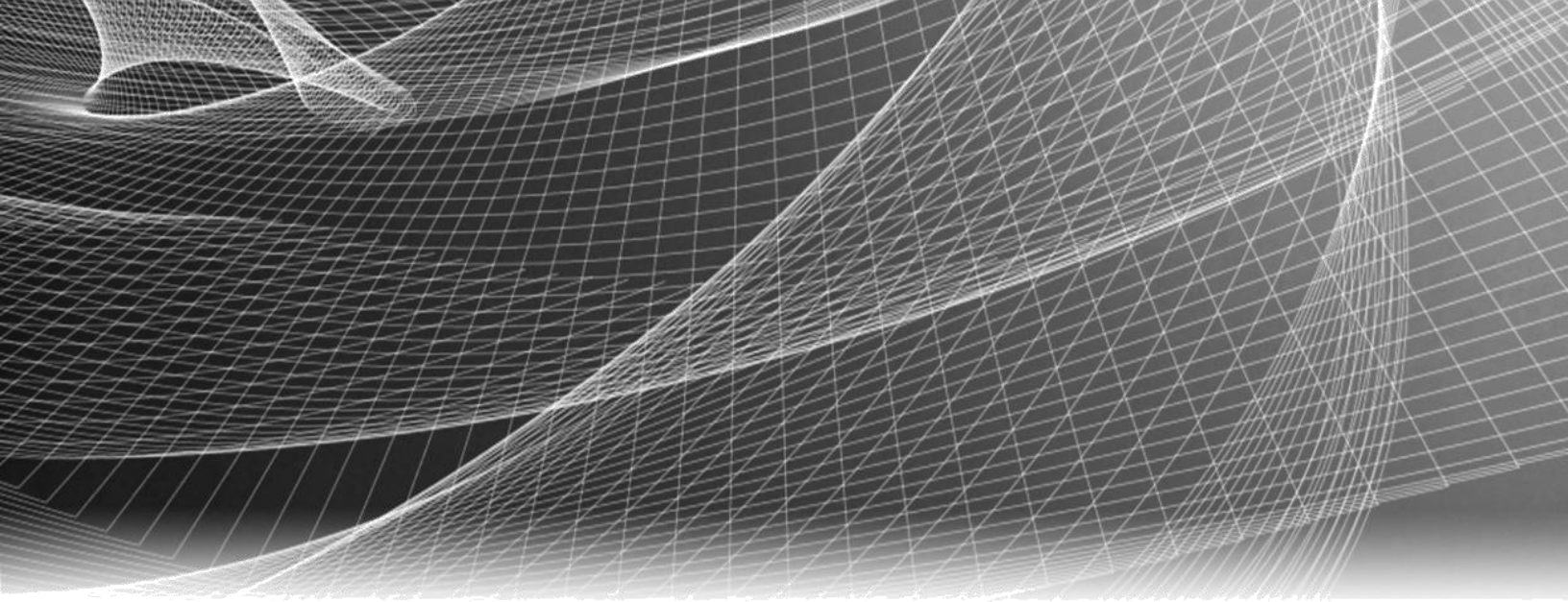


RSA Security Analytics

Instrucciones para la actualización a 10.6

RSA

EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto del acuerdo de licencia que se aplica al software de otros fabricantes en este producto puede encontrarse en el archivo thirdpartylicenses.pdf.

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

El uso, la copia y la distribución de cualquier software de EMC descrito en esta publicación requieren una licencia de software correspondiente. 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.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". EMC CORPORATION NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Instrucciones para la actualización a Security Analytics 10.6

Instrucciones para la actualización a Security Analytics 10.6

Security Analytics 10.6 proporciona nuevas funciones, mejoras y reparaciones para todos los productos del conjunto de aplicaciones Security Analytics. Los componentes del conjunto de aplicaciones son el servidor de Security Analytics, Broker, Concentrator, Log Decoder y Decoder, Hybrid, All-in-One, Malware Analysis, Archiver, Event Stream Analysis, Context Hub, Log Collector, Security Analytics Warehouse, Workbench, IPDB Extractor y Reporting Engine. Las instrucciones de esta guía se aplican a los hosts físicos y virtuales, salvo que se indique lo contrario.

Ruta de actualización

Las siguientes rutas de actualización son compatibles con Security Analytics 10.6.

- 10.4.1.x a 10.6.
- 10.5.0.x a 10.6.
- 10.5.1.x a 10.6.

Nota: Las versiones 10.5.2 y superiores no son compatibles como rutas de actualización a 10.6.

Precaución: 1.) Si está ejecutando la versión 9.8, póngase en contacto con el servicio al cliente para obtener instrucciones para la actualización. **2.)** Si está ejecutando Security Analytics versión 10.3.x, debe actualizar a 10.4.1 antes de poder actualizar a 10.6. Consulte la ***Guía de actualización de RSA Security Analytics 10.4.1*** en SCOL (https://knowledge.rsasecurity.com/) para obtener instrucciones detalladas sobre la actualización de 10.3.x a 10.4.1 (si usa Event Stream Analysis en 10.3.x, debe migrar sus reglas a 10.4.1). **No puede acceder a los RPM de actualización de 10.4.1 desde el repositorio de actualización de Live. Esto significa que debe descargar los RPM de actualización de 10.4.1 desde SCOL al repositorio de actualización local.**

Cambios de la terminología en 10.6

En la siguiente tabla se enumeran los cambios en la terminología de Security Analytics que se implementaron en 10.6. Se enumera cada término nuevo, el término de las versiones anteriores que reemplazó y una descripción de cada término.

Última modificación: 23 de febrero de 2016, 13:46 h

10.6.0.0	Antes de 10.6.0.0	Descripción
Repositorio de actualización de Live	repositorio Yum, SMCUPDATE	Repositorio de Live en el cual RSA publica las actualizaciones de las versiones de software de Security Analytics de manera habitual.
Repositorio de actualización local	Repositorio del servidor de SA, repositorio Yum de SA	Repositorio local en su implementación de Security Analytics desde el cual se aplican las actualizaciones de las versiones de software a un host. Tiene dos opciones para completar el repositorio de actualización local en su implementación de Security Analytics: • Opción 1: Conectarse al repositorio de actualización de Live. • Opción 2: Descargar actualizaciones de versiones desde SecureCare Online (SCOL) y cargarlas en el repositorio de actualización local.
Host que no es de servidor de Security Analytics		Cualquier host de la implementación de Security Analytics distinto de un host del servidor de SA. Consulte **Host del servidor de Security Analytics**.
Host del servidor de Security Analytics	Host de SA, dispositivo de SA	**Nota:** Se abrevia **host del servidor de SA** en los mensajes y en los gráficos donde hay restricciones de espacio. Host en el cual reside el servidor de Security Analytics. El servidor de Security Analytics contiene la interfaz del usuario y el servicio de administración de servicios (SMS). Cuando actualiza a una versión nueva, el servidor de Security Analytics se debe actualizar primero. Si tiene una implementación de Security Analytics con versiones combinadas, el servidor de Security Analytics debe tener la versión más reciente en su implementación.

Última modificación: 23 de febrero de 2016, 13:46 h

10.6.0.0	Antes de 10.6.0.0	Descripción
		Según su implementación, puede alojar los siguientes servicios en el host del servidor de Security Analytics además del servidor de Security Analytics y SMS: • Administración de orígenes de eventos • Reporting Engine • Malware Analysis • IPDB Extractor • Incident Management • Intermediador

Última modificación: 23 de febrero de 2016, 13:46 h

Mejoras en el proceso de actualización de los hosts

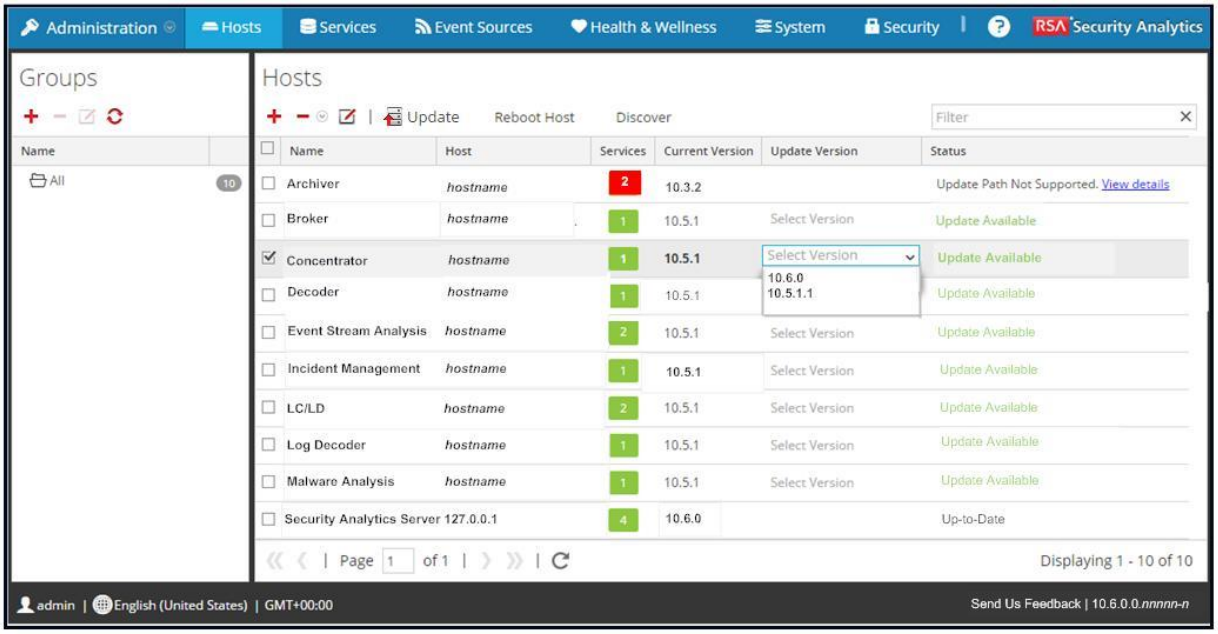
La jerarquía de actualizaciones de Security Analytics es la siguiente: versión principal, versión secundaria, service pack y parche. Es la convención de asignación de nombres de las actualizaciones es ***major-release.minor-release.service-pack.patch***. Por ejemplo, 10.6.1.2 representa:

- 10 = versión principal
- 6 = versión secundaria
- 1 = service pack
- 2 = parche.

Cambios en la vista Hosts

La vista Hosts se usa para actualizar un host a una versión nueva. Se hicieron varios cambios a esta vista en 10.6. Cuando hay actualizaciones de versiones disponibles para un host, se muestra Actualización disponible en la columna **Estado** y la versión de actualización disponible que se desea se elije en la columna **Seleccionar versión**. En la columna **Estado** se indica el estado actual del proceso de actualización a medida que avanza y se solicitan acciones en caso de ser necesarias. Consulte **Actualización de una versión de host** en la sección **Conceptos básicos** de la **Guía de introducción de hosts y servicios** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información sobre la vista Hosts en 10.6 y el proceso de actualización mejorado.

