Troubleshoot Connectivity Failure to Cluster Data Node Management IP Address after Software Upgrade

Contents

Issue

After a software upgrade, the connectivity to the management IP address of the cluster data usin the Internet Control Message Protocol (ICMP) node fails. In this article "node" or "unit" are used interchangeably.

Specific symptoms:

1. No Internet Control Message Protocol (ICMP) reply packets are generated for incoming echo packets on the data node management IP address.

2. Packet captures on the management interface show that the data unit redirects packets to the control unit as the unxlate owner instead of consuming and processing them locally.

3. Packet captures on the cluster control interface indicate that these redirected ICMP echo packets are dropped on the control node with drop reason **(acl-drop) Flow is denied by configured rule**.

Management interface in the context of this article refers to the nameif of the interface configured with the **management-only individual** command:

<#root>

```
unit1/control-node#
```

```
show run interface m1/1
```

```
!
interface Management1/1
```

```
 management-only individual
```

```
 nameif management


 security-level 100
 ip address 192.0.2.1 255.255.255.0 cluster-pool cpool
```

Environment

- Secure Adaptive Security Appliance Software (ASA) version 9.22.2.32 in a cluster setup with spanned interfaces. Other software versions can also be affected.
- ASA in multiple or single-context modes.
- Any software version later than 9.22.3 is affected.
- One or both of these conditions are satisfied:

1. The CiscoSSH stack is enabled and the **ssh x.x.x.x y.y.y.y.y <management_nameif>** command is configured. In this case, ICMP/Telnet/Hypertext Transfer Protocol Secure (HTTPS) connections to the data node fail:

```
<#root>

unit1/control-node#

show ssh


ssh secure copy : DISABLED

ciscoSSH stack  : ENABLED


…
unit1/control-node#

show run ssh


ssh stricthostkeycheck
ssh timeout 10
ssh key-exchange group dh-group14-sha256
ssh key-exchange hostkey ecdsa

ssh 0.0.0.0 0.0.0.0 management
```

The CiscoSSH stack is enabled by default and can be disabled in versions 9.19.1 and later. Additionally, in version 9.23.1 and later, this stack cannot be disabled.

2. The **snmp-server host <management_nameif>** command is configured.

```
<#root>

unit1/control-node(config)#

show run snmp-server



snmp-server host management 192.0.2.101 community ***** version 2c
```

In this case, ICMP/Telnet/HTTPS connections to the data node fail. SSH connections also fail if the CiscoSSH stack is disabled.

Resolution

Analysis

Packet capture on the data node management interface:

```
<#root>

unit2/data-node#

capture capi interface management trace match icmp any any


unit2/data-node#

show capture capi trace packet-number 1


2 packets captured

   1: 12:20:47.339566       192.0.2.1 > 198.51.100.100 icmp: echo request
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 7582 ns
Config:
```

```
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 7582 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NO-NAT
Subtype: self-addressed
Result: ALLOW
Elapsed time: 8028 ns
Config:
Additional Information:
NAT divert to egress interface identity

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Elapsed time: 1784 ns
Config:
Additional Information:
Input interface: 'management'
Flow type: NO FLOW
```

NAT: I (1) am redirecting packet to unxlate owner (0).

```
<- ICMP ECHO packet is not consumed, but redirected to the unxlate owner, in this case, the control uni

Result:
input-interface: management
input-status: up
input-line-status: up
Action: allow
Time Taken: 24976 ns
```

Packet capture on the control node cluster control interface:

<#root>

```
unit1/control-node#
```

capture ccl interface cluster trace match icmp any any

```
unit1/control-node#
```

show capture ccl trace packet-number 1

```
2 packets captured

   1: 12:20:47.336469       192.0.2.1 > 198.51.100.100 icmp: echo request
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 16948 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Elapsed time: 8474 ns
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 198.51.100.100 using egress ifc  management

Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Elapsed time: 4014 ns
Config:
Additional Information:
Input interface: 'management'
Flow type: NO FLOW
I (0) have been elected owner by (0).


Phase: 4



Type: ACCESS-LIST



Subtype: mgmt-deny-all


<- ICMP ECHO packets are dropped.
Result: DROP
Elapsed time: 2899 ns
Config:
Additional Information:

Result:
input-interface: cluster
input-status: up
input-line-status: up
output-interface: management
output-status: up
```

```
output-line-status: up
Action: drop
Time Taken: 32335 ns

Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame snp_classify_table_looku

<- Drop reason
```

Permanent resolution requires software upgrade to the version with the fix of Cisco bug ID CSCwv19381.

Workaround options:

a) Remove the **snmp-server host** commands over the management interface.

If the CiscoSSH stack is disabled, then removal of the **snmp-server host** commands over the management interface restores management connectivity for protocols like ICMP, HTTPS, SSH, Telnet. If the CiscoSSH stack enabled, connectivity for protocols like ICMP, HTTPS, and Telnet fails. The **snmp-server host** command over the management interface does not affect SSH connections over the management interface if the CiscoSSH stack is enabled.

b) Disable the CiscoSSH stack using the **no ssh stack cisco** command. Disabling this stack activates the ASA SSH stack. Additionally, management connectivity is restored for protocols like ICMP, HTTPS, Telnet. Before disabling the CiscoSSH stack ensure that you understand its impact. Refer to CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide for more details.

Cause

The symptoms are due to Cisco bug ID CSCwv19381.

Related Content

- Cisco bug ID CSCwv19381
- CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide