Limpie el servidor de acceso FAQ

Contenido

Introducción

Este documento trata sobre las preguntas más frecuentes (FAQ) relacionadas con Cisco Clean Access Server (antes Perfigo SecureSmart Server).

Los nombres del producto han cambiado. Esta tabla enumera los nombres anteriores y los nuevos nombres:

Viejo nombre	Nuevo nombre
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPIs	Clean Access APIs

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Instalación

Q. ¿Cómo instalo los driveres SCSI LSI para Dell 1750 u otros?

A. Complete estos pasos:

1. Salve el archivo del rawrite a C:\ y al driver LSI. Ponga al día los archivos en el mismo directorio.

2. Abra un comando prompt y ingrese **C:\rawrite**.
3. Ingrese el nombre completo del archivo de origen y del destino encendido a dos disquetes.
4. Inserte las máquinas limpias del Access Manager (antes CleanMachines) CD de instalación en el servidor de acceso limpio de Cisco o el Access Manager limpio de Cisco.
5. Ingrese la **aduana** en el prompt del `boot>`.
6. Siga las instrucciones de ingresar el disco de la actualización, y entonces el disco del driver.

Configuración

Q. ¿Cómo configuro los driveres Broadcom?

A. Complete estos pasos:

1. Consola en el cuadro: `cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/bcm5700`

   `insmod ./bcm5700.o`
2. Si el paso 1 da lugar a ningunos errores, ingrese el comando de **VI /etc/modules.conf** y agregue estas dos líneas: `alias eth0 bcm5700`

   `alias eth1 bcm5700`

Q. ¿Cómo configuro el servidor de acceso limpio de Cisco detrás de un gateway de NAT?

A. Complete estos pasos para cada servidor de acceso limpio de Cisco desplegado detrás de un gateway de NAT.

1. SSH al servidor SecureSmart o utiliza una consola en serie para iniciar sesión como raíz.
2. Edite el archivo de **/perfigo/access/bin/starttomcat**.
3. Añada al final del fichero **- Djava.rmi.server.hostname=<CAS_hostname> a la** línea **CATALINA_OPTS** variable.
4. **Reinicio del perfigo del servicio del** reinicio.
5. SSH al SmartManager o utiliza una consola en serie para iniciar sesión como raíz.
6. Edite el archivo de **/etc/hosts** y añada esta línea al final del fichero: `<public_IP_address> <securesmart_hostname> <securesmart_hostname>`

Duplex y configuraciones de la velocidad

Q. ¿Cómo fijo el duplex y la velocidad en el Network Interface Cards limpio del servidor de acceso de Cisco?

A. Utilice esto como guía para configurar el Network Interface Cards apropiado en el archivo de /etc/modules.conf.

Nota: Añada los parámetros de opciones al final del fichero en el extremo para el archivo de /etc/modules.conf con el uso del editor de Vi.

- Fije los indicadores luminosos LED amarillo de la placa muestra gravedad menor del

broadcom 5700 al 100 Mbps llenos - duplex:
options bcm5700 line_speed=100,100 auto_speed=0,0 duplex=1,1

- Fije los indicadores luminosos LED amarillo de la placa muestra gravedad menor del broadcom 5700 al 1000 Mbps llenos - duplex:
options bcm5700 line_speed=1000,1000 auto_speed=0,0 duplex=1,1
- Fije los indicadores luminosos LED amarillo de la placa muestra gravedad menor e1000 al 100 Mbps llenos - duplex:
options e1000 Speed=100,100 Duplex=2,2
- Fije los indicadores luminosos LED amarillo de la placa muestra gravedad menor e1000 al 1000 Mbps llenos - duplex:
options e1000 Speed=1000,1000 Duplex=2,2
- Fije los indicadores luminosos LED amarillo de la placa muestra gravedad menor eepro100 al 100 Mbps llenos - duplex:
options eepro100 option="0x30,0x30"

Q. ¿Cómo fijo el duplex/la velocidad en la interfaz de acceso limpia el "bnx2" de Cisco?

A. En los dispositivos limpios del servidor de acceso de Cisco (incluso en el CAM), hay los archivos para cada interfaz de la red que describen las propiedades y las configuraciones dúplex/velocidades.

Aquí están los pasos cómo realizarla manualmente:

1. Cambie el directorio a **/etc/sysconfig/network-scripts**. Para cada interfaz hay un archivo en este directorio nombrado ifcfg-ethX, donde X puede ser 0, 1, 2, etc.
2. Agregue esta línea para cualquier interfaz usted quiere poner en hard-code las configuraciones: `ETHTOOL_OPTS="speed 100 duplex full autoneg off"`
3. Después de que guarde el archivo, realice “un reinicio de la red de servicio”.
4. Aseegurese las configuraciones del switch se fijan manualmente. Marque sus configuraciones publicando el comando del **ethX de la Eth-herramienta** en el shell, donde X puede ser 0 o 1 para confirmar las configuraciones dúplex está puesto en hard-code.
Nota: Esto interrumpe el servicio momentáneamente. Mantenga esto la consideración si usted tiene que programar un tiempo muerto.

Q. ¿Cómo marco para ver el duplex y la velocidad en el Network Interface Cards limpio del servidor de acceso de Cisco (NIC)?

A. Funcione con la utilidad de la MII-**herramienta de la** línea de comando. Trabaja para el NIC a bordo, pero no soporta la fibra NIC.

Para la fibra NIC, utilice el **comando grep 'eth0'** en /var/log/messages.

Usted puede también publicar un **comando tail -f** en /var/log/messages. Esto visualiza los mensajes siempre que un NIC llegue a estar activo o inactivo.

Características admitidas

Q. ¿Cuál es el número de conexiones VPN soportadas por el servidor de acceso

limpio de Cisco?

A. No se pone ningún límite para el IPSec.

El PPTP y el L2TP se fijan actualmente a 32 hace un túnel cada uno.

Q. ¿Cómo cambio la dirección IP del servidor de acceso limpio de Cisco? ¿Necesito borrar y re-agregar el servidor de acceso limpio de Cisco?

A. Cisco recomienda que usted cambia la dirección IP del servidor de acceso limpio de Cisco vía el administrador UI. Cuando la dirección IP del servidor de acceso limpio de Cisco se cambia del administrador UI, reinicie el servidor de acceso limpio de Cisco. Intenta automáticamente conectar con Cisco el Access Manager limpio sobre la reinicialización. El Access Manager limpio de Cisco cambia la dirección IP del servidor de acceso limpio de Cisco en la base de datos y el SSKEY sigue siendo lo mismo.

Nota: Si usted borra y re-agrega el servidor de acceso limpio de Cisco, usted pierde todos los ajustes de la configuración del servidor de acceso limpio de Cisco.

Q. ¿Cómo limito el acceso SSH al Cisco Clean Access Server?

A. Agregue una línea similar a este ejemplo para cambiar el archivo de **/etc/ssh/sshd_config**:

```
ListenAddress IP_address_of_where_you_want_ssh_to_allow_connections
```

Por ejemplo:

```
ListenAddress 192.168.151.60
```

Publique el **comando service sshd restart** para recomenzar el proceso del SSHD.

Q. ¿Cómo la configuración de ráfaga del ancho de banda trabaja?

A. Bajo el CleanMachines, desmarque **Windows todo** y seleccione cada OS independientemente para el uso Require del SmartEnforcer o no.

Q. Leo recientemente adentro la versión limpia 3.3BETA de la instalación y de la guía de administración del servidor de acceso en la página 68 que el máximo recomendado de número de subredes por el servidor de acceso limpio es 1000. Necesito crear más de 1000. ¿Cuál es el límite?

A. El límite de 1000 es una advertencia solamente. Si la máquina tiene bastante memoria (más que 1G), usted puede configurar hasta 2500 subredes.

Q. Cómo manejo un lote de Puntos de acceso que tenga en un VLA N específico que sea manejado por el servidor de acceso limpio. ¿Los he agregado en la Administración de dispositivos del Punto de acceso?

A. Agregue las direcciones MAC de los Puntos de acceso al área de los **>Devices de los filtros** en comparación con la sección de Administración de dispositivos del Punto de acceso.

Q. Tengo subredes secundarias (secundario a veces múltiple) en cada VLA N. La subred 150 está para los clientes, y la subred 172 está para la Administración de nuestro engranaje del establecimiento de una red en el edificio. ¿Puede el servidor de acceso limpio ocuparse de las subredes múltiples en un solo VLA N?

