軟體升級後群集資料節點管理IP地址連線故障排除

目錄

問題

軟體升級後，使用網際網路控制訊息通訊協定(ICMP)節點的叢集資料管理IP位址連線失敗。在本文中，「節點」或「單元」是互換使用的。

特定症狀：

1.資料節點管理IP地址上的傳入回應資料包未生成網際網路控制消息協定(ICMP)應答資料包。

2.管理介面上的封包擷取顯示資料單元將封包重新導向為控制單元作為傳出擁有者，而不是使用封包並在本地處理封包。

3.集群控制介面上的資料包捕獲指示這些重定向的ICMP回應資料包在控制節點上被丟棄，同時帶有丟棄原因(acl-drop)Flow is denied by configured rule。

本文上下文中的管理介面是指使用management-only individual命令配置的介面的nameif:

<#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
```

環境

- 在具有跨區介面的群集設定中安全自適應安全裝置軟體(ASA)版本9.22.2.32。其他軟體版本也可能受到影響。
- 多情景模式或單情景模式下的ASA。
- 高於9.22.3的任何軟體版本都會受到影響。
- 滿足以下一個或兩個條件：

1.啟用CiscoSSH堆疊並配置ssh x.x.x.x y.y.y.y.y <management_nameif>命令。在這種情況下，到資料節點的ICMP/Telnet/超文本傳輸協定安全(HTTPS)連線失敗：

<#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
```

CiscoSSH堆疊預設處於啟用狀態，9.19.1版及更高版本中可禁用該堆疊。此外，在9.23.1及更新版本中，無法停用此堆疊。

2.已設定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
```

在這種情況下，到資料節點的ICMP/Telnet/HTTPS連線失敗。如果禁用了CiscoSSH堆疊，SSH連線也會失敗。

解析

分析

資料節點管理介面上的資料包捕獲：

<#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
```

控制節點集群控制介面上的資料包捕獲：

<#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
```

永久解決方案要求軟體升級為修正了思科錯誤ID CSCwv19381的版本。

解決方法選項：

a)在管理介面上刪除snmp-server host命令。

如果禁用CiscoSSH堆疊，則通過管理介面刪除snmp-server host命令將恢復ICMP、HTTPS、SSH和Telnet等協定的管理連線。如果啟用CiscoSSH堆疊，ICMP、HTTPS和Telnet等協定的連線將失敗。如果啟用了CiscoSSH堆疊，管理介面上的snmp-server host命令不會影響管理介面上的SSH連線。

b)使用no ssh stack cisco命令禁用CiscoSSH堆疊。禁用此堆疊會啟用ASA SSH堆疊。此外，還會恢復ICMP、HTTPS、Telnet等協定的管理連線。禁用CiscoSSH堆疊之前，請確保您瞭解其影響。請參閱CLI手冊1:Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide（Cisco Secure Firewall ASA系列常規操作CLI配置指南），瞭解更多詳細資訊。

原因

這些症狀是由思科錯誤ID CSCwv19381引起的。

相關內容

- 思科錯誤ID CSCwv19381
- CLI手冊1:Cisco Secure Firewall ASA系列常規操作CLI配置指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。