# Cisco NAC Appliance (Clean Access) 4.x: Configure las configuraciones del Syslog para el registro de eventos

## Contenido



## Introducción

Este documento describe cómo configurar las configuraciones del Syslog para registrar los eventos a un servidor externo en el dispositivo del Cisco Network Admission Control (NAC), conocido antes como acceso limpio de Cisco (CA).

## prerrequisitos

### Requisitos

Este documento asume que el Access Manager limpio de Cisco (CAM) y el Access Servers limpio de Cisco (CAS) están instalados y que trabajan correctamente.

### Componentes Utilizados

La información en este documento se basa en el dispositivo NAC de Cisco que funciona con la versión de software 4.0 y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

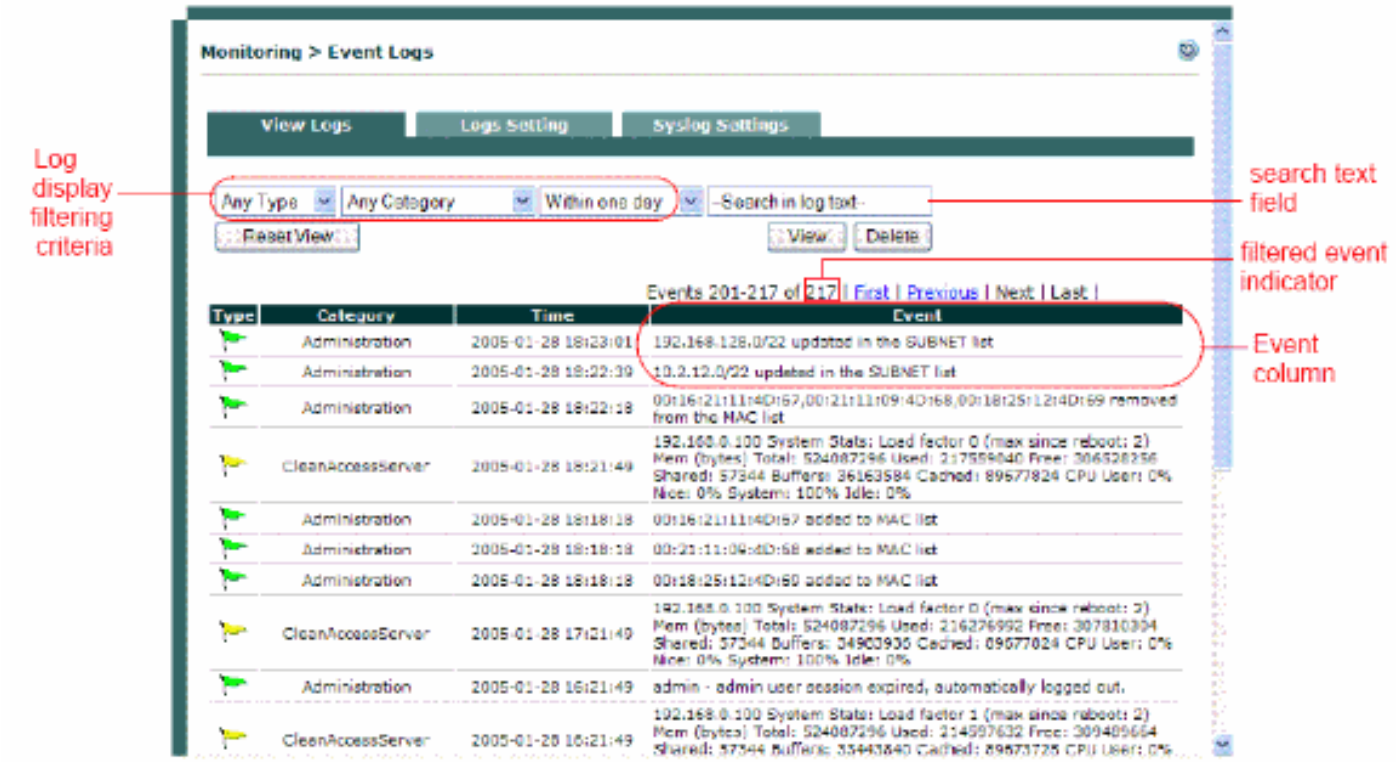
# Interpretación de los registros de acontecimientos

