RSA NETWITNESS® SUITE

Guía de integración de RSA Archer

para la versión 11.0

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (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 de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

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

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.

febrero 2018

Contenido

Integración de RSA Archer

Los administradores pueden integrar RSA NetWitness Suite con RSA NetWitness Security Operations (SecOps) Manager para enviar alertas e incidentes desde NetWitness Suite a Archer para la administración y corrección de incidentes. En esta guía se proporciona un flujo de trabajo general para configurar esta integración.

En la tabla siguiente se enumeran las opciones de integración de NetWitness Suite 11.0 con NetWitness SecOps Manager versión 1.3.1.2.

Versión de NetWitness SecOps Manager	Integración de NetWitness Suite 11.0	Referencia
1.3.1.2	Event Stream Analysis (ESA)	Para obtener más información, consulte la sección “Configurar Event Stream Analysis para la integración con Archer SecOps”.
1.3.1.2	Reporting Engine (RE)	Para obtener más información, consulte la sección “Configurar Reporting Engine para la integración con Archer SecOps”.
1.3.1.2	Respond	Para obtener más información, consulte la sección “Configurar Respond para la integración con Archer SecOps 1.3.1.2".
1.3.1.2	Feeds de Archer	Para obtener más información, consulte la sección “Feeds de RSA Archer”.

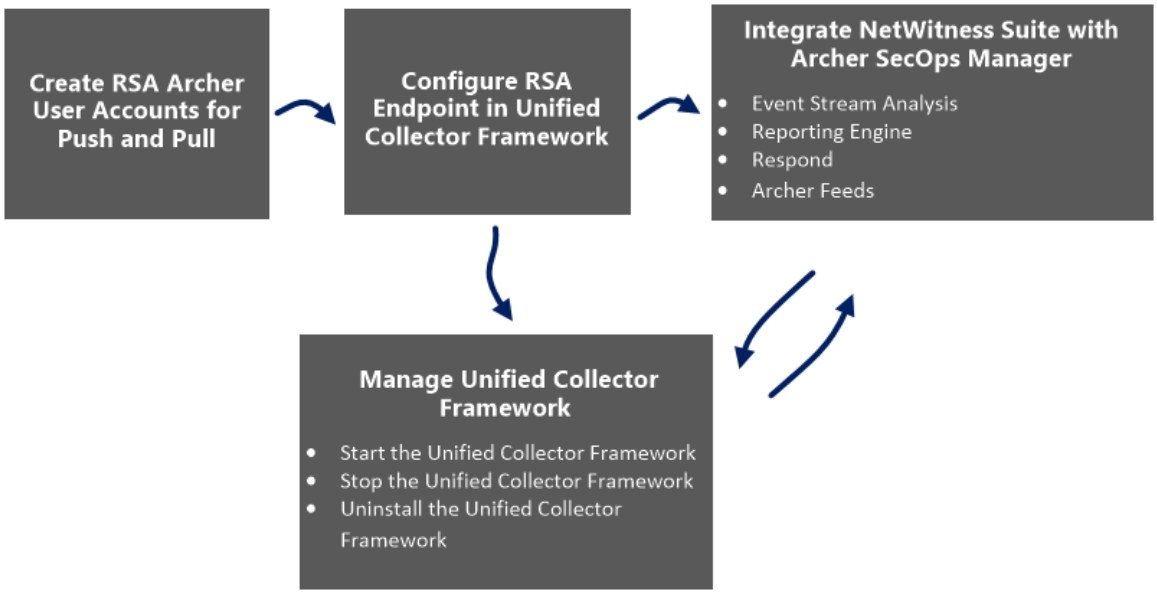
Configurar NetWitness para trabajar con Archer

La solución RSA NetWitness SecOps Manager permite agregar todas las alertas de seguridad útiles, lo cual brinda mayor eficacia, proactividad y orientación hacia la administración de respuesta ante incidentes y del SOC. Para obtener más información sobre las funcionalidades de RSA NetWitness SecOps, consulte la documentación de RSA Archer en la Comunidad de RSA Archer o en la Comunidad de RSA Archer Exchange.

La versión de RSA Archer determina cómo se integrará NetWitness Suite. Consulte la *Guía de instalación de SecOps* para conocer las plataformas compatibles con Archer.

NetWitness SecOps Manager 1.3.1.2 se integra con NetWitness Suite mediante RSA UCF (Unified Collector Framework) que consta del servicio de integración Security Analytics Incident Management (IM) y del servicio SecOps Watchdog.

Esta figura representa el flujo de integración de NetWitness Suite 11.0 con NetWitness SecOps Manager 1.3.1.2.



Crear cuentas de usuario de RSA Archer para migración y extracción

Debe crear una cuenta de usuario para el cliente del servicio web con el fin de transferir datos a la plataforma RSA Archer GRC.

Se requieren dos cuentas de usuario de RSA Archer para evitar conflictos al enviar y recibir datos de RSA NetWitness Suite.

Para crear una cuenta de usuario con fines de migración y extracción, realice lo siguiente:

1. En la interfaz del usuario de RSA Archer, haga clic en **Administration** > **Control de acceso** > **Usuarios** > **Agregar nuevo**.
2. En los campos **Nombre** y **Apellido**, escriba un nombre que indique que UCF usa esta cuenta para migrar datos a RSA Archer GRC. Por ejemplo, usuario de UCF, migrar.

   Nota: Al configurar la cuenta de extracción, escriba un nombre que indique que el UCF usa esta cuenta para extraer datos de RSA Archer GRC. Por ejemplo, usuario de UCF, extraer.
3. (Opcional) Ingrese un nombre de usuario para la nueva cuenta de usuario.

   Nota: Si no especifica un nombre de usuario, RSA Archer GRC Platform crea el nombre de usuario a partir del nombre y el apellido que ingresó cuando guardó la nueva cuenta de usuario.
4. En la sección **Información de contacto**, en el campo **Correo electrónico**, ingrese una dirección de correo electrónico para asociar a esta nueva cuenta de usuario.
5. En la sección **Localización**, cambie la zona horaria a la hora universal coordinada (UTC).

   Nota: El UCF utiliza la hora UTC para establecer todos los cálculos relacionados con hora.
6. En la sección **Mantenimiento de la cuenta**, ingrese y confirme una nueva contraseña para la nueva cuenta de usuario.

   Nota: Anote el nombre de usuario y la contraseña para la nueva cuenta de usuario que acaba de crear. Debe ingresar estas credenciales cuando configura el UCF para comunicarse con la plataforma RSA Archer GRC a través del cliente de servicio web.
7. Deseleccione la opción Forzar cambio de contraseña en el **próximo inicio de sesión**.
8. En el campo **Parámetro de seguridad**, seleccione el parámetro de seguridad que desea usar para este usuario.

   Nota: Si asigna un parámetro de seguridad predeterminado con un intervalo de cambio de contraseña de 90 días, también debe actualizar la contraseña de la cuenta de usuario almacenada en el servicio de integración de SA IM cada 90 días. Para evitar esto, puede crear de manera opcional un nuevo parámetro de seguridad para la cuenta de usuario del servicio de integración de SA IM y establecer el intervalo de cambio de contraseña en el valor máximo que permiten sus estándares corporativos.
9. Haga clic en la pestaña **Grupos** y realice lo siguiente:

a. En la sección **Grupos**, haga clic en **Búsqueda**.

b. En la ventana **Grupos disponibles**, expanda Grupos.

c. Desplácese hacia abajo y seleccione SOC: Administrador de soluciones y EM: Solo lectura.

d. Haga clic en **Aceptar**.

10. Haga clic en **Aplicar** y, a continuación, en **Guardar**.
11. Si el idioma de la máquina y la configuración regional del sistema RSA Archer GRC se configuran en cualquier valor que no sea inglés de Estados Unidos, realice lo siguiente:

a. Abra la cuenta de usuario que acaba de crear y, en la sección **Localización**, campo Configuración regional, seleccione **Inglés (Estados Unidos)** y haga clic en **Guardar**.

b. En el sistema de Windows que aloja RSA Archer GRC Platform, abra el Administrador de servicios de información de Internet (IIS).

c. Expanda su sitio de RSA Archer GRC, haga clic en **.Net Globalization**, en los campos **Cultura** y **Cultura de la interfaz del usuario** seleccione **Inglés (Estados Unidos)** y haga clic en **Aplicar**.

d. Reinicie el sitio de RSA Archer GRC.

12. Repita los pasos del 1 al 11 para crear una segunda cuenta de usuario de modo que el UCF extraiga datos de RSA Archer GRC.

Configurar extremos en RSA Unified Collector Framework

Los terminales proporcionan los detalles de conexión necesarios para que UCF se comunique con los sistemas de RSA NetWitness Suite y RSA Archer GRC.

Nota: Algunos extremos son necesarios para usar diferentes integraciones. En la siguiente lista se muestran los terminales obligatorios.

Integración de terminal obligatorio

- Terminal de migración de Archer
- Terminal de extracción de Archer
- Selección del modo: Modo SecOps o No SecOps.

Nota:
• Si se selecciona el modo No SecOps, los incidentes se administran en NetWitness Suite Respond en lugar de RSA Archer Security Operations Management.
• Debe configurar el puerto según el protocolo (TCP, UDP o TCP seguro).
• Asegúrese de que el nombre de sujeto del certificado para el servidor de RSA Archer GRC coincida con el nombre de host.

Procedimiento

1. En el sistema UCF, abra el administrador de conexión de la siguiente manera:
   a. Abra una línea de comandos.
   b. `Cambie de directorio a <install_dir>\SA IM integration service\data-collector`
   c. `Escriba: runConnectionManager.bat`
2. En el **administrador de conexión**, ingrese **1** para agregar el terminal.
3. Agregue un terminal para migrar datos a RSA Archer Security Operations Management, como se muestra a continuación:
   a. Ingrese el número de Archer.

      Nota: SSL debe estar habilitado para agregar los terminales de RSA Archer.

   b. Para el nombre del terminal, ingrese **push**.
   c. Ingrese la dirección URL de su sistema RSA Archer GRC.
   d. Ingrese el nombre de la instancia del sistema RSA Archer GRC.
   e. Ingrese el nombre de usuario de la cuenta de usuario que creó para migrar datos a su sistema RSA Archer GRC.
   f. Ingrese la contraseña para la cuenta de usuario que creó para migrar datos al sistema RSA Archer GRC y confírmela.
   g. Cuando se le pregunte si esta cuenta se usa para extraer datos, ingrese **False**.
4. Agregue un extremo para extraer datos de RSA Archer Security Operations Management, como se muestra a continuación:
   a. Ingrese el número de Archer.

