CHAPTER 9

IP 管理

この章では、IP 管理プロトコルを設定する場合に Cisco NX-OS が推奨するベスト プラクティス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。

Network Time Protocol（NTP）

ログのタイムスタンプおよびその他の管理データがすべてのデバイスで同期されるよう、すべてのネットワーク デバイスで NTP を設定することを推奨します。ネットワーク全体で相関しているネットワーク イベントの場合、NTP を使用すると利点があります。Cisco NX-OS では、NTP クライアント モードおよびピア モードでの動作がサポートされます。

冗長 NTP サーバ

導入：Cisco NX-OS Release 4.0(1)

冗長性のために、複数の NTP サーバを設定する必要があります。プライマリ NTP サーバは **prefer** オプションで設定し、VRF インスタンスは、アウトオブバンド接続に管理 VRF インスタンスを使用するよう、VRF インスタンスを設定する必要があります。

```
n7000(config)# ntp server a.a.a.a prefer use-vrf management
n7000(config)# ntp server a.a.a.a use-vrf management

n7000(config)# ntp peer b.b.b.b prefer use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
```

時間帯 / サマー タイム

導入：Cisco NX-OS Release 4.0(1)

デフォルト値が不要の場合、クロックの時間帯およびサマー タイムのパラメータを設定する必要があります。これらの値が設定されていない場合、クロックは、デフォルトで、サマー タイムの調整なしで UTC に設定されます。

```
n7000(config)# clock timezone PST -8 0
n7000(config)# clock summer-time PST
```

NTP 送信元インターフェイス/IP アドレス

導入：Cisco NX-OS Release 4.1(3)

管理 VRF インスタンス以外の VRF インスタンスを使用する場合は、NTP 送信元インターフェイスまたは IP アドレスを指定することを推奨します。これによって、ファイアウォールなどのセキュリティデバイスが、NTP パケットの送信元を特定できます。送信元インターフェイスまたは IP アドレスが指定されない場合、元の（アウトバンド）インターフェイスのプライマリ IP アドレスが使用されます。NTP トラフィックが管理 VRF インスタンスに関連付けられている場合、mgmt0 インターフェイスの IP アドレスが選択されます。NTP インターフェイスと IP 送信元アドレスを同時に設定することはできません。

```
n7000(config)# ntp source-interface ethernet 2/1

n7000(config)# ntp source x.x.x.x
```

NTP ロギング

導入：Cisco NX-OS Release 5.0(2a)

NTP ロギングはデフォルトでディセーブルになっています。NTP 同期の問題のトラブルシューティングを行う場合、NTP メッセージを記録してトラブルシューティングの参考にできます。

```
n7000(config)# ntp logging
```

MD5 認証

導入：Cisco NX-OS Release 5.0(2a)

デバイスで、そのクロックがルージュ NTP サーバまたはピアから同期されないようにするため、MD5 認証をイネーブルにする必要があります。NTP クライアント、ピア、サーバには、同じ信頼済み認証キーを設定する必要があります。異なる認証キーを使用して NTP サーバまたはピアから NTP メッセージを受信する場合、NTP クライアントではそのクロックと同期されません。

```
n7000(config)# ntp server a.a.a.a use-vrf management key 1
n7000(config)# ntp peer b.b.b.b use-vrf management key 1

n7000(config)# ntp authentication-key 1 md5 <password>
n7000(config)# ntp trusted-key 1
n7000(config)# ntp authenticate
```

アクセス コントロール リスト

導入：Cisco NX-OS Release 5.0(2a)

セキュリティを強化するには、特定の NTP ピアまたはサーバへのアクセスを制限して、Access Control List（ACL; アクセス コントロール リスト）を設定する必要があります。**statistics per-entry** での ACL 統計の収集はオプションですが、特定の NTP ピアまたはサーバから受信しているパケットの確認には効果的です。

```
n7000(config)# ntp server a.a.a.a use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
```

```
n7000(config)# ntp source x.x.x.x
n7000(config)# ntp access-group peer ntp-peers

n7000(config)# ip access-list ntp-peers
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit udp a.a.a.a/32 x.x.x.x/32 eq ntp
n7000(config-acl)# permit udp b.b.b.b/32 x.x.x.x/32 eq ntp
```

簡易ネットワーク管理プロトコル（SNMP）

Cisco NX-OS では、SNMP v1、v2c、および v3 がサポートされます。SNMPv3 では、ユーザ名、パスワード、およびペイロード データに対する認証機能および暗号化機能があるため、セキュリティを強化するには、SNMPv3 の使用を推奨します。

基本設定（連絡先 / 場所）

導入：Cisco NX-OS Release 4.0(1)

