ESR Berichtenbepaling

Inhoud

Inleiding

Dit document beschrijft hoe u de verwerking van een bericht kunt bepalen met de e-maillogs die u van verschillende opdrachten op de Cisco e-mail security applicatie (ESA) hebt opgeroepen.

Voorwaarden

De informatie in dit document is gebaseerd op:

- ESA
- Alle versies van AsyncOS

Berichtentracering

Als u AsyncOS voor e-mail versie 6.0 of later gebruikt, is de meest effectieve manier om te bepalen wat er met een bepaald bericht is gebeurd het gebruik van de pagina Berichttracering in het tabblad Monitor. Dit stelt u in staat om met een verscheidenheid aan opties in een makkelijk te gebruiken web interface te zoeken.

Als u een oudere versie uitvoert of alle loglijnen wilt verzamelen voor de doeleinden van de probleemoplossing, gebruikt u de opdrachten **vet** of **voorkomen** zoals in de volgende secties beschreven wordt.

Opdracht Afronden

Als u AsyncOS voor e-mail versie 5.1.2 of hoger hebt, maakt de CLI **Findvent** opdracht het eenvoudiger om naar een specifiek bericht te zoeken. **Findevent** laat je zoeken door de envelop van, de envelop ontvanger, of het bericht Onderwerp. Dit kan ook ongeacht het geval worden gedaan. Zodra u uw bericht hebt gevonden, kunt u elke loglijn die voor dat bericht relevant is, teruggeven. Als je **findevent** zonder argumenten runt, geeft deze een wizard die je door het proces leidt. Zoals altijd, kunt u de **help** opdracht gebruiken om de korte vorm te leren:

```
> help findevent
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```

Het eerste formulier zoekt een specifieke envelop van, onderwerp, of envelop naar binnen de genoemde log_name en maakt een lijst van de BerichtID's (MID's) die overeenkomen. De -i vlag kan worden gebruikt voor niet-gevalsgevoelige zoekopdrachten.

Het tweede formulier geeft alle loglijnen voor de betreffende MID weer.

Als u een oudere versie hebt, kan de CLI **grep** opdracht worden gebruikt om hetzelfde te bereiken. Het gebruik van de **grep**-opdracht vereist echter meer gedetailleerde kennis van de wijze waarop de ESA's blogberichten registreren.

Opdracht Grep

De eerste uitdaging bij het zoeken naar postlogs is het vinden van uw bericht. Je kan dit doen als je zoekt naar de zender, de ontvanger of de persoon. Nadat u uw bericht hebt gevonden, is het belangrijk om te begrijpen hoe de postlogbestanden zijn georganiseerd. De e-mailgebeurtenissen van de contentbeveiliging worden afkortingen gegeven. De belangrijkste gebeurtenissen zijn ICID, MID, RID en DCID.

Injectieverbinding-ID (ICID): Wanneer een externe host een verbinding met het apparaat maakt, krijgt die verbinding een ICID toegewezen. Eén ICID kan veel MID's kweken.

> Opmerking: **ICID 0** definieert een bericht dat van zichzelf werd geïnjecteerd. In feite verwijst het cijfer 0 na een ICID of DCID naar sessies open naar of van het aansluitnetadres van het apparaat.

MID: Zodra een verbinding wordt gevestigd, **van** elke succesvolle Eenvoudige Post Transfer Protocol (mtp) **van:** commando maakt een nieuwe MID. Een enkele MID kan veel RID's kweken.

Gebruikersnaam (RID): Elke begunstigde (in: CC: of Bcc krijgt een RID. RID's paaien alleen meerdere DCID's als er een zachte aanval (verbindingsfout) is en de levering wordt herleid.

Delivery Connection-id (DCID): Elke begunstigde die naar hetzelfde doeldomein gaat, ontvangt dezelfde DCID tot aan de grenzen van het ontvangende systeem. Als de ontvangers van een bericht allemaal naar hetzelfde domein gaan, dan is er één DCID voor alle RID's. Als in plaats daarvan elke RID naar een afzonderlijk domein gaat, is er een één-op-één correlatie.

> Opmerking: **DCID 0** definieert een bericht dat nooit is verstuurd. In feite verwijst het cijfer 0 na een ICID of DCID naar sessies open naar of van het aansluitnetadres van het apparaat.

Als je je bericht vindt, vind je de MID. Dan neem je de MID en de ICID en RID. Met het ICID kunt u de SenderBase Reputation Score (SBRS) voor de zender bepalen. Met het RID en dan het DCID, kunt u bepalen wat er gebeurde toen de ESA de levering probeerde.

> Opmerking: Zodra u de MID, ICID en DCID hebt, kunt u alle rijen voor dat bericht in één **grep** ophalen, als de oorsprong van het bericht niet ouder is dan uw oudste maillogbestand.

```
example.com> grep -e " MID 11123" -e " ICID 11092" -e " DCID 23349" mail_logs
```

Voorbeeld

1. Onderwerp bericht zoeken:

```
example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> test
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Mon Jan 23 10:25:03 2006 Info: SMTP listener testpairlist starting
Tue Jan 24 12:10:15 2006 Info: Message aborted MID 8 Dropped by filter
'testdrop'
Tue Jan 31 23:55:38 2006 Info: MID 32 Subject 'testmsgquarantine'
Wed Feb 1 00:23:59 2006 Info: MID 62 Subject 'testmsgquarantine'
Wed Feb 1 00:27:48 2006 Info: MID 64 Subject 'testmsg2'
Wed Feb 1 22:30:37 2006 Info: MID 80 Subject 'test zip'
Wed Feb 1 22:37:51 2006 Info: MID 83 Subject 'FW: test zip'
Wed Feb 1 22:41:50 2006 Info: MID 84 Subject 'FW: test zip'
Fri Feb 3 15:17:47 2006 Info: MID 94 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
```

Dit leverde verschillende overeenkomsten op die **test** in het onderwerp bevatten. Het bericht werd om ongeveer 15:42 uur verstuurd, zodat u die MID kunt gebruiken voor de volgende zoekopdracht.

Hier volgen enkele belangrijke opmerkingen over de vragen:

Wil je dat deze zoekopdracht ongevoelig is? [Y]>
Als u **ja** op deze vraag antwoordt, vindt het inzendingen ongeacht case.

Wil je de blogs achtervolgen? [N]>
Als u **ja** op deze vraag antwoordt, vindt het enkel nieuwe ingangen aangezien zij worden gegenereerd. U kunt niet alle logbestanden doorzoeken. Klik op **Nee** om alle logbestanden te doorzoeken.

Wilt u de uitvoer pagineren? [N]>
Als u **ja** op deze vraag antwoordt, geeft het de ingangen één pagina tegelijkertijd weer. Dit is handig als u een algemene zoekopdracht moet uitvoeren en verwacht veel items te herstellen. Hierdoor kunnen de items niet van de display worden uitgeschakeld.

2. MID zoeken:

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> MID 96
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:41:43 2006 Info: Start MID 96 ICID 10394
Fri Feb 3 15:41:43 2006 Info: MID 96 ICID 10394 From: <bob@example.net>
Fri Feb 3 15:41:58 2006 Info: MID 96 ICID 10394 RID 0 To:
<nasir@example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Message-ID
<4o8836$30@mail.example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 ready 23 bytes from
<bob@example.net>
Fri Feb 3 15:42:06 2006 Info: MID 96 matched all recipients for
per-recipient policy DEFAULT in the outbound table
Fri Feb 3 15:42:06 2006 Info: MID 96 antivirus negative
Fri Feb 3 15:42:06 2006 Info: MID 96 queued for delivery
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: MID 96 RID [0] Response '2.6.0
<4o8836$30@mail.example.com> Queued mail for delivery'
Fri Feb 3 15:42:06 2006 Info: Message finished MID 96 done
```

Merk op dat de MID-items meer informatie geven over de manier waarop het bericht wordt verwerkt. De MID-items verwijzen ook naar het ICID en het DCID. Als je meer wilt weten over de inkomende verbinding, neem dan de ICID in. Als je meer wilt weten over wat er gebeurde toen de ESA de levering probeerde, neem dan de DCID op.

3. Om te bepalen waar het bericht werd geleverd, moet u naar de DCID zoeken.

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> DCID 14
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:42:06 2006 Info: New SMTP DCID 14 interface 192.168.0.199
address 10.1.1.112 port 25
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:11 2006 Info: DCID 14 close
```

Merk op dat het bericht vanaf de 192.168.0.1999 is verzonden naar de host met IP-adres 10.1.1.12 via Port 25.

Als de levering niet werd geprobeerd, maar het bericht werd **in de wachtrij geplaatst voor levering**, geeft dit aan dat het systeem problemen kan hebben bij de communicatie met de doelserver. U kunt de **hoststatus** van de CLI gebruiken om te zien of de status van de ontvangende host **Down** is en om te controleren of de bestelde IP's overeenkomen met of de MTP-routes voor het doeldomein of de openbare MX-records, al naar gelang van toepassing.