      Nota: SSL debe estar habilitado para agregar los terminales de RSA Archer.

   b. Para el nombre del terminal, ingrese **pull**.

c. Ingrese la dirección URL de su sistema RSA Archer GRC.

d. Ingrese el nombre de la instancia del sistema RSA Archer GRC.

e. Ingrese el nombre de usuario de la cuenta de usuario que creó para extraer datos desde el sistema RSA Archer GRC.

f. Ingrese la contraseña para la cuenta de usuario que creó para extraer datos desde el sistema RSA Archer y confírmela.

g. Cuando se le pregunte si esta cuenta se usa para extraer datos, ingrese **True**.

5. Agregar un terminal para RSA NetWitness Suite.

- Para RESPOND

a. Ingrese el número de Security Analytics IM.

b. Ingrese un nombre para el extremo.

c. Ingrese la dirección IP del host de SA.

d. Para el puerto de mensajería de SA, ingrese **5671**.

e. Ingrese la línea de espera objetivo para las tareas de corrección. Si selecciona Todo, se procesa la integración de RSA Archer (GRC) y help desk de TI (operaciones).

f. Para agregar automáticamente certificados al almacén de confianza de NetWitness Suite, realice lo siguiente:

i. Ingrese **Sí**.

ii. Ingrese el nombre de usuario y la contraseña del host de NetWitness Suite.

> **Nota:** Si recibe un error que indica que el almacén de confianza de CA no se pudo configurar, consulte Solucionar problemas de integración de RSA Archer.

g. En el administrador de conexión de UCF, seleccione el modo, como se indica a continuación:

i. Ingrese el número para la selección de modo.

ii. Seleccione una de las siguientes opciones:

- Administrar el flujo de trabajo de incidentes en RSA NetWitness Suite.
- Administrar el flujo de trabajo de incidentes exclusivamente en RSA Archer Security Operations Management.

- Para Reporting Engine e Event Stream Analysis
  a. Para utilizar las integraciones de otros fabricantes, agregue el extremo del servidor de syslog, como se indica a continuación:
     i. Ingrese el número del extremo del servidor de syslog.
     ii. Ingrese la siguiente información:
     - Nombre definido por el usuario
     - Número de puerto TCP configurado de SSL

       Nota: El valor predeterminado es 1515. Si no desea alojar el servidor de syslog en este modo, ingrese **0**.
     - Número de puerto TCP: Ingrese el puerto TCP si el cliente de syslog envía el mensaje de syslog en el modo TCP.

       Nota: El valor predeterminado es 1514. Si no desea alojar el servidor de syslog en este modo, ingrese **0**.
     - Número de puerto UDP: Ingrese el puerto UDP si el cliente de syslog envía el mensaje de syslog en el modo UDP.

       Nota: El valor predeterminado es 514. Si no desea alojar el servidor de syslog en este modo, ingrese **0**.

     De forma predeterminada, el servidor de syslog se ejecutará en los tres modos anteriores, a menos que se deshabilite mediante el ingreso de **0**.
  b. Para probar el cliente de syslog, ingrese el número del cliente de syslog de prueba. Utilice el cliente de syslog de prueba con los archivos de `<install_dir>\SA IM integration service\config\mapping\test-files\`.
6. En el administrador de conexión, ingrese **5** para probar cada terminal.

Integrar NetWitness Suite con Archer SecOps Manager

Debe configurar los ajustes de integración del sistema para administrar el flujo de trabajo de incidentes en RSA NetWitness SecOps Manager.

Para obtener información sobre cómo configurar los ajustes de integración del sistema para administrar el flujo de trabajo de incidentes en RSA Archer Security Operations, consulte el tema “Configurar ajustes de integración para administrar incidentes en RSA Archer Security Operations” de la *Guía de NetWitness Respond*.

RSA Unified Collector Framework (UCF)

RSA NetWitness Suite se integra con RSA Archer SecOps Manager 1.3.1.2 mediante RSA Unified Collector Framework (UCF). RSA Unified Collector Framework (UCF) se integra con todas las herramientas compatibles de SIEM y con la solución RSA NetWitness SecOps Manager. Al integrar RSA NetWitness Suite Respond, puede administrar el flujo de trabajo de incidentes en NetWitness Suite Respond y permitir a los analistas la opción de elevar las tareas de corrección y las vulneraciones de datos abiertas para su administración y corrección en la solución RSA Archer Security Operations Management. Además, Unified Collector Framework transporta tareas de corrección (creadas como observaciones), vulneraciones de datos o ambas.

Nota:
• Debe configurar la misma opción en RSA NetWitness Suite y en Unified Collector Framework.
• La integración del módulo RSA NetWitness Respond con Reporting Engine o Event Stream Analysis puede hacer que se creen eventos e incidentes duplicados en RSA Archer SecOps Manager.

UCF es compatible con múltiples conexiones de herramientas SIEM al mismo tiempo; por ejemplo, es compatible con NetWitness Suite Reporting Engine, HP ArcSight y NetWitness Suite Respond. Sin embargo, distintas instancias de la misma herramienta SIEM no son compatibles; por ejemplo, dos servidores de NetWitness Suite conectados al mismo UCF.

