Cisco Nexus 1000V トラブルシューティング ガイド リリース 4.2(1)SV1(5.1)

2012 年 1 月 31 日

Text Part Number: OL-25387-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Nexus 1000V トラブルシューティング ガイド リリース 4.2(1)SV1(5.1)
© 2010-2012 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2012, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

新機能および変更された機能に関する情報 xi

はじめに xiii

対象読者 xiii

マニュアルの構成 xiii

ドキュメントの表記法 xiv

関連資料 xv

マニュアルの入手方法およびテクニカル サポート xvii

CHAPTER 1

トラブルシューティングの概要 1-1

トラブルシューティング プロセスの概要 1-1

ベスト プラクティスの概要 1-1

トラブルシューティングの基本 1-2

トラブルシューティングのガイドライン 1-2

情報の収集 1-3

ポートの確認 1-3

レイヤ 2 接続の確認 1-3

レイヤ 3 接続の確認 1-4

現象の概要 1-4

システム メッセージ 1-5

システム メッセージ テキスト 1-5

Syslog サーバの実装 1-5

ログによるトラブルシューティング 1-7

ログの表示 1-7

シスコのサポート コミュニティ 1-7

シスコまたは VMware のカスタマー サポートへの連絡 1-8

CHAPTER 2

トラブルシューティングで使用されるツール 2-1

コマンド 2-1

ping 2-2

traceroute 2-2

プロセスおよび CPU のモニタリング 2-2

実行中のプロセスおよびその状態の識別 2-2

CPU 使用率の表示 2-3

CPU およびメモリ情報の表示 2-4
RADIUS 2-5
Syslog 2-5
ログ レベル 2-6
Telnet または SSH へのロギングのイネーブル化 2-6

CHAPTER 3 インストール 3-1
インストールに関する問題の分離 3-1
VMware のライセンス バージョンの確認 3-2
分散仮想スイッチからホストを認識できない場合 3-3
vCenter Server 接続のリフレッシュ 3-4
パフォーマンスの向上 3-4
ドメイン設定の確認 3-4
VSM VM 仮想インターフェイスに対するポート グループ（PG）の割り当ての確認 3-5
VSM と vCenter Server の接続の確認 3-5
vCenter Server への接続のトラブルシューティング 3-6
ネットワーク管理者パスワードの回復 3-7
拡張キーの管理 3-7
拡張に関する既知の問題と解決方法 3-7
プラグインの競合の解決 3-7
Cisco Nexus 1000V での拡張キーの確認 3-8
特定の DVS に結び付けられた拡張キーの確認 3-9
拡張キーの確認 3-10
Cisco Nexus 1000V インストールの再作成 3-11
Cisco Nexus 1000V DVS からのホストの削除 3-12
vCenter Server からの Cisco Nexus 1000V の削除 3-12
vCenter Server の拡張キーの登録解除 3-13

CHAPTER 4 ライセンス 4-1
ライセンスに関する情報 4-1
ライセンス ファイルの内容 4-2
ライセンスのトラブルシューティングに関する前提条件 4-2
ライセンスに関する問題 4-3
ライセンスのトラブルシューティング コマンド 4-4

CHAPTER 5 アップグレード 5-1
アップグレードの概要 5-1
In Service Software Upgrade の問題 5-1

VEM のアップグレードの問題 5-5
GUI のアップグレードの問題 5-7
プライマリがアクティブな場合のセカンダリ VSM の回復 5-8
VSM アップグレードの停止 5-9
ブート変数の変更 5-10
VSM の電源投入 5-12
HA ロールの変更 5-12
セカンダリがアクティブな場合のプライマリ VSM の回復 5-13
ポート グループの接続解除 5-14
VSM の電源オフ 5-15
ポート グループの接続 5-16
アップグレードのトラブルシューティング コマンド 5-18

CHAPTER 6
ハイ アベイラビリティ 6-1
ハイ アベイラビリティについて 6-1
システムレベルのハイ アベイラビリティ 6-2
シングルまたはデュアル スーパーバイザ 6-2
ネットワークレベル ハイ アベイラビリティ 6-2
ハイ アベイラビリティでの問題 6-3
ハイ アベイラビリティのトラブルシューティング コマンド 6-5

CHAPTER 7
VSM および VEM モジュール 7-1
モジュールについて 7-1
VSM にモジュールが表示されない場合のトラブルシューティング 7-1
モジュールのトラブルシューティングに関する注意事項 7-2
モジュールのトラブルシューティングのフローチャート 7-3
VSM の問題 7-4
VSM が vCenter Server に接続されているかどうかの確認 7-6
VSM が正しく設定されているかどうかの確認 7-7
ドメイン設定の確認 7-7
システム ポート プロファイル設定の確認 7-8
コントロールおよびパケット VLAN の設定の確認 7-8
vCenter Server 設定の確認 7-9
VSM と VEM の間のネットワーク接続の確認 7-9
VEM 設定の確認 7-11
ログの収集 7-14
VSM および VEM のトラブルシューティング コマンド 7-15

CHAPTER 8 ポート 8-1
ポートの概要 8-1
インターフェイスの特性の概要 8-1
インターフェイス カウンタの概要 8-2
リンク フラッピングの概要 8-2
ポート セキュリティの概要 8-2
ポート診断チェックリスト 8-3
ポートの問題 8-3
インターフェイスをイネーブルにできない 8-4
ポートのリンク障害またはポートの非接続 8-4
リンク フラッピング 8-5
ポート errdisable 8-5
VM から保護されたポートに ping できない 8-6
ポート セキュリティ違反 8-7
ポートのトラブルシューティング コマンド 8-8

CHAPTER 9 ポート プロファイル 9-1
ポート プロファイルについて 9-1
ポート プロファイルの問題 9-2
検疫されたオフライン インターフェイスの回復 9-5
ポート プロファイルのログ 9-6
ポート プロファイルのトラブルシューティング コマンド 9-6

CHAPTER 10 ポート チャネルおよびトランキング 10-1
概要 10-1
ポート チャネルの概要 10-1
ポート チャネルの制限 10-2
トランキングの概要 10-2
トラブルシューティングの初期チェックリスト 10-2
非対称ポート チャネル（APC）のトラブルシューティング 10-3
ポート チャネルが作成できない 10-4
新しく追加したインターフェイスがポート チャネル内でオンラインにならない 10-4
ポート チャネルの特性をインターフェイスに強制する 10-5
ポート チャネルの設定の確認 10-5
VLAN トラフィックがトランクを通過しない 10-6

CHAPTER 11 レイヤ 2 スイッチング 11-1
レイヤ 2 イーサネット スイッチングについて 11-1

ポート モデル 11-1
VEM から見たポート 11-2
VSM から見たポート 11-3
ポート タイプ 11-4
レイヤ 2 スイッチングの問題 11-4
VEM ポート間の接続の確認 11-4
VEM 間の接続の確認 11-5
トラフィック中断の特定 11-6
レイヤ 2 スイッチングの確認 11-7
Microsoft NLB ユニキャスト モードのトラブルシューティング 11-12
制限事項と制約事項 11-12
vEthernet 上での自動スタティック MAC 学習のディセーブル化 11-12
VSM のステータスの確認 11-13
VEM のステータスの確認 11-13

CHAPTER 12 **VLAN** 12-1
VLAN について 12-1
トラブルシューティングの初期チェックリスト 12-2
VLAN を作成できない 12-3

CHAPTER 13 **プライベート VLAN** 13-1
プライベート VLAN について 13-1
プライベート VLAN ドメイン 13-1
複数のスイッチのスパニング 13-1
プライベート VLAN ポート 13-2
トラブルシューティングのガイドライン 13-2
プライベート VLAN トラブルシューティング コマンド 13-2

CHAPTER 14 **NetFlow** 14-1
NetFlow 情報 14-1
NetFlow トラブルシューティング コマンド 14-2
NetFlow の一般的な問題 14-3
ポリシー検証エラーのデバッグ 14-3
統計情報エクスポートのデバッグ 14-4

CHAPTER 15 **ACL** 15-1
アクセス コントロール リスト（ACL）について 15-1
ACL 設定の制限事項 15-2

ACL の制限事項 15-2
ACL のトラブルシューティング 15-2
VEM での ACL ポリシーの表示 15-3
ポリシー検証に関する問題のデバッグ 15-3

CHAPTER 16 **Quality of Service** 16-1
QoS について 16-1
QoS 設定の制限事項 16-2
QoS トラブルシューティング コマンド 16-2
VEM のトラブルシューティング 16-3
ポリシング検証エラーのデバッグ 16-4

CHAPTER 17 **SPAN** 17-1
SPAN に関する情報 17-1
SPAN セッションのガイドライン 17-1
SPAN の問題 17-2
SPAN のトラブルシューティング コマンド 17-3

CHAPTER 18 **マルチキャスト IGMP** 18-1
マルチキャストに関する情報 18-1
マルチキャスト IGMP スヌーピング 18-1
マルチキャスト IGMP スヌーピングの問題 18-2
トラブルシューティングのガイドライン 18-2
トラブルシューティング コマンド 18-3
現象、原因、および解決方法 18-5

CHAPTER 19 **DHCP、DAI、および IPSG** 19-1
DHCP スヌーピングの概要 19-1
ダイナミック ARP インスペクションに関する情報 19-2
IP ソース ガードの概要 19-2
トラブルシューティングの注意事項と制約事項 19-2
DHCP スヌーピングの問題 19-3
ドロップされた ARP 応答のトラブルシューティング 19-4
IP ソース ガードの問題 19-5
ログの収集と評価 19-5
VSM ロギング 19-5
ホスト ロギング 19-6

DHCP、DAI、および IPSG のトラブルシューティング コマンド 19-6

CHAPTER 20 仮想サービス ドメイン 20-1
仮想サービス ドメインの概要 20-1
仮想サービス ドメインの問題 20-1
ログの収集と評価 20-2
仮想サービス ドメインのトラブルシューティング コマンド 20-3

CHAPTER 21 システム 21-1
システムについて 21-1
vCenter Server の基本的な制限事項 21-2
拡張キー 21-2
DVS の回復 21-2
VSM のコピーが保存されている場合の DVS の回復 21-3
VSM のコピーが保存されていない場合の DVS の回復 21-4
VSM と vCenter Server 接続に関連した問題 21-5
ESX の再起動後の接続の失敗 21-6
システム MTU の設定 21-7
MTU の不一致によって失われた接続の回復 21-8
VSM の作成 21-9
ポート プロファイル 21-9
ポート プロファイルの問題 21-10
ホストでの問題 21-10
VM トラフィックでの問題 21-11
VEM トラブルシューティング コマンド 21-11
VEM ログ コマンド 21-12
エラー メッセージ 21-12

CHAPTER 22 Network Segmentation Manager 22-1
Network Segmentation Manager に関する情報 22-1
Network Segmentation Manager の問題 22-2
Network Segmentation Manager のトラブルシューティング コマンド 22-7

CHAPTER 23 VXLAN 23-1
VXLAN に関する情報 23-1
概要 23-1
VXLAN の VEM L3 IP インターフェイス 23-2

フラグメンテーション 23-2
スケーラビリティ 23-3
VXLAN の最大数 23-3
サポートされる機能 23-3
ジャンボ フレーム 23-3
VXLAN 機能のグローバルなディセーブル化 23-3
VXLAN のトラブルシューティング コマンド 23-3
VSM コマンド 23-3
VEM コマンド 23-5
VEM パケット パスのデバッグ 23-6
VEM マルチキャストのデバッグ 23-7
VXLAN Datapath のデバッグ 23-7
Vemlog デバッグ 23-7
HR 23-8
Vempkt 23-8
統計情報 23-8
show コマンド 23-9

CHAPTER 24 テクニカル サポートへ問い合わせる前の準備 24-1
シスコのサポート コミュニティ 24-1
テクニカル サポートへ問い合わせるための情報の収集 24-1
コア メモリ情報のファイルの取得 24-3
ファイルのコピー 24-3

INDEX

新機能および変更された機能に関する情報

このセクションでは、このマニュアルの各リリースで新たに追加または変更された情報について説明します。

新機能またはコマンドの変更の詳細については、次のものを参照してください。

- リリース ノート
- コマンド リファレンス

機能	説明	対象リリース	参照先
NSM	Network Segmentation Manager（NSM）のトラブルシューティングに関する章が新たに追加されました。	4.2(1)SV1(5.1)	「Network Segmentation Manager」
VXLAN	Virtual Extensible Local Area Network（VXLAN）のトラブルシューティングに関する章が新たに追加されました。	4.2(1)SV1(5.1)	「VXLAN」
ユニキャスト NLB	Microsoft Network Load Balancing ユニキャスト モードのトラブルシューティングに関する項が新たに追加されました。	4.2(1)SV1(5.1)	「レイヤ 2 スイッチング」
In Service Software Upgrade（ISSU）	ISSU のトラブルシューティングに関する項が新たに追加されました。	4.2(1)SV1(4a)	「アップグレード」
VEM ソフトウェア アップグレード	VEM ソフトウェア アップグレードのトラブルシューティングに関する項が新たに追加されました。	4.2(1)SV1(4a)	「アップグレード」
DHCP、DAI、IPSG	DHCP、ダイナミック ARP インスペクション、および IP ソース ガードのトラブルシューティングに関する項が新たに追加されました。	4.2(1)SV1(4)	「DHCP、DAI、および IPSG」
仮想サービス ドメイン	仮想サービス ドメインのトラブルシューティングに関する項が新たに追加されました。	4.2(1)SV1(4)	「仮想サービス ドメイン」
ポート プロファイル	ポート プロファイルに関する項と、検疫ポート プロファイルに関する情報が新たに追加されました。	4.2(1)SV1(4)	「ポート プロファイル」
アップグレード	アップグレードの問題に関する項が新たに追加されました。	4.2(1)SV1(4)	「アップグレード」

機能	説明	対象リリース	参照先
VEM ヘルス チェック	VEM ヘルス チェックでは、接続問題の原因と、トラブルシューティングで推奨される次のステップが示されます。	4.0(4)SV1(3)	「VSM と VEM の間のネットワーク接続の確認」（P.9）
ESX の再起動後の VSM 接続の失敗	このセクションでは、ESX の再起動後に MTU 不一致に関連して接続が失われるのを防ぐ方法について説明します。	4.0(4)SV1(3)	「ESX の再起動後の接続の失敗」

はじめに

トラブルシューティング マニュアルでは、問題を認識し、原因を判別し、考えられる解決策を見つける方法について説明します。

この「はじめに」では、このマニュアルの次の点について説明します。

- 「対象読者」（P.xiii）
- 「マニュアルの構成」（P.xiii）
- 「ドキュメントの表記法」（P.xiv）
- 「関連資料」（P.xv）
- 「マニュアルの入手方法およびテクニカル サポート」（P.xvii）

対象読者

このマニュアルは、Cisco Nexus 1000V の設定およびメンテナンスを担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

