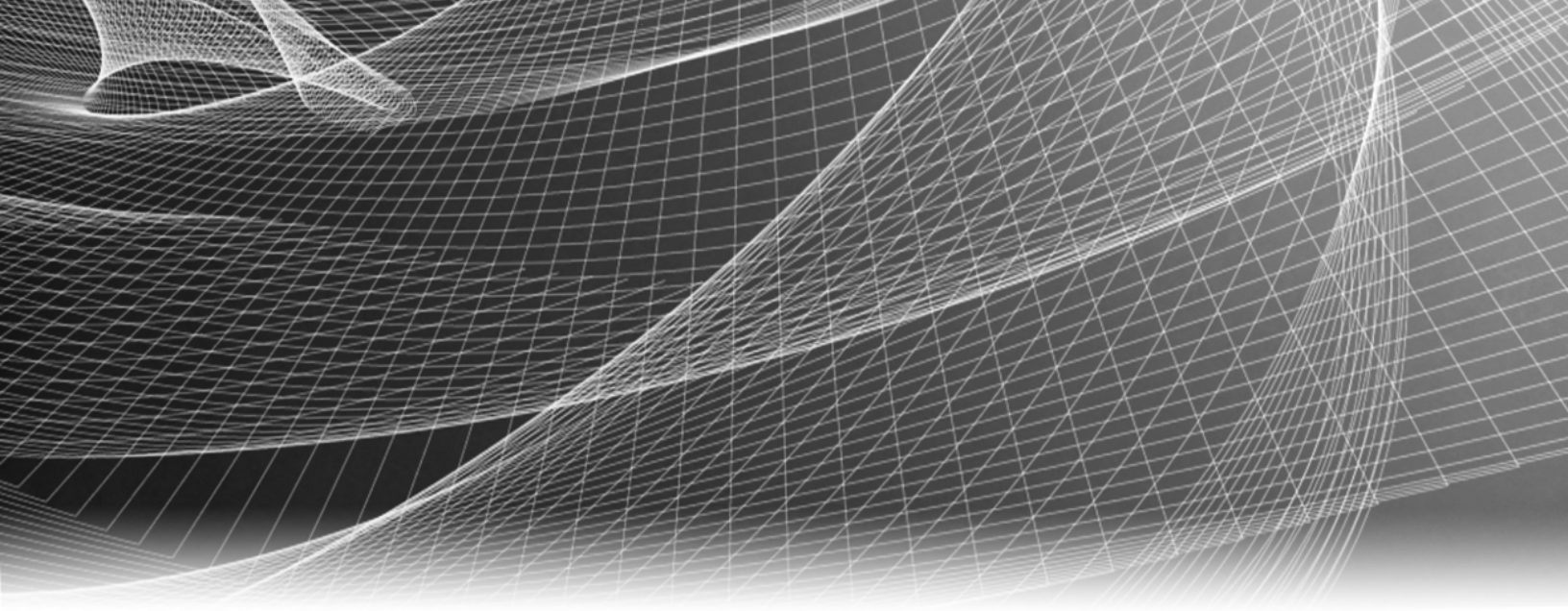


RSA Security Analytics

Guía de instalación de Event Stream Analysis serie 4

RSA

EMC²

Trademarks

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Guía de instalación de Event Stream Analysis serie 4

RSA

Guía de instalación de Event Stream Analysis serie 4

Descripción general

Este documento es una guía paso a paso para instalar el dispositivo Event Stream Analysis (ESA) de RSA Security Analytics y conectarlo a la red.

Contexto

Las instrucciones de instalación del hardware que se presentan en este documento se aplican solo al hardware y no a una versión específica del software de Security Analytics. Después de completar la instalación del hardware, continúe con la instalación y la configuración del dispositivo ESA como se describe en la documentación en línea de Security Analytics, a la cual se accede a través de la opción **Ayuda** de Security Analytics y en sadocs.emc.com/es-mx.

Last Modified: September 15 2016, 11:33AM

RSA

Descripción del hardware de SA Event Stream Analysis (ESA)

Descripción general

En este tema se presenta el dispositivo Event Stream Analysis serie 4 de RSA y se proporciona una descripción de los controles y los conectores, además de las especificaciones seleccionadas.

Introducción

Event Stream Analysis serie 4 de RSA incluye el software Event Stream Analysis instalado. La configuración inicial de Event Stream Analysis en la red implica los siguientes pasos:

1. Revisar los requisitos del sitio y la información de seguridad.
2. Montar el hardware de Event Stream Analysis.
3. Conectar Event Stream Analysis a la red y configurar parámetros de red en Event Stream Analysis.
4. Completar la instalación de Event Stream Analysis en Security Analytics.

Hay varias opciones para la conexión física inicial de Event Stream Analysis que dan paso a la configuración de los parámetros de software. Una vez establecida la conexión, la consola del dispositivo de Security Analytics se usa para realizar esos cambios en la configuración. Cada paso se describe detalladamente en este documento.

Puede obtener información sobre Security Analytics en la documentación en línea. Para ver la documentación de Security Analytics, inicie sesión en Security Analytics y seleccione la opción **Ayuda** en el menú de Security Analytics.

Contenido del paquete

Verifique el contenido de la caja de embalaje para comprobar que haya recibido todos los elementos necesarios para instalar y configurar Event Stream Analysis.

- Dispositivo Event Stream Analysis
- Ensamblajes de correderas (2)
- Cable de alimentación (2)

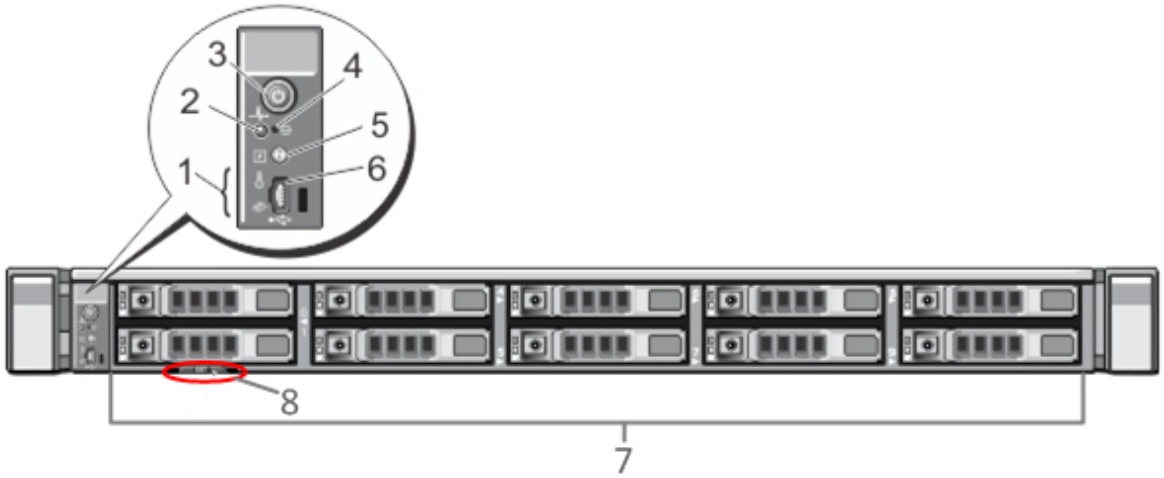
Last Modified: September 15 2016, 11:33AM

Materiales suministrados por el cliente

Para completar el procedimiento de instalación, necesitará:

- Un cable de red Ethernet
- Cables para conectar un monitor o adaptador KVM al puerto VGA y un teclado o adaptador KVM al puerto USB
- Herramientas estándar para instalar y montar el hardware de la computadora

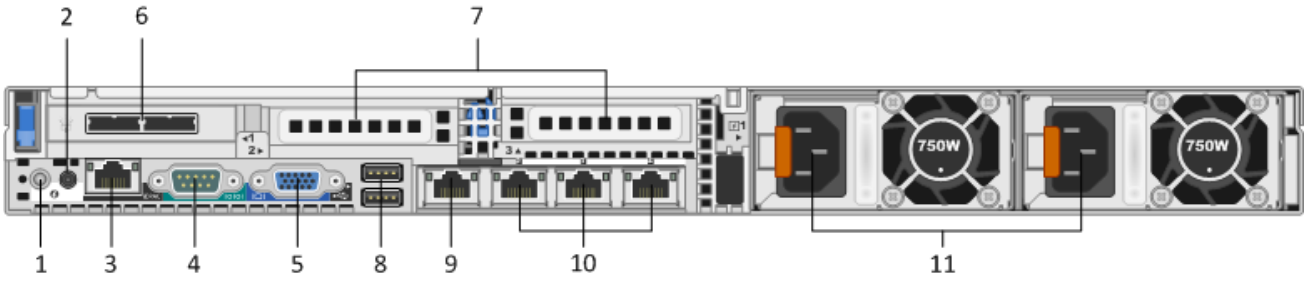
Vista frontal del dispositivo Event Stream Analysis