Requisitos previos

- Instale el paquete de RSA_Archer_Security_Operations_Management en Archer. Consulte la documentación de RSA Archer en la Comunidad de RSA Archer o en la pestaña Contenido en https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.
- Instale NetWitness SecOps Manager.
- Asegúrese de disponer de NetWitness Suite 11.0, ya que es compatible con NetWitness SecOps Manager 1.3.1.2.
- Asegúrese de que Respond esté configurado en RSA NetWitness Suite.

RSA Unified Collector Framework (UCF) permite integrar el sistema RSA Archer Security Operations Manager con lo siguiente:

- NetWitness Suite Respond
- NetWitness Suite Reporting Engine
- NetWitness Suite Event Stream Analysis
- Feeds de Archer

Configurar Respond para la integración con Archer SecOps

Para configurar Respond para Archer SecOps, realice lo siguiente en NetWitness Suite:

Paso 1: Seleccionar el modo para NetWitness Suite Respond

1. Seleccione **ADMIN > Servicios > Respond > Explorar**.
2. Navegue a `Respond/Aggregation/export`.
3. Habilite el campo `archer-secops-integration-enabled` en **true**.
4. Reinicie el servicio Respond.

Paso 2: Configurar NetWitness Suite Respond para reenviar alertas a UCF

1. Navegue a `C:\Program Files\RSA\SA IM integration service\cert-tool\certs` en la computadora de middleware de SecOps.
2. Copie `keystore.cert.pem` y `rootcastore.cert.pem` desde la carpeta certs (a la carpeta import del servidor de NW)
   ```
   cp rootcastore.crt.pem /etc/pki/nw/trust/import

   cp keystore.crt.pem /etc/pki/nw/trust/import
   ```
3. Acceda mediante el protocolo SSH a la computadora del servidor de NW.
   a. Ejecute el comando update-admin-node
      ```
      orchestration-cli-client --update-admin-node
      ```
   b. Reinicie el servidor de RabbitMQ
      ```
      service rabbitmq-server restart
      ```
   c. Cree el usuario archer y configure permisos para el host virtual "`/rsa/system`"
      ```
      rabbitmqctl add_user archer archer

      rabbitmqctl clear_password archer

      rabbitmqctl set_permissions -p /rsa/system archer ".*" ".*" ".*"
      ```

Paso 3: Reenviar alertas a NetWitness Suite Respond

- **Para reenviar alertas de NetWitness Suite Event Stream Analysis a NetWitness Respond, realice lo siguiente:**
  a. Seleccione **ADMIN > Servicios > servicio ESA**.
  b. Seleccione un servicio Event Stream Analysis y haga clic en **> Ver > Configuración**.
  c. Haga clic en la pestaña **Opciones avanzadas**.

d. Asegúrese de que la casilla de verificación **Reenviar alertas en bus de mensajes** esté seleccionada de manera predeterminada. Si no lo está, seleccione la casilla de verificación **Reenviar alertas en bus de mensajes** y haga clic en **Aplicar**.

- **Para reenviar alertas de NetWitness Suite Reporting Engine a NetWitness Respond, realice lo siguiente:**
  a. Seleccione **ADMIN > Servicios > servicio Reporting Engine**.
  b. Haga clic en **> Ver > Configuración** para el servicio Reporting Engine.
  c. Haga clic en la pestaña **General**.
  d. En la **sección Configuración del sistema**, seleccione la casilla de verificación **Reenviar alertas a Respond** y haga clic en **Aplicar**.
- **Para reenviar alertas de NetWitness Suite Malware Analysis a NetWitness Respond, realice lo siguiente:**
  a. Seleccione **ADMIN > Servicios > servicio Malware Analysis**
  b. Haga clic en > **Ver** > **Configuración** para el servicio Malware Analysis.
  c. Haga clic en la pestaña **Auditoría**.
  d. En la sección **Alerta de Respond**, verifique que la casilla de verificación **Valor de configuración activado** esté seleccionada. Si no lo está, selecciónela y haga clic en **Aplicar**.

Paso 4: Reenviar alertas de Endpoint a NetWitness Suite Respond

Las alertas de RSA Endpoint se pueden enviar a RSA Archer GRC a través de NetWitness Respond. Para obtener más información sobre cómo configurar alertas de NetWitness Endpoint mediante el bus de mensajes, consulte el tema “Configurar alertas de NetWitness Endpoint mediante el bus de mensajes” de la *Guía de integración de NetWitness Endpoint*.

Paso 5: Agregar alertas en incidentes

Las alertas que llegan a NetWitness Respond se pueden agregar automáticamente a incidentes y se reenvían a RSA Archer Security Operations Management. Las reglas de agregación se ejecutan automáticamente cada minuto y agregan las alertas en incidentes en función de las condiciones de coincidencia y las opciones de agrupación seleccionadas. Para obtener más información sobre la agregación de alertas, consulte el tema “Configurar orígenes de alertas para mostrar alertas en Respond” de la *Guía de configuración de NetWitness Respond*.

