软件升级后群集数据节点管理IP地址的连接故障排除

目录

问题

软件升级后，使用Internet控制消息协议(ICMP)节点到集群数据的管理IP地址的连接失败。在本文中，“节点”或“单元”可互换使用。

特定症状：

1.在数据节点管理IP地址上，不为传入回应数据包生成Internet控制消息协议(ICMP)应答数据包。

2.管理接口上的数据包捕获显示，数据单元将数据包重定向到作为转发所有者的控制单元，而不是在本地使用和处理数据包。

3.集群控制接口上的数据包捕获表示这些重定向ICMP回应数据包在控制节点上被丢弃，丢弃原因(acl-drop)流被配置的规则拒绝。

本文上下文中的管理接口是指使用management-only individual命令配置的接口的名称if:

<#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
```

环境

- 使用跨区接口的集群设置中的安全自适应安全设备软件(ASA)版本9.22.2.32。其他软件版本也可能受到影响。
- 多情景模式或单情景模式下的ASA。
- 高于9.22.3的任何软件版本都会受到影响。
- 满足以下一个或两个条件：

1.启用CiscoSSH堆栈并配置ssh x.x.x.x y.y.y.y <management_nameif>命令。在这种情况下，到数据节点的ICMP/Telnet/超文本传输协议安全(HTTPS)连接失败：

<#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
```

默认情况下，CiscoSSH堆栈处于启用状态，9.19.1版及更高版本中可禁用该堆栈。此外，在版本9.23.1及更高版本中，不能禁用此堆栈。

2.配置snmp-server host <management_nameif>命令。

<#root>

```
unit1/control-node(config)#

show run snmp-server



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

在这种情况下，与数据节点的ICMP/Telnet/HTTPS连接失败。如果禁用了CiscoSSH堆栈，SSH连接也会失败。

分辨率

分析

数据节点管理接口上的数据包捕获：

<#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
```

控制节点集群控制接口上的数据包捕获：

<#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
```

永久解决方案要求软件升级到版本并修复Cisco Bug ID CSCwv19381。

解决方法选项

1. — 在管理接口上删除snmp-server host命令。

   - 如果禁用CiscoSSH堆栈，则通过管理接口删除snmp-server host命令将恢复协议（如ICMP、HTTPS、SSH、Telnet）的管理连接。如果启用CiscoSSH堆栈，ICMP、HTTPS和Telnet等协议的连接将失败。如果启用了CiscoSSH堆栈，则管理接口上的snmp-server host命令不会影响管理接口上的SSH连接。

2. — 使用no ssh stack cisco命令禁用CiscoSSH堆栈。禁用此堆栈会激活ASA SSH堆栈。此外，还会恢复ICMP、HTTPS、Telnet等协议的管理连接。在禁用CiscoSSH堆栈之前，请确保您了解其影响。请参阅CLI手册1:Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide（Cisco Secure Firewall ASA系列常规操作CLI配置指南），了解更多详细信息。

原因

这些症状是由思科漏洞ID CSCwv19381引起的。

相关内容

- Cisco Bug ID CSCwv19381
- CLI手册1:思科安全防火墙ASA系列常规操作CLI配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。