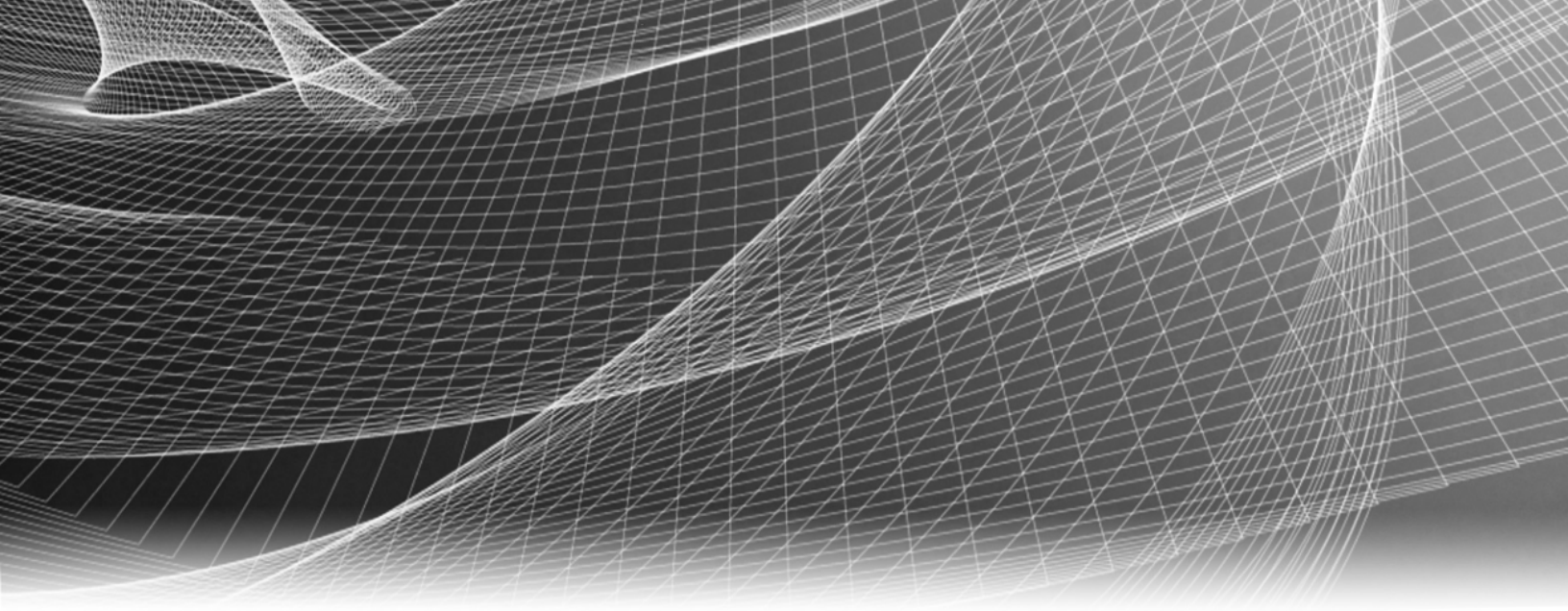


RSA Security Analytics

Guía de instalación de Decoder 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 Decoder serie 4

RSA

Guía de instalación de Decoder serie 4

Descripción general

Este documento es una guía paso a paso para instalar Decoder 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 de Decoder 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 Decoder

Descripción general

En este documento se presenta RSA Security Analytics Decoder y el procedimiento general para instalar Decoder y conectarlo a la red y al almacenamiento.

Introducción

El dispositivo RSA Security Analytics Decoder serie 4 incluye el software Decoder instalado. La configuración inicial de Decoder en la red implica los siguientes pasos:

1. Revisar los requisitos del sitio y la información de seguridad.
2. Montar el hardware de Decoder.
3. Conectar Decoder a la red y configurar parámetros de red en Decoder.
4. Conectar Decoder a un dispositivo de capacidad de conexión directa (DAC) o SAN, como se describe en la Guía de instalación de capacidad de conexión directa (DAC) serie 4.
5. Completar la instalación de Decoder en Security Analytics.

Hay varias opciones para la conexión física inicial de Decoder 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 Decoder de RSA.

