

Queest-ce que la « réception abandonnée » et la « réception abandonnée par l'expéditeur » dans les logs de messagerie fait-elle signifient ?

Contenu

[Introduction](#)

[Que la « réception abandonnée » dans les logs de messagerie signifie-t-elle ?](#)

[Queest-ce que la « réception abandonnée par l'expéditeur » dans les logs de messagerie signifie ?](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit la différence entre la « réception abandonnée » et la « réception abandonnée par l'expéditeur » comme vu dans le cheminement de logs et de message de messagerie associé avec l'appliance de sécurité du courrier électronique de Cisco (ESA) et l'appliance de Gestion de sécurité Cisco (SMA).

Que la « réception abandonnée » dans les logs de messagerie signifie-t-elle ?

La « réception du MID XXX abandonnée » indique que la connexion du côté réception a été finie par un problème de réseau, ou l'expéditeur juste a fermé la connexion abruptement. Le « MID XXX » est l'ID de message du message qui ne pourrait pas être avec succès injecté. Dans de nombreux cas de voir la « réception abandonnée » lui est un Pare-feu ou un périphérique de sécurité SMTP-averti qui interrompt le trafic.

L'exemple suivant montre un client distant établissant une connexion de SMTP à l'ESA suivi de la fermeture de connexion au-dessous de la couche application, typiquement vue quand l'appliance reçoit un indicateur prématuré de TCP [FIN] ou une connexion remise à l'état initial :

```
Thu Aug 14 11:04:31 2014 Info: New SMTP ICID 10293 interface Management
(192.168.0.199) address 192.168.0.200 reverse dns host ns.example.com verified no
Thu Aug 14 11:04:31 2014 Info: ICID 10293 RELAY SG RELAY_SG match 192.168.0.200
SBRS not enabled
Thu Aug 14 11:04:51 2014 Info: Start MID 1404 ICID 10293
Thu Aug 14 11:04:51 2014 Info: MID 1404 ICID 10293 From: <user@domain.com>
Thu Aug 14 11:05:00 2014 Info: MID 1404 ICID 10293 RID 0 To: <end_user@example.com>
Thu Aug 14 11:05:36 2014 Info: ICID 10293 lost
Thu Aug 14 11:05:36 2014 Info: Message aborted MID 1404 Receiving aborted
Thu Aug 14 11:05:36 2014 Info: Message finished MID 1404 aborted
```

Thu Aug 14 11:05:36 2014 Info: ICID 10293 close

Il peut également simplement signifier que le « délai d'attente pour les connexions entrantes infructueuses » a été atteint, qui est de cinq minutes par défaut, a configuré sur l'auditeur. Ceci se produit quand aucune donnée n'a été envoyée avant que le délai d'attente soit atteint :

Wed Aug 20 22:20:07 2014 Info: Start MID 1558778 ICID 3875465

Wed Aug 20 22:20:07 2014 Info: MID 1558778 ICID 3875465 From: <sndr@xyz.com>

Wed Aug 20 22:20:07 2014 Info: MID 1558778 ICID 3875465 RID 0 To: <recip@abc.com>

Wed Aug 20 22:25:07 2014 Info: Message aborted MID 1558778 Receiving aborted

Wed Aug 20 22:25:07 2014 Info: Message finished MID 1558778 aborted

Queest-ce que la « réception abandonnée par l'expéditeur » dans les logs de messagerie signifie ?

La « réception du MID XXX abandonnée par l'expéditeur » indique que c'est le côté d'expéditeur qui a envoyé « quitté » avant des « données » pour finir une conversation de SMTP. Le « MID XXX » est l'ID de message du message qui ne pourrait pas être avec succès injecté.

L'exemple suivant montre un client distant établissant une connexion de SMTP à l'ESA suivi du côté client fermant la connexion à la couche application avec la commande de SMTP « quittée » :

Thu Aug 14 13:08:49 2014 Info: New SMTP ICID 10318 interface Management

(192.168.0.199) address 192.168.0.200 reverse dns host ns.example.com verified no

Thu Aug 14 13:08:49 2014 Info: ICID 10318 RELAY SG RELAY_SG match 192.168.0.200

SBRS not enabled

Thu Aug 14 13:08:56 2014 Info: Start MID 1412 ICID 10318

Thu Aug 14 13:08:56 2014 Info: MID 1412 ICID 10318 From: <user@domain.com>

Thu Aug 14 13:09:03 2014 Info: MID 1412 ICID 10318 RID 0 To: <end_user@example.com>

Thu Aug 14 13:09:06 2014 Info: Message aborted MID 1412 Receiving aborted by sender

Thu Aug 14 13:09:06 2014 Info: Message finished MID 1412 aborted

Thu Aug 14 13:09:06 2014 Info: ICID 10318 close

Dépannez

- Pour étudier plus plus loin, l'injection installée mettent au point des logs pour le serveur de messagerie du domaine de partenaire en question. L'injection mettent au point des logs t'affichera exactement ce que vous obtenez de cet hôte à l'appliance.

Note: Vous pouvez devoir configurer l'injection mettez au point des logs pour chaque hôte de messagerie répertorié dans les enregistrements MX des DN du partenaire.

- Vous pouvez également trouver lui benefical pour exécuter une capture de paquet sur l'appliance pendant la transmission pour afficher la connexion et la prise de contact complètes, et les questions associées qui peuvent causer la connexion d'interrupted.

[Informations connexes](#)

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur](#)
- [Quel est un ID de message \(MID\), l'ID de connexion d'injection \(ICID\), ou l'ID de connexion de](#)

la livraison (DCID) ?

- Comment analysez-vous les questions intermittentes de distribution du courrier sur l'ESA ?
- Procédures de capture de paquet ESA
- Support et documentation techniques - Cisco Systems