Waar vind ik zachte bounce informatie in de blogs?

Inhoud

Inleiding

Dit document beschrijft welke zachte grenzen worden gedefinieerd als en waar zachte grenzen worden geregistreerd op Cisco e-mail security applicatie (ESA).

Waar vind ik zachte bounce informatie in de blogs?

Zachte boten zijn e-mails die tijdelijk niet te leveren zijn. Bijvoorbeeld, een brievenbus van een gebruiker?s kan volledig zijn. Deze berichten kunnen later opnieuw worden beproefd. (bijvoorbeeld een MTP 4XX-foutcode.)

> Opmerking: Zie voor meer informatie over 4XX foutcodes Simple Mail Transfer Protocol (MTP) uitgebreide statuscodes.

Zachte Bounces worden inlogd in de loggen van de Tekstmail van IronPort (mail_logs) en in de logbestanden van de Bounce (bounces). Het bounce log registreert alle informatie met betrekking tot elke begunstigde. Als u bovendien berichtgrootte hebt opgegeven om **loglijsten** of setup-**logheaders > logheaders** te loggen of in te stellen, zullen de bericht- en headerinformatie verschijnen na de stuitinformatie.

De ESA zal de levering opnieuw proberen op basis van de geconfigureerde **configuratie** parameters. De levering wordt op een later tijdstip opnieuw gestart, op basis van het geconfigureerde maximale aantal hermeldingen of de maximale tijd in de wachtrij.

Standaard genereert het systeem een weerkaatsing-bericht en stuurt het naar de oorspronkelijke zender voor elke vaste ontvanger. (Het bericht wordt verstuurd naar het adres dat is gedefinieerd in het adres van de zender van het bericht. Ook wel de Envelope Sender genoemd.) U kunt deze optie uitschakelen en in plaats daarvan vertrouwen op logbestanden voor informatie over vaste bronnen.

Zachte boetes worden zware boetes na de maximumtijd in de rij of het maximum aantal pogingen,

welke eerst komt.

Voorbeelden

Voorbeelden van een zachte aanval zoals die in mail_logs wordt gezien:

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 -
Unknown address error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31
20:01:23 2003
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address
172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

Voorbeeld van een zachte aanval zoals gezien in het Bounce-log:

```
Soft-Bounced Recipient (Bounce Type = Delayed)
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>
Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious activity
from your IP address (10.1.1.1). Have your system administrator send e-mail
to postmaster@sampledomain.com if you believe this block is in error'])"
```

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems