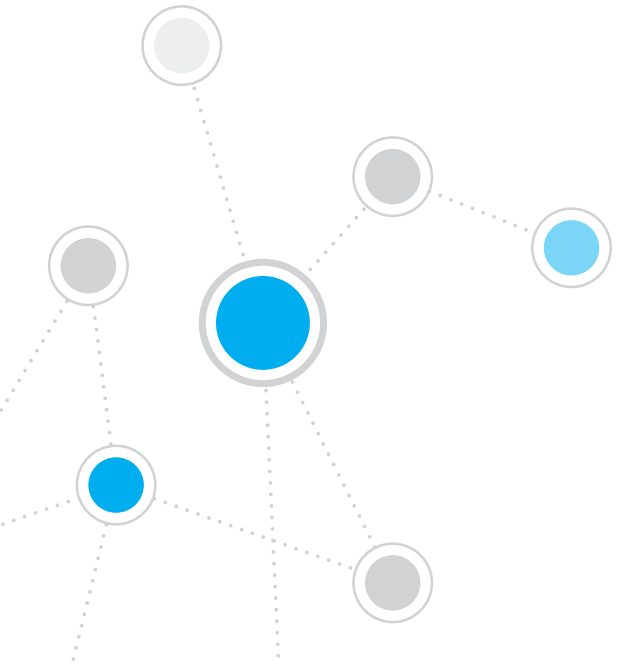
ForeScout CounterACT® 7

Equipo simple CounterACT

Guía de instalación rápida



Índice

Bienvenido a ForeScout CounterACT® Versión 7

ForeScout CounterACT es un dispositivo de seguridad virtual o físico que identifica dinámicamente y evalúa las aplicaciones y dispositivos de red en el momento en que se conectan a su red. Debido a que CounterACT no necesita un agente, funciona con sus dispositivos, administrados o no administrados, conocidos o desconocidos, PC o móviles, integrados o virtuales. CounterACT determina con rapidez el usuario, propietario, sistema operativo, configuración del dispositivo, software, servicio, estado de parches y la presencia de agentes de seguridad. Luego, proporciona reparación, control y supervisión continua de estos dispositivos debido a que vienen y parten de la red. Hace todo esto mientras se integra sin dificultades con su infraestructura actual de IT.

Esta guía describe la instalación de un equipo simple e independiente CounterACT.

Para más información detallada o información sobre la implementación de múltiples equipos para protección de redes en toda la empresa, consulte la Guía de Instalación CounterACT y el Manual del Usuario de la Consola. Estos documentos están ubicados en directorio /docs del CD de CounterACT.

Además puede navegar por el sitio web de soporte técnico ubicado en: https://www.forescout.com/support para acceder a la última documentación, conocer los artículos de base y acceder a actualizaciones para su equipo.

Incluido en su paquete CounterACT

- Equipo CounterACT
- Guía de instalación rápida
- CD de CounterACT con Software de la consola, Manual del usuario de la consola CounterACT y Guía de instalación
- Documento de garantía
- Abrazaderas de montaje
- Cable de energía
- Cable de conexión de la consola DB9 (para conexiones en serie únicamente)

Perspectiva general

Para configurar CounterACT realice lo siguiente:

1. Cree un plan de implementación
2. Configure su interruptor
3. Conecte la energía y los cables de la red
4. Configure el equipo
5. Administración remota
6. Verifique la conectividad
7. Configure la consola de CounterACT

1. Cree un plan de implementación

Antes de llevar a cabo la instalación, debe decidir dónde colocar el equipo y debe conocer las conexiones de interfaz del equipo.

Decida dónde implementar el equipo

La selección de la correcta ubicación de la red del equipo es crucial para el óptimo rendimiento y la exitosa implementación de CounterACT. La correcta ubicación dependerá de sus objetivos de implementación deseados y las políticas de acceso a la red. El equipo deberá poder controlar el tráfico relevante para la política deseada. Por ejemplo, si su política depende de los eventos de autorización de control desde los terminales hasta los servidores de autenticación corporativa, el equipo deberá estar instalado de manera que pueda ver el flujo de tráfico de los terminales a los servidores de autenticación.

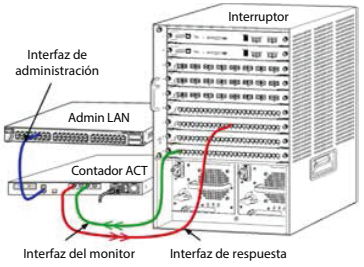
Para más información sobre la instalación y la implementación, consulte la Guía de Instalación de CounterACT, ubicada en el CD de CounterACT que recibió con este paquete.

Conexiones de interfaz del equipo

El equipo está generalmente configurado con tres conexiones al interruptor de red.

Interfaz de administración

Esta interfaz le permite administrar CounterACT y realizar preguntas y una inspección profunda de los terminales. La interfaz debe estar conectada a un puerto del interruptor que tenga acceso a todos los terminales de la red.



Cada equipo exige un conexión de administración única a la red. Esta conexión necesita de una dirección de IP en la red LAN local y acceso a un puerto 13000/ TCP desde las máquinas que harán funcionar la aplicación de la administración de la consola de CounterACT. La interfaz de administración debe tener acceso a lo siguiente en su red:

Puerto	Servicio	Hacia o desde CounterACT	Función
22/TCP	SSH	A	Permite el acceso a la interfaz de línea del comando CounterACT.
2222/TCP			(Alta disponibilidad) Permite acceso a los dispositivos físicos de CounterACT que son parte del grupo de terminales de alta disponibilidad. Use 22/TCP para acceder a la dirección compartida de IP (virtual) del grupo de terminales.

