



## CHAPTER 2

# トラブルシューティングで使用されるツール

この章では、Cisco Nexus 1000V に使用できるトラブルシューティング ツールについて説明します。この章の内容は次のとおりです。

- 「コマンド」 (P.2-1)
- 「ping」 (P.2-2)
- 「traceroute」 (P.2-2)
- 「プロセスおよび CPU のモニタリング」 (P.2-2)
- 「RADIUS」 (P.2-5)
- 「Syslog」 (P.2-5)

## コマンド

ローカル コンソールのコマンドライン インターフェイス (CLI) またはリモートで Telnet セッションまたは Secure Shell (SSH; セキュア シェル) セッションを使用します。CLI のコマンド構造は、状況依存ヘルプ、**show** コマンド、マルチユーザ サポート、ロールベースのアクセス コントロールを使用できるという点で、NX-OS ソフトウェアと似ています。

各機能には、機能の設定、ステータス、パフォーマンスに関する情報を提供する **show** コマンドが用意されています。また、次のコマンドを使用すると、さらに詳しい情報を確認することができます。

- **show system** : コア、エラー、および例外を含むシステムレベルのコンポーネントに関する情報を提供します。エラー コードに関する詳細を確認するには、**show system error-id** コマンドを使用します。

```
n1000v# copy running-config startup-config
[#####] 100%
2008 Jan 16 09:59:29 zoom %$ VDC-1 %$ %BOOTVAR-2-AUTOCOPY_FAILED: Autocopy of file
/bootflash/n1000-s1-dk9.4.0.0.837.bin.S8 to standby failed, error=0x401e0008
```

```
n1000v# show system error-id 0x401e0008
Error Facility: sysmgr
Error Description: request was aborted, standby disk may be full
```

## ping

`ping` ユーティリティは、TCP/IP インターネットワークを経由する宛先に対して、一連のエコーパケットを生成します。エコーパケットは、宛先に到達すると、再ルーティングされて送信元に戻されます。`ping` を使用すると、IP ルーティング ネットワーク 経由で特定の宛先への接続および遅延を確認できます。

`ping` コマンドでは、ポートまたはエンド デバイスを `ping` できます。IPv4 アドレスを指定することにより、宛先に一連のフレームが送信できます。これらのフレームは、ターゲット デバイスに到達し、タイムスタンプが付加されて、送信元にループバックされます。`ping` を使用すると、宛先への接続および遅延を確認できます。

## traceroute

`traceroute` は、次の目的で使用します。

- データ トラフィックが経由したルートを追跡します。
- スイッチ間（ホップ単位）の遅延を計算します。

`traceroute` ユーティリティでは、双方向のパスがホップバイホップ ベースで識別され、ホップごとにタイムスタンプが付加されます。`traceroute` を使用すると、発信スイッチと宛先に最も近いスイッチ間のパスに沿って、ポートの接続をテストできます。

この機能にアクセスするには、`traceroute CLI` コマンドを使用します。

宛先に到達できない場合には、パス検出が開始され、障害ポイントまでのパスがトラッキングされます。

## プロセスおよび CPU のモニタリング

CLI には、スイッチ プロセスと、CPU のステータスおよび使用率をモニタするための機能が用意されています。

ここでは、次の項目について説明します。

- 「[実行中のプロセスおよびその状態の識別](#)」(P.2-2)
- 「[CPU 使用率の表示](#)」(P.2-3)
- 「[CPU およびメモリ情報の表示](#)」(P.2-4)

### 実行中のプロセスおよびその状態の識別

実行中のプロセスおよび各プロセスのステータスを確認するには、`show processes` コマンドを使用します。(例 2-1 を参照)。コマンド出力には、次の情報が表示されます。

- PID = プロセス ID。
- State = プロセスの状態。
- PC = 現在のプログラム カウンタ (16 進形式)。
- Start\_cnt = プロセスがこれまでに開始 (または再開) された回数。
- TTY = プロセスを制御している端末。通常、「-」(ハイフン) は、特定の TTY 上で実行されていないデーモンを表します。
- Process = プロセスの名前。

プロセスの状態は次のとおりです。

- D = 中断なしで休止（通常 I/O）。
- R = 実行可能（実行キュー上）。
- S = 休止中。
- T = トレースまたは停止。
- Z = 存在しない（ゾンビ）プロセス。
- NR = 実行されていない。
- ER = 実行されているべきだが、現在は実行されていない。



(注)

