ACOS DNS SERVICES AND DNS FLAG DAY

PUBLISHED: JANUARY 30, 2019 | LAST UPDATE: FEBRUARY 15, 2019

SUMMARY

ABOUT DNS FLAG DAY

DNS Flag Day marks a major event in the industry, scheduled for February 1, 2019. On or around this date, major Domain Name Systems (DNS) service providers will remove DNS workarounds historically put in place to allow users to avoid compliance with the Extension Mechanisms Protocol for DNS (EDNS) standards. As a result of this stricter EDNS handling, these DNS providers will no longer support connections to non-compliant DNS servers.

For more information on DNS Flag Day, visit its website at www.dnsflagday.net. Tests for domain compliance can be performed using tools on this web page. Domains with test results indicating "All Ok!" or "Minor problems detected!" will not be affected by the DNS Flag Day event. Domains with test results indicating "Serious problem detected!" or "Fatal error detected" will be affected.

ACOS GSLB EXPECTATIONS

Hosted domains using ACOS Application Delivery Controller (ADC) products for Global Server Load Balancing (GSLB) and that make the ACOS device an authoritative server for the GSLB zone will continue to be available and accessible after DNS Flag Day. Testing with the tools from the Flag Day website will, however, report "Minor problems detected!" for deployments. Mitigating configuration procedures are available to change the test results to "All Ok" for ACOS 4.1.x release families, as described below.

ACOS DNS LOAD BALANCING EXPECTATIONS

Exposure to impacts from DNS Flag Day is dependent on EDNS compliance of the DNS servers of the hosted domains using ACOS ADC products for DNS load balancing. ACOS deployments with compliant DNS servers will not be affected by the DNS Flag Day event. Alternatively, deployments with non-compliant DNS servers will be affected; though these affects may be mitigatable using ACOS aFlex scripts and depending on the extent of compliance issues. Such mitigations are beyond the scope of this advisory.

DNS load balanced deployments with compliant servers that enable the DNS caching feature will also continue to be available and accessible after DNS Flag Day. These configurations will also show "Minor problems detected!" in results from test tools on the Flag Day website, which can also be mitigated to achieve "All Ok" for results for ACOS 4.1.x release families, as described below.

AFFECTED RELEASES

Support, as described above, for EDNS with the GSLB feature is available in all versions for the ACOS 4.1.0, 4.1.1, 4.1.2, 4.1.4, and 4.1.4-GR1 release families as well as for ACOS 2.7.2-P4, 2.7.1-GR1-P3, and their subsequent updates.

Support, as described above, for EDNS with the DNS Caching feature is available in all versions for the ACOS 4.1.0, 4.1.1, 4.1.2, 4.1.4, and 4.1.4-GR1 release families as well as for ACOS 2.7.2-P4, 2.7.1-GR1-P3, and their subsequent updates.

A10 will update ACOS in the future for supported ACOS 4.1.x release families to improve compliance with EDNS, initially to address the mitigations described below and subsequently for full compliance with the EDNS standards. These improvements to ACOS will be addressed in another, different Security Advisory.

ACOS 2.7.2 and 2.7.1-GR1 legacy deployments using these features, though not affected for this DNS Flag Day event, may be at greater risk to future events in the DNS industry and community. It is strongly recommended that these deployments update to supported ACOS 4.1.x release families to avoid potential impacts from these events.

WORKAROUNDS AND MITIGATIONS

Specific workarounds or mitigations to improve the reports of test tools from the DNS Flag Day website from "Minor problems detected!" to "All Ok!" are described below.

NOTE: These mitigations are not required to ensure availability and accessibility of ACOS systems after DNS Flag Day, since these systems will not be affected in this regard. The following mitigations only improve the results from DNS Flag Day compliance tests for ACOS 4.1.x release families.

NOTE: These mitigations are not available for ACOS 2.7.2 and 2.7.1-GR1 legacy release families. Though these releases will show "Minor problems detected!" in test results for ACOS systems with the described GSLB or DNS features enabled, as described above, these systems will continue to be available and accessible after DNS Flag Day.

ACOS GSLB MITIGATIONS

For ACOS GSLB deployments that make the ACOS device an authoritative server for the GSLB zone, apply workarounds described below to ensure "All Ok!" test results.

NOTE: ACOS configuration examples below use a fictitious domain, gslb-lab.com, with similarly named configuration object and subdomains. Replace these with names and conventions used in the target ACOS device. Step 1 includes addition example configurations elements that should have corresponding entries in the target ACOS device. Key ACOS configuration commands are indicated in **bold**.

1. Configure a DNS start of authority (SOA) record for the GSLB zone (if not already configured).

```
ACOS(config)#gslb policy gslb-lab
ACOS(config-policy:gslb-lab)#dns server authoritative ns

ACOS(config)#gslb zone gslb-lab.com
ACOS(config-zone:gslb-lab.com)#policy gslb-lab
ACOS(config-zone:gslb-lab.com)#dns-soa-record gslb-lab.com admin.gslb-lab.com
```

2. Configure a DNS name server record for the specified domain (if not already configured).

```
ACOS(config)#gslb zone gslb-lab.com
ACOS(config-zone:gslb-lab.com)#dns-ns-record ns1.gslb-lab.com
```

3. Create or Import an aFlex script named GSLB_EDNS1 with the following content.

```
when DNS_REQUEST {
    if { [DNS::opt version] != "" } {
        if { [DNS::opt version] != 0 } {
            DNS::header qr 1
            DNS::header ra 1

            set rrs [DNS::additional]
            set i 0
            foreach rr $rrs {
                incr i
            }
            if { [llength $rr] == 5 } {
                DNS::additional clear
                set rr1  "{} 16777216 c:4096 OPT \0\0\0\0"
                DNS::additional insert $rr1
                DNS::return
            } else {
                DNS::additional insert  [DNS::opt rcode 1]
                DNS::additional insert  [DNS::opt version 0]
                DNS::return
            }
        }
    }
}
```

4. Apply the GSLB_EDNS1 aFlex script to the DNS virtual server (VIP) used for GSLB for DNS on port 53.

```
ACOS(config)#slb virtual-server gslb-lab-dns-vip 10.30.0.53
ACOS(config-slb vserver)#port 53 dns-tcp
ACOS(config-slb vserver-vport)#gslb-enable
ACOS(config-slb vserver-vport)#aflex GSLB_EDNS1

ACOS(config-slb vserver)#port 53 dns-udp
ACOS(config-slb vserver-vport)#gslb-enable
ACOS(config-slb vserver-vport)#aflex GSLB_EDNS1
```

ACOS DNS CACHE MITIGATIONS

For ACOS DNS load balanced deployments that enable the DNS caching feature, apply workarounds described below to ensure "All Ok!" test results.

NOTE: ACOS configuration examples below includes additional configurations elements that should have corresponding entries in the target ACOS device. Key ACOS configuration commands are indicated in **bold**.

1. Create or Import an aFlex script named CACHE_EDNS1 with the following content with the same content as in Step 3 of the GSLB mitigations described above.

2. Apply the CACHE_EDNS1 aFlex script to the cached, DNS load balancing VIP.

```
ACOS(config)#slb template dns cached-lab-dnscache
ACOS(config-dns)#default-policy cache
ACOS(config-dns)#max-cache-size 100
ACOS(config-dns)#enable-cache-sharing

ACOS(config)#slb virtual-server cached-lab-dns-vip 7.7.7.1
ACOS(config-slb vserver)#port 53  dns-udp
ACOS(config-slb vserver-vport)#service-group dns-svrs-sg1-udp
ACOS(config-slb vserver-vport)#template dns cached-lab-dnscache
ACOS(config-slb vserver-vport)#aflex CACHE_EDNS1

ACOS(config-slb vserver)#port 53 dns-tcp
ACOS(config-slb vserver-vport)#service-group dns-svrs-sg1-tcp
ACOS(config-slb vserver-vport)#template dns cached-lab-dnscache
ACOS(config-slb vserver-vport)#aflex CACHE_EDNS1
```

SOFTWARE UPDATES

Not applicable for this advisory. Future updates to improve compliance for EDNS will be addressed in another, different Security Advisory.

VULNERABILITY DETAILS

Not applicable for this advisory.

RELATED LINKS

None.

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2019-01-30	Initial Publication
2.0	2019-02-01	Updated to reflect workarounds to improve test results to “All Ok!” only work for 4.1.x releases.
2.1	2019-02-01	Refinements, clarifications, and misc typos/corrections
2.2	2019-02-02	Added recommendation for 2.7.2 legacy deployments and future DNS Flag Days events.
2.3	2019-02-04	Restored published date published date to Jan-30.
2.4	2019-02-15	Added considerations for 2.7.1-GR1 legacy deployments