Puerto	Servicio	Hacia o desde CounterACT	Función
25/TCP	SMTP	Desde	Se usa para enviar correos desde CounterACT.
53/UDP	DNS	Desde	Permite que CounterACT resuelva direcciones internas de IP.
80/TCP	HTTP	A	Permite la redirección de HTTP.
123/UDP	NTP	Desde	Permite el acceso de CounterACT a un servidor de tiempo NTP. Por defecto, CounterACT usa ntp.foreScout.net.
135	WMI	Desde	Permite que CounterACT realice una profunda investigación y control de los terminales de Windows usando WMI.
139/TCP	SMB, MS-RPP	Desde	Permite la inspección remota de los terminales de Windows (para los terminales que funcionan con Windows 7 y versiones anteriores).
445/TCP			Permite la inspección remota de los terminales de Windows.
161/UDP	SNMP	Desde	Permite que CounterACT se comunique con un equipo de infraestructura de red, tal como interruptores y routers. Para más información sobre la configuración de SNMP consulte el *Manual del Usuario de la Consola de CounterACT.*
162/UDP	SNMP	A	Permite que CounterACT reciba trampas de SNMP desde la infraestructura de la red, tal como interruptores y routers. Para más información sobre la configuración de SNMP, consulte el *Manual del Usuario de la Consola de CounterACT.*
443/TCP	HTTPS	A	Permite la redirección de HTTP usando TLS.
2200/TCP	Secure Connector	A	Permite que SecureConnector cree una conexión segura (SSH encriptado) al equipo desde las máquinas Macintosh/ Linux. *SecureConnector* es un secuencia de comandos basada en un agente que permite la gestión de los terminales Macintosh y Linux mientras están conectados a la red.
10003/TCP	Secure Connector para Windows	A	Permite que SecureConnector cree una conexión segura (TLS encriptado) al equipo desde las máquinas Windows. *SecureConnector* es un agente que permite la gestión de los terminales de Windows mientras están conectados a la red. Consulte el *Manual del Usuario*

			de la Consola de CounterACT para obtener más información. Cuando SecureConnector se conecta a un equipo o al Administrador corporativo, se redirecciona al equipo al cual su host es asignado. Asegúrese de que este puerto esté abierto a todos los equipos y al Administrador corporativo para permitir una movilidad transparente dentro de la organización.
13000/TCP	CounterACT	A	Permite la conexión desde la consola al equipo. Para sistemas con equipos CounterACT múltiples, permite la conexión desde la consola al Administrador corporativo y desde el Administrador corporativo a cada equipo.

Interfaz del monitor

Esta conexión permite que el equipo controle y registre el tráfico de la red.

El equipo controla y duplica el tráfico a un puerto en el interruptor. Dependiendo del número de VLAN que se están reflejando, el tráfico puede ser o no 802.1Q VLAN marcado.

- **VLAN simple (sin marcar):** Cuando el tráfico controlado se genera desde una VLAN simple, el tráfico duplicado no necesita estar marcado en la VLAN.
- **Múltiples VLAN (marcadas):** Cuando el tráfico marcado proviene de más de una VLAN, el tráfico duplicado debe estar marcado 802.1Q VLAN.

Cuando dos interruptores están conectados a un par redundante, el equipo debe controlar el tráfico desde ambos interruptores.

No se exige ninguna dirección de IP en la interfaz del monitor.

Interfaz de respuesta

El equipo responde al tráfico usando esta interfaz. El tráfico de respuesta se usa para protegerse contra la actividad maliciosa y para llevar a cabo acciones de la política NAC. Estas acciones pueden incluir, por ejemplo, redireccionar los navegadores web o realizar un bloqueo del firewall. La configuración del puerto del interruptor relacionado depende del tráfico que se está monitoreando.

- **VLAN simple (sin marcar):** Cuando el tráfico monitoreado se genera desde una VLAN simple, la interfaz de respuesta debe estar configurada para ser parte de la misma VLAN. En este caso, el equipo exige una única dirección de IP en esa VLAN.
- **Múltiples VLAN (marcadas):** Si el tráfico marcado proviene de más de una VLAN, la interfaz de respuesta debe estar también configurada con marcado 802.1Q para las mismas VLAN. El equipo necesita una dirección de IP para cada VLAN protegida.

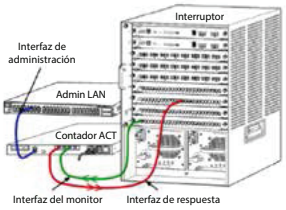
2. Configuración de su interruptor

A. Opciones de conexión del interruptor

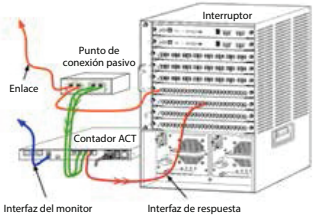
El equipo fue diseñado para integrarse sin problemas a una amplia variedad de entornos de red. Para integrar de manera exitosa el equipo a su red, verifique que su interruptor esté configurado para controlar el tráfico requerido.

Hay varias opciones disponibles para conectar el equipo a su interruptor.

1. **Implementación estándar (administración separada, interfaces de control y respuesta)**
   La implementación recomendada usa tres puertos separados. Estos puertos se describen en *Conexiones de interfaz del equipo*.

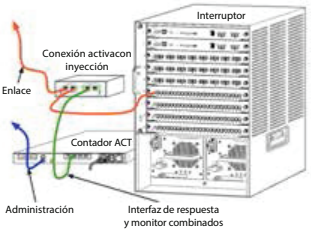


2. **Punto de conexión insertado pasivo**
   En lugar de conectar a un puerto de monitoreo con interruptor, el equipo puede usar un punto de conexión insertado pasivo.



   El punto de conexión pasivo necesita de dos puertos de monitoreo, excepto en el caso de unos puntos de conexión de "recombinación", que combinarán las dos corrientes dobles a un único puerto. El tráfico en el puerto conectado y la interfaz de respuesta debe estar configurado del mismo modo. Por ejemplo, si el tráfico en el puerto conectado está marcado VLAN (802.1Q), la interfaz de respuesta debe ser también un puerto marcado de VLAN.

3. **Conexión en línea activa (con inyección)**
   Cuando el equipo usa una conexión en línea que tiene *capacidad de inyección,* las interfaces de respuesta y de monitoreo pueden combinarse. No hay necesidad de configurar un puerto de respuesta separado en el interruptor. Esta opción puede usarse para todo tipo de configuración del interruptor con corriente ascendente o descendente.



4. **Respuesta de la capa de IP (para instalaciones de interruptor de 3 capas)** El equipo puede usar su propia interfaz de administración para responder al tráfico. A pesar de que esta opción puede usarse con un tráfico monitoreado, se la recomienda cuando el equipo monitorea puertos que no son parte de ninguna VLAN, y por lo tanto el equipo no puede responder al tráfico monitoreado usando cualquier otro puerto del interruptor. Esto ocurre generalmente cuando se controla un enlace que conecta a dos routers.

   Esta opción no puede responder a pedidos del Protocolo de Resolución de Direcciones (ARP, por sus siglas en inglés), que limita la capacidad del equipo de detectar escaneos dirigidos a las direcciones de IP incluidas en la subred monitoreada. Esta limitación no aplica cuando se está controlando el tráfico entre los dos routers.

B. Notas para la configuración del interruptor

Etiquetas VLAN (802.1Q)

- **Monitoreo de una única VLAN (tráfico no marcado):** Si el tráfico monitoreado proviene de una única VLAN, el tráfico no necesita etiquetas 802.1Q.
- **Monitoreo de múltiples VLAN (tráfico marcado):** Si el tráfico monitoreado proviene de dos o más VLAN, *ambas* interfaces la de control y la de respuesta deben tener capacidad de marcado 802.1Q. El monitoreo de múltiples VLAN es la opción recomendada ya que brinda la mejor cobertura general a la vez que minimiza el número de puertos que duplica.
- Si el interruptor no puede usar una etiqueta 802.1Q VLAN en los puertos reflejados, realice una de las siguientes acciones:
  - Duplique solo una VLAN
  - Duplique un puerto único, no marcado, enlazado
  - Use la opción de respuesta de capa de IP
- Si el interruptor puede duplicar solo un puerto, entonces duplique solo un puerto enlazado. Este puede estar marcado. En general, si el interruptor no incluye etiquetas 802.1Q VLAN, deberá usar la opción de respuesta de Capa de IP.

Adicional

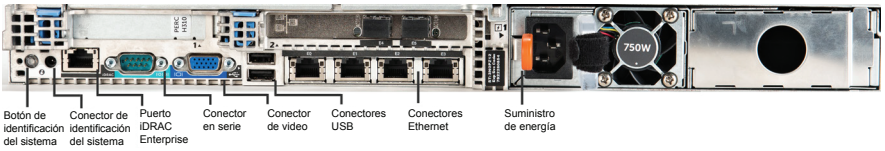
- Si el interruptor no puede duplicar el tráfico de recepción y de transmisión, monitoree el interruptor entero, las VLAN completas (esto ofrece recepción/transmisión) o solo una interfaz (que no permite recepción/transmisión). Verifique que no sobrecargue el puerto de duplicado o reflejado.
- Algunos interruptores (como Cisco 6509) pueden necesitar ex configuraciones de puerto completamente despejadas antes de ingresar nuevas configuraciones. El resultado más común cuando no se despeje información de puertos viejos es que el interruptor quite las etiquetas 802.1Q.

3. Conexión de los cables de la red y encendido

A. Desembalaje del equipo y conexión de los cables

1. Retire el equipo y el cable de energía del contenedor de envío.
2. Retire el kit de rieles que recibió con el equipo.
3. Monte el kit de rieles en el equipo y monte el equipo a la vía.
4. Conecte los cables de la red entre las interfaces de la red en el panel trasero del equipo y los puertos del interruptor.

Muestra del panel trasero — Dispositivo CounterACT



B. Registro de designaciones de interfaces

Luego de completar la instalación del equipo en el centro de datos y de instalar la consola CounterACT, el programa le pedirá que registre la designaciones de la interfaz. Estas designaciones, conocidas como *Definiciones de canal,* se ingresan en el Asistente de configuración inicial que se abre cuando usted ingresa por primera vez a la consola.