一般に、ER ステートは、プロセスの再起動回数が多すぎるために、システムが障害発生と判断してそのプロセスをディセーブルにしたことを示しています。

### 例 2-1 show processes コマンド

```
n1000v# show processes ?
cpu      Show processes CPU Info
log      Show information about process logs
memory   Show processes Memory Info

n1000v# show processes

PID      State  PC          Start_cnt  TTY  Process
-----  -----  -----  -----  ---  -----
   1      S     b7f9e468   1          -    init
   2      S           0          1      -    migration/0
   3      S           0          1      -    ksoftirqd/0
   4      S           0          1      -    desched/0
   5      S           0          1      -    migration/1
   6      S           0          1      -    ksoftirqd/1
   7      S           0          1      -    desched/1
   8      S           0          1      -    events/0
   9      S           0          1      -    events/1
  10      S           0          1      -    khelper
  15      S           0          1      -    kthread
  24      S           0          1      -    kacpid
 101      S           0          1      -    kblockd/0
 102      S           0          1      -    kblockd/1
 115      S           0          1      -    khubd
 191      S           0          1      -    pdflush
 192      S           0          1      -    pdflushn
...

```

## CPU 使用率の表示

CPU 使用率を表示するには、**show processes cpu** コマンドを使用します。コマンド出力には、次の情報が表示されます。

- Runtime(ms) = プロセスが使用した CPU 時間（ミリ秒単位）。
- Invoked = プロセスがこれまでに開始された回数。
- uSecs = プロセスの呼び出しごとの平均 CPU 時間（ミリ秒単位）。
- lSec = 最近の 1 秒間における CPU 使用率（パーセント単位）。

**例 2-2 show processes cpu コマンド**

```
n1000v# show processes cpu
```

PID	Runtime (ms)	Invoked	uSecs	lSec	Process
1	922	4294967295	0	0	init
2	580	377810	1	0	migration/0
3	889	3156260	0	0	ksoftirqd/0
4	1648	532020	3	0	desched/0
5	400	150060	2	0	migration/1
6	1929	2882820	0	0	ksoftirqd/1
7	1269	183010	6	0	desched/1
8	2520	47589180	0	0	events/0
9	1730	2874470	0	0	events/1
10	64	158960	0	0	khelper
15	0	106970	0	0	kthread
24	0	12870	0	0	kacpid
101	62	3737520	0	0	kblockd/0
102	82	3806840	0	0	kblockd/1
115	0	67290	0	0	khubd
191	0	5810	0	0	pdflush
192	983	4141020	0	0	pdflush
194	0	5700	0	0	aio/0
193	0	8890	0	0	kswapd0
195	0	5750	0	0	aio/1
...					

## CPU およびメモリ情報の表示

システム関連の CPU およびメモリの統計情報を表示するには、**show system resources** コマンドを使用します。このコマンドの出力には、次の情報が表示されます。

- **Load** は、実行中のプロセスの数として定義されます。Load average には、過去 1 分間、5 分間、および 15 分間のシステム負荷が表示されます。
- **Processes** には、システム内のプロセスの数、およびコマンドの実行時に実際に稼動していたプロセスの数が表示されます。
- **CPU states** には、直前の 1 秒間における CPU のユーザ モードとカーネル モードでの使用率およびアイドル時間がパーセントで表示されます。
- **Memory usage** には、合計メモリ、使用中メモリ、空きメモリ、バッファに使用されているメモリ、およびキャッシュに使用されているメモリが KB 単位で表示されます。また、**buffers** および **cache** の値には、使用中メモリの統計情報も含まれます。

**例 2-3 show system resources コマンド**

```
n1000v# show system resources
Load average: 1 minute: 0.30 5 minutes: 0.34 15 minutes: 0.28
Processes : 606 total, 2 running
CPU states : 0.0% user, 0.0% kernel, 100.0% idle
Memory usage: 2063268K total, 1725944K used, 337324K free
                2420K buffers, 857644K cache
```

# RADIUS

RADIUS は、ヘッドエンドの RADIUS サーバとクライアント デバイス間で、属性またはクレデンシアルを交換するために使用されるプロトコルです。これらの属性は、次の 3 つの Class of Service (CoS) に関連しています。

- 認証
- 許可
- アカウンティング

認証は、特定のデバイスにアクセスするユーザの認証を意味しています。RADIUS を使用して、Cisco Nexus 1000V デバイスにアクセスするユーザ アカウントを管理できます。デバイスへのログインを試みると、Cisco Nexus 1000V によって、中央の RADIUS サーバの情報に基づいてユーザ検証が行われます。

