

ESA でメール ループの状況を特定して対処するにはどうしますか。

目次

[はじめに](#)

[背景説明](#)

[解決策](#)

[どのようにメール ループが発生することを防ぐことができますか。](#)

概要

この資料に E メール セキュリティ アプライアンス (ESA) のメール ループを識別する方法を記述されています。

背景説明

Mail ループは 3 回以上インジェクトされた同じメッセージID のメッセージによって示すことができます。 Mail ループにより高CPU、遅い配信および全体的なパフォーマンス問題の現象を引き起こす場合があります。 通常インジェクトされたメッセージID は何度もループを示しますが、時々問題が理由で何度もインジェクトされます、または同じメッセージID の同じスパム メッセージをインジェクトし続けるのは薄く水っぽいスパムの発信者である可能性があります。

もっと一般的に メール ループはメッセージの同じメール サーバからのメール サーバにネットワークのまわりで際限なく競争するメッセージカセットを送信する メール インフラストラクチャ問題によって引き起こされます。 これらのメッセージが彼ら自身を非常に長い 時間の間このように心に抱いておく場合がある間、それはネットワーク帯域幅または負われる ESA 加工費のためのよい事柄ではないです。

解決策

これは問題であるかもしれないことを疑えばメール ループを識別することは通常それをじろじろ見る必要があるけれどもかなり容易です。

システムの Command Line Interface (CLI) にログイン すれば、これらのコマンドの 1 つを発行して下さい、最もよい見つけるように両方とも寄与します:

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

メール ループがあることを同じ ID の繰り返し例をそして丁度見れば特にメッセージID の検索のために、ために確認できます。 時々これがかもしれ役立ってメッセージID ヘッダを変更するか、または削除しますであるには十分どんなにでなくても、メール サーバ再び集まることの 1 つ

が支持するので同じメッセージは。従って何もメッセージID チェックと確認可能得なかったら先に行き、認証対象チェックを試みて下さい。

メッセージID によってループ メッセージを見つけることをどうにかしてこと仮定することはまたメッセージおよび親接続 (ICID) についての他の情報を調べたいと思います。同じ測程線のメッセージID および MID を与えられて実行できます:

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

結果として生じる出力にそこに与えられて関連した ICID および DCID を見つけ、実行できます:

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

この場合 (それが既に発生していたら) 完全な接続メッセージ トランザクションがあるはずで、どこにから来た、そしてどこに提供されたか表示できます。ループ メッセージを識別したら、次のステップは問題を解決できるようにメッセージの外観を得ることです。ループの原因の固定なしで、このメッセージおよび他がループし続けるか、または問題がやがて再発すること可能性が高いといえます。

この 1 と同じようなメッセージ フィルターを作成して下さい:

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

この場合その変更を保存し、メッセージをチェックするためにこのコマンドを発行して下さい:

```
tail looper
```

情報を利用してリモート システムについてによってメール ログの検知得ることができ、によってメッセージ自体の検知、得ることができる他の情報は問題がどこにあるか判別できるはずです。

どのようにメール ループが発生することを防ぐことができますか。

複雑な環境でこれはトラフィックはキーであること ESA のまたは別のデバイスへの新しいネットワーク変更が、どのように影響を与えるか-知識どのように環境のメール フロー、そして困難である場合もあります。逃亡メール ループの 1 つのコモン コーズは受け取ったヘッダの削除です。ESA は自動的に頻繁に悪いメールにループを導くメッセージの 100 つの受け取ったヘッダを見るが、ESA がこのヘッダの削除を可能にする場合メール ループを検出する、停止させます。*really* もっともな理由がへなかつたら、受け取ったヘッダを消さなければ、またはそれらを取除きます。

メール ループの防ぐか、または固定を助けることができるフィルタ例は下記にあります:

```
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"); }
```