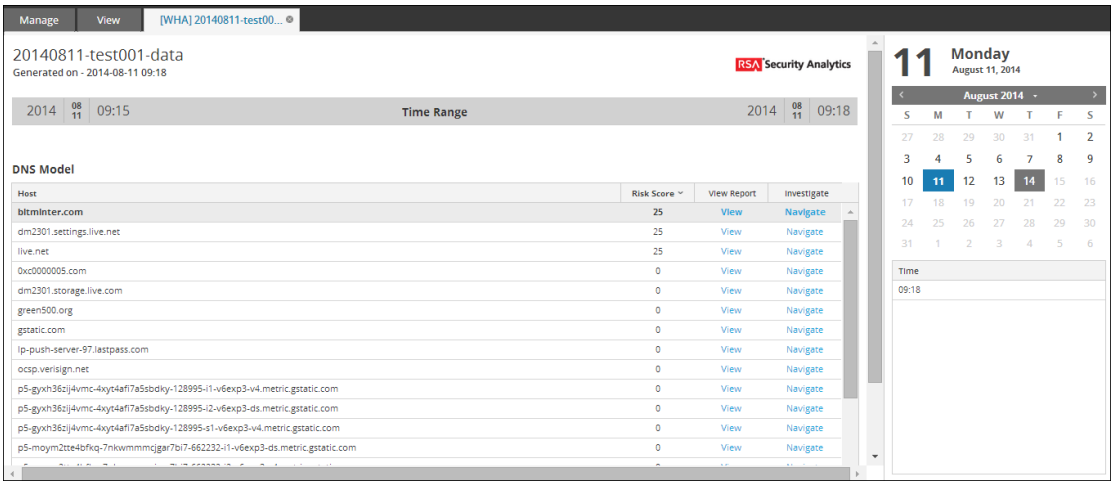


3. En la barra de herramientas de Warehouse Analytics, haga clic en **Ver todas las tareas**.

   Se muestra la pestaña Ver todas las tareas.

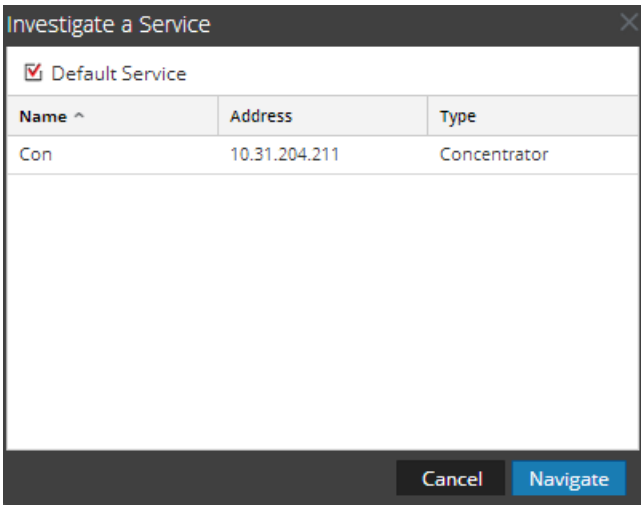
   Nota: Si no se muestran trabajos en Ver todas las tareas, seleccione una fecha para la cual desea mostrar los trabajos.

4. Haga doble clic en la ejecución del trabajo para ver los detalles del trabajo en la pestaña Ver un trabajo.



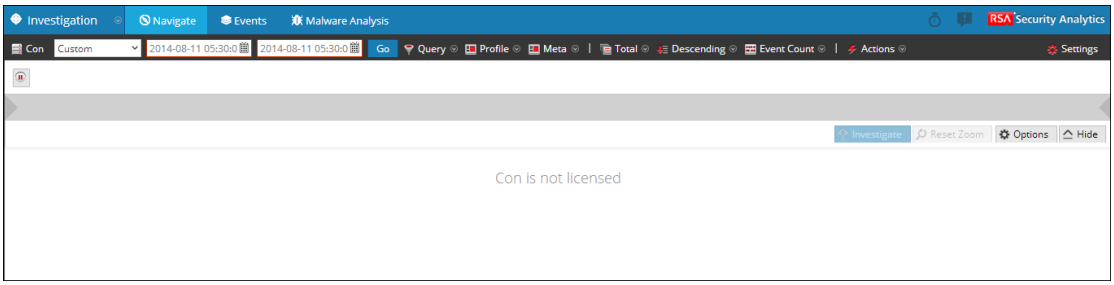
5. En la columna Investigar, haga clic en **Navegar**.

   Aparece el cuadro de diálogo Investigar un servicio.



6. Seleccione el servicio Concentrator.
7. Haga clic en **Navegar**.

   Se muestra la interfaz del usuario de navegación.



8. Seleccione un punto de datos en la interfaz del usuario de navegación.
9. Haga clic en **Investigar** para verla en el módulo Investigation.

Próximos pasos

Puede cambiar el tipo de gráfico y su visualización.

Procedimientos adicionales

Este tema es un conjunto de procedimientos adicionales para Warehouse Analytics. Estos procedimientos son para ciertos casos que no forman parte de los procedimientos necesarios para el uso de Warehouse Analytics y se presentan en orden alfabético.

Temas

Eliminar un trabajo de Warehouse Analytics

En esta sección se proporcionan instrucciones para eliminar trabajos de Warehouse Analytics.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Definición de trabajo. Para obtener más información, consulte Vista Definición de trabajo.

Eliminar un trabajo de Warehouse Analytics

Nota: los trabajos de ETL no se pueden editar ni eliminar.

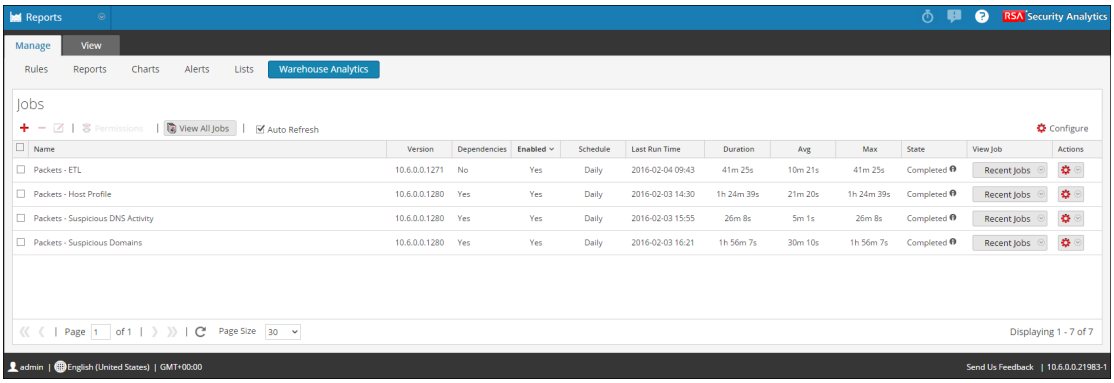
Para eliminar trabajos de Warehouse Analytics:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

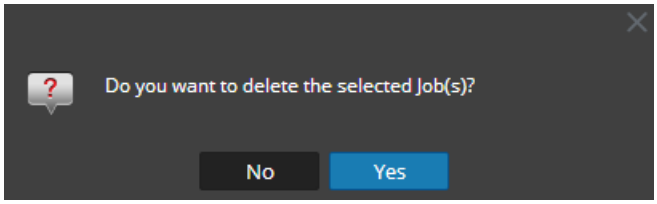
2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En el panel de lista de Warehouse Analytics, realice una de las siguientes acciones:
   - Seleccione los trabajos y haga clic en .
   - Mantenga el mouse sobre un trabajo y haga clic en > **Eliminar**.

     Se muestra un cuadro de diálogo de confirmación.



4. Haga clic en **Sí** para eliminar el trabajo.

   Se muestra un mensaje de confirmación que indica que el trabajo se eliminó correctamente.

Editar un trabajo de Warehouse Analytics

En este tema se proporcionan instrucciones para editar un trabajo de Warehouse Analytics.

Requisitos previos

Asegúrese de:

- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Comprender los componentes de la vista Definición de trabajo. Para obtener más información, consulte Vista Definición de trabajo.

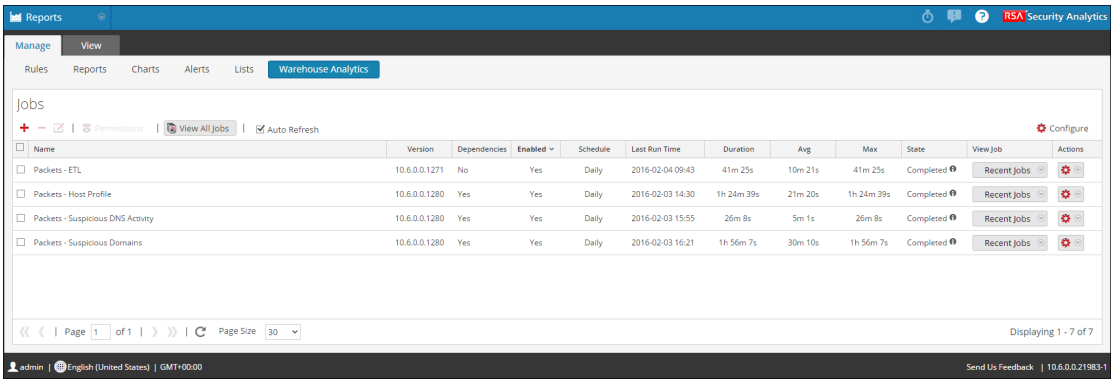
Procedimiento

Realice los siguientes pasos para editar un trabajo de Warehouse Analytics:

Nota: los nombres de trabajo de ETL son de solo lectura y no se pueden editar.

1. En el menú de Security Analytics, haga clic en **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.
   Aparece la vista Warehouse Analytics.



3. En el panel de lista de Warehouse Analytics, seleccione un trabajo y haga clic en  .
   Se muestra la pantalla **Generador de trabajos**.

4. (Opcional) Modifique el **Nombre** del trabajo.

5. (Opcional) En la lista desplegable **Warehouse**, seleccione el origen de datos que se creó en la página de configuración de Reporting Engine. (Por ejemplo, Pivotal o MapR).

6. En el menú desplegable **En**, seleccione el tipo de calendario de ejecución (Pasado o Rango) para ese rango de tiempo.

Nota: Durante la programación de un trabajo, si selecciona la opción **Pasado** o la opción **Rango (específico)** cerca de la hora actual, debe asegurarse de que se devuelvan los datos agregados en el origen de datos. Si hay una demora de agregación en el origen de datos, la hora de finalización que elija debe tener en cuenta la demora, de lo contrario, los trabajos pierden datos no agregados para ese rango de tiempo.

(Opcional) En el campo **Opciones avanzadas** , realice lo siguiente:

a. En el campo **Parámetros de modelo**, ingrese un nombre de columna y seleccione el valor de la columna en la ventana Selección de lista.

b. En el campo **Parámetros de HDFS**, ingrese un nombre y un valor de columna.

c. En el campo **Parámetros de MapReduce**, ingrese un nombre y un valor de columna.

d. En el campo **Parámetros de SandBox JVM**, ingrese un nombre y un valor de columna.

7. Haga clic en **Guardar**.

Se muestra un mensaje de confirmación que indica que el trabajo se guardó correctamente.

Activar o desactivar un trabajo programado

En este tema se proporcionan instrucciones para habilitar o inhabilitar un trabajo de Warehouse Analytics calendarizado.

Requisitos previos

Asegúrese de haber comprendido los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.

Activar o desactivar un trabajo programado

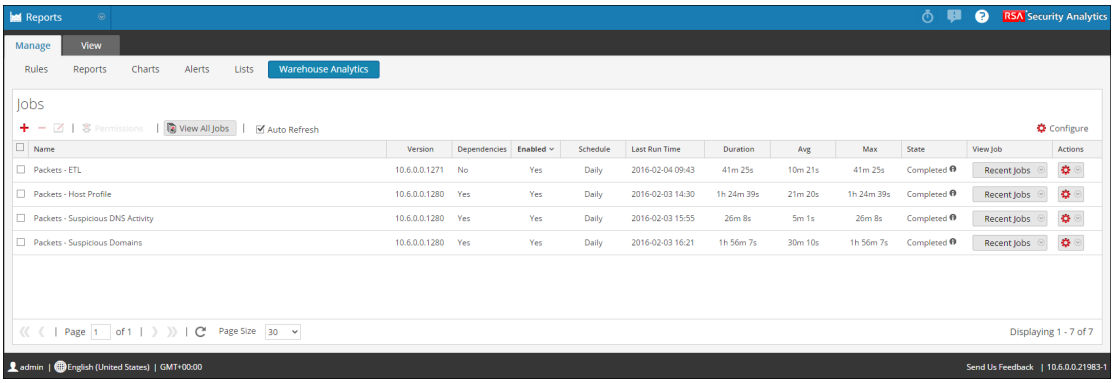
Para habilitar o deshabilitar un trabajo programado desde el panel Lista de Warehouse Analytics:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En el panel Lista de Warehouse Analytics, seleccione un trabajo y realice una de las siguientes acciones:

   - Haga clic en  > **Habilitar**.

     El estado del trabajo cambia a “En ejecución” si el informe está calendarizado para ejecutarse de inmediato.

   - Haga clic en  > **Desactivar**.

     El estado del informe cambia a “Inactivo”.

Actualizar una lista de trabajos

En este tema se proporcionan instrucciones para actualizar una lista de trabajos de Warehouse Analytics.

Requisitos previos

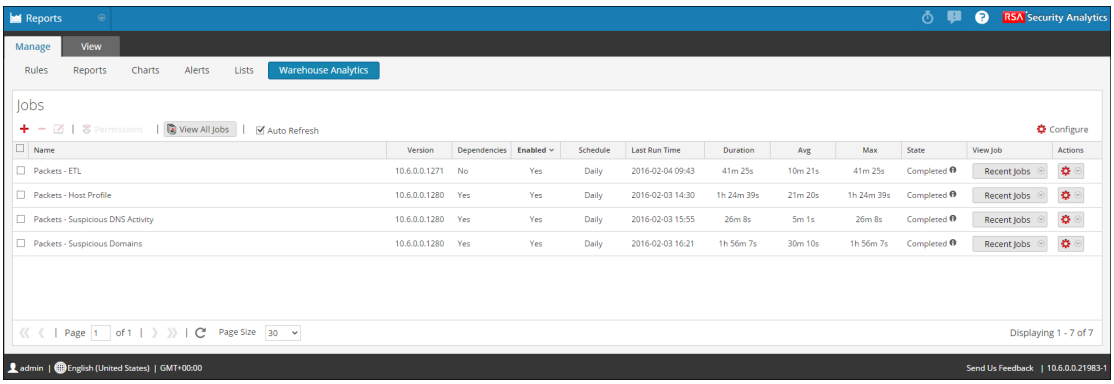
Asegúrese de comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.

Procedimiento

Realice los siguientes pasos para actualizar una lista de trabajos:

1. En el menú de Security Analytics, haga clic en **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.
   Aparece la vista Warehouse Analytics.



3. En el panel Lista de Warehouse Analytics, arrastre y suelte los trabajos.
   Los trabajos se mueven a la nueva ubicación.

4. Haga lo siguiente para actualizar una lista de trabajos:

   - En la barra de herramientas de Warehouse Analytics, seleccione **Actualización automática**.
     La lista de trabajos se actualiza automáticamente.

   - En el panel Lista de Warehouse Analytics, haga clic en .
     La lista de trabajos se actualiza inmediatamente.

Probar un trabajo de Warehouse Analytics

En este tema se proporcionan instrucciones para probar un trabajo de Warehouse Analytics.

Requisitos previos

Asegúrese de:

- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Comprender los componentes de la vista Definición de trabajo. Para obtener más información, consulte Vista Definición de trabajo.

Probar un trabajo

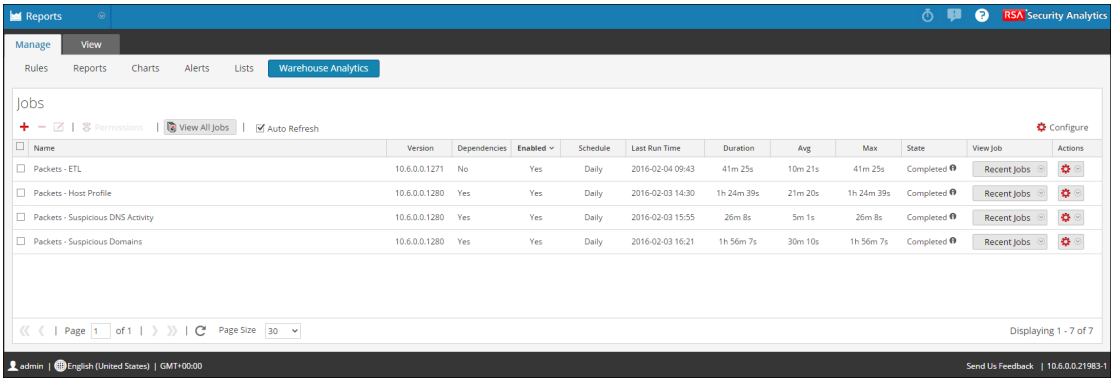
Para probar un trabajo en el panel Lista de Warehouse Analytics:

1. En el menú de Security Analytics, haga clic en **Informes**.

   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.

   Aparece la vista Warehouse Analytics.



3. En el panel Lista de Warehouse Analytics, seleccione un trabajo y haga clic en  > **Probar**.

   Se muestra la página Configuración del trabajo de prueba.

   Nota: El campo **Nombre** muestra el nombre del trabajo que se está probando y es de solo lectura.

4. (Opcional) En la lista desplegable **Warehouse**, seleccione el origen de datos que se creó en la página de configuración de Reporting Engine. (Por ejemplo, Pivotal o MapR).
5. En la lista desplegable **En**, seleccione el tipo de calendario de ejecución:

- **Pasado:** seleccione la cantidad de días.
- **Rango (específico):** Seleccione la fecha y la hora en los campos **De** y **Hasta.**
- **Pasado:** seleccione la cantidad de días.
- **Rango (específico):** Seleccione la fecha y la hora en los campos **De** y **Hasta.**

6. (Opcional) En el campo **Opciones avanzadas** , realice lo siguiente:
   a. En el campo **Parámetros de modelo**, ingrese un nombre de columna y seleccione el valor de la columna en la ventana Selección de lista.
   b. En el campo **Parámetros de HDFS**, ingrese un nombre y un valor de columna.
   c. En el campo **Parámetros de MapReduce**, ingrese un nombre y un valor de columna.
   d. En el campo **Parámetros de SandBox JVM**, ingrese un nombre y un valor de columna.
7. Haga clic en **Guardar**.

   Se muestra un mensaje de confirmación que indica que el trabajo se guardó correctamente.

Ver todas las tareas

En este tema se proporcionan instrucciones para ver una lista de todos los trabajos de Warehouse Analytics.

Requisitos previos

Asegúrese de:

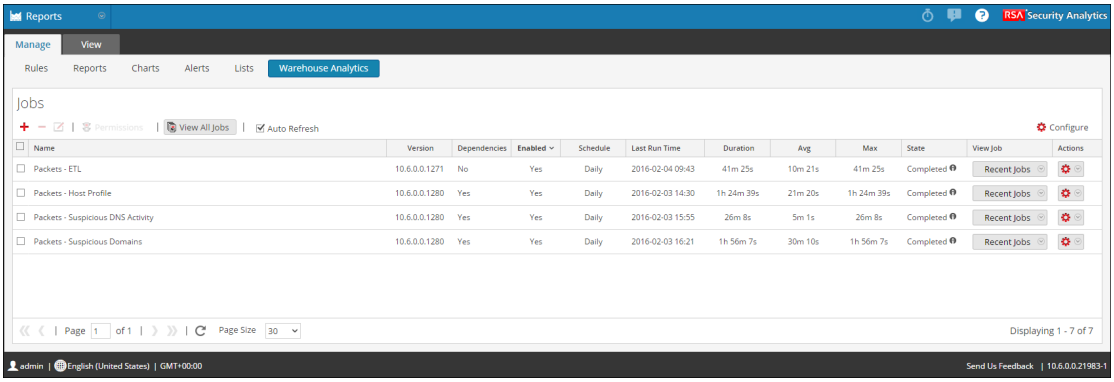
- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Comprender los componentes del panel Ver todas las tareas. Para obtener más información, consulte Panel Ver todas las tareas.

Procedimiento

Realice los siguientes pasos para ver una lista de todos los trabajos:

1. En el menú de Security Analytics, haga clic en **Informes**.
   Se muestra la pestaña Administrar.

2. Haga clic en **Warehouse Analytics**.
   Aparece la vista Warehouse Analytics.



3. En la barra de herramientas de Warehouse Analytics, haga clic en **Ver todas las tareas**.
   En la pestaña Ver se muestra una lista de trabajos junto con el nombre del calendario y la hora.

Nota: Si no se muestra ninguna lista, seleccione una fecha del calendario para ver una lista de trabajos.

4. Haga doble clic en una ejecución para ver los detalles del trabajo en pantalla completa.

Los próximos pasos

Realice las siguientes tareas:

1. Puede ver trabajos en pantalla completa.

2. Puede seleccionar una fecha del calendario para ver una lista de los trabajos que se ejecutaron correctamente para la fecha seleccionada.

Ver un trabajo programado

En este tema se proporcionan instrucciones para ver un trabajo programado que consta de una lista de dominios sospechosos. La visualización de un trabajo calendarizado permite comprender el puntaje de riesgo, ver un informe del trabajo e investigar un trabajo calendarizado. Si el trabajo calendarizado está en un estado **detenido** o **inhabilitado**, puede iniciarlo o habilitarlo.

Requisitos previos

Asegúrese de:

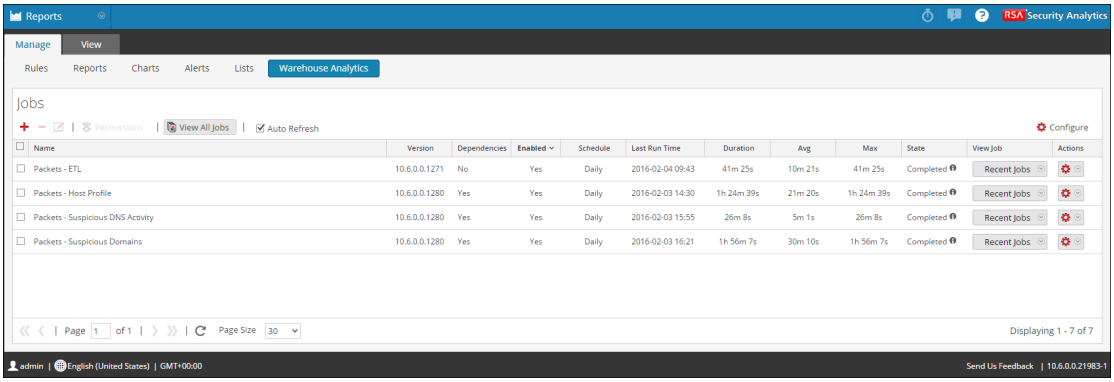
- Comprender los componentes de la vista Warehouse Analytics. Para obtener más información, consulte Vista Warehouse Analytics.
- Comprender los componentes de Ver un trabajo programado. Para obtener más información, consulte Panel Ver un trabajo programado.

Procedimiento

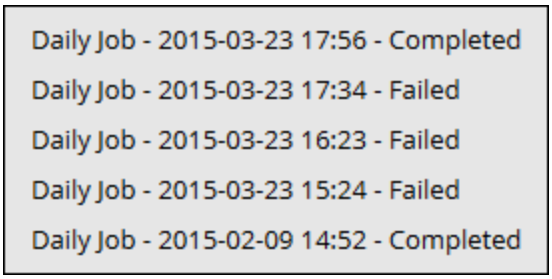
Realice los siguientes pasos para ver un trabajo programado:

Nota: los trabajos de ETL no tienen una lista de trabajos recientes y, por lo tanto, no se puede ver ningún informe.

1. En el menú de Security Analytics, haga clic en **Informes**.
   Se muestra la pestaña Administrar.
2. Haga clic en **Warehouse Analytics**.
   Aparece la vista Warehouse Analytics.



3. Seleccione el trabajo y, en la columna **Ver trabajo**, seleccione **Trabajos recientes**.
   Se muestra la lista de trabajos recientes.



Los próximos pasos

Realice las siguientes tareas:

1. Puede ver los detalles del informe de Warehouse Analytics en pantalla completa.

2. Puede investigar a partir de un informe de Warehouse Analytics.

3. Puede seleccionar una fecha del calendario para ver una lista de los trabajos que se ejecutaron correctamente para la fecha seleccionada.

Referencias

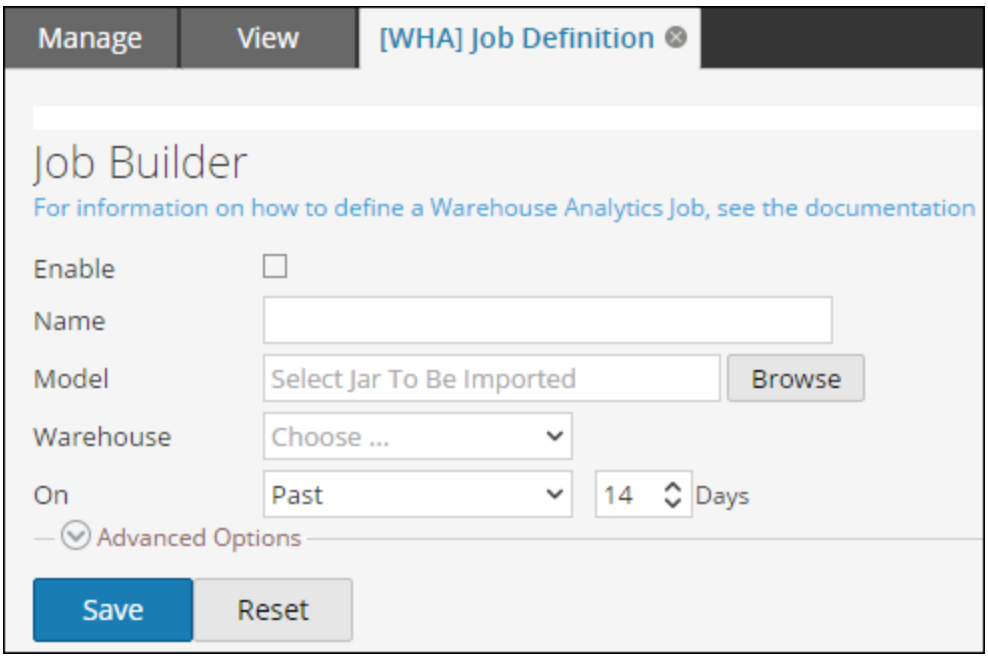
Este tema es un conjunto de referencias que describen las funciones de Warehouse Analytics.

