Fehlerbehebung bei Verbindungsfehlern bei der IP-Adresse für das Cluster-Datenknotenmanagement nach dem Software-Upgrade

Inhalt

Problem

Nach einem Software-Upgrade schlägt die Verbindung mit der Management-IP-Adresse der Clusterdaten über den ICMP-Knoten (Internet Control Message Protocol) fehl. In diesem Artikel werden "Knoten" oder "Einheit" austauschbar verwendet.

Besondere Symptome:

1. Für eingehende Echo-Pakete an der IP-Adresse des Datenknotenmanagements werden keine ICMP-Antwortpakete (Internet Control Message Protocol) generiert.

2. Paketerfassungen auf der Verwaltungsschnittstelle zeigen, dass die Dateneinheit Pakete an die Steuereinheit als unerklärlichen Eigentümer umleitet, anstatt sie lokal zu verbrauchen und zu verarbeiten.

3. Paketerfassungen an der Cluster-Steuerungsschnittstelle zeigen an, dass diese umgeleiteten ICMP-Echo-Pakete auf dem Steuerungsknoten mit dem Verwerfungsgrund (acl-drop) verworfen werden. Der Datenfluss wird durch die konfigurierte Regel abgelehnt.

Management-Schnittstelle im Kontext dieses Artikels bezieht sich auf den Namen der Schnittstelle, die mit dem individuellen Befehl management-only konfiguriert wurde:

<#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
```

Umwelt

- Secure Adaptive Security Appliance Software (ASA) Version 9.22.2.32 in einer Cluster-Konfiguration mit übergreifenden Schnittstellen. Auch andere Softwareversionen können betroffen sein.
- ASA im Multiple- oder Single-Context-Modus
- Alle Softwareversionen nach 9.22.3 sind betroffen.
- Eine oder beide der folgenden Bedingungen sind erfüllt:

1. Der CiscoSSH-Stack ist aktiviert, und der Befehl ssh x.x.x.x y.y.y <management_name> wird konfiguriert. In diesem Fall schlagen die sicheren Verbindungen des ICMP/Telnet/Hypertext Transfer Protocol (HTTPS) zum Datenknoten fehl:

<#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

Der Cisco SSH-Stack ist standardmäßig aktiviert und kann in Version 9.19.1 und höher deaktiviert werden. Außerdem kann dieser Stack in Version 9.23.1 und höher nicht deaktiviert werden.

2. Der Befehl snmp-server host <management_nameif> wird konfiguriert.

<#root>

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

show run snmp-server

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

In diesem Fall schlagen die ICMP/Telnet/HTTPS-Verbindungen zum Datenknoten fehl. SSH-Verbindungen schlagen ebenfalls fehl, wenn der Cisco SSH-Stack deaktiviert ist.

Auflösung

Analyse

Paketerfassung über die Datenknoten-Verwaltungsschnittstelle:

<#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
```

Paketerfassung auf der Steuerknoten-Cluster-Steuerschnittstelle:

<#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
```

Für eine dauerhafte Behebung ist ein Software-Upgrade auf die Version mit der Cisco Bug-ID CSCwv19381 erforderlich.

Problemumgehungsoptionen:

a) Entfernen Sie die snmp-server host-Befehle über die Management-Schnittstelle.

Wenn der Cisco SSH-Stack deaktiviert ist, wird durch Entfernen der snmp-server-host-Befehle über die Verwaltungsschnittstelle die Managementverbindung für Protokolle wie ICMP, HTTPS, SSH oder Telnet wiederhergestellt. Bei Aktivierung des Cisco SSH-Stacks schlägt die Verbindung für Protokolle wie ICMP, HTTPS und Telnet fehl. Der Befehl snmp-server host über die Management-Schnittstelle wirkt sich nicht auf SSH-Verbindungen über die Management-Schnittstelle aus, wenn der CiscoSSH-Stack aktiviert ist.

b) Deaktivieren Sie den Cisco SSH-Stack mit dem Befehl no ssh stack cisco. Durch Deaktivieren dieses Stacks wird der ASA SSH-Stack aktiviert. Zusätzlich wird die Managementverbindung für Protokolle wie ICMP, HTTPS oder Telnet wiederhergestellt. Stellen Sie vor der Deaktivierung des Cisco SSH-Stacks sicher, dass Sie dessen Auswirkungen kennen. Weitere Informationen finden Sie im CLI-Buch 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide für weitere Informationen.

Ursache

Die Symptome sind auf den Cisco Bug "CSCwv19381" zurückzuführen.

Verwandte Inhalte

- Cisco Bug-ID CSCwv19381
- CLI-Buch 1: Allgemeine Konfigurationsanleitung für die CLI der Cisco Secure Firewall ASA-Serie

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.