Registre las designaciones de la interfaz física abajo y úselas cuando complete la configuración del canal en la consola.

Interfaz de Ethernet	Designación de interfaz (por ej. Administración, Monitoreo, Respuesta)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Encendido del equipo

1. Conecte el cable de energía al conector de potencia en el panel trasero del equipo.
2. Conecte el otro extremo el cable de energía al enchufe a tierra de CA.
3. Conecte el teclado y el monitor al equipo o configure el equipo para una conexión en serie. Consulte la *Guía de Instalación CounterACT* que se encuentra en el CD de CounterACT.
4. Encienda el equipo desde el panel frontal.

Importante: Desconecte la energía de la máquina antes de desenchufar.

4. Configuración del equipo

Prepare la siguiente información antes de configurar el equipo:

☐ Nombre del host del equipo	
☐ Contraseña del administrador de CounterACT	**Conserve la contraseña en un lugar seguro**
☐ Interfaz de administración	
☐ Dirección de IP del equipo	
☐ Máscara de la red	
☐ Dirección de IP de la pasarela predeterminada	
☐ Nombre del dominio DNS	
☐ Direcciones del servidor de DNS	

Luego de conectarlo a la energía, el programa le pedirá que comience la configuración con el siguiente mensaje:

```
El arranque del equipo CounterACT está completo.
Presione <Enter> para continuar.
```

1. Presione **Enter** para mostrar el siguiente menú:

```
1) Configurar CounterACT
2) Restaurar la configuración guardada de CounterACT
3) Identificar y renumerar las interfaces de la red
4) Configurar el teclado
5) Apagar la máquina
6) Reiniciar la máquina
Opción (1-6) :1
```

2. Seleccionar **1** – Configurar CounterACT. Cuando se lo soliciten:

   `Continuar:¿(sí/no)?`

   Presione **Enter** para iniciar el menú:

3. Se abre el menú de **`Modo de alta disponibilidad.`** Presione **Enter** para seleccionar la instalación estándar.
4. Aparece el mensaje **`Configuración Inicial de CounterACT.`** Presione **Enter** para continuar.
5. Se abre el menú **`Seleccionar tipo de instalación de CounterACT.`** Ingrese **1** y presione **Enter** para instalar un equipo estándar CounterACT. Se inicia la configuración. Esto puede llevar un momento.

6. Cuando aparece el mensaje **`Ingrese descripción de la máquina,`** ingrese un corto mensaje de identificación de este dispositivo y presione **Enter**.
   Aparecerá lo siguiente:

```
>>>>>> Establezca la contraseña del Administrador
  <<<<<<
Esta contraseña se usa para ingresar como 'raíz'
para el Sistema de operación de la máquina y
como 'admin' para la consola de CounterACT.
La contraseña deberá tener entre 6 y 15
caracteres de largo y debe contener como mínimo
un carácter no alfabético.

Contraseña del administrador:
```

7. Cuando aparece el mensaje **`Establecer Contraseña del Administrador,`** ingrese la secuencia que será su contraseña (la secuencia no se verá en la pantalla) y presione **Enter**. Se le solicitará que confirme la contraseña. La contraseña deberá tener entre seis y 15 caracteres de largo y debe contener como mínimo un carácter no alfabético.

   Ingrese en el equipo como raíz, *e ingrese en la consola como* admin.

8. Cuando aparezca el mensaje **`Establecer Nombre del Host,`** ingrese un nombre para el host y presione **Enter**. El nombre del host puede usarse cuando se inicie sesión en la consola, y se muestra en la consola para ayudar a identificar el equipo CounterACT que está visualizando.

9. La pantalla **`Configurar los ajustes de la red`** le muestra una serie de parámetros de configuración. Ingrese un valor para cada pedido y presione **Enter** para continuar.
   - Los componentes de CounterACT se comunican a través de interfaces de administración. El número de interfaces de comunicaciones enumerado depende del modelo del equipo.
   - La **Dirección de IP de administración** es la dirección de la interfaz a través de la cual se comunican los componentes CounterACT. Agregue una identificación VLAN para esta interfaz solamente si la interfaz usada para comunicarse entre los componentes CounterACT se conecta con un puerto marcado.
   - Si hay más de una **dirección de servidor DNS,** separe cada dirección con un espacio—La mayoría de los servidores internos DNS resuelven las direcciones externas e internas pero quizás necesite incluir un servidor DNS de resolución externa. Como casi todas las preguntas DNS realizadas por el equipo serán para direcciones externas, el servidor externo DNS deberá estar enumerado al final.

10. Aparece la pantalla de **`Resumen de configuración.`** Le indicarán que realice las pruebas generales de conectividad, reconfigure los ajustes o complete la configuración. Ingrese **D** para completar la configuración.

Licencia

Luego de la instalación, debe instalar la licencia inicial de demostración que le provee el representante de CounterACT. La licencia se instala durante la configuración inicial de la consola. Esta licencia inicial de demostración es válida para cierto número de días. Deberá instalar una licencia permanente antes de que transcurra este periodo. Se comunicarán con usted por correo electrónico en relación a la fecha de vencimiento. Además, se muestra información sobre la fecha de vencimiento y el estado de la licencia en la consola, panel de Equipos/Dispositivos.