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

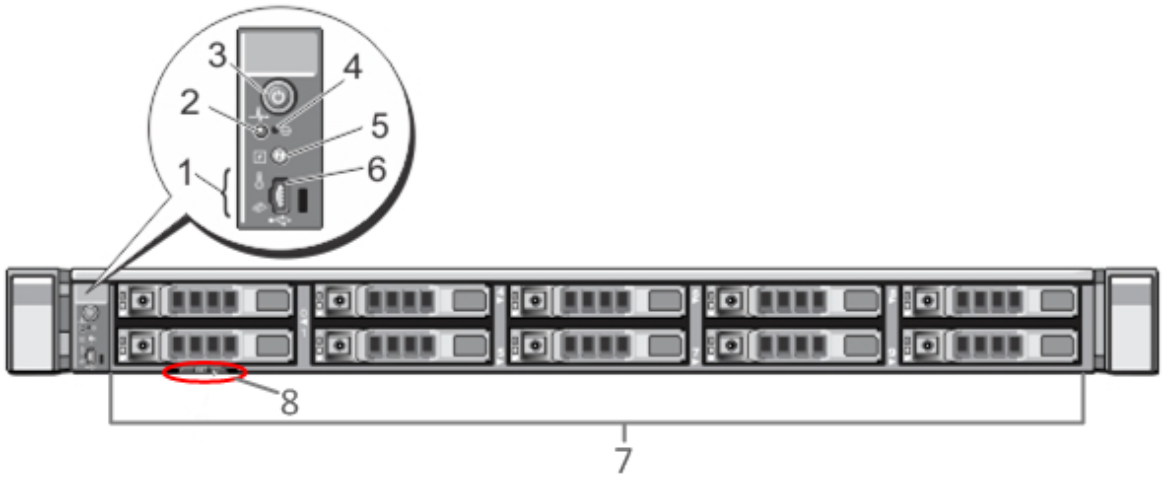
Materiales suministrados por el cliente

Para completar el procedimiento de instalación, necesitará:

Last Modified: September 15 2016, 11:33AM

- Múltiples cables de red Ethernet (uno para administración y uno para cada interfaz de captura)
- 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

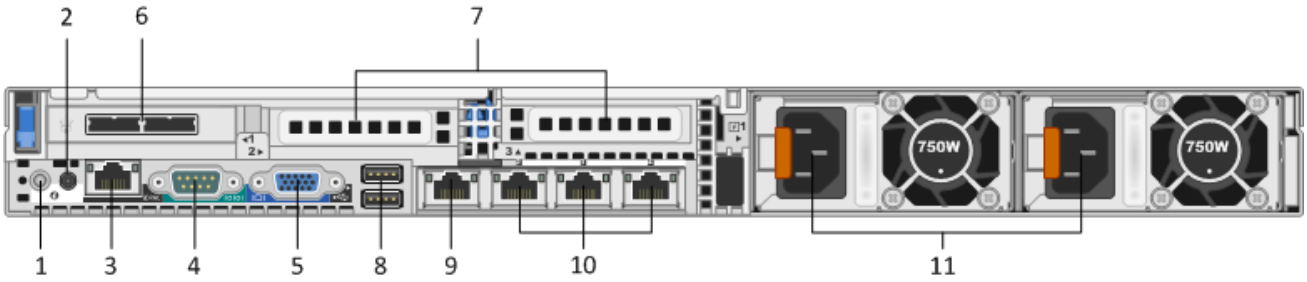
Vista frontal de Decoder



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. Decoder tiene dos unidades de 146 GB y dos 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 de Decoder



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 = puertos de monitoreo
11	Fuente de alimentación reemplazable en caliente 1 y 2

Especificaciones de Decoder

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)
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 serie 4 a la red y configurar en él los parámetros de administración iniciales.

> ⚠ **Caution:** Si está instalando la capacidad de conexión directa (DAC), debe instalarla antes de obtener la licencia para el dispositivo e iniciar los servicios. Consulte instrucciones para obtener licencias para los dispositivos en la **Guía de licencia de Security Analytics**, a la cual puede acceder a través de la opción **Ayuda** de Security Analytics y en sadocs.emc.com/es-mx.

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:

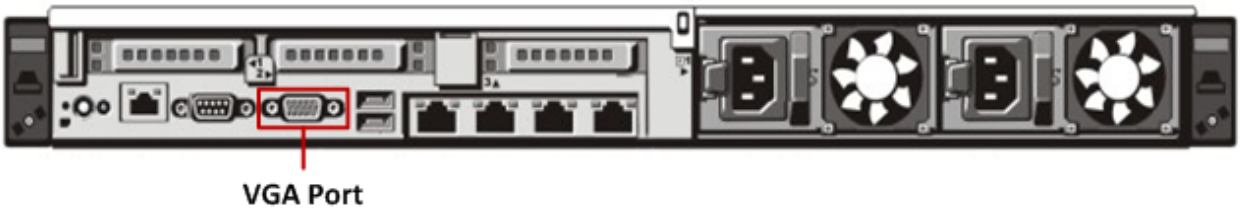
- Consola del dispositivo a través de la conexión VGA: teclado (puerto USB) y monitor (puerto VGA).
- Consola del dispositivo a través de la conexión de red: Computadora que usa un cliente del protocolo SSH conectado al dispositivo mediante un cable Ethernet al puerto de admón. (em1), el cual está configurado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

Last Modified: September 15 2016, 11:33AM

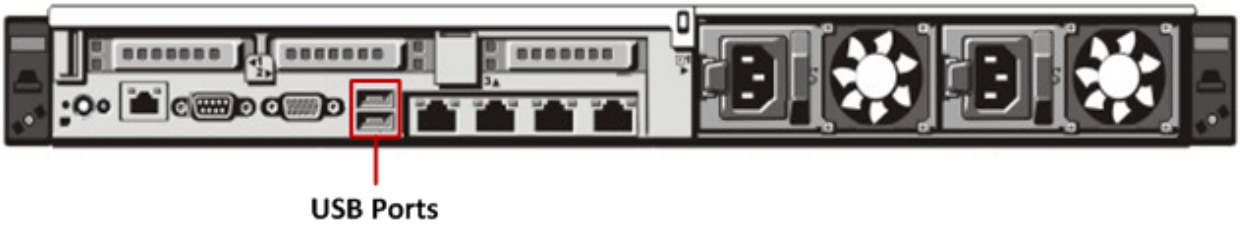
Consola del dispositivo a través de la conexión VGA

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 la dirección IP** más adelante.

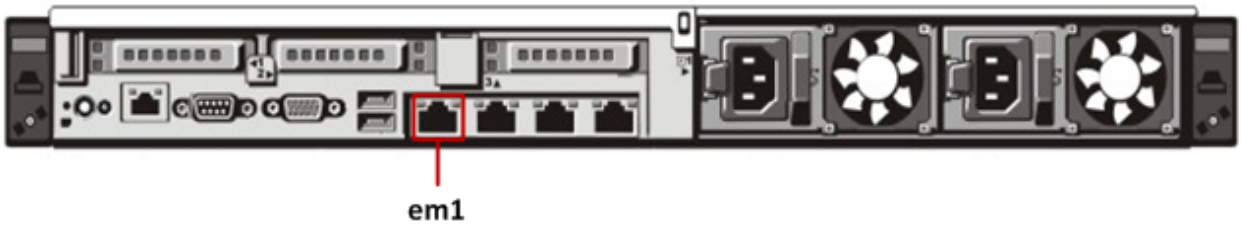
Consola del dispositivo a través de la conexión de red

> ⚠ **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.

Last Modified: September 15 2016, 11:33AM

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. Acepte la clave del protocolo SSH.
5. En el indicador de inicio de sesión, use las credenciales predeterminadas para obtener acceso al sistema operativo.
6. Continúe con la sección **Configurar la dirección IP** más adelante.

Configurar la dirección IP

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

Configurar una dirección IP estática

Para configurar una dirección IP estática:

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 <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 #>`
3. 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>`

Last Modified: September 15 2016, 11:33AM

- 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.

4. 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

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

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.

Last Modified: September 15 2016, 11:33AM

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 #>
   ```
4. 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`**
5. Cuando vea la salida `Success`, escriba **`exit`** para cerrar la sesión y salir del programa NwConsole.
6. Reinicie el servidor mediante el comando: **`reboot`**

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

Especificar al origen del reloj de red

> **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 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:

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 #>
   ```
4. En el indicador del host local: `[localhost:50006] />`
   escriba el siguiente comando:
   `appliance setNTP source=<NTP_server_hostname or IP_address>`

Last Modified: September 15 2016, 11:33AM

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**

5. 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

Para configurar una dirección IP estática:

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.

Last Modified: September 15 2016, 11:33AM

RSA

Completar la configuración de Decoder en Security Analytics

Descripción general

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

Introducción

> **Caution:** antes de dar inicio a la instalación final en Security Analytics, debe ejecutar el script de inicialización de DAC para configurar el primer arreglo de almacenamiento, como se describe en la Guía de instalación de capacidad de conexión directa (DAC) serie 4.

Los pasos finales para configurar Decoder se realizan en el servidor de Security Analytics. Son los siguientes:

1. Agregar Decoder a Security Analytics en la vista Dispositivos.
2. Aplicar una licencia (o autorización) de dispositivo a Decoder.
3. Configurar feeds y analizadores.
4. Configurar e iniciar la captura.
5. Agregar uno o más Decoders a Concentrator como dispositivos agregados.

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

- Para el paso 2, las licencias (o autorizaciones) del dispositivo de Security Analytics deben estar disponibles para habilitar los dispositivos.
- Para el paso 5, se debe instalar y configurar por lo menos un servicio Concentrator, se debe obtener licencia para él y el servicio debe estar listo para agregar datos desde Decoder.

Inicie sesión en Security Analytics y siga las instrucciones de la ayuda en línea para completar la instalación de Decoder.

Last Modified: September 15 2016, 11:33AM