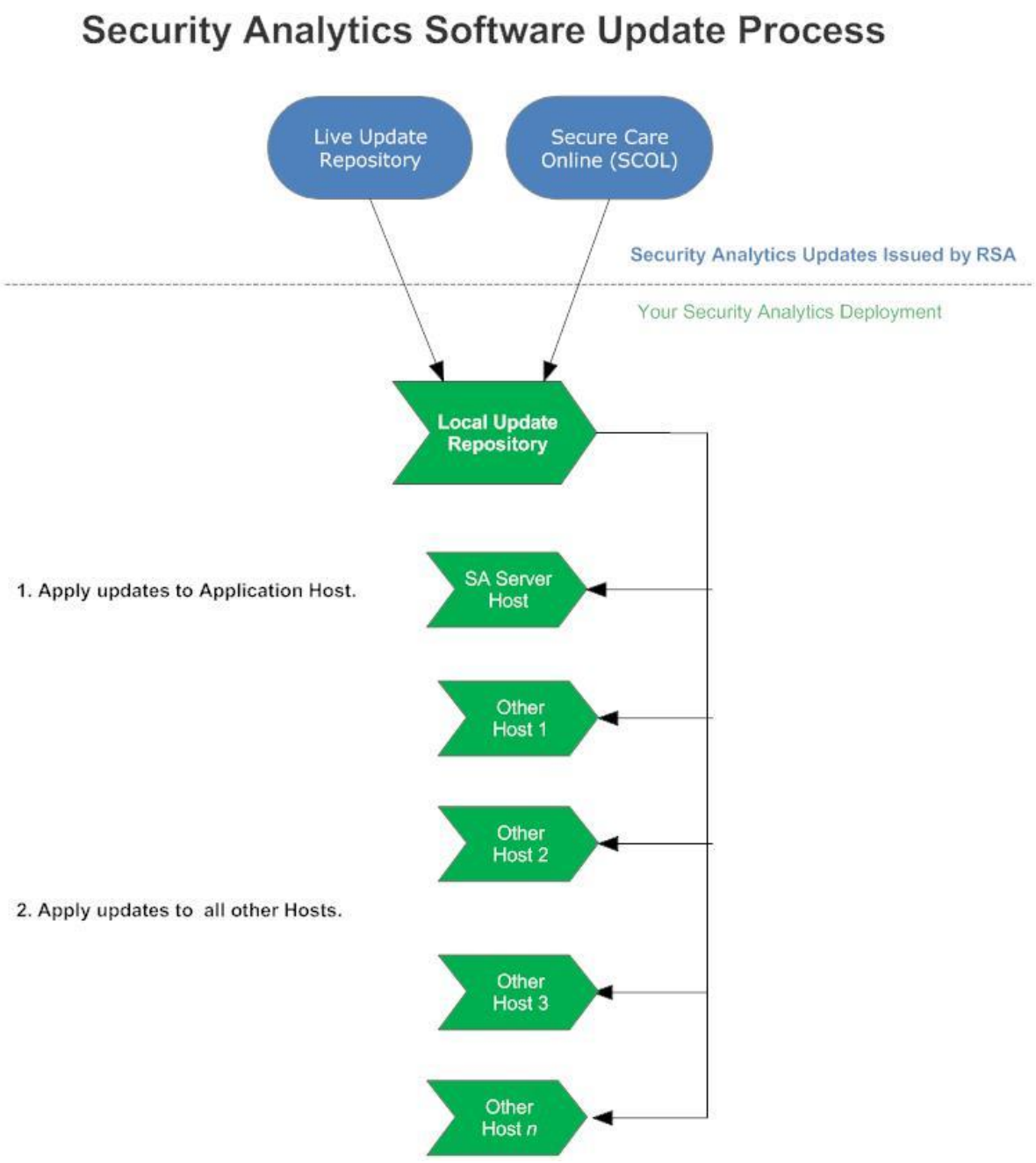
Nota: La información sobre **Memoria total**, **CPU**, **SO** y **Tiempo de actividad** ya no se muestra en la vista Hosts. Puede monitorear esta información en Administration > Estado y condición > Navegador de estadísticas del sistema si selecciona el host y especifica la estadística (por ejemplo, **Memoria total**).



Última modificación: 23 de febrero de 2016, 13:46 h

Proceso de actualización de Security Analytics

En la siguiente figura se ilustra cómo se completa el repositorio de actualización local con las actualizaciones de versiones de Security Analytics más recientes y cómo se aplican estas actualizaciones a los hosts.



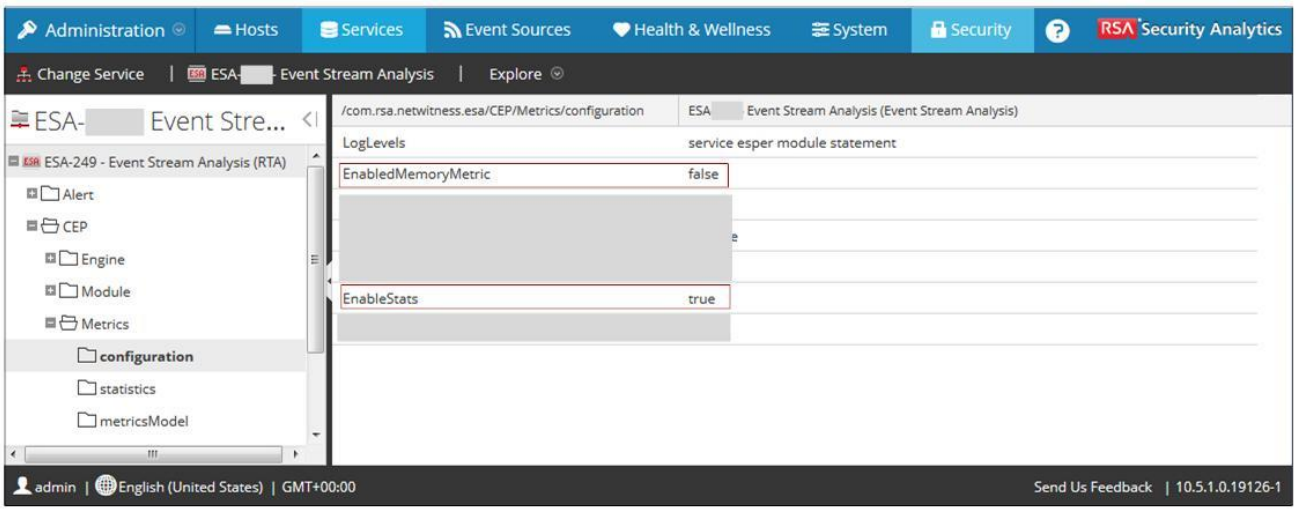
Cambios en los parámetros de configuración de Event Stream Analysis para los clientes que actualizan a 10.6 desde 10.5.0.x

En 10.5.1, RSA presentó un nuevo parámetro de Event Stream Analysis denominado `EnableStats`. Si actualiza a 10.6 desde 10.5.0.x, `EnableStats` está habilitado (configurado en `true`) en forma predeterminada. Este parámetro habilita la nueva función Uso estimado de la memoria que permite ver el uso estimado de la memoria para cada regla en Estado y condición > Navegador de estadísticas del sistema.

En 10.6, RSA inhabilitó la función de métricas de memoria de 10.5.0.x (el parámetro `EnableMemoryMetric` se configuró en `false`) de forma predeterminada porque tiene un impacto muy negativo en el rendimiento.

Advertencia: RSA recomienda habilitar el parámetro `EnableMemoryMetric` (configurar el parámetro `EnableMemoryMetric` en `true`) únicamente con fines de depuración.

La siguiente vista Explorar es un ejemplo de cómo los parámetros `EnableStats` y `EnableMemoryMetric` se configuran de inmediato después de la actualización a 10.6.



Configuración del “modo estricto” para 10.6

Desde 10.2 en adelante, Security Analytics ha utilizado un analizador moderno para las reglas y las consultas, el cual define estrictamente la sintaxis válida. Cuando un servicio principal encuentra sintaxis obsoleta, escribe una advertencia acerca de esta en los registros de Security Analytics. Security Analytics ahora aplica el análisis estricto a las reglas de aplicación, red y correlación nuevas. El analizador antiguo de las generaciones anteriores, ahora obsoleto, permite una sintaxis ambigua que puede dar lugar a resultados imprevistos.

Última modificación: 23 de febrero de 2016, 13:46 h

Nota: Security Analytics continuará siendo compatible con la sintaxis obsoleta en 10.6.x.x, pero no lo será en las versiones posteriores.

RSA recomienda corregir las reglas anteriores a 10.6 que contengan sintaxis obsoleta antes de actualizar a 10.6. Puede corregir la sintaxis obsoleta antes o después de la actualización a 10.6 de acuerdo con su preferencia.

Después de la actualización a Security Analytics 10.6, las reglas con sintaxis obsoleta se resaltan en la interfaz del usuario. En el Editor de regla se proporcionan mensajes de globo adicionales. Después de corregir las reglas, los elementos resaltados desaparecen.

Las estadísticas **/decoder/config/rules/rule.errors** y **/concentrator/config/rules/rule.errors** que se incorporaron en 10.6 contienen el conteo de reglas con errores. Si **rule.errors** es distinto de cero, Security Analytics genera una alerta de Estado y condición para indicar que debe corregir las reglas.

Además, existe una ruta de migración para las consultas desde Reporting e Investigation. Después de una actualización desde una versión anterior, el sistema funciona en el modo obsoleto (lo controla **/sdk/config/query.parse**). En el modo obsoleto, el servicio continúa utilizando el analizador antiguo para todas las consultas que no pasan el análisis estricto. Los errores se registran y se envía un mensaje al cliente en el cual se informa la falla del análisis estricto, pero la consulta se ejecuta y devuelve resultados como en las versiones anteriores. Debe monitorear los registros y los clientes externos en busca de informes, tableros, reglas, etc. que estén escritos con sintaxis obsoleta y resolver esos problemas a medida que los encuentra.

Después de resolver los problemas, puede cambiar todos los servicios principales (Decoders, Log Decoders, Concentrators, Brokers y Archivers) al modo estricto y monitorearlos en busca de problemas. En el modo estricto no se utiliza el analizador antiguo y cualquier infracción en el análisis devuelve errores. Esta tarea se debe ejecutar antes de cualquier actualización principal después de 10.6, porque el analizador antiguo se puede eliminar en versiones futuras y no existiría la opción de funcionamiento en el modo obsoleto.

De manera predeterminada, todas las instalaciones funcionan en el modo estricto. Si planea agregar un dispositivo nuevo a una infraestructura existente que se ejecuta en el modo obsoleto, en la vista Explorar (Administration > Servicios > seleccione un servicio y, en el menú Acciones, seleccione Ver > Explorar), puede cambiar **/sdk/config/query.parse** al modo obsoleto hasta que la plataforma completa se haya cambiado al modo estricto.

En Security Analytics 10.6, toda la validación de reglas funcionará siempre en el modo estricto para impedir la creación de problemas de sintaxis.

Para obtener información adicional, consulte **Guía de reglas y consultas** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/).

Parche de seguridad de RSA Security Analytics del cuarto trimestre de 2015

El paquete de actualización de Security Analytics 10.6 contiene el parche de seguridad de RSA Security Analytics del cuarto trimestre de 2015.

Última modificación: 23 de febrero de 2016, 13:46 h

Tareas de preparación para la actualización

En este tema se enumeran las tareas necesarias para preparar la actualización a Security Analytics 10.6.

Solo para 10.4.1.x a 10.6: Tarea 1. Asegurarse de que haya espacio suficiente para la base de datos de Reporting Engine 10.6

Como parte de esta actualización, los datos de Reporting Engine se migran a nuevas bases de datos. Antes de la actualización, asegúrese de que haya espacio en disco suficiente disponible para la migración. Security Analytics respalda automáticamente la base de datos de Reporting Engine en la siguiente ubicación en el host del servidor de Security Analytics, `/home/rsasoc/soc/reporting-engine/ statusdb/statusmanager.h2.db`, para que pueda volver a esta si encuentra un problema inusual, como los que se describen en Monitorear la migración de Reporting Engine.

1. Asegúrese de contar con un espacio libre en disco mínimo correspondiente a 1.2 veces el tamaño de `statusmanager.h2.db` en el volumen donde existe el archivo.
   Por ejemplo, si `statusmanager.h2.db` tiene un tamaño de 1 gigabyte, deben estar disponibles por lo menos 1.2 gigabytes de espacio libre en disco para migrar la base de datos.

