



CHAPTER 7

システム管理上の問題のトラブルシューティング

Cisco Nexus 5000 シリーズ スイッチのシステム管理機能を使用してネットワークをモニタし、管理することで、デバイスの効率的な使用、ロールベースのアクセス制御、SNMP 通信、診断、ロギングなどを実現できます。

この章では、システム管理と Cisco Nexus 5000 シリーズ スイッチで発生する可能性のある問題を特定して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

- 「SNMP」
- 「ロギング」
- 「トラップ」

SNMP

SNMP のメモリ使用量が連続的に増加する

SNMP のメモリ使用量が連続的に増加していることが「show proc mem | inc snmp」コマンドで示されます。

考えられる原因

複数のさまざまなモニタステーションで SNMP 要求を処理していると、SNMP のメモリ使用量が増加します。普通は時間の経過とともにメモリ使用量は一定の範囲に落ち着きます。メモリ使用量が安定せずに増加し続ける場合は、メモリリークが発生している SNMP 要求が存在します。

解決方法

「show system internal snmp mem-stats detail」コマンドの実行結果を確認します。

次のモニタステーションで SNMP 要求を処理しているときに、サンプルスナップショットを取得します。

- 「show clock」
- 「show system internal mem-stats detail」
- 「show tech snmp」

SNMP が応答しない

SNMP 要求に対する応答がないか、応答が遅延します。

考えられる原因

GET、GETNEXT、WALK などの SNMP 操作でスイッチの CPU 使用率が高くなると、応答が極端に遅くなり、場合によってはタイムアウトになって応答が得られません。

解決方法

SNMP が応答しない場合は、次のコマンドで CPU 使用率を確認します。

- 「show proc cpu history」
- 「show proc cpu sort」

このコマンドの実行結果から、Nexus 5000 のコンポーネントのうち、CPU のリソースを大量に消費しているものはどれであるかがわかります。

SNMP が応答せず、SNMP がタイムアウトしたことが「show snmp」で報告される

SNMP が応答せず、SNMP がタイムアウトしたことが「show snmp」コマンドで報告されます。

考えられる原因

SNMP プロセスは終了していますが、クラッシュしていない可能性があります。

解決方法

「show system internal sysmgr service name snmpd」コマンドを実行して、ステータスが「SRV_STATE_HANDSHAKED」であることが示される必要があります。

例：

```
Service "snmpd" ("snmpd", 74):
UUID = 0x1A, PID = 4131, SAP = 28
State: SRV_STATE_HANDSHAKED (entered at time Mon Jun 14 17:12:15 2010).
Restart count: 1
Time of last restart: Mon Jun 14 17:12:14 2010.
The service never crashed since the last reboot.
Tag = N/A
Plugin ID: 0
```

SNMP の SET 操作を実行できない

SNMP の SET 操作を実行しようとすると、次のエラーが表示されます。

```
bash-2.05b$ snmpset -v2c -c private 10.78.25.211 .1.3.6.1.4.1.9.9.305.1.1.6.0 i 1
Error in packet.
Reason: notWritable
```

考えられる原因

SNMP コミュニティに書き込み権限がありません。

解決方法

「show snmp community」コマンドの実行結果で、書き込み権限がイネーブルであることを確認します。

例：

```
Community          Group / Access    context    acl_filter

private            network-operator
public             network-admin

Only "network-admin" has write permissions.
snmpset -v2c -c public 10.78.25.211 .1.3.6.1.4.1.9.9.305.1.1.6.0 i 1
enterprises.9.9.305.1.1.6.0 =
```

BRIDGE-MIB で実行する SNMP

BRIDGE-MIB で実行する SNMP の GET 操作で正しい値が返されず、エラーになります。

考えられる原因

BRIDGE-MIB がサポートされていない可能性があります。

解決方法

該当のリリース ノートを調べ、4.2 (1) 以降のリリースで BRIDGE-MIB がサポートされていることを確認します。

ロギング

システムが応答しない

システムのパフォーマンスが著しく低いか、応答がありません。

考えられる原因

利用率が異常に高いシステム リソースがあることが考えられます。たとえば、ロギング レベルが正しくないと大量のメッセージが生成され、システム リソースを圧迫することがあります。

解決方法

シャーシに対するロギング レベルを確認します。6 や 7 などのロギング レベルを設定するとメッセージが大量に生成されるので、パフォーマンスに影響することがあります。次のコマンドを使用して、現在のリソース使用量を表示します。

- 「sho proc cpu | inc syslogd」
- 「sho proc cpu」
- 「show run | inc logging」
- 「show system resource」

DUT からのメッセージを Syslog サーバで受信できない

Syslog サーバは設定済みですが、宛先の Syslog サーバでは DUT からのメッセージを受信していません。

考えられる原因

Syslog サーバがアクセス不能になっているか、ロギング レベルが不適切であることが考えられます。

解決方法

- VRF 管理から宛先の Syslog サーバがアクセス可能であるかどうかを確認します。「ping <dest-ip> vrf management」コマンドを使用して、サーバに ping を送信します。
- DUT の Syslog 設定に use-vrf management があることを確認します。

例：

```
logging server 10.193.12.1 5 use-vrf management
```

- ロギング メッセージを送信するために適切なロギング レベルがイネーブルになっていることを確認します。「show logging info」コマンドを使用します。ロギング レベルが不適切な場合は、「logging level <feature> <log-level>」コマンドを使用して適切なレベルを設定します。

トラップ

トラップを受信できない

トラップの結果が受信されません。

考えられる原因

トラップがイネーブルになっていないか、SNMP ホストがアクセス不能になっている可能性があります。

次の原因が考えられます。

- トラップがイネーブルになっていない。
- SNMP ホストがアクセス不能になっている。
- ファイアウォールでアクセスがブロックされている。
- アクセスリストで UDP ポート 162 がブロックされている。

解決方法

次のコマンドを使用して、適切な VRF が SNMP ホストに設定されているかどうか、トラップがイネーブルになっているかどうかを確認します。

- 「snmp-server enable traps <trapname>」
- 「snmp-server host x.x.x.x use-vrf <vrf-name>」
x.x.x.x は、トラップを受信するデバイスの IP アドレスです。