Lista de verificación de la actualización a Security Analytics 10.6

Tareas de preparación para la actualización

Tarea	Descripción	✓
1.	**Solo para 10.4.1.x a 10.6:** Asegúrese de que haya espacio suficiente para la base de datos de Reporting Engine 10.6. 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.	
2.	Revise los puertos principales en 10.6 y abra los puertos del firewall. Descubra los cambios a los puertos principales que se señalan en el tema **Arquitectura y puertos de red** de la ayuda de Security Analytics 10.6 (**https://sadocs.emc.com/**). El puerto del servicio Context Hub de Event Stream Analysis (ESA) debe estar disponible para 10.6. 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.	
3.	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.	

Última modificación: 22 de febrero de 2016, 09:03 h

4.	Corrija 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`.	
5.	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.	
6.	Respalde el archivo de configuración de Malware Analysis: a. 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. b. Elimine `/var/lib/rsamalware/spectrum/conf/malwareCEFDictionaryConfiguration.xml`	
7.	Respalde la configuración. 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.	
8.	Prepare la STIG para la actualización. Para todos los hosts en los cuales está aplicada la STIG hardening: • Acceda al host mediante el protocolo SSH y escriba las siguientes cadenas de comandos. `yum update glibc reboot`	

Tareas de actualización: 10.4.1-10.5.0.x a 10.6

Tarea	Descripción	✓
1.	Complete el repositorio de actualización local del servidor de Security Analytics con los paquetes de actualización a 10.6. • Opción 1: Security Analytics está conectado a Internet (a través de una cuenta de LIVE de Security Analytics): Vaya a **Administration** > **Sistema** > **Actualizaciones** > y haga clic en **Sincronizar ahora**. • Opción 2: Security Analytics no está conectado a Internet (a través de Download Central): 1. Descargue el archivo **SA-10.6.0.0-UpdatePack-EL6.zip** desde **Download Central** (https://download.rsasecurity.com/). 2. Cargue **SA-10.6.0.0-UpdatePack-EL6.zip** en el repositorio del servidor de Security Analytics antes de actualizar el host de Security Analytics. ⚠ **Precaución:** No seleccione el archivo **SA-10.6.0.0-Manifest-EL6.zip**.	
2.	Actualice los hosts de su implementación de Security Analytics. 1. Actualice el host del servidor de Security Analytics desde la línea de comandos mediante el script de la línea de comandos `sasrv10_4.1-5.xupgd.py` y reinicie el host. 2. Inicie sesión en Security Analytics 10.6 y vaya a **Administration** > vista **Hosts**. 3. Actualice los hosts que no son de servidor de Security Analytics 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/).	
3.	Actualice o instale la recopilación de registros de Windows existente. Consulte **Instrucciones de actualización e instalación de la recopilación de Windows existente de SA 10.6** en SCOL (https://knowledge.rsasecurity.com) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows existente.	

Última modificación: 22 de febrero de 2016, 09:03 h

Tareas de actualización: 10.5.1.x a 10.6

Tarea	Descripción	✓
1.	Complete el repositorio de actualización local del servidor de Security Analytics con los paquetes de actualización a 10.6. • Opción 1: Security Analytics está conectado a Internet (a través de una cuenta de LIVE de Security Analytics): Vaya a **Administration** > **Sistema** > **Actualizaciones** > y haga clic en **Sincronizar ahora**. • Opción 2: Security Analytics no está conectado a Internet (a través de Download Central): a. Descargue los archivos **SA-10.6.0.0-UpdatePack-EL6.zip** y **SA-10.6.0.0-Manifest-EL6.zip** desde **Download Central** (https://download.rsasecurity.com/). b. Cargue estos archivos en el repositorio del servidor de Security Analytics antes de actualizar el host de Security Analytics.	
2.	Actualice los hosts de su implementación de Security Analytics. 1. Inicie sesión en Security Analytics 10.5.1.x y vaya a **Administration** > vista **Hosts**. 2. Actualice el host del servidor de Security Analytics a 10.6 y reinícielo. 3. Inicie sesión en Security Analytics 10.6 y vaya a **Administration** > vista **Hosts**. 4. Actualice los hosts que no son de servidor de Security Analytics 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/).	
3.	Actualice o instale la recopilación de registros de Windows existente. Consulte **Instrucciones de actualización e instalación de la recopilación de Windows existente de SA 10.6** en SCOL (https://knowledge.rsasecurity.com) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows existente.	

Última modificación: 22 de febrero de 2016, 09:03 h

Actualizar o instalar la recopilación de Windows existente

Tarea	Descripción	✓
1.	Actualice o instale la recopilación de registros de Windows existente. Consulte **Instrucciones de actualización e instalación de la recopilación de Windows existente de SA 10.6** en SCOL (https://knowledge.rsasecurity.com) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows existente.	

Tareas posteriores a la actualización

Tarea	Descripción	✓
1.	**Solo para 10.4.1.x a 10.6:** Monitoree la migración de datos de Reporting Engine. **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.	
2.	**Solo para 10.4.1.x a 10.6:** Restaure los directorios de configuración de Incident Management que Security Analytics respaldó antes de la actualización a 10.6. **Nota:** Si no personalizó plantillas de correo, scripts o campos en 10.4.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.	

Última modificación: 22 de febrero de 2016, 09:03 h

3.	**Solo para 10.4.1.x a 10.6:** 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 de Security Analytics mediante el protocolo SSH y escribir el siguiente comando. `reboot` 2. Acceder al host que ejecuta Malware Analysis mediante el protocolo SSH y escribir el siguiente comando. `reboot`	
4.	**Solo para clientes nuevos de Security Analytics a partir de 10.5.0.x:** Restablezca el parámetro `UsingEventTime` de Event Stream Analysis a `true`.	
0.5	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.	
6.	Habilite 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.	
7.	Establezca 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.	

8.	Restaure 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	
9.	Restablezca 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.	

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)