Problemen oplossen met Connectiviteit en registratie met AMP voor FireSIGHT Management Center

Inhoud

Inleiding

Een FireSIGHT Management Center in uw installatie kan verbinding maken met de Cisco-cloud. Nadat u een FireSIGHT Management Center hebt ingesteld voor de aansluiting op de cloud, kunt u records met scans, malware detecties en quarantaine ontvangen. De records worden opgeslagen in de FireSIGHT Management Center-database als malware gebeurtenissen. Standaard stuurt de cloud malware gebeurtenissen voor alle groepen binnen uw organisatie, maar u kunt per groep beperken wanneer u de verbinding vormt. In dit document worden verschillende problemen behandeld en worden stappen beschreven voor het oplossen van problemen bij Advanced Malware Protection (AMP) van een FireSIGHT Management Center.

Port of Server is geblokkeerd in firewall

Als een FireSIGHT Management Center niet in staat is om verbinding te maken met de FireAMP Cloud Console of als u geen malware-gebeurtenissen ontvangt, moet u controleren of de vereiste poorten door de firewall zijn geblokkeerd. Een FireSIGHT Management Center gebruikt poort 443 om malware gebeurtenissen op endpoints te ontvangen vanuit de FirePOWER-console. Port 32137 is vereist voor FirePOWER-apparaten om malware raadpleging in de Cisco Cloud uit te voeren.

Lees de volgende documenten om meer te weten te komen over de vereiste poortnummers en serveradressen:

- Vereiste communicatiepoorten voor FireSIGHT System werking

- Vereiste servers voor AMP-werking

MAC-adres in gebruik

Symptoom

Wanneer u probeert een FireSIGHT Management Center voor een privécloud te registreren en de eerste verbinding uit te voeren, kunt u een bericht ontvangen dat aangeeft dat het MAC-adres al in gebruik is.

reden

Wanneer een FireSIGHT Management Center wordt vervangen door een hardwarestoring en de vervangende eenheid niet correct is geregistreerd vanuit de cloud, kunt u dit probleem ervaren.

Oplossing

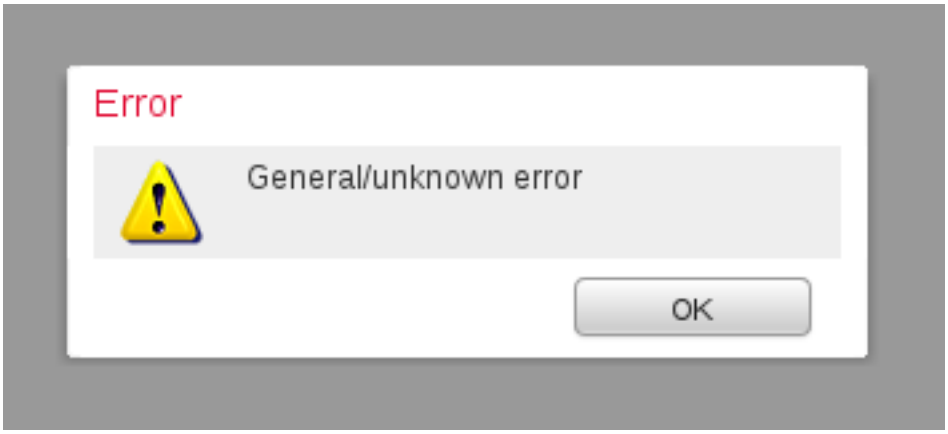
Voordat u een apparaat vervangt, moet u het FireSIGHT Management Center van de FireAMP Cloud dereguleren. U dient ook uw FireSIGHT Management Center van de FireAMP-cloud te verwijderen. Dit voorkomt dat een MAC-adres als in gebruik wordt gezien.

> **Tip**: Lees dit document om meer te weten te komen over de manier waarop u een apparaat kunt dereguleren vanuit de FireAMP Cloud en verwijder een cloud van het FireSIGHT Management Center.

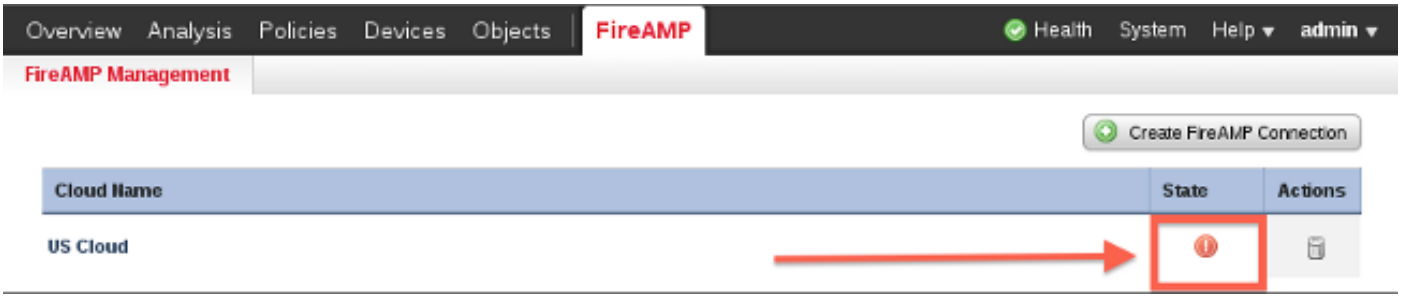
Algemene/Onbekende fout wordt weergegeven

Symptoom

Bij het aansluiten van een nieuw beeld of het vervangen van FireSIGHT Management Center op een FirePOWER-console, verschijnt er een foutmelding. Er wordt een algemene/onbekende fout weergegeven.