A. Un ejemplo de este problema es:

```
!
  interface Vlan 106
   ip address 150.135.47.1 255.255.255.0
   ip address 172.16.10.1 255.255.255.192 secondary
  !
```

El servidor de acceso limpio está en el modo de gateway virtual:

- En este caso, el servidor de acceso limpio no cuida sobre el número de subredes o de sus etiquetas asociadas del VLA N. Todos los pasos de la información de VLAN a través sin las excepciones.

El servidor de acceso limpio está en un modo del gateway (real-IP o NAT):

- En este caso, el servidor de acceso limpio también funciona como un relé DHCP o un servidor DHCP. En la situación, el rango de los IP Addresses afectado un aparato depende de la etiqueta del VLA N o de la dirección del gateway que también depende de la etiqueta del VLA N.Por lo tanto, el servidor de acceso limpio no puede distinguir (desde un punto de vista del DHCP) entre dos subredes en el mismo VLA N. La una limitación es que una de las dos subredes en el mismo VLA N no debe utilizar el DHCP para la asignación de dirección. En lugar, la necesidad de los IP Addresses de ser asignado estáticamente. Esto es más probable el caso para la subred 172 en la red puesto que consiste en el engranaje de la red.

Q. ¿Por qué no puedo agregar el servidor de acceso limpio al Access Manager limpio (CAM)?

A. Si usted no puede agregar el servidor de acceso limpio al CAM, después esto es una emisión de la licencia. Aseegurese que las licencias del servidor están generadas sobre la base de la dirección MAC del ethernet0 CAM primario. Las direcciones MAC en la licencia del servidor deben hacer juego la dirección MAC (primaria) del CAM.

1. Van al **CAM EL GUI > la administración > Access Manager limpio > autorizando**.
2. Realice “quitan todas las licencias”.
3. Reinstale los archivos de la licencia del servidor otra vez.

Q. ¿Debo generar un nuevo CSR para renovar el certificado en el servidor de acceso limpio?

A. No. Para la renovación del certificado en el servidor de acceso limpio, no genere un nuevo CSR. Sin embargo, si usted está generando un nuevo CSR, después usted tiene que cargar la clave privada en el servidor de acceso limpio. Después de cargar la clave privada, reinicie el servidor de acceso limpio. Esto completa el proceso de renovación.

Q. ¿Es posible pasar a través del tráfico Multicast a través CCA?

A. No, Multicast no se soporta bajo el gateway real inband. Sin embargo, trabajará para el gateway fuera de banda o virtual.

Q. ¿El NAC soporta el servidor 64-bit de Windows 2008?

A. No, pero él soporta el servidor de 32 bits de Windows 2008.

Q. ¿El NAC incluye una característica para duplicar los rol del usuario y las directivas/las propiedades asociadas a ella a un papel de usuario nuevo?

A. No. Esto no puede ser hecha pues no hay tal disposición en el GUI.

Mensajes del registro

Q. En /var/log/messages o los mensajes de /var/log/ha-log veo varios mensajes de latido para la Conmutación por falla. ¿Por qué es esto y cómo lo reparo?

A. Éstos son los mensajes de latido que usted ve:

```
heartbeat: 2004/09/15_11:23:27 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_14:19:17 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_18:59:53 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_19:36:18 info: Heartbeat restart on node ss1
```

Usted ve estos mensajes cuando el servidor de peer está para arriba después de una reinicialización. Usted puede también verla en el inicio el servidor primario cuando:

- Usted publica la **parada del perfigo del servicio** y después **mantiene el comienzo del perfigo** en el par o la máquina espera.o
- Reinicie un par o una máquina espera.

Nota: Cuando usted publica el **comando service perfigo restart**, no acciona este registro.

Q. Veo las Estadísticas del sistema limpias del servidor de acceso 2004-08-30 11:30:28 192.168.151.60: Factor de carga 0 (máximo desde la reinicialización: 3) mem: 261160960 237854720 23306240 212992 47259648 99737600 CPU 188552 153 91405324 194183 mensajes en mis registros de acontecimientos. ¿Qué él significa?

A. Las estadísticas del sistema se generan para cada servidor de acceso limpio manejado por el Access Manager limpio cada hora por abandono. La información proporcionada incluye el Factor de carga de cada servidor, la carga máxima desde la reinicialización, la memoria, y el USO de la CPU.

- **Factor de carga** — El Factor de carga es un número que describe el número de paquetes que esperen para ser procesados por el servidor (por ejemplo, la carga actual que es manejada por el servidor de acceso limpio). Cuando el Factor de carga crece, es una indicación que los paquetes están esperando en la cola que se procesará. Si el Factor de carga es mayor de

500 para cualquier período de tiempo constante (por ejemplo, 5 minutos), después es indicativo que el servidor de acceso limpio tiene una mucha carga constante del tráfico/de los paquetes que vienen adentro. Usted necesita ser referido si el número alcanza 500 o el más alto.
- **Máximo desde la reinicialización** — La cantidad máxima de paquete en la cola a cualquier momento (por ejemplo, la carga máxima manejada por el servidor de acceso limpio).
- **Mem** — Las estadísticas del uso de la memoria. Hay seis números (la unidad es bytes). Estos números representan el total, utilizado, libre, compartido, los buffers, y memoria ocult0.
- **CPU** — La carga del procesador en el hardware. Hay cuatro números que proporcionan la información sobre el USO de la CPU (la unidad es segunditos - en la mayoría de los sistemas, un segundito es una unidad de tiempo de 10 ms). Los números indican el tiempo pasado por el sistema en el usuario, agradable, el sistema, y los procesos ociosos.

Por el ejemplo proporcionó, sistema % = 91405324*100/(188552+153+91405324+194183) = 99.58%. Semejantemente, usted puede calcular los otros también. Sin embargo, en un servidor de acceso limpio, el Tiempo del sistema es típicamente mayor del 90 por ciento. Ésta es la muestra de un sistema saludable.

Mensajes de error

Q. ¿Por qué recibo `no puedo agregar el` mensaje de error `limpio del servidor de acceso`?

A. Marque estos elementos:

- El secreto compartido es lo mismo en el servidor de acceso limpio de Cisco y el Access Manager limpio de Cisco.
- Los Certificados están correctos.
- La Conectividad entre el servidor de acceso limpio de Cisco y el Access Manager limpio y el ése de Cisco allí no es ninguna reglas de firewall que bloquean los puertos RMI.

Q. Porqué recibo el `Error de red de CAS: El servidor de acceso limpio no podía establecer una conexión segura para limpiar el Access Manager en la falta de información.` ?

A. Usted puede ser que reciba este error si el certificado limpio del Access Manager ha expirado, no se puede confiar en, ni puede ser alcanzado. El error es básicamente debido a los problemas de comunicación de CAS o CAM.

Para resolver el problema, verifique estos elementos:

- Aseegurese CAS y el CAM es la misma versión.
- Si usted utiliza un nombre para el certificado, aseegurese el nombre puede ser resuelto usando el nslookup.
- Utilice el IP del servicio para el certificado de la Conmutación por falla.
- Aseegurese los son tiempo sincronizado antes de generar el certificado.
- Aseegurese la coincidencia de los secretos compartidos.
- El Firewall no debe bloque ACL ninguna comunicación SSL.
- Agregue el certificado CAM como raíz no estándar a CAS.
- Marque para saber si hay resolución de nombre DNS.
- Aseegurese la encaminamiento para el accesibilidad entre el CAM y CAS está correcto.

Q. ¿Por qué recibo el **error encontrado mientras que la Cadena de certificados constructiva X509… no puede encontrar el certificado para el** mensaje de error **siguiente del Certificate Authority**?

A. Usted debe utilizar el certificado raíz correcto. Si se utiliza Microsoft Certificate Authority (CA), salve el certificado en el base64 bastante que el valor por defecto codificado.

Q. Consigo el error de comunicación del servidor de la autenticación 2004-11-01 15:53:40, el baronet de 172.19.168.42 del ## [00:0E:35:5F:F9:91] y el error de comunicación del servidor de la autenticación 2004-11-01 15:53:13, los errores bart de 172.19.168.42 del ## [00:0E:35:5F:F9:91] en los registros de acontecimientos. ¿Cómo resuelvo este problema?

A. Si usted funciona con el servidor de acceso limpio de la Conmutación por falla en el modo de gateway virtual, después edite el archivo de VI /etc/hosts y cambie (servidor de acceso limpio) el direccionamiento SS-1 al IP del servicio (dirección virtual). Usted necesita cambiarlos en ambos limpia el Access Servers, el active y el recurso seguro.

- localhost del localhost de 127.0.0.1
- 192.168.1.2 SS-1 SS-1

Q. Consigo la firma de la pila de TCP/IP: Mensaje DESCONOCIDO el DESCONOCIDO [65535:64:1:64:M1460,N,W2,N,N,T0,S,E:P] {}. ¿Cómo reparo esto y cómo puedo inhabilitar instalo del cliente para los iPhones?

A. Aquí están las instrucciones que deben trabajar para no requerir el agente para los iPhones:

1. Elija el papel bajo **acceso limpio > configuración > login generales del agente**.
2. Elija **MAC_ALL** configurar los requisitos del agente para el iPhone o el tacto de iPod. Aseegurese el **uso TODAS LAS configuraciones** para la familia del MAC OS si no se especifica se desmarcan ningunas configuraciones versión-específicas, así que no utiliza la configuración compartida de “TODOS”. También, aseegurese el agente del requerir que se desmarca la opción de la transferencia, así que el servidor de acceso limpio no pedirá que el cliente (iPhone/tacto de iPod) descargue el agente.
3. Elija **MAC_OSX** configurar los requisitos del agente para el MAC OS. Usted puede marcar **TODA LA opción Settings** o desmarcarla para configurar este OS específico. La opción de la transferencia del agente del requerir debe ser marcada si usted quisiera que los usuarios regulares del MAC OS descargaran el agente MAC.

Q. Usted puede ser que reciba este mensaje de error: **Error: Carga fallada. Esto certificado firmado por CA no hace juego la clave privada en la base de datos dominante.** ¿Cómo puedo solucionar esto?

A. Para resolver el problema, complete estos pasos:

1. Genere un CSR.
2. Salve la clave privada.
3. Cargue el nuevo certificado con la clave privada guardada.

Q. Recibí este mensaje de error: **Registro del servidor del invitado del NAC: usuario _SYSTEM_ (- 172.16.98.9) que intenta autenticar de la ubicación no válida: XXX@YYY.com 2011 15-Jan-2010 11:41:44.** ¿Cómo puedo resolver este error?

A. Este problema releated para introducir errores de funcionamiento CSCsq86376 (clientes registrados solamente) y aparecería si usted no está utilizando los IP Addresses en sus paquetes RADIUS del WLC.

Q. Recibí este meaage del error mientras que actualiza CAS con el CD: **"El error entrada-salida del buffer en el dispositivo tenía, bloque lógico".** ¿Cómo puedo resolver este error?

A. Este problema ocurre cuando se corrompe el CD o se quema generalmente en la velocidad. Con un ISO más grande el CD no se debe quemar en más que la velocidad 10X o 8X.

Q. Usted puede ser que reciba este mensaje de error cuando usted conecta el CAM con CAS: **Error: RMISocketFactory: Crear el socket RMI no pudo recibir.** ¿Cómo se resuelve este problema?

A. Este mensaje de error pudo ocurrir debido a las versiones unidas mal en el CAM y CAS o debido a los Certificados unidos mal o al secreto compartido usado. Para más información sobre cómo resolver los problemas del certificado, refiera al NAC (CCA): Cómo reparar los errores del certificado en el CAM/CAS después de la actualización a 4.1.6.

Q. Recibí este mensaje de error: **El emisor del certificado para este sitio es untrusted o desconocido. ¿Usted desea proceder?** ¿Cómo puedo resolver este error?

A. Este mensaje aparece porque el certificado usado en CAS uno mismo-**se publica** y no se salva en el almacén de certificados de los clientes. Este error puede ser resuelto cargando un certificado de un vendedor externo (tal como Verisign, confíe, etc.) que se conozca ya a las máquinas del cliente. Esto requiere la compra de un certificado a partir del uno de estos vendedores y instalarlo en CAS, o usted puede utilizar su propio Certificate Authority (sin embargo, usted necesita instalar manualmente el certificado de CA de esto en cada cliente).

Nota: Reinstalar el certificado en CAS requiere la eliminación de él y re-agregarlo al CAM. Esto puede ser perturbador a su red. Esto se recomienda altamente solamente cuando hay una ventana posible de la caída del sistema.

Miscelánea

Q. El servicio limpio del DHCP del servidor de acceso no recomienza o de vez en cuando las paradas. ¿Qué necesita ser hecha?

A. Las configuraciones del DHCP *se compilan* en el servidor de acceso limpio. Estas configuraciones compiladas pueden a veces corromperse, especialmente después de una actualización al software del Access Server limpio. La solución es forzar el servidor de acceso limpio al recompile las configuraciones. Para hacer esto, realice un cambio, y haga clic la **actualización**.

Síntomas:

El servidor DHCP no comienza, o falla de vez en cuando en el servidor de acceso limpio.

Instrucciones:

1. Si la daemon del DHCP del servidor no comienza, vaya al administrador, abren a ese servidor determinado, y el tecleo **maneja**.
2. Seleccione la **red > el DHCP > la lista de la subred**, y el tecleo **edita** para una de las listas de la subred.
3. Realice cualquier cambio a la subred (por ejemplo, aumente el Tiempo de validez en 1 minuto), y haga clic la **actualización**.
4. Vuelva a la página del estatus y vea si el servicio del DHCP ha comenzado. En este momento las configuraciones del DHCP se deben compilar otra vez.

Nota: Otra situación que puede hacer al servidor DHCP no comenzar está solapando las configuraciones de subred. Comprobación para esto también.

Q. Configuré el temporizador Heartbeat (de latido) para terminar una sesión un dispositivo el sistema después de una cierta hora inactiva. En el registro de acontecimientos, estado que no puede hacer ping el dispositivo pero el dispositivo continúa pasando el tráfico hacia adelante y hacia atrás. ¿Cómo resuelvo este problema?

A. Éste es un ejemplo del error:

```
Authentication  2004-08-26 12:13:48
Unable to ping 149.151.206.251, going to logout user user1
```

Marque para ver si el dispositivo tiene algunos escudos de protección incorporados que bloqueen los paquetes ARP del servidor de acceso limpio de Cisco. El servidor de acceso limpio de Cisco realiza el ping ARP. Esto es un mensaje ARP y no debe ser bloqueado.

Q. Configuré el temporizador Heartbeat (de latido) de modo que un dispositivo termine una sesión el sistema después de un cierto período de inactividad. En el registro de acontecimientos, estado que no puede hacer ping el dispositivo pero el dispositivo todavía pasa el tráfico hacia adelante y hacia atrás. ¿Cómo resuelvo este problema?

A. Aseegurese que usted configura un puerto serial para la conexión de recuperación tras falla.

Si el ordenador que funciona con el software del Access Server limpio de Cisco tiene dos puertos seriales, usted puede utilizar el puerto adicional para la conexión de cable serial. Por abandono, el primer conector serial detectado en el servidor se configura para la entrada-salida de la consola (facilitar la instalación y otros tipos de acceso administrativo). Si el ordenador tiene solamente un puerto serial (ttyS0) y usted no se prepone utilizarlo para el acceso administrativo, usted puede configurar de nuevo el puerto para servir como la conexión de recuperación tras falla.

Complete estos pasos para configurar de nuevo el ttyS0 como la conexión de latido:

1. De un cliente SSH, acceda el servidor de acceso limpio de Cisco como usuario raíz.
2. Edite **/etc/lilo.conf** y quítelo o comente hacia fuera la línea más reciente:

`append="console=ttyS0....."` Esta línea hace la salida de la consola ser reorientada al puerto serial. **Nota:** Agregue a **#** carácter al comienzo de la línea para comentar hacia fuera una línea. Se ignoran las líneas que comienzan con este carácter.
3. Edite **/etc/inittab** y quítelo o comente hacia fuera la línea más reciente: `co:2345:respawn ...vt100`Esta línea hace un terminal de inicio comenzar en el puerto serial.
4. **Lilo** y Presione ENTER del tipo en el comando prompt. Esto comienza a Lilo, el cargador de arranque de Linux.
5. Ingrese el **comando reboot** de reiniciar el ordenador.
6. Relance los pasos en el servidor de acceso limpio de Cisco del par de la Conmutación por falla.

Q. ¡Cuánto tiempo lo hace para tomar al Cisco el Access Manager limpio (antes SmartManager) para medir el tiempo hacia fuera del servidor de acceso limpio de Cisco y para el **SecureSmart 2004-08-26 12:26:42 192.168.1.1 es inaccesible!** ¿mensaje a visualizar?

A. El Access Manager limpio de Cisco lleva a tres minutos el descanso cada servidor de acceso limpio de Cisco antes de que visualice el estatus no conectado.

Q. ¿Cuál es el impacto de cambiar el Network Interface Cards (NIC) en el servidor de acceso limpio de Cisco?

A. Si usted tiene una licencia del NON-sitio, usted no necesita informar al Soporte técnico de Cisco el cambio en la dirección MAC. Usted necesita solamente informar al Soporte técnico de Cisco cuando su número de Access Servers limpio cambia. Si usted tiene una licencia del sitio, usted no necesita informar al Soporte técnico de Cisco.

Q. Puedo conseguir una dirección IP del servidor DHCP limpio del acceso, pero después de ese, continúo viendo una “página no encontrar” el mensaje cuando intento abrir a un navegador en una dirección externa. Me nunca reorientaron a la página de registro de la red. ¿Por qué ocurre esto?

A. Usted puede experimentar uno de estos problemas:

- El DNS del servidor de acceso limpio de Cisco no se fija en el servidor DNS.Le reorientan al nombre DNS para la página de registro de la red. Usted pudo no haber asociado securesmart.company.com a 192.168.0.1 en su entrada DNS.
- El certificado utiliza el nombre DNS.No han asociado las aplicaciones securesmart.company.com del certificado sino al servidor DNS al nombre. La validación de la certificación falla.
- El certificado se crea o es incorrectamente inválido. Marque para ver **/perfigo/access/apache/logs/error_log**. Si usted ve estos errores, reconstruya su certificado SSL.`[root@securesmart logs]# cat error_log`

```
[Thu Sep 16 18:00:04 2004] [error] Unable to configure RSA
server private key

[Thu Sep 16 18:00:04 2004] [error] SSL Library Error:
185073780 error:0B080074:x509 certificate routines:
```

`X509_check_private_key:key values mismatch`**Nota:** ¿Refiérase a [donde están los archivos del registro en el Access Manager limpio?] para todos los archivos del registro.

- El httpd no se comienza. Marque para ver si el HTTP se comienza con el **netstat - al |** comando **HTTP del grep**. Usted debe ver este anuncio. Si no, publique el **comando service perfigo restart**.`tcp 0 0 *:http *:* LISTEN`

  `tcp 0 0 *:https *:* LISTEN`

Q. ¿Necesito poner al día cualquier cosa después de que substituya un servidor de acceso limpio defectuoso de Cisco?

A. A veces, el ss_key es no más lo mismo. Complete estos pasos.

1. SSH al Access Manager limpio de Cisco y obtiene el **ss_key**.
2. Publique el **psql - h 127.0.0.1 -** comando del **controlsmartdb del postgres U**.
3. Seleccione *** del** securesmart_info. `ss_key | ss_group | ss_type | ss_ip | ss_loc`

   `00_40_33_60_43_D2_04_54_48_55_66_D5 | | standard_gateway | 10.0.0.1 |`
4. SSH al servidor de acceso limpio de Cisco y obtiene/actualización el ss_key.
5. Publique el **[!ENTITY! etc] # el** comando de **/etc/.GUSSK del gato**. `[root@securesmart etc]# cat /etc/.GUSSK`

   `00_30_48_80_43_D6_00_30_48_80_43_D5`
6. Edite **/etc/.GUSSK** y póngalo al día con el ss_key del Access Manager limpio.
7. Realice una reinicialización.

Q. Se pierde la Conectividad SSH mientras que apaga el servicio del perfigo en un CAS usando el comando shut del perfigo del servicio. No puedo volver a conectar a menos que alguien esté físicamente en el cuadro y puedo recomenzarlo. ¿Cómo puedo resolver este problema?

A. Este problema se puede resolver usando el comando del **mantenimiento del perfigo del servicio** en las versiones 4.1 del NAC y posterior.

Q. No puedo iniciar el dispositivo NAC con el nuevo CD CAS/CAM que tengo. ¿Qué debo hacer?

A. Verifique el siguiente para resolver esto:

- Asegúrese de que usted haya validado la suma de comprobación para la imagen ISO descargada para CAS/CAM.
- Queme la imagen ISO a la velocidad ardiente posible más lenta.

Información Relacionada

- Agente de Acceso de Mantenimiento de Cisco FAQ
- Preguntas Frecuentes sobre Cisco Clean Access Manager
- Preguntas Frecuentes sobre Cisco Clean Access Manager 2

- Soporte Técnico - Cisco Systems