



# RSA Security Analytics

Guía de instalación del  
dispositivo Malware Analysis  
serie 4

## 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](http://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 del dispositivo Malware Analysis serie 4

- [Guía de instalación del dispositivo Malware Analysis serie 4](#) 4
  - [Descripción del hardware del dispositivo SA Malware Analysis](#) 5
  - [Montar el dispositivo y configurar parámetros de red](#) 9
  - [Completar la configuración del dispositivo Malware Analysis en Security Analytics](#) 17



# Guía de instalación del dispositivo Malware Analysis serie 4

---

## Descripción general

Este documento es una guía paso a paso para instalar el dispositivo Malware Analysis 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 Malware Analysis como se describe en la documentación en línea de Security Analytics en [sadoes.emc.com/es-mx](http://sadoes.emc.com/es-mx).



# Descripción del hardware del dispositivo SA Malware Analysis

---

## Descripción general

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

---

## Introducción

El dispositivo RSA Security Analytics Malware Analysis serie 4 incluye el software Malware Analysis y Broker instalado. Este Broker es solo para el servidor de Malware Analysis. La configuración inicial del dispositivo Malware Analysis en la red implica los siguientes pasos:

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

Hay varias opciones para la conexión física inicial del dispositivo Malware 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.

---

## Contenido del paquete

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

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

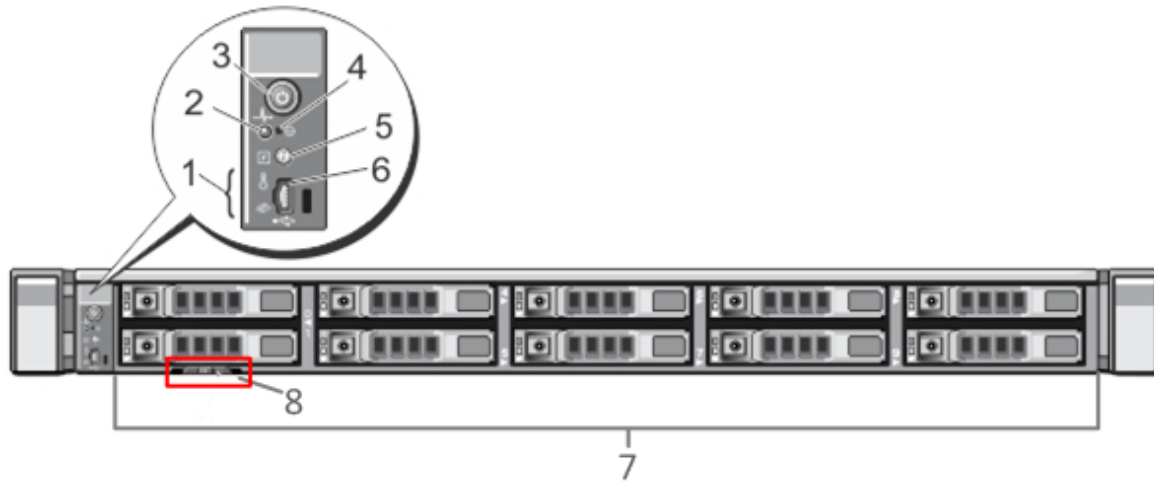
---

## Materiales suministrados por el cliente

Para completar el procedimiento de instalación, necesitará:

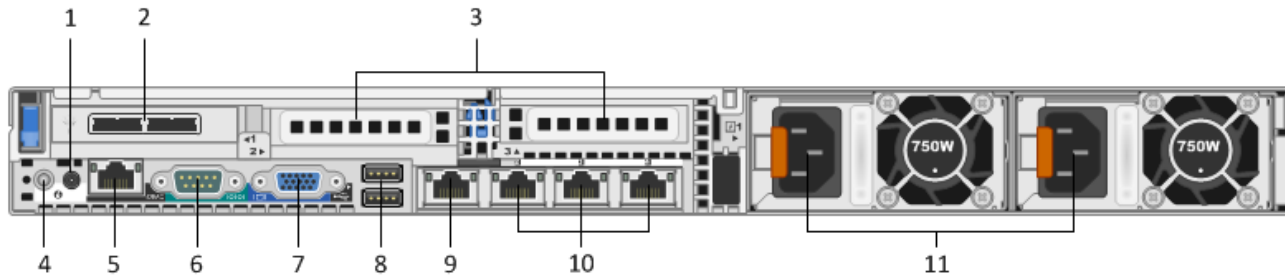
- Un cable de red Ethernet
- Cables para conectar un monitor o adaptador KVM al puerto VGA y un teclado o adaptador KVM al puerto USB
- Herramientas estándar para instalar y montar el hardware de la computadora

## Vista frontal del dispositivo Malware 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. El dispositivo Malware 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

## Vista posterior del dispositivo Malware Analysis



Clave	Descripción
1	Luz de identificación del sistema
2	Controlador SAS instalado con dos puertos de interfaz de DAC para la conexión a los arreglos de almacenamiento en disco
3	Slots de expansión para tarjetas opcionales
4	Botón 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)
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 Malware Analysis

Factor de forma	1U, profundidad completa
Peso	19.75 kg (43.56 lb)
Dimensiones (aproximadas)	Con bisel: 434.0 mm (ancho) x 787.1 mm (profundidad) x 42.8 mm (alto) Sin bisel: 434.0 mm (ancho) x 752.1 mm (profundidad) x 42.8 mm (alto)

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 Security Analytics serie 4 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 RSA Security Analytics serie 4 consiste en configurar la dirección IP predeterminada, el origen del reloj de red y el nombre de host, y, a continuación, los servidores DNS. 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 el programa NwConsole para modificar la configuración de administración del dispositivo. Use la línea de comandos del SO para configurar los servidores DNS.

Método	Nombre de usuario	Contraseña predeterminada
ssh/cli	raíz	netwitness
dispositivo	admin	netwitness

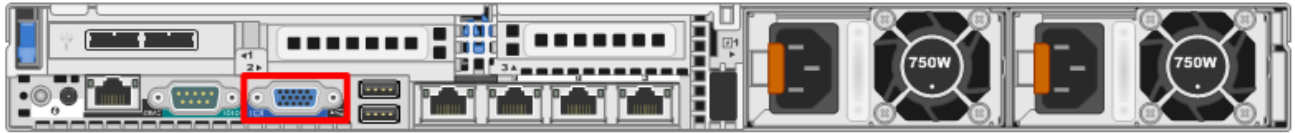
Elija uno de estos métodos para la conexión inicial:

- 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.

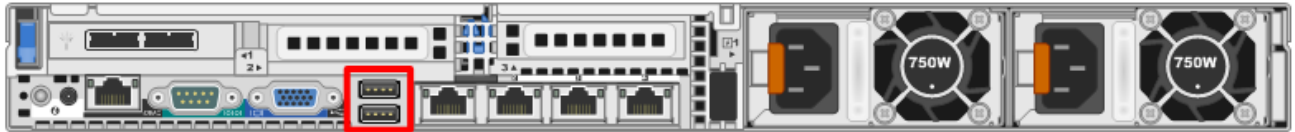
## Consola del dispositivo a través de la conexión VGA

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.

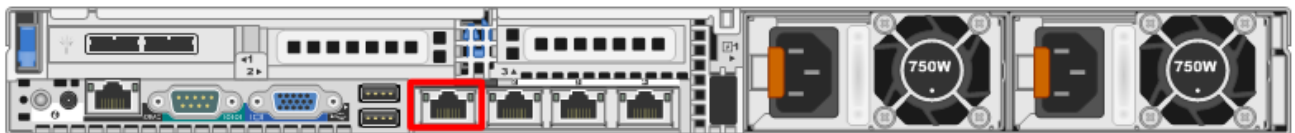
4. En el indicador de inicio de sesión, use las credenciales predeterminadas para obtener acceso al sistema operativo (`root/netwitness`).
5. Continúe con la sección **Configurar parámetros de red (dispositivos 10.3.x y anteriores)** o **Configurar parámetros de red (dispositivos 10.4.x y posteriores)**, según la versión del software de Security Analytics.

## 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 (em1) de la parte posterior del dispositivo.



2. Conecte los cables de alimentación a los conectores de alimentación del dispositivo y a un tomacorriente.

- 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.

- Acepte la clave del protocolo SSH.
- En el indicador de inicio de sesión, inicie sesión como raíz para obtener acceso al sistema operativo. Si recibe un indicador que solicita ingresar la dirección IP del servidor de Security Analytics, presione **CTRL+C** para salir de él.
- Continúe con la sección **Configurar parámetros de red (dispositivos 10.3.x y anteriores)** o **Configurar parámetros de red (dispositivos 10.4.x y posteriores)**, según la versión del software de Security Analytics.