SNMP 管理デバイスからポーリングされているときにデバイスが識別されるよう、連絡先および場所の情報を指定します。

```
n7000(config)# snmp contact Cisco Systems
n7000(config)# snmp location San Jose, CA
```

ユーザ（バージョン 3）

導入：Cisco NX-OS Release 4.0(1)

追加のセキュリティ認証および暗号メカニズムのため、SNMPv3 が SNMP の推奨バージョンです。デフォルトでは、ローカル データベースにあるすべてのユーザ アカウントは、SNMPv3 要求を認証する場合に SNMP サーバが使用できる SNMP ユーザに同期されます。SNMP ポーリングおよび SNMP インフォーム通知の送信用に、追加のユーザ アカウント /SNMP ユーザ アカウントを作成できます。次の例では、デフォルトの「admin」ユーザが表示され、「snmp-user」という名前の別の SNMP ユーザが作成されます。v3 通知を送信するには、SNMP ユーザに対してエンジン ID のみを設定する必要があります（エンジン ID の値は、SNMP 通知サーバのエンジン ID に基づいています）。

```
n7000# show run snmp

snmp-server user admin network-admin auth md5 0x272298231264cbf31dbd423455345253 priv
aes-128 0x272298231264cbf31dbd423455345253 localizedkey

n7000(config)# snmp-server user snmp-user auth md5 <password> priv aes-128 <password>
engineID 80:00:00:09:03:00:0C:29:13:92:B9
```

コミュニティ ストリング（バージョン 1 および 2c）

導入：Cisco NX-OS Release 4.0(1)

SNMPv3 対応の管理サーバが使用できない場合、**snmp-server community** コマンドを使用して SNMP バージョン 1 および 2c をイネーブルにできます。SNMP v2c では、SNMPv1 以上の追加機能が提供されます。SNMP は、読み取り専用アクセスまたは読み取り / 書き込みアクセスに設定できます。セキュリティを強化するには、読み取り専用（ネットワーク オペレータ）アクセスのみをイネーブルにします。

```
n7000(config)# snmp-server community <password> group network-operator

n7000(config)# snmp-server community <password> group network-admin
```

（注）　**snmp-server community <password> ro** コマンドは、**snmp-server community <password> group network-operator** コマンドに自動的に変換されます。**snmp-server community <password> rw** コマンドは、**snmp-server <password> group network-admin** コマンドに自動的に変換されます。

通知 / トラップ受信機

導入：Cisco NX-OS Release 4.0(1)

ネットワーク イベントについて SNMP ネットワーク管理サーバに通知するには、SNMP 通知受信機を設定する必要があります。受信機は、特定の VRF インスタンスの SNMPv1、SNMPv2c、および SNMPv3 に対して設定できます。追加認証機能と暗号化機能のため、SNMP v3 を推奨します。SNMPv3 では、SNMP 受信者エンジン ID で設定された SNMP ユーザが必要です。

バージョン 3（推奨）

```
n7000(config)# snmp-server host x.x.x.x version 3 priv snmp-user
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

バージョン 2c

```
n7000(config)# snmp-server host x.x.x.x traps version 2c <password>
n7000(config)# snmp-server host x.x.x.x informs version 2c <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

バージョン 1

```
n7000(config)# snmp-server host x.x.x.x traps version 1 <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

通知 / トラップ イベント

導入：Cisco NX-OS Release 4.0(1)

重要なイベントについて SNMP ネットワーク管理サーバに通知するには、SNMP 通知またはトラップを設定する必要があります。すべての SNMP 通知 / トラップをイネーブルにするか、または、イネーブルな機能に関連する特定の通知 / トラップをイネーブルにします。一部の通知 / トラップはデフォルトでイネーブルになっています。イネーブルになっているトラップを確認するには、**show snmp-server trap** コマンドを使用します。SNMP ホスト受信者の設定方法によって、SNMP 通知またはトラップが送信されます。

すべての通知 / トラップをイネーブルにする

```
n7000(config)# snmp-server enable traps
```

個々の通知 / トラップをイネーブルにする

```
n7000(config)# snmp-server enable traps feature-control
n7000(config)# snmp-server enable traps callhome smtp-send-fail
n7000(config)# snmp-server enable traps snmp authentication
```

インターフェイス リンク ステータス トラップ

導入：Cisco NX-OS Release 4.0(1)

SNMP インターフェイス リンク ステータス トラップは、デフォルトでイネーブルになっています。SNMP リンク ステータス トラップは、インターフェイスごとにディセーブルにできます。特定の環境では、インターフェイス トラップをディセーブルにすることは効果的です。ただし、重要なインフラストラクチャまたはサーバ インターフェイスでは、インターフェイス トラップをイネーブルにすることを常に推奨します。

