Troubleshoot Delivery Issues on the ESA

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Troubleshooting Steps

- tophosts command
- hoststatus command
- nslookup command
- dnsflush command
- SMTPPING tool
- delivernow command

Related Information

Introduction

This document describes how to troubleshoot delivery issues on the Email Security Appliance (ESA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Track an outbound message through the mail logs or Message Tracking
- Access to the CLI of the ESA

Components Used

The information in this document is based on AsyncOS for Email Security.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The ESA is able to receive mail but messages do not appear to be arriving at their destination. How do I determine why the ESA is not sending mail to a specific domain or domains? There are a variety of reasons an ESA is not able to send messages. This article focuses on debugging issues with a remote domain.

Troubleshooting Steps

tophosts command

To get immediate information about the email queue and determine if a particular recipient host has delivery problems — such as a queue buildup — use the tophosts command. The tophosts command returns a list of the top 20 recipient hosts in the queue. The list can be sorted by a number of different statistics, including active recipients, connections out, delivered recipients, soft bounced events, and hard bounced recipients.

Run the tophosts command and sort by Active Recipients in order to see which hosts have the largest delivery queue.

<#root>

```
mail.example.com >
```

tophosts

```
Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>
```

hoststatus command

Run the hoststatus command in order to check the used MX records and the status. If **Host up/down:** is unknown or down, try sending a message to that host using the SMTPPING tool as shown next and see if the status changes. Host status shows the status of the last attempted delivery.

<#root>

```
mail.example.com>
```

hoststatus cisco.com

```
Host mail status for: 'cisco.com'
Status as of:         Wed Sep 17 11:49:42 2014 CEST
```

Host up/down: **unknown**

```
Counters:
  Queue
    Soft Bounced Events                     0
  Completion
    Completed Recipients                    0
      Hard Bounced Recipients               0
```

```
        DNS Hard Bounces                    0
        5XX Hard Bounces                    0
        Filter Hard Bounces                 0
        Expired Hard Bounces                0
        Other Hard Bounces                  0
      Delivered Recipients                  0
      Deleted Recipients                    0

Gauges:
  Queue
    Active Recipients                       0
      Unattempted Recipients                0
      Attempted Recipients                  0
    Connections
      Current Outbound Connections          0
      Pending Outbound Connections          0

Oldest Message        No Messages
Last Activity         Wed Sep 17 11:49:39 2014 CEST
Ordered IP addresses: (expiring at Tue Mar 04 08:16:06 2014 CET)
    Preference   IPs
    10           172.31.147.230:25


MX Records:


    Preference   TTL        Hostname
    10           1d12s      alln-mx-01.cisco.com
```

nslookup command

Run the **nslookup** command in order to verify if MX records for recipient domain is valid.

```
<#root>

mail.example.com>

nslookup



Please enter the host or IP address to resolve.
[]>

cisco.com



Choose the query type:
1. A       the host's IP address
2. AAAA    the host's IPv6 address
3. CNAME   the canonical name for an alias

4. MX      the mail exchanger


5. NS      the name server for the named zone
6. PTR     the hostname if the query is an Internet address,

 otherwise the pointer to other information
```

```
7. SOA     the domain's "start-of-authority" information
8. TXT     the text information
[1]> 4

MX=rcdn-mx-01.cisco.com PREF=20 TTL=1d
MX=aer-mx-01.cisco.com PREF=30 TTL=1d
MX=alln-mx-01.cisco.com PREF=10 TTL=1d
```

dnsflush command

Run the dnsflush command, if the DNS record has been corrected in order to pick up new MX record.

<#root>

```
mail.example.com>

dnsflush



Are you sure you want to clear out the DNS cache? [N]>

Y
```

SMTPPING tool

Run the SMTPPING tool for connectivity test and send a test message.

<#root>

```
mail.example.com>

diagnostic



Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[]> network


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.

- SMTPPING - Test a remote SMTP server.


- TCPDUMP - Dump ethernet packets.
```

```
[]>
```

smtpping

```
Enter the hostname or IP address of the SMTP server:
[mail.example.com]>
```

cisco.com

```
The domain you entered has MX records.
Would you like to select an MX host to test instead? [Y]>

Select an MX host to test.
1. aer-mx-01.cisco.com
2. alln-mx-01.cisco.com
3. rcdn-mx-01.cisco.com
[1]>
```

2

```
Select a network interface to use for the test.
1. Management
2. auto
[2]>

Do you want to type in a test message to send?  If not, the connection can be
tested but no email can be sent. [N]>
```

Y

```
Enter the From e-mail address:
[from@example.com]>

Enter the To e-mail address:
[to@example.com]> postmaster@cisco.com

Enter the Subject:
[Test Message]>

Enter the Body of the message one line at a time.  End with a "." on a line by itself.
Test only
.
```

Starting SMTP test of host alln-mx-01.cisco.com.

Resolved 'alln-mx-01.cisco.com' to 172.31.147.230.

Connection to 172.31.147.230 succeeded.

Command EHLO succeeded

```
Command MAIL FROM succeeded.


Command RCPT TO succeeded.


Command DATA succeeded.


Mesage body accepted.


Test complete.  Total time elapsed 1.48 seconds


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets
```

delivernow command

Run the delivernow command and force the ESA to re-attempt delivery to all hosts or a specific host.

```
<#root>

mail.example.com>

delivernow


Please choose an option for scheduling immediate delivery.
1. By recipient domain
2. All messages
[1]>

2
```

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **Cisco Technical Support & Downloads**