Wat kan ertoe leiden dat de SMTP-banner wordt vertraagd?

Inhoud

Vraag:

Wat kan ertoe leiden dat de SMTP-banner wordt vertraagd?

Meestal wanneer u Telnet naar poort 25 van een mailserver, krijgt u de SMTP banner zeer snel. Hier zijn voorbeelden van SMTP banners:

```
220 host.example.com ESMTP
554 host.example.com
Soms is er een vertraging en alles wat je krijgt is de
verbindingsinformatie in je display. Hierna volgt een voorbeeld:
host.voorbeeld.com> telnet 10.92.152.18 25
Proef 10.92.152.18...
Verbonden met host.example.com.
Escape is '^]'.
```

Merk op dat de banner in dit voorbeeld ontbreekt. Na enige tijd moet de banner eindelijk op de volgende regel worden weergegeven. Dit artikel gaat over deze specifieke situatie. Er zijn vier gemeenschappelijke oorzaken die we zullen bespreken: DNS-problemen, hoog CPU-gebruik, de modus voor het behoud van bronnen en firewalls.

DNS-problemen

De meest voorkomende oorzaak van vertraagde SMTP-banner is dat de DNS-lookups langer duurden dan normaal of uitgesteld. Er zijn drie lookups die plaatsvinden tussen de connect en het bannerdisplay: een omgekeerde DNS (of PTR record) lookup, dan een voorwaartse (of A record) lookup van de hostnaam gegeven in het PTR record, en dan een SenderBase lookup om de verbindende host SBRS (SenderBase Reputation Score) te krijgen.

Deze lookups worden gebruikt om te bepalen tot welke Sender Group de verbindende host behoort. Dit bepaalt welk Mail Flow Policy wordt gebruikt en of e-mail zal worden geaccepteerd van deze host. Dit beïnvloedt welke post banner, als om het even welk, zal worden verzonden. Daarom is het van cruciaal belang dat deze opzoekingen gebeuren voordat het spandoek wordt gegeven.

Om te bepalen of het probleem DNS-gerelateerd is, moet u zich aanmelden bij de opdrachtregel (CLI) van de ESA en de opdracht nslookup gebruiken. Het is belangrijk dat u dit vanuit het apparaat zelf doet, dus u werkt vanuit het perspectief van het apparaat. Eerst moet u het IP-adres weten dat probeert verbinding te maken. Je kunt de mail_logs of Message Tracking gebruiken om het IP-adres te krijgen.

Zodra u IP kent, kunt u beginnen te gebruiken nslookup om te testen. Vergeet niet te tellen hoeveel seconden het duurt voor elk van deze

DNS-lookups! Eerst de omgekeerde DNS raadpleging:

```
host.voorbeeld.com> nslookup 10.92.152.18
PTR= host.example.com TTL=2h 35m 43s
```

Dan doe een raadpleging op de hostname die terugkwam op de omgekeerde DNS lookup, als zo:

```
host.example.com> nslookup host.example.com
A=10.92.152.18 TTL=2h 34m 16s
```

Als de totale tijd voor deze twee lookups ongeveer overeenkomt met hoe lang de banner wordt uitgesteld, hebt u de oorzaak gevonden en zal u de DNS situatie verder willen herzien. De volgende stappen zouden het testen van andere IP-adressen uit verschillende netwerken kunnen omvatten. Dit zal je vertellen of de kwestie geïsoleerd is voor specifieke hosts of netwerken, of dat er een algemenere DNS kwestie is.

Hoog CPU-gebruik

Een andere mogelijke oorzaak van de SMTP bannervertraging is zeer hoog CPU-gebruik.

Als een systeem zwaar belast is, duurt het langer om dat te doen. U kunt dit controleren door naar de pagina Systeemstatus van het tabblad Monitor te gaan, of door de CLI-opdracht 'statusdetails' te gebruiken. Beide geven de CPU-gebruiksstatistieken in het gedeelte Meters. Hierna volgt een voorbeeld:

```
CPU-gebruik
Totaal 67%
MGA 16%
SITUATIE 46%
Brightmail AntiSpam 0%
AntiVirus 0%
Rapportage 4%
```

```
Quarantaine 0%
```

Als het totaal erg hoog is (95% of hoger) en enkele minuten hoog blijft, is CPU-gebruik waarschijnlijk de oorzaak van

de SMTP-banner vertraagt.

Modus voor behoud van bronnen

Een andere mogelijke oorzaak van de SMTP-bannervertraging is dat het systeem de Resource Conservation-modus heeft ingevoerd. In deze modus beschermt het systeem zichzelf door de stroom van e-mailacceptatie te vertragen. Het doet dit door elke SMTP-reactie die het verstuurt, opzettelijk uit te stellen. Om te bepalen of het systeem zich in de modus voor resourceconservatie bevindt, gaat u naar de pagina Systeemstatus van het tabblad Monitor of gebruikt u de CLI-opdracht 'statusdetails'. Zoek naar de regel voor het behoud van bronnen in het gedeelte Meters.

Hierna volgt een voorbeeld:

```
Resourceconservering 0
```

Elk niet-nul getal betekent dat het systeem zichzelf probeert te beschermen door de reactie van de SMTP te vertragen. Je kunt hier meer lezen over Resourceconservatie:

[Wat is de modus voor grondstoffenbehoud?]

Firewalls

De laatste gemeenschappelijke oorzaak van de vertragingen van de SMTP-banner zijn firewalls die zich bewust zijn van SMTP. Deze kenmerken zijn bijvoorbeeld het uitvoeren van 'SMTP fixup' of het uitvoeren van beveiligingsscans op alle SMTP-content. Soms kan een firewall de banner vertragen terwijl het scant en mogelijk de inhoud van de SMTP banner wijzigt. Hier is een voorbeeld van een populaire firewall die de SMTP-banner verandert:

```
220
*****
02**************************************************0****0****
0 ***************2******200**0*********0*00
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.