```
n7000(config)# interface ethernet 1/1
n7000(config-if)# no snmp trap link-status
```

コミュニティ ストリングのアクセス コントロール リスト

導入：Cisco NX-OS Release 4.2(1)

特定の送信元 IP アドレスまたは宛先 IP アドレスへのアクセスを制限するには、Access Control List（ACL; アクセス コントロール リスト）をコミュニティ ストリング（SNMP v1 および v2c）に常に適用する必要があります。

```
n7000(config)# ip access-list snmp-acl
n7000(config-acl)# permit udp host x.x.x.x host x.x.x.x eq snmp

n7000(config)# snmp-server community <password> group network-operator
n7000(config)# snmp-server community <password> use-acl snmp-acl
```

送信元インターフェイス

導入：Cisco NX-OS Release 4.2(1)

管理 VRF インスタンスが使用中ではない場合、**通知**および**トラップ**の送信元インターフェイスを指定します。これによって、ファイアウォールなどのセキュリティ デバイスが、SNMP パケットの送信元を特定できます。送信元インターフェイスまたは IP アドレスが指定されない場合、元の（アウトバンド）インターフェイスのプライマリ IP アドレスが選択されます。**通知**機能は、SNMP v2c および v3 にのみ適用されます。すべての SNMP ホストにグローバルに、または、SNMP ホストごとに、送信元インターフェイスを設定できます。

グローバルに設定：

```
n7000(config)# snmp source-interface informs loopback0
n7000(config)# snmp source-interface traps loopback0
```

サーバごとに設定：

```
n7000(config)# snmp-server host a.a.a.a source-interface loopback0
```

SNMP のディセーブル化

導入：Cisco NX-OS Release 4.2(1)

SNMP はデフォルトでイネーブルになっています。ただし、コミュニティ ストリングが設定されていない場合、SNMP v1 および v2c は SNMP 要求には応答しません。SNMPv3 対応のサーバが Cisco Nexus 7000 シリーズ デバイスをポーリングする場合、SNMPv3 は SNMP 要求に応答します（SNMP ユーザ「admin」がデフォルトで設定されています）。SNMP が必須ではない場合、次のコマンドを使用してディセーブルにし、セキュリティを強化する必要があります。

```
n7000(config)# no snmp-server protocol enable
```

システム メッセージ ロギング

Cisco NX-OS ソフトウェアでは、DRAM にあるローカル ログ ファイル（log:messages）にシステム メッセージが保存されます（最新の 100 個の重大度 0、1、または 2 のメッセージは、NVRAM に保存されます）。Cisco NX-OS ソフトウェアでは、logflash: にもシステム メッセージが記録されます。logflash: は、システムのリロード後にも、一貫性のあるデータを提供します（logflash://sup-local/logs/messages）。

Syslog サーバ

導入：Cisco NX-OS Release 4.0(1)

最大 3 台の Syslog サーバを設定し、システム メッセージを受信できます。トラフィックを分離するために管理 VRF インスタンスを使用し、冗長性を保つ目的で少なくとも 2 台の Syslog サーバを設定することを推奨します。ログ メッセージの重大度は、サーバごとに指定できます。次に、重大度 5 を指定することによって、各サーバにメッセージ 0（Emergency）から 5（Notification）までを記録する例を示します。

```
n7000(config)# logging server a.a.a.a 5 use-vrf management
n7000(config)# logging server b.b.b.b 5 use-vrf management
```

送信元インターフェイス

導入：Cisco NX-OS Release 4.0(1)

デフォルト VRF インスタンスを使用して Syslog サーバに到達する場合、ループバック インターフェイスを送信元 IP アドレスとして指定できます。これによって、ファイアウォールなどのセキュリティ デバイスが、Syslog パケットの送信元を特定できます。送信元インターフェイスが指定されない場合、元の（アウトバンド）インターフェイスのプライマリ IP アドレスが選択されます。

```
n7000(config)# logging source-interface loopback 0
```

リンク ステータス イベント

導入：Cisco NX-OS Release 4.0(1)

すべてのインターフェイス リンク ステータス（Up/Down）メッセージが、デフォルトで記録されます。リンク ステータス イベントは、グローバルに、または、インターフェイスごとに、設定できます。次のグローバル コマンドによって、すべてのインターフェイスのリンク ステータス ロギング メッセージがディセーブルにされます。インターフェイス コマンドによって、特定のインターフェイスのリンク ステータス ロギング メッセージがイネーブルにされます。このシナリオは、ミッション クリティカルなインフラストラクチャまたはサーバ インターフェイスを除き、過度なメッセージをフィルタ処理する場合に便利です。

```
n7000(config)# no logging event link-status default

n7000(config)# interface ethernet x/x
n7000(config-if)# logging event port link-status
```

タイムスタンプ

導入：Cisco NX-OS Release 4.0(1)

システム メッセージ ロギングは、デフォルトで、1 秒単位で記録されます。より精度を高めるために、タイムスタンプをミリ秒単位およびマイクロ秒単位に設定できます。時間が重要な問題についてトラブルシューティングする場合は、ミリ秒単位またはマイクロ秒単位でタイムスタンプを使用することを推奨します。

```
n7000(config)# logging timestamp milliseconds
```

機能ごとの重大度レベル

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS ソフトウェアでは、機能ごとに設定された重大度レベルがサポートされます。ネットワークで管理可能なより高度なレベルが必要な機能については、重大度レベルを設定することを推奨します。次に、NTP の設定および確認のコマンドの例を示します。すべての機能の現在の重大度レベルを変更するには、**logging level all <severity #>** コマンドを使用できます。

```
n7000(config)# logging level ntp 7

n7000# show logging level ntp
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
ntp                     2                       7

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

n7000(config)# logging level all 5
```

ログ ファイルの内容の表示

導入：Cisco NX-OS Release 4.0(1)

次の **show logging** コマンドは、システム メッセージ ログ ファイルの表示および管理に役に立ちます。

```
n7000# show logging logfile  <-  Displays the contents of the default log file.

n7000# show logging last 10  <-  Displays the last # of lines of the default log file.

n7000# show logging NVRAM   <- Displays contents of the log file stored in NVRAM.

n7000# show file logflash://sup-local/log/messages <- Displays contents in logflash.
```

ログ ファイルの内容の削除

導入：Cisco NX-OS Release 4.0(1)

次の **clear** コマンドは、システム メッセージ ログ ファイルの内容を削除が必要な場合に、役に立ちます。

```
n7000# clear logging logfile  <- Clears the contents of the default log file.
```

```
n7000# clear logging nvram    <- Clears the contents of the default log file stored in
NVRAM.
```

Smart Call Home

Smart Call Home では、Network Operation Center（NOC）、特定のエンジニア、または Cisco TAC などの受信者に対して、標準的なテキスト電子メールまたは XML 通知を送信し、TAC ケースを自動生成する、自動的な方法が提供されます。問題の解決を早めるには、内部受信者と Cisco TAC 受信者の両方に対して Call Home をイネーブルにすることを推奨します。

内部受信者と Cisco TAC 受信者（宛先プロファイル）

導入：Cisco NX-OS Release 4.0(1)

Smart Call は Cisco NX-OS Release 4.0(1) で導入されましたが、次の例は Cisco NX-OS Release 5.0(2a) CLI の構文に基づいています。例：トラフィックを分離する管理 VRF インスタンスを使用して、冗長性の目的で 2 台の異なる電子メール サーバにフル テキスト電子メールを送信するよう、Call Home が設定されます。宛先プロファイル「Internal-NOC」では、プライオリティがより低いため、メール サーバ a.a.a.a が優先されます。応答がない場合は、メール サーバ b.b.b.b が使用されます。

```
n7000(config)# callhome

n7000(config-callhome)# contract-id Cisco-Contract-#
n7000(config-callhome)# customer-id xyz.com

n7000(config-callhome)# site-id n7000-Kirkland-DC
n7000(config-callhome)# streetaddress 12345 Street NE, Kirkland, WA
n7000(config-callhome)# email-contact Cisco-Customer@xyz.com
n7000(config-callhome)# phone-contact +1-800-123-4567

n7000(config-callhome)# destination-profile Internal-NOC
n7000(config-callhome)# destination-profile Internal-NOC format full-txt
n7000(config-callhome)# destination-profile Internal-NOC email-addr call-home-noc@xyz.com
n7000(config-callhome)# destination-profile Internal-NOC alert-group all

n7000(config-callhome)# destination-profile CiscoTAC-1 email-addr callhome@cisco.com

n7000(config-callhome)# transport email mail-server a.a.a.a priority 10 use-vrf management
n7000(config-callhome)# transport email mail-server b.b.b.b use-vrf management

n7000(config-callhome)# transport email from call-home@xyz.com
n7000(config-callhome)# transport email reply-to call-home@xy.com
```

（注）　**transport email snmp-server** コマンドは、Cisco NX-OS Release 4.x および NX-OS Release 5.x ソフトウェアでサポートされている元のコマンドです。複数のサーバおよびプライオリティへのサポートを追加するため、NX-OS Release 5.0(2a) で **transport email mail-server** コマンドが導入されました。

Call Home 受信者のテスト

導入：Cisco NX-OS Release 4.0(1)

Call Home の初期設定時に Call Home 受信者についてテストし、Call Home が想定どおりに動作することを確認します。

```
n7000# callhome test
```