# ソフトウェアのアップグレード後にデータノード管理IPアドレスをクラスタ化する接続障害のトラブルシューティング

## 内容

## お問い合わせ内容

ソフトウェアのアップグレード後、インターネット制御メッセージプロトコル(ICMP)ノードを使用してクラスタデータの管理IPアドレスに接続できなくなります。この記事では、「ノード」または「ユニット」は同じ意味で使用されます。

具体的な症状：

1. データノード管理IPアドレス上の着信エコーパケットに対して、インターネット制御メッセージプロトコル(ICMP)応答パケットが生成されません。

2. 管理インターフェイス上のパケットキャプチャは、データユニットがパケットをローカルで消費および処理するのではなく、非同期の所有者としてコントロールユニットにリダイレクトすることを示しています。

3. クラスタ制御インターフェイス上のパケットキャプチャは、これらのリダイレクトされたICMPエコーパケットがドロップ理由(acl-drop)で制御ノードにドロップされたことを示します。設定されたルールにより、フローが拒否されます。

この記事のコンテキスト内の管理インターフェイスは、management-only individualコマンドで設定されたインターフェイスのnameifを参照します。

<#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
```

# 環境

- スパンインターフェイスを使用したクラスタ設定でのセキュア適応型セキュリティアプライアンスソフトウェア(ASA)バージョン9.22.2.32他のソフトウェアバージョンも影響を受ける可能性があります。
- マルチコンテキストモードまたはシングルコンテキストモードのASA
- 9.22.3より後のソフトウェアバージョンが影響を受けます。
- 次の条件のいずれかまたは両方が満たされます。

1. CiscoSSHスタックが有効で、ssh x.x.x.x y.y.y.y <management_nameif>コマンドが設定されている。この場合、データノードへのICMP/Telnet/Hypertext Transfer Protocol Secure(HTTPS)接続が失敗します。

<#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
```

CiscoSSHスタックはデフォルトで有効になっており、バージョン9.19.1以降では無効にできます。また、バージョン9.23.1以降では、このスタックを無効にすることはできません。

2. snmp-server host <management_nameif>コマンドが設定されていること。

<#root>

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

show run snmp-server



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

この場合、データノードへのICMP/Telnet/HTTPS接続が失敗します。CiscoSSHスタックが無効になっている場合も、SSH接続は失敗します。

# 解決策

分析

データノード管理インターフェイスでのパケットキャプチャ：

<#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
```

制御ノードクラスタ制御インターフェイスでのパケットキャプチャ：

<#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
```

永続的な解決には、Cisco Bug ID CSCwv19381の修正によるバージョンへのソフトウェアアップグレードが必要です。

回避策のオプション：

a)管理インターフェイスからsnmp-server hostコマンドを削除します。

CiscoSSHスタックが無効になっている場合は、管理インターフェイスからsnmp-server hostコマンドを削除すると、ICMP、HTTPS、SSH、Telnetなどのプロトコルの管理接続が復元されます。CiscoSSHスタックを有効にすると、ICMP、HTTPS、Telnetなどのプロトコルの接続が失敗します。CiscoSSHスタックが有効になっている場合、管理インターフェイスを介したsnmp-server hostコマンドは、管理インターフェイスを介したSSH接続には影響しません。

b) no ssh stack ciscoコマンドを使用して、CiscoSSHスタックを無効にします。このスタックを無効にすると、ASA SSHスタックがアクティブになります。さらに、ICMP、HTTPS、Telnetなどのプロトコルの管理接続が復元されます。CiscoSSHスタックを無効にする前に、その影響について理解しておいてください。詳細については、『CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide』を参照してください。

# 原因

この症状は、Cisco Bug ID CSCwv19381が原因で発生します。

# 関連コンテンツ

- Cisco Bug ID CSCwv19381
- CLIブック1:Cisco Secure Firewall ASAシリーズ一般操作CLIコンフィギュレーションガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。