   Nota: Security Analytics asigna 200 gigabytes de espacio para Reporting Engine, espacio que usa el servicio Reporting Engine y su base de datos.

   - Use el siguiente comando para determinar la cantidad de espacio en disco disponible en el volumen donde existe el archivo `statusmanager.h2.db`.
     `df -h`

     El ejemplo muestra 198 gigabytes de espacio libre en disco.

     ```
     Filesystem            Size  Used Avail Use% Mounted on
     /dev/mapper/VolGroup02-rsasoc
                           200G  2.3G  198G   2% /home/rsasoc
     ```

   - Use el siguiente comando para determinar el tamaño del archivo `statusmanager.h2.db`.
     `du -h /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`

     Si el archivo `statusmanager.h2.db` tiene un tamaño de 1 gigabyte, pero el espacio libre disponible es de solo 1 gigabyte, libere por lo menos 0.2 gigabytes de espacio en disco, como se explica en el paso siguiente.
   - Si no tiene espacio en disco suficiente, puede usar las siguientes tareas para liberar espacio en disco.
     - Transfiera los archivos archivados de `/home/rsasoc/rsa/soc/reporting-engine/archives/` a otro volumen. El siguiente comando es un ejemplo de cómo transferir archivos archivados:
       `mv /home/rsasoc/rsa/soc/reporting-engine/archives/contentstore.20150302170101.tgz target-director`

Nota: De manera rutinaria, Security Analytics archiva un subconjunto de contenido de creación de informes en `/home/rsasoc/rsa/soc/reporting-engine/archives/`. Puede transferir cualquier archivo que se archive en `home/rsasoc/rsa/soc/reporting-engine/archives/` a otra ubicación y regresarlo una vez que Reporting Engine se actualice a 10.6.

- Elimine los archivos no deseados del volumen en el cual existe `statusmanagerdb`.
  "Archivos no deseados" se refiere a los archivos que crea el usuario en el volumen.

Tarea 2. Revisar los puertos principales en 10.6 y abrir los puertos del firewall

Revise los cambios a los puertos principales en el tema **Arquitectura y puertos de red** de la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para que pueda reconfigurar los servicios de Security Analytics y el firewall. El siguiente puerto debe estar disponible para 10.6

- Puerto del servicio Context Hub de Event Stream Analysis (ESA). Asegúrese de que el host de ESA que ejecuta el servicio Context Hub pueda acceder al puerto 50022.

Precaución: No realice la actualización hasta que los puertos del firewall estén configurados.

Tarea 3. Asegurarse de que los puntos de montaje de IPDB estén accesibles

Asegúrese de que todos los puntos de montaje de IPDB Extractor estén accesibles. Consulte **Paso 1. Montar la IPDB** en la sección **Configurar el servicio IPDB Extractor** de la **Guía de configuración del servicio IPDB Extractor** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener instrucciones detalladas sobre cómo configurar los puntos de montaje de IPDB.

Tarea 4. Corregir las reglas

Todas las consultas y las condiciones de regla en los servicios de Security Analytics Core deben seguir estas pautas:

> **Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP.**

Por ejemplo:

- `extension = 'torrent'`
- `time='2015-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

Nota: El espacio a la derecha y a la izquierda de un operador es opcional.
Por ejemplo, puede usar `service=80` o `service = 80`.

Tarea 5. Designar un servidor primario y servidores secundarios de Security Analytics

Si dispone de una implementación de múltiples servidores de Security Analytics, debe especificar un servidor primario y servidores secundarios de Security Analytics y comprobar el archivo `rsa.repo`. Consulte **Implementación de múltiples servidores de Security Analytics** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información sobre este tipo de implementación.

Si implementa múltiples servidores de Security Analytics, tenga en cuenta lo siguiente:

1. Antes de actualizar el host del servidor de Security Analytics a 10.6, designe un servidor primario y servidores secundarios de Security Analytics. Consulte el tema **Secuencia de actualización de hosts** de la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener una descripción de esta implementación.
2. Antes de que actualice los demás hosts a 10.6, compruebe el archivo `rsa.repo` y asegúrese de que baseurl señale el host primario de Security Analytics con la siguiente cadena de comandos.
   ```
   # cat /etc/yum.repos.d/rsa.repo
   ```
   Se muestra la siguiente salida. `baseurl=http://Primary-SA-IP-Address/rsa/updates`

> **Precaución:** Un servidor secundario de Security Analytics tiene las siguientes limitaciones:
> - La funcionalidad de actualización de versiones de la vista Hosts es válida exclusivamente para el servidor primario de Security Analytics. Refleja el estado incorrecto para los servidores secundarios de Security Analytics, de modo que no debe actualizar a versiones nuevas de Security Analytics desde la vista Hosts de un servidor secundario de Security Analytics.
> - No puede usar las vistas Estado y condición.
> - No puede usar la función de conexiones de confianza.

Tarea 6. Respaldar el archivo de configuración de Malware Analysis en otro directorio

1. Respalde `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` en otro directorio seguro.
   Debe recuperar los valores de parámetros personalizados desde este respaldo después de actualizar el host de Malware Analysis a 10.6. La actualización crea un archivo de configuración nuevo con todos los parámetros configurados en los valores predeterminados.
2. Elimine `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml`.

Tarea 7. Respaldar la configuración

RSA recomienda crear una copia de respaldo de la configuración antes de realizar la actualización.
Consulte el tema **Respaldar y restaurar datos para hosts y servicios** de la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener reglas relacionadas con el respaldo de la configuración.

Tarea 8. Preparar la STIG para la actualización a 10.6

Si se aplicó el RPM de la STIG hardening de la Agencia de Sistemas de Información de Defensa (DISA) en Security Analytics, debe realizar la siguiente tarea para migrarlo a 10.6.

Para todos los hosts en los cuales está aplicada la STIG:

1. Obtenga acceso al host mediante el protocolo SSH.
2. `yum update glibc`
3. `reinicio del sistema`

En este punto, puede continuar con las tareas de actualización.

Tareas de actualización a 10.6 para las versiones 10.4.1.x a 10.5.0.x

En este tema se enumeran las tareas que debe completar para realizar la actualización a 10.6 desde las versiones 10.4.1.x a 10.5.0.x. Consulte Tareas de actualización a 10.6 para la versión 10.5.1.x si está actualizando desde 10.5.1.x.

Última modificación: 18 de febrero de 2016, 14:12 h

Tarea 1. Completar el repositorio de actualización local

Opciones

Tiene dos opciones para completar el repositorio de actualización local:

- Opción 1: Conectarse al repositorio de actualización de Live.
  Esto conecta el repositorio de actualización local de Security Analytics al repositorio de actualización de RSA Live a través de Internet con su cuenta de Live.
- Opción 2: Descargar actualizaciones de versiones desde **Download Central** (https://download.rsasecurity.com/).
  Si no permite que su implementación de Security Analytics se conecte a Internet, debe descargar los paquetes de actualización desde Download Central a un directorio local y, a continuación, cargarlos en el repositorio de actualización local de Security Analytics.

Opción 1: Conectarse al repositorio de actualización de Live

El acceso al repositorio de actualización de Live requiere y usa las credenciales de la cuenta de Live configuradas en **Administration** > **Sistema** > **Live**.

Nota: Cuando establezca la conexión inicial al repositorio de actualización de Live, accederá a todos los paquetes del sistema CentOS 6 y a los paquetes de producción de RSA. Esta descarga de más de 2.5 GB de datos tardará una cantidad indeterminada de tiempo de acuerdo con la conexión a Internet del servidor de Security Analytics y el tráfico del repositorio de RSA. El uso del repositorio de actualización de Live NO es obligatorio.

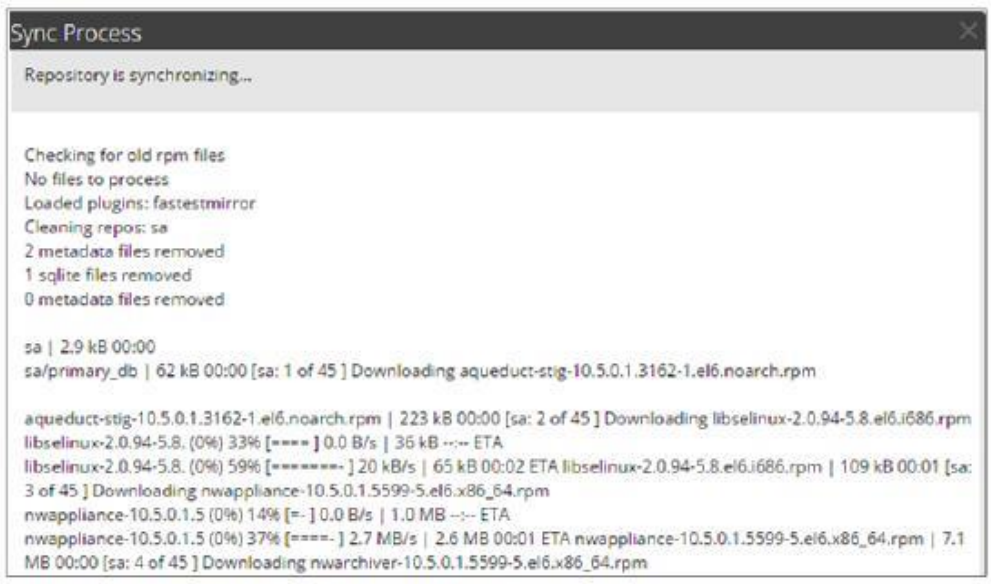
Para conectarse al repositorio de actualización de Live:

Nota: Si necesita usar un proxy para establecer conexión al repositorio de actualización de Live, puede configurar valores en Host proxy, Nombre de usuario de proxy y Contraseña de proxy. Consulte **Configurar un proxy para Security Analytics** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para la versión desde la cual está realizando la actualización.

1. Navegue a la vista **Administration** > **Sistema**, seleccione **Live** en el panel de opciones y asegúrese de que las credenciales estén configuradas. Si no lo están, configúrelas ahora y haga clic en **Probar conexión** y, a continuación, en **Aplicar**.
   Asegúrese de que **Probar conexión** se ejecute correctamente debido a que esta cuenta se usa para acceder al repositorio de actualización de Live.
2. Seleccione la pestaña **Actualizaciones** > **Configuración**.
3. Seleccione la casilla **Activado** y haga clic en **Aplicar**.
4. Use el botón **Probar conexión** para comprobar la conectividad. Asegúrese de que la prueba se ejecute correctamente.
   Se crea automáticamente un archivo `sa.repo` en el directorio `/etc/yum.repos.d/` del host del servidor de Security Analytics, el cual usa el repositorio de actualización local para comunicarse con el repositorio de actualización de Live.

Una vez habilitado, el repositorio de actualización de Live sincronizará y descargará todos los paquetes disponibles en el próximo evento calendarizado. También puede forzar un trabajo de sincronización desde la pestaña **Repositorio de actualizaciones** mediante la opción **Sincronizar ahora**. Después de actualizar ambos repositorios de actualización (el de Live y el local), puede ver todos los paquetes RPM descargados en la pestaña **Repositorio de actualizaciones** del panel **Administration** > **Actualizaciones**.

5. En el menú de Security Analytics, seleccione **Administration** > **Sistema**. Se muestra la vista **Información**.
6. En el panel izquierdo, seleccione **Actualizaciones**.
7. En la pestaña **Repositorio de actualizaciones**, haga clic en Synchronize Now.



Se muestra la pestaña **Repositorio de actualizaciones** con las actualizaciones que recuperó mediante la sincronización.

