Comment est-ce que je peux identifier et adresser une situation de boucle de messagerie sur l'ESA ?

Contenu

Introduction

Ce document décrit comment identifier une boucle de messagerie sur l'appliance de sécurité du courrier électronique (ESA).

Informations générales

Des boucles de messagerie peuvent être indiquées par les messages avec le même Message-ID qui ont été injectés plus de 3 fois. Les boucles de messagerie peuvent entraîner des symptômes de CPU de haute, de livraison lente et de questions de performance globale. Normalement les id de message injectés plus d'une fois indiqueraient le bouclage, mais parfois ils sont injectés plus d'une fois en raison des problèmes, ou ce pourrait être un spammer désordonné qui continue à injecter le même message spam avec le même Message-ID.

Plus typique une boucle de messagerie est provoqué par par un problème d'infrastructure d'email qui envoie le même message ou ensemble de messages emballant autour de votre réseau du serveur de messagerie au serveur de messagerie sans fin. Tandis que ces messages peuvent se maintenir amusés de cette façon pendant très un longtemps, ce n'est pas une bonne chose pour votre bande passante de réseau ou le coût de traitement ESA engagé.

Solution

Identifier une boucle de messagerie, si vous suspectez que ceci puisse être le problème, est habituellement assez facile bien que vous deviez le regarder.
Connectez-vous dans l'interface de ligne de commande (CLI) du système et émettez une de ces commandes, ou chacun des deux comme vous trouvez meilleur vous bénéficient :

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

En particulier pour la recherche sur le Message-ID, si vous voyez des exemples récurrents exactement du même ID puis vous saurez que vous avez une boucle de messagerie. Toutefois parfois ce n'est pas assez, parce qu'un du rassemblement de serveurs de messagerie soutiennent le même message pourrait être utilement changeant ou retirant l'en-tête de Message-ID. Ainsi si vous n'obtenez rien identifiable avec le contrôle de Message-ID avancez et essayez le contrôle soumis.

Vous supposer que vous avez géré pour trouver le message de bouclage par le Message-ID voudra également découvrir d'autres informations sur le message et sa connexion de parent (ICID). Etant donné le Message-ID et un MID dans la même ligne de log vous pouvez exécuter :

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

Etant donné la sortie résultante là vous peut trouver l'ICID et le DCID appropriés et les exécuter :

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

Maintenant vous devriez avoir la connexion complète - transaction de message et pouvez voir à où elle est provenue et à où elle a été fournie (si cela s'est déjà produite). Une fois que vous avez identifié le message de bouclage, votre étape suivante est d'obtenir un regarder le message de sorte que vous puissiez réparer le problème. Sans réparer la cause de la boucle, il est probable que ce message et d'autres continuent à faire une boucle ou que le problème se reproduira bientôt.

Créez un filtre de message semblable à celui-ci :

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

Maintenant commettez cette modification et fournissez cette commande au contrôle le message :

```
tail looper
```

Avec les informations vous pouvez gagner au sujet du système distant en regardant les logs de messagerie, et d'autres informations que vous pouvez obtenir en regardant le message lui-même, vous devraient pouvoir déterminer où votre problème est.

Comment pouvez-vous empêcher des boucles de messagerie de se produire ?

Dans les environnements complexes ceci peut être difficile - comprenant comment des flux de courrier dans votre environnement et comment une nouvelle modification de réseau, sur l'ESA ou à un autre périphérique, affectera que le trafic est clé. Une cause classique des boucles de messagerie d'emballement est la suppression de l'en-tête reçue. L'ESA automatiquement détectera et arrêtera une boucle de messagerie quand il voit 100 en-têtes reçues dans un message, mais l'ESA tient compte de la suppression de cette en-tête, qui mènent souvent à une mauvaise boucle de messagerie. À moins qu'il y ait une bonne raison de *really* à, s'il vous plaît n'arrêtez pas l'en-tête reçue, ou causez-les d'être retiré.

Est ci-dessous un exemple de filtre qui peut aider à empêcher ou réparer une boucle de messagerie :

```
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"); }
```