



RSA Security Analytics

Guía de instalación de RSA
Analytics Warehouse serie 4
(basado en MapR)

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 RSA Analytics Warehouse serie 4 (basado en MapR)

- [Guía de instalación de RSA Analytics Warehouse serie 4 \(basado en MapR\)](#) 4
 - [Descripción del hardware de Warehouse serie 4](#) 5
 - [Montar el dispositivo y configurar parámetros de red](#) 9
 - [Completar la configuración de Warehouse en Security Analytics](#) 15



Guía de instalación de RSA Analytics Warehouse serie 4 (basado en MapR)

Descripción general

Este documento es una guía paso a paso para instalar RSA Analytics Warehouse (MapR) y conectarlo a la red. A Warehouse se le conocía como Security Analytics Warehouse (SAW).

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 Warehouse 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 sadoes.emc.com/es-mx.

Note: cuando consulte una guía impresa, tenga en cuenta que una versión más reciente puede estar disponible en línea en sadoes.emc.com/es-mx. Esta guía está disponible en la ayuda en línea de Security Analytics bajo Guías de instalación del hardware.



Descripción del hardware de Warehouse serie 4

Descripción general

En este tema se presenta Warehouse serie 4 de RSA y se proporciona una descripción de los controles y los conectores, además de las especificaciones seleccionadas.

Introducción

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

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

Hay varias opciones para la conexión física inicial de Warehouse 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.

Contenido del paquete

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

- Dispositivo Warehouse serie 4
- Ensamblajes de correderas (2)
- Cable de alimentación (2)

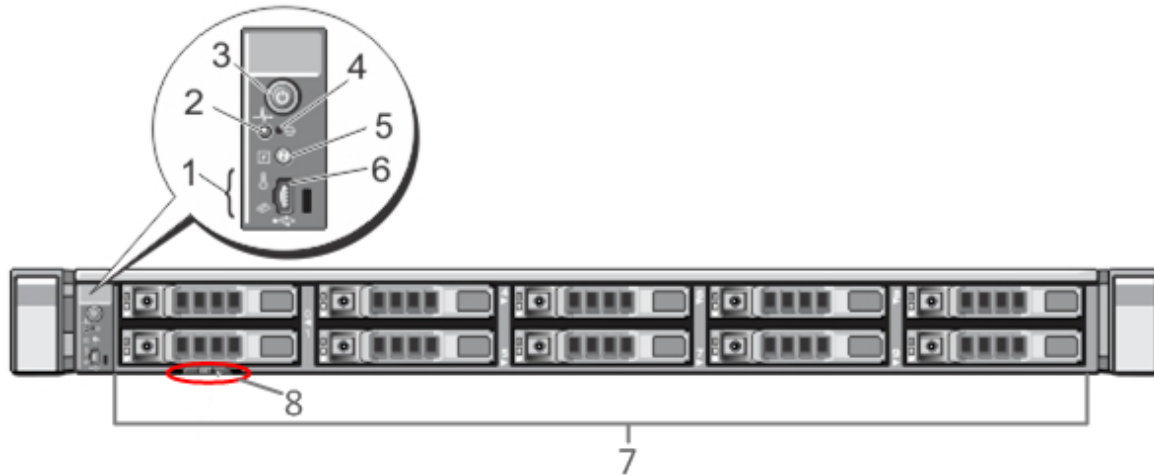
Materiales suministrados por el cliente

Para completar el procedimiento de instalación, necesitará:

- Dos cables de red Ethernet
- Cables para conectar un monitor o adaptador KVM al puerto VGA y un teclado o adaptador KVM al puerto USB

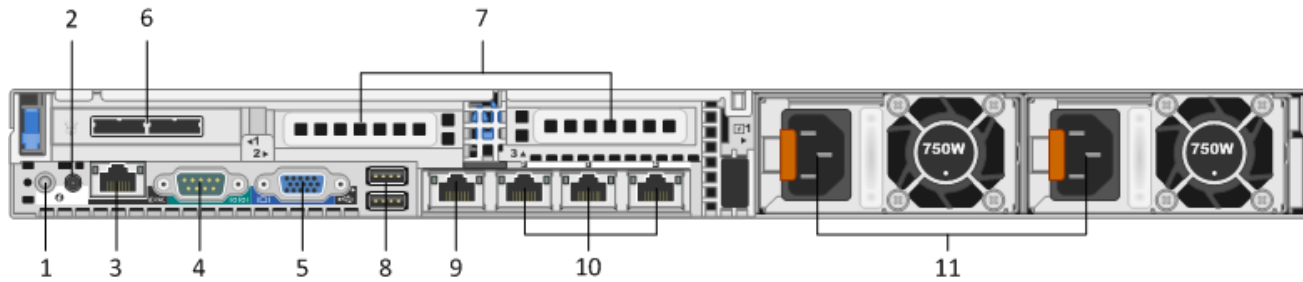
- Herramientas estándar para instalar y montar el hardware de la computadora

Vista frontal de Warehouse



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. Warehouse 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

Vista posterior de Warehouse



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: <ul style="list-style-type: none"> 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 de Warehouse

Factor de forma	1U, profundidad completa
-----------------	--------------------------

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



Montar el dispositivo y configurar parámetros de red

Descripción general

En este tema se proporcionan instrucciones para conectar un dispositivo serie 4 de RSA 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 serie 4 de RSA consiste en configurar la dirección IP predeterminada y el nombre de host, configurar los servidores DNS y el archivo **/etc/hosts** 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

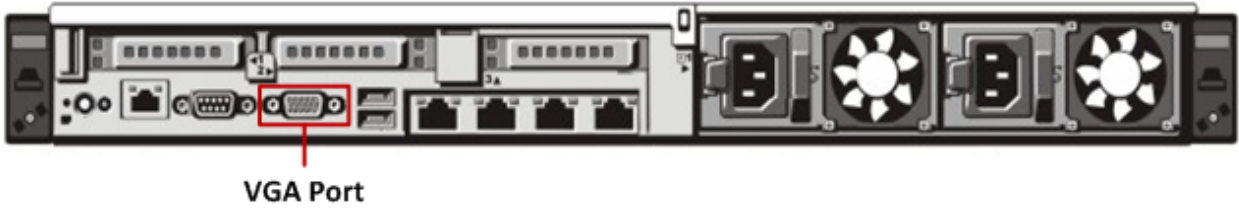
Elija uno de estos métodos para la conexión inicial:

- 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.

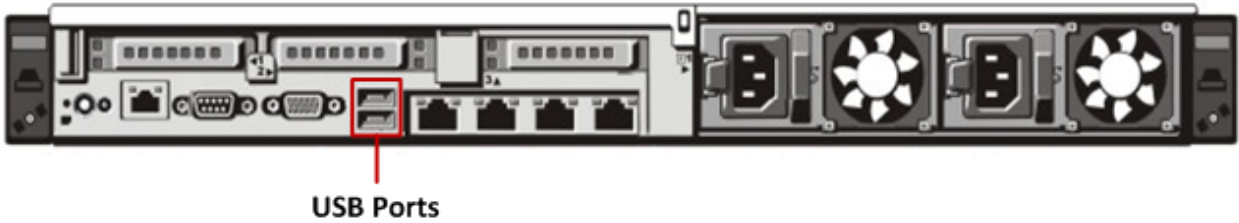
Consola del dispositivo a través de la conexión VGA

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

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.

⚠ 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.

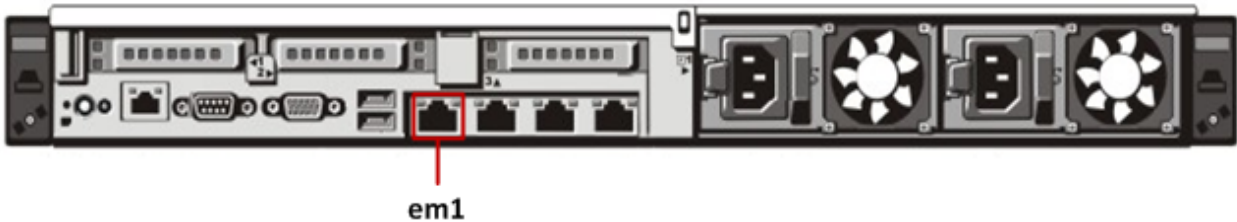
4. En el indicador de inicio de sesión, use las credenciales predeterminadas (`root/netwitness`) para obtener acceso al sistema operativo.
5. Continúe con la sección **Configurar la dirección IP** más adelante.

Consola del dispositivo a través de la conexión de red

⚠ Caution: 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:

1. Conecte un cable Ethernet 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. En el indicador de inicio de sesión, use las credenciales predeterminadas (`root/netwitness`) para obtener acceso al sistema operativo.
5. Continúe con la sección **Configurar la dirección IP** más adelante.

Configurar la dirección IP

Debe configurar manualmente la red en el dispositivo Warehouse. Si está planificando tener un cluster de dispositivos de Warehouse, asegúrese de realizar las siguientes tareas en todos los dispositivos del cluster. Cada dispositivo del clúster debe tener direcciones IP configuradas a través de la consola del dispositivo o de Dell Remote Access Console (iDRAC). Para obtener información sobre iDRAC, consulte la documentación de Dell.