Clave	Descripción
1	LED de diagnóstico
2	Luz de identificación del sistema
3	Encendido/apagado
4	Botón de interrupción no enmascarable (NMI) embutido
5	Botón de identificación del sistema
6	Puerto micro-USB
7	10 bahías de disco duro de 2.5 in. Event Stream Analysis tiene diez unidades de 1 TB instaladas. También hay un módulo de tarjeta Secure Digital (SD) interno en el cual se instalan dos tarjetas de 32 GB. Es aquí donde se instala el sistema operativo de manera predeterminada.
8	Detalles de etiquetas de servicios

Last Modified: September 15 2016, 11:33AM

Vista posterior del dispositivo Event Stream Analysis



Clave	Descripción
1	Botón de identificación del sistema
2	Luz de identificación del sistema
3	Puerto iDRAC
4	Puerto en serie RS232 (conexión en serie a laptop a través de DB9 o servidor en serie)
5	Puerto de video VGA (monitor)
6	Slot de tarjetas de interfaz de red: controlador SAS instalado con dos puertos de interfaz de DAC para la conexión a los arreglos de almacenamiento en disco.
7	Slots de expansión de tarjetas de interfaz de red para tarjetas opcionales. Las opciones posibles son: • Tarjeta de captura de red de fibra/cobre de 10 Gbps (RJ45) • Tarjeta HBA Fibre Channel que se usa para la conexión a una SAN
8	Puertos USB (teclado)
9	Puerto Gigabit Ethernet 1: em1 = puerto de administración.
10	Puertos Gigabit Ethernet (del 2 al 4): em 2 al 4
11	Fuente de alimentación reemplazable en caliente 1 y 2

Especificaciones del dispositivo Event Stream Analysis

Factor de forma	1U, profundidad completa

Last Modified: September 15 2016, 11:33AM

Peso	17.69 kg (39 lb)
Dimensiones	48.23 (ancho) x 77.19 (profundidad) x 4.26 (alto) cm (18.99 x 30.39 x 1.68 in)
Se accede a las fuentes de alimentación	Reemplazable en caliente, 750 W redundantes, 100 V a 240 V con detección automática
almacenamiento	Dos de seis cores a 2.66 GHZ
RAM	96 GB

Last Modified: September 15 2016, 11:33AM

RSA

Montar el dispositivo y configurar parámetros de red

Descripción general

En este tema se proporcionan instrucciones para conectar un dispositivo Security Analytics a la red y configurar en él los parámetros de administración iniciales.

Introducción

Antes de que comience a configurar la red, monte o coloque el dispositivo con seguridad de acuerdo con los requisitos del sitio.

La configuración de parámetros de red para un dispositivo consiste en configurar la dirección IP predeterminada y el nombre de host, configurar los servidores DNS y, a continuación, el origen del reloj de red. Para configurar estos parámetros, puede conectarse a la consola del dispositivo mediante un teclado y un mouse o la conexión Ethernet. En ambos casos, inicie sesión en el dispositivo como raíz. Cuando pueda iniciar sesión en el dispositivo, use la línea de comandos del SO para modificar la configuración de administración del dispositivo y configurar los servidores DNS.

