소프트웨어 업그레이드 후 클러스터 데이터 노드 관리 IP 주소에 대한 연결 실패 트러블슈팅

목차

문제

소프트웨어 업그레이드 후 ICMP(Internet Control Message Protocol) 노드를 사용하는 클러스터 데이터의 관리 IP 주소에 대한 연결이 실패합니다. 이 글에서는 "노드" 또는 "유닛"을 혼용하여 사용합니다.

특정 증상:

1. 데이터 노드 관리 IP 주소의 수신 에코 패킷에 대해 ICMP(Internet Control Message Protocol) 응답 패킷이 생성되지 않습니다.

2. 관리 인터페이스의 패킷 캡처는 데이터 유닛이 패킷을 로컬에서 소비하고 처리하는 대신 익스플릿 소유자로서 제어 유닛에 리디렉션한다는 것을 보여줍니다.

3. 클러스터 제어 인터페이스의 패킷 캡처는 이러한 리디렉션된 ICMP 에코 패킷이 삭제 사유(acl-drop) 흐름이 구성된 규칙에 의해 거부된 상태로 제어 노드에서 삭제되었음을 나타냅니다.

이 문서의 컨텍스트에서 관리 인터페이스는 관리 전용 개별 명령으로 구성된 인터페이스의 nameif를 참조합니다.

<#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
```

환경

- Spanned 인터페이스가 있는 클러스터 설정의 ASA(Secure Adaptive Security Appliance Software) 버전 9.22.2.32. 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- 다중 또는 단일 컨텍스트 모드의 ASA.
- 9.22.3 이상의 모든 소프트웨어 버전이 영향을 받습니다.
- 다음 조건 중 하나 또는 둘 다 충족됩니다.

1. CiscoSSH 스택이 활성화되고 ssh x.x.x y.y.y.y <management_nameif> 명령이 구성됩니다. 이 경우 데이터 노드에 대한 ICMP/텔넷/HTTPS(Hypertext Transfer Protocol Secure) 연결이 실패합니다.

```
<#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 스택은 기본적으로 활성화되어 있으며 버전 9.19.1 이상에서 비활성화할 수 있습니다. 또한 버전 9.23.1 이상에서는 이 스택을 비활성화할 수 없습니다.

2. snmp-server host <management_nameif> 명령이 구성되었습니다.

<#root>

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

show run snmp-server



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

이 경우 데이터 노드에 대한 ICMP/텔넷/HTTPS 연결이 실패합니다. CiscoSSH 스택이 비활성화되면 SSH 연결도 실패합니다.

해결

분석

데이터 노드 관리 인터페이스의 패킷 캡처:

<#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
```

제어 노드 클러스터 제어 인터페이스의 패킷 캡처:

<#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
```

영구 확인을 위해서는 Cisco 버그 ID CSCwv19381이 수정된 버전으로 소프트웨어를 업그레이드해야 합니다.

해결 방법:

a) 관리 인터페이스를 통해 snmp-server host 명령을 제거합니다.

CiscoSSH 스택이 비활성화된 경우 관리 인터페이스를 통해 snmp-server host 명령을 제거하면 ICMP, HTTPS, SSH, 텔넷과 같은 프로토콜에 대한 관리 연결이 복원됩니다. CiscoSSH 스택이 활성화된 경우 ICMP, HTTPS, 텔넷과 같은 프로토콜에 대한 연결이 실패합니다. CiscoSSH 스택이 활성화된 경우 관리 인터페이스를 통한 snmp-server host 명령은 관리 인터페이스를 통한 SSH 연결에 영향을 주지 않습니다.

b) no ssh stack cisco 명령을 사용하여 CiscoSSH 스택을 비활성화합니다. 이 스택을 비활성화하면 ASA SSH 스택이 활성화됩니다. 또한 ICMP, HTTPS, 텔넷과 같은 프로토콜에 대한 관리 연결이 복원됩니다. CiscoSSH 스택을 비활성화하기 전에 그 영향을 이해해야 합니다. CLI Book 1을 참조하십시오. 자세한 내용은 Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide를 참조하십시오.

원인

이러한 증상은 Cisco 버그 ID CSCwv19381에 의한 것입니다.

관련 콘텐츠

- Cisco 버그 ID CSCwv19381
- CLI 책 1: Cisco Secure Firewall ASA Series 일반 운영 CLI 컨피그레이션 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.