## Configurar parámetros de red (dispositivos 10.3.x y anteriores)

Siga los procedimientos de esta sección para configurar los parámetros de red para dispositivos 10.3.x y anteriores.

### Configurar la dirección IP (10.3.x y anteriores)

Use uno de los siguientes procedimientos para configurar la dirección IP de administración en el dispositivo.

#### Configurar una dirección IP estática (10.3.x y anteriores)

Para configurar una dirección IP estática:

- En el indicador de la raíz: `[root@NwAppliance~]#`  
escriba el siguiente comando:  
`NwConsole`  
NwConsole se inicia y se muestra el siguiente mensaje:  
`RSA Security Analytics Console 10.2`  
`Copyright 2001-2012, RSA Security Inc. Todos los derechos reservados.`
- En NwConsole, escriba el siguiente comando:  
`login localhost:50006 <adminusername> <password>`  
Por ejemplo: `login localhost:50006 admin 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] />`  
escriba el siguiente comando:  
`appliance setNet mode=static address=<desired IP address> netmask=<desired netmask>`  
`gateway=<desired network gateway>`  
Por ejemplo: Para configurar la dirección IP de la interfaz em1 del dispositivo en 10.1.2.35 para una red clase C con gateway 10.1.2.1, ejecute el siguiente comando:  
`appliance setNet mode=static address=10.1.2.35 netmask=255.255.255.0 gateway=10.1.2.1`  
Los servicios de red se reinician automáticamente en el dispositivo y se aplica la nueva configuración.
- Si el dispositivo está conectado mediante una conexión de red, tendrá que volver a conectarse a él y usar la nueva dirección IP para continuar. Si transfirió el dispositivo a una nueva subred, también puede ser necesario realizar cambios en las redes cliente.

5. Para cerrar sesión y salir de NwConsole, escriba `exit`.

## Configurar una dirección IP dinámica (10.3.x y anteriores)

Para configurar una dirección IP dinámica:

1. En el indicador de la raíz: `[root@NwAppliance~]#`  
escriba el siguiente comando:  
`NwConsole`  
NwConsole se inicia y se muestra el siguiente mensaje:  
`RSA Security Analytics Console 10.2`  
`Copyright 2001-2012, RSA Security Inc. Todos los derechos reservados.`
2. En NwConsole, escriba el siguiente comando:  
`login localhost:50006 <username> <password>`  
Se inicia la sesión en el dispositivo y se muestra el siguiente mensaje:  
`Successfully logged in as session <session #>`
3. En el indicador del host local: `[localhost:50006] />`  
escriba el siguiente comando:  
`appliance setNet mode=dhcp`
4. Los servicios de red se reinician automáticamente en el dispositivo y se aplica la nueva configuración. Si el dispositivo está conectado mediante una conexión de red, tendrá que volver a conectarse a él y usar la nueva dirección IP para continuar. Si transfirió el dispositivo a una nueva subred, también puede ser necesario realizar cambios en las redes cliente.

**⚠ Caution:** si elige DHCP, es posible que no haya manera de determinar la nueva dirección. Debe conectarse directamente a la consola del dispositivo para determinarla.

## Configurar el nombre de host (10.3.x y anteriores)

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.

1. Si la sesión en NwConsole continúa iniciada, omita los pasos 2 y 3.
2. En el indicador de la raíz: `[root@NwAppliance~]#`  
escriba el siguiente comando:  
`NwConsole`  
NwConsole se inicia y se muestra el siguiente mensaje:  
`RSA Security Analytics Console 10.2`  
`Copyright 2001-2012, RSA Security Inc. Todos los derechos reservados.`
3. En NwConsole, escriba el siguiente comando:  
`login localhost:50006 <username> <password>`  
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] />` escriba el siguiente comando:  
`appliance hostname name=<desired_name_for_appliance>`  
Por ejemplo: `appliance hostname name=myserver`
- Cuando vea la salida `Success`, escriba `exit` para cerrar la sesión y salir del programa NwConsole.
- Reinicie el servidor mediante el comando: `reboot`

**Note:** se recomienda reiniciar el sistema después de cambiar el nombre de host.

## Especificar el origen del reloj de red (10.3.x y anteriores)

**Note:** 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 SA.

Se recomienda sincronizar todos los sistemas del conjunto de aplicaciones Security Analytics mediante un origen de tiempo de red, de modo que todos los servicios y 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.

