



RSA Security Analytics

Guía de instalación de los
dispositivos Security Analytics
serie 5

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

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 los dispositivos Security Analytics serie 5

- [Guía de instalación de los dispositivos Security Analytics serie 5](#) 4
- [Descripción del hardware de los dispositivos R630 serie 5](#) 5
- [Instalar un adaptador de rack profundo para un dispositivo R630](#) 11
- [Descripción del hardware del dispositivo Hybrid R730xd serie 5](#) 14
- [Instalar un adaptador de rack profundo para un dispositivo Hybrid R730xd](#) 19
- [Conectar el dispositivo y configurar los parámetros de red](#) 22
- [Completar la configuración del dispositivo en Security Analytics](#) 27



Guía de instalación de los dispositivos Security Analytics serie 5

Descripción general

Este documento es una guía paso a paso para instalar los dispositivos RSA Security Analytics serie 5 y conectarlos 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 de los dispositivos Security Analytics como se describe en la documentación en línea de Security Analytics en sadoes.emc.com/es-mx.

Este documento no reemplaza la documentación del fabricante original; contiene información que corresponde específicamente a los dispositivos Security Analytics.



Descripción del hardware de los dispositivos R630 serie 5

Introducción

Todos los dispositivos RSA Security Analytics serie 5, menos uno, se basan en el chasis Dell PowerEdge R630. La excepción es el dispositivo Hybrid, el cual se basa en el chasis Dell PowerEdge R730xd. Los dispositivos serie 5 incluyen el software Security Analytics 10.5 instalado.

En este tema se describen los dispositivos serie 5 que se basan en el chasis Dell PowerEdge R630:

- Decoder y Log Decoder
- Concentrator
- Intermediador
- Archiver
- Máquinas Security Analytics
- Malware Analysis
- Event Stream Analysis (ESA)

Excepto por el dispositivo ESA, todos los dispositivos basados en Dell PowerEdge R630 tienen los mismos componentes y especificaciones físicas. El dispositivo ESA tiene discos duros y memoria adicionales, y otro CPU. En [Especificaciones del dispositivo Security Analytics ESA](#) se proporcionan detalles.

La configuración inicial de un dispositivo serie 5 en la red implica los siguientes pasos:

1. Revisar los requisitos del sitio y la información de seguridad en la *Guía de implementación* de la versión del software Security Analytics correspondiente: [Security Analytics 10.5](#).
2. Montar o colocar el hardware del dispositivo de forma segura de acuerdo con los requisitos del sitio.
3. Conectar el dispositivo a la red y configurar parámetros de red en el dispositivo: [Conectar el dispositivo y Configurar los parámetros de red](#).
4. Completar la instalación del dispositivo en Security Analytics: [Completar la configuración del dispositivo en Security Analytics](#).

⚠ Caution: Para evitar dañar los servidores y los dispositivos de Security Analytics, extráigalos del rack y desmóntelo antes de transportarlo a otra ubicación. Siga las recomendaciones del fabricante del servidor y del fabricante del rack en términos del embalaje, el transporte y la instalación. RSA no admite el reenvío de servidores en rack. El cliente asume todo el riesgo y la responsabilidad del transporte de los servidores y los dispositivos de Security Analytics montados en un rack.

Contenido del paquete

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

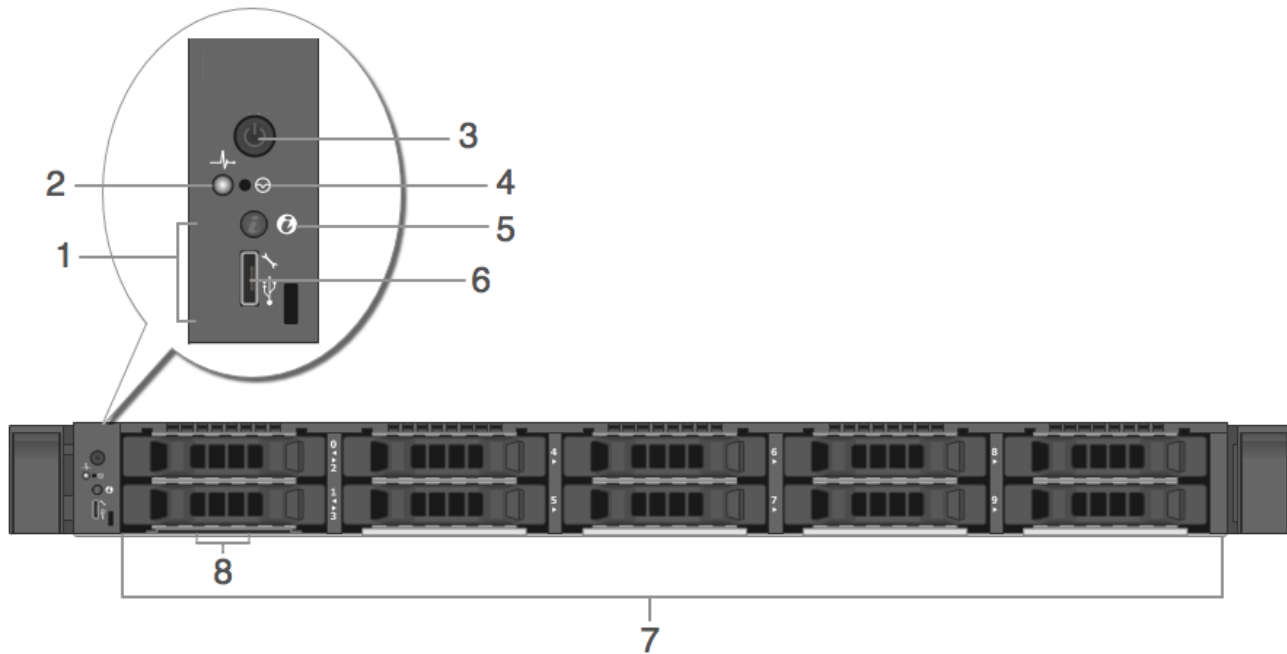
- Dispositivo Security Analytics serie 5 (Decoder, Concentrator, Broker, Archiver, Security Analytics Server, Malware Analysis o ESA)
- Riel fijo ReadyRails (un conjunto)
- Adaptador de riel izquierdo para rack profundo de EMC
- Bisel de RSA (1): las llaves vienen pegadas con cinta al bisel.
- Cable de alimentación (2)
- Manual Dell Product Information Guide (1)
- Carpeta de documentación de RSA (1)
- EULA de RSA (1)