Una vez que reciba la licencia permanente, la licencia se validará diariamente a través del Servidor de Licencia de ForeScout. Las violaciones y las alertas de la licencia se muestran en el panel de Detalles del Dispositivo.

Las licencias que no pueden ser validadas durante un mes serán revocadas. Consulte la Guía de Instalación de CounterACT para acceder a más detalles sobre las licencias.

Requisitos de conexión de la red

Como mínimo un dispositivo de CounterACT (Equipo o Administrador de empresa) deberá tener acceso a internet. Esta conexión se usa para validar las licencias CounterACT con el servidor de la Licencia de ForeScout.

Las licencias que no pueden ser autenticadas durante un mes serán revocadas. CounterACT le enviará un correo electrónico de advertencia una vez al día indicando que existe un error de comunicación con el servidor.

5. Administración remota

Configuración de iDRAC

El Controlador Integrado de Acceso Remoto (iDRAC) es una solución de sistema de servidor integrado que le ofrece acceso remoto OS/ubicación independiente en la red LAN o Internet para los Administradores de empresa/ Equipos CounterACT. Use el módulo para acceder a KVM, encender/apagar/ reiniciar y realizar tareas de mantenimiento y de resolución de problemas.

Realice lo siguiente para trabajar con el módulo iDRAC:

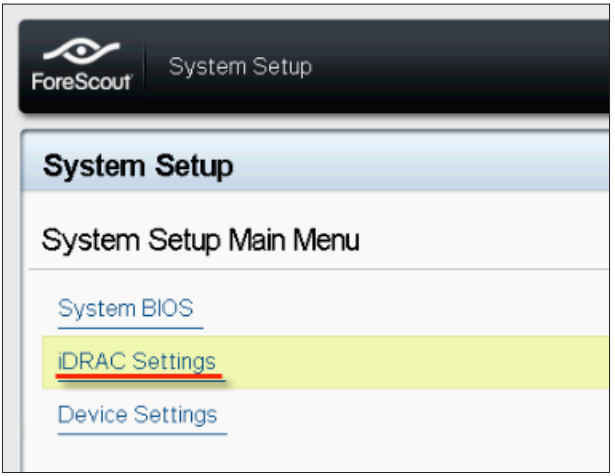
- *Habilite y configure el módulo iDRAC.*
- *Conecte el módulo a la red*
- *Inicie sesión en iDRAC*

Habilite y configure el módulo iDRAC

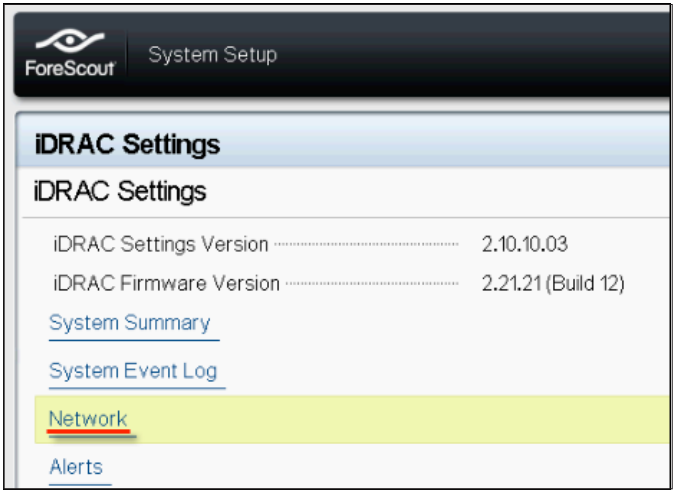
Cambie las configuraciones de iDRAC parta habilitar el acceso remoto en el dispositivo CounterACT. Esta sección describe los ajustes de integración básica necesaria para trabajar con CounterACT.

Para configurar iDRAC:

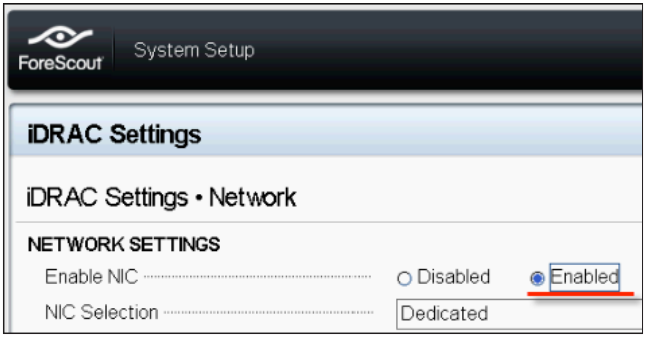
1. Encienda el sistema administrado.
2. Seleccione F2 durante la Prueba Automática de Encendido (POST, por su siglas en inglés).
3. En la página Menú Principal de la Configuración del Sistema, seleccione los **Ajustes de iDRAC**.