Haga clic los **registros de acontecimientos** conectan en el módulo de la **supervisión** para ver el evento Syslog-basado abre una sesión la consola admin. Hay tres lenguetas de los registros de acontecimientos:

- **Registros de la visión**
- **Configuraciones de los registros**
- **Configuraciones del Syslog**

## Registros de la visión

**Figura 1**




La lengueta de los registros de la visión incluye esta información:

- Estadísticas del sistema para el Access Servers limpio, que se generan cada hora por abandono.
- Actividad del usuario, con los tiempos del inicio del usuario, tiempos del cierre de sesión, tentativas falladas del inicio, y más.
- Eventos de la configuración de red, que incluyen los cambios las listas al Media Access Control (MAC) o del passthrough IP, y adición o retiro del Access Servers limpio.
- Eventos del administrador de switches para fuera de banda (OOB), que incluyen cuando se reciben las trampas de interrupción de link, y cuando un puerto cambia al auth o al Virtual LAN (VLAN) del acceso.

- Cambios o actualizaciones a las verificaciones de acceso limpias, a las reglas, y al antivirus/a la lista soportados del producto de AntiSpyware.
- Cambios a la configuración limpia del Protocolo de configuración dinámica de host (DHCP) del servidor de acceso.

Las estadísticas del sistema se generan para cada CAS manejado por el Access Manager limpio cada hora por abandono. Vea que configurando la orden de apertura de sesión del Syslog para cambiar cuantas veces ocurren las revisiones del sistema.

**Note**: Los eventos más recientes aparecen primero en la columna de los eventos.

El cuadro 1 describe la navegación, las capacidades de la búsqueda, y el Syslog real visualizado en los registros de la visión.

**Tabla 1**

| | Columna | Descripción |
|---|---|---|
| Navegación | **Primero/anterior/después/último** | Página de estos links de la navegación a través del registro de acontecimientos. Los eventos más recientes aparecen primero en la columna de los eventos. El link **más reciente** le muestra los más viejos eventos en el registro. Un máximo de 25 entradas se visualiza en una página. |
| | **Columna** | Haga clic un encabezado de la columna, tal como tipo o categoría, para clasificar el registro de acontecimientos por esa columna. |
| Criterios de búsqueda | Tipo | Busque por estos criterios de la columna del tipo, y después haga clic la **visión**:<br>• Ningunos teclean<br>• Falla<br>• Información<br>• Éxito |
| | **Categoría** | Busque por estos criterios de la columna de la categoría, y después haga clic la **visión**:<br>• Autenticación [1]<br>• Administración<br>• Cliente<br>• Clean Access Server<br>• Limpie el acceso<br>• SW_Management, si OOB se habilita<br>• Miscelánea<br>• DHCP |
| | | |

| | | |
|---|---|---|
| | Hora | Busque por estos criterios del tiempo, y después haga clic la **visión**:<br>• En el plazo de una hora<br>• En el plazo de un día<br>• En el plazo de dos días<br>• En el plazo de una semana<br>• Siempre<br>• Hace una hora<br>• Hace un día<br>• Hace dos días<br>• Hace una semana |
| | **Búsqueda en el texto del registro** | Teclee el texto deseado de la búsqueda y haga clic la **visión**. |
| Controles | **Visión** | Después de que se elijan los criterios de búsqueda deseados, haga clic la **visión** para visualizar los resultados. |
| | **Reajuste la visión** | Si usted hace clic la **opinión de la restauración**, restablece la vista predeterminada, en la cual los registros en el plazo de un día se visualizan. |
| | **Cancelación** | Si usted hace clic la **cancelación**, quita los eventos filtrados con los criterios de búsqueda a través del número de páginas aplicables. La cancelación quita los eventos filtrados del almacenamiento limpio del Access Manager. Si no, el registro de acontecimientos persiste con el cierre del sistema. Utilice el indicador del evento del filtro mostrado en el cuadro 1 para ver el número total de eventos filtrados que estén conforme a la cancelacíon. |
| Se muestra el estado | Tipo | • Indicación roja (  ) = error — indica un error o de otra manera un Evento inesperado<br>• Indicador verde (  ) = éxito — indica un evento acertado o de la utilización normal, tal como registración satisfactoria y |

| | | |
|---|---|---|
| | | actividad de la configuración<br>• Indicador amarillo (  ) = información — indica la información del rendimiento del sistema, tal como información de carga y uso de la memoria |
| | **Categoría** | Indica el módulo o al componente del sistema que iniciaron el evento del registro. Para una lista, refiera a la **categoría** bajo criterios de búsqueda de la sección. Observe que, por abandono, las estadísticas del sistema están generadas cada hora para cada servidor de acceso limpio que sea manejado por el Access Manager limpio. |
| | Hora | Visualiza la fecha y hora (hh: milímetro: ss) del evento, con los eventos más recientes primero de la lista. |
| | **Evento** | Visualiza el evento para el módulo, con los eventos más recientes enumerados primero. Vea el cuadro 2 - Campos de columna del evento por un ejemplo de un evento limpio del servidor de acceso. |

## Notas a pie de página - Cuadro 1

1 Las entradas del tipo de autenticación pueden incluir proveedor del elemento ": type> del <provider, Punto de acceso: N/A, red: N/A." para continuar proporcionando el soporte para el cliente de red inalámbrica de la herencia del fin de vida (EOL), si es presente y preconfigurado en el administrador, "el Punto de acceso: N/A, red: Campos N/A los" proporcionan el punto de acceso MAC y la información del Service Set Identifier (SSID) respectivamente para el cliente de la herencia.

## Ejemplo del registro de acontecimientos

El cuadro 2 explica el ejemplo limpio típico del evento de estado del servidor de acceso:

```
CleanAccessServer 2006-04-03 15:07:53 192.168.151.55 System Stats:
 Load factor 0 (max since reboot: 9) Mem Total: 261095424 bytes Used: 246120448
 bytes Free: 14974976 bytes Shared: 212992 bytes Buffers: 53051392 bytes Cached:
 106442752 bytes CPU User: 0% Nice: 0% System: 97% Idle: 1%
```

**Cuadro 2 - Campos de columna del evento**

| Valor | Descripción |
| --- | --- |
| CleanAccessServer | Un servidor de acceso limpio señala el evento |
| 2006-04-03 15:07:53 | Fecha y hora del evento |
| 192.168.151.55 | Dirección IP de señalar el servidor de acceso limpio |
| Factor de carga 0 | El Factor de carga indica el número de paquetes que esperen para ser procesados por el servidor de acceso limpio, es decir, la carga actual que es manejada por CAS. Cuando el Factor de carga crece, es una indicación que los paquetes esperan en la cola que se procesará. Si el Factor de carga excede de 500 para cualquier período de tiempo constante, tal como cinco minutos, éste indica que el servidor de acceso limpio tiene una mucha carga constante del tráfico entrante/de los paquetes. Trátese si este número aumenta a 500 o más alto. |
| (máximo desde la reinicialización: <n>) | La cantidad máxima de paquete en la cola a cualquier momento. Es decir la carga máxima manejada por el servidor de acceso limpio. |
| Total del mem: 261095424 bytes<br>Utilizado: 246120448 bytes<br>Libre: 14974976 bytes<br>Compartido: 212992 bytes<br>Buffers: 53051392 bytes<br>Ocultado: 106442752 bytes | Éstas son las estadísticas del uso de la memoria. Hay seis números mostrados aquí:<br>• memoria total<br>• memoria usada<br>• memoria libre<br>• memoria compartida<br>• memoria intermedia<br>• memoria ocult0 |
| Usuario CPU: el 0%<br>Agradable: el 0%<br>Sistema: el 97%<br>Marcha lenta: | Estos números indican la carga del procesador de la CPU en el hardware, en los porcentajes. Estos cuatro números indican el tiempo pasado por el sistema en el usuario, agradable, el sistema, y los procesos ociosos. **Note**: El tiempo pasado por el CPU en el proceso del sistema es típicamente mayor del |

| | |
|---|---|
| el 1% | 90 por ciento en un servidor de acceso limpio. Esto indica un sistema saludable. |

## Limite el número de eventos registrados

El umbral del registro de acontecimientos es el número de eventos que se salvarán en la base de datos limpia del Access Manager. El número máximo de eventos del registro guardados en el CAM, por abandono, es 100,000. Usted puede especificar un umbral del registro de acontecimientos de hasta 200,000 entradas que se salvarán en el en un momento de la base de datos CAM. El registro de acontecimientos es un registro circular. Las más viejas entradas están sobregrabadas cuando el registro pasa el umbral del registro de acontecimientos.

**Para cambiar el número máximo de eventos:**

1. Haga clic los **registros que fijan la** lengueta en las páginas de la **supervisión > de los registros de acontecimientos**.
2. Ingrese el nuevo número en los campos de los **registros de evento máximo**.
3. Haga clic en **Update** (Actualizar).

## Configure el registro del Syslog

Las estadísticas del sistema se generan cada hora, por abandono, para cada servidor de acceso limpio que sea manejado por el Access Manager limpio. Por abandono, los registros de acontecimientos se escriben al CAM. Usted puede reorientar los registros de acontecimientos CAM a otro servidor, tal como su propio servidor de Syslog.

Además, usted puede configurar cuantas veces usted quisiera que el CAM registrara la información de estado del sistema. Para hacer esto, fije el valor en el campo del **intervalo del registro de la salud del Syslog**. El valor por defecto es **60** minutos.

Para configurar el registro del Syslog:

1. Elija la **supervisión > los registros de acontecimientos > las configuraciones del Syslog**.
2. Ingrese el IP Address del servidor de Syslog en el campo de **dirección del servidor de Syslog**. El valor por defecto es **127.0.0.1**.
3. Ingrese el puerto para el servidor de Syslog en el campo de **puerto de servidor de Syslog**. El valor por defecto es **514**.
4. Ingrese cuantas veces usted quisiera que el CAM registrara la información de estado del sistema, en los minutos, en el campo del **intervalo del registro de los Estados generales del sistema**. El valor por defecto es **60** minutos. Esta configuración determina cómo con frecuencia las estadísticas CAS se abren una sesión el registro de acontecimientos.
5. **Actualización del** tecleo para salvar sus cambios.**Note**: Después de que usted configure a su servidor de Syslog en el CAM, usted puede probar su configuración. Para hacer esto, el cierre de sesión y el registro nuevamente dentro de la consola CAM admin. Esto genera un evento de syslog. Si el evento CAM no se considera en su servidor de Syslog, aseegurese que el servidor de Syslog recibe el User Datagram Protocol (UDP) 514 paquetes y que no están bloqueados a otra parte en su red.**Note**: Configurar a los servidores de Syslog múltiple no es posible pues no se soporta. Usted puede remitir solamente a un servidor de Syslog.

## Archivos del registro

El registro de acontecimientos está situado en la tabla de base de datos limpia del Access Manager y nombrado tabla del log_info. enumera otro abre una sesión el Access Manager limpio.

Cuadro 3

| Archivo | Descripción |
|---|---|
| `/var/log/messages` | Lanzamiento |
| `/var/log/dhcplog` | Relé DHCP, registros del DHCP |
| `/tmp/perfigo-log0.log.*` | Registros de servicio del perfigo para 3.5(4) y anterior [1] |
| `/perfigo/logs/perfigo-log0.log.*` | Registros de servicio del perfigo para 3.5(5) y posterior [1,2] |
| `/perfigo/logs/perfigo-redirect-log0.log.0` | errores de conexión Certificado-relacionados CAM/CAS |
| `/var/nessus/logs/nessusd.messages` | Plug-in Nessus pruebe los registros |
| `/perfigo/control/apache/logs/*` | Asegure los Certificados de la capa de socketes (SSL), los registros de error de Apache |
| `/perfigo/control/tomcat/logs/localhost *.` | Tomcat, reorienta, JavaServer pagina los registros (JSP) |
| `/var/log/ha-log` | Registros de gran disponibilidad para el CAM y CAS |

### Notas a pie de página - Cuadro 3

1. 0 en vez de * muestra el registro más reciente.

2. El administrador de switches que los eventos para las notificaciones recibidas por el CAM del Switches se escriben solamente al abre una sesión el sistema de archivos (/perfigo/logs/perfigo-log0.log.0). Además, estos eventos se escriben al disco solamente cuando el nivel del registro se fija a la INFORMACIÓN o más fino.

# Información Relacionada

- Página de soporte del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems