Fehlerbehebung bei Verbindungs- und Registrierungsproblemen mit AMP auf FireSIGHT Management Center

Inhalt

Einleitung

Ein FireSIGHT Management Center in Ihrer Bereitstellung kann eine Verbindung zur Cisco Cloud herstellen. Nachdem Sie ein FireSIGHT Management Center für die Verbindung mit der Cloud konfiguriert haben, können Sie Aufzeichnungen über Scans, Malware-Erkennungen und Quarantänen empfangen. Die Datensätze werden als Malware-Ereignisse in der FireSIGHT Management Center-Datenbank gespeichert. Standardmäßig sendet die Cloud Malware-Ereignisse für alle Gruppen in Ihrem Unternehmen. Sie können jedoch bei der Konfiguration der Verbindung nach Gruppen einschränken. In diesem Dokument werden verschiedene Probleme und Schritte zur Fehlerbehebung für die AMP-Funktion (Advanced Malware Protection) eines FireSIGHT Management Center beschrieben.

Port oder Server wird in der Firewall blockiert

Wenn ein FireSIGHT Management Center keine Verbindung zur FireAMP Cloud Console herstellen oder keine Malware-Ereignisse empfangen kann, müssen Sie überprüfen, ob die erforderlichen Ports von der Firewall blockiert werden. Ein FireSIGHT Management Center verwendet Port 443, um endpunktbasierte Malware-Ereignisse von der FireAMP-Konsole zu empfangen. Der Port 32137 ist erforderlich, damit FirePOWER-Appliances Malware-Suchvorgänge in der Cisco Cloud durchführen können.

Lesen Sie die folgenden Dokumente, um mehr über die erforderlichen Portnummern und Serveradressen zu erfahren:

- Erforderliche Kommunikationsports für den Betrieb des FireSIGHT-Systems
- Erforderliche Server für den AMP-Betrieb

Verwendete MAC-Adresse

Symptom

Wenn Sie versuchen, ein FireSIGHT Management Center in einer Private Cloud zu registrieren und die erste Verbindung herzustellen, erhalten Sie möglicherweise eine Meldung, dass die MAC-Adresse bereits verwendet wird.

Grund

Wenn ein FireSIGHT Management Center aufgrund eines Hardwarefehlers ausgetauscht wird und die Ersatzeinheit nicht ordnungsgemäß von der Cloud aus registriert ist, tritt dieses Problem möglicherweise auf.

Lösung

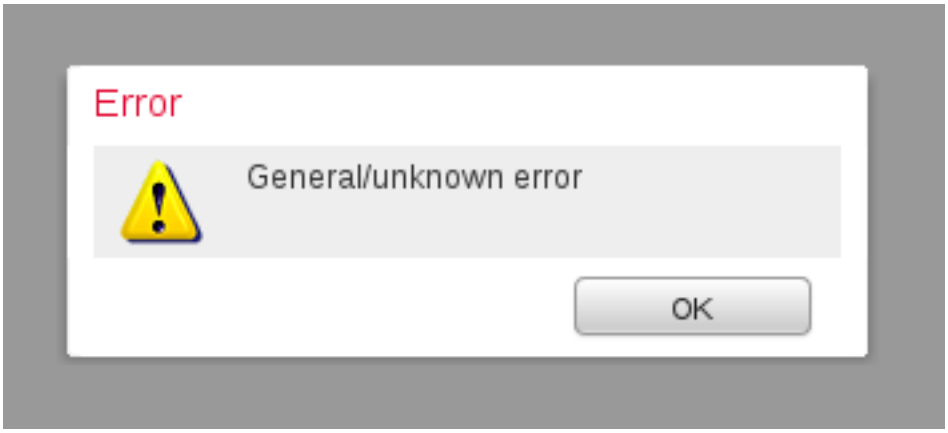
Bevor Sie eine Appliance austauschen, müssen Sie die Registrierung des FireSIGHT Management Center in der FireAMP Cloud aufheben. Sie sollten Ihr FireSIGHT Management Center auch aus der FireAMP-Cloud entfernen. Dadurch wird verhindert, dass eine MAC-Adresse als verwendet wahrgenommen wird.

> **Tipp:** In diesem Dokument erfahren Sie, wie Sie eine Appliance aus der FireAMP Cloud entfernen und eine Cloud aus dem FireSIGHT Management Center löschen können.

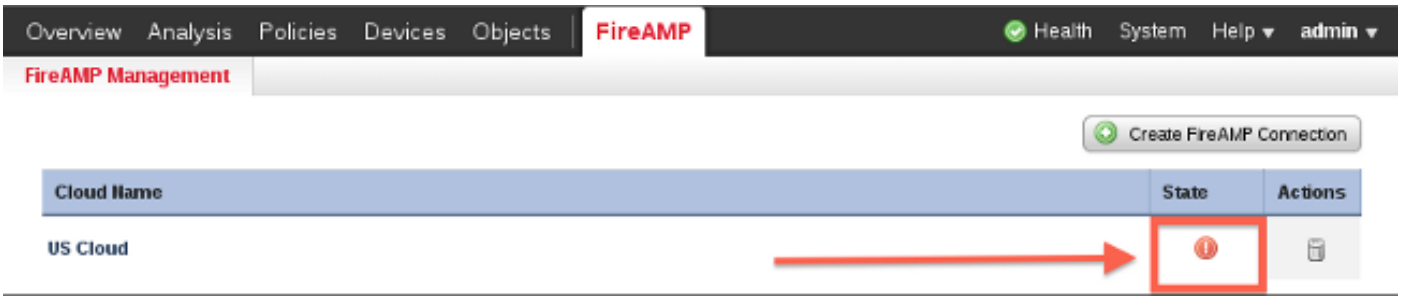
Allgemeiner/Unbekannter Fehler wird angezeigt.

Symptom

Wenn Sie ein neues Image erstellen oder ein FireSIGHT Management Center mit einer FireAMP-Konsole ersetzen, wird eine Fehlermeldung angezeigt. Es wird ein allgemeiner/unbekannter Fehler angezeigt.



Wenn die Meldung Allgemein/Unbekannt angezeigt wird, ist der Zustand der FireAMP-Verbindung im FireSIGHT Management Center entscheidend. Die Webschnittstelle zeigt ein rotes Symbol an.



Grund

Dieses Problem tritt auf, wenn eine MAC-Adresse eines FireSIGHT Management Center, für das gerade ein neues Image erstellt oder ersetzt wurde, noch in einer FireAMP-Konsole registriert wird.

Lösung

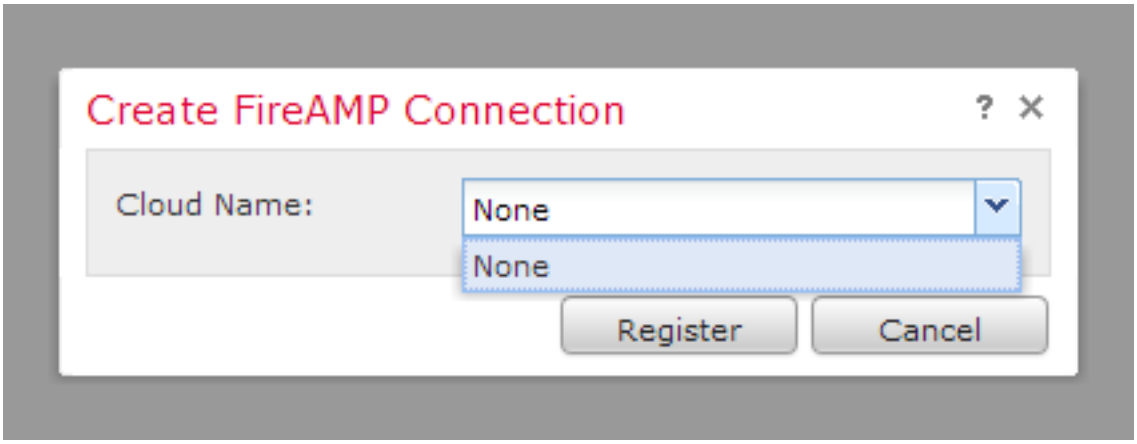
Bevor Sie ein neues Image erstellen oder eine Appliance ersetzen, müssen Sie die Registrierung des FireSIGHT Management Center in der FireAMP Cloud aufheben. Sie sollten Ihr FireSIGHT Management Center auch aus der FireAMP-Cloud entfernen. Dadurch wird verhindert, dass eine MAC-Adresse als verwendet wahrgenommen wird.

> **Tipp:** In diesem Dokument erfahren Sie, wie Sie eine Appliance aus der FireAMP Cloud entfernen und eine Cloud aus dem FireSIGHT Management Center löschen können.

Keine Cloud-Auswahl möglich

Symptom

Beim Herstellen einer Verbindung von einem FireSIGHT Management Center zur FireAMP Cloud Console sind keine Dropdown-Optionen für die US-Cloud oder die EU-Cloud verfügbar.



Grund

Dieses Problem tritt auf, wenn ein FireSIGHT Management Center den Hostnamen

api.amp.sourcefire.com nicht beheben kann.

Um das Problem zu überprüfen, führen Sie eine nslookup-Suche in der CLI von FireSIGHT Management Center durch. Überprüfen Sie, ob die DNS-Einstellungen im FireSIGHT Management Center ordnungsgemäß konfiguriert sind:

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

Die folgende Ausgabe wird angezeigt, wenn DNS den Hostnamen im FireSIGHT Management Center nicht auflösen kann:

```
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
```

Im Folgenden sehen Sie die Ausgabe, wenn DNS im FireSIGHT Management Center ordnungsgemäß aufgelöst wird:

```
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
```

Lösung

- Wenn ein FireSIGHT Management Center den Hostnamen nicht auflösen kann, müssen Sie überprüfen, ob die DNS-Einstellungen im Management Center korrekt sind.
- Wenn ein FireSIGHT Management Center den Hostnamen auflösen kann, aber nicht über eine Firewall auf api.amp.sourcefire.com zugreifen kann, überprüfen Sie die Firewall-Regeln und -Einstellungen.

Wenn ein FireSIGHT Management Center den Hostnamen nicht auflösen kann, wird während der Verbindungserstellung die folgende Fehlermeldung im httpsd_error_log protokolliert:

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

Die folgende Protokollausgabe zeigt beispielsweise, dass das Defense Center den Befehl curl auf api.amp.sourcefire.com nicht abgeschlossen hat:

```
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/
```

Wenn beim Erstellen der Verbindung die folgende Meldung fehlerfrei im httpsd_error_log protokolliert wird, weist dies darauf hin, dass das FireSIGHT Management Center den Hostnamen auflösen kann:

```
getCloudData completed
```

Die folgende Ausgabe zeigt beispielsweise, dass ein Management Center einen Curl-Befehl für api.amp.sourcefire.com ausführt:

```
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/
```