Materiales suministrados por el cliente

Para completar el procedimiento de instalación, necesitará:

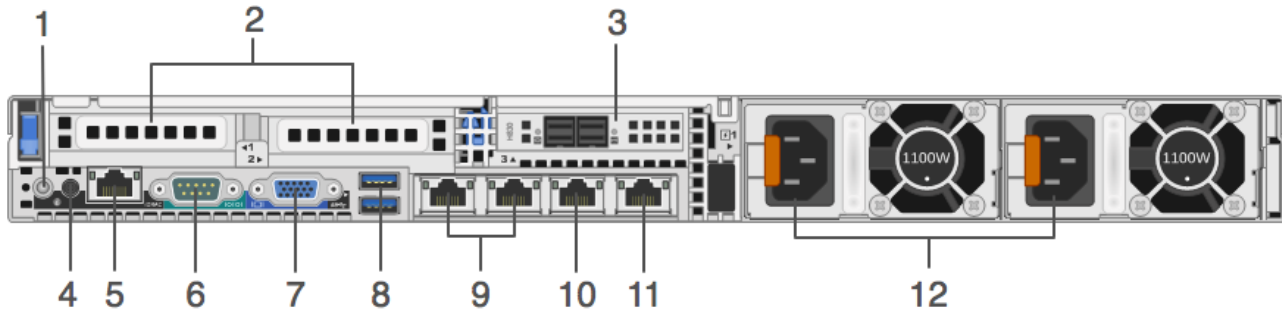
- Un cable de red Ethernet
- Cables para conectar un monitor o adaptador KVM al puerto VGA y un teclado o adaptador KVM al puerto USB
- Herramientas estándares

Vista frontal de los dispositivos serie 5 (excepto Hybrid)



Clave	Descripción
1	Ubicación del indicador de diagnóstico. Los indicadores de diagnóstico aparecen y muestran el estado en caso de error.
2	Indicador de estado del sistema. Parpadea de color ámbar cuando se detecta una falla del sistema.
3	Encendido/apagado
4	Botón de interrupción no enmascarable (NMI) embutido
5	Botón de identificación del sistema
6	Puerto micro-USB/iDRAC Direct
7	10 bahías de disco duro de 2.5 in (de reemplazo en sitio). Las especificaciones que aparecen a continuación identifican la cantidad y los tipos de discos duros instalados en los dispositivos.
8	Ubicación de la etiqueta de información

Vista posterior de los dispositivos serie 5 (excepto Hybrid)



Clave	Descripción
1	Botón de identificación del sistema
2	Slots de expansión LP PCIe 1 y 2. Decoder 10G puede usar un slot LP PCIe para una tarjeta de interfaz de red óptica Intel X520 opcional.
3	Controlador RAID PERC H830. Se muestra en el slot LP PCIe 3, pero se puede instalar en otro slot LP PCIe. PERC H830 es el controlador RAID para la DAC de expansión del almacenamiento. Se requiere un cable con un puerto mini-SAS para la conexión a la DAC.
4	Conector de identificación del sistema
5	Puerto iDRAC
6	Puerto en serie RS232 (conexión en serie a laptop a través de DB9 o servidor en serie)
7	Puerto de video VGA (monitor)
8	Puertos USB (teclado, mouse, memoria USB, etc.)
9	Puertos Ethernet 10GBASE-T em3 y em4
10	Puerto de administración 1000BASE-T de la red principal: em1
11	Puerto 1000BASE-T de la red secundaria: em2
12	Fuente de alimentación reemplazable en caliente 1 y 2 (de reemplazo en sitio)

Note: El controlador RAID PERC H830 requiere un cable con un puerto mini-SAS para la conexión a la DAC.

Especificaciones del dispositivo serie 5 (excepto Hybrid y ESA)

Elemento	Descripción
Factor de forma	1U, profundidad completa
Peso (aproximado)	18.4 kg (40.5 lb)
Dimensiones (aproximadas)	Con bisel: 482.43 mm (18.99 in) [ancho] x 808.59 mm (31.83 in) [profundidad] x 42.80 mm (1.69 in) [alto] Sin bisel: 482.43 mm (18.99 in) [ancho] x 776.16 mm (30.56 in) [profundidad] x 42.80 mm (1.69 in) [alto]
Se accede a las fuentes de alimentación	Fuente de alimentación redundante doble de conexión en caliente (1+1), 1100 W
almacenamiento	Dos E5-2667v3
RAM	16 RDIMM de 8 GB y 2133 MT/s (128 GB)
Discos duros (de reemplazo en sitio)	Dos discos duros de conexión en caliente SAS NL de 1 TB, 7,200 r/min, 6 Gbps y 2.5 in Dos discos duros de conexión en caliente SAS NL 512e de 2 TB, 7,200 r/min, 12 Gbps y 2.5 in
Controlador RAID	Externo: RAID PERC H830 Interno: PERC H730P
Tarjeta de interfaz de red	Intel Ethernet X540 de 10 Gb BT DP + Tarjeta secundaria de red I350 de 1 Gb BT DP

