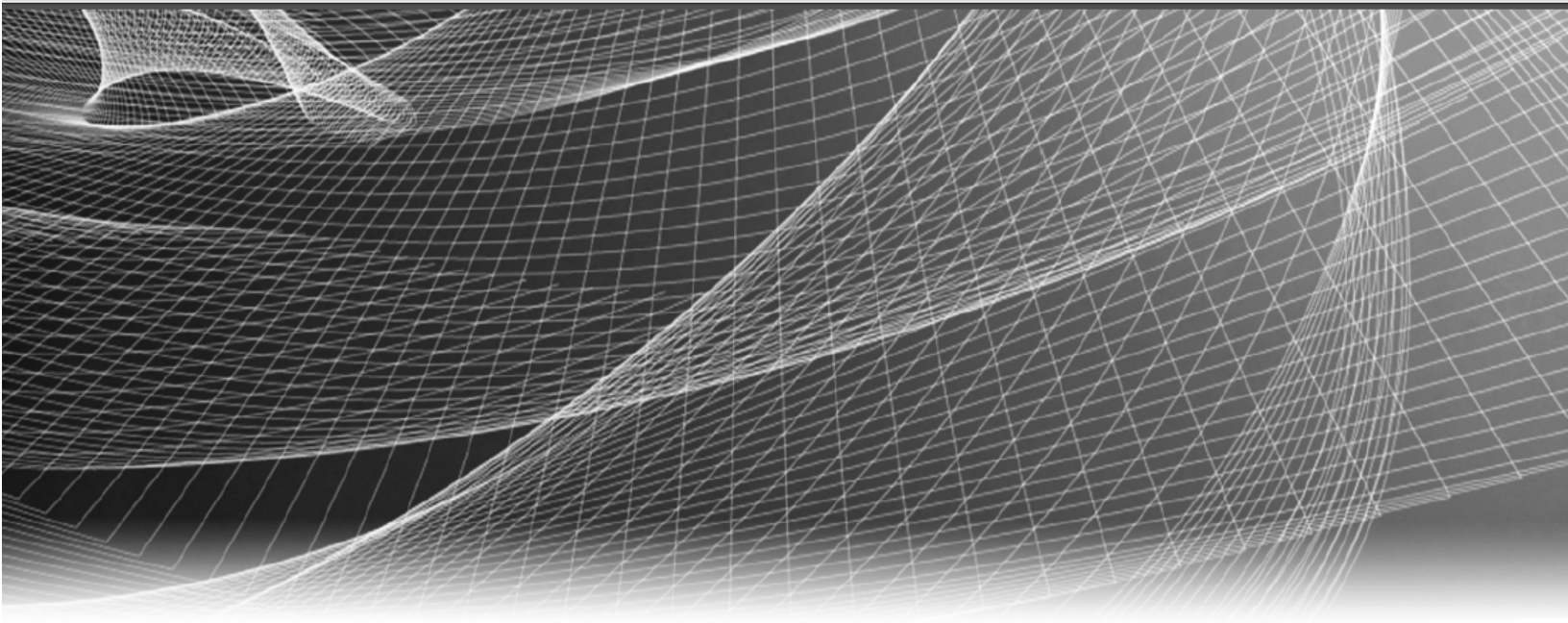

RSA Security Analytics

Lista de verificación de la actualización de 10.5.x.x a 10.6.3.0

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Lista de verificación de la actualización de Security Analytics 10.5.x.x a 10.6.3.0

En esta lista de verificación, se describen las tareas que deben ejecutarse para actualizar las versiones siguientes de Security Analytics 10.5.x.x a 10.6.3.0.

- De 10.5.1.0 a 10.6.3.0
- De 10.5.1.1 a 10.6.3.0
- De 10.5.1.2 a 10.6.3.0
- De 10.5.2.0 a 10.6.3.0
- De 10.5.2.1 a 10.6.3.0
- De 10.5.3.0 a 10.6.3.0

Tareas de preparación para la actualización

Tarea	Descripción	√
1.	**Revisar los puertos principales y abrir los puertos del firewall** Revise los cambios en los puertos de Core en el tema ***Arquitectura y puertos de red*** de la ***Guía de implementación*** disponible en la ayuda de Security Analytics (https://community.rsa.com/) para reconfigurar los servicios de Security Analytics y el firewall. El puerto del servicio Context Hub de Event Stream Analysis (ESA) debe estar disponible para 10.6.3.0. 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.	
2.	**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 ***Montar la IPDB*** en la ***Guía de configuración del servicio IPDB Extractor*** disponible en la ayuda de Security Analytics (https://community.rsa.com/) para obtener instrucciones detalladas para configurar los puntos de montaje de IPDB.	
3.	**Corregir las reglas** Consulte la páginas 9 y 10 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
4.	**Designar servidores primarios y secundarios de Security Analytics** Consulte la página 10 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	

Tarea	Descripción	√
5.	**Respaldar la configuración** Consulte el tema ***Respaldar y restaurar datos para hosts y servicios*** de la ***Guía de mantenimiento del sistema*** disponible en la ayuda de Security Analytics 10.6.3 (https://community.rsa.com/) para obtener reglas sobre cómo respaldar su configuración. **Nota:** Si utiliza el driver de hardware de Decoder 10G y personalizó el script `/etc/init.d/pf_ring` para utilizar la MTU desde el archivo `/etc/pf_ring/mtu.conf`, los archivos `/etc/init.d/pf_ring` y `/etc/pf_ring/mtu.conf` se respaldarán automáticamente durante el proceso de actualización. Sin embargo, deberá restaurarlos en forma manual después de la actualización. Los archivos respaldados se ubicarán en el directorio `../etc/init/pfring_bkup`.	
	Respaldar el archivo de configuración de Malware Analysis en otro directorio Consulte la página 11 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
6.	**Detener la captura y la agregación de datos** RSA recomienda detener la captura y la agregación de paquetes y registros antes de actualizar a 10.6.3.0. Consulte las páginas de la 11 a la 13 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
7.	**Preparar ESA, MA y los dispositivos de SA** Ejecute el comando siguiente en Event Stream Analysis (ESA), Malware Analysis (MA) y los dispositivos de Security Analytics (SA) para asegurar el correcto funcionamiento de la autenticación durante las investigaciones: `chattr -i /var/lib/puppet/lib/puppet/provider/java_ks/keytool.rb`	
8.	**Configurar Reporting Engine para los gráficos de uso inmediato** Para que los gráficos de uso inmediato se ejecuten después de la actualización, debe configurar el origen de datos predeterminado en la página Configuración de Reporting Engine antes de ejecutar la actualización. Si no ejecuta esta tarea, debe configurar manualmente el origen de datos después de la actualización. Para obtener más información sobre los orígenes de datos de Reporting Engine, consulte la Guía de configuración de Reporting Engine (https://community.rsa.com/).	

Tareas de actualización

Tarea	Descripción	√
1.	**Completar el repositorio de actualización local** Consulte las páginas de la 15 a la 18 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
2.	**Actualizar los servidores de Security Analytics** Consulte las páginas de la 19 a la 21 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
3.	**Actualizar hosts de servicio de Security Analytics** Consulte las páginas 21 y 22 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	

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 heredado de RSA Security Analytics***en RSA Link (https://community.rsa.com/) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows heredado. **Nota:** Después de actualizar o instalar la recopilación de Windows heredada, reinicie el sistema para asegurar el correcto funcionamiento de la recopilación de registros.	

Tareas posteriores a la actualización

Tarea	Descripción	√
1.	**Actualizar las configuraciones de ssl.cipher.list y reiniciar los servicios** Este paso aplica una reparación que deshabilita la compatibilidad con los codificadores DES y 3DES, lo que resuelve la vulnerabilidad de SWEET32. Consulte las páginas 31 y 32 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
2.	**Iniciar la captura y la agregación de datos** Consulte las páginas 32 y 33 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
3.	**Asegurarse de que el almacén de confianza tenga certificados para la notificación de syslog del modo TCP** Consulte las páginas 33 y 34 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
4.	**Habilitar el servicio Context Hub** Consulte las páginas 34 y 35 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
5.	**Establecer permisos para el servicio Context Hub** Consulte las páginas 35 y 36 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
6.	**Restaurar valores de parámetros personalizados de Malware Analysis al archivo de configuración creado recientemente** Consulte las páginas 36 y 37 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	

7.	**Restaurar los archivos etc/init.d/pf_ring y /etc/pf_ring/mtu.conf**
	Si utiliza el driver de hardware de Decoder 10G y personalizó el script `/etc/init.d/pf_ring` para utilizar la MTU desde el archivo `/etc/pf_ring/mtu.conf`, restaure los siguientes archivos que respaldó durante las tareas previas a la actualización:
	`/etc/init.d/pf_ring`
	`/etc/pf_ring/mtu.conf`
	Los archivos están ubicados en el directorio `../etc/init/pfring_bkup`.	

Tarea	Descripción	√
8.	**Migrar la STIG de la DISA** Consulte la página 37 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.	
9.	**Restablecer el valor de sistema estable del Lockbox de Log Collector** Debe restablecer el **valor de sistema estable** del Lockbox de Log Collector debido a las actualizaciones del kernel. 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.	
10.	**Comprobar las políticas de estado y condición para los cambios que conlleva la actualización** Compruebe las políticas de estado y condición para los cambios realizados por la actualización. Para obtener información sobre cómo comprobar las políticas de estado y condición, consulte el tema ***Monitorear el estado y la condición de Security Analytics*** de la ***Guía de mantenimiento del sistema de Security Analytics*** disponible en RSA Link (https://community.rsa.com/). Asimismo, puede consultar la ***lista de verificación de mantenimiento del sistema***, que también se encuentra en la ***Guía de mantenimiento del sistema*** de ***Security Analytics*** disponible en RSA Link (https://community.rsa.com/).	
11.	**(Opcional) Actualizar la seguridad de MapR 3.1 o MapR 4.1** Para actualizar las reparaciones de seguridad de MapR 3.1 o 4.1, consulte el artículo de la base de conocimientos donde se describe este procedimiento, disponible en RSA Link (https://community.rsa.com/). (En la base de conocimientos, busque el artículo titulado Security Updates for MapR 3.1 or 4.1).	
12.	**Verificar que los nombres de driver de ODBC sean correctos** En Security Analytics 10.6.2 y versiones posteriores, el driver de Open Database Connectivity (ODBC) se ha actualizado a **27.so**. Obtenga el driver de ODBC más reciente desde Live. A continuación, seleccione los nombres de driver en sus nombres de orígenes de datos (DSN) y, si aún se muestran como **26.so**, actualícelos a **27.so**. Por ejemplo, en la plantilla predeterminada MSSQL_ Server_Windows_Template, tendría que actualizar `/opt/netwitness/odbc/lib/R3sqls26.so` a `opt/netwitness/odbc/lib/R3sqls27.so`.	

Historial de revisiones

Revisión	Fecha	Descripción	Autor
.00	22 de marzo	Versión preliminar inicial	Info Dev and Design
.01	28 de marzo	Versión preliminar final	Info Dev and Design