タイトル	説明
第 1 章「トラブルシューティングの概要」	基本的なトラブルシューティングの方法について説明します。
第 2 章「トラブルシューティングで使用されるツール」	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。
第 3 章「インストール」	インストールに関する問題のトラブルシューティングの方法について説明します。
第 4 章「ライセンス」	Cisco Nexus 1000V のライセンスに関連する問題を識別して解決する方法について説明します。
第 5 章「アップグレード」	アップグレードに関する問題のトラブルシューティングの方法について説明します。
第 6 章「ハイ アベイラビリティ」	ハイ アベイラビリティ（HA）に関する問題を識別して解決する方法について説明します。

タイトル	説明
第 7 章「VSM および VEM モジュール」	モジュールに関する問題を識別して解決する方法について説明します。
第 8 章「ポート」	ポートに関する問題を識別して解決する方法について説明します。
第 9 章「ポート プロファイル」	ポート プロファイルに関する問題を識別して解決する方法について説明します。
第 10 章「ポート チャネルおよびトランキング」	ポート チャネルとトランクに関する問題を識別して解決する方法について説明します。
第 11 章「レイヤ 2 スイッチング」	レイヤ 2 スイッチングに関する問題を識別して解決する方法について説明します。
第 12 章「VLAN」	VLAN に関する問題を識別して解決する方法について説明します。
第 13 章「プライベート VLAN」	プライベート VLAN に関する問題を識別して解決する方法について説明します。
第 14 章「NetFlow」	NetFlow に関する問題を識別して解決する方法について説明します。
第 15 章「ACL」	Access Control List（ACL; アクセス コントロール リスト）に関する問題を識別して解決する方法について説明します。
第 16 章「Quality of Service」	Quality of Service（QoS）に関連する問題を識別して解決する方法について説明します。
第 17 章「SPAN」	Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）に関する問題を識別して解決する方法について説明します。
第 18 章「マルチキャスト IGMP」	マルチキャストに関する問題を識別して解決する方法について説明します。
第 19 章「DHCP、DAI、および IPSG」	DHCP スヌーピング、ダイナミック ARP インスペクション、および IP ソース ガードに関する問題を識別して解決する方法について説明します。
第 20 章「仮想サービス ドメイン」	Virtual Service Domain（VSD; 仮想サービス ドメイン）に関する問題を識別して解決する方法について説明します。
第 21 章「システム」	VMware に関する問題を識別して解決する方法について説明します。
第 24 章「テクニカル サポートへ問い合わせる前の準備」	テクニカルサポートを要求する前に従う手順について説明します

ドキュメントの表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。

[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

`screen` フォント	スイッチに表示される端末セッションおよび情報は、screen フォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の `screen` フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」の意味です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

この項では、Cisco Nexus 1000V とともに使用されるマニュアルの一覧を示します。これらのマニュアルは、Cisco.com の次に示す URL で入手できます。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

一般情報

『Cisco Nexus 1000V Documentation Roadmap, Release 4.2(1)SV1(5.1)』

『Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.1)』

『Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)』

『Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(3)』

インストール & アップグレード

『Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)』

『Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide』

『*Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(3)*』

コンフィギュレーション ガイド

『*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(3)*』

プログラミング

『*Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SV1(5.1)*』

リファレンス

『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V MIB Quick Reference*』

『*Cisco Nexus 1010 Command Reference, Release 4.2(1)SP1(3)*』

トラブルシューティング & アラート

『*Cisco Nexus 1000V トラブルシューティング ガイド リリース 4.2(1)SV1(5.1)*』

『*Cisco Nexus 1000V Password Recovery Guide*』

『*Cisco NX-OS System Messages Reference*』

Virtual Security Gateway マニュアル

Cisco Virtual Security Gateway for Nexus 1000V Series Switch

Virtual Network Management Center

Cisco Virtual Network Management Center

ネットワーク解析モジュール マニュアル

『*Cisco Prime Network Analysis Module Software Documentation Guide, 5.1*』

『*Cisco Prime Network Analysis Module (NAM) for Nexus 1010 Installation and Configuration Guide, 5.1*』

『*Cisco Prime Network Analysis Module Command Reference Guide 5.1*』

『*Cisco Prime Network Analysis Module Software 5.1 Release Notes*』

『*Cisco Prime Network Analysis Module Software 5.1 User Guide*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は Really Simple Syndication（RSS）フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

トラブルシューティングの概要

この章では、Cisco Nexus 1000V の設定または使用時に発生する可能性のある問題のトラブルシューティングについて、基本的な概念、方法、および一般的なガイドラインを紹介します。

この章は、次の内容で構成されています。

- 「トラブルシューティング プロセスの概要」（P.1-1）
- 「ベスト プラクティスの概要」（P.1-1）
- 「トラブルシューティングの基本」（P.1-2）
- 「現象の概要」（P.1-4）
- 「システム メッセージ」（P.1-5）
- 「ログによるトラブルシューティング」（P.1-7）
- 「シスコのサポート コミュニティ」（P.1-7）
- 「シスコまたは VMware のカスタマー サポートへの連絡」（P.1-8）

トラブルシューティング プロセスの概要

ネットワークに関するトラブルシューティングの一般的な手順は、次のとおりです。

ステップ 1 特定の現象に関する情報を収集します。

ステップ 2 現象の原因となり得る潜在的な問題をすべて識別します。

ステップ 3 現象が見られなくなるまで、潜在的な問題を系統的に 1 つずつ（最も可能性の高いものから低いものの順に）排除していきます。

ベスト プラクティスの概要

ベスト プラクティスとは、ネットワークが正常に動作していることを確認するために従う、推奨される手順です。次の一般的なベスト プラクティスは、ほとんどのネットワークに推奨されます。

- すべてのネットワーク デバイスで、Cisco Nexus 1000V リリースの一貫性を保持します。
- Cisco Nexus 1000V リリースのリリース ノートを参照して、最新の機能、制限事項、および注意事項を確認します。

- システム メッセージ ロギングをイネーブルにします。「現象の概要」（P.1-4）を参照してください。
- 変更を実装したら、新しい設定変更を確認してトラブルシューティングを実施します。

トラブルシューティングの基本

ここでは、Cisco Nexus 1000V または接続されているデバイスに関する問題のトラブルシューティングを実施する際に寄せられる質問を紹介します。これらの質問への回答に従って、問題の範囲を識別し、一連の処置を計画します。

ここでは、次の内容について説明します。

- 「トラブルシューティングのガイドライン」（P.1-2）
- 「情報の収集」（P.1-3）
- 「ポートの確認」（P.1-3）
- 「レイヤ 2 接続の確認」（P.1-3）
- 「レイヤ 3 接続の確認」（P.1-4）

トラブルシューティングのガイドライン

次の質問に回答することにより、従う必要がある手順および詳細に調査する必要があるコンポーネントを決定できます。

次の質問に回答することにより、インストールのステータスを判別します。

- 新たにインストールしたシステムであるか、既存のシステムであるかを確認します（新規のホスト、スイッチ、または Virtual Local Area Network（VLAN; バーチャル LAN）である可能性があります）。
- これまでにホストがネットワークを認識していたかどうかを確認します。
- 既存のアプリケーションの問題（遅い、遅延が長い、応答時間が極端に長い）を解決しようとしているのか、最近出現した問題であるかを確認します。
- アプリケーションで問題が発生する直前に、設定またはインフラストラクチャ全体にどのような変更を加えたかを確認します。

ネットワークの問題を検出するには、次の一般的なネットワーク トラブルシューティング手順に従います。

ステップ 1　システムにおける問題に関する情報を収集します。「情報の収集」（P.1-3）を参照してください。

ステップ 2　レイヤ 2 接続を確認します。「レイヤ 2 接続の確認」（P.1-3）を参照してください。

ステップ 3　エンド デバイス（ストレージ サブシステムおよびサーバ）の設定を確認します。

ステップ 4　エンドツーエンド接続を確認します。「レイヤ 3 接続の確認」（P.1-4）を参照してください。

情報の収集

ここでは、ネットワークにおける問題のトラブルシューティングで一般的に使用されるツールについて説明します。これらのツールは、特定の問題のトラブルシューティングに使用する可能性があるツールの一部です。

各章には、その章に関連する現象および考えられる問題に個別に対応するツールおよびコマンドが掲載されています。

問題領域を絞り込むためには、ネットワークの正確なトポロジを把握している必要もあります。

次のコマンドを実行して、出力を調べます。

- **show module**
- **show version**
- **show running-config**
- **show logging log**
- **show interfaces brief**
- **show vlan**
- **show accounting log**
- **show tech support svs**

（注）　**internal** キーワードを指定してコマンドを実行するには、ネットワーク管理者ロールを使用してログインする必要があります。

ポートの確認

ポートを確認するには、次の質問に回答します。

- 正しいメディア（銅線、光）およびファイバ タイプを使用していることを確認します。
- メディアが故障または破損していないことを確認します。
- 仮想イーサネットポートを検査していることを確認します。検査している場合は、**show interface brief** コマンドを使用します。ステータスが up である必要があります。
- 物理イーサネットポートを検査していることを確認します。検査している場合は、サーバを調べるか、アップストリーム スイッチを調べる必要があります。
- Virtual Supervisor Module（VSM; 仮想スーパーバイザ モジュール）Virtual Machine（VM; 仮想マシン）のネットワーク アダプタに正しいポート グループが割り当てられているかどうか、およびそれらがすべて vSphere Client に接続されているかどうかを調べます。

レイヤ 2 接続の確認

レイヤ 2 接続を確認するには、次の質問に回答します。

- 必要なインターフェイスが同一の VLAN 内に存在することを確認します。
- 速度、デュプレックス、トランクの各モードについて、ポート チャネル内のすべてのポートの設定が同じであることを確認します。

show vlan brief コマンドを使用します。ステータスが up である必要があります。

ポートのプロファイル設定を調べるには、**show port-profile** コマンドを使用します。

仮想イーサネット ポートまたは物理イーサネット ポートのステータスを調べるには、**show interface-brief** コマンドを使用します。

レイヤ 3 接続の確認

レイヤ 3 接続を確認するには、次の質問に回答します。

- ラスト リゾート ゲートウェイを設定したことを確認します。
- IP アクセス リスト、フィルタ、ルート マップによって、ルート アップデートがブロックされていないことを確認します。

接続を確認するには、**ping** コマンドまたは **trace** コマンドを使用します。詳細については、次のセクションを参照してください。

- 「ping」（P.2-2）
- 「traceroute」（P.2-2）

現象の概要

現象に基づいたトラブルシューティング手法では、問題を診断して解決するための複数の方法が提供されます。このマニュアルは、解決方法へのリンクを含む複数のエントリ ポイントを使用することにより、さまざまな指標によって認識される同一の問題を持つ可能性があるユーザに役立つように設計されています。必要な情報に効率的にアクセスするためのエントリ ポイントとして、この PDF 形式のマニュアルを検索する、インデックスを使用する、または各章に記載されている現象と診断の説明に従います。

最小限のネットワークの中断で問題を解決するには、記載されている観察可能なネットワークの現象に基づいて、ソフトウェアの設定の問題や操作不可能なハードウェア コンポーネントを診断して修正できることが重要です。次に、問題と対処方法を示します。

- 主要な Cisco Nexus 1000V トラブルシューティング ツールを特定します。
- CLI で Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）または Ethanalyzer を使用し、プロトコル トレースを取得して分析します。
- 物理ポートの問題を識別または除外します。
- スイッチ モジュールの問題を識別または除外します。
- レイヤ 2 の問題を診断および修正します。
- レイヤ 3 の問題を診断および修正します。
- Technical Assistance Center（TAC）で使用されるコア ダンプおよびその他の診断データを取得します。
- スイッチをアップグレードの障害から復旧します。

システム メッセージ

システム ソフトウェアは、動作中に、Syslog（システム）メッセージをコンソール（およびオプションとして別のシステム上にあるログ収集サーバ）に送信します。ただし、すべてのメッセージがシステムの問題を表すとは限りません。一部のメッセージは単に情報を示すだけですが、リンク、内蔵ハードウェア、またはシステム ソフトウェアに関する問題の診断に役立つメッセージもあります。

ここでは、次の項目について説明します。

- 「システム メッセージ テキスト」（P.1-5）
- 「Syslog サーバの実装」（P.1-5）

システム メッセージ テキスト

メッセージ テキストは、状態を説明するテキスト ストリングです。メッセージのこの部分には、イベントについての詳細な情報が含まれている場合があります。含まれる情報は、端末ポート番号、ネットワーク アドレス、またはシステム メモリのアドレス空間内での位置に対応するアドレスです。この可変フィールドの情報はメッセージごとに異なるので、ここでは角カッコで囲んだ短い文字列で示します。たとえば 10 進数は [dec] で表します。

```
2009 Apr 29 12:35:51 n1000v %KERN-1-SYSTEM_MSG: stun_set_domain_id : Setting domain ID
(1024) - kernel
```

この文字列を使用して、『*Cisco NX-OS System Messages Reference System Messages Reference*』で一致するシステム メッセージを検索してください。

各システム メッセージのあとには、説明と推奨処置が記載されています。この処置は「No action required」のような簡単なものであることもありますが、次の例のように、修正方法に関するものやテクニカル サポートへの連絡を推奨するものもあります。

エラー メッセージ　`2009 Apr 29 14:57:23 n1000v %MODULE-5-MOD_OK: Module 3 is online (serial: )`

説明　VEM モジュールがスロット 3 に正常に挿入されました。

推奨処置　なし。これは、通知のメッセージです。スロット 3 にあるモジュールを確認するには「show module」を使用してください。

Syslog サーバの実装

Syslog ファシリティを使用して、Cisco Nexus 1000V デバイスからメッセージ ログのコピーをホストに送信すると、ログ用により多くの永続的ストレージを確保できます。この方法は、長期間にわたってログを調べる必要がある場合や、Cisco Nexus 1000V デバイスにアクセスできない場合に役立つ可能性があります。

次に、Solaris プラットフォーム上で Syslog ファシリティを使用するように Cisco Nexus 1000V デバイスを設定する例を示します。ここでは Solaris ホストを使用しますが、すべての UNIX および Linux システムにおける Syslog の設定は非常によく似ています。

Syslog では、ファシリティの概念を使用して、Syslog サーバ上での処理方法とメッセージの重大度が決定されます。このため、Syslog サーバでは、異なるメッセージの重大度を異なる方法で処理できます。たとえば、メッセージを別々のファイルに記録することや、特定のユーザに電子メールで送信することもできます。重大度を指定すると、そのレベル以上の重大度（より低い数値）のすべてのメッセージに対して処理が行われます。

（注）Cisco Nexus 1000V メッセージは、他社の Syslog メッセージと競合しないように、標準 Syslog ファイルとは別のファイルに記録される必要があります。/ ファイル システムがログ メッセージでいっぱいになることを防ぐため、ログファイルは / ファイル システムに配置しないでください。
Syslog クライアント：switch1
Syslog サーバ：172.22.36.211（Solaris）
Syslog ファシリティ：local1
Syslog の重大度：通知（レベル 5、デフォルト）
Cisco Nexus 1000V メッセージを記録するログ ファイル：/var/adm/nxos_logs