Advertencia: Si configura Public Key Infrastructure (PKI) en 10.5.0.2, Synchronize Now estará inhabilitado, razón por la cual debe asegurarse de que se haya realizado la sincronización automática del repositorio de actualizaciones antes de intentar la actualización de un host a 10.6 en la vista **Hosts**.

Opción 2: Descargar actualizaciones de versiones desde Download Central.

Debe completar el repositorio de actualizaciones de Security Analytics desde Download Central por los siguientes motivos:

- Si las actualizaciones de versiones que desea no están en el repositorio de actualización local (es decir, no aparecen en la lista Actualizaciones disponibles para un host en la columna Actualizaciones de la vista Hosts).
- Si su implementación de Security Analytics no tiene acceso a Internet.

Advertencia: Después de actualizar un host a 10.6 desde el repositorio de actualización local, tal vez no pueda acceder a versiones anteriores para actualizar otros hosts. Esto es producto del método que usa Security Analytics para administrar la estructura de archivos del repositorio de actualización local cuando usted completa este repositorio manualmente desde Download Central. Por ejemplo, si actualizó el host del servidor de Security Analytics a 10.5.1 y, a continuación, a 10.6, 10.5.1 no estará disponible para actualizar otros hosts. Debe descargar 10.5.1 desde Download Central y volver a actualizar manualmente el repositorio de actualización local.

Para completar el repositorio de actualización local desde Download Central:

1. Descargue el archivo **SA-10.6.0.0-UpdatePack-EL6.zip**, que contiene todos los archivos de actualización de Security Analytics 10.6, desde **Download Central** (https://download.rsasecurity.com/) a un directorio local.
2. En el menú de Security Analytics, seleccione **Administration** > **Sistema**.
3. En el panel izquierdo, seleccione **Actualizaciones**.
4. En la pestaña **Configuración**, asegúrese de que la casilla de verificación **Activar** no esté seleccionada.

5. En la pestaña **Actualizaciones manuales**, haga clic en **Cargar archivos**. Se muestra el cuadro de diálogo Cargar archivo.
6. Haga clic en , navegue hasta el directorio local donde colocó el archivo **SA-10.6.0.0-UpdatePack-EL6.zip** y selecciónelo.

   Nota: El archivo ZIP es muy grande y su carga en Security Analytics podría plantear problemas. Si esto ocurre, descomprímalo y cargue los archivos en grupos de menor tamaño.

   Los RPM de actualización de 10.6 se muestran en la pestaña **Actualizaciones manuales**.
   El estado de carga se muestra en la esquina inferior izquierda. Cuando la carga finaliza, el servidor de SA descomprime todos los paquetes rpm y los muestra en la pestaña **Actualizaciones manuales**.
7. Seleccione todos los archivos en la lista Actualizaciones manuales y haga clic en **Aplicar**.
   Esto transfiere los archivos RPM al repositorio de actualización local en el servidor de Security Analytics y los pone a disposición de los hosts.

   Precaución: No seleccione el archivo **SA-10.6.0.0-Manifest-EL6.zip**.

Tarea 2. Actualizar los hosts a 10.6 desde las versiones 10.4.1.x a 10.5.0.x

RSA incorporó la capacidad de actualizar un host desde la vista Hosts de 10.5.1. Esto significa que si está actualizando desde una versión anterior a 10.5.1, debe actualizar el host del servidor de SA (Security Analytics) mediante el script de la línea de comandos `sasrv10_4.1-5.xupgd.py` (no desde la vista Hosts). El host del servidor de Security Analytics es el host en el cual reside el servidor de Security Analytics.

Nota: Cuando actualiza el host del servidor de Security Analytics, Security Analytics respalda los archivos de configuración del servicio de administración del sistema (SMS) (excluido el archivo `wrapper.conf`) del directorio `/opt/rsa/sms/conf` al directorio `/opt/rsa/sms/conf_%timestamp%`. Esta es una medida preventiva para una situación aislada en la cual podría ser necesario restaurar la configuración de SMS desde el respaldo. Para hacer esto, reemplace los archivos del directorio `/opt/rsa/sms/conf` por los archivos respaldados en el `/opt/rsa/sms/conf_%timestamp%` después de la actualización.

1. Actualice el host del servidor de Security Analytics (servidor primario de Security Analytics si tiene una implementación de múltiples servidores de Security Analytics) desde la línea de comandos mediante el script de la línea de comandos `sasrv10_4.1-5.xupgd.py`.
   a. Descargue `sasrv10_4.1-5.xupgd.py.zip` desde SCOL (https://knowledge.rsasecurity.com) a su directorio local.
   b. Copie `sasrv10_4.1-5.xupgd.py.zip` en el directorio raíz del host del servidor de Security Analytics.
   c. Acceda al host del servidor de Security Analytics mediante el protocolo SSH.
   d. Extraiga `sasrv10_4.1-5.xupgd.py` desde el archivo zip.
      `[root@Security Analytics ServerHost]# unzip sasrv10_4-5upgd.py.zip`
   e. Ejecute el script `sasrv10_4.1-5.xupgd.py` desde el directorio raíz.
      `[root@Security Analytics ServerHost]# ./sasrv10_4-5upgd.py`
      El script tarda al menos 15 minutos en completarse y puede tardar más según la implementación. Si tiene un host del servidor de Security Analytics que ejecuta Reporting Engine, IPDB Extractor y otros servicios, o si tiene una implementación de host de múltiples servidores de Security Analytics, la ejecución del script tardará más.

      El script crea el archivo `sasrv10_4-5upgd.log` en el directorio `[root@Security Analytics ServerHost]`, el cual se puede usar para solucionar problemas una vez que se completa el script. La siguiente salida de la consola es un ejemplo que ilustra los mensajes que se reciben durante la actualización cuando esta se ejecuta correctamente.

```
installing rsa-sa-gpg-pubkeys-
10.5.0.0 upgrading rsa-sa-gpg-pubkeys
updating system and application software this may take several minutes,
please wait…
do not log out or disconnect your session while the update is running
```

```
update in progress, time elapsed: nn seconds
    .    .    .        .    .    .    .
    .    .    .        .    .    .    .
    .    .    .        .    .    .    .
update in progress, time elapsed: nnn seconds

update process was successful total time for upgrade: nnn sec(s): nn min(s) nn
sec(s) system reboot required to finish upgrade Type y and press Enter to reboot
or just press Enter if you do not want to reboot: y
```

f. Escriba `y` y presione [Intro].

En la siguiente tabla se enumeran los errores del script de actualización que se pueden mostrar en la consola durante la actualización, junto con la causa posible y la solución sugerida.

Error del script de actualización	Causa posible	Solución
`missing 10.6 packages detected. did you update your repository? update process cannot proceed. exiting`	El script no encontró paquetes de actualización válidos en el repositorio de actualización local	Completar el repositorio de actualización local.
`update failure, possible missing dependencies or signing key errors`	No se ejecutaron todas las tareas de preparación para la actualización.	Asegúrese de haber completado todas las Tareas de preparación para la actualización.

2. (Condicional: solo para implementaciones de host de múltiples servidores de Security Analytics):
   a. Copie `sasrv10_4.1-5.xupgd.py.zip` desde su directorio local al directorio raíz de los hosts de los servidores secundarios de Security Analytics.
   b. Acceda a cada host de servidor secundario de Security Analytics mediante el protocolo SSH y asegúrese de que puppetmaster esté habilitado mediante los siguientes comandos:
   ```
   chkconfig --add puppetmaster chkconfig --level 3 puppetmaster
   on/etc/init.d/puppetmaster start
   ```
   c. Repita los pasos del 1c al 1f en cada host de servidor secundario de Security Analytics de su implementación de Security Analytics.
3. Actualice los hosts que no son de servidor de Security Analytics desde la vista Hosts
   a. Inicie sesión en Security Analytics.
   b. En el menú de Security Analytics, seleccione **Administration** > **Hosts**.

> **Nota:** Si tiene un host que no es de servidor de Security Analytics, el cual ejecuta una versión anterior a la ruta de actualización de 10.6.0 (es decir, anterior a 10.4.1), y actualizó su host del servidor de Security Analytics a 10.6.0, el host que no es de servidor de Security Analytics mostrará "**La ruta de actualización no es compatible"** en la columna **Estado** de la vista Hosts y usted no podrá actualizarlo desde esta vista. Póngase en contacto con el servicio al cliente para actualizar el host que no es de servidor de Security Analytics en la ruta no compatible.

   c. Actualice los hosts en la secuencia que se recomienda en el tema **Actualizar los hosts en la secuencia correcta** de la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/).

d. Seleccione la versión que desea aplicar en la columna **Versión de actualización**. Si desea actualizar más de un host a esa versión, seleccione la casilla de verificación a la izquierda de los hosts.
Se muestra Actualización disponible en la columna **Estado** si tiene una actualización de versión en el repositorio de actualización local para los hosts seleccionados.
Si:
   - No puede encontrar la versión que desea, complete el repositorio de actualización local.
   - No tiene espacio en disco suficiente en el repositorio de actualización local para descargar una actualización de versión, aparecerá el cuadro de diálogo **Administración de espacio del repositorio** con el contenido y el estado del espacio en disco del repositorio. Puede eliminar las versiones que no necesita para liberar espacio en disco suficiente con el fin de descargar la versión que desea. Consulte **Liberar espacio en disco del repositorio de actualización local** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener instrucciones.

e. Haga clic en **Actualizar** en la barra de herramientas. En la columna **Estado** se indica lo que está sucediendo en cada una de las siguientes etapas de la actualización:
   - Descarga de paquetes de actualización.
   - Comprobación de su configuración de versión actual para asegurarse de que no tenga conflictos. Muestra:
     - Advertencia de actualización. Vea los detalles si hay un posible conflicto.
     - Conflicto de actualización. Vea los detalles si hay un conflicto.
       Consulte **Solución de advertencias, conflictos y errores previos a la actualización y durante la actualización a 10.6** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información sobre cómo abordar estas advertencias y conflictos de configuración.
   - Inicio de la actualización si no hay conflictos.
   - Actualización de los paquetes de actualización.
     Muestra Error en la actualización. Vea detalles si hay un error en la aplicación de un paquete que bloquea la actualización. Consulte **Solución de advertencias, conflictos y errores previos a la actualización y durante la actualización a 10.6** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información sobre cómo resolver estos errores.

Después de la actualización del host, Security Analytics le solicita que ejecute la acción **Reiniciar host**.

f. Haga clic en **Reiniciar host** en la barra de herramientas.
Security Analytics muestra el estado **Reiniciando…** hasta que el host vuelve a estar línea. Una vez que el host vuelve a estar línea, en **Estado** se muestra **Actualizado**. Póngase en contacto con el servicio al cliente si el host no vuelve a estar en línea.

> **Nota:** Si la STIG de la DISA está habilitada, la apertura de los servicios principales puede tardar aproximadamente entre cinco y 10 minutos. La generación de los nuevos certificados es la causa de este retraso.

Tareas de actualización a 10.6 para la versión 10.5.1.x

En este tema se enumeran las tareas que debe completar para realizar la actualización a 10.6 desde la versión 10.5.1.x. Consulte Tareas de actualización a 10.6 para las versiones 10.4.1.x a 10.5.0.x para obtener instrucciones si está actualizando desde las versiones 10.4.1.x a 10.5.0.x.

Última modificación: 18 de febrero de 2016, 14:12 h

Tarea 1. Completar el repositorio de actualización local

Opciones

Tiene dos opciones para completar el repositorio de actualización local:

- Opción 1: Conectarse al repositorio de actualización de Live.
  Esto conecta el repositorio de actualización local de Security Analytics al repositorio de actualización de RSA Live a través de Internet con su cuenta de Live.
- Opción 2: Descargar actualizaciones de versiones desde **Download Central** (https://download.rsasecurity.com/).
  Si no permite que su implementación de Security Analytics se conecte a Internet, debe descargar los paquetes de actualización desde Download Central a un directorio local y, a continuación, cargarlos en el repositorio de actualización local de Security Analytics.

Opción 1: Conectarse al repositorio de actualización de Live

El acceso al repositorio de actualización de Live requiere y usa las credenciales de la cuenta de Live configuradas en **Administration** > **Sistema** > **Live**.

Nota: Cuando establezca la conexión inicial al repositorio de actualización de Live, accederá a todos los paquetes del sistema CentOS 6 y a los paquetes de producción de RSA. Esta descarga de más de 2.5 GB de datos tardará una cantidad indeterminada de tiempo de acuerdo con la conexión a Internet del servidor de Security Analytics y el tráfico del repositorio de RSA. El uso del repositorio de actualización de Live NO es obligatorio.

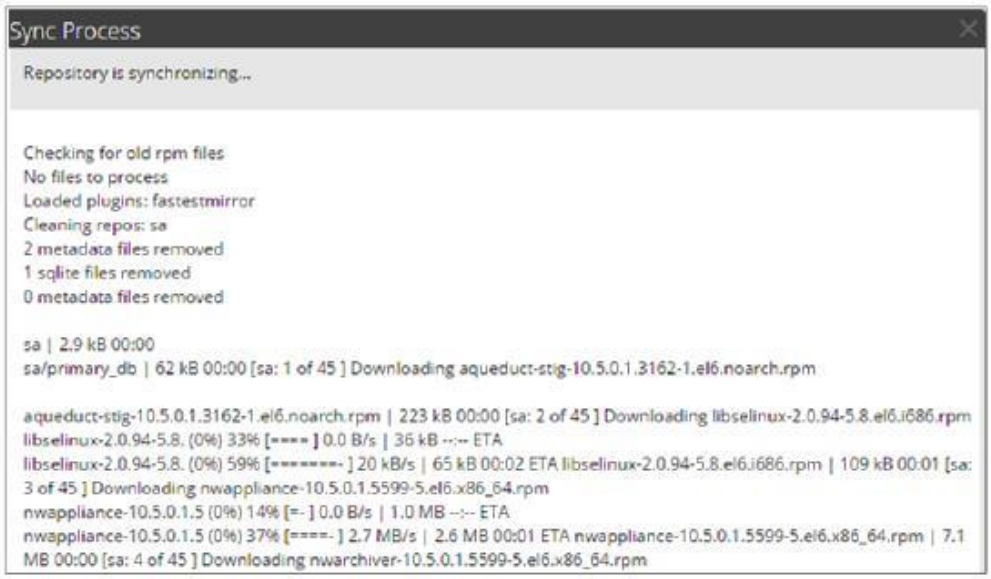
Para conectarse al repositorio de actualización de Live:

Nota: Si necesita usar un proxy para establecer conexión al repositorio de actualización de Live, puede configurar valores en Host proxy, Nombre de usuario de proxy y Contraseña de proxy. Consulte **Configurar un proxy para Security Analytics** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para la versión desde la cual está realizando la actualización.

1. Navegue a la vista **Administration** > **Sistema**, seleccione **Live** en el panel de opciones y asegúrese de que las credenciales estén configuradas. Si no lo están, configúrelas ahora y haga clic en **Probar conexión** y, a continuación, en **Aplicar**.
   Asegúrese de que **Probar conexión** se ejecute correctamente debido a que esta cuenta se usa para acceder al repositorio de actualización de Live.
2. Seleccione la pestaña **Actualizaciones** > **Configuración**.
3. Seleccione la casilla **Activado** y haga clic en **Aplicar**.
4. Use el botón **Probar conexión** para comprobar la conectividad. Asegúrese de que la prueba se ejecute correctamente. Se crea automáticamente un archivo `sa.repo` en el directorio `/etc/yum.repos.d/` del host del servidor de Security Analytics, el cual usa el repositorio de actualización local para comunicarse con el repositorio de actualización de Live.

Una vez habilitado, el repositorio de actualización de Live sincronizará y descargará todos los paquetes disponibles en el próximo evento calendarizado. También puede forzar un trabajo de sincronización desde la pestaña **Repositorio de actualizaciones** mediante la opción **Sincronizar ahora**. Después de actualizar ambos repositorios de actualización (el de Live y el local), puede ver todos los paquetes RPM descargados en la pestaña **Repositorio de actualizaciones** del panel **Administration** > **Actualizaciones**.

5. En el menú de Security Analytics, seleccione **Administration** > **Sistema**. Se muestra la vista **Información**.
6. En el panel izquierdo, seleccione **Actualizaciones**.
7. En la pestaña **Repositorio de actualizaciones**, haga clic en Synchronize Now.



Se muestra la pestaña **Repositorio de actualizaciones** con las actualizaciones que recuperó mediante la sincronización.

Advertencia: Si configura Public Key Infrastructure (PKI) en 10.5.0.2, Synchronize Now estará inhabilitado, razón por la cual debe asegurarse de que se haya realizado la sincronización automática del repositorio de actualizaciones antes de intentar la actualización de un host a 10.6 en la vista **Hosts**.

Opción 2: Descargar actualizaciones de versiones desde Download Central.

Debe completar el repositorio de actualizaciones de Security Analytics desde Download Central por los siguientes motivos:

- Si las actualizaciones de versiones que desea no están en el repositorio de actualización local (es decir, no aparecen en la lista Actualizaciones disponibles para un host en la columna Actualizaciones de la vista Hosts).
- Si su implementación de Security Analytics no tiene acceso a Internet.

Advertencia: Después de actualizar un host a 10.6 desde el repositorio de actualización local, tal vez no pueda acceder a versiones anteriores para actualizar otros hosts. Esto es producto del método que usa Security Analytics para administrar la estructura de archivos del repositorio de actualización local cuando usted completa este repositorio manualmente desde Download Central. Por ejemplo, si actualizó el host del servidor de Security Analytics a 10.5.1 y, a continuación, a 10.6, 10.5.1 no estará disponible para actualizar otros hosts. Debe descargar 10.5.1 desde Download Central y volver a actualizar manualmente el repositorio de actualización local.

Para completar el repositorio de actualización local desde Download Central:

1. Descargue los archivos **SA-10.6.0.0-UpdatePack-EL6.zip** y **SA-10.6.0.0-Manifest-EL6.zip**, que contienen todos los archivos de actualización de Security Analytics 10.6, desde **Download Central** (https://download.rsasecurity.com/) a un directorio local.
2. En el menú de Security Analytics, seleccione **Administration** > **Sistema**.
3. En el panel izquierdo, seleccione **Actualizaciones**.
4. En la pestaña **Configuración**, asegúrese de que la casilla de verificación **Activar** no esté seleccionada.

5. En la pestaña **Actualizaciones manuales**, haga clic en **Cargar archivos**. Se muestra el cuadro de diálogo Cargar archivo.
6. Haga clic en , navegue hasta el directorio local donde colocó los archivos **SA-10.6.0.0-UpdatePack-EL6.zip** y **SA-10.6.0.0-Manifest-EL6.zip** y selecciónelos.

Nota: El archivo **SA-10.6.0.0-UpdatePack-EL6.zip** es muy grande y su carga en Security Analytics podría plantear problemas. Si esto ocurre, descomprímalo y cargue los archivos en grupos de menor tamaño.

Los RPM de actualización de 10.6 se muestran en la pestaña **Actualizaciones manuales**.
El estado de carga se muestra en la esquina inferior izquierda. Cuando la carga finaliza, el servidor de SA descomprime todos los paquetes rpm y los muestra en la pestaña **Actualizaciones manuales**.

7. Seleccione todos los archivos en la lista Actualizaciones manuales y haga clic en **Aplicar**.
   Esto transfiere los archivos RPM al repositorio de actualización local en el servidor de Security Analytics y los pone a disposición de los hosts.

Tarea 2. Actualizar los hosts a 10.6 desde 10.5.1.x

Nota: Cuando actualiza el host del servidor de SA (Security Analytics), Security Analytics respalda los archivos de configuración del servicio de administración del sistema (SMS) (excluido el archivo `wrapper.conf`) del directorio `/opt/rsa/sms/conf` al directorio `/opt/rsa/sms/conf_%timestamp%`. Esta es una medida preventiva para una situación aislada en la cual podría ser necesario restaurar la configuración de SMS desde el respaldo. Para hacer esto, reemplace los archivos del directorio `/opt/rsa/sms/conf` por los archivos respaldados en el `/opt/rsa/sms/conf_%timestamp%` después de la actualización.

1. **(Condicional) Solo para implementaciones de múltiples servidores de Security Analytics**: Acceda a cada host de servidor secundario de SA mediante el protocolo SSH y asegúrese de que puppetmaster esté habilitado mediante los siguientes comandos:
   ```
   chkconfig --add puppetmaster
   chkconfig --level 3 puppetmaster /etc/init.d/puppetmaster start
   ```
2. Inicie sesión en Security Analytics.
3. En el menú de Security Analytics, seleccione **Administration** > **Hosts**.
4. Actualice el host de Security Analytics.
   a. Seleccione el host del servidor de Security Analytics y haga clic en **Actualizar** > **Buscar actualizaciones**.

En la columna Actualizaciones se muestra **Comprobando…** a medida que Security Analytics recupera las actualizaciones más recientes para 10.6.

Cuando termina de recuperar todas las actualizaciones para 10.6, se muestra Update en la columna **Actualizaciones**.

Actualizar se muestra de dos maneras:

- Sin un triángulo de precaución: indica que la actualización incluye exclusivamente las actualizaciones del paquete.
- Con un triángulo de precaución: indica que la actualización incluye las actualizaciones del paquete y las actualizaciones adicionales, como un kernel.

Por ejemplo:

> **Nota:** Si la configuración del host anterior a la actualización presenta problemas que impiden una actualización correcta a 10.6, Security Analytics muestra Conflicts (2). Consulte **Solución de errores previos a la actualización y durante la actualización a 10.5.1** en la ayuda de Security Analytics 10.5 (https://sadocs.emc.com/) para obtener instrucciones sobre cómo resolver los errores previos a la actualización.

b. Haga clic en **Actualizar**.
Se muestra el cuadro de diálogo **Actualizaciones**.
Puede hacer clic en un nombre de host para mostrar los paquetes de 10.6 que se aplicarán a ese host.
Si ve el siguiente mensaje en el cuadro de diálogo **Actualizar** después de hacer clic en **Actualizar**, el kernel en el host es más antiguo que el kernel compatible con 10.6. Este error no es un obstáculo. Puede continuar con la actualización si desea actualizar el kernel en el host a la versión compatible con 10.6.
La versión del kernel en el host es más antigua que la versión ***n.n.nn-nnn.nn.n*** compatible con Security Analytics.
Si hace clic en **Iniciar actualización**, la versión del kernel ***n.n.nn-nnn.nn.n*** se instalará en el host.

c. Haga clic en Begin Update.
Se muestra Iniciando… en la columna **Actualizaciones** a medida que Security Analytics comienza a aplicar las actualizaciones más recientes para 10.6.

> **Nota:** Si Security Analytics encuentra un error durante el proceso de actualización, muestra Update Error en la columna **Actualizaciones** de la vista Hosts. Consulte **Solución de errores previos a la actualización y durante la actualización a 10.5.1** en la ayuda de Security Analytics 10.5 (https://sadocs.emc.com/) para obtener instrucciones sobre cómo resolver los errores durante la actualización.