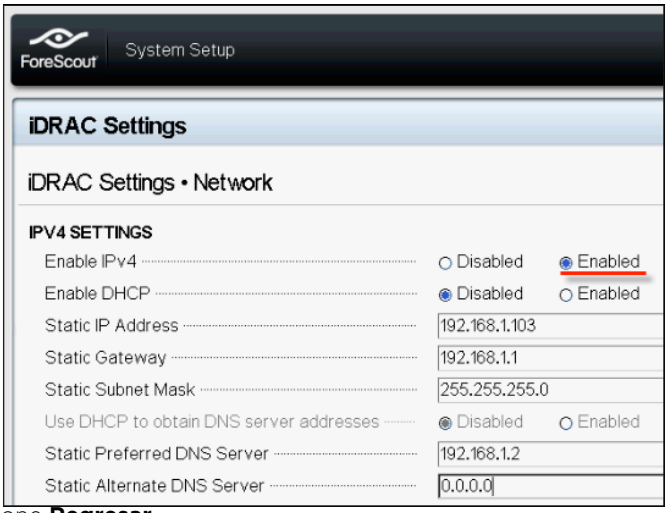
4. En la página de Ajustes de iDRAC, seleccione **Red.**



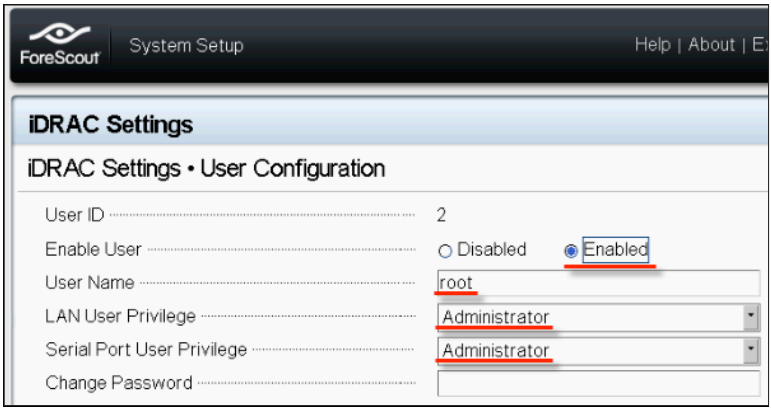
5. Configure los siguientes ajustes de la Red:
   - ***Ajustes de la Red.*** Verifique que el campo **Habilitar NIC** esté **Habilitado**.



   - ***Ajustes comunes.*** En el campo Nombre de DNS DRAC, puede actualizar un DNS dinámico (opcional).
   - ***Ajustes de IPV4.*** Verifique que el campo **Habilitar IPv4** esté **Habilitado**. Marque el campo **Habilitar DHCP** como **Habilitado** para usar la Dirección de IP Dinámica o como Deshabilitado para usar la Dirección de IP Estática. Si está habilitado, el DHCP automáticamente asignará la dirección de IP, la pasarela y la máscara de subred a iDRAC7. Si se desactiva, ingrese los valores para los campos de **Dirección de IP Estática, Pasarela Estática** y **Máscara de Subred Estática**.



6. Seleccione **Regresar.**
7. Seleccione **Configuración del Usuario**.
8. Configure los siguientes campos de Configuración del Usuario:
   - ***Habilite el usuario***. Verifique que este campo esté configurado a Habilitado.
   - ***Nombre del usuario***. Ingrese un nombre de usuario.
   - ***Privilegios de Usuario de Puerto en Serie y LAN***. Establezca los niveles de privilegio al Administrador.
   - ***Cambie la contraseña***. Establezca una contraseña para iniciar sesión con el usuario.



9. Seleccione **Regresar** y luego selecciones **Finalizar**. Confirme los ajustes cambiados. Se guardan los ajustes de la red y el sistema se reinicia.

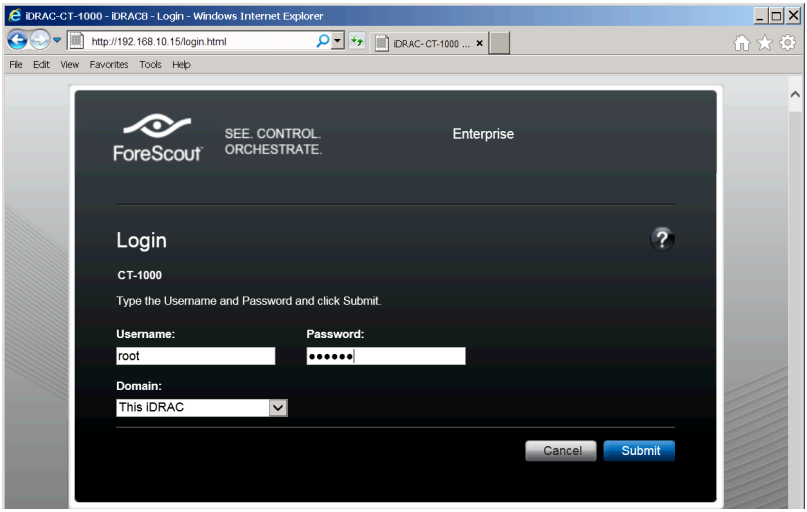
Conecte el módulo a la red

El iDRAC se conecta a una red de Ethernet. Es común que se conecte a una red de administración. La siguiente imagen muestra la ubicación del puerto iDRAC en el panel trasero del equipo CT-1000:

Inicie sesión en iDRAC

Para iniciar sesión en iDRAC:

1. Navegue por la dirección de IP o el nombre de dominio configurado en **Ajustes de iDRAC > Red.**



2. Ingrese el Nombre de usuario y la Contraseña configurada en la página de Configuración del Usuario de la configuración del sistema iDRAC.
3. Seleccione **Enviar.**

Para más información sobre iDRAC, consulte la Guía del Usuario de iDRAC.