Método	Nombre de usuario	Contraseña predeterminada
consola	raíz	netwitness

Elija uno de estos métodos para la conexión inicial:

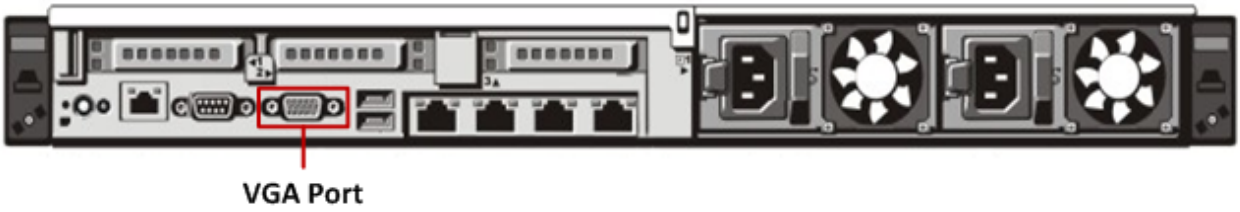
- Consola del dispositivo a través de la conexión VGA: teclado (puerto USB) y monitor (puerto VGA).
- Consola del dispositivo a través de la conexión de red: Computadora que usa un cliente del protocolo SSH conectado al dispositivo mediante un cable Ethernet al puerto de admón. (em1), el cual está configurado de manera predeterminada en 192.168.1.1.

Consola del dispositivo a través de la conexión VGA

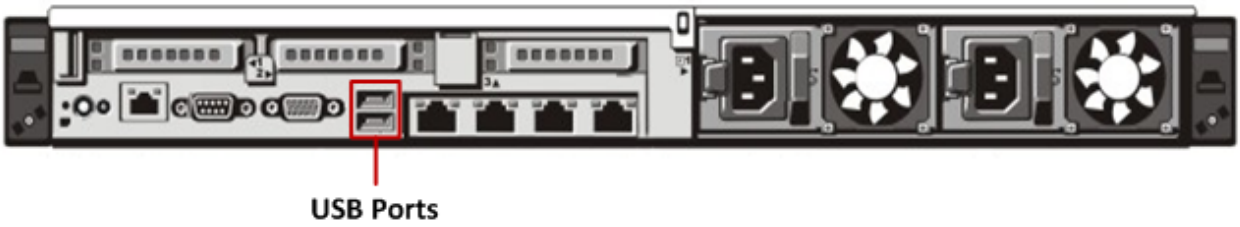
Para usar la consola del dispositivo a través de la conexión VGA:

Last Modified: September 15 2016, 11:33AM

1. Conecte un monitor o un adaptador KVM al puerto VGA de la parte posterior del dispositivo.



2. Conecte un teclado o un adaptador KVM a uno de los puertos USB de la parte posterior del dispositivo.



3. Conecte un cable de alimentación a cada una de las dos fuentes de alimentación de la parte posterior del dispositivo. Conecte los cables de alimentación a una fuente de alimentación. Para lograr una instalación más sólida, conecte cada fuente de alimentación a un circuito distinto.

> **Note:**
> La alimentación en standby de 5 V permanece activa mientras el sistema está conectado. Para cortar la alimentación del sistema, debe desconectar ambos cables de alimentación de CA de la fuente de alimentación.

4. En el indicador de inicio de sesión, use las credenciales predeterminadas para obtener acceso al sistema operativo (`root/netwitness`).
5. Continúe con la sección **Configurar la interfaz de red** más adelante.

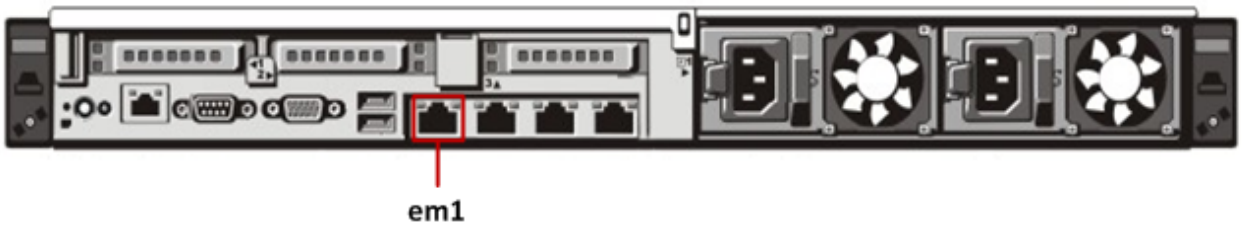
Consola del dispositivo a través de la conexión de red

> **Note:**
> la dirección IP predeterminada del dispositivo está configurada de fábrica en 192.168.1.1. El uso de 192.168.1.1 es bastante común y es posible que la dirección IP ya esté presente en el archivo known_hosts del protocolo SSH del sistema. Puede ser necesario eliminar la línea específica de esa dirección IP.

