# Solucionar Problemas de Falha de Conectividade do Endereço IP de Gerenciamento de Nó de Dados de Cluster após Atualização de Software

## Contents

## Problema

Após um upgrade de software, a conectividade com o endereço IP de gerenciamento dos dados do cluster usando o nó do Internet Control Message Protocol (ICMP) falha. Neste artigo, "nó" ou "unidade" são usados de forma intercambiável.

Sintomas específicos

1. Nenhum pacote de resposta do protocolo ICMP (Internet Control Message Protocol) é gerado para pacotes de eco de entrada no endereço IP de gerenciamento do nó de dados.

2. Capturas de pacotes na interface de gerenciamento mostram que a unidade de dados redireciona pacotes para a unidade de controle como o proprietário unxlate em vez de consumi-los e processá-los localmente.

3. Capturas de pacotes na interface de controle do cluster indicam que esses pacotes de eco ICMP redirecionados são descartados no nó de controle com razão de descarte (acl-drop). O fluxo é negado pela regra configurada.

A interface de gerenciamento no contexto deste artigo se refere ao nome da interface configurada com o 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
```

# Ambiente

- Secure Adaptive Security Appliance Software (ASA) versão 9.22.2.32 em uma configuração de cluster com interfaces estendidas. Outras versões de software também podem ser afetadas.
- ASA em modos de contexto único ou múltiplo.
- Qualquer versão de software posterior à 9.22.3 é afetada.
- Uma ou ambas as condições são satisfeitas:

1. A pilha do CiscoSSH está ativada e o comando ssh x.x.x.x y.y.y.y.y <management_nameif> está configurado. Nesse caso, as conexões ICMP/Telnet/Hypertext Transfer Protocol Secure (HTTPS) com o nó de dados falham:

```
<#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
```

A pilha CiscoSSH é habilitada por padrão e pode ser desabilitada nas versões 9.19.1 e posteriores. Além disso, na versão 9.23.1 e posterior, essa pilha não pode ser desativada.

2. O comando snmp-server host <management_nameif> está configurado.

<#root>

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

show run snmp-server



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

Nesse caso, as conexões ICMP/Telnet/HTTPS com o nó de dados falham. As conexões SSH também falharão se a pilha CiscoSSH estiver desativada.

# Resolução

Análise

Captura de pacotes na interface de gerenciamento do nó de dados:

<#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 pacotes na interface de controle de cluster do nó de controle:

<#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
```

A resolução permanente requer atualização de software para a versão com a correção do bug da Cisco ID CSCwv19381.

Opções de solução:

a) Remova os comandos snmp-server host na interface de gerenciamento.

Se a pilha CiscoSSH estiver desativada, a remoção dos comandos snmp-server host sobre a interface de gerenciamento restaura a conectividade de gerenciamento para protocolos como ICMP, HTTPS, SSH, Telnet. Se a pilha CiscoSSH estiver habilitada, a conectividade para protocolos como ICMP, HTTPS e Telnet falhará. O comando snmp-server host na interface de gerenciamento não afeta as conexões SSH na interface de gerenciamento se a pilha CiscoSSH estiver habilitada.

b) Desative a pilha CiscoSSH usando o comando no ssh stack cisco. Desabilitar essa pilha ativa a pilha ASA SSH. Além disso, a conectividade de gerenciamento é restaurada para protocolos como ICMP, HTTPS, Telnet. Antes de desativar a pilha CiscoSSH, certifique-se de que você compreende seu impacto. Consulte o livro 1 do CLI: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide para obter mais detalhes.

# Causa

Os sintomas se devem ao bug da Cisco ID CSCwv19381.

## Conteúdo relacionado

- ID de bug da Cisco CSCwv19381
- Livro CLI 1: Guia de configuração da CLI de operações gerais do Cisco Secure Firewall ASA Series

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.