Temas

Vista Definición de trabajo

En este tema se describen las funciones y las tareas de la vista Definición de trabajo. La vista Definición de trabajo permite crear y administrar nuevos trabajos.

En la siguiente figura se muestra la vista Definición de trabajo.

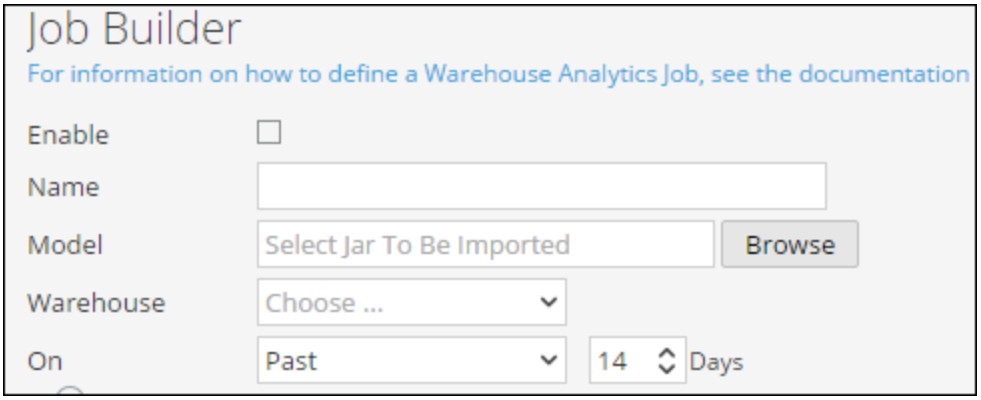


La vista Definición de trabajo consta de las siguientes secciones:

1. Definición de trabajo
2. Opciones avanzadas

Panel Definición de trabajo

El panel Definición de trabajo permite definir y programar trabajos de Warehouse Analytics.



En la siguiente tabla se describen los campos del panel Definición de trabajo.

Campo	Descripción
Activar	Activa los calendarios de informes y ejecuta el informe.
Nombre	El nombre único del informe.
Model	El nombre del modelo de ciencia de datos o archivo jar que se desea importar. Esta opción es visible solo cuando se define un trabajo. **Nota:** Según el modelo escogido, los valores se completan previamente en el panel Opciones avanzadas.
Warehouse	El nombre del origen de datos de Warehouse. (Por ejemplo, MapR o Pivotal).
Encendido	Pasado: permite especificar la cantidad de días en los cuales se ejecuta la consulta. Rango específico: permite seleccionar un rango de fechas **De** y **Hasta** para las cuales se ejecuta la consulta.

Panel Opciones avanzadas

El panel Opciones avanzadas permite definir o personalizar varios parámetros, como los siguientes:
Modelo, HDFS, MapR y Sandbox JVM del trabajo de Warehouse Analytics.

En la siguiente tabla se indican los campos del panel Opciones avanzadas.

Campo	Descripción
Parámetros de modelo	Parámetro de modelo o trabajo de Warehouse Analytics. **Nota:** Según el modelo elegido, se muestra una lista de dominios en lista blanca en la sección Parámetros de modelo. Los modelos se enumeran, pero con el puntaje **-1**. Por ejemplo, un dominio con el nombre *example.com* no aparece en la lista de dominios sospechosos.
Nombre	El nombre del parámetro de modelo.
Valor	El valor del parámetro de modelo.
	Muestra la ventana Selección de lista. Para obtener más información, consulte el tema Panel Generar una lista de la Guía de Reporting.
Parámetros de HDFS	Parámetros de configuración de HDFS.
Nombre	El nombre del parámetro de Hadoop Distributed File System (HDFS).
Valor	El valor del parámetro de HDFS.
Parámetros de MapR	Parámetros de configuración de Hadoop o MapR.
Nombre	El nombre del parámetro de MapR.
Valor	El valor del parámetro de MapR.

Campo	Descripción
Parámetros de Sandbox JVM	Parámetros de JVM o parámetros del sistema para JVM que ejecuta el modelo de Warehouse Analytics.
Nombre	El nombre del parámetro de Sandbox JVM.
Valor	El valor del parámetro de Sandbox JVM.
Guardar	Calendariza el trabajo.
Restablecer	Restablece el trabajo calendarizado.

Vista Recurso de Live

La vista Recurso de Live muestra una vista detallada de un recurso seleccionado y cuenta con opciones para:

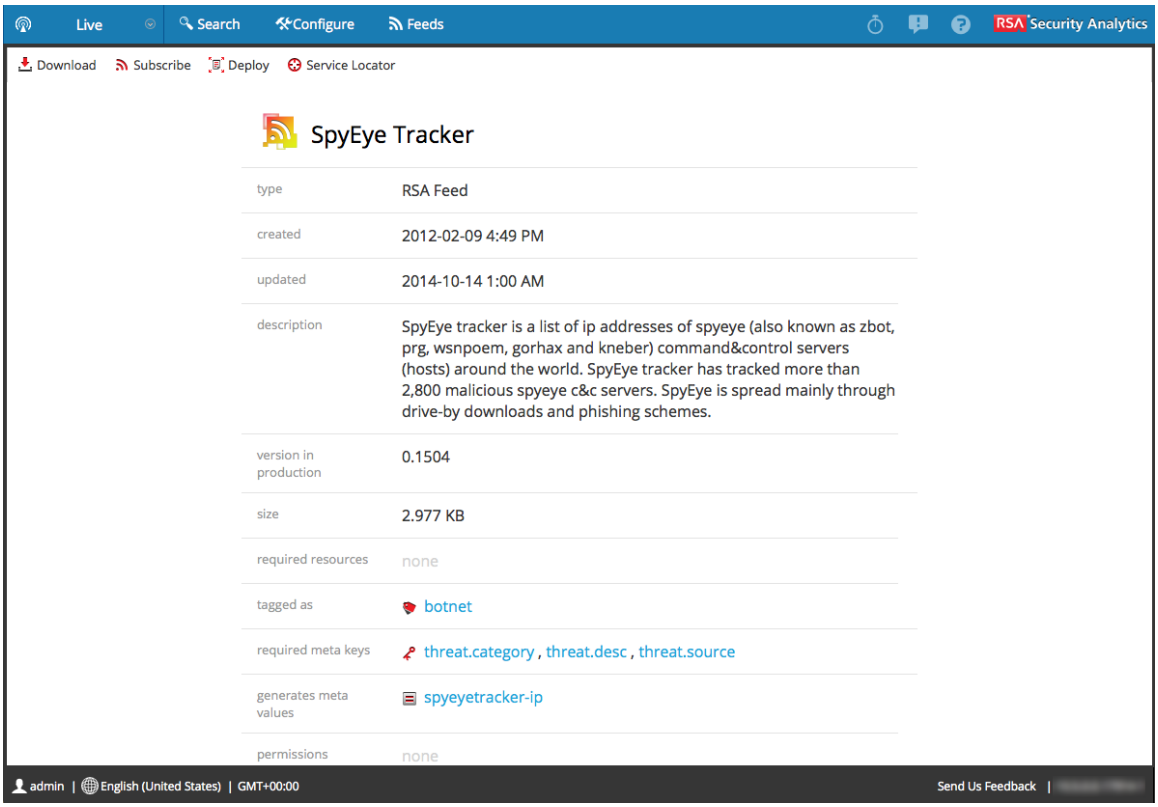
- Descargar el recurso.
- Suscribirse o cancelar la suscripción a un recurso.
- Implementar el recurso en los servicios.
- Encontrar servicios en los cuales se ha implementado el recurso y eliminar el recurso de los servicios.

El permiso necesario para tener acceso a esta vista es Ver detalles de recursos de Live.

Para tener acceso a esta vista, realice una de las opciones siguientes:

1. En el menú de **Security Analytics**, seleccione **Live > Buscar > Tipos de recursos.**
2. En la vista Buscar en Live, **Resultados en detalle**, haga clic en el ícono tipo de recurso o en el nombre del recurso.
3. En la vista Buscar en Live **Recursos en cuadrícula**, haga doble clic en un recurso o seleccione un recurso y haga clic en **Detalles**.

Este es un ejemplo de la vista Recurso.



La vista Recurso de Live tiene una vista detallada de un único recurso y una barra de herramientas.

Detalles de recursos

Este es un ejemplo de los detalles de recursos que se muestran en la vista Recurso.

En la siguiente tabla se describen los elementos de la sección Detalles de recursos.

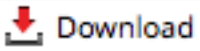
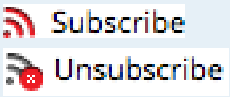
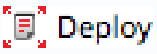
Característica	Descripción
Ícono Tipo de recurso	Una representación gráfica del tipo de recurso, por ejemplo  .
Nombre	El nombre del recurso, por ejemplo,**fingerprint_office_lua**.

