Dépannage de l'échec de connectivité au cluster Data Node Management IP Address après la mise à niveau logicielle

Table des matières

Problème

Après une mise à niveau logicielle, la connectivité à l'adresse IP de gestion des données de cluster à l'aide du noeud ICMP (Internet Control Message Protocol) échoue. Dans cet article "noeud" ou "unité" sont utilisés de façon interchangeable.

Symptômes spécifiques :

1. Aucun paquet de réponse ICMP (Internet Control Message Protocol) n’est généré pour les paquets d’écho entrants sur l’adresse IP de gestion du noeud de données.

2. Les captures de paquets sur l’interface de gestion montrent que l’unité de données redirige les paquets vers l’unité de contrôle en tant que propriétaire d’unxlate au lieu de les consommer et de les traiter localement.

3. Les captures de paquets sur l’interface de contrôle de cluster indiquent que ces paquets d’écho ICMP redirigés sont abandonnés sur le noeud de contrôle avec raison d’abandon (acl-drop). Le flux est refusé par la règle configurée.

L'interface de gestion dans le contexte de cet article se réfère au nom de l'interface configurée avec la commande management-only individual :

<#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
```

Environnement

- Secure Adaptive Security Appliance Software (ASA) version 9.22.2.32 dans une configuration en cluster avec des interfaces étendues. D'autres versions logicielles peuvent également être affectées.
- ASA en mode multicontexte ou à contexte unique.
- Toute version du logiciel postérieure à la version 9.2.3 est affectée.
- L'une de ces conditions ou les deux sont remplies :

1. La pile CiscoSSH est activée et la commande ssh x.x.x.x y.y.y.y <management_nameif> est configurée. Dans ce cas, les connexions ICMP/Telnet/HTTPS (Hypertext Transfer Protocol Secure) au noeud de données échouent :

<#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
```

La pile CiscoSSH est activée par défaut et peut être désactivée dans les versions 9.19.1 et ultérieures. En outre, dans les versions 9.23.1 et ultérieures, cette pile ne peut pas être désactivée.

2. La commande snmp-server host <management_name> est configurée.

<#root>

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

show run snmp-server



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

Dans ce cas, les connexions ICMP/Telnet/HTTPS au noeud de données échouent. Les connexions SSH échouent également si la pile CiscoSSH est désactivée.

Résolution

Analyse

Capture de paquets sur l’interface de gestion du noeud de données :

<#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

Capture de paquets sur l'interface de contrôle du cluster du noeud de contrôle :

<#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
```

La résolution permanente nécessite une mise à niveau logicielle vers la version avec le correctif de l'ID de bogue Cisco CSCwv19381.

Options de contournement :

a) Supprimez les commandes snmp-server host sur l'interface de gestion.

Si la pile CiscoSSH est désactivée, alors la suppression des commandes snmp-server host sur l'interface de gestion restaure la connectivité de gestion pour les protocoles comme ICMP, HTTPS, SSH, Telnet. Si la pile CiscoSSH est activée, la connectivité des protocoles tels que ICMP, HTTPS et Telnet échoue. La commande snmp-server host sur l'interface de gestion n'affecte pas les connexions SSH sur l'interface de gestion si la pile CiscoSSH est activée.

b) Désactivez la pile CiscoSSH à l'aide de la commande no ssh stack cisco. La désactivation de cette pile active la pile SSH ASA. En outre, la connectivité de gestion est restaurée pour les protocoles tels que ICMP, HTTPS, Telnet. Avant de désactiver la pile CiscoSSH, assurez-vous de bien comprendre son impact. Reportez-vous au manuel CLI 1 : Guide de configuration CLI des opérations générales de la gamme Cisco Secure Firewall ASA pour plus de détails.

Motif

Les symptômes sont dus à l'ID de bogue Cisco CSCwv19381.

Autres informations utiles

- ID de bogue Cisco CSCwv19381
- Livre CLI 1 : Guide de configuration CLI des opérations générales de la gamme Cisco Secure Firewall ASA

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.