Especificaciones del dispositivo Security Analytics ESA

Elemento	Descripción
Factor de forma	1U, profundidad completa
Peso (aproximado)	18.4 kg (40.5 lb)
Dimensiones (aproximadas)	Con bisel: 482.43 mm (18.99 in) [ancho] x 808.59 mm (31.83 in) [profundidad] x 42.80 mm (1.69 in) [alto] Sin bisel: 482.43 mm (18.99 in) [ancho] x 776.16 mm (30.56 in) [profundidad] x 42.80 mm (1.69 in) [alto]
Se accede a las fuentes de alimentación	Fuente de alimentación redundante doble de conexión en caliente (1+1), 1100 W
almacenamiento	Dos E5-2680v3

Elemento	Descripción
RAM	Ocho RDIMM de 32 GB y 2133 MT/s (256 GB)
Discos duros (de reemplazo en sitio)	Dos discos duros de conexión en caliente SAS NL de 1 TB, 7,200 r/min, 6 Gbps y 2.5 in Cuatro discos duros de conexión en caliente SAS NL 512e de 2 TB, 7,200 r/min, 12 Gbps y 2.5 in
Controlador RAID	Externo: RAID PERC H830 Interno: PERC H730P
Tarjeta de interfaz de red	Intel Ethernet X540 de 10 Gb BT DP + Tarjeta secundaria de red I350 de 1 Gb BT DP

⚠ Caution: La apertura del chasis del dispositivo anulará la garantía, a menos que la Atención al cliente de RSA se lo haya indicado específicamente. Un técnico calificado puede reemplazar en sitio los discos duros y las fuentes de alimentación.



Instalar un adaptador de rack profundo para un dispositivo R630

Procedimiento

Note: Este procedimiento solo se aplica si está instalando el dispositivo R630 serie 5 en el rack EMC Titan D Ultra.

Cuando se instala el dispositivo R630 serie 5 en el rack EMC Titan D Ultra, se requiere un adaptador de rack profundo de 1U. Siga este procedimiento para instalar un nuevo soporte en los rieles del servidor.

1. Busque el soporte de riel alternativo en la caja de accesorios del empaque del dispositivo R630.



2. Quite el riel del lado izquierdo del empaque del riel.



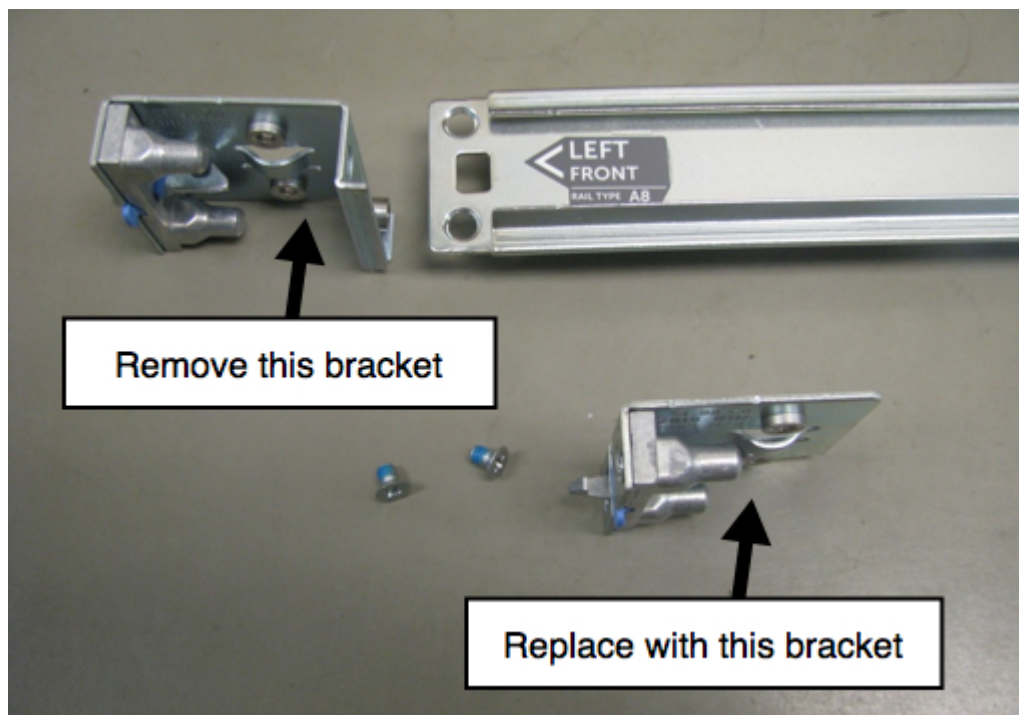
Cada riel está marcado.



3. Utilice un destornillador Phillips para quitar los dos tornillos de montaje.



4. Extraiga el soporte y reemplácelo por el nuevo.



5. Vuelva a usar los tornillos para sujetar el nuevo soporte en su posición.



El riel ahora está listo para la instalación del dispositivo R630.



Descripción del hardware del dispositivo Hybrid R730xd serie 5

Introducción

El dispositivo Hybrid serie 5 de RSA Security Analytics se basa en el chasis Dell PowerEdge R730xd. El dispositivo Hybrid serie 5 de RSA Security Analytics incluye el software del dispositivo Hybrid de Security Analytics 10.5 instalado. El software del dispositivo Hybrid incluye Concentrator y Decoder (Log o Packet, no ambos).

La configuración inicial de un dispositivo serie 5 en la red implica los siguientes pasos:

1. Revisar los requisitos del sitio y la información de seguridad en la *Guía de implementación* de la versión del software Security Analytics correspondiente: [Security Analytics 10.5](#).
2. Montar o colocar el hardware del dispositivo de forma segura de acuerdo con los requisitos del sitio.
3. Conectar el dispositivo a la red y configurar parámetros de red en el dispositivo: [Conectar el dispositivo y Configurar los parámetros de red](#).
4. Completar la instalación del dispositivo en Security Analytics: [Completar la configuración del dispositivo en Security Analytics](#).

⚠ Caution: Para evitar dañar los servidores y los dispositivos de Security Analytics, extráigalos del rack y desmonte el rack antes de transportarlo a otra ubicación. Siga las recomendaciones del fabricante del servidor y del fabricante del rack en términos del embalaje, el transporte y la instalación. RSA no admite el reenvío de servidores en rack. El cliente asume todo el riesgo y la responsabilidad del transporte de los servidores y los dispositivos de Security Analytics montados en un rack.

Contenido del paquete

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

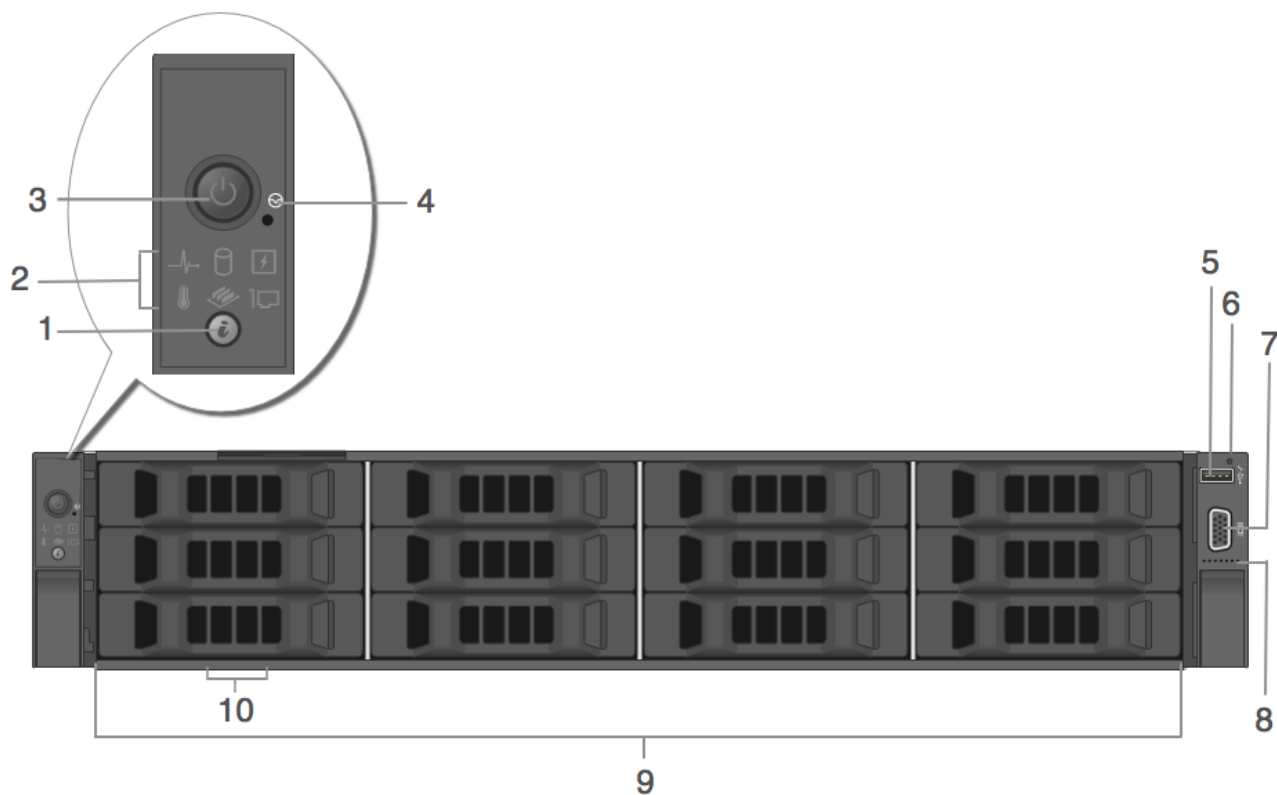
- Dispositivo Hybrid serie 5
- Riel fijo ReadyRails (un conjunto)
- Adaptador de 2U de riel izquierdo para rack profundo de EMC
- Bisel de RSA de 2U (1): las llaves vienen pegadas con cinta al bisel
- Cable de alimentación (2)
- Manual Dell Product Information Guide (1)
- Carpeta de documentación de RSA (1)
- EULA de RSA (1)

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 estándares

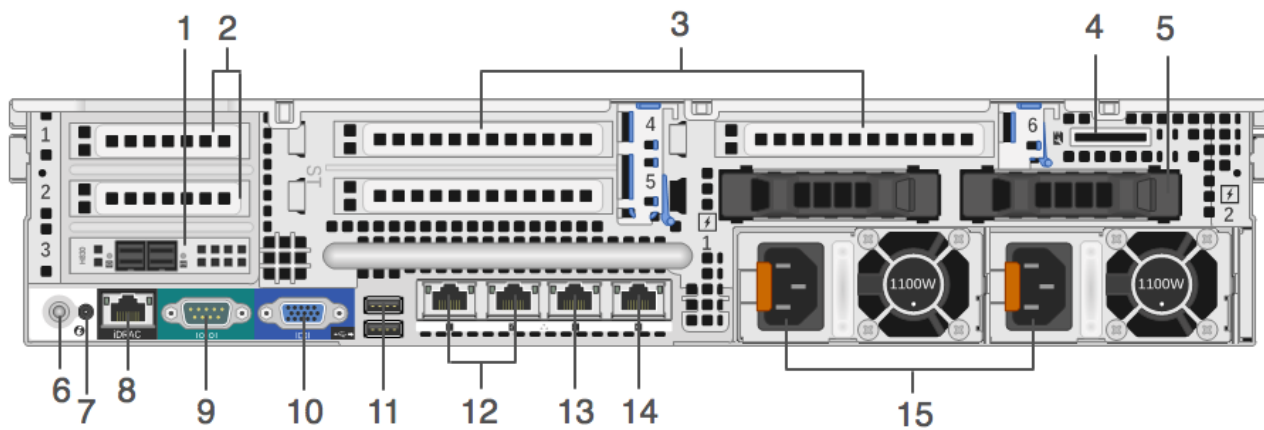
Vista frontal del dispositivo Hybrid de Security Analytics



Clave	Descripción
1	Botón de identificación del sistema
2	Indicadores de diagnóstico
3	Encendido/apagado
4	Botón de interrupción no enmascarable (NMI) embutido
5	Puerto de administración USB/iDRAC Direct

Clave	Descripción
6	Indicador LED de iDRAC Direct
7	Conector de video
8	Quick Sync (opcional)
9	12 discos duros de 3.5 in (de reemplazo en sitio). El dispositivo Hybrid de Security Analytics tiene un total de 14 discos. Hay 12 discos duros en la parte frontal y dos discos de estado sólido (SSD) en la parte posterior. Consulte detalles adicionales en las especificaciones del dispositivo que aparecen a continuación.
10	Ubicación de la etiqueta de información

Vista posterior del dispositivo Hybrid de Security Analytics



Clave	Descripción
1	Controlador RAID PERC H830. Se muestra en el slot de tarjeta PCIe 3 de altura media, pero se puede instalar en otro slot PCIe de altura media. PERC H830 es el controlador RAID para la DAC de expansión del almacenamiento. Se requiere un cable con un puerto mini-SAS para la conexión a la DAC.
2	Slots de tarjeta de expansión PCIe de altura media 1 y 2
3	Slots de tarjeta de expansión PCIe de altura completa (3)
4	Slot de tarjeta de medios vFlash
5	Dos discos SSD de 2.5 in (reemplazables en caliente)
6	Botón de identificación del sistema
7	Conector de identificación del sistema
8	Puerto iDRAC8 Enterprise

Clave	Descripción
9	Puerto en serie RS232 (conexión en serie a laptop a través de DB9 o servidor en serie)
10	Puerto de video VGA (monitor)
11	Puertos USB (teclado, mouse, memoria USB, etc.)
12	Puertos Gigabit Ethernet 10GBASE-T : em3-4
13	Puerto de administración 1000BASE-T de la red principal: em1
14	Puerto 1000BASE-T de la red secundaria: em2
15	Fuente de alimentación reemplazable en caliente 1 y 2 (de reemplazo en sitio)

Note: El controlador RAID PERC H830 requiere un cable con un puerto mini-SAS para la conexión a la DAC.

Especificaciones del dispositivo Hybrid de Security Analytics

Elemento	Descripción
Factor de forma	2U, profundidad completa
Peso (aproximado)	36.5 kg (80.47 lb)
Dimensiones (aproximadas)	Alto: 8.73 cm (3.44 in) x Ancho: 48.2 cm (18.98 in) x Profundidad: 75.58 cm (29.75 in)
Se accede a las fuentes de alimentación	Fuente de alimentación redundante doble de conexión en caliente (1+1), 1100 W
almacenamiento	Dos E5-2680v3
RAM	16 RDIMM de 8 GB y 2133 MT/s (128 GB)
Discos duros	El dispositivo Hybrid de Security Analytics tiene un total de 14 discos. Hay 12 discos duros en la parte frontal y dos discos de estado sólido (SSD) en la parte posterior. Dos discos SSD de 800 GB (parte posterior) Cuatro discos SAS NL de 1 TB. 7,200 r/min y 6 Gbps Ocho discos SAS NL de 6 TB. 7,200 r/min y 6 Gbps
Controlador RAID	Externo: RAID PERC H830 Interno: PERC H730P
Tarjeta de interfaz de red	Intel Ethernet X540 de 10 Gb BT DP + Tarjeta secundaria de red I350 de 1 Gb BT DP

⚠ Caution: La apertura del chasis del dispositivo anulará la garantía, a menos que la Atención al cliente de RSA se lo haya indicado específicamente. Un técnico calificado puede reemplazar en sitio los discos duros y las fuentes de alimentación.



Instalar un adaptador de rack profundo para un dispositivo Hybrid R730xd

Procedimiento

Note: Este procedimiento solo se aplica si está instalando el dispositivo Hybrid R730xd serie 5 en el rack EMC Titan D Ultra.

Cuando se instala el dispositivo Hybrid R730xd serie 5 en el rack EMC Titan D Ultra, se requiere un adaptador de rack profundo de 2U. Siga este procedimiento para instalar un nuevo soporte en los rieles del servidor.

1. Busque el soporte de riel alternativo en la caja de accesorios del empaque del dispositivo Hybrid R730xd.



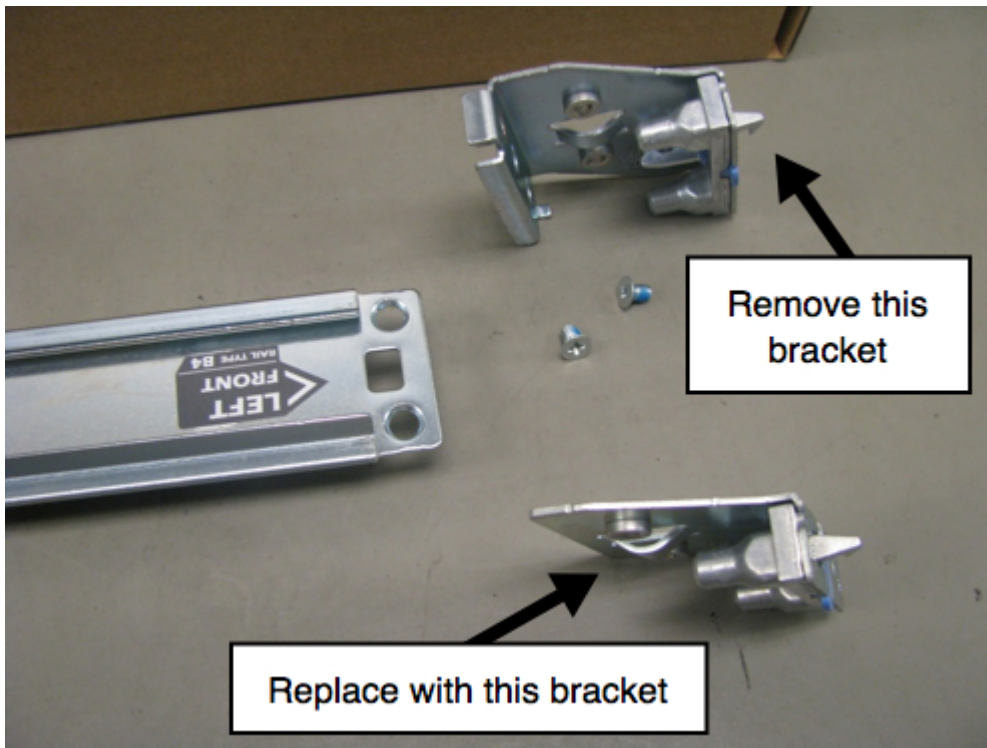
2. Quite el riel del lado izquierdo del empaque del riel. Cada riel está marcado.



3. Utilice un destornillador Phillips para quitar los dos tornillos de montaje.



4. Extraiga el soporte y reemplácelo por el nuevo.



5. Vuelva a usar los tornillos para sujetar el nuevo soporte en su posición.



El riel ahora está listo para la instalación del dispositivo Hybrid R730xd.



Conectar el dispositivo y configurar los parámetros de red

Descripción general

En este tema se proporcionan instrucciones para conectar un dispositivo Security Analytics serie 5 a la red y configurar en él los parámetros de red.

Requisitos previos

Para cada dispositivo Security Analytics serie 5, obtenga y escriba la información en la siguiente tabla.

Configuración	Opción predeterminada	Su dispositivo
Inicio de sesión	raíz	
Contraseña	netwitness	
Dirección IP del sistema	192.168.1.1	
Máscara de red del sistema	255.255.255.0	
Gateway predeterminado		
Servidor DNS principal Dirección IP		
Servidor DNS secundario IP		
Nombre de dominio local (o ninguno)		
Nombre no completo del host	NWAPPLIANCE<xxxxxx>, donde <xxxxxx> es un número aleatorio generado.	
Dirección IP del servidor de Security Analytics		

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

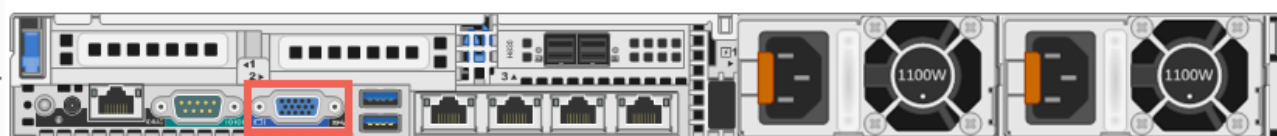
Introducción

La configuración de parámetros de red para un dispositivo RSA Security Analytics serie 5 consiste en configurar la dirección IP predeterminada, los servidores DNS, el nombre de host y el origen del reloj de red. Para configurar estos parámetros, puede conectarse a la consola del dispositivo mediante un teclado y un mouse.

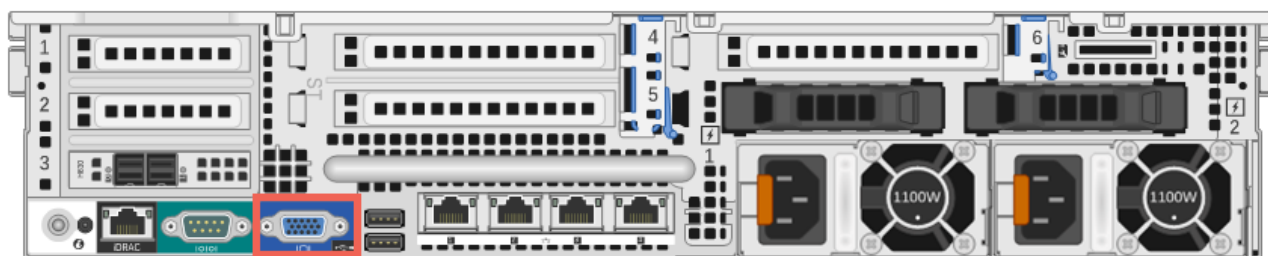
La práctica recomendada es provisionar el servidor de Security Analytics antes de configurar los otros dispositivos de Security Analytics.

Conectarse a la consola del dispositivo

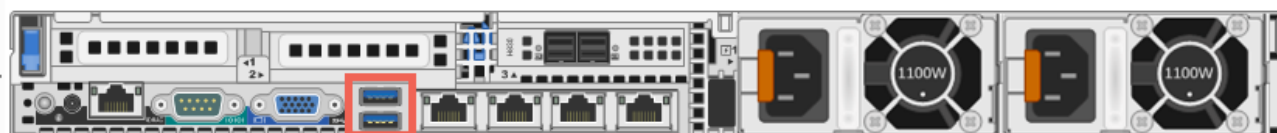
1. Conecte un monitor o un adaptador KVM al puerto VGA de la parte posterior del dispositivo.



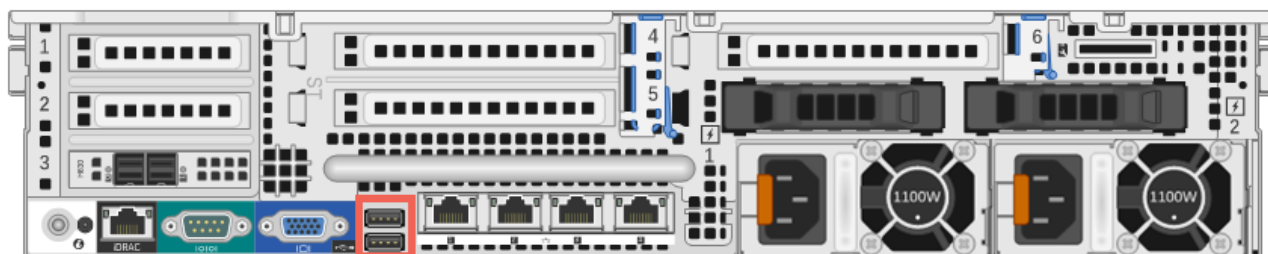
En la siguiente figura se muestra la ubicación del puerto VGA en el dispositivo Hybrid.



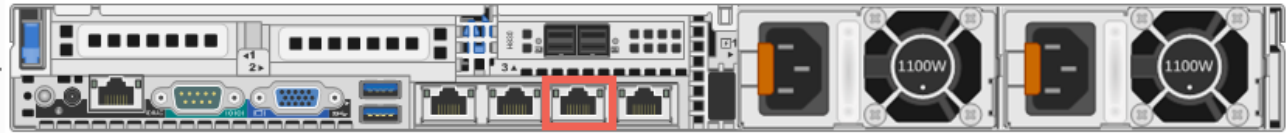
2. Conecte un teclado o un adaptador KVM a uno de los puertos USB de la parte posterior del dispositivo.



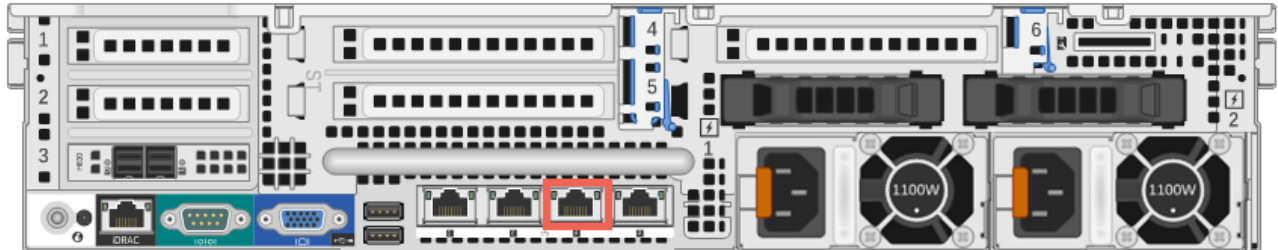
En la siguiente figura se muestra la ubicación del puerto USB en el dispositivo Hybrid.



- Conecte un cable Ethernet desde la red al puerto em1 en la parte posterior del dispositivo.



En la siguiente figura se muestra la ubicación del puerto em1 en el dispositivo Hybrid.



- 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.

⚠ Caution: 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.

- Encienda el dispositivo y continúe a la sección [Configurar los parámetros de red](#).

Configurar los parámetros de red

- En el indicador de inicio de sesión, ingrese las credenciales predeterminadas para obtener acceso al sistema operativo:


```
NWAPPLIANCE<xxxxxxx> login: root
Password: netwitness
```

Note: Si no recibe los indicadores para configurar los parámetros de red, puede ejecutar `#netconfig.sh` desde la línea de comandos, donde se le solicitará ingresar las opciones de configuración.

- Ingrese la siguiente información cuando se le solicite:
 - Dirección IP del sistema (o **d** para DHCP)
 - Máscara de red del sistema
 - Gateway predeterminado
 - Dirección IP del servidor DNS principal
 - Dirección IP del servidor DNS secundario (o presione **Intro** para no especificar ninguna)
 - Nombre de dominio local (o presione **Intro** para no especificar ninguna)
 - Nombre no completo del host

Cuando haya completado la configuración inicial, deberá ver un indicador que permite guardar la configuración, como se muestra en la siguiente figura.

```

you entered the following network parameters
IP Address: 192.168.1.20
Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
Primary DNS: 192.168.1.2
Secondary DNS: 192.168.1.3
Local Domain: SampleDomain.com
Host Name: SA-Server
-----
enter y to confirm and save
enter q to quit without saving
enter d for don't save or ask me this
enter 1 to re-enter IP address
enter 2 to re-enter netmask
enter 3 to re-enter default gateway
enter 4 to re-enter primary DNS
enter 5 to re-enter secondary DNS
enter 6 to re-enter local domain
enter 7 to re-enter host name
enter a to re-enter all network data
-----
? █

```

3. Verifique la información ingresada e ingrese **y** para guardar la configuración. Esto establece la información de red y reinicia los servicios de red.
4. Si su dispositivo no es un servidor de Security Analytics, **espere aproximadamente 15 segundos hasta que aparezca un indicador y**, a continuación, ingrese en él la dirección IP del servidor de Security Analytics.
5. Envíe el comando ping a su servidor DNS para verificar la conectividad de red.
6. Continúe con la sección [Especificar el origen del reloj de red](#).

Especificar al origen del reloj de red

es necesario configurar la sincronización de la hora entre los servicios y los dispositivos. Se recomienda enfáticamente usar un origen de tiempo NTP para la sincronización. La hora es fundamental para las comunicaciones subyacentes entre los servicios, y si los dispositivos no están sincronizados, se puede producir una falta de coincidencia en las horas que se muestran durante el análisis de datos. Si el servidor NTP no está configurado o está inaccesible en este momento, la configuración del origen del reloj de red fallará, pero se puede establecer posteriormente en la interfaz de Security Analytics.

Mejores prácticas

RSA recomienda las siguientes mejores prácticas:

Para una mejor integridad de los datos, configure el servidor de Security Analytics como el origen del reloj para los demás dispositivos. Todos los dispositivos, incluido Event Stream Analysis (ESA), obtienen su hora del servidor de Security Analytics. Solo el servidor de Security Analytics está configurado en un origen de hora NTP externo.

Para el dispositivo del servidor de Security Analytics, use la utilidad NwConsole con el fin de conectarse al origen de hora NTP.

Si en los otros dispositivos está instalado Security Analytics 10.5.1 o superior, la hora se establece automáticamente en todos los dispositivos conectados al dispositivo del servidor de Security Analytics. Si Security Analytics 10.5.1 o superior no está instalado en los otros dispositivos, configure la hora manualmente de modo que señale al servidor de Security Analytics.

Establecer la hora en el servidor de Security Analytics mediante la utilidad NwConsole

Para configurar el origen del reloj de red en el servidor de Security Analytics mediante la utilidad NwConsole:

- En el indicador de la raíz [`root@NwAppliance~`]# escriba el siguiente comando:
`NwConsole`
 NwConsole se inicia y se muestra un mensaje que indica una versión y una fecha:
`RSA Security Analytics Console`
- En NwConsole, escriba el siguiente comando:
`login localhost:50006 <username> <password>`
 El nombre de usuario de la cuenta de administrador del sistema para Security Analytics es **admin** y la contraseña predeterminada es **netwitness**.
 Se inicia la sesión en el dispositivo y se muestra el siguiente mensaje:
`Successfully logged in as session <session #>`
- En el indicador del host local [`localhost:50006`] /> realice una de las siguientes acciones:
 - Si desea usar su origen del reloj de red, escriba el siguiente comando:
`appliance setNTP source=<NTP_server_hostname or IP_address>`
 Por ejemplo: `appliance setNTP source=0.pool.ntp.org`
 - Si desea usar el reloj del dispositivo como un origen del reloj, escriba: `appliance setNTP source=local`
- Cuando la salida del comando se muestre como `Success`, escriba `exit` para cerrar la sesión y salir del programa NwConsole.

Note: Si especificó un origen del reloj NTP local, el reloj del dispositivo actúa como origen del reloj y la hora se configura mediante el uso de Definir reloj integrado de dispositivo, como se describe en la ayuda en línea de Security Analytics.



Completar la configuración del dispositivo en Security Analytics

Introducción

Para completar la configuración de un dispositivo serie 5, debe iniciar sesión en Security Analytics y utilizar las opciones de configuración disponibles en el módulo Security Analytics Administration. Los pasos de configuración de cada tipo de dispositivo varían levemente. En esta sección se proporciona información básica y vínculos a documentos de ayuda en línea que lo guiarán en el proceso.

Inicie sesión en Security Analytics.

RSA Security Analytics es una aplicación web que se inicia en una ventana del navegador. Entre los navegadores compatibles se incluye cualquier navegador que sea compatible con WebSockets, LocalStorage y la API HTML5 History: Google Chrome, Apple Safari, Mozilla Firefox e Internet Explorer 10 y superiores.

1. En el navegador web, escriba lo siguiente:
`https://<hostname or IP address>/login`
Donde `<hostname or IP address>` es el nombre de host o la dirección IP del servidor de Security Analytics.

Aparece la pantalla de inicio de sesión de Security Analytics.



2. Escriba el nombre de usuario y la contraseña, y haga clic en **Inicio de sesión**.
El nombre de usuario de la cuenta de administrador del sistema para Security Analytics es **admin** y la contraseña predeterminada es **netwitness**.

Abrir la ayuda en línea

Las instrucciones para configurar dispositivos individuales se proporcionan en función de la versión del software instalada en el dispositivo.

Para Security Analytics 10.5, lea estos documentos: [Guías de configuración de hosts y servicios](#) y [Guía de licencia](#). La *Guía de introducción de hosts y servicios* es un buen punto de partida para comprender el proceso de configuración general y comenzar con la configuración.