Para configurar la agregación de alertas:

1. Seleccione **CONFIGURAR > Reglas de incidentes**.
2. Para habilitar las reglas que se proporcionan de manera inmediata, realice lo siguiente:
   a. Haga doble clic en la regla.
   b. Seleccione **Activado**.
   c. Haga clic en **Guardar**.
   d. Repita los pasos a-c para cada regla.
3. Para agregar una nueva regla, realice lo siguiente:
   a. Haga clic en +.
   b. Seleccione **Activado**.
   c. Complete los siguientes campos:
      - Nombre de la regla
      - Acción
      - Condiciones de coincidencia
      - Opciones de agrupación
      - Opciones de incidente
      - Prioridad
      - Notificaciones
4. Haga clic en **Guardar**.

Configurar Reporting Engine para la integración con NetWitness SecOps Manager

Para configurar una acción de salida de syslog para Reporting Engine, realice lo siguiente:

1. Seleccione **ADMIN > Servicios**.
2. Seleccione el servicio Reporting Engine y haga clic en **Ver** > **Configuración**.
3. Haga clic en la pestaña **Acciones de salida**.
4. En la sección **Configuración de NetWitness Suite**, en el campo **Nombre del host**, ingrese el nombre de host o la dirección IP del servidor de Reporting Engine.

5. En la sección **Configuración de Syslog**, agregue la configuración de syslog como se indica a continuación:
   a. En el campo **Nombre del servidor**, ingrese el nombre de host de UCF.
   b. En el campo **Puerto del servidor**, ingrese el puerto que seleccionó en la configuración de syslog de UCF.
   c. En el campo **Protocolo**, seleccione el protocolo de transporte.

   Nota: Si selecciona TCP seguro, se debe configurar SSL.
6. Haga clic en **Guardar**.

Para configurar el protocolo SSL de NetWitness Suite Reporting Engine para el servidor de syslog seguro:

Si el servidor de syslog está configurado con TCP seguro, configure el SSL.

1. Copie el certificado `keystore.crt.der` desde la máquina de UCF a la computadora del servidor de NetWitness Suite en `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3.x86_64/jre/lib/security`.
2. Ejecute el siguiente comando:

   ```
   keytool -import -file keystore.crt.der -alias ucf-syslog -keystore /etc/pki/nw/trust/truststore.jks -storepass changeit
   ```

   Nota: No copie ni pegue el código anterior. Escríbalo para evitar errores.
3. Habilite **ServerCertificateValidationEnabled** en **true:**
   - Navegue a **ADMIN** > **Servicio**.
   - Haga clic en > **Ver > Explorar** en el servicio Reporting Engine.
   - Expanda **com.rsa.soc.re** > **Configuración** > **SSLContextConfiguration**.
   - Expanda **sslContextConfiguration** y configure **ServerCertificateValidationEnabled** en **true**.
4. Reinicie el servicio Reporting Engine.

Para configurar reglas en NetWitness Suite:

1. Haga clic en **MONITOR >Informes > Administrar**.
   Se muestra la pestaña Administrar.
2. En el panel **Grupos de reglas**, haga clic en +.
3. Introduzca un nombre para el nuevo grupo.

4. Seleccione el grupo que creó y, en la barra de herramientas Regla, haga clic en ✚.
5. En el campo **Tipo de regla**, seleccione Base de datos de NetWitness.
6. Ingrese un nombre para la regla.
7. Ingrese valores en los campos **Select** y **Where** en función de la regla que desea crear.

   Nota: Agregue la configuración de syslog con el nombre de syslog definido anteriormente.

8. Haga clic en **Guardar**.

Nota: Para ver la misma cantidad de alertas en Reporting Engine y RSA Archer GRC, asegúrese de haber seleccionado Una vez para ejecución en las pestañas Syslog y Registro.

Para agregar plantillas de alerta para Reporting Engine en NetWitness Suite:

La configuración de syslog UCF viene con plantillas de alerta listas para usar que puede utilizar cuando crea una alerta con una acción de salida de syslog. Estas plantillas definen los criterios que se usan para agregar alertas a incidentes en su RSA Archer GRC Platform.

Las plantillas de ejemplo se encuentran en la siguiente ubicación del sistema UCF:

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates`

1. Haga clic en **MONITOR > Informes > Administrar > Alertas**.
2. Haga clic en la pestaña **Plantilla**.
3. Haga clic en ✚.
4. En el campo **Nombre**, ingrese un nombre para la plantilla de alerta.
5. En el campo **Mensaje**, ingrese el mensaje de alerta.
6. Haga clic en **Crear**.
7. Repita los pasos 3 a 6 para cada plantilla de alerta que desea agregar.

Para configurar alertas en NetWitness Suite:

En RSA NetWitness Suite Reporting Engine, una alerta es una regla que puede programar para que se ejecute de forma continua y registre sus observaciones en varias salidas de alerta diferentes.

1. Haga clic en **MONITOR > Informes > Administrar > Alertas**.
2. Haga clic en ✚.
3. Seleccione **Habilitar**.
4. Seleccione la regla que creó.

5. Seleccione **Migrar a decodificadores**.

   Nota: Si no ingresa un valor en este campo, el vínculo en la aplicación RSA Archer Security Alerts a RSA NetWitness Suite no funcionará.

6. En la lista Orígenes de datos, seleccione su origen de datos.
7. En la sección **Notificación**, seleccione **Syslog**.
8. Haga clic en +.
9. Complete los campos de configuración de syslog.
10. En el campo **Plantilla de cuerpo**, seleccione la plantilla que desea usar para esta alerta de syslog.
11. Haga clic en **Guardar**.

Configurar Event Stream Analysis para la integración con Archer SecOps

Para configurar los ajustes de notificación de syslog en Event Stream Analysis en NetWitness Suite:

1. Haga clic en **ADMIN** > **Sistema** > **Notificaciones globales**.
2. Haga clic en la pestaña **Salida**.
3. Defina y habilite una notificación de syslog de Event Stream Analysis.
4. Haga clic en la pestaña **Servidores**.
5. Defina y habilite un servidor de notificación de syslog.
6. En la sección Configuración del servidor de syslog, ingrese lo siguiente:

   Descripción de los campos:

   - Nombre: Especifique el nombre personalizado.
   - IP del servidor (nombre de host): Especifique el nombre de host o la dirección IP del sistema en el que instaló UCF.
   - Puerto: Especifique el número de puerto en el que desea que UCF escuche.
   - Funcionalidad: Especifique la funcionalidad de syslog.
   - Protocolo: Seleccione el protocolo.

7. Haga clic en **Guardar**.

Para configurar el protocolo SSL de NetWitness Suite Event Stream Analysis para el servidor de syslog seguro:

Si el servidor de syslog está configurado con TCP seguro, configure el SSL.

1. Seleccione **ADMIN > Servicios**.
2. Seleccione el servicio Event Stream Analysis. Vaya a **Explorar > Configuración > SSL**.
3. Configure **ServerCertificateValidationEnabled** en **true.**
4. Copie `rootcastore.cert.pem` de la máquina de UCF al servidor de Event Stream Analysis en `/etc/pki/ca-trust/source/anchors`.
5. Ejecute el siguiente comando:

   ```
   update-ca-trust
   ```

6. Reinicie el servidor de Event Stream Analysis.

Para agregar plantillas de alerta de Event Stream Analysis

La configuración de syslog UCF viene con plantillas de alerta listas para usar que puede utilizar cuando crea una alerta con una acción de salida de syslog. Estas plantillas definen los criterios que se usan para agregar alertas a incidentes en su RSA Archer GRC Platform.

Las plantillas de ejemplo se encuentran en la siguiente ubicación del sistema UCF:

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_`

`Templates\SecOps_SA_ESA_templates.txt`

1. Seleccione **ADMIN > Sistema > Notificaciones globales**.
2. Haga clic en la pestaña **Plantillas**.
3. Haga clic en ✚.
4. En el campo **Tipo de plantilla**, seleccione Event Stream Analysis.
5. En el campo **Nombre**, ingrese el nombre de la plantilla.
6. (Opcional) En el campo **Descripción**, ingrese una descripción breve de la plantilla.
7. En el campo **Plantilla**, ingrese el mensaje de alerta.
8. Haga clic en **Guardar**.
9. Repita los pasos del 3 al 8 para cada plantilla de alerta que desea agregar.

Para crear reglas de Event Stream Analysis

1. Haga clic en **CONFIGURAR** > **Reglas de ESA**.
2. En la **Biblioteca de reglas**, haga clic en ✚.
3. Seleccione **Generador de reglas**.

4. En el campo **Nombre de la regla**, ingrese un nombre para la regla.
5. En el campo **Descripción**, escriba una descripción para la regla.
6. Seleccione la **Gravedad**.
7. En la sección **Condición**, realice lo siguiente:
   a. Haga clic en ✚ para crear una declaración.
   b. Ingrese un nombre, seleccione un tipo de condición y agregue pares de metadatos/valores para la declaración.
   c. Haga clic en **Guardar**.
   d. Repita los pasos del a al c hasta que haya creado todas las declaraciones para la regla.
8. En la sección **Notificaciones**, seleccione **Syslog**.
9. Seleccione la notificación, el servidor de syslog y la plantilla que se crearon anteriormente.
10. Haga clic en **Save** y **Close**.
11. Haga clic en **Configurar** > **Implementaciones**.
12. Haga clic en ✚ para la sección de servicios de Event Stream Analysis.
13. Seleccione el servicio Event Stream Analysis.
14. Haga clic en **Implementar ahora**.
15. En la sección **Reglas de Event Stream Analysis**, haga clic en ✚ para elegir la regla de Event Stream Analysis que creó y haga clic en **Implementar ahora**.

Feed de RSA Archer

De forma predeterminada, solo los campos Dirección IP y Clasificación de criticidad de la aplicación RSA Archer Devices se alimentan en RSA NetWitness Suite mediante el servicio de integración de SA IM. Puede personalizar el plug-in de Enterprise Management para incluir los campos Unidad de negocios y Funcionalidad que tienen referencia cruzada en la aplicación Dispositivos en el feed. Para obtener más detalles, consulte la documentación de Archer en https://community.emc.com/community/connect/grc_ecosystem/rsa archer o https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.

Nota: Si planea incluir información de Unidad de Negocio y Funcionalidad desde RSA Archer GRC Platform en Live, también debe agregar claves para estos campos en el archivo index-concentrator-custom.xml.

Actualizar los servicios de Concentrator y Decoder

El servicio de integración de SA IM en NetWitness SecOps Manager administra los archivos para un feed personalizado y los deposita en una carpeta local que se especifica cuando se configura el terminal de Enterprise Management. El módulo Live de RSA NetWitness Suite recupera los archivos de feed de esta carpeta. A continuación, Live inserta el feed en los Decoders, los cuales comienzan a crear metadatos según el tráfico de red capturado y la definición del feed. Para que cada Concentrator reconozca los metadatos nuevos que crean los Decoders, debe editar los archivos `index-concentrator-custom.xml`, `index-logdecoder-custom.xml` y `index-decoder-custom.xml files`.

1. Seleccione **ADMIN > Servicios**.
2. Seleccione el Concentrator y elija  > **Ver > Configuración**.
3. Haga clic en la pestaña **Archivos**.
4. En la lista desplegable, seleccione index-concentrator-custom.xml. Realice una de las siguientes acciones:
   - Si el contenido ya existe en el archivo, agregue una clave para el nuevo elemento de metadatos de la siguiente manera:

     ```
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     ```

     Nota: No copie ni pegue el código. Escríbalo para evitar errores.
   - Si el archivo está en blanco, agregue el siguiente contenido:

     ```
     <?xml version="1.0" encoding="utf-8"?>
     <language level="IndexNone" defaultAction="Auto">
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     </language>
     ```
5. Haga clic en **Aplicar**.
6. Para agregar varios dispositivos, realice lo siguiente:
   a. Haga clic en **Migrar.**
   b. Seleccione los dispositivos a los que desea migrar este archivo.
   c. Haga clic en **Aceptar**.
7. Repita los pasos 1 al 7 para los Log Decoders e Index Decoders mediante index-logdecoder-custom.xml e index-decoder-custom.xml.
8. Reinicie los servicios Concentrator y Decoder.

Agregar el extremo de RSA Archer Enterprise Management en el UCF

1. En el administrador de conexión de UCF, seleccione el modo, como se indica a continuación:
   a. Ingrese el número para la selección de modo.
   b. Seleccione una de las siguientes opciones:
      - Administrar el flujo de trabajo de incidentes en RSA NetWitness Suite.
      - Administrar el flujo de trabajo de incidentes exclusivamente en RSA Archer Security Operations Management.
2. Agregar el extremo de RSA Archer Enterprise Management, de la siguiente manera:
   a. Ingrese el número para Enterprise Management.
   b. Complete los campos en la siguiente tabla.

Campo	Descripción
Nombre del terminal	Nombre del extremo opcional.
Puerto del servidor web	El valor predeterminado es 9090. Puede configurarse para alojar la url del servidor web. Se debe proporcionar la dirección URL con el número de puerto como la URL en el feed de NetWitness Suite Live: http://hostname:port/archer/sa/feed
Importancia	Importancia de los recursos que se extraen de RSA Archer GRC. Si es **falso**, extraiga los recursos que tengan cualquier criticidad. Si es **verdadero**, extraiga los recursos que solo tengan criticidad alta. Para configurarlo manualmente, edite la propiedad em.criticality en el archivo de propiedades de collector-config para proporcionar una lista de criticidades separada por comas: BAJA, MEDIA, ALTA.
Directorio de feed	Directorio donde se guarda el archivo CSV de recursos de RSA Archer GRC. **Nota:** Debe existir la ruta del directorio proporcionada.

Campo	Descripción
Nombre de usuario del servidor web	Nombre de usuario para autenticación en el servidor web de EM. **Nota:** Esta información se proporciona durante la configuración del feed de NetWitness Suite Live.
Contraseña del servidor web	Contraseña para autenticación del servidor web de EM. **Nota:** Esta información se proporciona durante la configuración del feed de NetWitness Suite Live.
Modo SSL	Se configura de manera predeterminada en No. Si es **No**, la dirección URL utiliza `http mode: http://hostname:port/archer/sa/feed` Si no ha actualizado el archivo host, consulte la sección "Actualizar el archivo host de RSA NetWitness Suite". **Nota:** Actualmente, NetWitness Suite no admite feeds recurrentes de Archer en modo SSL.

Actualizar el archivo host de RSA NetWitness Suite

1. Edite el archivo host en el servidor de NetWitness Suite en la siguiente ubicación: vi /etc/hosts
2. Ingrese lo siguiente para la dirección IP del host de UCF:

   ```
   <ucf-host-ip> <ucf-host-name>
   ```

3. Reinicie el servidor de NetWitness Suite mediante la ejecución del siguiente comando:

   ```
   service jetty restart
   ```

4. Mientras se configura el feed de NetWitness Suite Live, ingrese el nombre de host para la dirección URL en lugar de la dirección IP y el número de puerto configurados para el terminal de Enterprise Management en UCF:

   ```
   http: //<ucf-host-name> : <EM_Port>/archer/sa/feed.
   ```

5. Verifique que la conexión funcione.

Crear una tarea de feed recurrente

Para que RSA NetWitness Suite descargue los archivos de feed desde el servicio de integración de NetWitness Respond y migre los feeds a los Decoders, debe crear una tarea de feed recurrente y definir la configuración del feed.

