



# CHAPTER 10

## 使いやすくするための管理ツール

この章では、デバイスの管理に推奨する Cisco NX-OS ソフトウェアについて説明します。設定の変更、スーパーバイザ モジュール ステータスの確認、またはハードウェアの交換についても説明します。

この章で説明する内容は、次のとおりです。

- 「設定の変更」
- 「スーパーバイザ冗長性」
- 「ロケータ LED」
- 「Ethanalyzer」
- 「スイッチド ポート アナライザ」
- 「デバッグの実行」

## 設定の変更

ここでは、Cisco NX-OS の設定を変更する場合に推奨される手順面でのベスト プラクティスについて説明します。

## 設定のロールバック

### 導入 : Cisco NX-OS Release 4.0(1)

設定のロールバック機能を使用すると、管理者は、新しい設定への変更が想定どおりに動作しなかった場合に設定を簡単にロールバックできるようにするための、設定チェックポイントを作成できます。実稼動ネットワークで変更制御手順によって変更を行う前に、設定のチェックポイントを作成するための設定ロールバック機能を使用することを推奨します。これによって、予見できない問題が発生した場合に、1 つのコマンドで元の設定を再適用できます。Cisco NX-OS Release 4.2(1) から、(手動またはライセンスの期限切れによって) 機能がディセーブルの場合に、自動チェックポイントが作成されます。ライセンスの期限切れによる VDC の削除では、自動チェックポイントは生成されません。Cisco NX-OS Release 4.2(1) チェックポイントから、**checkpoint file** コマンドを使用して作成しない場合に、チェックポイントがスタンバイ スーパーバイザに保存されます。次に、基本的なチェックポイントおよびロールバックの動作に関する例を示します。

```
n7000# checkpoint ospf-change-control
.....Done

n7000(config)# interface ethernet x/x
n7000(config-if)# ip address x.x.x.x/xx
```

```

n7000(config-if)# ip router ospf 10 area 0
n7000(config-if)# no shutdown

n7000# show run interface ethernet x/x

interface Ethernetx/x
 ip address x.x.x.x/xx
 ip router ospf 10 area 0.0.0.0
 no shutdown

n7000# rollback running-config checkpoint ospf-change-control
Note: Applying config parallely may fail Rollback verification
Collecting Running-Config
Generating Rollback Patch
Executing Rollback Patch
Generating Running-config for verification
Generating Patch for verification

n7000# show run interface ethernet x/x

```

## Session Manager

### 導入 : Cisco NX-OS Release 4.0(1)

Session Manager を使用すると、ACL および QoS の設定を、バッチ モードで実行コンフィギュレーションに設定できます。これは、設定を適用する前に、TCAM スペースなどのハードウェア リソースが使用可能かどうかを確認する場合に役に立ちます。ACL を適用する場合か、QoS を設定する場合には、Session Manager を常に使用する必要があります。次に、インターフェイスに対して ACL を設定、確認、および適用する処理について説明します。

```

n7000# configure session apply-acl
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
n7000(config-s)# ip access-list inbound-acl
n7000(config-s-acl)# deny ip 10.0.0.0/8 any
n7000(config-s-acl)# deny ip 172.16.0.0/12 any
n7000(config-s-acl)# deny ip 192.168.0.0/16 any
n7000(config-s-acl)# interface ethernet x/x
n7000(config-s-if)# ip access-group inbound-acl in
n7000(config-s-if)# verify
Verification Successful
n7000(config-s)# commit
Commit Successful

```

## スーパーバイザ冗長性

ハイ アベイラビリティを使用するには、シャードごとに 2 つのスーパーバイザ モジュールを取り付けることを推奨します。ここでは、冗長スーパーバイザ モジュールのステータスを確認し、必要な場合に手動でスーパーバイザ スイッチオーバーを実行する場合の情報について、説明します。

## スーパーバイザ ステータスの確認

### 導入 : Cisco NX-OS Release 4.0(1)

2 つのスーパーバイザ モジュールがある場合、スイッチの通常の動作中には、1 つのスーパーバイザ モジュールは「Active with HA standby」状態で、もう 1 つのスーパーバイザ モジュールは「HA Standby」状態である必要があります。

```
n7000# show system redundancy status

Redundancy mode
-----
      administrative:   HA
      operational:     HA

This supervisor (sup-1)
-----
      Redundancy state: Active
      Supervisor state: Active
      Internal state:   Active with HA standby

Other supervisor (sup-2)
-----
      Redundancy state: Standby
      Supervisor state: HA standby
```

