Dépannage des journaux d'envoi du pare-feu vers le serveur Syslog précédemment configuré (hérité)

Table des matières

Problème

Le pare-feu envoie des messages syslog à un serveur syslog précédemment configuré (hérité) à l'adresse IP 198.51.100.100. Cette adresse IP est absente de la configuration du pare-feu.

Environnement

Les plates-formes concernées sont spécifiquement Firepower 2100 exécutant ASA en mode plate-forme.

Résolution

Étape 1 : recherche de l’adresse IP source des messages syslog

Sur la base de l'analyse des messages reçus par le serveur syslog hérité, l'adresse IP d'origine est l'adresse IP de gestion du châssis Firepower.

L'adresse IP configurée dans le système d'exploitation extensible Firepower (FXOS) est 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
```

Étape 2. Vérification de la configuration Syslog FXOS :

- La configuration de l'interface de ligne de commande FXOS ne contient pas l'adresse du serveur syslog hérité :

<#root>

```
device #

scope monitoring


device /monitoring #

show configuration | i 198.51.100.100


device /monitoring #

show configuration all | i 198.51.100.100
```

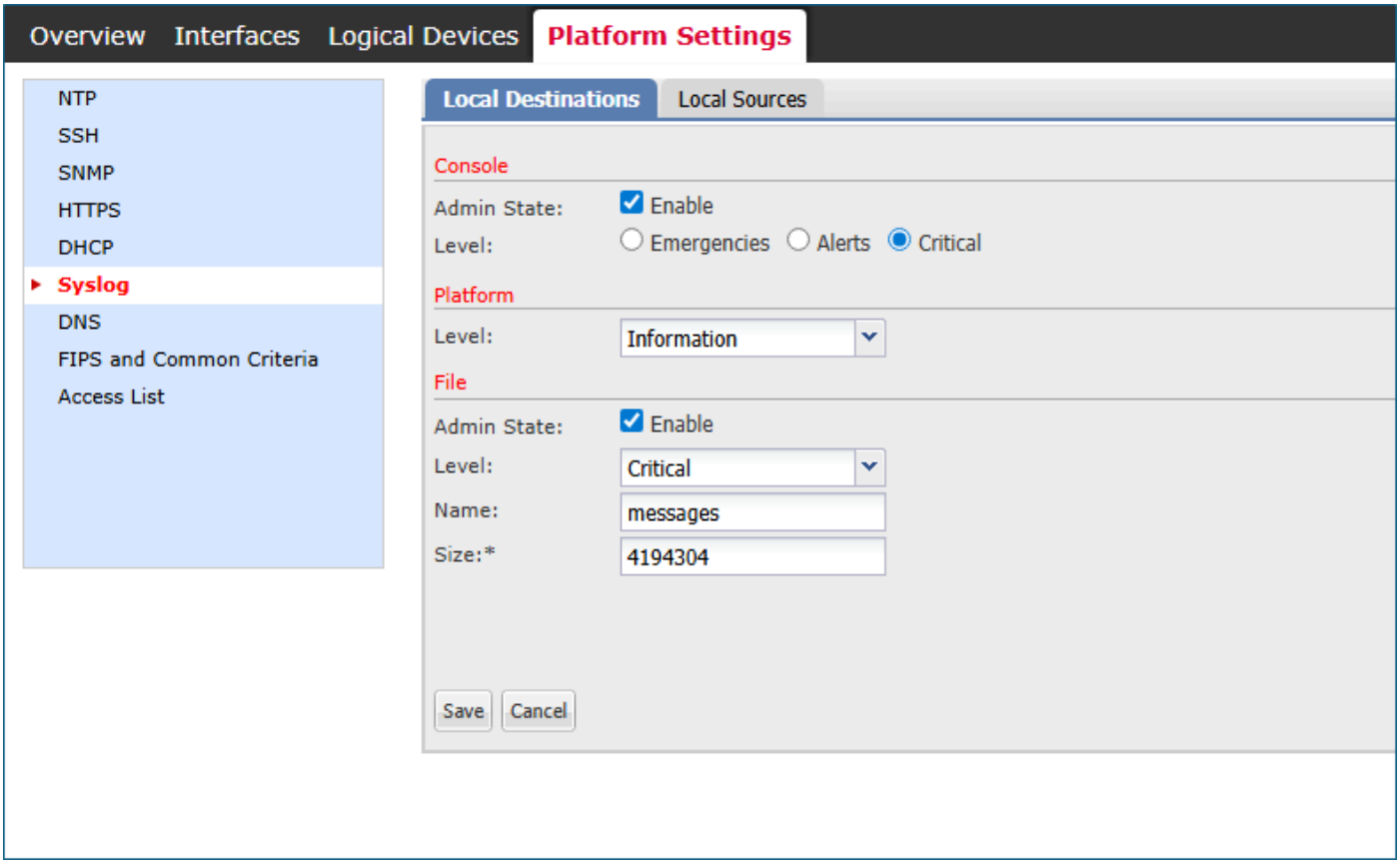
- Dans le même temps, le résultat de la commande show syslog dans la portée de surveillance montre l'adresse IP du serveur :

<#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
```

- L'interface utilisateur de Firepower Chassis Manager (FCM) > Platform Settings > Syslog n'indique pas la configuration du serveur Syslog.



fcm_syslogs_configuration.png

Étape 3. Essayez de modifier ou de supprimer le serveur 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 conclusion est que ni l'interface de ligne de commande FXOS ni l'interface utilisateur FCM ne permettent de créer, modifier ou supprimer un serveur Syslog, y compris 198.51.100.100.

Motif

Considérez trois défauts logiciels :

ID de bogue Cisco CSCvn19025

Les versions du logiciel avec la correction de ce défaut ne permettent pas la configuration Syslog

à distance FXOS dans l'interface CLI ou FCM.

ID de bogue Cisco CSCvt85766

La correction de ce défaut supprime la section « destinations distantes » du résultat de la commande FXOS show syslog.

Versions sans correctif :

<#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
```

Les versions avec le correctif ne contiennent pas la section « destinations distantes » :

<#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
```

Bien qu'il manque la section « destinations distantes », les serveurs syslog sont visibles dans la section « plate-forme ».

ID de bogue Cisco CSCwu12470

Après la mise à niveau logicielle vers la version avec le correctif de l'ID de bogue Cisco CSCvn19025, la gestion des serveurs syslog distants, c'est-à-dire la création, la modification ou la suppression, est interdite dans l'interface de ligne de commande FXOS ou l'interface utilisateur FCM. Cette limitation s'applique également aux serveurs configurés avant la mise à niveau. Malgré cela, après la mise à niveau logicielle, le logiciel FXOS affiche les serveurs syslog dans la section « platform » de la sortie de commande show syslog et envoie les messages syslog à ces serveurs. Les utilisateurs ne peuvent pas administrer la configuration syslog distante FXOS existante, qui est suivie dans l'ID de bogue Cisco CSCwu12470.

Autres informations utiles

- ID de bogue Cisco CSCvn19025
- ID de bogue Cisco CSCvt85766
- ID de bogue Cisco CSCwu12470

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.