



RSA | Security Analytics

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

Copyright © 2017 EMC Corporation. Todos los derechos reservados.

Marcas comerciales

RSA, el logotipo de RSA y EMC son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales incluidas/utilizadas en este documento pertenecen a sus respectivos propietarios. Para obtener una lista de las marcas comerciales de EMC, visite <http://mexico.emc.com/legal/emc-corporation-trademarks.htm> (visite el sitio web de su país correspondiente).

Acuerdo de licencia

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

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal. Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por EMC.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto 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 COMERCIALIZABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Contenido

Lista de verificación de la actualización de Security Analytics 10.5.x.x a 10.6.3.0	4
Tareas de preparación para la actualización	5
Tareas de actualización	7
Actualizar o instalar la recopilación de Windows existente	8
Tareas posteriores a la actualización	9
Historial de revisiones	11

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.	<p>Revisar los puertos principales y abrir los puertos del firewall</p> <p>Revise los cambios en los puertos de Core en el tema <i>Arquitectura y puertos de red</i> de la <i>Guía de implementación</i> 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.</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p>Precaución: No realice la actualización hasta que los puertos del firewall estén configurados.</p> </div>	
2.	<p>Asegurarse de que los puntos de montaje de IPDB estén accesibles</p> <p>Asegúrese de que todos los puntos de montaje de IPDB Extractor estén accesibles. Consulte <i>Montar la IPDB</i> en la <i>Guía de configuración del servicio IPDB Extractor</i> disponible en la ayuda de Security Analytics (https://community.rsa.com/) para obtener instrucciones detalladas para configurar los puntos de montaje de IPDB.</p>	
3.	<p>Corregir las reglas</p> <p>Consulte la páginas 9 y 10 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
4.	<p>Designar servidores primarios y secundarios de Security Analytics</p> <p>Consulte la página 10 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	

Tarea	Descripción	✓
5.	<p>Respaldar la configuración</p> <p>Consulte el tema <i>Respaldar y restaurar datos para hosts y servicios</i> de la <i>Guía de mantenimiento del sistema</i> disponible en la ayuda de Security Analytics 10.6.3 (https://community.rsa.com/) para obtener reglas sobre cómo respaldar su configuración.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Nota: Si utiliza el driver de hardware de Decoder 10G y personalizó el script <code>/etc/init.d/pf_ring</code> para utilizar la MTU desde el archivo <code>/etc/pf_ring/mtu.conf</code>, los archivos <code>/etc/init.d/pf_ring</code> y <code>/etc/pf_ring/mtu.conf</code> 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 <code>../etc/init/pfring_bkup</code>.</p> </div>	
	<p>Respaldar el archivo de configuración de Malware Analysis en otro directorio</p> <p>Consulte la página 11 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
6.	<p>Detener la captura y la agregación de datos</p> <p>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.</p>	
7.	<p>Preparar ESA, MA y los dispositivos de SA</p> <p>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:</p> <pre>chattr -i /var/lib/puppet/lib/puppet/provider/java_ks/keytool.rb</pre>	
8.	<p>Configurar Reporting Engine para los gráficos de uso inmediato</p> <p>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/).</p>	

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.	<p data-bbox="305 489 1175 520">Actualice o instale la recopilación de registros de Windows existente.</p> <p data-bbox="305 552 1211 695">Consulte <i>Instrucciones de actualización e instalación de la recopilación de Windows heredado de RSA Security Analytics</i> en RSA Link (https://community.rsa.com/) para obtener detalles acerca de cómo instalar o actualizar la recopilación de Windows heredado.</p> <div data-bbox="310 716 1265 846" style="border: 1px solid green; padding: 5px;"><p data-bbox="318 730 1256 835">Nota: Después de actualizar o instalar la recopilación de Windows heredada, reinicie el sistema para asegurar el correcto funcionamiento de la recopilación de registros.</p></div>	

Tareas posteriores a la actualización

Tarea	Descripción	✓
1.	<p>Actualizar las configuraciones de <code>ssl.cipher.list</code> y reiniciar los servicios</p> <p>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.</p>	
2.	<p>Iniciar la captura y la agregación de datos</p> <p>Consulte las páginas 32 y 33 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
3.	<p>Asegurarse de que el almacén de confianza tenga certificados para la notificación de syslog del modo TCP</p> <p>Consulte las páginas 33 y 34 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
4.	<p>Habilitar el servicio Context Hub</p> <p>Consulte las páginas 34 y 35 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
5.	<p>Establecer permisos para el servicio Context Hub</p> <p>Consulte las páginas 35 y 36 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
6.	<p>Restaurar valores de parámetros personalizados de Malware Analysis al archivo de configuración creado recientemente</p> <p>Consulte las páginas 36 y 37 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
7.	<p>Restaurar los archivos <code>etc/init.d/pf_ring</code> y <code>etc/pf_ring/mtu.conf</code></p> <p>Si utiliza el driver de hardware de Decoder 10G y personalizó el script <code>/etc/init.d/pf_ring</code> para utilizar la MTU desde el archivo <code>/etc/pf_ring/mtu.conf</code>, restaure los siguientes archivos que respaldó durante las tareas previas a la actualización:</p> <pre>/etc/init.d/pf_ring /etc/pf_ring/mtu.conf</pre> <p>Los archivos están ubicados en el directorio <code>../etc/init/pfring_bkup</code>.</p>	

Tarea	Descripción	✓
8.	<p>Migrar la STIG de la DISA</p> <p>Consulte la página 37 del documento Instrucciones para la actualización a Security Analytics 10.6.3.0.</p>	
9.	<p>Restablecer el valor de sistema estable del Lockbox de Log Collector</p> <p>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.</p>	
10.	<p>Comprobar las políticas de estado y condición para los cambios que conlleva la actualización</p> <p>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 <i>Monitorear el estado y la condición de Security Analytics</i> de la <i>Guía de mantenimiento del sistema de Security Analytics</i> disponible en RSA Link (https://community.rsa.com/). Asimismo, puede consultar la <i>lista de verificación de mantenimiento del sistema</i>, que también se encuentra en la <i>Guía de mantenimiento del sistema de Security Analytics</i> disponible en RSA Link (https://community.rsa.com/).</p>	
11.	<p>(Opcional) Actualizar la seguridad de MapR 3.1 o MapR 4.1</p> <p>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).</p>	
12.	<p>Verificar que los nombres de driver de ODBC sean correctos</p> <p>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</p> <pre data-bbox="315 1629 911 1696">/opt/netwitness/odbc/lib/R3sqls26.so a opt/netwitness/odbc/lib/R3sqls27.so.</pre>	

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