Una vez instalados todos los paquetes de 10.6 para el host del servidor de Security Analytics, se muestra Reboot Required en la columna **Actualizaciones**.

d. Haga clic en Reboot Required.

> **Nota:** Si la STIG de la DISA está habilitada, la apertura de los servicios principales puede tardar aproximadamente entre cinco y 10 minutos. La generación de los nuevos certificados es la causa de este retraso.

Después del reinicio, el host del servidor de Security Analytics se actualiza a 10.6 y, por lo tanto, la vista Hosts de 10.5.1.x ya no está disponible y se muestra el mensaje “Esta página web no está disponible”.

5. Actualice los hosts que no son de servidor de Security Analytics a 10.6.
   a. Inicie sesión en Security Analytics.
   b. En el menú de Security Analytics, seleccione **Administration** > **Hosts**.

> **Nota:** Si tiene un host que no es de servidor de Security Analytics, el cual ejecuta una versión anterior a la ruta de actualización de 10.6.0 (es decir, anterior a 10.4.1), y actualizó su host del servidor de Security Analytics a 10.6.0, el host que no es de servidor de Security Analytics mostrará “**La ruta de actualización no es compatible”** en la columna **Estado** de la vista Hosts y usted no podrá actualizarlo desde esta vista. Póngase en contacto con el servicio al cliente para actualizar el host que no es de servidor de Security Analytics en la ruta no compatible.

c. Actualice los hosts en la secuencia que se recomienda en el tema **Actualizar los hosts en la secuencia correcta** de la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/).

d. Seleccione la versión que desea aplicar en la columna **Versión de actualización**. Si desea actualizar más de un host a esa versión, seleccione la casilla de verificación a la izquierda de los hosts.
Se muestra Actualización disponible en la columna **Estado** si tiene una actualización de versión en el repositorio de actualización local para los hosts seleccionados.
Si:
   - No puede encontrar la versión que desea, complete el repositorio de actualización local.
   - No tiene espacio en disco suficiente en el repositorio de actualización local para descargar una actualización de versión, aparecerá el cuadro de diálogo **Administración de espacio del repositorio** con el contenido y el estado del espacio en disco del repositorio. Puede eliminar las versiones que no necesita para liberar espacio en disco suficiente con el fin de descargar la versión que desea. Consulte **Liberar espacio en disco del repositorio de actualización local** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener instrucciones.

e. Haga clic en **Actualizar** en la barra de herramientas. En la columna **Estado** se indica lo que está sucediendo en cada una de las siguientes etapas de la actualización:
   - Descarga de paquetes de actualización.
   - Comprobación de su configuración de versión actual para asegurarse de que no tenga conflictos. Muestra:
     - Advertencia de actualización. Vea los detalles si hay un posible conflicto.
     - Conflicto de actualización. Vea los detalles si hay un conflicto.
       Consulte **Solución de advertencias, conflictos y errores previos a la actualización y durante la actualización a 10.6** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información sobre cómo abordar estas advertencias y conflictos de configuración.
   - Inicio de la actualización si no hay conflictos.
   - Actualización de los paquetes de actualización.
     Muestra Error en la actualización. Vea detalles si hay un error en la aplicación de un paquete que bloquea la actualización. Consulte **Solución de advertencias, conflictos y errores previos a la actualización y durante la actualización a 10.6** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información sobre cómo resolver estos errores.
     Después de la actualización del host, Security Analytics le solicita que ejecute la acción **Reiniciar host**.

f. Haga clic en **Reiniciar host** en la barra de herramientas.
Security Analytics muestra el estado **Reiniciando…** hasta que el host del servidor de Security Analytics vuelve a estar línea. Una vez que el host del servidor de Security Analytics vuelve a estar línea, en **Estado** se muestra **Actualizado**.
Póngase en contacto con el servicio al cliente si el host no vuelve a estar en línea.

> **Nota:** Si la STIG de la DISA está habilitada, la apertura de los servicios principales puede tardar aproximadamente entre cinco y 10 minutos. La generación de los nuevos certificados es la causa de este retraso.

Actualizar o instalar la recopilación de Windows existente

Consulte **Instrucciones de actualización e instalación de la recopilación de Windows existente de Security Analytics 10.6** en SCOL (https://knowledge.rsasecurity.com) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows existente.

Última modificación: 16 de febrero de 2016, 15:58 h

Tareas posteriores a la actualización

Solo para 10.4.1.x a 10.6: Tarea 1. Monitorear la migración de datos de Reporting Engine

En este tema se indica cómo monitorear la migración de los datos de Security Analytics Reporting Engine a 10.6. También se indica cómo solucionar fallas en caso de que se presenten.

Nota: La actualización de Security Analytics a 10.6 habilita automáticamente la migración de datos de Reporting Engine. En este tema se indica cómo monitorear la migración. Normalmente, los problemas que se señalan en este tema no se presentarán. La información que se proporciona en este tema brinda consejos de solución de problemas en caso de que se presente alguno. Póngase en contacto con el servicio al cliente si tiene dificultades para resolver estos problemas.

Internamente, el proceso de migración de datos de Reporting Engine tiene dos etapas:

- Etapa 1: copiar estadísticas y datos de ejecución históricos más recientes
- Etapa 2: copiar los datos restantes y realizar una limpieza

Durante el proceso de migración, Security Analytics copia contenido solo con fines informativos:

- De: `/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
- A: `home/rsasoc/rsa/soc/reporting-engine/statusdb/alertstatusmanager.h2.db` and `/home/rsasoc/rsa/soc/reportingengine/statusdb/reportstatusmanager.h2.db`

Contexto

En este tema se abordan las siguientes materias.

- Cálculos de tiempo aproximados de la migración.
- Proceso de migración de Reporting Engine.
- Ubicación del archivo de registro de la migración y cómo interpretarlo.
- Solución de problemas.

Cálculo de la duración de la migración

Los cálculos de la siguiente tabla se basan en el tiempo que tardó en completarse la migración en el ambiente de pruebas de RSA. La etapa 1 se completa antes del inicio de Reporting Engine, por lo que es posible usar la información de la etapa 1 en la tabla para calcular aproximadamente cuánto puede tardar el inicio. La etapa 2 comienza en segundo plano después del inicio, por lo que es posible usar la información de la etapa 2 en la tabla para calcular aproximadamente por cuánto tiempo sería necesario monitorear los registros de migración en busca de posibles errores.

Precaución: Las métricas de la siguiente tabla se obtuvieron en un ambiente de laboratorio y, por lo tanto, solo son cálculos con fines de planificación.

Security Analytics asigna 200 gigabytes (GB) de espacio para Reporting Engine, lo cual incluye el servicio Reporting Engine completo y la base de datos.

Volumen de datos de `statusdb` típico (en GB)	**Cantidad de alertas**	**Cantidad de informes**	**Etapa 1 Tiempo consumido (segundos)**	**Etapa 2 Tiempo consumido (minutos)**
3.5	2,139,046	15,169	10	17
10	2,139,046	205,171	16	23
40	2,139,046	1,395,171	20	70

Proceso de migración de Reporting Engine

En el procedimiento siguiente se explica qué sucede internamente durante el proceso de migración de datos de Security Analytics Reporting Engine.

Nota: Puede continuar creando, calendarizando y ejecutando informes, alertas y gráficos aunque la migración esté en curso. Sin embargo, todos los datos de ejecución históricos no estarán disponibles hasta que la migración se complete correctamente.

Cuando complete la actualización del host de Security Analytics mediante el reinicio del host, el proceso de migración de Reporting Engine se iniciará automáticamente. La migración tiene dos etapas:

Etapa 1: Copiar estadísticas y datos de ejecución históricos más recientes: Reporting Engine copia las estadísticas y los registros de ejecución de alertas e informes más recientes cuando se inicia.

Si las tareas de la etapa 1 se realizan correctamente, los 20,000 registros de ejecución de alertas e informes más recientes se copian de manera satisfactoria a la nueva base de datos. Ahora puede ver las estadísticas y los datos de ejecución más recientes en la interfaz de Security Analytics.

Etapa 2: Copiar los datos restantes y realizar una limpieza: Una vez que Reporting Engine está en funcionamiento, la etapa 2 se inicia en segundo plano. Durante esta etapa, el resto de los registros de ejecución se copia en lotes y estos registros quedan a disposición de los usuarios en la interfaz del usuario de Security Analytics. Después de la copia correcta de todos los registros, los datos antiguos se eliminan.

Localizar e interpretar el archivo de registro de la migración

Los registros de la migración se almacenan en `/home/rsasoc/rsa/soc/reporting-engine/logs/migration.log`. Busque los mensajes `begin`, `end`, `progress` y de error durante la migración.

- Una vez que comienza la migración de datos, se muestra el siguiente mensaje.
  `**********Database migration Started **********`
  Si no dispone de espacio libre en disco suficiente para la migración (es decir, espacio en disco equivalente por lo menos a 1.2 veces el tamaño del archivo `statusmanager.h2.db`), el servicio Reporting Engine no se inicia y se muestra un mensaje similar al siguiente mensaje de error.
  ```
  Available Disk Space : 8,112 MB. Required disk space 10,048 MB.
  CRITICAL : Available Disk Space is not sufficient to proceed with migration.
  Shutting down reporting engine. Please cleanup data and start reporting engine
  ```
  Consulte el **Problema 1: Reporting Engine no se inicia**, **Causa posible 2** en la sección **Solución de problemas** de esta tarea.

- Durante la migración, Security Analytics escribe mensajes de registro que indican la cantidad de registros copiados a la base de datos de destino. Por ejemplo:
  `'20,000' out of 29,812 Records are inserted into 'AlertStatus' table`
- Cuando se completa la migración, se muestra el siguiente mensaje.
  `**********Database migration Completed **********`
- Si la copia de estadísticas de informes o alertas falla, Security Analytics registra el siguiente mensaje.
  `Migration of Report/Alert Statistics failed. Interpreted property re.proceed_if_stats_init_fails as: false. Shutting down reporting engine`
  Consulte el **Problema 1: Reporting Engine no se inicia** en la sección **Solución de problemas** de esta tarea.
- Si la migración no se completa debido a que no pudo copiar ninguno de los registros, el archivo `statusmanager.h2.db` antiguo no se limpiará y Security Analytics registrará el siguiente mensaje.
  `Additional rows are available for migration. Cannot clean up DB objects just now`
  Consulte los siguientes mensajes en la sección **Solución de problemas** de esta tarea.
  - **Problema 2: La migración se debe reiniciar desde el principio**
  - **Problema 3: La migración migra correctamente todos los registros, pero `statusmanager.h2.db` aún existe.**
- Si todos los registros se migran correctamente, pero falla la limpieza del archivo `statusmanager.h2.db` antiguo, Security Analytics registra el siguiente mensaje.
  `Failed to cleanup legacy status manager database`
  Consulte el **Problema 3: La migración migra correctamente todos los registros, pero statusmanager.h2.db aún** existe en la sección **Solución de problemas** de esta tarea.

Solución de problemas

Nota: Si no puede resolver ninguno de los problemas de la migración con los siguientes consejos de solución de problemas, póngase en contacto con el servicio al cliente.

Problema 1	**Reporting Engine no se inicia.**
Causa posible 1	No se migraron los registros históricos correctos de las estadísticas de ejecución de alertas e informes.
Solución 1	Revise los mensajes de registro y corrija el problema que causó la falla. Si no puede corregir un problema que se presentó durante la copia de las estadísticas, omita la falla y continúe con la migración. Establezca la propiedad del sistema JVM como `true`: en `/home/rsasoc/rsa/soc/reporting-engine/conf/server.conf:` `re.proceed_if_stats_init_fails=true` para omitir la falla en la migración de estadísticas e iniciar el servicio Reporting Engine. Si decide omitir la falla de la migración de estadísticas y la migración continúa, las nuevas estadísticas disponibles en Reporting Engine reemplazan a las antiguas.