Para usar la consola del dispositivo a través de la conexión de red:

Last Modified: September 15 2016, 11:33AM

1. Conecte un cable cruzado entre una computadora y el puerto de administración Ethernet de la parte posterior del dispositivo.



2. Conecte los cables de alimentación a los conectores de alimentación del dispositivo y a un tomacorriente.
3. La dirección IP predeterminada del dispositivo está configurada de fábrica en 192.168.1.1; por lo tanto, configure la dirección IP del sistema cliente en la misma subred. Por ejemplo, configure la laptop en 192.168.1.15 con un gateway predeterminado de 192.168.1.1 y, a continuación, mediante un cliente del protocolo SSH, conéctese al dispositivo.

> **Note:**
> tenga en cuenta que si cambia los parámetros de red mientras está conectado a través del protocolo SSH, la sesión del protocolo SSH se interrumpirá y tendrá que volver a conectarse al dispositivo en su nueva dirección.

4. Acepte la clave del protocolo SSH.
5. En el indicador de inicio de sesión, use las credenciales predeterminadas para obtener acceso al sistema operativo.

Continúe con la sección *Configurar la interfaz de red* más adelante.

Configurar la interfaz de red

Use el siguiente procedimiento para configurar la dirección IP de administración en el dispositivo.

> **Note:**
> la dirección IP que configura para el dispositivo debe ser única dentro del rango de direcciones IP privadas en el ambiente de red.

Para configurar la red:

1. Inicie sesión en el dispositivo como usuario raíz.
2. Para configurar la interfaz de red em1, edite el archivo **/etc/sysconfig/network-scripts/ifcfg-em1**. Escriba el siguiente comando:
   `vi /etc/sysconfig/network-scripts/ifcfg-em1`
   Proporcione valores adecuados para los siguientes parámetros del archivo:

Parámetro	Valor
DEVICE	Tipo de interfaz de red. Por ejemplo, em1.
BOOTPROTO	static
IPADDR	Dirección IP de la interfaz de red

Last Modified: September 15 2016, 11:33AM

Parámetro	Valor
NETMASK	Dirección de la máscara de subred
GATEWAY	La dirección del gateway predeterminado.
HWADDR	Dirección MAC del dispositivo
ONBOOT	yes
TYPE	Tipo de red

3. Para reiniciar el servicio de red, escriba el siguiente comando:
   `service network restart`

Configurar el nombre de host

La creación del nombre de host del sistema es una tarea relativamente simple, pero prestarle atención puede ayudar a limitar problemas comunes. Si busca orientación para elegir un nombre de host, consulte la RFC 1178. En lo que concierne a Security Analytics, las bases de datos en los dispositivos están asociadas al nombre de host. Si la recopilación o la agregación se iniciaron (esta es la razón por la cual no están activadas de manera predeterminada), se crea la base de datos, y el cambio del nombre de host después de esto crea una segunda base de datos. El nombre de host solo debe contener caracteres alfanuméricos (no caracteres especiales como #, _, @ y -) para eliminar los problemas de comunicación.

Note: asegúrese de no modificar los detalles de loopback de IPv4 o IPv6.

Para configurar el nombre de host:

1. Inicie sesión en el dispositivo como usuario raíz.
2. Para configurar el nombre de host del dispositivo, edite el archivo **/etc/sysconfig/network**. Escriba el siguiente comando:
   `vi /etc/sysconfig/network`
3. Agregue/modifique la configuración de la siguiente manera:
   `NETWORKING=yes`
   `HOSTNAME=myserver.example.com`
4. Guarde los cambios y salga del editor vi. Escriba el siguiente comando:
   `:wq`
5. Reinicie la red mediante el siguiente comando:
   `service network restart`
6. Verifique si el nombre de host se configuró correctamente. Escriba el siguiente comando:
   `nombre de host`
   Se muestra el nombre de host que configuró.

Configurar servidores DNS

Para configurar servidores DNS:

1. Inicie sesión en el dispositivo como usuario raíz.
2. Escriba el siguiente comando:
   vi /etc/resolv.conf
3. Agregue las siguientes líneas al archivo para cada servidor DNS:
   nameserver <DNS_server_ip_address>
   search <domain_name>
   donde <DNS_server_ip_address> es la dirección IP de su servidor DNS, y <domain_name> es el nombre del dominio.
   Por ejemplo:
   nameserver 192.168.0.1
   search acmecorp.com
4. Guarde los cambios y salga del editor vi. Escriba el siguiente comando:
   :wq

Configurar el archivo /etc/hosts

Edite el archivo hosts del dispositivo e incluya la dirección IP y el nombre de host de la computadora de ESA.

> ⚠ **Caution:** el nombre de host de la computadora de ESA no debe aparecer como parte de la configuración de la dirección de loopback.

Para configurar el archivo **/etc/hosts**:

1. Inicie sesión en el dispositivo como usuario raíz.
2. Escriba el siguiente comando:
   vi/etc/hosts
3. Agregue las siguientes líneas al archivo:
   <node_private_ip_address> <node_fqdn> <node_hostname>
   Donde:
   - <node_private_ip_address> es la interfaz privada de la computadora de ESA.
   - <node_fqdn> es el nombre de dominio calificado de la computadora de ESA.
   - <node_hostname> es el nombre de host de la computadora de ESA.

El siguiente es un ejemplo del archivo **/etc/hosts** que incluye detalles de la computadora de ESA:

```
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
192.168.1.10 esabox.domainname.com esabox
```

4. Guarde los cambios y salga del editor vi. Escriba el siguiente comando:
   :wq

Especificar al origen del reloj de red

Se recomienda sincronizar todos los sistemas del conjunto de aplicaciones Security Analytics mediante un origen de tiempo de red, de modo que todos los dispositivos muestren exactamente la misma hora. Si esto no se realiza, la hora en los dispositivos puede perder la sincronización, lo cual hace que las consultas para una hora específica no devuelvan los resultados previstos.

Debe actualizar manualmente la configuración de NTP que se proporciona en el archivo **/etc/ntp.conf** del dispositivo SAW.

Para actualizar la configuración de NTP:

1. Inicie sesión en el dispositivo como usuario raíz.
2. Para editar el archivo **/etc/ntp.conf**, escriba el siguiente comando:
   ```
   vi /etc/ntp.conf
   ```
3. Desplácese hasta las líneas del servidor que contienen los sitios NTP y actualice los servidores enumerados para reflejar los sitios NTP apropiados.
   Ejemplo:
   Detalles del servidor proporcionados como nombre de dominio calificado:
   ```
   server 0.centos.pool.ntp.org
   ```
   Los detalles del servidor anteriores también se pueden proporcionar si se usa la dirección IP de la siguiente manera:
   ```
   server 91.121.92.90
   ```
4. Guarde los cambios y salga del editor vi. Escriba el siguiente comando:
   ```
   :wq
   ```
5. Reinicie el servicio ntpd mediante el siguiente comando:
   ```
   service ntpd restart
   ```


Last Modified: September 15 2016, 11:33AM

RSA

Completar la configuración de Event Stream Analysis (ESA) en Security Analytics

Descripción general

En este tema se proporcionan instrucciones para completar la configuración de Event Stream Analysis y dar inicio a la agregación en Security Analytics.

Introducción

Los pasos finales para configurar el dispositivo Event Stream Analysis se realizan mediante Security Analytics. Son los siguientes:

1. Agregar Event Stream Analysis a Security Analytics en la vista Dispositivos.
2. Aplicar una licencia (o autorización) de dispositivo a Event Stream Analysis.
3. Agregar uno o más Concentrators a Event Stream Analysis como dispositivos agregados.
4. Configurar e iniciar la agregación.

Varios de estos pasos solo se pueden completar cuando otras partes de la red de Security Analytics están establecidas:

- Se debe instalar y configurar por lo menos un servicio Concentrator, se debe obtener licencia para él y el servicio debe capturar datos para generar los metadatos que Event Stream Analysis puede recuperar.
- Las licencias (o autorizaciones) del dispositivo de Security Analytics deben estar disponibles para habilitar los dispositivos.

Inicie sesión en Security Analytics y siga las instrucciones de la ayuda en línea para completar la instalación de Event Stream Analysis como parte del conjunto de aplicaciones Security Analytics.

Last Modified: September 15 2016, 11:33AM