## 手動スイッチオーバー

### 導入 : Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

スーパーバイザ スイッチオーバーは、2 つのスーパーバイザ モジュールがある場合に、シャーシを使用して手動で起動できます。スイッチオーバーが実行されると、前のアクティブなスーパーバイザ モジュールはリロードされ、スタンバイ スーパーバイザ としてオンライン状態に戻ります。スタンバイ スーパーバイザ が「HA standby」ではない場合、スイッチオーバーを手動で実行することはできません。

```
n7000# system switchover
```

## ロケータ LED

### 導入 : Cisco NX-OS Release 4.0(1)

Cisco NX-OS ソフトウェアでは、イーサネット I/O モジュール上でハードウェア コンポーネント (シャーシ、ファン、ファブリック、モジュール、電源) およびポートを識別する場合に役に立つ、ロケータ LED 機能がサポートされます。ハードウェアの交換またはイーサネット ポートに関する作業 (追加、移動など) の物理的な作業を担当する、リモート サポート チームとともに作業を行う場合には、ロケータ LED 機能を使用する必要があります。シャーシ コンポーネントまたはインターフェイスのロケータ LED をディセーブルにするには、**no locator-led** コマンドを使用します。

```
n7000# locator-led chassis
n7000# locator-led fan 1
n7000# locator-led module 1
n7000# locator-led powersupply 1
n7000# locator-led xbar 1

n7000(config)# interface ethernet 1/1
```

```
n7000(config-if)# beacon

n7000# show locator-led status
Component          Locator LED Status
-----
Chassis            ON
Module 1           ON
Module 2           off
Module 5           off
Xbar 1             ON
Xbar 2             off
Xbar 3             off
PowerSupply 1     ON
PowerSupply 2     off
PowerSupply 3     off
Fan 1              ON
Fan 2              off
Fan 3              off
```



(注)

Cisco NX-OS CLI の構文は、Cisco NX-OS Release 4.1(2) で変更されました。**locator-led** コマンドが、廃止予定の **blink** コマンドに置き換わりました。I/O モジュールのイーサネット ポートのステータスは、**show locator-led status** コマンドの出力には表示されません。ポート ロケータ LED (ビーコン) がイネーブルかディセーブル化を判断するには、**show interface** コマンドを使用するか、または実行コンフィギュレーションを表示します。

## Ethalyzer

### 導入 : Cisco NX-OS Release 4.0(1)

コントロールプレーンプロトコルおよび CPU の使用率が高い場合にトラブルシューティングを行うには、イーサネット アナライザを使用します。イーサネット アナライザを使用すると、管理者は、スーパーバイザ モジュール CPU へ、およびスーパーバイザ モジュール CPU から、送信されるパケットを記録できます。CLI を使用して、パケットごとの簡略情報または詳細情報を記録して表示するか、または、Wireshark などのプロトコル アナライザにエクスポートできます。トラブルシューティングをする場合、対象パケットを特定するには簡略な記録を実行し、対象パケットをより詳細に分析するには詳細な記録を実行する必要があります。記録は、**write** または **>** オプションを使用してファイルにリダイレクトし、ローカルに保存できます。イーサネット アナライザでは、デフォルトで 10 フレームが記録されます。フレーム数を増加するには、**limit-captured-frames <0- 2147483647>** オプションを使用できます。値 **0** は、制限がないことを意味し、10MB の循環バッファが作成されます。

### 簡略記録 :

```
n7000# ethalyzer local interface inband
Capturing on inband
2010-06-02 20:44:40.327808 192.168.20.1 -> 224.0.0.5    OSPF Hello Packet
2010-06-02 20:44:41.480658 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730633 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730638 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com
2010-06-02 20:44:42.480586 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com
```

<テキストは省略>

## 詳細記録:

```
n7000# ethanalyzer local interface inband limit-captured-frames 100 detail
Capturing on inband
Capturing on inband
Frame 1 (60 bytes on wire, 60 bytes captured)
  Arrival Time: Oct  2, 2010 22:07:57.150394000
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 60 bytes
  Capture Length: 60 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:llc:stp]
IEEE 802.3 Ethernet
  Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
  Address: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
```

<テキストは省略>

## 簡略記録のファイルへの書き込み:

```
n7000# ethanalyzer local interface inband write bootflash:cpu.
```

## 記録ファイルの読み取り:

```
n7000# ethanalyzer local read bootflash:cpu.txt
```

## 詳細記録のファイルへのリダイレクト:

```
n7000# ethanalyzer local interface detail > cpu-1.txt
```

## 記録ファイルの読み取り:

```
n7000# show file bootflash:cpu-1.txt
```



(注) **inband** オプションでは、I/O モジュールのパケットが記録され、**mgmt** オプションでは、スーパーバイザ モジュール **mgmt0** ポートが記録されます。



(注) CLI の構文は、Cisco NX-OS Release 4.x から Release 5.x で、少し変更されました。この CLI の出力は、NX-OS Release 5.1(1) から記録されます。

## スイッチドポートアナライザ

### 導入 : Cisco NX-OS Release 4.0(1)

Intrusion Prevention Systems (IPS; 侵入防御システム) などのネットワーク サービスでトラブルシューティングまたはデータの提供を行う場合、Switched Port Analyzer (SPAN; スイッチドポートアナライザ) を使用して、送信元から宛先へトラフィックをミラーできます。このマニュアルでは、SPAN の詳細については説明しませんが、トラブルシューティング後にアクティブにする必要がない場合には、ローカルセッションおよび ERSPAN セッションで **shut** コマンドを使用してディセーブルにすることを推奨します。これによって、ハードウェア リソースで、ファブリック全体に不要なトラフィックが充満することを防ぐことができます。ERSPAN 機能が、Cisco NX-OS Release 5.1(1) で導入されました。

#### ローカル SPAN :

```
n7000(config)# monitor session 1
n7000(config-monitor)# shut
```

#### Encapsulated Remote (ERSPAN; カプセル化リモート) :

```
n7000(config)# monitor session 1 type erspan-source
n7000(config-erspan-src)# shut

n7000(config)# monitor session 1 type erspan-destination
n7000(config-erspan-dst)# shut
```

## デバッグの実行

ここでは、デバッグを実行する場合の Cisco NX-OS 推奨のベスト プラクティスについて説明します。ネットワークのパフォーマンスに影響が及ぼされる可能性があるため、デバッグ コマンドの実行時には、常に注意を払ってください。

## ファイルへの出力のリダイレクト

### 導入 : Cisco NX-OS Release 4.0(1)

デバッグの出力は、デフォルトで、コンソールセッションおよびモニタリングセッション (SSH/Telnet) に記録されます。これは、ネットワーク パフォーマンスに影響を及ぼす可能性があります。デバッグの実行時には、スーパーバイザ モジュール CPU での処理のオーバーヘッドを抑制するには、出力を、コンソールセッションまたはターミナルセッションではなく、ファイルにリダイレクトする必要があります。次に、分析のためにデバッグの出力がファイルにリダイレクトされる例を示します。リダイレクトされたデバッグの出力は、**log:** ディレクトリに保存されます。デバッグの出力がファイルにリダイレクトされると、リモートの宛先に出力を表示するか、または、コピーできます。**pipe** オプションを使用すると、ログ ファイルを解析できます。**show debug** コマンドによって現在のデバッグ ステータスが表示され、**no debug all** コマンドによってすべてのデバッグがディセーブルになります。



(注) 必要ではない、意図しないデバッグを実行したままにしないでください。

```
n7000# debug logfile cdp-debug
n7000# debug cdp all
n7000# no debug cdp all

n7000# dir log:cdp-debug
14560 Nov 01 22:05:18 2010 cdp-debug

n7000# show debug logfile cdp-debug
2010 Nov 1 22:02:02.948577 cdp: Going to send CDP version 2 pkt on Ethernet7/3
2010 Nov 1 22:02:02.948662 cdp: Sent CDP packet untagged on interface 0x1a30200
0
2010 Nov 1 22:02:02.948696 cdp: Going to send CDP version 2 pkt on Ethernet10/1
8

<テキストは省略>

n7000# show debug logfile cdp-debug | include Ethernet10/1
```