**Note:** los comandos de estas instrucciones distinguen mayúsculas de minúsculas.

Para configurar el origen del reloj de red:

- Si la sesión en NwConsole continúa iniciada, omita los pasos 2 y 3.
- En el indicador de la raíz: `[root@NwAppliance~]#` escriba el siguiente comando:  
`NwConsole`  
NwConsole se inicia y se muestra el siguiente mensaje:  
`RSA Security Analytics Console 10.2`  
`Copyright 2001-2012, RSA Security Inc. Todos los derechos reservados.`
- En NwConsole, escriba el siguiente comando:  
`login localhost:50006 <username> <password>`  
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] />` escriba el siguiente comando:  
`appliance setNTP source=<NTP_server_hostname or IP_address>`  
Por ejemplo: `appliance setNTP source=0.pool.ntp.org`  
O, 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.

## Configurar servidores DNS (10.3.x y anteriores)

Para configurar la dirección del servidor DNS:

1. En el indicador de la raíz: `[root@NwAppliance~]#`  
escriba el siguiente comando:  
`vi /etc/resolv.conf`
2. 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`
3. Guarde los cambios y salga del editor vi.

---

## Configurar parámetros de red (dispositivos 10.4.x y posteriores)

Cuando enciende el sistema e inicia sesión en él por primera vez, se le solicita ejecutar **netconfig.sh** para optimizar el establecimiento de configuraciones de red estáticas o dinámicas. Si no recibe el indicador, puede ejecutar `#netconfig.sh` desde la línea de comandos, donde se le solicitará ingresar las opciones de configuración. Cuando haya completado la configuración inicial, deberá ver un indicador que le solicita guardar, 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
-----
? █

```

## Especificar el origen del reloj de red (10.4.x y posteriores)

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.

**⚠ Caution:** es necesario configurar la sincronización de la hora entre los servicios y los dispositivos. Se recomienda enfáticamente utilizar 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.

Los comandos de las siguientes instrucciones distinguen mayúsculas de minúsculas.

Para configurar el origen del reloj de red:

1. Si la sesión en NwConsole continúa iniciada, omite los pasos 2 y 3.
2. En el indicador de la raíz: `[root@NwAppliance~]#` escriba el siguiente comando:  
**NwConsole**  
NwConsole se inicia y se muestra el siguiente mensaje:  
RSA Security Analytics Console 10.2  
Copyright 2001-2012, RSA Security Inc. Todos los derechos reservados.

- En NwConsole, escriba el siguiente comando:  

```
login localhost:50006 <username> <password>
```

 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] />`  
 escriba el siguiente comando:  

```
appliance setNTP source=<NTP_server_hostname or IP_address>
```

 Por ejemplo: `appliance setNTP source=0.pool.ntp.org`  
 O, 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.

## Configurar servidores DNS (10.4.x y posteriores)

Para configurar la dirección del servidor DNS:

- En el indicador de la raíz: `[root@NwAppliance~]#`  
 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
```
- Guarde los cambios y salga del editor vi.

## Configurar la dirección IP del servidor de Security Analytics (10.4.x y posteriores)

Para configurar la dirección IP del servidor de Security Analytics:

- Una vez que haya completado la configuración inicial, reinicie el dispositivo.
- Inicie sesión en el dispositivo como raíz.
- Cuando se le solicite, escriba la dirección IP del servidor de Security Analytics.





# Completar la configuración del dispositivo Malware Analysis en Security Analytics

---

## Descripción general

En este tema se proporcionan instrucciones para completar la configuración del dispositivo Malware Analysis en Security Analytics.

---

## Introducción

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

1. Agregar el dispositivo (y el servicio) Malware Analysis y el servicio Broker integrado a Security Analytics.
2. Aplicar una licencia (o autorización) al servicio Malware Analysis.
3. Configurar Malware Analysis.
4. (Opcional) Ajustar el servicio Malware Analysis e implementar la personalización avanzada. Por ejemplo, habilitar contenido YARA personalizado.

Para obtener instrucciones detalladas, consulte la *Guía de configuración de Malware Analysis* y la *Guía de licencia* correspondientes a su versión de Security Analytics en la ayuda en línea en [sadoes.emc.com/es-mx](http://sadoes.emc.com/es-mx).