Syslog サーバを設定するには、次の手順に従います。

ステップ 1　Cisco Nexus 1000V を設定します。

```
n1000v# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# logging server 192.0.2.1 6 facility local1
```

設定を表示するには、次のように入力します。

```
n1000v# show logging server
Logging server: enabled
{192.0.2.1}
     server severity: notifications
     server facility: local1
```

ステップ 2　Syslog サーバを設定します。

a. local1 のメッセージを処理するように、/etc/syslog.conf を変更します。Solaris の場合は、facility.severity と処置（/var/adm/nxos_logs）の間に少なくとも 1 つのタブが必要です。

```
#Below is for the NX-OS logging
local1.notice /var/adm/nxos_logs
```

b. ログ ファイルを作成します。

```
#touch /var/adm/nxos_logs
```

c. Syslog を再起動します。

```
# /etc/init.d/syslog stop
# /etc/init.d/syslog start
syslog service starting.
```

d. Syslog が再起動されたことを確認します。

```
# ps -ef |grep syslogd
     root 23508 1 0 11:01:41 ? 0:00 /usr/sbin/syslogd
```

ステップ 3　Cisco Nexus 1000V でイベントを作成して、Syslog サーバをテストします。この場合、ポート e1/2 はバウンスされ、Syslog サーバ上で次のように表示されます。スイッチの IP アドレスは角カッコで囲まれています。

```
# tail -f /var/adm/nxos_logs
Sep 17 11:07:41 [172.22.36.142.2.2] : 2004 Sep 17 11:17:29 pacific:
%PORT-5-IF_DOWN_INITIALIZING: %$VLAN 1%$ Interface e 1/2 is down (Initializing)
```

```
Sep 17 11:07:49 [172.22.36.142.2.2] : 2004 Sep 17 11:17:36 pacific: %PORT-5-IF_UP:
%$VLAN 1%$ Interface e 1/2 is up in mode access
Sep 17 11:07:51 [172.22.36.142.2.2] : 2004 Sep 17 11:17:39 pacific:
%VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
(dhcp-171-71-49-125.cisco.com)
```

ログによるトラブルシューティング

Cisco Nexus 1000V では、スイッチ上でさまざまなタイプのシステム メッセージを生成して、Syslog サーバに送信します。これらのメッセージを確認することにより、現在発生している問題の原因となった可能性のあるイベントを判別できます。

ログの表示

Cisco Nexus 1000V のログにアクセスして表示するには、次のコマンドを使用します。

```
n1000v# show logging ?

console        Show console logging configuration
info           Show logging configuration
internal       syslog syslog internal information
last           Show last few lines of logfile
level          Show facility logging configuration
logfile        Show contents of logfile
loopback       Show logging loopback configuration
module         Show module logging configuration
monitor        Show monitor logging configuration
nvram          Show NVRAM log
pending        server address pending configuration
pending-diff   server address pending configuration diff
server         Show server logging configuration
session        Show logging session status
status         Show logging status
timestamp      Show logging timestamp configuration
|              Pipe command output to filter
```

例 1-1 に、**show logging** コマンドの出力例を示します。

例 1-1　show logging コマンド

```
n1000v# show logging server
Logging server: enabled
{192.0.1.1}
server severity: critical
server facility: user
```

シスコのサポート コミュニティ

詳細については、次のいずれかのサポート コミュニティにアクセスしてください。

- Cisco Support Community for Server Networking
- Cisco Communities : Nexus 1000V

シスコまたは VMware のカスタマー サポートへの連絡

このマニュアルのトラブルシューティング情報を使用しても問題を解決できない場合には、カスタマーサービス担当者に連絡して、支援および詳細な指示を受けてください。担当者ができる限りすばやいサポートを行えるように、連絡する前に次の情報を用意してください。

- 実行している Nexus 1000V ソフトウェアのバージョン
- 実行している ESX Server および vCenter Server ソフトウェアのバージョン
- 連絡先電話番号
- 問題点の要約
- 問題を特定し、解決するためにすでに実施した手順の簡単な説明

Cisco Nexus 1000V およびサポート契約をシスコから購入された場合は、シスコに Nexus 1000V のサポートをご依頼ください。シスコは、L1、L2、および L3 のサポートを提供します。

Cisco Nexus 1000V および SNS を VMware から購入された場合は、VMware に Nexus 1000V のサポートをご依頼ください。VMware は、L1 および L2 のサポートを提供します。シスコは、L3 のサポートを提供します。

これらの情報を収集してから、「関連資料」（P.xv）を参照してください。

テクニカル サポートへ問い合わせる前に実施する手順の詳細については、「テクニカル サポートへ問い合わせるための情報の収集」（P.24-1）を参照してください。

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）。
- 1Sec = 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  1Sec   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ャ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。

CHAPTER 3

インストール

この章では、インストールに関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「インストールに関する問題の分離」（P.3-1）
- 「パフォーマンスの向上」（P.3-4）
- 「ドメイン設定の確認」（P.3-4）
- 「VSM VM 仮想インターフェイスに対するポート グループ（PG）の割り当ての確認」（P.3-5）
- 「VSM と vCenter Server の接続の確認」（P.3-5）
- 「vCenter Server への接続のトラブルシューティング」（P.3-6）
- 「ネットワーク管理者パスワードの回復」（P.3-7）
- 「拡張キーの管理」（P.3-7）
- 「Cisco Nexus 1000V インストールの再作成」（P.3-11）

インストールに関する問題の分離

ここでは、インストールに関する問題を分離する方法について説明します。次のトピックについて取り上げます。

- 「VMware のライセンス バージョンの確認」（P.3-2）
- 「分散仮想スイッチからホストを認識できない場合」（P.3-3）
- 「vCenter Server 接続のリフレッシュ」（P.3-4）

VMware のライセンス バージョンの確認

インストールに関する問題のトラブルシューティングを開始する前に、次の手順に従って、使用している ESX Server に VMware Enterprise Plus がライセンスされていることを確認します。このライセンスには、Distributed Virtual Switch（DVS; 分散仮想スイッチ）機能が含まれます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

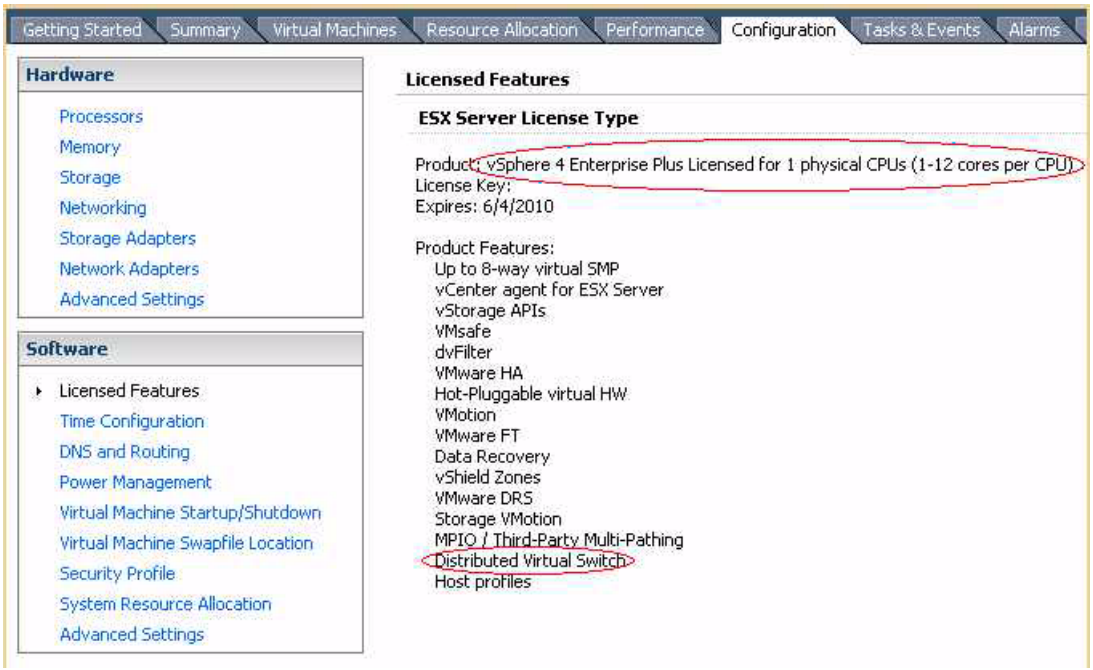
- ESX Server 上で vSphere Client にログインしていること。
- Cisco Nexus 1000V のコマンドライン インターフェイス（CLI）に EXEC モードでログインしていること。
- この手順では、ESX Server が VMware Enterprise Plus のライセンスを使用することを理解します。このライセンスには、Cisco Nexus 1000V を認識できるようにする分散仮想スイッチ機能が含まれています。
- vSphere ESX Server に Enterprise Plus がライセンスされていない場合は、ライセンスをアップグレードする必要があります。

手順の詳細

ステップ 1　vSphere Client で、Enterprise Plus が付与されているかどうかを確認するホストを選択します。

ステップ 2　[Configuration] タブをクリックし、[Licensed Features] をクリックします。

Enterprise Plus にライセンスされている機能が表示されます。



ステップ 3　[Licensed Features] に、次の情報が表示されていることを確認します。

- Enterprise Plus のライセンス
- 分散仮想スイッチ機能

ステップ 4　次のいずれかを実行します。

- ESX Server に Enterprise Plus がライセンスされている場合は、正しいライセンスが示され、Cisco Nexus 1000V が認識されます。
- ESX Server に Enterprise Plus がライセンスされていない場合は、Cisco Nexus 1000V が認識されるように、VMware のライセンスを Enterprise Plus にアップグレードする必要があります。

分散仮想スイッチからホストを認識できない場合

仮想スーパーバイザ モジュール（VSM）を使用してホストとアダプタを追加した場合は、図 3-1 に示す [vCenter Client Add Host to Distributed Virtual Switch] ダイアログボックスでもそれらを追加する必要があります。

図 3-1　分散仮想スイッチからホストを認識できる場合

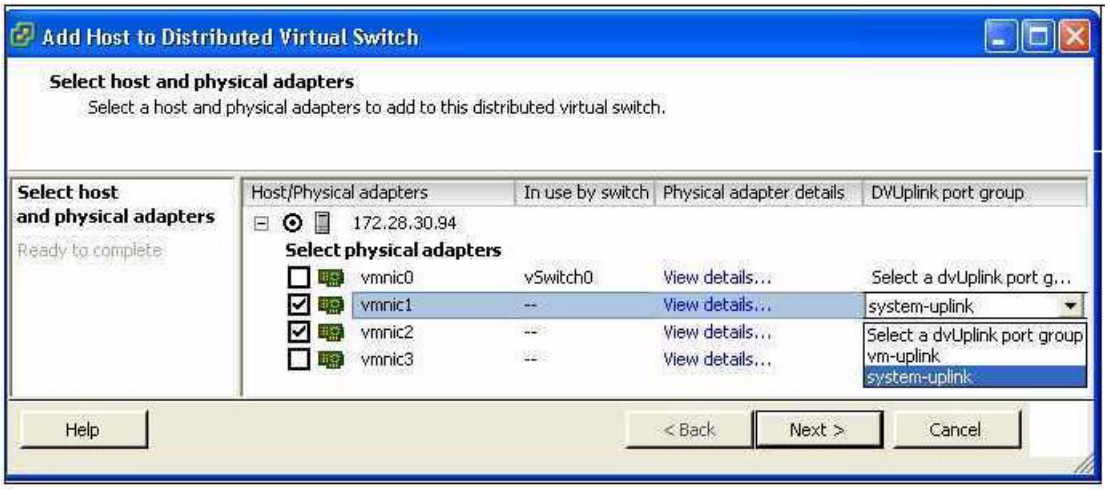
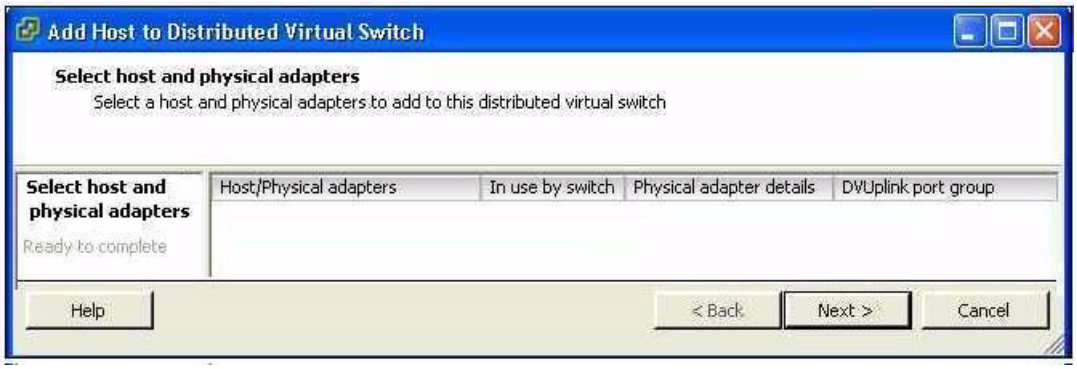


図 3-2 に示すように、このダイアログボックスにホストとアダプタが表示されない場合は、ESX Server にインストールされている VMware ライセンスが正しくない可能性があります。

「VMware のライセンス バージョンの確認」（P.3-2）の手順に従って確認してください。

図 3-2　分散仮想スイッチからホストを認識できない場合



vCenter Server 接続のリフレッシュ

Cisco Nexus 1000V と vCenter Server の間の接続をリフレッシュするには、次の手順に従います。

ステップ 1　VSM の Cisco Nexus 1000V 接続コンフィギュレーション モードで、次のコマンド シーケンスを入力します。

例：

```
n1000v# config t
n1000v(config)# svs connection s1
n1000v(config-svs-conn)# no connect
n1000v(config-svs-conn)# connect
```

ステップ 2　これで手順は完了です。

パフォーマンスの向上

ESX ホストおよび仮想マシン（VM）のパフォーマンスを向上させるには、次の点を確認します。

- ハードウェア アクセラレーションを「フル」に設定して、vCenter Server VM に VMware ツールをインストールする。
- VM では、グラフィカル インターフェイスではなく、できる限り、コマンドライン インターフェイスを使用する。

ドメイン設定の確認

仮想スーパーバイザ モジュール（VSM）と Virtual Ethernet Module（VEM; 仮想イーサネット モジュール）は、レイヤ 2 ドメイン内で分離されています。VSM と VEM のペアが同じレイヤ 2 ドメイン内で通信するためには、各ペアが同じ識別子を持つ必要があります。ドメイン ID は、VSM と VEM のペアが同じレイヤ 2 ドメイン内で通信できるようにするための一意の識別子の役割を果たします。

Cisco Nexus 1000V のインストール手順に従って、ドメイン ID を設定していること確認します。ドメイン ID が設定されていない場合、VSM は vCenter Server に接続できません。次の注意事項に従ってください。

