Ejemplo de la configuración de syslog ASA

Contenido

Introducción

Este documento proporciona una configuración de muestra que demuestre cómo configurar diversas opciones de registro en un dispositivo de seguridad adaptante (ASA) esa versión del código 8.4 de los funcionamientos o más adelante.

La Versión de ASA 8.4 ha introducido las técnicas de filtrado muy granulares para permitir que solamente ciertos mensajes de Syslog especificados sean presentados. La sección básica del Syslog de este documento demuestra una configuración de syslog tradicional. La sección avanzada del Syslog de este documento muestra las nuevas características del Syslog en la versión 8.4. Refiera a los mensajes del registro del sistema guía del dispositivo del Cisco Security, versión 8.x y 9.x para la guía completa de los mensajes del registro del sistema.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5515 con la versión de software 8.4 ASA
- Versión 7.1.6 del Cisco Adaptive Security Device Manager (ASDM)

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.

> Nota: Refiera a ASA 8.2: Configure el Syslog usando el ASDM para más información para los detalles de la configuración similares con la versión 7.1 y posterior del ASDM.

Syslog básico

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Ingrese estos comandos para habilitar la registración, vea los registros, y vea los ajustes de la configuración.

- **permiso de registración** - Habilita la transmisión de los mensajes de Syslog a todas las ubicaciones de la salida.
- **ningún permiso del registro -** Neutralizaciones que registran a todas las ubicaciones de la salida.

- **registro de la demostración -** Enumera el contenido del buffer del Syslog e información y las estadísticas que pertenecen a la configuración actual.

El ASA puede enviar los mensajes de Syslog a los diversos destinos. Ingrese los comandos en estas secciones para especificar las ubicaciones que le como la Información de syslog enviarían:

Envíe la información de ingreso al sistema al búfer interno

```
logging buffered severity_level
```

El software externo o el soporte físico no se requiere cuando usted salva los mensajes de Syslog en el búfer interno ASA. Ingrese el **comando show logging** para ver los mensajes de Syslog salvados. El búfer interno tiene un tamaño máximo del 1 MB (configurable con el comando del **tamaño de almacén intermedio del registro**). Como consecuencia, puede ser que envuelva muy rápidamente. Tenga esto presente cuando usted elige un nivel de registro para el búfer interno como niveles más prolijos de registración pudieron llenar rápidamente, y el abrigo, el búfer interno.

Envíe la información de ingreso al sistema a un servidor de Syslog

```
logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap severity_level
logging facility number
```

Un servidor que ejecuta una aplicación syslog se requiere para enviar los mensajes de Syslog a un host externo. El ASA envía el Syslog en el puerto 514 UDP por abandono, pero el protocolo y el puerto pueden ser elegidos. Si el TCP se elige como el protocolo del registro, éste hace el ASA enviar los Syslog vía una conexión TCP al servidor de Syslog. Si el servidor es inaccesible, o la conexión TCP al servidor no puede ser establecida, el ASA, por abandono, bloqueará TODAS LAS nuevas conexiones. Este comportamiento puede ser inhabilitado si usted habilita el **permiso-hostdown del registro**. Vea la guía de configuración para más información sobre el comando del **permiso-hostdown del registro**.

Envíe la información de ingreso al sistema como email

```
logging mail severity_level
logging recipient-address email_address
logging from-address email_address
smtp-server ip_address
```

Requieren a un servidor SMTP cuando usted envía los mensajes de Syslog en los email. La configuración correcta en el servidor SMTP es necesaria para asegurarse de que usted puede retransmitir con éxito los email del ASA al cliente de email especificado. Si este nivel de registro se fija a un nivel muy prolijo, tal como *debug* o *informativo,* usted puede ser que genere un número significativo de Syslog puesto que cada email enviado por esta configuración de registro causa hacia arriba de registros cuatro o más adicionales que se generarán.

