Problemen met connectiviteit oplossen Mislukking bij clusterbeheer van gegevensknooppunten IP-adres na software-upgrade

Inhoud

uitgeven

Na een software-upgrade mislukt de verbinding met het IP-beheeradres van de clustergegevens via de ICMP-node (Internet Control Message Protocol). In dit artikel worden "node" of "unit" door elkaar gebruikt.

Specifieke symptomen:

1. Er worden geen ICMP-antwoordpakketten (Internet Control Message Protocol) gegenereerd voor inkomende echopakketten op het IP-adres voor gegevensknooppuntbeheer.

2. Uit pakketopnames op de beheerinterface blijkt dat de gegevenseenheid pakketten omleidt naar de besturingseenheid als de unxlate-eigenaar in plaats van ze lokaal te consumeren en te verwerken.

3. Packet captures op de interface voor clusterbesturing geven aan dat deze omgeleide ICMP-echopakketten op de besturingsnode worden gedropt met reden (acl-drop) Flow wordt geweigerd door de geconfigureerde regel.

Beheerinterface in de context van dit artikel verwijst naar de naam van de interface die is geconfigureerd met de individuele opdracht alleen voor beheer:

<#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
```

milieu

- Secure Adaptive Security Appliance Software (ASA) versie 9.22.2.32 in een clusteropstelling met gespande interfaces. Ook andere softwareversies kunnen worden beïnvloed.
- ASA in meerdere of enkelvoudige contextmodi.
- Elke softwareversie later dan 9.22.3 wordt beïnvloed.
- Aan één of beide voorwaarden is voldaan:

1. De CiscoSSH-stack is ingeschakeld en de opdracht ssh x.x.x.y.y.y <management_nameif> is geconfigureerd. In dit geval mislukken ICMP/Telnet/Hypertext Transfer Protocol Secure (HTTPS)-verbindingen met de gegevensknoop:

<#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
```

De CiscoSSH-stack is standaard ingeschakeld en kan worden uitgeschakeld in versies 9.19.1 en hoger. Bovendien kan deze stapel in versie 9.23.1 en hoger niet worden uitgeschakeld.

2. De opdracht snmp-server host <management_nameif> is geconfigureerd.

<#root>

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

show run snmp-server



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

In dit geval mislukken de ICMP/Telnet/HTTPS-verbindingen met de gegevensknoop. SSH-verbindingen mislukken ook als de CiscoSSH-stack is uitgeschakeld.

resolutie

analyse

Packet capture op de beheerinterface van de gegevensknooppunten:

<#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
```

Pakketvastlegging op de besturingsinterface van het cluster van de controlenode:

<#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
```

Permanente oplossing vereist software-upgrade naar de versie met de oplossing van Cisco bug ID CSCwv19381.

Opties voor tijdelijke oplossingen:

a) Verwijder de hostopdrachten van de snmp-server via de beheerinterface.

Als de CiscoSSH-stack is uitgeschakeld, worden de beheerconnectiviteit voor protocollen zoals ICMP, HTTPS, SSH en Telnet hersteld door de snmp-server-hostopdrachten via de beheerinterface te verwijderen. Als de CiscoSSH-stack is ingeschakeld, mislukt de connectiviteit voor protocollen zoals ICMP, HTTPS en Telnet. De opdracht snmp-server host via de beheerinterface heeft geen invloed op SSH-verbindingen via de beheerinterface als de CiscoSSH-stack is ingeschakeld.

b) Schakel de CiscoSSH-stack uit met de opdracht geen ssh-stack cisco. Als u deze stapel uitschakelt, wordt de ASA SSH-stapel geactiveerd. Bovendien wordt de beheerconnectiviteit hersteld voor protocollen zoals ICMP, HTTPS en Telnet. Voordat u de CiscoSSH-stack uitschakelt, moet u ervoor zorgen dat u de impact ervan begrijpt. Raadpleeg de CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide voor meer informatie.

Oorzaak

De symptomen zijn te wijten aan Cisco bug ID CSCwv19381.

Verwante inhoud

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.