- ドメイン ID は、1 ～ 4095 の範囲の値である必要がある。
- VSM と VEM の間のすべての制御トラフィックは、設定されているコントロール VLAN 経由で伝送される。
- VSM と VEM の間のすべてのデータ トラフィックは、設定されているパケット VLAN 経由で伝送される。
- VSM および VEM VM をホスティングしているホストの物理ネットワーク インターフェイス カード（NIC）が接続されているアップストリーム スイッチのポート上で、コントロール VLAN とパケット VLAN が許可されていることを確認する。

VSM VM 仮想インターフェイスに対するポート グループ（PG）の割り当ての確認

vCenter Server を介して VSM VM をホスティングしている ESX 上に 2 つの Port Group（PG; ポート グループ）が作成されていることを確認するには、次の手順に従います。次のポート グループ（PG）が作成されている必要があります。

- 制御 PG（VLAN = コントロール VLAN）
- パケット PG（VLAN = パケット VLAN）
- 管理 PG（VLAN = 管理 VLAN）

ポート グループが次の順序で VSM VM の 3 つの仮想インターフェイスに割り当てられていることを確認します。

仮想インターフェイス番号	ポート グループ
ネットワーク アダプタ 1	制御 PG
ネットワーク アダプタ 2	管理 PG
ネットワーク アダプタ 3	パケット PG

VSM VM のネットワーク アダプタ 1、ネットワーク アダプタ 2、およびネットワーク アダプタ 3 がコントロール VLAN、管理 VLAN、およびパケット VLAN を伝送していることを確認するには、次の手順に従います。

ステップ 1　アップストリーム スイッチで、**show mac address-table dynamic interface vlan** *control-vlan* コマンドを入力します。

予想される出力：VSM VM のネットワーク アダプタ 1 MAC アドレス。

ステップ 2　アップストリーム スイッチで、**show mac address-table dynamic interface vlan** *mgmt-vlan* コマンドを入力します。

予想される出力：VSM VM のネットワーク アダプタ 2 MAC アドレス。

ステップ 3　アップストリーム スイッチで、**show mac address-table dynamic interface vlan** *packet-vlan* コマンドを入力します。

予想される出力：VSM VM のネットワーク アダプタ 3 MAC アドレス。

VSM と vCenter Server の接続の確認

VSM と vCenter Server の間の接続のトラブルシューティング時には、次の注意事項に従ってください。

- ドメイン パラメータが正しく設定されていることを確認する。
- vCenter Server をホスティングしている Windows VM マシンの次のポートが開いていることを確認します。
  - ポート 80
  - ポート 443
- 上記の手順を確認しても接続に失敗する場合は、VSM のリロードを試みる。

- Web ブラウザで https://your-virtual-center/mob/ を参照し、[Content] > [Extension Manager] をクリックすることにより、vCenter Server によって VSM 拡張作成されているかどうかを調べる。

VSM と vCenter Server 間の接続をトラブルシューティングするには、次の手順に従います。

ステップ 1　Nexus N1000V VSM VM のネットワーク アダプタが適切に設定されていることを確認します。

ステップ 2　vCenter Server をホスティングしている Windows VM マシンの次のポートが開いていることを確認します。

- ポート 80
- ポート 443

ステップ 3　Nexus 1000V VSM から、vCenter Server を ping します。

ステップ 4　VMware VirtualCenter Server サービスが実行されていることを確認します。

vCenter Server への接続のトラブルシューティング

Cisco Nexus 1000V VSM と vCenter Server 間の接続をトラブルシューティングするには、次の手順に従います。

ステップ 1　Web ブラウザで、パス http://<VSM-IP> を入力します。

ステップ 2　cisco_nexus_1000v_extension.xml ファイルをデスクトップにダウンロードします。

ステップ 3　vCenter Server メニューから、[Plugins] → [Manage Plugins] を選択します。空の領域を右クリックし、ステップ 2 のプラグインを新しいエクステンションとして選択します。

上記の手順に従わない場合、最新でない .xml ファイルが使用される可能性があります。

拡張を使用できることを確認するには、次の手順に従います。

ステップ 1　Web ブラウザで、パス http://<vCenter-Server-IP>/mob を入力します。

ステップ 2　[Content] をクリックします。

ステップ 3　[extensionManager] をクリックします。

ステップ 4　VALUE カラムに「extensionList[Cisco_Nexus_1000v_584325821]」と表示されている場合は、次の手順に進んで VSM に接続します。

（注）　「Cisco_Nexus_1000V_584325821」は、実際の値とは異なります。この値は、cisco_nexus_1000v_extension.xml ファイルの拡張キーと一致します。

ネットワーク管理者パスワードの回復

ネットワーク管理者パスワードの回復の詳細については、『*Cisco Nexus 1000V Password Recovery Guide*』を参照してください。

拡張キーの管理

ここでは、次の内容について説明します。

- 「拡張に関する既知の問題と解決方法」（P.3-7）
- 「プラグインの競合の解決」（P.3-7）
- 「Cisco Nexus 1000V での拡張キーの確認」（P.3-8）
- 「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）
- 「拡張キーの確認」（P.3-10）

拡張に関する既知の問題と解決方法

表 3-1 に、プラグインと拡張に関する既知の問題のトラブルシューティングと解決方法を示します。

表 3-1　拡張に関する既知の問題と解決方法

問題	解決策
拡張がただちにプラグインに表示されない。	VI クライアントをいったん閉じてから、再び開きます。
拡張を VI クライアントから削除できない。	MOB を使用して拡張を削除すると、VI クライアント画面が更新されずに、更新が削除されたことが示されることがあります。この場合は、VI クライアントをいったん閉じてから、再び開きます。
拡張の [download and instal] リンクをクリックすると、無効な Uniform Resource Identifier（URI）エラーが表示される。	なし。[download and install] をクリックする必要はありません。クリックしても、インストールや接続には作用しません。プラグインは、vCenter と一緒にインストールする必要があります。

プラグインの競合の解決

vCenter Server で Nexus 1000V プラグインを作成しているときに「The specified parameter was not correct」というエラーが表示される場合は、すでに登録されているプラグインを登録しようとしています。

この問題を解決するには、次の手順に従います。

ステップ 1　正しい cisco_nexus1000v_extension.xml ファイルを使用していることを確認します。

ステップ 2　このファイルがキャッシュされたあとに、ブラウザをリフレッシュしたことを確認します。ブラウザをリフレッシュしていない場合、古い内容が同じファイル名でキャッシュされている可能性があります。

ステップ 3　「拡張キーの確認」（P.3-10）の手順に従って、VSM にインストールされている拡張キーと vCenter Server にインストールされているプラグインを比較します。

Cisco Nexus 1000V での拡張キーの確認

次の手順に従って、Cisco Nexus 1000V で拡張キーを確認できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- Cisco Nexus 1000V VSM CLI に EXEC モードでログインしている。
- 「vCenter Server の拡張キーの登録解除」（P.3-13）の手順で見つけた拡張キーを使用できる。

手順の詳細

ステップ 1　表示する拡張キーを保有している VSM の Cisco Nexus 1000V から、次のコマンドを入力します。

show vmware vc extension-key

例：

```
n1000v# show vmware vc extension-key
Extension ID: Cisco_Nexus_1000V_1935882621
n1000v#
```

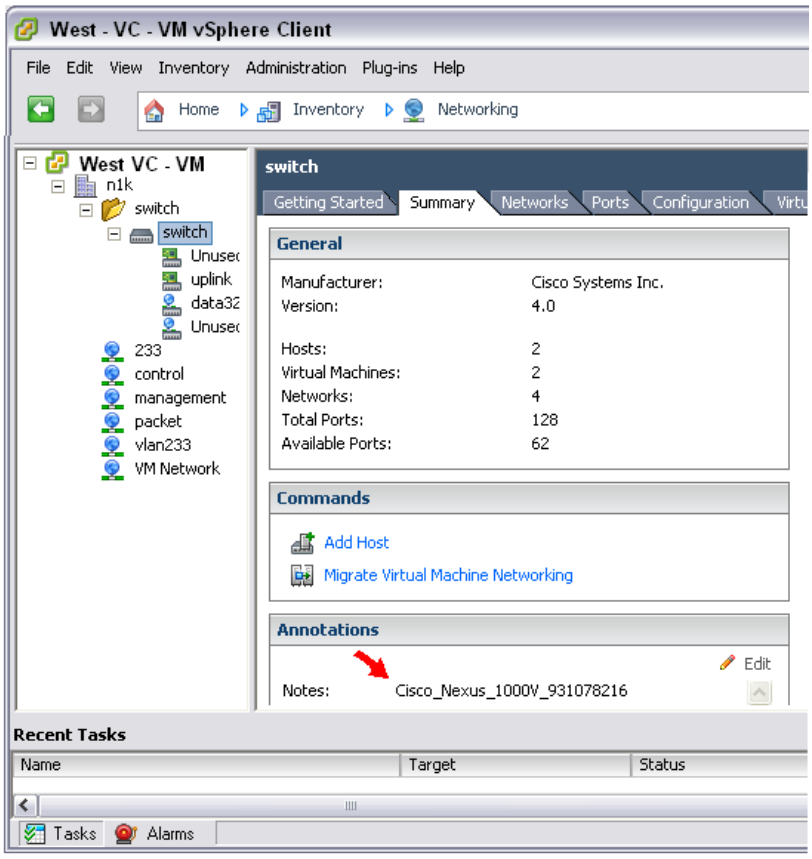
特定の DVS に結び付けられた拡張キーの確認

次の手順に従って、特定の DVS に結び付けられた拡張キーを確認できます。

ステップ 1　vSphere クライアントから、確認する拡張キーを保有している DVS を選択します。

ステップ 2　[Summary] タブをクリックします。

[Summary] タブが開き、[Annotations] ブロックの [Notes] セクションに拡張キーが表示されます。



拡張キーの確認

次の手順に従って、Cisco Nexus 1000V と vCenter Server が同じ拡張キーを使用していることを確認できます。

手順の詳細

ステップ 1　「Cisco Nexus 1000V での拡張キーの確認」（P.3-8）に従って、Cisco Nexus 1000V で使用されている拡張キーを見つけます。

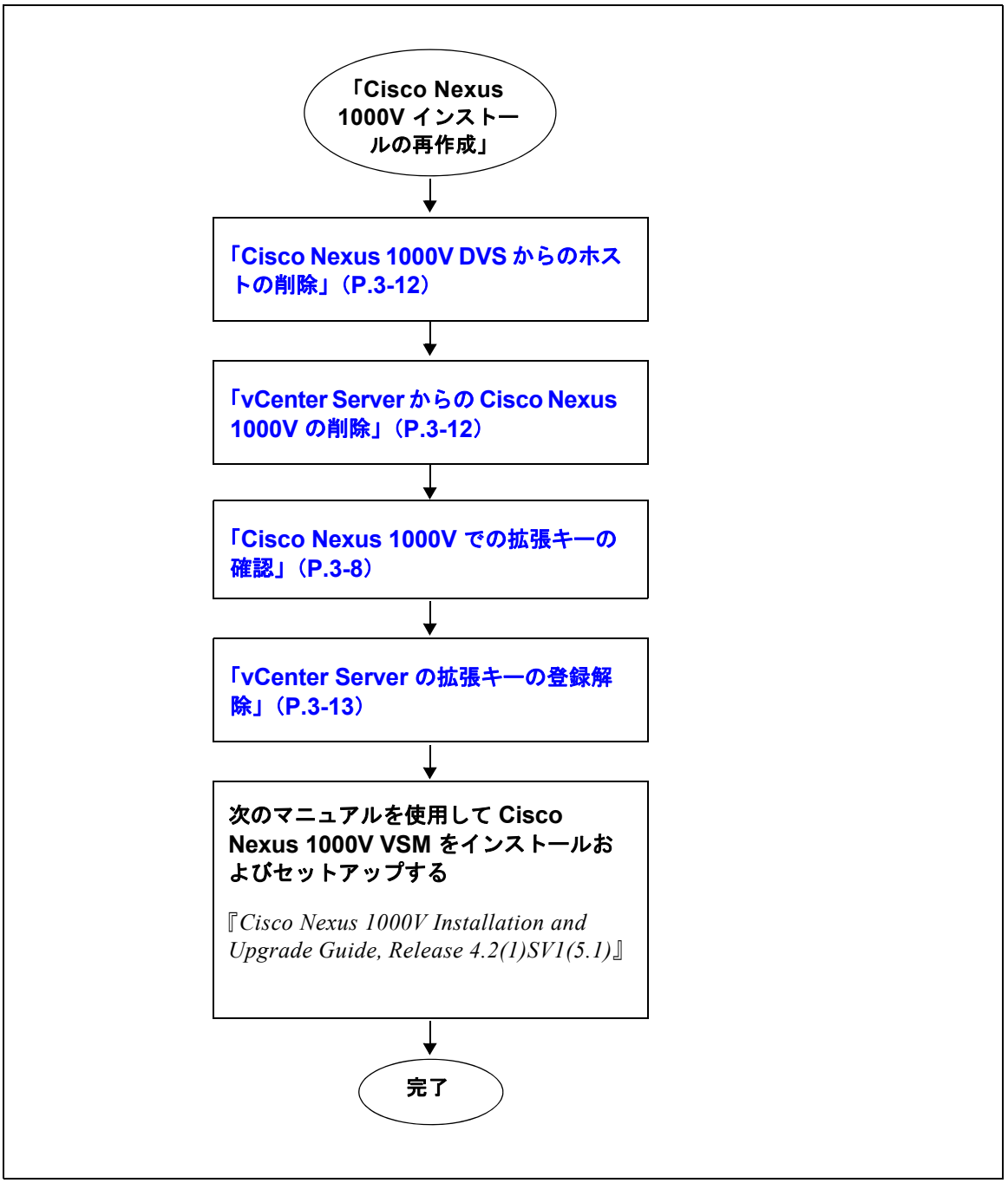
ステップ 2　「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）に従って、vCenter Server で使用されている拡張キーを見つけます。

ステップ 3　（ステップ 1 とステップ 2 で見つかった）2 つの拡張キーが同一であることを確認します。

Cisco Nexus 1000V インストールの再作成

他の回避策を使用して解決できない問題が持続する場合は、次の手順に従って、Cisco Nexus 1000V の設定全体を再作成します。

フローチャート：「Cisco Nexus 1000V インストールの再作成」



Cisco Nexus 1000V DVS からのホストの削除

次の手順に従って、Cisco Nexus 1000V DVS からホストを削除します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- vSphere クライアントにログインしている。
- vCenter Server から削除する Cisco Nexus 1000V DVS の名前を確認する。

手順の詳細

ステップ 1　vSphere Client で、[Inventory] → [Networking] を選択します。

ステップ 2　Cisco Nexus 1000V の DVS を選択し、[Hosts] タブをクリックします。

[Host] タブが開きます。

ステップ 3　各ホストを右クリックし、[Remove from Distributed Virtual Switch] を選択します。

これで、ホストは DVS から削除されました。

vCenter Server からの Cisco Nexus 1000V の削除

次の手順に従って、vCenter Server から Cisco Nexus 1000V DVS を削除できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- VSM CLI に EXEC モードでログインしている。