Es muy importante actualizar las credenciales predeterminadas.

6. Verificación de conectividad

Verificar la conexión de la interfaz de administración

Para probar la conexión de la interfaz de administración, inicie sesión en el equipo y ejecute el siguiente comando:

`fstool linktest`

Aparecerá la siguiente información:

```
Estado de la interfaz de administración
Rastreo de la información de la pasarela predeterminada
Estadística de rastreo
Llevando a cabo la prueba de resolución de nombre
Resumen de la prueba
```

Verificar la conectividad del interruptor/equipo

Verifique que el interruptor esté correctamente conectado al equipo antes de salir del centro de datos. Para hacerlo, ejecute el comando `fstool ifcount` en el equipo para cada interfaz detectada.

`fstool ifcount eth0 eth1 eth2`
(Separe cada interfaz con un espacio).

Esta herramienta continuamente muestra el tráfico de la red en las interfaces especificadas. Funciona de dos modos: por interfaz o por VLAN. El modo puede cambiarse desde la pantalla. Se muestran los bits totales por segundo y el porcentaje de cada una de las siguientes categorías de tráfico:

- La interfaz de monitoreo debe principalmente ver el tráfico reflejado — por encima del 90%.
- La interfaz de respuesta debe ver principalmente el tráfico transmitido.
- La interfaz de respuesta y el monitor deben ver las VLAN esperadas.

Opciones de comando:

`v – se muestra en modo VLAN`
`I – se muestra en modo interfaz`
`P – se muestra lo anterior`
`N – se muestra lo siguiente`
`q – salir`

Modo VLAN:

```
actualizar=[4]  [eth3: 14 vlans]
IInterfaz/Vlan Total transmitidas duplicadas *Desde mi MAC *Hacia
mi MAC
eth3.untagged   4Mbps   0.2%       99.8%     0.0%        0.0%
eth3.1          9Mbps   0.0%       100.0%    0.0%        0.0%
eth3.2          3Mbps   0.1%       99.9%     0.0%        0.0%
eth3.4          542bps  100.0%     0.0%      0.0%        0.0%
eth3.20         1Kbps   100.0%     0.0%      0.0%        0.0%
Muestra [v]lans [i]nterfaces <-[p]rev [n]ext->      [q]uit
```

Modo interfaz:

```
actualizar=[31]         [eth0: 32 vlans] [eth1: 1 vlans]
Interface     Total     transmitidas  reflejadas    *Desde     *Hacia
                                                    mi MAC     mi MAC
eth0          3Kbps     42.3%         0.0%          14.1%      43.7%
eth1          475bps    0.0%          100.0%        0.0%       0.0%
```

*Hacia mi MAC — Destino MAC es la MAC del equipo.

*Desde mi MAC — Tráfico enviado por este equipo (la fuente MAC es la MAC del equipo. Destino puede ser transmisión o unidifusión).

Si no ve tráfico, verifique que la interfaz esté activa. Use el siguiente comando en el equipo:

`ifconfig [nombre de la interfaz] activa`

Realizar la prueba de rastreo

Ejecute la prueba de rastreo desde el equipo al escritorio de la red para verificar la conectividad.

Para ejecutar la prueba:

1. Inicie sesión en el equipo.
2. Ejecute el siguiente comando: **`Rastreo [IP del escritorio de la red]`** Por defecto, el equipo mismo no responde al rastreo.

7. Configure la consola de CounterACT

Instale la consola de CounterACT

La consola de CounterACT es una aplicación de administración central que se usa para visualizar, registrar y analizar la actividad que detecta el equipo. NAC, Threat Protection, Firewall y otras políticas pueden definirse desde la consola. Consulte el *Manual del usuario de la Consola de CounterACT* para más información.

Debe suministrar una máquina para alojar el software de aplicación de la Consola CounterACT. Los requisitos mínimos de hardware son:

- Máquinas no dedicadas, en funcionamiento:
  - Windows XP, Windows Vista o Windows 7
  - Windows Server 2003 o Server 2008
  - Linux
- Pentium 3, 1GHz
- Memoria de 2GB
- Espacio en disco de 1GB

Hay dos métodos disponibles para realizar la instalación de la consola:

Use el software de instalación incorporado en su equipo.

1. Abra una ventana del navegador desde la computadora de la consola.
2. Ingrese lo siguiente en la línea de la dirección del navegador
   `http://<Appliance ip>/install`
   Donde <Appliance ip> es la dirección de IP de este equipo. El navegador mostrará la ventana de instalación de la consola.
3. Siga las instrucciones que aparecen en la pantalla.

Instale desde el CD-ROM de CounterACT

1. Inserte el CD ROM de CounterACT en la unidad de DVD.
2. Abra el archivo **`ManagementSetup.htm`** desde el CD ROM con un navegador.
3. Siga las instrucciones que aparecen en la pantalla.

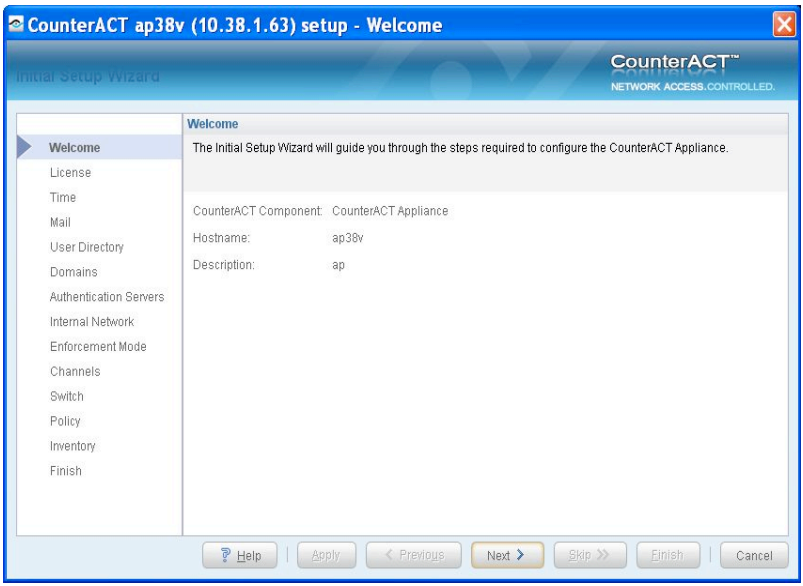
Inicie sesión

Luego de completar la instalación, puede iniciar sesión en la consola de CounterACT.

1. Seleccione el icono de CounterACT desde la ubicación del atajo que creó.
2. Ingrese la dirección de IP o nombre del host del equipo en el campo **IP/Nombre.**
3. En el campo **Nombre de usuario,** ingrese **admin**.
4. En el campo **Contraseña,** ingrese la contraseña que usted creó durante la instalación del equipo.
5. Seleccione **Iniciar sesión** para lanzar la consola.

Configuración inicial

Luego de iniciar sesión por primera vez, aparecerá el Asistente de configuración inicial. El Asistente lo guiará por los pasos esenciales de configuración para garantizar que CounterACT esté funcionando de manera rápida y eficiente.



Antes de comenzar con la Configuración inicial

Prepare la siguiente información antes de trabajar con el Asistente:

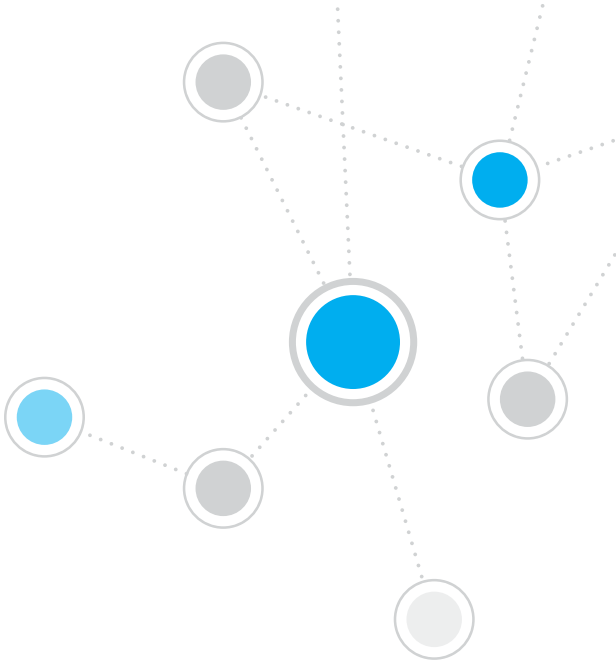
Información	Valores
☐ Direcciones de servidor NTP que usa su organización (opcional).	
☐ Dirección de IP de relé de correo interno. Esto permite la entrega de correo electrónico desde CounterACT si el tráfico SMTP no está permitido desde el equipo (opcional).	
☐ Dirección de correo electrónico del administrador de CounterACT.	
☐ Designaciones de interfaz de respuesta y control definidos en el Centro de Datos.	
☐ Para segmentos o VLAN sin DHCP, el segmento de la red o VLAN a la que la interfaz de monitoreo está directamente conectada y una dirección de IP permanente a ser usada por CounterACT en cada VLAN. Esta información no es necesaria para la configuración del Administrador Corporativo.	
☐ Variaciones de la dirección de IP que el equipo protegerá (todas las direcciones internas, incluyendo las direcciones no usadas).	
☐ La información de la cuenta del Directorio del Usuario y la dirección de IP del servidor del Directorio del Usuario.	
☐ Credenciales de dominio, incluyendo la contraseña y nombre de la cuenta administrativa del dominio.	
☐ Servidores de autenticación para que CounterACT pueda analizar qué hosts de red se han autenticado exitosamente.	
☐ Dirección de IP del interruptor central, proveedor y parámetros de SNMP.	

Consulte el *Manual del Usuario de la Consola de CounterACT* o la Ayuda en línea para recibir información sobre cómo trabajar con el Asistente.

Información de contacto

Si necesita soporte técnico de ForeScout envíe un correo electrónico a support@forescout.com o llame:

- Línea gratuita (EE. UU.): 1.866.377.8771
- Teléfono (internacional): 1.408.213.3191
- Soporte técnico: 1.708.237.6591
- Fax: 1.408.371.2284



ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Línea gratuita (EE. UU.): +1-866-377-8771
Teléfono (internacional): +1-408-213-3191
Soporte técnico: +1-708-237-6591
Fax +1-408-371-2284

400-00020-01