Solución 2	Para realizar la migración, necesita un mínimo de 1.2 veces el tamaño del archivo `statusmanager.h2.db` de espacio en disco disponible en el volumen en el cual existe `statusmanager.h2.db`. Si no tiene espacio en disco suficiente, los siguientes métodos pueden ayudarlo a liberar espacio en disco. • Libere algo de espacio mediante la transferencia de archivos archivados en `/home/rsasoc/rsa/soc/reporting-engine/archives/` a cualquier otro volumen que tenga espacio libre. El siguiente comando es un ejemplo de cómo transferir archivos archivados: `mv/home/rsasoc/rsa/soc/reporting-engine/archives/contentstore.20150302170101.tgz` *`target-directory`* • Elimine los archivos no deseados del volumen en el cual existe `statusmanager.h2.db`. Consulte **Agregar espacio adicional para informes grandes** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para conocer los procedimientos de adición destinados a liberar espacio.
Problema 2	**La migración se debe reiniciar desde el principio (Etapa 1).**
Causa posible	Se encontraron fallas durante el monitoreo de la migración (por ejemplo, `statusmanager.h2.db` se dañó durante la migración).

Solución	1. Recupere el respaldo que hizo del archivo `statusmanager.h2.db`.
	2. Acceda mediante el protocolo SSH al host que ejecuta Reporting Engine.
	3. Detenga Reporting Engine con la siguiente cadena de comandos.
	`stop rsasoc_re`
	4. Elimine el archivo `db` dañado con la siguiente cadena de comandos:
	`rm /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
	5. Elimine los nuevos archivos `db` que se crearon durante la migración con las siguientes cadenas de comandos.
	`rm /home/rsasoc/rsa/soc/reporting-engine/statusdb/alertstatusmanager.h2.db`
	`rm/home/rsasoc/rsa/soc/reportingengine/statusdb/reportstatusmanager.h2.db`
	6. Elimine la carpeta bookmarks que rastrea el estado actual de la migración con la siguiente cadena de comandos.
	`rm/home/rsasoc/rsa/soc/reporting-engine/statusdb/bookmarks`
	7. Restaure el archivo `statusmanager.h2.db` respaldado al directorio `/home/rsasoc/rsa/soc/reporting-engine/statusdb/` con la siguiente cadena de comandos.
	`tar –xvf statusdb.tar.gz`
	8. Asegúrese de que el archivo `statusmanager.h2.db` restaurado tenga permiso para el usuario `rsasoc`. Si no es así, use la siguiente cadena de comandos para restablecer el privilegio del usuario.
	`chown –R rsasoc:rsasoc /home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`
	9. Inicie Reporting Engine con la siguiente cadena de comandos.
	`start rsasoc_re`

Problema 3	**La migración migra correctamente todos los registros, pero `statusmanager.h2.db` aún existe.**
Causa posible	La migración no eliminó el archivo `statusmanager.h2.db`.
Solución 1	Archive el archivo `statusmanager.h2.db` antiguo. 1. Detenga Reporting Engine con la siguiente cadena de comandos. `stop rsasoc_re` 2. Cree un archivo `tar.gz` de `/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db` con la siguiente cadena de comandos. `tar cvfj statusdb.tar.gz /home/rsasoc/rsa/soc/reporting-engine/statusdb/ statusmanager.h2.db` 3. Transfiera el archivo a otra ubicación de almacenamiento.
Solución 2	Elimine el archivo `statusmanager.h2.db` con la siguiente cadena de comandos. `rm/home/rsasoc/rsa/soc/reporting-engine/statusdb/statusmanager.h2.db`

Solo para 10.4.1.x a 10.6: Tarea 2. Restaurar las personalizaciones de Incident Management

Antes de ejecutar la actualización a 10.6, si personalizó plantillas de correo, scripts y campos de Incident Management en 10.4.1.x, debe restaurar esta información del contenido del archivo zip de respaldo.

Nota: Si no personalizó plantillas de correo, scripts o campos en 10.4.1.x, no necesita realizar el siguiente procedimiento. Además, Web Threat Detection se integró con Incident Management en 10.6. Esto significa que si los scripts se personalizan exclusivamente para WTD, no es necesario que los combine.

Para restaurar la información de Incident Management personalizada:

1. Descomprima el archivo `/opt/rsa/im/backup/timestamp.zip`.
   El archivo zip contiene los siguientes directorios:
   `mailtemplates`
   `scripts`
   `fields`

2. Restaure los datos personalizados de Incident Management desde el contenido del archivo `/opt/rsa/im/backup/timestamp.zip:`
   - **Plantillas de correo**, sobrescriba el directorio `/opt/rsa/im/mailtemplates` de 10.6 con el directorio `mailtemplates` del archivo zip.
   - **Scripts**, combine los scripts de 10.4.1.x de `scripts` en el archivo zip con el contenido del directorio /opt/rsa/im/scripts `/opt/rsa/ im/scripts` de 10.6.
   - **Campos**, combine los campos de 10.4.1.x de `fields` en el archivo zip con el contenido del directorio `/opt/rsa/im/fields` de 10.6.

Solo para 10.4.1.x a 10.6: Tarea 3. Reinicie el host de Security Analytics y el host de Malware Analysis si se produce un error

En el host que ejecuta Malware Analysis, busque varios mensajes de error similares al siguiente en el archivo `/var/lib/netwitness/rsamalware/spectrum/logs/spectrum.log` después de la actualización a 10.6.

```
2015-05-12 12:53:32,818 [ActiveMQ BrokerService[2437abe8-51ed-46ec-bcf7-b76e533eea83] Task-2] ERROR org.apache.activemq.broker.TransportConnector - Could not accept connection from tcp://10.31.204.101:45728: javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate
```

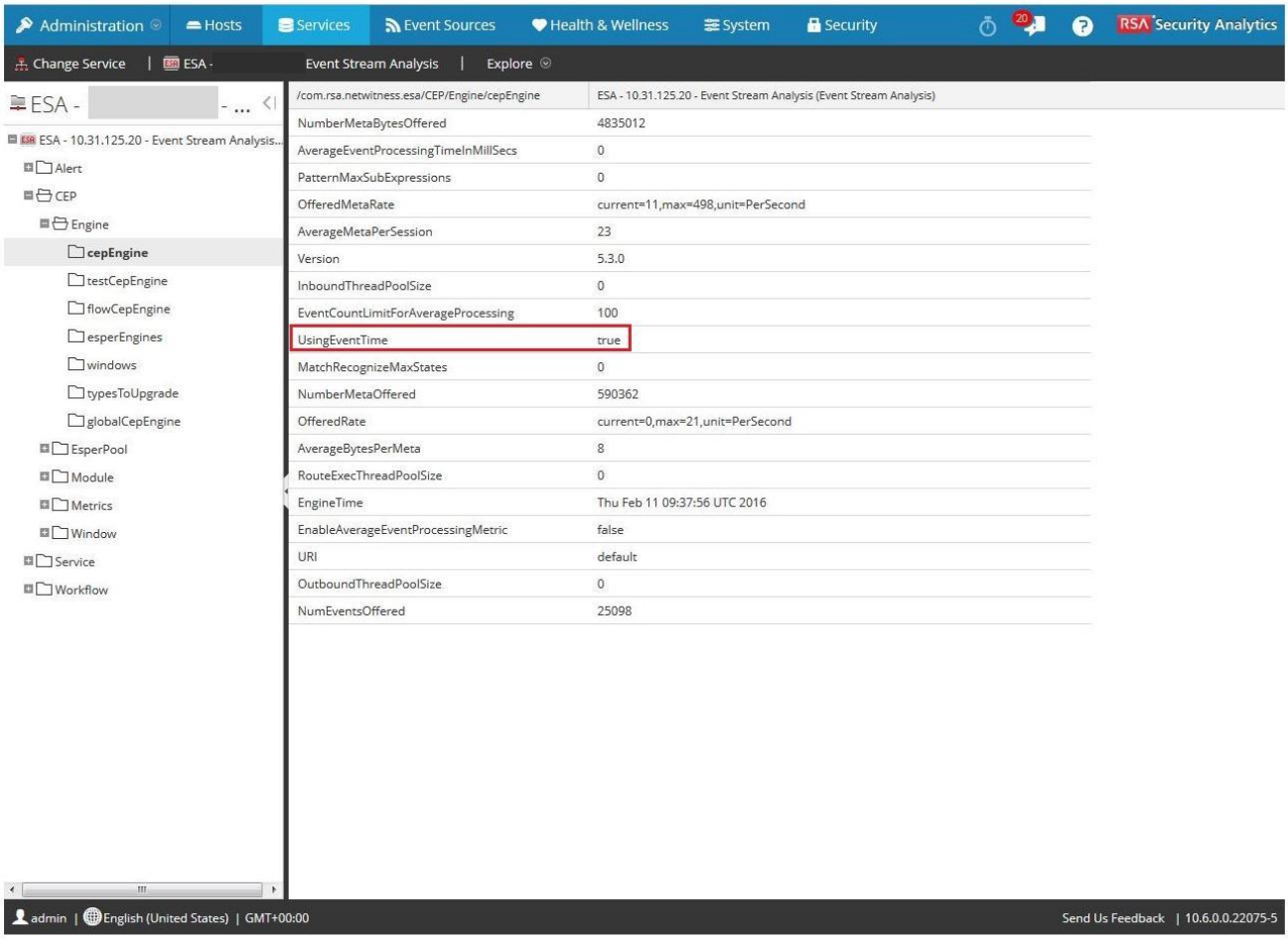
Si ve este tipo de error, debe:

1. Acceder al host del servidor de Security Analytics mediante el protocolo SSH
2. `reinicio del sistema`
3. Obtener acceso al host que ejecuta Malware Analysis mediante el protocolo SSH.
4. `reinicio del sistema`

Solo para clientes nuevos de Security Analytics a partir de 10.5.0.x: Tarea 4. Restablecer el parámetro UsingEventTime de Event Stream Analysis a True

Si su instalación inicial de Security Analytics era 10.5, 10.5.0.1 o 10.5.0.2, debe restablecer `UsingEventTime` a `true` (consulte la captura de pantalla).