Envíe la información de ingreso al sistema a la consola en serie

```
logging console severity_level
```

El registro de la consola permite a los mensajes de Syslog para visualizar en la consola ASA (equipo teleescritor) como ocurren. Si se configura el registro de la consola, toda la generación

del registro en el ASA ratelimited a 9800 BPS, la velocidad de la consola en serie ASA. Esto pudo hacer los Syslog ser caído a todos los destinos, que incluyen el búfer interno. No utilice el registro de la consola para los Syslog prolijos por este motivo.

Envíe la información de ingreso al sistema a una sesión del telnet/SSH

```
logging monitor severity_level
terminal monitor
```

El monitor de registración permite a los mensajes de Syslog para visualizar mientras que ocurren cuando usted accede la consola ASA con Telnet o ejecutan SSH y al comando terminal monitor de esa sesión. Para parar la impresión de los registros a su sesión, no ingrese el **ningún comando terminal monitor**.

Visualice los mensajes del registro en el ASDM

```
logging asdm severity_level
```

El ASDM también tiene un buffer que se pueda utilizar para salvar los mensajes de Syslog. Ingrese el **comando show logging asdm** para visualizar el contenido del buffer del Syslog del ASDM.

Envíe los registros a una estación de la administración de SNMP

```
logging history severity_level
snmp-server host [if_name] ip_addr
snmp-server location text
snmp-server contact text
snmp-server community key
snmp-server enable traps
```

Los usuarios necesitan un entorno funcional existente del Simple Network Management Protocol (SNMP) para enviar los mensajes de Syslog con el SNMP. Vea los comandos para fijar y manejo de los destinos de salida para una referencia completa en los comandos que usted puede utilizar para fijar y para manejar los destinos de salida. Vea los mensajes enumerados por el nivel de gravedad para los mensajes enumerados por el nivel de gravedad.

Agregue los grupos fecha/hora a los Syslog

Para ayudar a alinear y los eventos de la orden, los grupos fecha/hora se pueden agregar a los Syslog. Esto se recomienda para ayudar a localizar los problemas basados el tiempo. Para habilitar los grupos fecha/hora, ingrese el **comando logging timestamp**. Aquí están dos ejemplos del Syslog, uno sin el grupo fecha/hora y uno con:

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
442 TCP Reset-I
```

Ejemplo 1

Esta salida muestra una configuración de muestra para registrar en el **buffer** con el nivel de gravedad de **debugging**.

```
logging enable
logging buffered debugging
```

Ésta es una salida de ejemplo.

```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

Syslog básico de la configuración con el ASDM

Este procedimiento demuestra la Configuración de ASDM para todos los destinos de syslog disponibles.

1. Para habilitar la apertura de sesión del ASA, primero configure los parámetros básicos del registro. Elija la **configuración > las características > las propiedades > el registro > la configuración del registro**. Marque la casilla de verificación del **registro del permiso** para habilitar los Syslog.
2. Para configurar a un servidor externo como el destino para los Syslog, elegir a los **servidores de Syslog** en el registro y el tecleo **agregue** para agregar a un servidor de Syslog. Ingrese a los detalles del servidor de Syslog en el rectángulo del servidor de Syslog del agregar y elija **OK** cuando le hacen.
3. Elija la **configuración del email** en la orden de apertura de sesión para enviar los mensajes de Syslog como email a los beneficiarios específicos. Especifique la dirección de correo electrónico de la fuente en el cuadro de la dirección de correo electrónico de la fuente y elija **agregan** para configurar la dirección de correo electrónico del destino de los beneficiarios del email y del nivel de gravedad de mensaje. Haga Click en OK cuando le hacen.
4. Elija **Device Administration (Administración del dispositivo)**, **registrando,** elija el **S TP**, y ingrese el IP Address del servidor primario para especificar el IP Address del servidor SMTP.
5. Si usted quiere enviar los Syslog como SNMP traps, usted debe primero definir a un servidor SNMP. Elija el **SNMP** adentro en el menú del **Acceso de administración** para especificar el direccionamiento de las estaciones de la administración de SNMP y de sus propiedades específicas.
6. Elija **agregan** para agregar una estación de la administración de SNMP. Ingrese los detalles del host SNMP y haga clic la **AUTORIZACIÓN**.
7. Para habilitar los registros que se enviarán a los destinos mencionados anteriores uces de los, elija los **filtros del registro** en la sección del registro. Esto le presenta con cada destino de registro posible y el nivel actual de registros que se envíen a esos destinos. Elija el destino de registro deseado y el tecleo **edita**. En este ejemplo, destino se modifica el “de los servidores de Syslog.
8. Elija una gravedad apropiada, en este caso **informativa, del filtro en la** lista desplegable de la **gravedad**. Haga Click en OK cuando le hacen.
9. El tecleo **se aplica** después de que usted vuelva a la ventana de los filtros del registro.

Envíe los mensajes de Syslog sobre un VPN a un servidor de Syslog

En el diseño simple o del VPN de sitio a sitio complicado diseño de hub y spoke, el administrador pudo querer monitorear todos los Firewall del telecontrol ASA con el servidor SNMP y el servidor de Syslog situados en un sitio central.

Para configurar IPSec sitio a sitio la configuración VPN, refiera al PIX/ASA 7.x y arriba: Ejemplo de la configuración del túnel PIX-a-PIX VPN. Aparte de la configuración VPN, usted tiene que configurar el SNMP y el tráfico interesante para el servidor de Syslog en la central y el sitio local.

Configuración central ASA

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514


logging enable
logging trap debugging

!--- Define logging host information.
logging facility 16
logging host inside 172.22.1.5

!--- Define the SNMP configuration.
snmp-server host inside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Configuración remota ASA

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.
access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
!--- interface to the SYSLOG server.
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514

!--- Define syslog server.
logging facility 23
logging host outside 172.22.1.5

!--- Define SNMP server.
snmp-server host outside 172.22.1.5 community ***** version 2c
```

```
snmp-server community *****
```
Refiera a monitorear el Firewall seguro de Cisco ASA usando SNMP y Syslog a través del túnel VPN para más información sobre cómo configurar la Versión de ASA 8.4

Syslog avanzado

La Versión de ASA 8.4 proporciona varios mecanismos que le permitan para configurar y para manejar los mensajes de Syslog en los grupos. Estos mecanismos incluyen el nivel de gravedad de mensaje, la clase de mensaje, el ID del mensaje, o una lista del mensaje personalizado que usted crea. Con el uso de estos mecanismos, usted puede ingresar un comando único que se aplique a los grupos pequeños o grandes de mensajes. Cuando usted configura los Syslog esta manera, usted puede capturar los mensajes del grupo especificado del mensaje y no más todos los mensajes de la misma gravedad.

Utilice la lista del mensaje

Utilice la lista del mensaje para incluir solamente los mensajes de Syslog interesados por el nivel de gravedad y el ID en un grupo, después asocie esta lista del mensaje al destino deseado.

Complete estos pasos para configurar una lista del mensaje:

1. Ingrese el ***message_list de la*** **lista de registración /** comando ***llano del [class message_class] del severity_level*** para crear una lista del mensaje que incluye los mensajes con una lista especificada del nivel de gravedad o del mensaje.
2. Ingrese el **comando logging list message_list message syslog_id-syslog_id2** para agregar los mensajes adicionales a la lista del mensaje apenas creada.
3. Ingrese el **comando logging destination message_list** para especificar el destino de la lista del mensaje creada.

‘Ejemplo 2’

Ingrese estos comandos para crear una lista del mensaje, que incluye toda la gravedad 2 mensajes (críticos) con la adición del mensaje 611101 a 611323, y también téngalos enviados a la consola:

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

Configuración de ASDM

Este procedimiento muestra una Configuración de ASDM por ejemplo 2 con el uso de la lista del mensaje.

1. Elija las **Listas de eventos** bajo registro y el tecleo **agrega** para crear una lista del mensaje.
2. Ingrese el nombre de la lista del mensaje en el cuadro de nombre. En este caso los **my_critical_messages** se utilizan. El tecleo **agrega** bajo los filtros de la clase de evento/de la gravedad.

3. Elija **todos de la** lista desplegable de la clase de evento. Elija **crítico de la** lista desplegable de la gravedad. Haga Click en OK cuando le hacen.
4. El tecleo **agrega** bajo los filtros del ID del mensaje si se requieren los mensajes adicionales. En este caso, usted necesita poner en los mensajes con ID 611101-611323.
5. Ponga en el rango ID en el cuadro de los ID del mensaje y haga clic la **AUTORIZACIÓN**.
6. Vuelva al menú de los **filtros del registro** y elija la **consola** como el destino.
7. Elija los **my_critical_messages de la** lista desplegable de la **Lista de eventos del uso**. Haga Click en OK cuando le hacen.
8. El tecleo **se aplica** después de que usted vuelva a la ventana de los filtros del registro.

Esto completa las Configuraciones de ASDM con el uso de una lista del mensaje tal y como se muestra en del ejemplo 2.

Utilice la clase de mensaje

Utilice la clase de mensaje para enviar todos los mensajes asociados a una clase a la ubicación especificada de la salida. Cuando usted especifica un umbral del nivel de gravedad, usted puede limitar el número de mensajes enviados a la ubicación de la salida.