Wanneer het algemene/onbekende foutbericht verschijnt, wordt de toestand van de FireAMP-verbinding op FireSIGHT Management Center kritiek. De web interface toont een rood pictogram.



reden

Dit probleem doet zich voor wanneer een MAC-adres van een FireSIGHT Management Center, dat net is opgewaardeerd of vervangen, nog steeds is geregistreerd op een FireAMP-console.

Oplossing

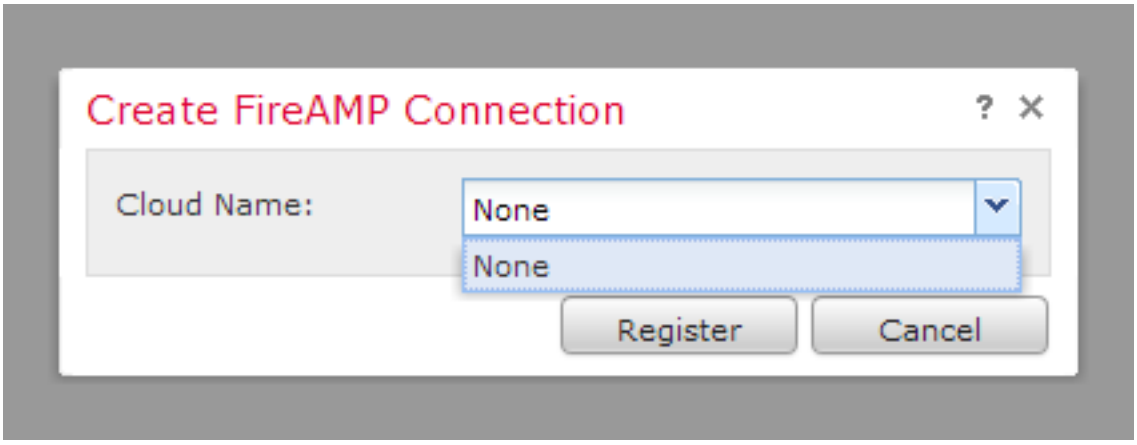
Voordat u een apparaat opnieuw installeert of vervangt, moet u het FireSIGHT Management Center van de FireAMP Cloud opnieuw installeren. U dient ook uw FireSIGHT Management Center van de FireAMP-cloud te verwijderen. Dit voorkomt dat een MAC-adres als in gebruik wordt gezien.

> **Tip**: Lees dit document om meer te weten te komen over de manier waarop u een apparaat kunt dereguleren vanuit de FireAMP Cloud en verwijder een cloud van het FireSIGHT Management Center.

Kan een cloud niet selecteren

Symptoom

Wanneer u een verbinding maakt van een FireSIGHT Management Center naar de FireAMP Cloud Console, zijn er geen uitrolopties gevonden voor de Amerikaanse Cloud of de EU Cloud.



reden

Dit probleem doet zich voor wanneer een FireSIGHT Management Center de hostname api.amp.sourcefire.com niet kan oplossen.

Om de kwestie te verifiëren, voer een nslookup uit op het CLI van FireSIGHT Management

Center. Controleer of de DNS-instellingen correct in het FireSIGHT Management Center zijn ingesteld:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
```

De volgende uitvoer wordt weergegeven wanneer DNS niet in staat is om de hostname op FireSIGHT Management Center op te lossen:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com

Server:         192.168.45.2
Address:        192.168.45.2#53

** server can't find api.amp.sourcefire.com
```

Hieronder wordt de output weergegeven als DNS juist is opgelost in FireSIGHT Management Center:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
Server:         192.168.45.1
Address:        192.168.45.1#53

Non-authoritative answer:
api.amp.sourcefire.com
Name:   xxxx.xxxx.xxxx
Address: xx.xx.xx.xx
```

Oplossing

- Als een FireSIGHT Management Center de hostname niet kan oplossen, moet u controleren of de DNS-instellingen in het Management Center juist zijn.
- Als een FireSIGHT Management Center de hostname kan oplossen maar niet in staat is om api.amp.sourcefire.com toegang te krijgen via een firewall, controleer dan de firewallregels en -instellingen.

Tijdens het maken van verbinding, als een FireSIGHT Management Center niet in staat is om de hostname op te lossen, wordt de volgende foutmelding ingelogd in httpsd_error_log:

```
Error attempting curl for FireAMP: System
```

De volgende loguitvoer toont bijvoorbeeld het Defense Center dat de curl-opdracht niet naar api.amp.sourcefire.com is voltooid:

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:38:13.433765 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:14.338174 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
```

```
[Thu Jul 18 12:38:24.352374 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
Error attempting curl for FireAMP: System (/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L
--max-redirs 5 --max-filesize 104857600 --sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H
Accept: application/vnd.sourcefire.fireamp.dc+json; version=1
https://api.amp.sourcefire.com/clouds) Failed at /usr/local/sf/lib/perl/5.10.1/SF/System.pm line
7499., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352432 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
No cloud data returned at /usr/local/sf/lib/perl/5.10.1/SF/FireAMP.pm line 145., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352478 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```

Tijdens het maken van verbinding, als het volgende bericht zonder fout is ingelogd in het httpsd_error_log, geeft dit aan dat het FireSIGHT Management Center in staat is om de hostname op te lossen:

```
getCloudData completed
```

De volgende output toont bijvoorbeeld dat een Management Center een curl opdracht naar api.amp.sourcefire.com voltooit:

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:42:54.949461 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.856432 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.931106 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```