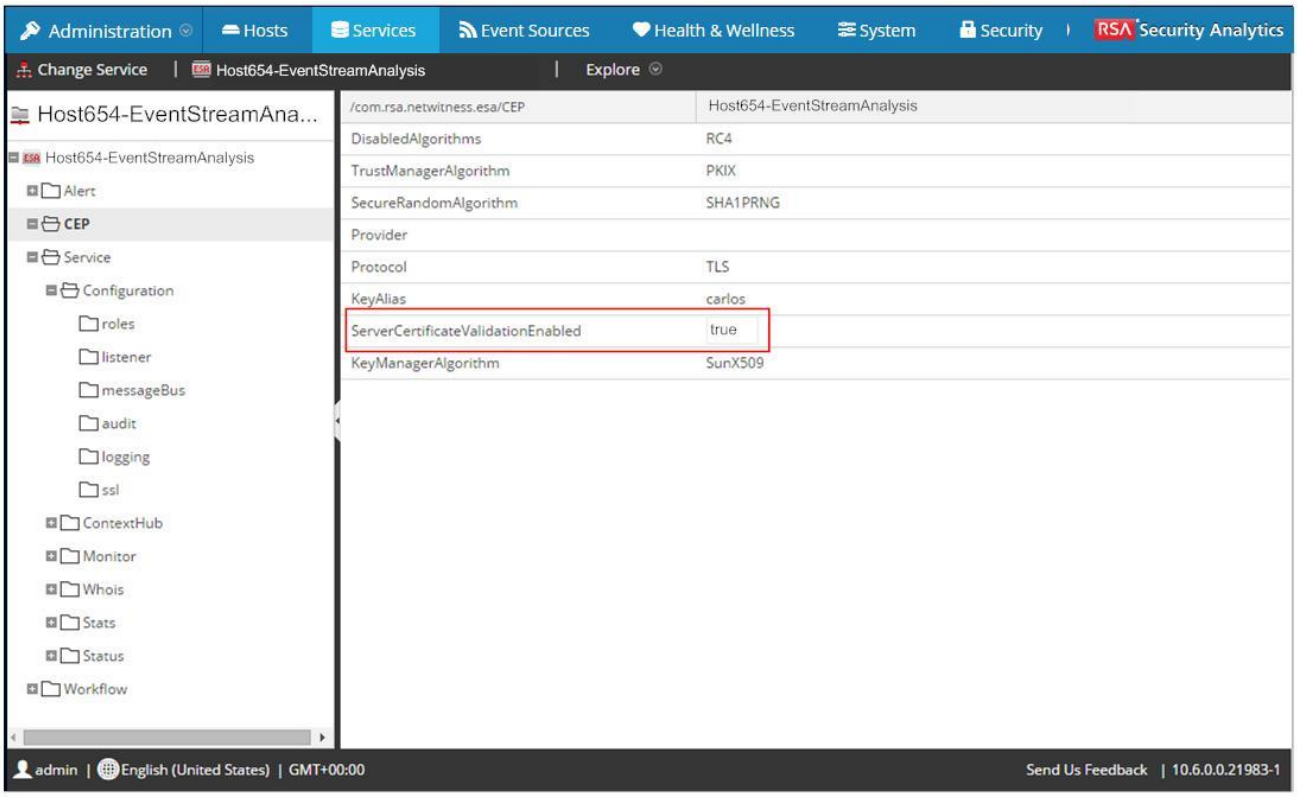
En la siguiente vista Explorar se muestra el parámetro `UsingEventTime` restablecido a `true`.



Tarea 5. Asegurarse de que el área de almacenamiento de confianza tenga certificados para la notificación de syslog del modo TCP

Si establece el modo TCP para la notificación de syslog y **ServerCertificateValidateEnable** estaba configurado en **false** antes de la actualización a 10.6:

1. Configure el parámetro **ServerCertificateValidateEnable** de Event Stream Analysis en **true**.



2. Agregue los certificados del cliente de syslog en el almacenamiento de claves java de Event Stream Analysis.

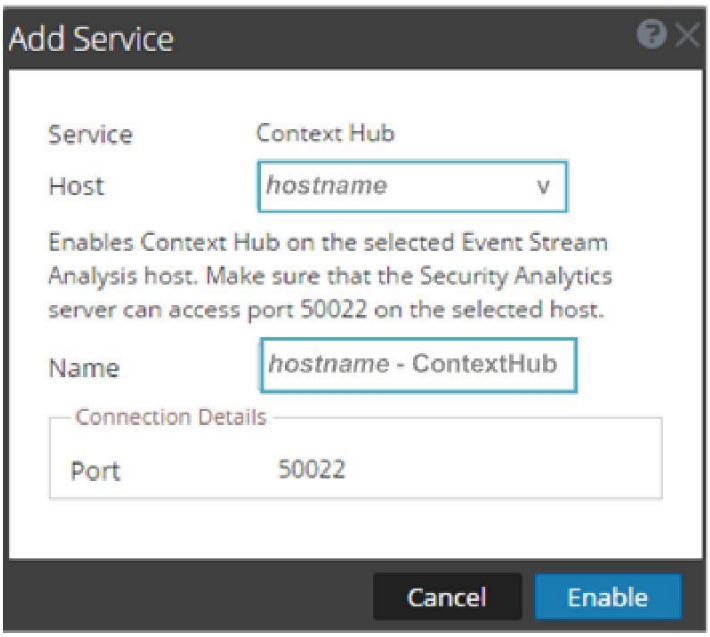
Tarea 6. Habilitar el servicio Context Hub

Cuando actualizó el host de Event Stream Analysis (ESA) a 10.6, Context Hub se instaló en el host de ESA, pero se inhabilitó de forma predeterminada. Context Hub es un servicio opcional; por lo tanto, habilítelo solo si desea usarlo. Consulte **Descripción general del servicio Context Hub** en la ayuda de Security Analytics 10.6 (https://sadocs.emc.com/) para obtener más información acerca de este servicio.

Nota: Solo puede tener una instancia del servicio Context Hub en su implementación de Security Analytics.

Realice el siguiente procedimiento para habilitar el servicio Context Hub.

1. Inicie sesión en Security Analytics.
2. Haga clic en **Administration** > **Servicios**.
3. Haga clic en + y seleccione **Context Hub**.
   Se muestra el cuadro de diálogo **Agregar servicio**.
4. En **Host**, seleccione el host de ESA y haga clic en **Habilitar**.
   Security Analytics completa el **Nombre** del servicio con el ***nombre de host*** de ESA: **Context Hub** de forma predeterminada. Si lo desea, puede cambiar el nombre del servicio.



Nota: Asegúrese de que el host de ESA que ejecuta el servicio Context Hub pueda acceder al puerto 50022.

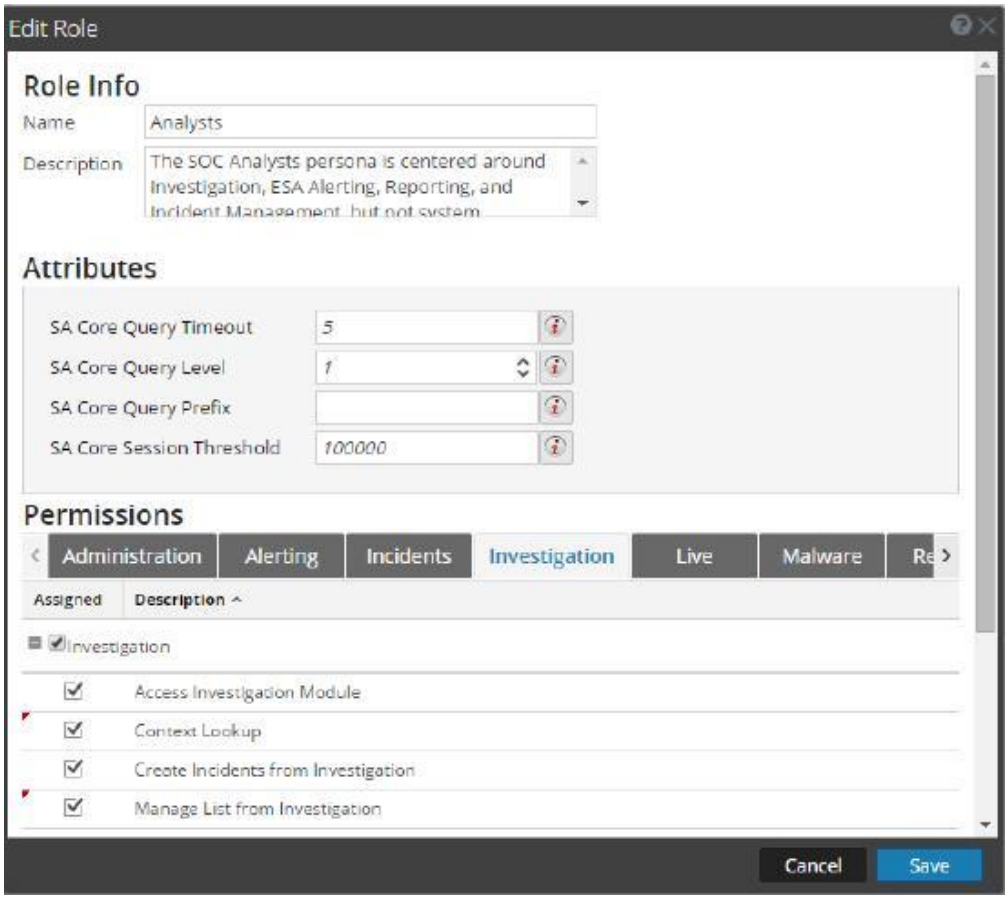
Tarea 7. Establecer permisos para el servicio Context Hub

Después de actualizar a 10.6, debe establecer los permisos **Investigation**: **Búsqueda de contexto** e **Investigation: Administrar lista desde Investigation** para las funciones apropiadas.

Realice los siguientes pasos para configurar los permisos **Búsqueda de contexto** y **Administrar lista desde Investigation**.

1. Inicie sesión en Security Analytics.
2. Vaya a Administration > Seguridad > pestaña Funciones.
3. Seleccione la función para la cual desea establecer el permiso y haga clic en .

4. Haga clic en **Investigation** bajo **Permisos** y seleccione **Búsqueda de contexto** y **Administrar lista desde Investigation**.



5. Haga clic en **Guardar**.

Tarea 8. Restaurar valores de parámetros personalizados de Malware Analysis al archivo de configuración creado recientemente

Reemplace los valores predeterminados del archivo de configuración `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` creado recientemente por los valores de parámetros personalizados del archivo `malwareCEFDictionaryConfiguration.xml` respaldados con anterioridad a la actualización a 10.6

1. Vea las diferencias entre `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` y el archivo respaldado `malwareCEFDictionaryConfiguration.xml`.
2. Reemplace los valores predeterminados del nuevo archivo `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml` por los valores personalizados del respaldo para conservar los valores predeterminados de los parámetros nuevos que se agregaron en 10.6.

Tarea 9. Migrar la STIG de la DISA a 10.6.

Si se aplicó el RPM de la STIG hardening de la Agencia de Sistemas de Información de Defensa (DISA) en Security Analytics, debe realizar la siguiente tarea para migrarlo a 10.6.

Para todos los hosts en los cuales se aplicó la STIG:

1. Obtenga acceso al host mediante el protocolo SSH.
2. `cd /opt/rsa/AqueductSTIG/`
3. `./GEN001000.sh`
4. `reboot`

Tarea 10. Restablezca el valor de sistema estable del Lockbox de Log Collector

Debe restablecer el **valor de sistema estable** del Lockbox de Log Collector debido al parche de seguridad del tercer trimestre. Si no restablece el **valor de sistema estable**, la regla **Falla de acceso a Lockbox** activará una alarma crítica en la vista Administración > Estado y condición > Alarmas para Log Collector.

Contacto con el servicio al cliente

RSA SecurCare:	https://knowledge.rsasecurity.com
Teléfono:	1 800 995 5095, opción 3
Contactos internacionales:	http://mexico.emc.com/support/rsa/contact/phone-numbers.htm (visite el sitio web de su país correspondiente)
Correo electrónico:	nwsupport@rsa.com
Comunidad:	http://mexico.emc.com/security/security-analytics/security-analytics.htm (visite el sitio web de su país correspondiente)
Soporte básico:	El soporte técnico relacionado con problemas técnicos está disponible de lunes a viernes, de 8:00 h a 17:00 h (hora local).
Soporte Plus:	El soporte técnico está disponible por teléfono durante todo el año solo para los problemas de severidad 1 y 2.

Preparación para ponerse en contacto con el servicio al cliente

Cuando se pone en contacto con el servicio al cliente, debe encontrarse en su computadora. Prepárese para proporcionar la siguiente información:

1. El número de versión del producto o la aplicación de RSA Security Analytics que está usando.
2. El tipo de hardware que está usando.

Historial de revisiones

Revisión	Fecha	Descripción	Autor
1.0	16 de febrero de 2016	Versión inicial	Info Design & Devel (dfo)
1.1	23 de febrero de 2016	Cambios adicionales de revisión de QE.	Info Design & Devel (dfo)