What do 'invalid DNS Response' errors in system logs mean?

Document ID: 118483

Contributed by Martin Ding and Siddharth Rajpathak, Cisco TAC Engineers.

Oct 13, 2014

Contents

Question

What do entries like this in the log mean?

```
Tue Apr 29 10:25:33 2008 Warning: Received an invalid DNS Response: rcode=ServFail
data="'\\xadX\\x81\\x82\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x04Example\\x02Com\\
x00\\x00\\x0f\\x00\\x01'" to IP 10.10.3.11 looking up example.com

Tue Apr 29 10:25:33 2008 Info: ICID 1905953 Address: <test@example.com>
sender rejected, envelope sender domain could not be resolved.
```

Environment

Cisco Web Security appliance (WSA) any AsyncOS version, Cisco Email Security appliance (ESA) any AsyncOS version

This indicates that the DNS server returned a 'SERVFAIL' error when it attempted to look up the domain in DNS. SERVFAIL means that the domain does exist and the root name servers have information on this domain, but that the authoritative name servers are not answering queries for this domain.

You can run a manual DNS query from the CLI using the "nslookup" command to verify if DNS resolution of the domain is working properly. Typically, seeing many of these messages in the logs indicates that there are lots of emails going to sites that have bad DNS replies. If the error messages are seen very frequently, it could also indicate that the local/configured DNS server/s may be having issue in resolving domain names.