Hoe kan ik een postnetsituatie in de ESA identificeren en aanpakken?

Inhoud

Inleiding

In dit document wordt beschreven hoe een e-maillus op de e-mail security applicatie (ESA) kan worden herkend.

Achtergrondinformatie

Mail Loops kan worden aangegeven door berichten met dezelfde Message-ID die meer dan drie keer zijn ingespoten. Mail Loops kan symptomen van hoge CPU, trage levering en algehele prestatiekwesties veroorzaken. Gewoonlijk zou de meer dan eenmaal geïnjecteerde boodschap-ID's een achteruitgang betekenen, maar soms worden ze meer dan eens geïnjecteerd vanwege problemen, of het kan een slordig spammer zijn die hetzelfde spambericht blijft injecteren met dezelfde Bericht-ID.

Meestal wordt een maillus veroorzaakt door een probleem met de e-mailinfrastructuur dat hetzelfde bericht of dezelfde reeks berichten verstuurt die van mailserver naar mailserver eindig rondlopen. Hoewel deze berichten zichzelf heel lang op deze manier kunnen onderhouden, is dat niet goed voor de bandbreedte van het netwerk of de kosten van de ESA-verwerking.

Oplossing

Het identificeren van een maillus, als je vermoedt dat dit het probleem kan zijn, is meestal makkelijk, hoewel je het moet zien.
Log in op de opdrachtregel interface (CLI) van het systeem en geef een van deze opdrachten uit, of beide omdat u de beste voordelen hebt:

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

Met name voor het zoeken op Message-ID, als u terugkerende voorbeelden ziet van exact dezelfde ID, dan weet u dat u een postlus hebt. Maar soms is dit niet genoeg, omdat een van de mailservers die hetzelfde bericht terugbellen, de berichtgeving-ID header kan veranderen of

verwijderen. Dus als je niets identificeerbaar vindt met de bericht-ID controle, ga dan door en probeer de onderwerpregel.

Aangenomen dat u het loopende bericht door de Bericht-ID hebt weten te vinden zult u ook andere informatie over het bericht en zijn ouderverbinding (ICID) willen weten. Gezien de Bericht-ID en een MID in de zelfde loglijn kunt u uitvoeren:

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

Gezien de resulterende output daar kunt u de relevante ICID en DCID vinden en uitvoeren:

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

U dient nu de volledige verbinding te hebben - een bericht-transactie en u kunt zien waar deze vandaan kwam en waar deze aan is geleverd (indien dit al is gebeurd). Zodra u het achterloopbericht hebt geïdentificeerd, is uw volgende stap om een blik op het bericht te krijgen zodat u het probleem kunt oplossen. Zonder de oorzaak van de loop te repareren is het waarschijnlijk dat dit bericht en anderen blijven herhalen of dat het probleem zich binnenkort opnieuw zal voordoen.

Maak een vergelijkbaar berichtfilter:

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

Stel deze wijziging nu in en geef deze opdracht uit om het bericht te bekijken:

```
tail looper
```

Met de informatie die u over het afstandssysteem kunt opdoen door naar de postbestanden te kijken en andere informatie die u kunt opvragen door naar het bericht zelf te kijken, kunt u bepalen waar uw probleem zich bevindt.

Hoe kunt u voorkomen dat er postlijnen plaatsvinden?

In complexe omgevingen kan dit moeilijk zijn - begrijpen hoe de mail in uw omgeving stroomt en hoe een nieuwe netwerkverandering, op de ESA of op een ander apparaat, dat verkeer van essentieel belang zal beïnvloeden. Eén veel voorkomende oorzaak van de tweede mailreeks is de verwijdering van de ontvangen header. De ESA zal een postlus automatisch detecteren en stoppen als er 100 Ontvangen kopregels in een bericht staan, maar het ESA laat wel toe deze header te verwijderen, wat vaak leidt tot een slechte maillus. Tenzij er een *echt* goede reden is, schakelt u de Ontvangen header niet uit of laat deze verwijderen.

Hieronder staat een filtervoorbeeld dat u kunt helpen om een maillus te voorkomen of te repareren:

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
 if (header("X-ExtLoopCount2")) {
```

```
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
                  $RemoteIP");}}
           else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
         else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
       else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
     else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
   else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
 else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```