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

Las siguientes son las interfaces de red que debe configurar de acuerdo con su requisito:

Interfaces	Propósito
em1	Pública, conexión al switch del cliente
em2	Privada, conexión al switch exclusivo de Warehouse
em3	Abierto, conexión a cualquier switch o red
em4	Abierto, conexión a cualquier switch o red

Para configurar la red:

1. Inicie sesión en el dispositivo como usuario raíz.

- 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 apropiados para los siguientes parámetros del archivo:

Parámetro	Valor
DEVICE	Tipo de interfaz de red. Por ejemplo, eth0.
BOOTPROTO	static
IPADDR	Dirección IP de la interfaz de red
NETMASK	Dirección de la máscara de subred
GATEWAY	La dirección del gateway predeterminado.
HWADDR	Dirección MAC del dispositivo
ONBOOT	yes
TYPE	Tipo de red

- Para reiniciar el servicio de red, escriba el siguiente comando:
`service network restart`
- (Opcional) Configure la interfaz de red em2 si la interfaz interna que usa el dispositivo Warehouse individual para comunicarse con otros dispositivos Warehouse del clúster se establece a través de un switch. El archivo de configuración respectivo es `/etc/sysconfig/network-scripts/ifcfg-em2`.

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.

Para configurar el nombre de host:

- Inicie sesión en el dispositivo como usuario raíz.
- Para configurar el nombre de host del dispositivo, edite el archivo `/etc/sysconfig/network` mediante el siguiente comando:
`vi /etc/sysconfig/network`
- Agregue lo siguiente a la configuración o modifíquela de la siguiente manera:
`NETWORKING=[yes|no]`
`HOSTNAME=<sawnode_hostname>`
donde `<sawnode_hostname>` es el nombre de host del dispositivo Warehouse.
`DOMAINNAME = <value>`

Note: puede ingresar un valor para `DOMAINNAME` si la empresa requiere un nombre de dominio para los nombres de host del nodo de Warehouse. Si decide no usar un nombre de dominio, deje este valor en blanco.

- Para guardar los cambios y salir del editor vi, escriba el siguiente comando:
:wq
- Para reiniciar la red, escriba el siguiente comando:
`service network restart`
- Para verificar 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:

- Inicie sesión en el dispositivo como usuario raíz.
- Escriba el siguiente comando:
`vi /etc/resolv.conf`
- 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`
- Para guardar los cambios y salir del editor vi, escriba el siguiente comando:
:wq

Configurar el archivo /etc/hosts

Edite el archivo **hosts** del dispositivo para incluir la dirección IP y el nombre de host de cada uno de los nodos de Warehouse del clúster.

Caution: el nombre de host de los nodos de Warehouse no debe aparecer como parte de la configuración de la dirección de loopback.

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

- Inicie sesión en el dispositivo como usuario raíz.
- Escriba el siguiente comando:
`vi /etc/hosts`
- Agregue la siguiente línea al archivo para cada uno de los nodos de Warehouse:
`<node_private_ip_address> <node_fqdn> <node_hostname>`
Donde:
`<node_private_ip_address>` es la interfaz privada del nodo en el clúster de Warehouse.
`<node_fqdn>` es el nombre de dominio calificado del nodo en el clúster de Warehouse.

`<node_hostname>` es el nombre de host del nodo en el clúster de Warehouse.

Agregue los detalles de todos los nodos del clúster de Warehouse en líneas por separado en el archivo `/etc/hosts`.

El siguiente es un ejemplo del archivo `/etc/hosts` que incluye detalles de todos los nodos del clúster de Warehouse:

```
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
192.168.1.10 sawnode1.domainname.com sawnode1
192.168.1.11 sawnode2.domainname.com sawnode2
192.168.1.12 sawnode3.domainname.com sawnode3
```

- Para guardar los cambios y salir 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 Warehouse.

Para actualizar la configuración de NTP:

- Inicie sesión en el dispositivo como usuario raíz.
- Para editar el archivo `/etc/ntp.conf`, escriba el siguiente comando:
`vi /etc/ntp.conf`
- 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`
- Para guardar los cambios y salir del editor vi, escriba el siguiente comando:
:wq
- Para reiniciar el servicio, escriba el siguiente comando:
`service ntpd restart`



Completar la configuración de Warehouse en Security Analytics

Descripción general

En este tema se proporcionan instrucciones para completar la configuración de RSA Analytics Warehouse (MapR).

Introducción

Los pasos finales para configurar Warehouse pueden incluir:

1. Generar y actualizar el UUID predeterminado en los dispositivos.
2. Actualizar la versión del servidor de Hive en el dispositivo.
3. Actualizar el archivo de la plantilla de configuración en el dispositivo Warehouse.
4. Instalar el archivo de licencia de Warehouse.
5. Generar la dirección IP virtual para el dispositivo Warehouse.
6. Configurar Warehouse Connector para que escriba en Warehouse.
7. Agregar orígenes de datos de Warehouse a Reporting Engine.

Para obtener instrucciones detalladas, consulte la *Guía de configuración de RSA Analytics Warehouse (MapR)* (Security Analytics 10.4) o la *Guía de configuración de Security Analytics Warehouse* (Security Analytics 10.3 y anteriores) en la ayuda en línea en sadoes.emc.com/es-mx.