許可は、認証されたユーザのアクセス許可範囲を意味しています。ユーザに割り当てたロールは、ユーザにアクセスを許可する実デバイスのリストとともに、RADIUS サーバに保管できます。ユーザが認証されると、スイッチは RADIUS サーバを参照して、スイッチ ネットワーク内でのユーザのアクセス範囲を決定します。

アカウンティングは、スイッチの管理セッションごとに保管されるログ情報を意味しています。この情報を使用して、トラブルシューティングおよびユーザ アカウンタビリティのレポートを生成できます。アカウンティングは、(RADIUS を使用して) ローカルまたはリモートで実装できます。

次に、アカウンティング ログ エントリの例を示します。

```
n1000v# show accounting log
Sun Dec 15 04:02:27 2002:start:/dev/pts/0_1039924947:admin
Sun Dec 15 04:02:28 2002:stop:/dev/pts/0_1039924947:admin:vsh exited normally
Sun Dec 15 04:02:33 2002:start:/dev/pts/0_1039924953:admin
Sun Dec 15 04:02:34 2002:stop:/dev/pts/0_1039924953:admin:vsh exited normally
Sun Dec 15 05:02:08 2002:start:snmp_1039928528_172.22.95.167:public
Sun Dec 15 05:02:08 2002:update:snmp_1039928528_172.22.95.167:public:Switchname
```



(注)

アカウンティング ログは、各セッションの最初と最後（開始と終了）だけを表示します。

# Syslog

システム メッセージ ロギング ソフトウェアを使用して、メッセージをログ ファイルに保存するか、または他のデバイスに転送します。この機能では、次のことができます。

- モニタリングおよびトラブルシューティングのためのログ情報の記録
- キャプチャするログ情報のタイプの選択
- キャプチャするログ情報の宛先の選択

Syslog を使用すると、システム メッセージを時間順にローカルに保存したり、中央の Syslog サーバに送信したりできます。Syslog メッセージをコンソールに出力すると、すぐに使用できます。これらのメッセージの詳細は、選択した設定によって異なります。

Syslog メッセージは、イベントの重大度に応じて、*debug* から *critical* までの 7 つのカテゴリに分類されます。スイッチ内の特定のサービスについて、レポートされる重大度を制限できます。

ログ メッセージは、システム再起動後には消去されています。ただし、重大度が *critical* 以下（レベル 0、1、および 2）のログ メッセージは、最大 100 個までローカル ファイルまたはサーバに保存されます。

## ログ レベル

Cisco Nexus 1000V では、次のログ レベルがサポートされています。

- 0-emergency (緊急)
- 1-alert (警報)
- 2-critical (重大)
- 3-error (エラー)
- 4-warning (警告)
- 5-notification (通知)
- 6-informational (情報)
- 7-debugging (デバッグ)

デフォルトでは、標準的かつ重要なシステム メッセージがログ ファイルに記録され、システム コンソールに送信されます。ユーザは、ファシリティ タイプおよび重大度に基づいて、保存するシステム メッセージを指定できます。リアルタイムのデバッグおよび管理を強化するために、メッセージにはタイムスタンプが付加されます。

## Telnet または SSH へのロギングのイネーブル化

システム ロギング メッセージは、デフォルトまたは設定済みのロギング ファシリティおよび重大度の値に基づいてコンソールに送信されます。

ユーザは、コンソールへのロギングをディセーブルにしたり、または特定の Telnet セッションまたは SSH セッションへのロギングをイネーブルにしたりできます。

- コンソールへのロギングをディセーブルにするには、コンフィギュレーション モードで **no logging console** コマンドを使用します。
- Telnet または SSH へのロギングをイネーブルにするには、EXEC モードで **terminal monitor** コマンドを使用します。



(注)

コンソール セッションへのロギングをディセーブルまたはイネーブルにすると、その状態は、それ以後のすべてのコンソール セッションに適用されます。ユーザがセッションを終了して新規のセッションに再びログインした場合、状態は維持されています。ただし、Telnet セッションまたは SSH セッションへのロギングをイネーブルまたはディセーブルにすると、その状態はそのセッションだけに適用されます。ユーザがセッションを終了したあとは、その状態は維持されません。

例 2-4 に示す **no logging console** コマンドには、次の特徴があります。

- コンソールへのロギングをディセーブルにする。
- デフォルトでイネーブルになっている。

### 例 2-4 no logging console コマンド

```
n1000v(config)# no logging console
```

例 2-5 に示す **terminal monitor** コマンドには、次の特徴があります。

- Telnet または SSH へのロギングをイネーブルする。
- デフォルトでは、ディセーブルになっている。

**例 2-5 terminal monitor コマンド**

```
n1000v# terminal monitor
```

Syslog の設定の詳細については、『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