Nota: Para RSA Archer SecOps 1.2: Para que RSA NetWitness Suite descargue los archivos de feed desde la máquina de RCF y migre los feeds a los Decoders, debe crear una tarea de feed recurrente y definir la configuración del feed. El procedimiento es similar a RSA Archer SecOps 1.3, con algunas excepciones. Consulte la documentación en la Comunidad RSA Archer Exchange para obtener detalles.

1. Seleccione **CONFIGURAR > Feeds personalizados**.
2. En la vista Feeds, haga clic en +.
3. Seleccione **Feed personalizado** y haga clic en **Siguiente**.
4. Seleccione **Recurrente**.
5. Ingrese un nombre para el feed.
6. En el campo URL, ingrese lo siguiente:

   `http://ucf_hostname/archer/sa/feed`

   donde *`http :ucf_hostname_or_ip:port`* es la dirección del sistema del servicio de integración de NetWitness Respond. Por ejemplo: `http://10.10.10.10:9090`.

   Nota: Si Respond se está ejecutando en modo SSL, se debe utilizar el nombre de host en la dirección URL.
7. Seleccione **Autenticado**.
8. En los campos **Nombre de usuario** y **Contraseña**, ingrese las credenciales de la cuenta de usuario que creó para que RSA NetWitness Suite las utilice con el fin de acceder a los archivos del sistema del servicio de integración de NetWitness Respond.
9. Defina el intervalo de periodicidad para el feed.
10. En la sección **Rango de fechas**, defina una fecha de inicio y una fecha de finalización para el feed y haga clic en **Siguiente.**
11. Seleccione cada Decoder al cual desea enviar este feed y haga clic en **Siguiente**.
12. En el campo **Tipo**, asegúrese de que la dirección IP esté seleccionada.
13. En el campo **Columna de índice**, seleccione 1.
14. En la segunda columna, establezca el valor clave para la criticidad y haga clic en **Siguiente**.
15. Revise los detalles de configuración del feed y haga clic en **Finalizar**.

Administrar Unified Collector Framework

En esta sección se proporcionan tareas adicionales para configurar y administrar el RSA Unified Collector Framework (UCF) para la integración de Archer SecOps 1.3.1.2.

Iniciar el RSA Unified Collector Framework

1. Haga clic en **Panel de control > Herramientas administrativas > Servicios**.
2. Seleccione RSA Unified Collector Framework.
3. Haga clic en **Iniciar**.

Detener el RSA Unified Collector Framework

1. Haga clic en **Panel de control > Herramientas administrativas > Servicios**.
2. Detenga el servicio de vigilancia de RSA SecOps.

   Nota: Si no detiene el servicio de vigilancia, este inicia el servicio NetWitness Respond antes de lo previsto.
3. Seleccione RSA Unified Collector Framework.
4. Haga clic en **Detener**.

Nota: Si el servicio tarda demasiado en apagarse, utilice el Administrador de tareas para finalizar RSASAIMDCService.

Desinstalar el RSA Unified Collector Framework

1. Haga clic en **Panel de control**> **Programas y funciones**.
2. Seleccione **RSA Unified Collector Framework**.
3. Haga clic en **Desinstalar**.

Solucionar problemas de integración de RSA Archer

En esta sección se proporcionan soluciones a problemas comunes que pueden surgir durante la configuración de Archer SecOps 1.3.1.2 con NetWitness Suite Respond.

Configuración del almacén de confianza de CA

Problema: Después de agregar el terminal para NetWitness Suite Respond, el almacén de confianza de CA no se puede configurar.

Solución:

1. Asegúrese de que las credenciales del protocolo SSH para el host de NetWitness Suite sean válidas.
2. Si las credenciales están correctas, pero el error persiste, copie manualmente los certificados.

Tareas de corrección en RSA Archer Security Operations Manager

Problema: Las tareas de corrección que se migran a la línea de espera de operaciones a través del UCF no aparecen en RSA Archer Security Operations Management como observaciones.

Solución:

1. Abra el administrador de conexión:
   - Abra una línea de comandos
   - `Cambie de directorio a <install_dir>\SA IM integration service\data-collector.`
   - `Escriba: runConnectionManager.bat`
2. Ingrese 2 para editar el terminal.
3. Ingrese 3 para NetWitness Suite Respond.
4. Asegúrese de que la línea de espera objetivo esté configurada en Todo o en Operaciones.

Errores entre RSA NetWitness Suite y RSA Unified Collector Framework

Problema: En `<install_dir>\SA IM integration service\logs\collector.log`, hay errores de SSL entre RSA NetWitness Suite y RSA Unified Collector Framework.

Solución:

1. Verifique que los certificados de SSL sean válidos.

   Nota: Los certificados de NetWitness Suite Respond tienen una validez de dos años.

2. Si sus certificados están vencidos, vuelva a generarlos y copie los certificados vencidos.

Para volver a generar y copiar los certificados, realice lo siguiente:

1. En el símbolo del sistema, vaya a `<install_dir>\SA IM integration service\data-collector`.
2. Escriba: `runConnectionManager.bat`
3. Ingrese el número correspondiente a Regenerar el certificado del servicio de integración de SA IM.
4. En el terminal de NetWitness Suite Respond, en el administrador de conexión, ingrese el número correspondiente a Editar terminal.
5. Ingrese Sí para copiar automáticamente los certificados en el almacén de confianza de NetWitness Suite.

Nota: Si los certificados no se copian, cópielos manualmente.