```
logging class message_class destination | severity_level
```

Ejemplo 3

Ingrese este comando para enviar todos los mensajes de la clase Ca con un nivel de gravedad de emergencias o más alto a la consola.

```
logging class ca console emergencies
```

Configuración de ASDM

Este procedimiento muestra las Configuraciones de ASDM por ejemplo 3 con el uso de la lista del mensaje.

1. Elija el menú de los **filtros del registro** y elija la **consola** como el destino.
2. Haga clic el **registro de la neutralización de todas las clases de evento**.
3. Bajo los Syslog de las clases de evento específico, elija la clase de evento y la gravedad que usted quiere agregar.Este procedimiento utiliza el **Ca** y las **emergencias** respectivamente.
4. El tecleo **agrega** para agregar esto en la clase de mensaje y hacer clic la **AUTORIZACIÓN**.
5. El tecleo **se aplica** después de que usted vuelva a la ventana de los filtros del registro. La consola ahora recoge el mensaje de la clase Ca con las emergencias del nivel de gravedad como se muestra en la ventana de los filtros del registro.

Esto completa la Configuración de ASDM por ejemplo 3. refiere a los mensajes enumerados por el nivel de gravedad para una lista de los niveles de gravedad del mensaje del registro.

Envíe los mensajes del registro del debug a un servidor de Syslog

Para el Troubleshooting avanzado, se requieren los registros específicos del debug de la característica/del protocolo. Por abandono, estos mensajes del registro se visualizan en la

terminal (SSH/Telnet). El dependiente en el tipo de debug, y el índice de mensajes del debug generados, uso del CLI pudieron probar difícil si se habilitan los debugs. Opcionalmente, los mensajes del debug se pueden reorientar al proceso de Syslog y generar como Syslog. Estos Syslog se pueden enviar a cualquier destino de syslog como cualquier otro Syslog. Para desviar los debugs a los Syslog, ingrese el comando de **registración de la debug-traza**. Esta configuración envía la salida de los debugs, como Syslog, a un servidor de Syslog.

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

Uso de la lista y de las clases de mensaje de registro junto

Ingrese el **comando list de registración** para capturar el Syslog para el LAN a LAN y los mensajes del IPSec VPN del Acceso Remoto solamente. Este ejemplo captura todos los mensajes del registro del sistema de la clase VPN (IKE y IPSec) con el nivel de debugging o más arriba.

Ejemplo:

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

Golpes del registro ACL

Agregue el *registro a* cada elemento de la lista de acceso (ACE) que usted desea para registrar cuando se golpea una lista de acceso. Utilice este sintaxis:

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Ejemplo:

```
ASAfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

Los ACL, por abandono, registran cada paquete negado. No hay necesidad de agregar la opción del registro **para negar los** ACL para generar los Syslog para los paquetes negados. Cuando se especifica la opción del *registro*, genera el mensaje de Syslog `106100` para ACE a las cuales es aplicado. El mensaje de Syslog `106100` se genera para cada flujo de ACE del permit or deny que corresponde con que pase con el Firewall ASA. Se oculta el flujo de la primero-coincidencia. Las coincidencias subsiguientes incrementan la cuenta del golpe visualizada en el **comando show access-list**. Se genera se genera el comportamiento predeterminado del registro de la lista de acceso, que es la palabra clave del *registro* no especificada, es que si se niega un paquete, después el mensaje `106023`, y si se permite un paquete, después ningún mensaje de Syslog.

Un nivel opcional del Syslog (0 - 7) se puede especificar para los mensajes de Syslog generados (`106100`). Si no se especifica ningún nivel, el nivel predeterminado es 6 (informativo) para nuevo ACE. Si existe ACE ya, después sigue habiendo su nivel actual del registro sin cambiar. Si se especifica la opción de la *neutralización del registro*, el registro de la lista de acceso se inhabilita totalmente. No se genera ningún mensaje de Syslog, incluyendo el mensaje `106023`. La opción predeterminada del *registro* restablece el comportamiento predeterminado del registro de la lista de acceso.

Complete estos pasos para permitir al mensaje de Syslog `106100` para ver en la salida de la

consola:

1. Ingrese el **comando logging enable** para habilitar la transmisión de los mensajes del registro del sistema a todas las ubicaciones de la salida. Usted debe fijar una ubicación de la salida de registro para ver cualquier registro.
2. Ingrese el comando del *<severity_level> del* **nivel del** *<message_number> del* **mensaje de registración** para fijar el nivel de gravedad de un mensaje del registro del sistema específico.En este caso, ingrese el comando del **mensaje de registración 106100** para habilitar el mensaje `106100`.
3. Ingrese el **message_list de la consola de registro |** comando del **severity_level** para permitir a los mensajes del registro del sistema para visualizar en la consola del dispositivo de seguridad (equipo teleescritor) como ocurren. Fije el `severity_level` a partir de la 1 a 7 o utilice el nombre llano. Usted puede también especificar qué mensajes se envían con la variable del `message_list`.
4. Ingrese el comando del **mensaje de registración de la demostración** para visualizar una lista de mensajes del mensaje del registro del sistema que se han modificado de la configuración predeterminada, que son los mensajes que se han asignado un diverso nivel de gravedad y los mensajes se han inhabilitado que.Ésta es salida de muestra del comando del **mensaje de registración de la demostración**:`ASAfirewall#`**`show logging message 106100`**
```
syslog 106100: default-level informational (enabled)
ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Si usted quiere suprimir un mensaje de Syslog específico que se enviará al servidor de Syslog, después usted debe ingresar el comando como se muestra.

`hostname(config)#`**`no logging message`** *`<syslog_id>`*
Refiera al comando del mensaje de registración para más información.

%ASA-3-201008: Rechazo de las nuevas conexiones

`El %ASA-3-201008: Rechazo de las nuevas conexiones.` se considera el mensaje de error cuando un ASA no puede entrar en contacto al servidor de Syslog y no se permite ningunas nuevas conexiones.

Solución

Este mensaje aparece cuando usted ha habilitado la Mensajería del registro de sistema TCP y el servidor de Syslog no puede ser alcanzado, o cuando usted utiliza al servidor de Syslog de Cisco ASA (PFSS) y el disco en el sistema del Windows NT es lleno. Complete estos pasos para

resolver este mensaje de error:

- Inhabilite la Mensajería del registro de sistema TCP si se habilita.
- Si usted utiliza el PFSS, libere para arriba el espacio en el sistema del Windows NT donde reside el PFSS.
- Asegúrese de que el servidor de Syslog sea ascendente y usted puede hacer ping el host de la consola de Cisco ASA.
- Recomience la orden de apertura de sesión del mensaje de sistema TCP para permitir el tráfico.

Si va el servidor de Syslog abajo y se configura el registro TCP, utilice el comando del permiso-hostdown del registro o conmutelo al registro UDP.

Información Relacionada

- Software de firewall de Cisco ASA
- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems