Abrufen von System Event Archive (SEA)-Protokollen von Catalyst 6500/6800-Plattformen

Inhalt

Einführung

In diesem Dokument wird die Funktion der Systemereignisarchiv (SEA) im Allgemeinen beschrieben, die auf den Catalyst 6500/6800-Plattformen verfügbar ist. Außerdem werden Schritte zum Auffinden der SEA-Archive beschrieben, um diese in Textformate für weitere Analysen umzuwandeln.

Hintergrundinformationen

System Events Archive (SEA) ist eine der Sicherheitslücken im Bereich Gerätemanagement der Cat 6500/6800-Plattformen. SEA aktiviert die CPUs im Switch erstellt Archive der Ereignisse, und diese Archive werden in einem lokalen, nicht flüchtigen Dateisystem gespeichert.

Die SEA verwaltet zwei Dateien: sea_log.dat und sea_console.dat.

sea_log.dat = Archiv der Ereignisse, die von jeder Anwendung im IOS gemeldet wurden (z. B. GOLD)

sea_console.dat = Archiv der Konsolenmeldungen

SEA-Funktion weist 32 MB Speicher für jede dieser Dateien (also insgesamt 64 MB) in einem lokalen Dateisystem zu - z.B. bootdisk:

Beachten Sie, dass diese 32 MB ein **zirkulärer** Puffer ist und die ältesten Nachrichten überschreiben wird.

Die Konfigurationsanleitungen (im Abschnitt "Relavant Documents" weiter unten) enthalten Befehle, um zu überprüfen, ob das Feature aktiviert ist, das für das Archiv ausgewählte Dateisystem, wie Archivdateien gelöscht werden usw.

Beispielbefehle:

Anzeigeprotokollierungssystem

Anzeigeprotokolldatenträger

Anzeige der Systemgröße

Löschprotokollierungssystem

Suchen von SEA-Protokollen

Führen Sie den Befehl "dir all" aus, um die Dateien sea_console.dat und sea_log.dat zu finden.

In einer Catalyst 6800 VSS-Konfiguration:

```
6800-A# show switch virtual

Switch-Modus: Virtueller Switch
Domänennummer des virtuellen Switches: 10
Lokale Switch-Nummer: 1
Betriebsrolle des lokalen Switches: Virtueller Switch aktiv
Peer-Switch-Nummer: 2
Betriebsrolle des Peer-Switches: Virtueller Switch Standby

6800-A#-Verzeichnis alle

<Snip>

Verzeichnis von bootdisk:/ <== Von Sw1
    1 -rw- 33554432 014 03:11:52 +00:00 sea_console.dat
    3 -rw- 33554432 8. März 2014 03:12:30 +00:00 sea_log.dat

<Snip>

Verzeichnis der Slavebootdisk:/ <=== Von Sw2
    1 -rw- 33554432 10. März 2014 05:12:12 +00:00 sea_log.dat
    3 -rw- 33554432 10. März 2014 05:12:50 +00:00 sea_console.dat

<Snip>
```

In einer Catalyst 6500 VSS-Konfiguration:

```
VS6500# Switch-Virus anzeigen
Switch-Modus: Virtueller Switch
Domänennummer des virtuellen Switches: 1
Lokale Switch-Nummer: 1
Betriebsrolle des lokalen Switches: Virtueller Switch aktiv
Peer-Switch-Nummer: 2
Betriebsrolle des Peer-Switches: Virtueller Switch Standby

VS6500#-Verzeichnis alle

<Snip>

Verzeichnis von sup-bootdisk:/ <== Von Sw1
    1 -rw- 33554432, 29. August 2014, 14:06:42 -04:00 sea_console.dat
    3 -rw- 33554432 Nov. 8 2012 16:59:38 -05:00 sea_log.dat
```

```
<Snip>

Verzeichnis von Slavesup-bootdisk:/ <= Von Sw1
    1 -rw- 33554432 Sep. 8 2014 08:34:02 -04:00 sea_log.dat
    2 -rw- 33554432 19. März 2015 12:36:16 -04:00 sea_console.dat

<Snip>
```

Abrufen von SEA-Protokollen

Es wird dringend empfohlen, dem Dateinamen Folgendes hinzuzufügen:

Switch-Name

Switch-Nr. (bei VSS)

Modul-Nr. (falls Module 5 und 6 im selben Chassis vorhanden sind)

Dateiinhalte (Seekonsole oder Protokoll)

Datum

Im Folgenden finden Sie die Schritte zum Konvertieren der .dat-Dateien in Textdateien.

(1) Umwandeln der Protokolle in Text

USe führt folgende Befehle aus, um die Archive in Text zu konvertieren. Bitte beachten Sie, dass "show logging system console" zum Konvertieren der Datei sea_console.dat verwendet wird und "show logging system disk" zum Konvertieren der Datei sea_log.dat verwendet wird.

Aus einer Catalyst 6800 VSS-Konfiguration (obiges Beispiel):

Für Aktiv/Sw1:

6800A# show logging system console file bootdisk:sea_console.dat | Redirect bootdisk:6800A-Sw1-SEA-Console-Jul082015.txt

6800A# show logging system disk bootdisk:sea_log.dat | Redirect bootdisk:6800A-Sw1-SEA-Log-Jul082015.txt

Für Standby/Sw2:

6800A# show logging system console file slavebootdisk:sea_console.dat | Redirect slavebootdisk:6800A-Sw2-SEA-Console-Jul082015.txt

6800A# show logging system disk slavebootdisk:sea_log.dat | Redirect slavebootdisk:6800A-Sw2-SEA-Log-Jul082015.txt

(2) Stellen Sie sicher, dass die Textdateien erstellt wurden und sich im Dateisystem befinden:

Stellen Sie sicher, dass die Dateigrößen nicht 0 sind. Es ist NICHT erforderlich, dass die Textdateien 32 MB groß sind.

32 MB ist nur ein "zugewiesener" Speicherplatz für die .dat-Dateien, die nicht unbedingt verwendet werden.

Darüber hinaus sind die Dateien in verschiedenen Formaten - Daten vs. TXT.

```
6800A#-Rootdisk:

<Snip>

   56 -rw- 57875 Jul 9 2015 19:32:38 +00:00 6800A-Sw1-SEA-Console-
Jul082015.txt
  57 -rw- 31136641 Jul 9 2015 19:53:56 +00:00 6800A-Sw1-SEA-Log-
Jul082015.txt

<Snip>

6800A# dir slavebootdisk:

<Snip>

   56 -rw- 5325 Jul 9 2015 20:07:31 +00:00 6800A-Sw2-SEA-Console-
Jul082015.txt
  57 -rw- 2899567 Jul 9 2015 20:12:47 +00:00 6800A-Sw2-SEA-Log-
Jul082015.txt

<Snip>
```

(3) Stellen Sie sicher, dass die Dateien verfügbar/lesbar sind, bevor Sie sie auf den TFTP/FTP-Server exportieren.

```
6800A#more bootdisk:6800A-Sw1-SEA-Log-Jul082015.txt
SCHNELL: MM/TT/JJJ HH:MM:SS SW/MOD/SUB: SEV, COMP, MELDUNG
========================================================================
========================================
 1: 09.07.15 19:38:00 05.01-1: MAJ, GOLD,
diag_get_fabric_link_status:fexmgr_axs_fport_info_sdp_up hat api_rc=1
zurückgegeben
 2: 09.07.15 19:37:57 1/5/-1: MAJ, GOLD,
diag_get_fabric_link_status:fexmgr_axs_fport_info_sdp_up hat api_rc=1
zurückgegeben
 3: 09.07.15 19:37:57 1/5/-1: MAJ, GOLD,
diag_get_fabric_link_status:fexmgr_axs_fport_info_sdp_up hat api_rc=1
zurückgegeben
 4: 09.07.15 19:37:52 05.01-1: MAJ, GOLD,
diag_get_fabric_link_status:fexmgr_axs_fport_info_sdp_up hat api_rc=1
zurückgegeben
 5: 09.07.15 19:37:52 05.01-1: MAJ, GOLD,
diag_get_fabric_link_status:fexmgr_axs_fport_info_sdp_up hat api_rc=1
zurückgegeben
```

Relevante Dokumente

SEA-Konfigurationsleitfaden für 12.2SX-Versionen

SEA-Konfigurationsleitfaden für 15.0SY-Versionen