Solución de problemas de firewall que envía registros al servidor Syslog previamente configurado (heredado)

Contenido

Problema

El firewall envía mensajes syslog a un servidor syslog previamente configurado (heredado) en la dirección IP 198.51.100.100. Esta dirección IP no se encuentra en la configuración del firewall.

Entorno

Las plataformas afectadas son específicamente Firepower 2100 que ejecuta ASA en modo plataforma.

Resolución

Paso 1. Busque la dirección IP de origen de los mensajes de syslog:

Según el análisis de los mensajes recibidos por el servidor syslog heredado, la dirección IP de origen es la dirección IP de administración del chasis Firepower.

La dirección IP configurada en el sistema operativo extensible (FXOS) de Firepower es 192.0.2.100:

<#root>

```
2026-04-27 15:22:49    User.Error
```

```
192.0.2.100

    Apr 27 09:22:49 firepower FPRM: <<%FPRM-3-NTP_CONFIG_FAILED>> [F1329][major][ntp-config-failed][sys
2026-04-27 15:22:54   User.Error

192.0.2.100

    Apr 27 09:22:54 firepower FPRM: <<%FPRM-3-NTP_CONFIG_FAILED>> [F1329][cleared][ntp-config-failed][s
```

Paso 2. Verifique y verifique la configuración de syslog de FXOS:

- La configuración de la interfaz de línea de comandos (CLI) de FXOS no contiene la dirección del servidor syslog heredado:

<#root>

```
device #

scope monitoring


device /monitoring #

show configuration | i 198.51.100.100


device /monitoring #

show configuration all | i 198.51.100.100
```

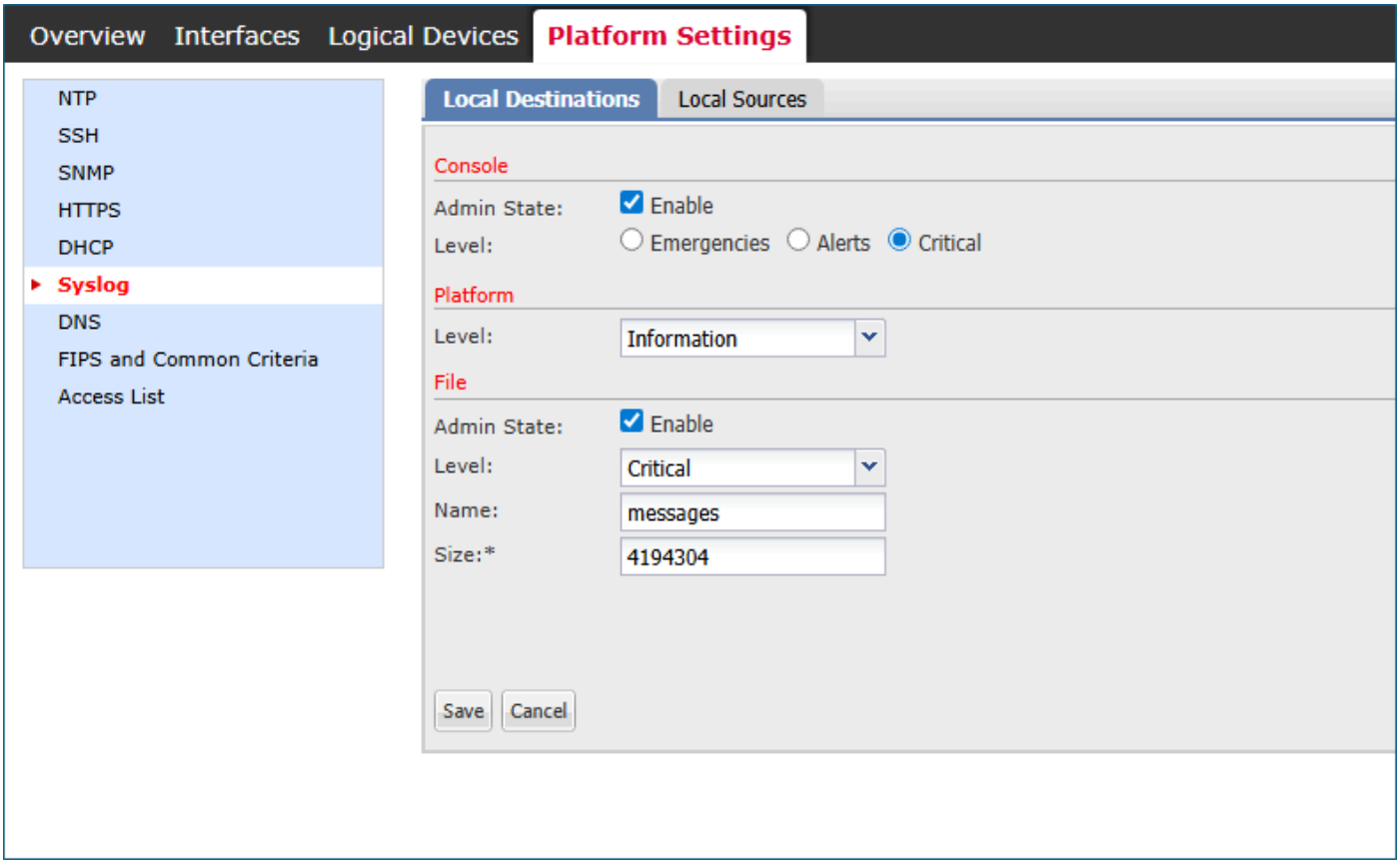
- Al mismo tiempo, la salida del comando show syslog en el ámbito de monitoreo muestra la dirección IP del servidor:

<#root>

```
device #

scope monitoring


device /monitoring #

show syslog
```

```
console
    state: Disabled
    level: Critical

platform
    state: Enabled
    level: Information
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 198.51.100.10        Enabled  Warnings      Local7


Server 2 198.51.100.100       Enabled  Warnings      Local7 <---- legacy server


    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Disabled
```

- Firepower Chassis Manager (FCM) User Interface (UI) > Platform Settings > Syslog no indica la configuración del servidor syslog.



fcm_syslogs_configuration.png

Paso 3. Intente modificar o eliminar el servidor syslog:

<#root>

```
device#

scope monitoring



device /monitoring #

delete


  <---
  snmp-trap  SNMP trap hostname or IP address
  snmp-user  SNMPv3 User

device /monitoring #

set syslog


  <---
  console   Console
  file      File
  platform  Platform

device /monitoring #

set syslog platform


 <---
  level  Level
```

La conclusión es que ni FXOS CLI ni FCM UI proporcionan una manera de crear, modificar o eliminar cualquier servidor syslog, incluido 198.51.100.100.

Causa

Tenga en cuenta tres defectos de software:

ID de bug de Cisco CSCvn19025

Las versiones de software con la corrección de este defecto no permiten la configuración de

syslog remoto FXOS en la interfaz de usuario de CLI o FCM.

ID de bug de Cisco CSCvt85766

La corrección de este defecto elimina la sección "destinos remotos" de la salida del comando FXOS show syslog.

Versiones sin corrección:

<#root>

```
device#

scope monitoring


device /monitoring #

show syslog



console
    state: Enabled
    level: Critical

platform
    state: Enabled
    level: Information

file
    state: Enabled
    level: Critical
    name:  messages
    size:  4194304

remote destinations <----------------
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 192.0.2.1            Enabled  Information   Local7
    Server 2 192.0.2.2            Enabled  Information   Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Disabled
```

Las versiones con la corrección carecen de la sección "destinos remotos":

<#root>

```
device #

scope monitoring


device /monitoring #

show syslog



console
    state: Enabled
    level: Critical

platform
    state: Enabled
    level: Information
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 192.0.2.1            Enabled  Information   Local7
    Server 2 192.0.2.2            Enabled  Information   Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Disabled
```

A pesar de no haber encontrado la sección "destinos remotos", los servidores syslog están visibles en la sección "plataforma".

ID de bug de Cisco CSCwu12470

Después de la actualización de software a la versión con la corrección del Id. de error de Cisco CSCvn19025, la administración de los servidores syslog remotos, es decir, la creación, modificación o eliminación, no está permitida en la CLI de FXOS o la interfaz de usuario de FCM. Esta limitación también se aplica a los servidores configurados antes de la actualización. A pesar de esto, después de la actualización del software, el software FXOS muestra los servidores syslog en la sección "plataforma" de la salida del comando show syslog y envía los mensajes syslog a estos servidores. Los usuarios no pueden administrar la configuración de syslog remoto FXOS existente, que se rastrea en el Id. de error de Cisco CSCwu12470.

Contenido relacionado

- ID de bug de Cisco CSCvn19025
- ID de bug de Cisco CSCvt85766
- ID de bug de Cisco CSCwu12470

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).