Risoluzione dei problemi di connettività all'indirizzo IP di gestione dei nodi dati del cluster dopo l'aggiornamento del software

Sommario

Problema

Dopo un aggiornamento del software, la connettività all'indirizzo IP di gestione dei dati del cluster tramite il nodo ICMP (Internet Control Message Protocol) non riesce. In questo articolo "nodo" o "unità" sono utilizzati in modo intercambiabile.

Sintomi specifici:

1. Non vengono generati pacchetti di risposta ICMP (Internet Control Message Protocol) per i pacchetti echo in arrivo sull'indirizzo IP di gestione del nodo dati.

2. Le acquisizioni dei pacchetti sull'interfaccia di gestione mostrano che l'unità di dati reindirizza i pacchetti all'unità di controllo come proprietario unificatore anziché consumarli ed elaborarli localmente.

3. Le acquisizioni di pacchetti sull'interfaccia di controllo del cluster indicano che questi pacchetti echo ICMP reindirizzati vengono scartati sul nodo di controllo con flusso a causa dell'eliminazione (acl-drop) negato dalla regola configurata.

Nel contesto di questo articolo, per interfaccia di gestione si intende il nome dell'interfaccia configurata con il comando individuale di sola gestione:

<#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
```

Ambiente

- Software ASA (Secure Adaptive Security Appliance) versione 9.2.2.32 in una configurazione cluster con interfacce con spanning. Il problema può riguardare anche altre versioni del software.
- ASA in modalità contesto singolo o multiplo.
- Il problema riguarda tutte le versioni software successive alla 9.2.3.
- Sono soddisfatte una o entrambe le condizioni seguenti:

1. Lo stack Cisco SSH è abilitato e il comando ssh x.x.x.x.y.y.y <management_name> è configurato. In questo caso, le connessioni ICMP/Telnet/Hypertext Transfer Protocol Secure (HTTPS) al nodo di dati hanno esito negativo:

<#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
```

Lo stack Cisco SSH è abilitato per impostazione predefinita e può essere disabilitato nelle versioni 9.19.1 e successive. Inoltre, nella versione 9.23.1 e successive, questo stack non può essere disabilitato.

2. Il comando snmp-server host <management_name> è configurato.

<#root>

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

show run snmp-server



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

In questo caso, le connessioni ICMP/Telnet/HTTPS al nodo di dati hanno esito negativo. Le connessioni SSH hanno esito negativo anche se lo stack Cisco SSH è disabilitato.

Risoluzione

Analisi

Acquisizione dei pacchetti sull'interfaccia di gestione del nodo dati:

<#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

Acquisizione pacchetti nell'interfaccia di controllo del cluster del nodo di controllo:

<#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 risoluzione permanente richiede l'aggiornamento del software alla versione con la correzione dell'ID bug Cisco CSCwv19381.

Opzioni per la soluzione:

a) Rimuovere i comandi host snmp-server sull'interfaccia di gestione.

Se lo stack Cisco SSH è disabilitato, la rimozione dei comandi dell'host snmp-server sull'interfaccia di gestione ripristina la connettività di gestione per protocolli come ICMP, HTTPS, SSH, Telnet. Se lo stack Cisco SSH è abilitato, la connettività per protocolli come ICMP, HTTPS e Telnet non riesce. Se lo stack Cisco SSH è abilitato, il comando snmp-server host sull'interfaccia di gestione non influisce sulle connessioni SSH sull'interfaccia di gestione.

b) Disabilitare lo stack Cisco SSH usando il comando no ssh stack cisco. La disabilitazione di questo stack comporta l'attivazione dello stack SSH ASA. Inoltre, viene ripristinata la connettività di gestione per protocolli quali ICMP, HTTPS, Telnet. Prima di disabilitare lo stack Cisco SSH, accertarsi di averne compreso l'impatto. Fare riferimento al manuale CLI 1: Per ulteriori informazioni, consultare la guida alla configurazione della CLI per le operazioni generali di Cisco Secure Firewall serie ASA.

Causa

I sintomi sono dovuti all'ID bug Cisco CSCwv19381.

Contenuto correlato

- ID bug Cisco CSCwv19381
- CLI Book 1: Guida alla configurazione della CLI per le operazioni generali di Cisco Secure Firewall serie ASA

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).