Resolución de problemas de falla de conectividad a la dirección IP de administración del nodo de datos del clúster después de la actualización de software

Contenido

Problema

Después de una actualización de software, la conectividad con la dirección IP de administración de los datos del clúster mediante el nodo ICMP (Protocolo de mensajes de control de Internet) falla. En este artículo "nodo" o "unidad" se utilizan indistintamente.

Síntomas específicos:

1. No se generan paquetes de respuesta de protocolo de mensajes de control de Internet (ICMP) para los paquetes de eco entrantes en la dirección IP de administración del nodo de datos.

2. Las capturas de paquetes en la interfaz de administración muestran que la unidad de datos redirige los paquetes a la unidad de control como el propietario unxlate en lugar de consumirlos y procesarlos localmente.

3. Las capturas de paquetes en la interfaz de control del clúster indican que estos paquetes de eco ICMP redirigidos se descartan en el nodo de control con motivo de la caída (acl-drop). La regla configurada deniega el flujo.

La interfaz de administración en el contexto de este artículo se refiere al nombre de la interfaz configurada con el comando 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
```

Entorno

- Versión 9.2.2.32 del software Secure Adaptive Security Appliance (ASA) en una configuración de clúster con interfaces ampliadas. Otras versiones de software también pueden verse afectadas.
- ASA en modos de contexto múltiple o único.
- Cualquier versión de software posterior a la 9.2.3 se ve afectada.
- Se cumple una o ambas de estas condiciones:

1. La pila CiscoSSH está habilitada y se configura el comando ssh x.x.x y.y.y.y.y <management_nameif>. En este caso, las conexiones ICMP/Telnet/Protocolo seguro de transferencia de hipertexto (HTTPS) al nodo de datos fallan:

<#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 pila CiscoSSH está habilitada de forma predeterminada y se puede inhabilitar en las versiones 9.19.1 y posteriores. Además, en la versión 9.23.1 y posteriores, esta pila no se puede deshabilitar.

2. Se configura el comando snmp-server host <management_name if>.

```
<#root>

unit1/control-node(config)#

show run snmp-server



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

En este caso, las conexiones ICMP/Telnet/HTTPS con el nodo de datos fallan. Las conexiones SSH también fallan si la pila CiscoSSH está inhabilitada.

Resolución

Análisis

Captura de paquetes en la interfaz de administración del nodo de datos:

```
<#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
```

Captura de paquetes en la interfaz de control del clúster del nodo de control:

<#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 resolución permanente requiere la actualización de software a la versión con la corrección del Id. de error de Cisco CSCwv19381.

Opciones alternativas:

a) Quite los comandos snmp-server host en la interfaz de administración.

Si la pila CiscoSSH está inhabilitada, la remoción de los comandos snmp-server host sobre la interfaz de administración restaura la conectividad de administración para protocolos como ICMP, HTTPS, SSH, Telnet. Si la pila CiscoSSH está habilitada, la conectividad para protocolos como ICMP, HTTPS y Telnet falla. El comando snmp-server host sobre la interfaz de administración no afecta las conexiones SSH sobre la interfaz de administración si la pila CiscoSSH está habilitada.

b) Inhabilite la pila CiscoSSH usando el comando no ssh stack cisco. Al deshabilitar esta pila se activa la pila SSH de ASA. Además, se restaura la conectividad de administración para protocolos como ICMP, HTTPS y Telnet. Antes de desactivar la pila CiscoSSH, asegúrese de comprender su impacto. Consulte el Libro CLI 1: Guía de configuración de la CLI de operaciones generales de Cisco Secure Firewall ASA Series para obtener más información.

Causa

Los síntomas se deben al Id. de bug Cisco CSCwv19381.

Contenido relacionado

- ID de bug de Cisco CSCwv19381
- Libro CLI 1: Guía de configuración de CLI de operaciones generales de Cisco Secure Firewall ASA Series

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).