Característica	Descripción
Tipo	El tipo de recurso, por ejemplo, **RSA Lua Parser**.
Created	La fecha en que se creó el recurso; por ejemplo, **2013-09-15 02:16 PM**.
Fragmento C	La fecha en que el recurso se actualizó por última vez; por ejemplo, **2013-09-15 02:16 PM**.
Descripción	La descripción del recurso, por ejemplo, **Identifica documentos Word, Excel y PowerPoint de Microsoft Office 95, 2007**.
Versión en producción	La versión del recurso, por ejemplo, **0.1**.
Tamaño	El tamaño del recurso, por ejemplo, **9,079 KB**.
Recursos requeridos	Una lista de recursos de los cuales depende este recurso, por ejemplo, **NetWitness Lua Library**. Cuando se hace clic en un recurso, los detalles que se muestran actualmente se remplazan por los detalles del recurso en el que se hizo clic.
Etiquetado como	Las etiquetas que se aplican al recurso. En el ejemplo, la etiqueta es **featured, informational**. Cuando se hace clic en una etiqueta, se abre la vista Buscar en Live con la búsqueda restringida para encontrar los recursos que contienen esa etiqueta.
Claves de metadatos requeridas	Las claves de metadatos que se aplican al recurso. En el ejemplo, no se requieren claves de metadatos. Cuando se hace clic en una clave de metadatos, se abre la vista Buscar en Live con la búsqueda restringida para encontrar recursos que contienen esa clave de metadatos.
Genera valores de metadatos	Los valores de metadatos que el recurso genera. En el ejemplo, no se generan valores de metadatos. Cuando se hace clic en un valor de metadatos, se abre la vista Buscar en Live con la búsqueda restringida para encontrar recursos que contienen ese valor de metadatos.

Característica	Descripción
Permisos	Los permisos necesarios para el recurso.

Barra de herramientas de la vista Recurso

En esta tabla se describen las opciones de la barra de herramientas de la vista Recurso de Live.

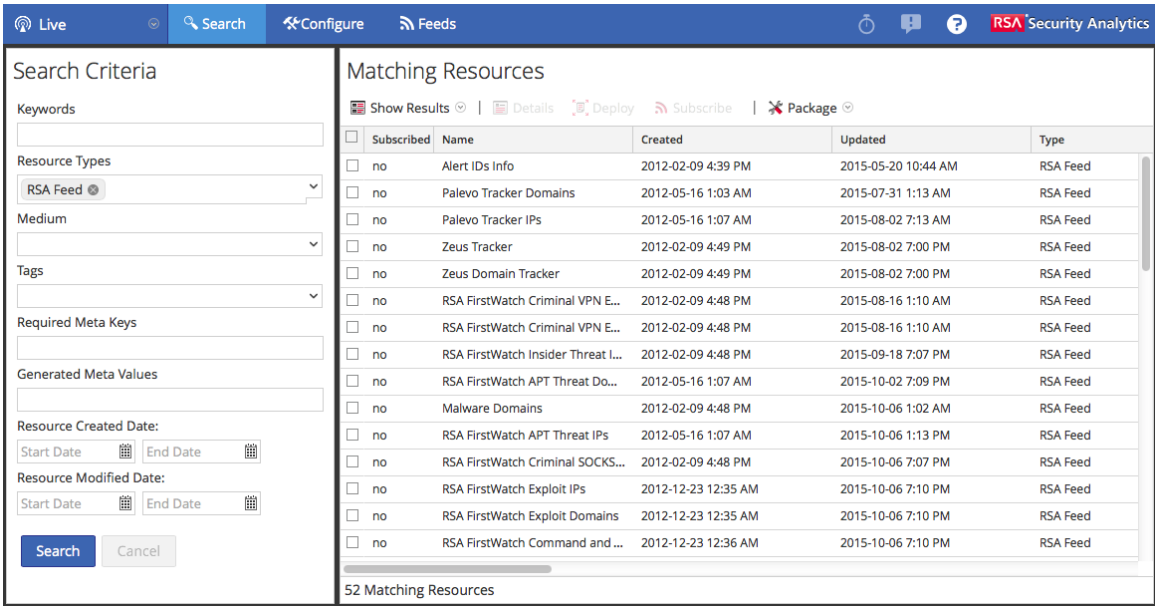
Característica	Ícono	Descripción
Descarga		Esta opción descarga el recurso que se muestra actualmente en la vista Recurso.
Suscribirse o cancelar suscripción		Esta opción suscribe o cancela la suscripción al recurso que se muestra actualmente en la vista Recurso. • Al hacer clic en **Suscribir** se abre un cuadro de diálogo que debe aceptar para recibir una notificación cuando se actualicen los recursos seleccionados. Puede cancelar o hacer clic en **Aceptar**. • Al hacer clic en **Cancelar suscripción** se pide la confirmación de que desea dejar de recibir la notificación de actualización de los recursos seleccionados. A continuación, puede elegir cancelar o puede hacer clic en **Cancelar suscripción** o en **Cancelar la suscripción y eliminar**, lo cual elimina el recurso de los servicios en los cuales se ha implementado.
Implementación		Esta opción proporciona una manera de implementar el recurso que se muestra actualmente en la vista Recurso. Al hacer clic en **Implementar** se abre el cuadro de diálogo Implementación manual de recursos.

Característica	Ícono	Descripción
Localizador de servicios	Service Locator	Esta opción muestra una lista de los servicios en los cuales se ha implementado el recurso que se muestra actualmente. Puede eliminar el recurso de todos los servicios o solo de los servicios seleccionados.

Vista Buscar en Live

La vista Buscar en Live proporciona la capacidad para navegar por los recursos del CMS Live configurado. Una vez que se encuentran las coincidencias de recursos, puede ver los detalles, suscribirse a los recursos e implementar los recursos en servicios y grupos de servicios.

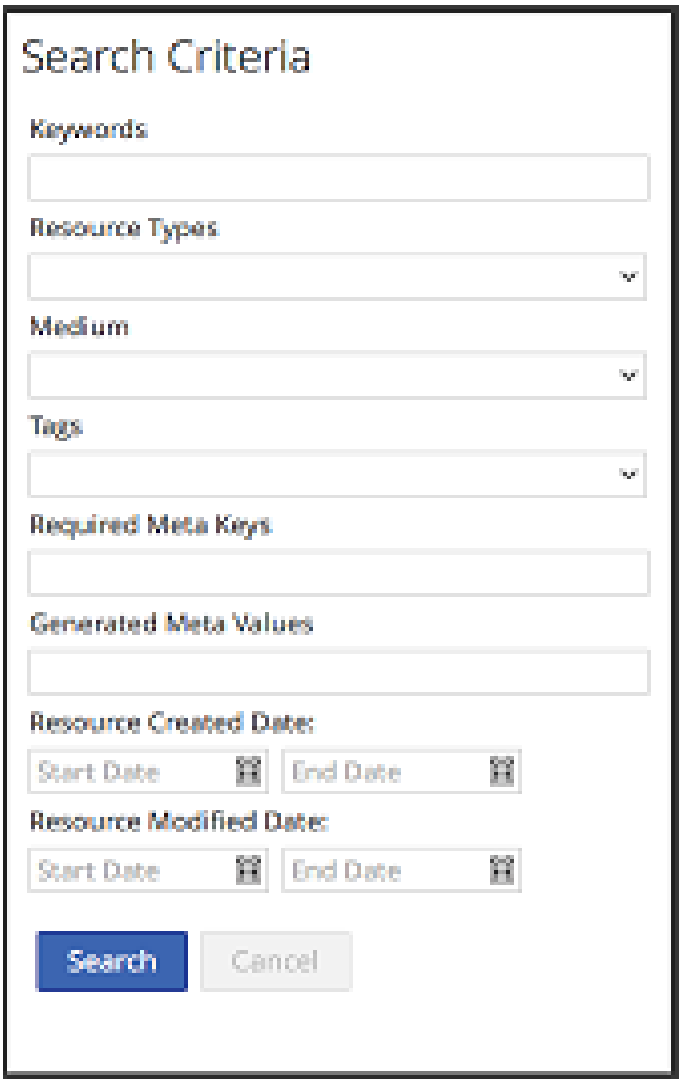
Este es un ejemplo de la vista Buscar.



La vista Buscar en Live tiene un panel para especificar los criterios de búsqueda y un panel que muestra las coincidencias de recursos. El panel Criterios de búsqueda se expande para proporcionar mayor ancho de visualización del panel Coincidencias de recursos.

Panel Criterios de búsqueda

Este es un ejemplo del panel Criterios de búsqueda.



En la siguiente tabla se proporcionan descripciones de las funciones del panel Criterios de búsqueda.

Característica	Descripción
Palabras clave	Ingrese una o más palabras clave para buscar recursos que incluyen estas palabras en su nombre o descripción. Cuando ingresa una palabra clave, puede utilizar comodines.

Característica	Descripción
Tipos de recursos	Seleccione los tipos de recursos en la lista desplegable para filtrar los recursos por tipo. Los valores posibles son: • Analítica avanzada (Warehouse) • Regla de aplicación de RSA • Módulo RSA CEP • Contenido de RSA • Regla de correlación de RSA • Regla de RSA Event Stream Analysis • Feed de RSA • RSA FlexParser • Acción personalizada de investigador de RSA • Log Collector de RSA • RSA Log Device • Analizador Lua de RSA • Reglas de malware de RSA • Clave de metadatos de RSA • Lista de RSA Security Analytics • Informe de RSA Security Analytics • Regla de RSA Security Analytics • Documento de orígenes de RSA

Característica	Descripción
(10.5.1 o posterior) Mediano	Seleccione uno o más medios en la lista desplegable para buscar contenido en función del origen de metadatos. Los valores disponibles para medio son los siguientes: • **registro**: se aplica al contenido que utiliza metadatos derivados de datos de registros • **paquete**: se aplica al contenido que utiliza metadatos derivados de paquetes de red • **paquetes y registros**: se aplica al contenido que correlaciona metadatos derivados a través de datos de paquetes y registros
Etiquetas	Seleccione las etiquetas de metadatos en la lista desplegable para navegar en función del etiquetado de los metadatos. Por ejemplo, para buscar recursos en un Log Decoder, seleccione la etiqueta **netwitness para registros**. Como alternativa, puede hacer clic en una etiqueta en el panel Coincidencias de recursos para insertarla en este campo.
Claves de metadatos requeridas	Ingrese una clave de metadatos específica; por ejemplo, **threat.source**. Como alternativa, puede hacer clic en una clave de metadatos en el panel Coincidencias de recursos para insertar esa etiqueta en este campo.
Valores de metadatos generados	Ingrese un valor de metadatos generado; por ejemplo, **netwitness**. Como alternativa, puede hacer clic en una clave de metadatos generada en el panel Coincidencias de recursos para insertar esa etiqueta en este campo.
Fecha de creación de investigación	Especifique un rango de fechas durante el cual se crearon los recursos. Por ejemplo, para navegar por los recursos que se crearon entre el 1 y el 4 de enero, seleccione 1 de enero como la fecha inicial y 4 de enero como la fecha de finalización. Debe ingresar fechas en formato mm/dd/aaaa o hacer clic en  y elegir fechas de un calendario.

Característica	Descripción
Fecha de modificación de investigación	Especifique un rango de fechas durante el cual se modificaron los recursos. Por ejemplo, para navegar por los recursos que se modificaron entre el 1 y el 4 de enero, seleccione 1 de enero como la fecha inicial y 4 de enero como la fecha de finalización. Debe ingresar fechas en formato mm/dd/aaaa o hacer clic en y elegir fechas de un calendario.
Buscar	Haga clic en **Buscar** para enviar la solicitud de búsqueda al servidor de Live. Los criterios de búsqueda más específicos revuelven coincidencias de recursos más rápidamente.
Cancelar	Haga clic en **Cancelar** para cancelar la búsqueda en curso.

Panel Coincidencias de recursos

El panel Coincidencias de recursos presenta cada recurso según las selecciones realizadas en el panel Criterios de búsqueda. Los resultados se muestran inicialmente en una cuadrícula, pero puede cambiar entre dos opciones para mostrar resultados: en detalle o en cuadrícula.

Resultados en detalle

En los resultados en detalle, puede hacer clic en una etiqueta, clave de metadatos o valor de metadatos de un recurso para completar automáticamente el panel Criterios de búsqueda y agilizar los resultados de la búsqueda.

En la siguiente tabla se describen los elementos de los resultados detallados.

Característica	Descripción
Ícono Tipo de recurso	Una representación gráfica del tupo de recurso. Por ejemplo
Nombre	El nombre del recurso, por ejemplo, **Administración de grupos**.
Tipo	El tipo de recurso, por ejemplo, **Regla**.
Fragmento C	La fecha en que el recurso se actualizó por última vez, por ejemplo, **2015-09-15 4:27 PM**.
Versión	La versión del recurso, por ejemplo, **0.1**.

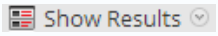
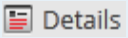
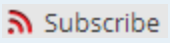
Característica	Descripción
Tamaño	El tamaño del recurso, por ejemplo, **153 B**.
Subscribed	Estado de suscripción: • **sí**: Esta instancia de Security Analytics está suscrita a este recurso de contenido. • **no**: Esta instancia de Security Analytics no se ha suscrito a este recurso de contenido.
Descripción	La descripción del recurso, por ejemplo, **Administración de grupos-reglas de cumplimiento de normas**.
Etiquetas	Las etiquetas que se aplican al recurso. Cuando se hace clic en una etiqueta, la búsqueda se restringe a los recursos que contienen esa etiqueta. Por ejemplo, featured, apt.
Claves de metadatos	Las claves de metadatos que se aplican al recurso. Cuando se hace clic en una clave de metadatos, la búsqueda se restringe a los recursos que contienen esa clave de metadatos. Por ejemplo, threat.category, threat.desc, threat.source.
Valores de metadatos de recursos	Los valores de metadatos que generó el recurso. Cuando se hace clic en un valor de metadatos, la búsqueda se restringe a los recursos que generaron el valor de metadatos. Por ejemplo, netwitness.

Resultados en cuadrícula

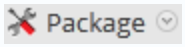
En la vista de cuadrícula, puede seleccionar uno o más recursos y utilizar las opciones adicionales en la barra de herramientas para ver los detalles de un único recurso, suscribirse a los recursos e implementar recursos.

En la siguiente tabla se describen los elementos de los resultados de la cuadrícula.

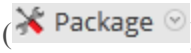
Característica	Descripción
	Cuadrícula

Característica	Descripción
Subscribed	Estado de suscripción: • **sí**: Esta instancia de Security Analytics está suscrita a este recurso de contenido. • **no**: Esta instancia de Security Analytics no se ha suscrito a este recurso de contenido.
Nombre	El nombre del recurso, por ejemplo, **Administración de grupos**.
Created	La fecha en que se creó el recurso, por ejemplo, **2015-08-12 3:11 PM**.
Fragmento C	La fecha en que el recurso se actualizó por última vez, por ejemplo, **2015-09-15 4:27 PM**.
Tipo	El tipo de recurso, por ejemplo, **Regla**.
Descripción	La descripción del recurso, por ejemplo, **Administración de grupos-reglas de cumplimiento de normas**.
Barra de herramientas	
	Este menú ofrece dos formas para ver los resultados de búsqueda: **en detalle** y **en cuadrícula**.
	Esta opción se aplica a un único recurso seleccionado. Al hacer clic en **Detalles** se abre el recurso seleccionado en la vista Recurso de Live.
	Esta opción se aplica a uno o más recursos seleccionados.
	Esta opción se aplica a uno o más recursos seleccionados. Al hacer clic en **Suscribir** se abre un cuadro de diálogo que pide confirmar que desea recibir una notificación cuando se actualicen los recursos seleccionados.

Característica	Descripción

	Este menú ofrece dos funciones de creación de paquetes para los recursos seleccionados:
	• **Crear**: crea un archivo **resourceBundle.zip** que contiene los recursos seleccionados y abre un cuadro de diálogo en el que puede:
	  • abrir el archivo, o
	  • guardar el archivo para su posterior implementación.
	• **Implementar**: Abre el asistente de implementación, en el cual puede escoger un archivo **resourceBundle.zip** e implementarlo.

Consulte también

Para obtener más detalles sobre la implementación () o la implementación de un paquete (), consulte Implementar modelos de Warehouse Analytics.

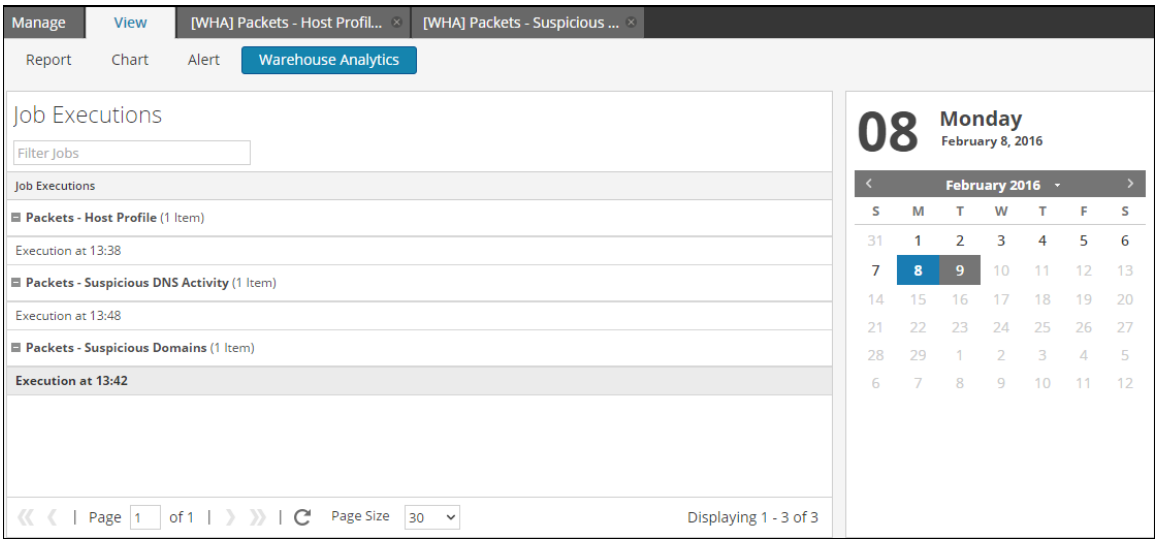
Panel Ver todas las tareas

El panel Ver todas las tareas muestra todos los trabajos y su información.

La página Ver todas las tareas incluye los siguientes paneles:

1. Salida de trabajos
2. Calendario de trabajos
3. Hora de trabajos

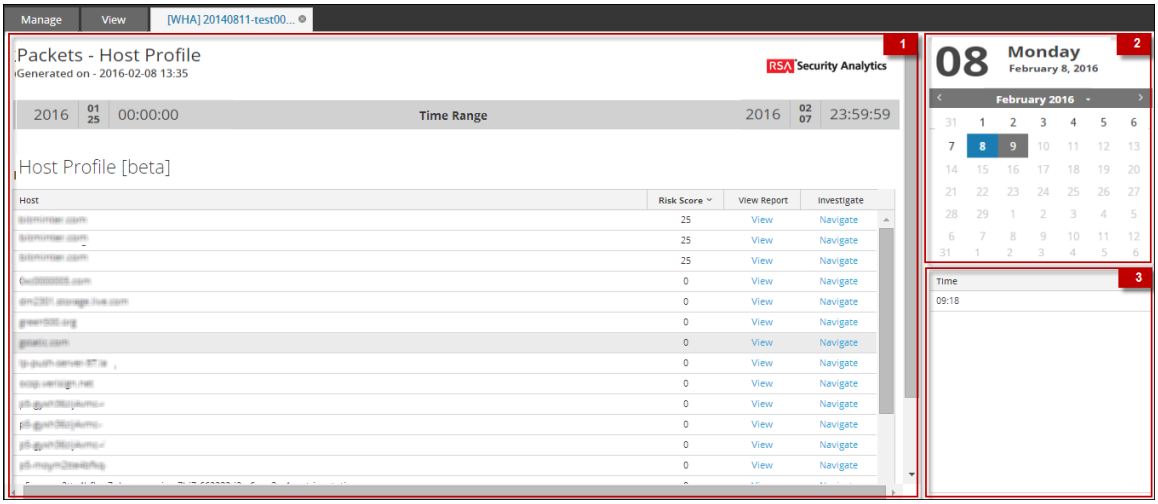
En la siguiente figura se muestran los diferentes paneles de esta vista.



En la siguiente tabla se indican las operaciones de la barra de herramientas Ejecuciones de trabajos.

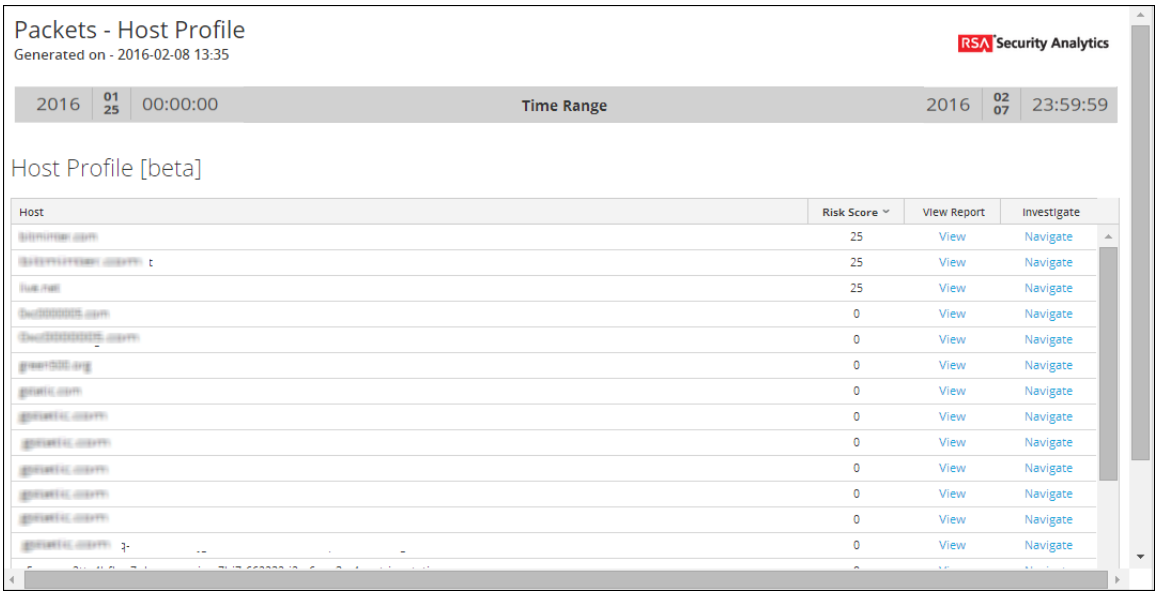
Operation	Descripción
Filter Jobs	Busca calendarios en función del nombre del trabajo calendarizado para un día calendario seleccionado.

Haga clic en cualquiera de los trabajos mostrados para verlo.



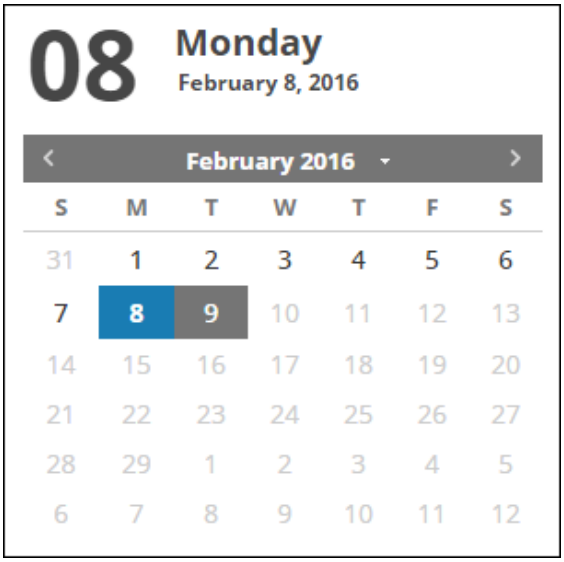
Panel Salida de trabajos

El panel Salida de trabajos muestra el trabajo con el nombre del calendario de trabajos, la hora de generación del trabajo y el trabajo real con la lista de dominios sospechosos y su puntaje de riesgo.



Panel Calendario de trabajos

El panel Calendario de trabajos se usa para seleccionar una fecha en el calendario. De acuerdo con la fecha que selecciona, se muestra la lista de trabajos que se ejecutaron correctamente en esa fecha.



Panel Hora de trabajos

El panel Hora de informes muestra la hora en que se ejecutó realmente el trabajo.

Panel Ver un trabajo programado

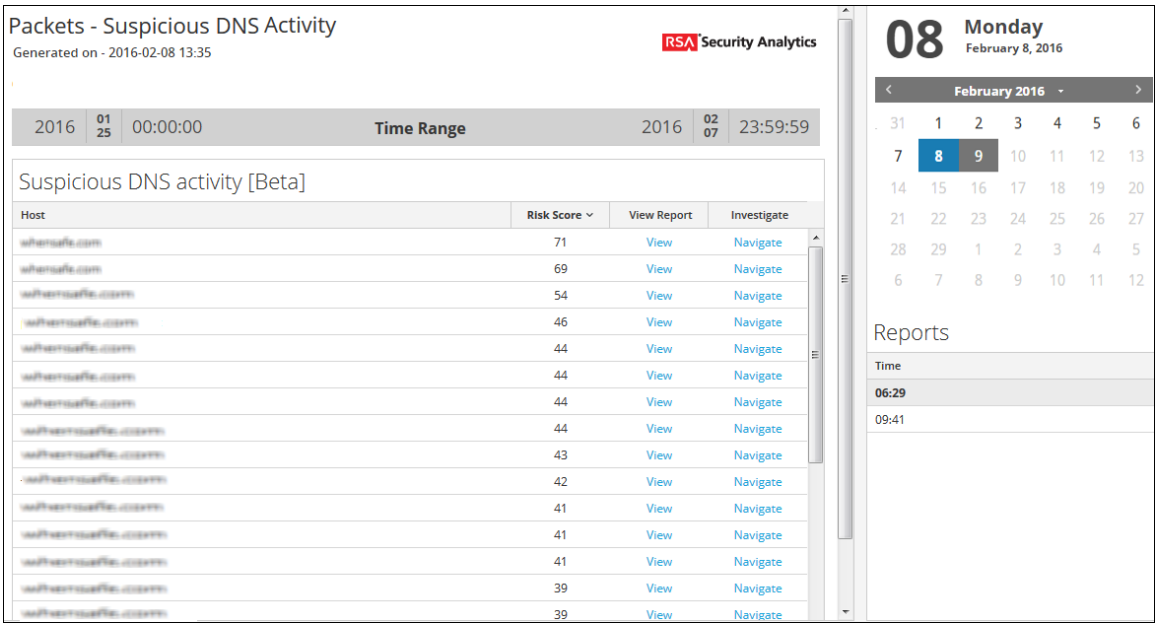
En este tema se describen las funciones del panel Ver un trabajo programado. En el panel Ver un trabajo programado se muestran todos los trabajos calendarizados y las opciones para cada uno de ellos y permite ver informes.

El panel Ver un trabajo programado incluye los siguientes paneles:

- Salida de trabajos
- Calendario de trabajos
- Hora de trabajos

Para obtener más información sobre cada uno de estos paneles, consulte Panel Ver todas las tareas.

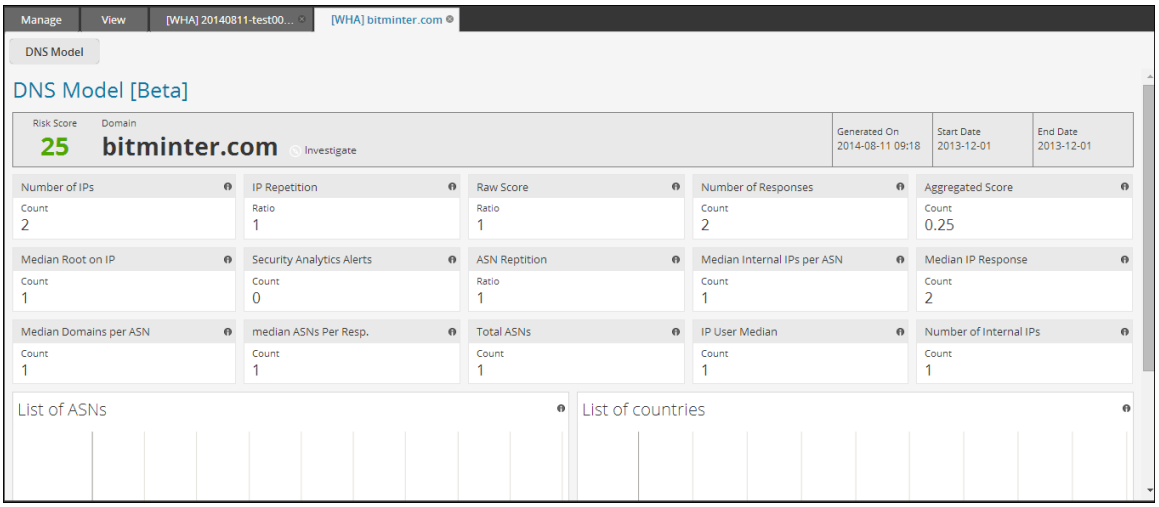
En la siguiente figura se muestra el panel Ver un trabajo programado.



En la siguiente tabla se indican las diversas columnas del panel Ver un trabajo programado.

Columna	Descripción
Host	La lista de dominios sospechosos.
Puntaje de riesgo	Indica el puntaje en función del dominio que se considera sospechoso. Por ejemplo, el puntaje de riesgo 100 indica que el dominio es altamente sospechoso.
Ver informe	Haga clic para ver un informe en la página Paso 4. Analizar un informe de Warehouse Analytics .
Investigar	Haga clic para investigar a partir de un informe de Warehouse Analytics.

Haga clic en cualquiera de los dominios sospechosos que se enumeran y, a continuación, haga clic en **Ver** para ver el informe deseado.

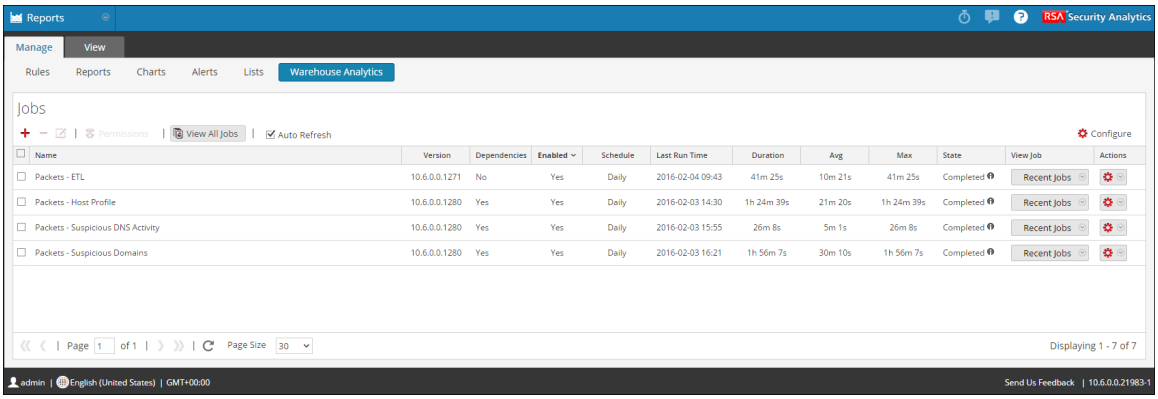


Vista Warehouse Analytics

En este tema se describen las funciones de la vista Warehouse Analytics. La vista Warehouse Analytics permite administrar, ver y configurar permisos para trabajos.

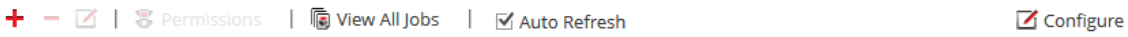
La vista Warehouse Analytics consta de lo siguiente:

- Barra de herramientas de Warehouse Analytics
- Lista de Warehouse Analytics

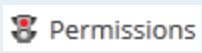
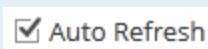
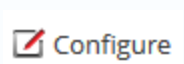


Barra de herramientas de Warehouse Analytics

La barra de herramientas de Warehouse Analytics permite agregar, editar, eliminar y ver todos los trabajos. Con este panel, también puede establecer permisos para un trabajo.



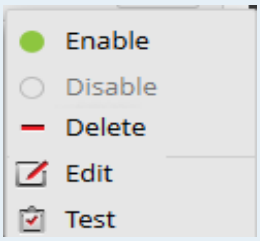
En la siguiente tabla se indican las operaciones disponibles en la barra de herramientas de Warehouse Analytics.

Operation	Descripción
	Cree un nuevo calendario de trabajos o un trabajo calendarizado.
	Elimina el calendario de trabajos seleccionado.
	Edita el calendario de trabajos seleccionado. **Nota:** Haga doble clic en un calendario de trabajos deseado para editarlo.
	Establezca el permiso de acceso para un calendario de trabajos.
	Vea todos los calendarios de trabajos.
	Actualice automáticamente la lista de trabajos calendarizados.
	Permite configurar trabajos de Warehouse Analytics.

Lista de Warehouse Analytics

La lista de Warehouse Analytics muestra todos los trabajos en formato tabular. En la siguiente tabla se indican las diversas columnas de la lista de Warehouse Analytics y su descripción.

Columna	Descripción
Nombre	El nombre del trabajo. **Nota:** Cuando actualiza a 10.6, los trabajos para los modelos Dominios sospechosos, Actividad de DNS sospechosa y Perfil de host aparecen como OBSOLETOS. Debe crear nuevos trabajos para cada uno de estos modelos y puede usar los trabajos "OBSOLETOS" como referencia.
Versión	La versión del trabajo.
Dependencias	Si el trabajo tiene una dependencia, se enumera con **Sí** en esta columna. Cuando mantiene el mouse sobre la dependencia, puede ver el nombre de la dependencia.
Activado	Indica si el trabajo está o no habilitado.
Calendario	El tipo de calendario para la configuración de la ejecución. Esta es una ejecución diaria.
Hora de última ejecución	La última vez que se ejecutó el trabajo.
Duración	El tiempo que tardó la ejecución del trabajo.
Prom.	El tiempo promedio que tardó la ejecución del trabajo.
Máx.	El tiempo máximo que tardó la ejecución del trabajo.

Columna	Descripción
State	Indica el estado del trabajo calendarizado. • **Programado**: Si un trabajo está calendarizado para ejecutarse de forma diaria, semanal o mensual o más adelante, su estado se muestra como calendarizado para la primera ejecución. • **En línea de espera**: si un trabajo aún espera su ejecución, su estado se muestra como en línea de espera. • **En ejecución**: Si el programa de trabajos está en curso, su estado se muestra como en ejecución. • **Fallido**: si en un trabajo con un modelo seleccionado fallan las ejecuciones del calendario, el estado del trabajo se muestra como fallido. • **Completado**: Si el calendario de trabajos se ejecuta correctamente, el estado del trabajo se muestra como completado.
Ver trabajo	La lista de trabajos recientes.
Acciones 	• Habilitar un trabajo programado, consulte Activar o desactivar un trabajo programado. • Deshabilitar un trabajo programado, consulte Activar o desactivar un trabajo programado • Eliminar un trabajo, consulte Eliminar un trabajo de Warehouse Analytics • Editar un trabajo, consulte Editar un trabajo de Warehouse Analytics • Probar un trabajo, consulte Probar un trabajo de Warehouse Analytics.