手順の詳細

ステップ 1　Cisco Nexus 1000V VSM から次のコマンドを使用して、vCenter Server から DVS を削除します。

config t
svs connection vc
no vmware dvs

例：

```
n1000v# conf t
n1000v(config)# svs connection vc
n1000v(config-svs-conn)# no vmware dvs
n1000v(config-svs-conn)#
```

DVS が vCenter Server から削除されます。

ステップ 2　これで手順は完了です。

「フローチャート：「Cisco Nexus 1000V インストールの再作成」」（P.3-11）に戻ってください。

vCenter Server の拡張キーの登録解除

次の手順に従って、vCenter Server の Cisco Nexus 1000V 拡張キーを登録解除できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

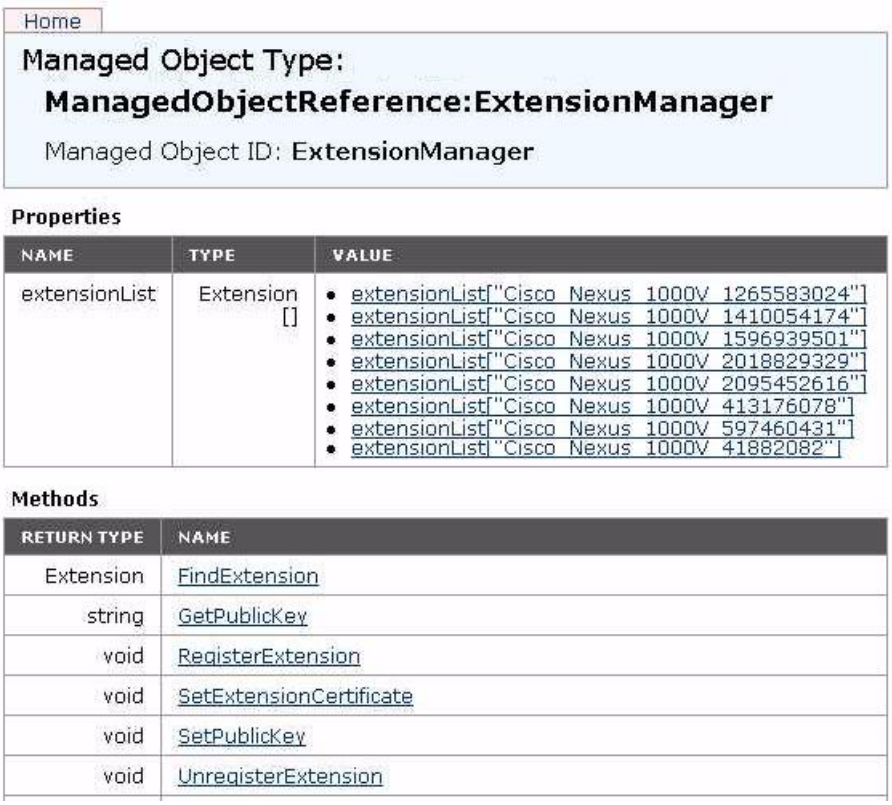
- ブラウザ ウィンドウが開いている。
- この手順では、拡張キー名を vCenter Server MOB に貼り付ける必要がある。すでに、「Cisco Nexus 1000V での拡張キーの確認」（P.3-8）の手順で見つけた拡張キーが存在することを確認してください。
- この手順を使用して vCenter Server の拡張キーを登録解除した後、Cisco Nexus 1000V VSM ソフトウェアの新たなインストールを開始できる。

手順の詳細

ステップ 1　ブラウザで、次の URL を参照します。

https://<vc-ip>/mob/?moid=ExtensionManager

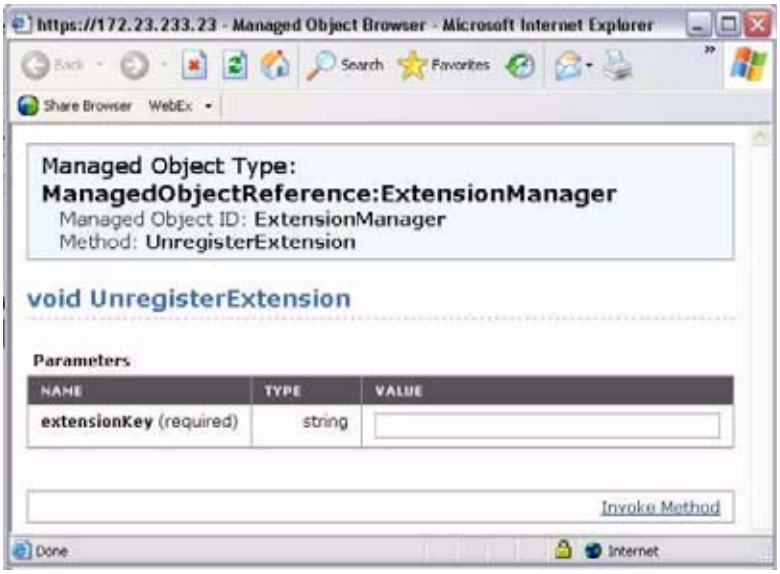
Manager Object Browser（MOB）に Extension Manager が開きます。



ステップ 2　[Unregister Extension] をクリックします。

https://<vc-ip>/mob/?moid=ExtensionManager&method=unregisterExtension

拡張を登録解除するためのダイアログボックスが開きます。



ステップ 3　値フィールドに、「Cisco Nexus 1000V での拡張キーの確認」（P.3-8）の手順で見つけた拡張キーを貼り付けて、[Invoke Method] をクリックします。

vCenter Server の拡張キーが登録解除されて、Cisco Nexus 1000V VSM ソフトウェアの新たなインストールを開始できるようになります。

ステップ 4　これで手順は完了です。

「フローチャート：「Cisco Nexus 1000V インストールの再作成」」（P.3-11）に戻ってください。

CHAPTER 4

ライセンス

この章では、ライセンスに関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「ライセンスに関する情報」（P.4-1）
- 「ライセンスのトラブルシューティングに関する前提条件」（P.4-2）
- 「ライセンスに関する問題」（P.4-3）
- 「ライセンスのトラブルシューティング コマンド」（P.4-4）

ライセンスに関する情報

Cisco Nexus 1000V ライセンス パッケージの名前は、NEXUS1000V_LAN_SERVICES_PKG です。デフォルトでは、VSM とともに 16 のライセンスがインストールされます。これらのデフォルト ライセンスは、60 日間有効です。期限切れのない永続ライセンスを購入できます。

ライセンシングは、VEM として VSM に接続されている ESX Server の CPU ソケットの数に基づきます。

モジュールには「ライセンス付き」と「ライセンスなし」があります。

- ライセンス付きモジュール：VSM にインストールされた使用可能ライセンスのプールから、すべての CPU ソケットのライセンスを取得している場合、VEM はライセンス付きとなります。
- ライセンスなしモジュール：VSM にインストールされた使用可能ライセンスのプールから、すべての CPU ソケットのライセンスを取得していない場合、VEM はライセンスされていない状態です。

  VEM がライセンスなしの場合、その仮想マシン（VM）に対応する仮想イーサネット ポートがダウンしたままとなり、ライセンスなし（unlicensed）として表示されます。

（注） サーバ管理者は VEM ライセンスに関する情報を把握していません。ライセンスされていないモジュールの vEthernet インターフェイス上をトラフィックが通過できないことを把握できるように、サーバ管理者に VEM のライセンスの状態を連絡する必要があります。

ライセンスの購入またはインストール方法や、インストールしたライセンスの削除方法などのライセンシングの詳細については、『*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ライセンス ファイルの内容

Cisco Nexus 1000V ライセンス ファイルの内容から、購入したライセンスの数とホスト ID がわかります。ライセンス ファイルの内容を表示するには、**show license file** *license_name* コマンドを使用します。

```
n1000v# show license file sample.lic
sample.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 16 ¥
        HOSTID=VDH=8449368321243879080 ¥
        NOTICE="<LicFileID>sample.lic</LicFileID><LicLineID>0</LicLineID> ¥
        <PAK>dummyPak</PAK>" SIGN=34FCB2B24AE8
```

ライセンス ファイルに示されるホスト ID は、VSM 上で示されたものと一致する必要があります。これを確認するには、**show license host-id** コマンドを使用します。例 4-6（P.4-6）を参照してください。

注意　ライセンス ファイルの内容を編集しない。内容が変更されると、ライセンスが無効になります。すでに編集している場合は、シスコのカスタマー サポート アカウント チームに連絡してください。

ライセンスのトラブルシューティングに関する前提条件

ライセンスのトラブルシューティングを開始する前に、このチェックリストの情報を確認してください。

- ライセンス ファイルの名前が 32 文字未満であることを確認する。

  show license usage コマンドを使用します。例 4-3（P.4-5）を参照してください。

- 同じ名前の他のライセンス ファイルが VSM にインストールされていないことを確認する。同じ名前のライセンス ファイルが存在する場合は、新しいライセンス ファイルの名前を変更してください。

  show license usage コマンドを使用します。例 4-3（P.4-5）を参照してください。

- ライセンス ファイルの内容を編集しない。すでに編集している場合は、シスコのカスタマー サポート アカウント チームに連絡してください。

- 次のコマンドを使用して、ライセンス ファイルのホスト ID がスイッチ上のホスト ID と同じであることを確認してください。

  show license host-id 例 4-6（P.4-6）を参照してください。

  show license file 例 4-7（P.4-6）を参照してください。

ライセンスに関する問題

次に、ライセンスの問題について現象、考えられる原因、および解決方法を示します。

症状	考えられる原因	解決策
Cisco Nexus 1000V ポート グループのポートを持つ仮想マシンの電源をオンにすると、インターフェイスがアップせず、次のステータスが表示される。 `VEM Unlicensed`	VSM に接続されているすべての VEM の CPU ソケットへのライセンス供与に十分なライセンスが取得されなかった。	**1.** ライセンスの使用状況を確認します。 **show license usage** *license_name* 例 4-4（P.4-5）を参照してください。 **2.** VEM に搭載されたソケットを表示することによって、必要なライセンスの数を判断します。 **show module vem license-info** 例 4-2（P.4-5）を参照してください。 **3.** 追加のライセンスを取得するには、シスコのカスタマー サポート アカウント チームに連絡してください。

次のシステム メッセージが表示される。
`PLATFORM-2-PFM_LIC_WARN_EXP Syslog`
`2008 Dec 19 22:28:30 N1KV %PLATFORM-2-PFM_LIC_WARN_EXP: WARNING License for VEMs is about to expire in 1 days! The VEMs' VNICS will be brought down if license is allowed to expire. Please contact your Cisco account team or partner to purchase Licenses. To activate your purchased licenses, click on www.cisco.com/go/license.`
	使用中のデフォルト ライセンスまたは評価ライセンスが間もなく期限切れになる。
	（注） 永続ライセンスは期限切れになりません。
		1. ライセンスの使用状況を確認します。
		show license usage *license_name*
		例 4-4（P.4-5）を参照してください。
		2. 追加のライセンスを取得するには、シスコのカスタマー サポート アカウント チームに連絡してください。

次のシステム メッセージが表示される。 `%LICMGR-2-LOG_LIC_USAGE: Feature NEXUS1000V_LAN_SERVICES_PKG is using 17 licenses, only 16 licenses are installed.`	インストールされているよりも多くのライセンスが使用されている。	**1.** ライセンスの使用状況を確認します。 **show license usage** *license_name* 例 4-4（P.4-5）を参照してください。 **2.** 追加のライセンスを取得するには、シスコのカスタマー サポート アカウント チームに連絡してください。

ライセンスのトラブルシューティング コマンド

ライセンスに関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	目的
show module	ライセンス状態（「ライセンスなし」または「アクティブ」）を含むモジュール情報を表示します。 例 4-1（P.4-4）を参照してください。
show module vem license info	ライセンス ステータス、ライセンス バージョン、ソケット カウントなど、VEM ライセンス情報を表示します。 例 4-2（P.4-5）を参照してください。
show license usage [*license_name*]	ライセンスに関する情報と、それらが使用されている場所を表示します。特定のライセンスについて表示すると、VEM とソケットの情報が示されます。 例 4-3（P.4-5）を参照してください。 例 4-4（P.4-5）を参照してください。
show interface veth	Cisco Nexus 1000V 内のポート プロファイル イベントについてログに記録されたメッセージを表示します。 例 4-5（P.4-5）を参照してください。
show license host-id	Cisco Nexus 1000V ライセンスのシリアル番号を表示します。 例 4-6（P.4-6）を参照してください。
show license file	指定のライセンス ファイルの内容を表示します。 例 4-7（P.4-6）を参照してください。
show license brief	VSM にインストールされているライセンス ファイルの一覧を表示します。 例 4-8（P.4-6）を参照してください。

show コマンド出力の詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

例

例 4-1　show module

```
n1000v# show module
Mod  Ports  Module-Type                        Model              Status
--   -----  -------------------------------- ------------------ ------------
1    0      Virtual Supervisor Module         Nexus1000V         active *
5    248    Virtual Ethernet Module           NA                 unlicensed
Mod  Sw                Hw
--   ---------------   ------
1    4.0(4)SV1(1)      0.0
5    4.0(4)SV1(1)      0.4
```

```
Mod  MAC-Address(es)                          Serial-Num
--  -------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
5    02-00-0c-00-05-00 to 02-00-0c-00-05-80  NA
Mod  Server-IP        Server-UUID                            Server-Name
--  ---------------  ------------------------------------  --------------------
1    172.23.232.140   NA                                     NA
5    172.23.233.100   33393935-3234-5553-4539-30364e345630  172.23.233.100
```

例 4-2　show module vem license-info

```
n1000v# show module vem license-info
Licenses are Sticky
Mod   Socket Count   License Usage Count   License Version   License Status
---   ------------   -------------------   ---------------   --------------
3     2              -                     -                 unlicensed
n1000v#
```

例 4-3　show license usage

```
n1000v# show license usage
Feature                      Ins  Lic   Status   Expiry Date   Comments
                                 Count
--------------------------------------------------------------------------------
NEXUS_VSG_SERVICES_PKG        No    0   Unused             -
NEXUS1000V_LAN_SERVICES_PKG   Yes   16  In use   Never     -
--------------------------------------------------------------------------------
n1000v#
```

例 4-4　show license usage <license_name>

```
n1000v# show license usage NEXUS1000V_LAN_SERVICES_PKG
--------------------------------------
Feature Usage Info
--------------------------------------
       Installed Licenses :    10
            Eval Licenses :   0
   Max Overdraft Licenses :    16
Installed Licenses in Use :    4
Overdraft Licenses in Use :    0
     Eval Licenses in Use :    0
       Licenses Available :   22
--------------------------------------
Application
--------------------------------------
VEM 3 - Socket 1
VEM 3 - Socket 2
VEM 4 - Socket 1
VEM 4 - Socket 2
--------------------------------------
n1000v#
```

例 4-5　show interface vethernet

```
n1000v# show int veth1
Vethernet1 is down (VEM Unlicensed)
     Port description is VM-Pri, Network Adapter 1
     Hardware is Virtual, address is 0050.56b7.1c7b
     Owner is VM "VM-Pri", adapter is Network Adapter 1
     Active on module 5
     VMware DVS port 32
```

```
Port-Profile is dhcp-profile
Port mode is access
Rx
5002 Input Packets 4008 Unicast Packets
85 Multicast Packets 909 Broadcast Packets
846478 Bytes
Tx
608046 Output Packets 17129 Unicast Packets
502543 Multicast Packets 88374 Broadcast Packets 0 Flood Packets
38144480 Bytes
20 Input Packet Drops 0 Output Packet Drops
```

例 4-6　show license host-id

```
n1000v# show license host-id
License hostid: VDH=8449368321243879080
n1000v#
```

例 4-7　show license file

```
n1000v# show license file sample.lic
sample.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 16 ¥
        HOSTID=VDH=8449368321243879080 ¥
        NOTICE="<LicFileID>sample.lic</LicFileID><LicLineID>0</LicLineID> ¥
        <PAK>dummyPak</PAK>" SIGN=34FCB2B24AE8

n1000v#
```

例 4-8　show license brief

```
n1000v# show license brief
license_file.lic
n1000v#
```

CHAPTER 5

アップグレード

この章では、VSM ソフトウェアのアップグレードに関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「アップグレードの概要」（P.5-1）
- 「In Service Software Upgrade の問題」（P.5-1）
- 「VEM のアップグレードの問題」（P.5-5）
- 「GUI のアップグレードの問題」（P.5-7）
- 「アップグレードのトラブルシューティング コマンド」（P.5-18）

アップグレードの概要

Cisco Nexus 1000V のアップグレードには、VSM と VEM の両方でのソフトウェアのアップグレードが含まれます。

In Service Software Upgrade（ISSU）を、VSM で実行されている Cisco Nexus 1000V イメージのステートフル アップグレードに使用できます。ステートフル アップグレードは、スイッチで提供されるデータ プレーン サービスの顕著な中断がないアップグレードです。

詳細については、次のマニュアルを参照してください。

- 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』

In Service Software Upgrade の問題

次に、In Service Software Upgrade（ISSU）を使用したソフトウェア アップグレードの問題について現象、考えられる原因、および解決方法を示します。

表 5-1　ISSU の問題

症状	考えられる原因	解決策

エラー メッセージ：
`Pre-Upgrade check failed.`
`Return code 0x40930062 (free space in the filesystem is below threshold).`
	このエラーは、/var/sysmgr パーティションに十分なスペースがないことを示す。	**1.** システムを再起動します。

表 5-1　ISSU の問題 （続き）

症状	考えられる原因	解決策
エラー メッセージ： `Pre-Upgrade check failed.Return code 0x4093000A (SRG collection failed)`	モジュールが、アップグレード時に削除されている。	**1.** モジュールの削除が完了したことを確認します。 **2.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。
エラー メッセージ： `Pre-Upgrade check failed.Return code 0x40930076 (Standby sup is offline.ISSU will not proceed)`	スタンバイ VSM が存在しないか、アクティブ VSM と同期されないため、VSM が安定した HA ペアを形成しない。	**1.** HA の同期状態を確認します。 **show system redundancy status** show コマンドの出力が次を示す必要があります。 Active VSM：HA スタンバイとアクティブ Standby VSM：HA スタンバイ **2.** show コマンドの出力が VSM が同期されないことを示している場合は、「ハイ アベイラビリティでの問題」（P.6-3）を参照してください。 **3.** VSM が同期されたら、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再開します。

エラー メッセージ：
`Pre-Upgrade check failed. Return code 0x807B0002 (No such file or directory)`
エラー メッセージ：
`Pre-Upgrade check failed.Return code 0x4093000F (Failed to copy image)`
	アップグレードに必要なソフトウェア イメージ ファイルが存在しない、または bootflash: リポジトリにコピーされていない。
	ファイルのコピーに十分な領域が bootflash: にない可能性があります。
		1. イメージ ファイルのブートフラッシュに領域が十分にあることを確認します。
		dir
		2. 次のいずれかを実行します。
		– さらにスペースが必要な場合、ソフトウェア イメージ ファイルの領域を作るために、bootflash リポジトリから他のファイルを削除します。
		delete
		⚠ **注意** ブートフラッシュからキックスタートまたはシステム イメージ ファイルを削除しないでください。ブート フラッシュにイメージ ファイルがない場合、システムは必要に応じて再起動できません。
		– 該当しない場合は、次の手順に進みます。
		3. www.cisco.com から bootflash: リポジトリに必要なイメージをダウンロードします。
		4. 正しいイメージが bootflash: リポジトリにあることを確認します。
		show boot
		5. 正しいソフトウェア イメージが bootflash: リポジトリにある場合は、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再開します。

表 5-1　ISSU の問題 （続き）

症状	考えられる原因	解決策

install コマンドが失敗し、次のエラーが表示される。
`Return code 0x4045001F (image MD5 checksum error)`
`Pre-Upgrade check failed.Return code 0x40930011 (Image verification failed)`
	アップグレードに必要なソフトウェア イメージ ファイルが MD5 チェックサム検証を受け渡さず、アップグレードの続行するための正しいファイルが bootflash: に存在しないことを示す。
	ファイルはコピーする際に切り捨てることができます。
		1. www.cisco.com のアップグレード zip フォルダの README ファイルを使用して、各イメージ ファイルの MD5 チェックサムを確認します。
		show file bootflash: *filename* **md5sum**
		2. 一致しないファイルを置き換えます。
		3. 正しいイメージが bootflash: リポジトリ上にあり、チェックサムが一致することを確認します。
		show file bootflash: *filename* **md5sum**
		4. 正しいソフトウェア イメージが bootflash: リポジトリにある場合は、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再開します。

エラー メッセージ： `Install has failed.Return code 0x40970001 (Incompatible image)`	install all コマンドの入力時に誤ったファイル名を使用した可能性がある。	新しいソフトウェア イメージの正しいファイル名を使用してソフトウェア アップグレードを再開します。 **install all kickstart** *filename1* **system** *filename2*
アップグレード後、VSM で新しいソフトウェア バージョンが稼動していない。	ブート変数が正しく設定されていない。	**1.** 実行イメージおよびブート変数がアップグレード バージョンと一致していることを確認します。 **show version** **show boot** **2.** 必要に応じて、必要なイメージを www.cisco.com からローカル bootflash: リポジトリにダウンロードします。 **3.** 正しいイメージが bootflash: リポジトリにあることを確認します。 **show boot** **4.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。 **5.** 問題が解決されない場合は、アップグレードの詳細を収集し、サポート ケースを開きます。 **show system internal log install details**

表 5-1　ISSU の問題 （続き）

症状	考えられる原因	解決策

設定のコピー処理の実行に失敗し、アップグレードが停止する。
`Performing configuration copy.`
`[####----------] 30%`
	サービスまたはシステム エラー。	**1.** 設定を手動でコピーします。
		copy running-config startup-config
		2. 次のいずれかを実行します。
		– 経過表示バーが 1 分以上 100% の前で停止している場合は、アップグレードの詳細を収集し、サポートケースを開きます。
		show system internal log install details
		– コピーが遅延なく成功したら、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細手順を使用して、ソフトウェア アップグレードを再開します。

エラー メッセージ： `Another install procedure may be in progress.(0x401E0007)`	別のアップグレード セッションが VSM コンソールまたは SSH/Telnet から進行中。	次のいずれかを実行します。 • 進行中の最初のアップグレード セッションを続行します。 • アップグレードを停止し、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、1 つのセッションのみを再開します。
インストール コマンドが次のエラー メッセージで失敗する。 `-- FAIL. Return code 0x4093001E (Standby failed to come online) Install has failed.Return code 0x4093001E (Standby failed to come online)`	新しいイメージでのスタンバイ VSM の起動が失敗する。	次のいずれかを実行します。 • 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。 • アップグレードを延期し、ブート変数を元のファイル名にリセットします。 **boot kickstart** *filename* [**sup-1**] [**sup-2**]
インストール コマンドが次のエラー メッセージで失敗する。 `Install has failed. Return code 0x4093001F (Standby installer failed to take over the installation). Please identify the cause of the failure, and try "install all" again"`	スタンバイ VSM をアクティブにし、アクティブな VSM との安定した HA ペアを形成するのに 10 分以上かかる。	**1.** ブート変数を元のファイル名にリセットします。 **boot kickstart** *filename* [**sup-1**] [**sup-2**] **2.** スタンバイがまだ新しいソフトウェア バージョンを実行している場合は、そのファイルをリロードします。 **reload** 両方で元のソフトウェア バージョンが動作しているように、スタンバイをアクティブと同期します。

表 5-1　ISSU の問題（続き）

症状	考えられる原因	解決策

インストール コマンドが次のエラー メッセージで失敗する。
`Module 2: Waiting for module online.`
`-- SUCCESS`
`-- Install has failed. Return code 0x40930000 (Current operation failed to complete within specified time)`
	スタンバイ VSM での失敗により、「**Continuing with installation, please wait**」メッセージの後、スイッチオーバーの前にリロードが行われる。	**1.** ログを検査します。
		show logging
		2. プロセス障害によって生じたスタンバイのリロードを探します。
		show cores
		プロセスのクラッシュが見られる場合は、アップグレードの詳細を収集し、サポート ケースを開きます。
		show system internal log install details
		3. 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。

Pre-Upgrade check failed Return code 0x40930062 (free space in the filesystem is below threshold).		**1.**

VEM のアップグレードの問題

次に、VEM ソフトウェア アップグレードの問題について現象、考えられる原因、および解決方法を示します。

表 5-2　VEM のアップグレードの問題

症状	考えられる原因	解決策
VSM コンソールから VEM のアップグレードを開始した後、VUM が新しい VEM でホストのアップグレードをスキップする。	次の 1 つまたは複数が、ホスト クラスタでイネーブルである。 • VMware High Availability（HA） • VMware Fault Tolerance（FT） • Vmware Distributed Power Management（DPM）	**1.** アップグレードの障害を確認します。 **show vmware vem upgrade status** **2.** vCenter server から、クラスタの HA、FT、および DPM をディセーブルにします。 **3.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、VEM ソフトウェア アップグレードを再始動します。
VEM のアップグレードが失敗する。	誤った VUM のバージョンを使用している。	**1.** 『*Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*』を使用して、アップグレードに必要な VUM のバージョンを識別します。 **2.** 正しい VUM のバージョンにアップグレードします。 **3.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。

表 5-2　VEM のアップグレードの問題 （続き）

症状	考えられる原因	解決策
アップグレード後、ホストが VSM に追加されない。	誤った VEM ソフトウェア バージョンがホストにインストールされている。	**1.** 『*Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*』を使用して、アップグレードに必要な VEM ソフトウェア バージョンを識別します。 **2.** 適切な VEM ソフトウェア バージョンおよび『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、アップグレードを続行します。
VEM のアップグレードが失敗する。	誤った VEM BundleID が vCenter サーバに指定されている。	**1.** 『*Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*』を使用して、アップグレードに必要な BundleID を識別します。 **2.** vCenter Server で使用されている BundleID を確認します。 **show vmware vem upgrade status** **3.** アップグレードの vCenter Server を通知し、アップグレードを開始します。 **vmware vem upgrade notify** **vmware vem upgrade proceed** bundleID が vCenter Server で更新されます。 **4.** BundleID がアップグレード バージョンに正しく更新されていることを確認します。 **show vmware vem upgrade status** **5.** 次のいずれかを実行します。 – BundleID が正しく更新された場合は、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用してアップグレードを続行します。 – 正しく更新されていない場合は、アップグレードの詳細を収集し、サポート ケースを開きます。 **show system internal log install details**

表 5-2　VEM のアップグレードの問題 （続き）

症状	考えられる原因	解決策
シェルのメッセージが、モジュールのアンロードが失敗したことを通知する。	アップグレードを開始する前に、モジュールがメンテナンス モード（すべての VM が VMotion された状態）にならなかった。	**1.** ホストをメンテナンス モードにします。 **2.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、アップグレードを続行します。
	ホストに、新しいモジュールをロードするだけの十分なメモリがない。 ホストに 2 GB 以上の物理 RAM が必要です。Cisco Nexus 1000V VSM VM もホストする場合は、4 GB 以上の物理 RAM が必要です。vCenter Server VM もホストする場合は、追加メモリが必要なことがあります。	**1.** ホストに新しいモジュールをロードするだけの十分なメモリがあることを確認します。 RAM および CPU の割り当ての詳細については、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』を参照してください。 **2.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、アップグレードを続行します。

GUI のアップグレードの問題

次に、GUI アップグレード アプリケーションを使用したソフトウェア アップグレードの問題について現象、考えられる原因、および解決方法を示します。

（注）　SV1(4) から SV1(4a) に直接アップグレードする場合は、GUI は使用せず、この項の内容は該当しません。ここで説明する内容は、SV1(4a) へのアップグレードの前に、SV1(3x) リリースから SV1(4) への中間アップグレードに GUI を使用する場合にだけ該当します。

表 5-3　GUI のアップグレードの問題

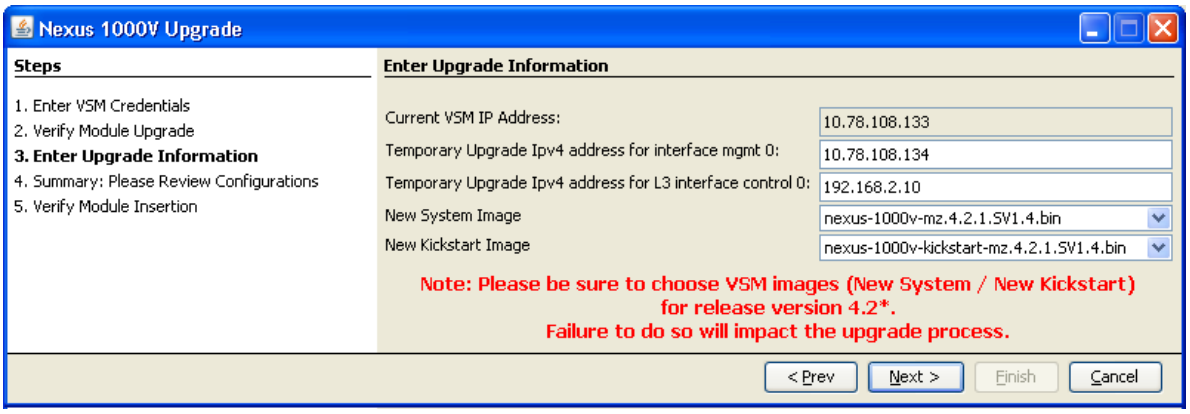
症状	考えられる原因	解決策
アップグレードの GUI が 10 分後に停止してタイムアウトになり、次のメッセージが表示される。 「Error: Could not contact the upgraded VSM at *n.n.n.n*.Please check the connection.」	アップグレード時に、mgmt0 インターフェイスに到達不能な IP アドレスを設定した。 この場合、冗長ペアの一方の VSM は新規のソフトウェアがインストールされた状態で到達不能になり、もう一方の VSM はアップグレード前の元のソフトウェア バージョンがインストールされた状態で到達可能になります。	**1.** 以前のソフトウェア バージョンに VSM ペアを戻すには、次のいずれかの手順を実行します。 – 「プライマリがアクティブな場合のセカンダリ VSM の回復」（P.5-8） – 「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13） **2.** 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。

表 5-3　GUI のアップグレードの問題 （続き）

症状	考えられる原因	解決策
アップグレードの GUI が 10 分後に停止してタイムアウトになり、次のメッセージが表示される。 「Error: Could not contact the upgraded VSM at 10.104.244.150.Please check the connection.」 タイムアウト後に、一方の VSM がスイッチ（ブート）モードでアップする。	アップグレードに互換性のない、または適切でない VSM ソフトウェア イメージを選択した。 GUI の選択リストから選択したソフトウェア イメージに、あるソフトウェア バージョンのシステムイメージ、および別のソフトウェア バージョンのキックスタート イメージが含まれていた。これらのイメージは、同じソフトウェア バージョンである必要があります。 アップグレード時にソフトウェア イメージを選択する例については、例 5-1 を参照してください。	1. アップグレードを続行するには、まず、次のいずれかを使用して VSM を回復させます。 – 「プライマリがアクティブな場合のセカンダリ VSM の回復」（P.5-8） – 「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13） 2. 『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』にある詳細な手順を使用して、ソフトウェア アップグレードを再始動します。

例 5-1　アップグレード：アップグレード情報の入力

次に、アップグレード プロセス時にシステム イメージとキックスタート イメージを指定する例を示します。この例で指定されているイメージは、同じリリース SV1.4 のものです。あるリリースからキックスタート イメージを指定し、別のリリースからシステム イメージを指定すると、アップグレードを続行できません。



プライマリがアクティブな場合のセカンダリ VSM の回復

プライマリ VSM がアクティブの場合は、次の手順を使用してセカンダリ VSM を回復できます。

（注）　この項の情報は、Release 4.2(1)SV1(4) から Release 4.2(1)SV1(5.1) にアップグレードする場合は該当しません。

ステップ 1　「VSM アップグレードの停止」（P.5-9）の手順を使用して、VSM でのアップグレードを停止します。

ステップ 2　「ブート変数の変更」（P.5-10）の手順を使用して、ブート変数を以前のバージョンに戻します。

ステップ 3　vCenter Server の左側のパネルで、セカンダリ VSM を右クリックし、[Delete from Disk] を選択します。

セカンダリ VSM が削除されます。

ステップ 4　vSphere client Deploy OVF Template ウィザードを使用し、次を指定してソフトウェアを再インストールし、新しい VSM を作成します。

- Nexus 1000V セカンダリの設定方法
  （GUI セットアップ ダイアログで HA ペアのセカンダリ VSM を設定）
- プライマリ VSM のホストまたはクラスタ
- プライマリ VSM と同じドメイン ID およびパスワード

詳細な手順については、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

VSM がアップして、スタンドアロン VSM が新たに作成された HA ペアを形成します。VSM には、以前のバージョンのソフトウェアがインストールされています。

VSM アップグレードの停止

次の手順に従って、進行中の VSM アップグレードを停止できます。

はじめる前に

- EXEC モードで CLI にログインしていること。

（注）　この項の情報は、Release 4.2(1)SV1(4) から Release 4.2(1)SV1(5.1) にアップグレードする場合は該当しません。

手順の詳細

ステップ 1　アップグレード ステータスを表示します。

show svs upgrade status

例：
```
n1000v# show svs upgrade status
Upgrade State: Start
Upgrade mgmt0 ipv4 addr: 1.1.1.1
Upgrade mgmt0 ipv6 addr:
Upgrade control0 ipv4 addr:
```

ステップ 2　アップグレードを停止します。

configure terminal

no svs upgrade start

例：
```
n1000v# configure terminal
n1000v#(config)# no svs upgrade start
WARNING! VSM upgrade process is aborted
```

```
n1000v#(config)#
```

ステップ 3　アップグレード ステータスを表示します。

show svs upgrade status

例：
```
n1000v#(config)# show svs upgrade status
Upgrade State: Abort
Upgrade mgmt0 ipv4 addr:
Upgrade mgmt0 ipv6 addr:
Upgrade control0 ipv4 addr:
```

ステップ 4　これで手順は完了です。次に示されるプロセスに戻ります。

- 「プライマリがアクティブな場合のセカンダリ VSM の回復」（P.5-8）
- 「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）

ブート変数の変更

次の手順に従って、VSM のブートに使用するソフトウェア イメージを置換できます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- アップグレード前のシステムのファイル名と、適用するキックスタート イメージ ファイルがわかっている。

手順の詳細

ステップ 1　現在のブート変数を表示します。

show boot

例：
```
n1000v# show boot
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4.bin
system variable = bootflash:/nexus-1000v-mzg.4.2.1.SV1.4.bin
No module boot variable set
n1000v(config)#
```

ステップ 2　現在のシステムおよびキックスタート ブート変数を削除します。

configure terminal

no boot system

no boot kickstart

例：
```
n1000v# configure terminal
n1000v(config)# no boot system
n1000v(config)# no boot kickstart
n1000v#(config)#
```

ステップ 3　システムおよびキックスタート ブート変数をアップグレード前の元のファイル名に復元します。

boot system bootflash:*system-boot-variable-name*

boot system bootflash:*kickstart-boot-variable-name*

例：
```
n1000v#(config)# boot system bootflash:nexus-1000v-mz.4.0.4.SV1.3a.bin
n1000v#(config)# boot kickstart bootflash:nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
n1000v#(config)#
```

ステップ 4　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

copy run start

例：
```
n1000v#(config)# copy run start
[########################################] 100%e
n1000v#(config)#
```

ステップ 5　システムおよびキックスタート ブート変数の変更を確認します。

show boot

例：
```
n1000v#(config)# show boot
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
No module boot variable set
n1000v#(config)#
```

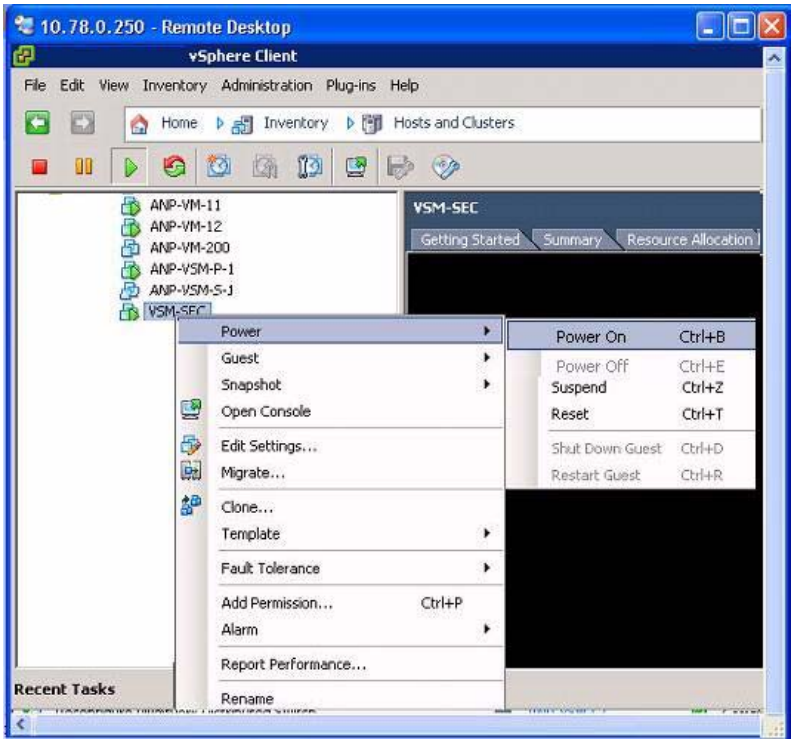
ステップ 6　これで手順は完了です。次に示されるプロセスに戻ります。

- 「プライマリがアクティブな場合のセカンダリ VSM の回復」（P.5-8）
- 「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）

VSM の電源投入

新たに作成した VSM の電源を投入するには、ここに示す手順を実行します。

ステップ 1　vCenter Server の左側のパネルで、VSM を右クリックし、[Power] > [Power On] を選択します。VSM が起動します。



ステップ 2　これで手順は完了です。「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）に戻ってください。

HA ロールの変更

次の手順に従って、VSM の HA ロールを変更できます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- 既存の VSM のドメイン ID がわかっている。

手順の詳細

ステップ 1　既存の VSM のドメインに移動します。

configure terminal

svs-domain

domain id *domain-id*

例：
```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 1941
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
```

ステップ 2　HA ロールを変更します。

system redundancy role [primary | secondary | standalone]

例：
```
n1000v(config-svs-domain)# system redundancy role secondary
Setting will be activated on next reload.
n1000v(config-svs-domain)#
```

例：
```
n1000v(config-svs-domain)# system redundancy role primary
Setting will be activated on next reload.
n1000v(config-svs-domain)#
```

ステップ 3　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

copy run start

例：
```
n1000v#(config-svs-domain)# copy run start
[########################################] 100%e
n1000v#(config-svs-domain)#
```

ステップ 4　これで手順は完了です。「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）に戻ってください。

セカンダリがアクティブな場合のプライマリ VSM の回復

次のプロセスに従って、セカンダリ VSM がアクティブである場合にプライマリ VSM を回復させることができます。

ステップ 1　「VSM アップグレードの停止」（P.5-9）の手順を使用して、セカンダリ VSM でのアップグレードを停止します。

ステップ 2　「ブート変数の変更」（P.5-10）の手順を使用して、ブート変数を以前のバージョンに戻します。

ステップ 3　vCenter Server の左側のパネルで、プライマリ VSM を右クリックし、[Delete from Disk] を選択します。

プライマリ VSM が削除されます。

ステップ 4　OVA からソフトウェアを再インストールし、次の情報を指定することによって、新規の VSM を作成します。

- GUI に代わる手動（CLI）設定方法
- 既存のセカンダリ VSM のホストまたはクラスタ

詳細なインストール手順については、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ステップ 5　「ポート グループの接続解除」（P.5-14）の手順を使用して、新規の VSM に電源を投入するときに、ホスト サーバと VSM 間のポート グループが接続していないことを確認します。

ステップ 6　「VSM の電源投入」（P.5-12）の手順を使用して、新たに作成した VSM に電源を投入します。

VSM がスタンドアロン HA ロールでアップします。

ステップ 7　「HA ロールの変更」（P.5-12）の手順を使用して、新たに作成したスタンドアロンの VSM の HA ロールをプライマリに変更し、設定を保存します。

ステップ 8　「VSM の電源オフ」（P.5-15）の手順を使用して、新たに作成した VSM の電源を切ります。

ステップ 9　「ポート グループの接続」（P.5-16）の手順を使用して、新規の VSM に電源を投入するときに、ホスト サーバと VSM 間のポート グループが接続していることを確認します。

ステップ 10　「VSM の電源投入」（P.5-12）の手順を使用して、新たに作成した VSM に電源を投入します。

VSM がアップしてホスト サーバと接続し、既存のプライマリ VSM との HA ペアを形成します。

ポート グループの接続解除

ポート グループと VSM の接続を解除して、ホスト サーバへの接続を防止するには、ここに示す手順を実行します。

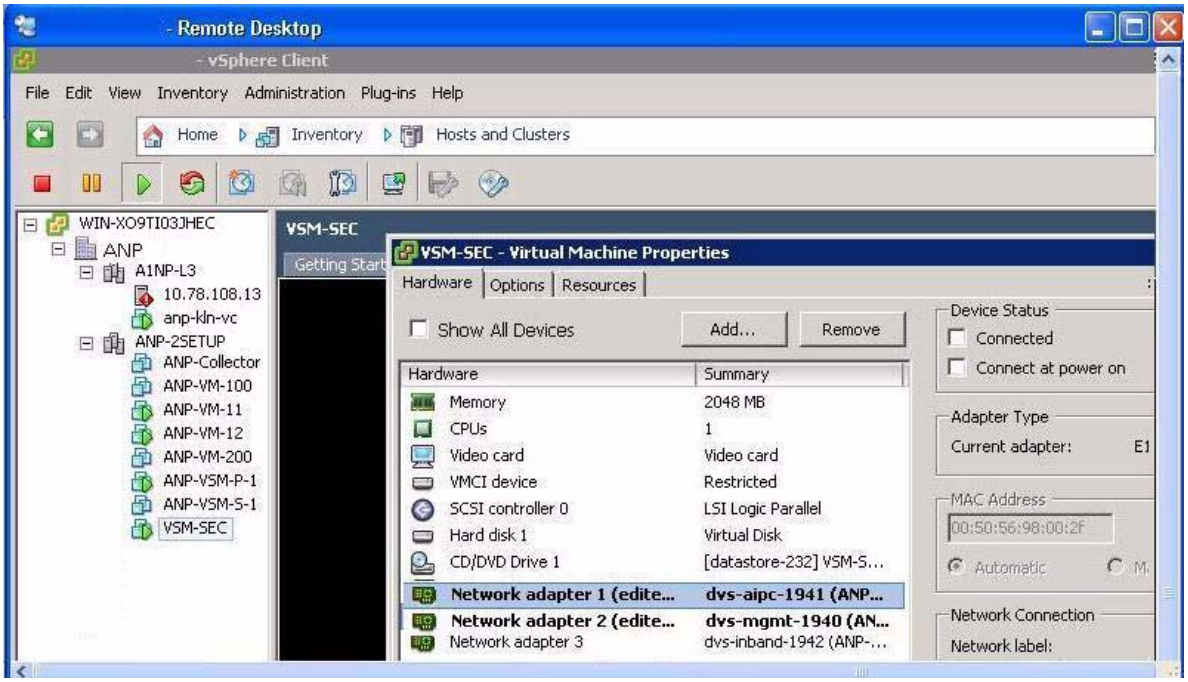
ステップ 1　vCenter Server で VSM を選択し、[Edit] > [Settings] を選択します。

[Virtual Machine Properties] ダイアログボックスが開きます。

ステップ 2　制御ポート グループを選択し、次の [Device Settings] のチェックボックスをオフにします。

- [Connected]
- [Connect at Power On]

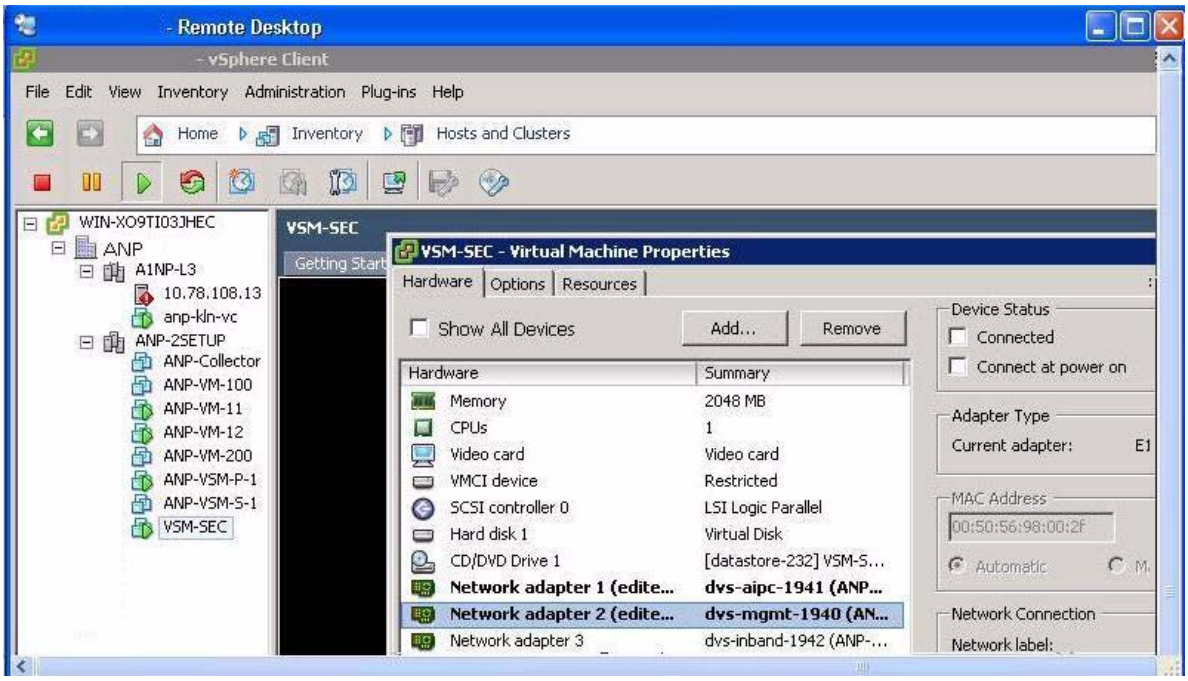
制御ポートを介した VSM からホスト サーバへの接続がドロップされ、VSM に電源投入しても復元されません。



ステップ 3　管理ポート グループを選択し、次の [Device Settings] のチェックボックスをオフにします。

- [Connected]
- [Connect at Power On]

管理ポートを介した VSM からホスト サーバへの接続がドロップされ、VSM に電源投入しても復元されません。



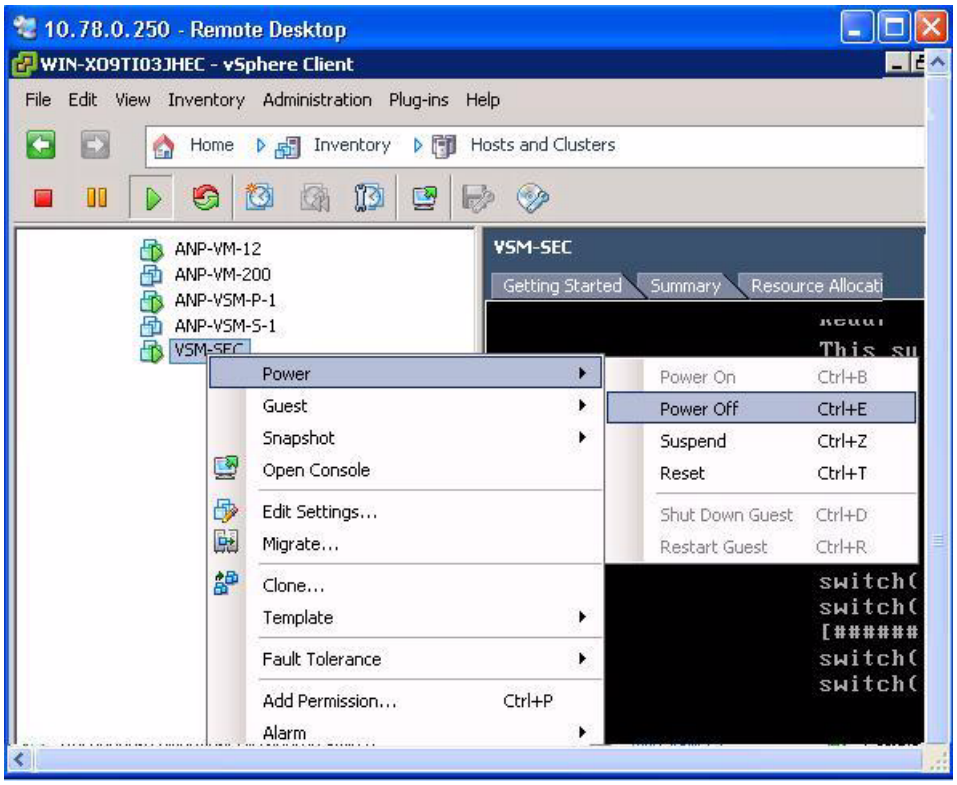
ステップ 4　これで手順は完了です。「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）に戻ってください。

VSM の電源オフ

新たに作成した VSM の電源を切るには、ここに示す手順を実行します。

ステップ 1　vCenter Server の左側のパネルで、VSM を右クリックし、[Power] > [Power Off] を選択します。

VSM がシャットダウンします。



ステップ 2　これで手順は完了です。「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）に戻ってください。

ポート グループの接続

VSM に電源を投入するときに、ポート グループをホストに接続させるには、ここに示す手順を実行します。

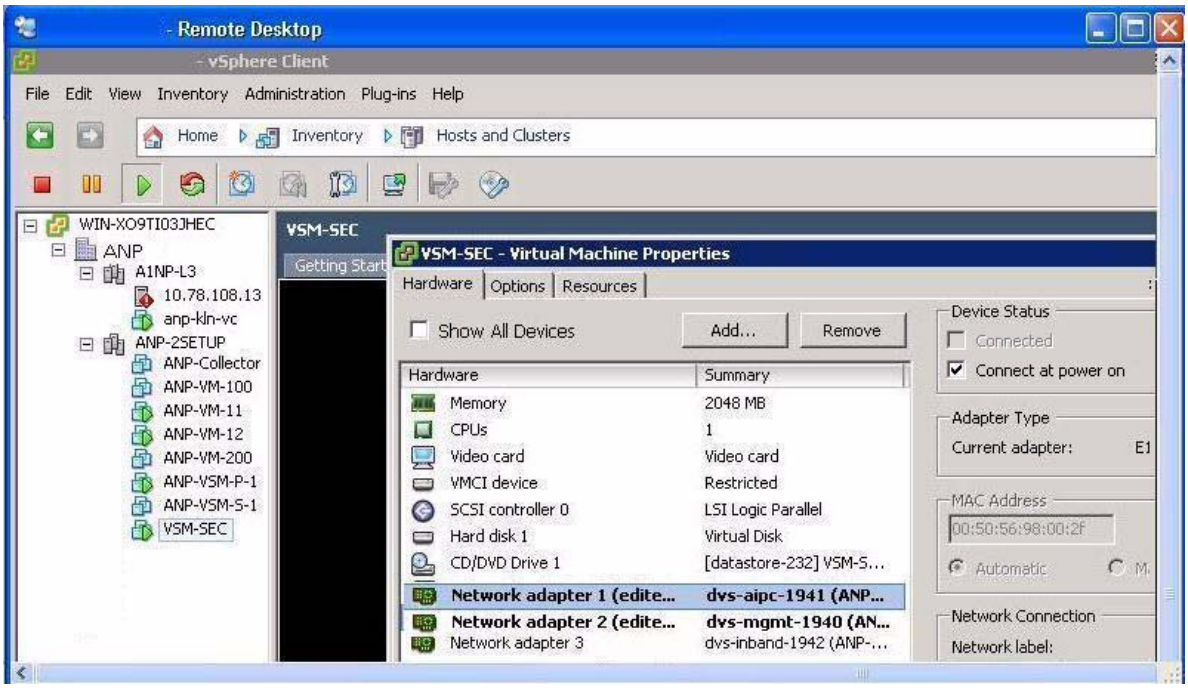
ステップ 1　vCenter Server で VSM を選択し、[Edit] > [Settings] を選択します。

[Virtual Machine Properties] ダイアログボックスが開きます。

ステップ 2　制御ポート グループを選択し、次の [Device Settings] のチェックボックスをオンにします。

- [Connect at Power On]

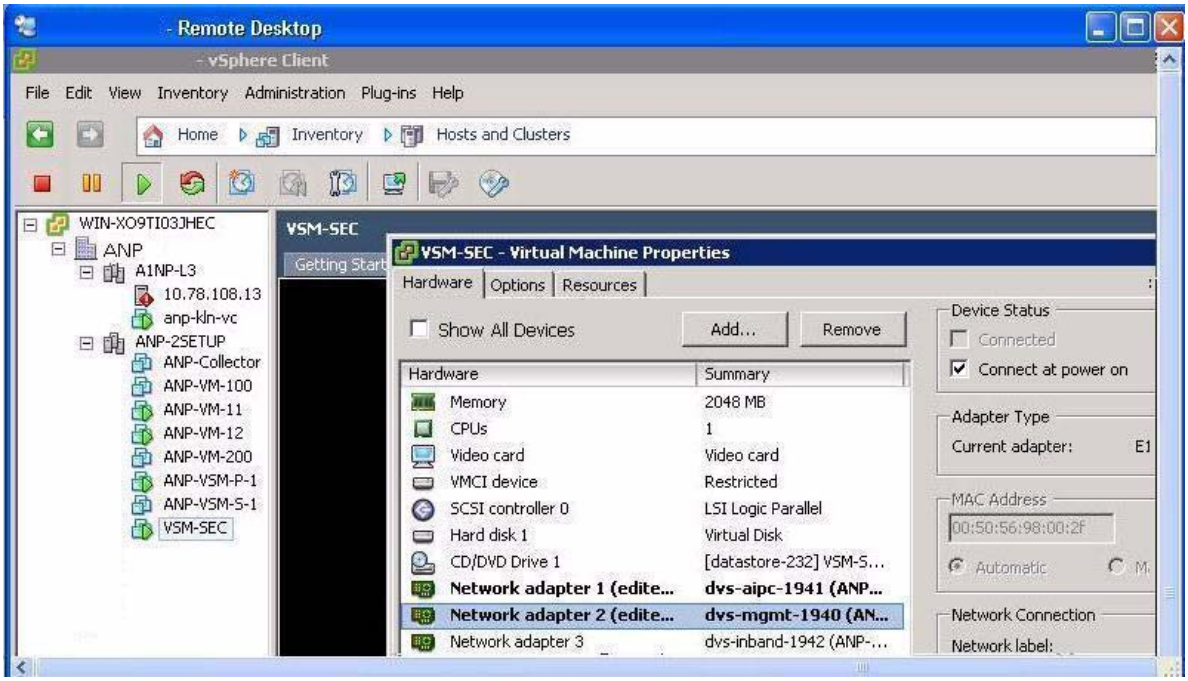
VSM に電源を投入すると、制御ポートを介してホスト サーバに接続します。



ステップ 3　管理ポート グループを選択し、次の [Device Settings] のチェックボックスをオンにします。

- [Connect at Power On]

VSM に電源を投入すると、管理ポートを介してホスト サーバに接続します。



ステップ 4　これで手順は完了です。「セカンダリがアクティブな場合のプライマリ VSM の回復」（P.5-13）に戻ってください。

アップグレードのトラブルシューティング コマンド

アップグレードに関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	説明
show boot	ブート変数の定義を表示します。VSM のブートに使用されるソフトウェア イメージの名前が示されます。 例 5-2（P.5-18）を参照してください。
show module See	アクティブ VSM およびスタンバイ VSM のモジュール状態を表示します。 例 5-4（P.5-19）（ISSU）を参照してください。 例 5-4（P.5-19）を参照してください。
show running-config | in boot	実行コンフィギュレーションの現在のブート変数を表示します。 例 5-5（P.5-19）を参照してください。
show startup-config | in boot	スタートアップ コンフィギュレーションの現在のブート変数を表示します。 例 5-6（P.5-20）を参照してください。
show svs connections	VSM と VMware ホスト サーバ間の現在の接続を表示します。 例 5-7（P.5-20）を参照してください。
show svs upgrade status	アップグレード状態を表示します。 例 5-8（P.5-20）を参照してください。
show system redundancy status	VSM の現在の冗長性状態を表示します。 例 5-9（P.5-20）を参照してください。
show vmware vem upgrade status	アップグレード状態を表示します。 例 5-10（P.5-21）を参照してください。

例 5-2　show boot

```
n1000v# show boot
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3a.bin
system variable = bootflash:/nexus-1000v-mz.4.0.4.SV1.3a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4.bin
system variable = bootflash:/nexus-1000v-mzg.4.2.1.SV1.4.bin
No module boot variable set
n1000v#
```

例 5-3　show module（ISSU で VSM が最初にアップグレードされ、VEM のアップグレードは保留中）

```
n1000v# show module
Mod Ports Module-Type                       Model              Status
--- ----- ------------------------------- ------------------ ------------
1   0     Virtual Supervisor Module        Nexus1000V         ha-standby
2   0     Virtual Supervisor Module        Nexus1000V         active *
3   248   Virtual Ethernet Module          NA                 ok
Mod Sw              Hw
--- --------------- ------
1   4.2(1)SV1(4a)   0.0
2   4.2(1)SV1(4a)   0.0
3   4.2(1)SV1(4)    1.9
Mod MAC-Address(es)                         Serial-Num
--- -------------------------------------- ----------
1   00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 NA
2   00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 NA
3   02-00-0c-00-03-00 to 02-00-0c-00-03-80 NA
Mod Server-IP       Server-UUID                          Server-Name
--- --------------- ------------------------------------ --------------------
1   10.78.109.43    NA                                   NA
2   10.78.109.43    NA                                   NA
3   10.78.109.51    4220900d-76d3-89c5-17d7-b5a7d1a2487f 10.78.109.51
n1000v#
```

例 5-4　show module（VEM および VSM がアップグレードされる）

```
n1000v# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  ------------------------------- ------------------ ------------
1    0      Virtual Supervisor Module        Nexus1000V         ha-standby
2    0      Virtual Supervisor Module        Nexus1000V         active *
3    248    Virtual Ethernet Module          NA                 ok

Mod  Sw               Hw
---  ---------------  ------
1    4.0(4)SV1(3)     0.0
2    4.0(4)SV1(3)     0.0
3    4.2(1)SV1(4)     1.9

Mod  MAC-Address(es)                         Serial-Num
---  -------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.78.109.43     NA                                    NA
2    10.78.109.43     NA                                    NA
3    10.78.109.51     4220900d-76d3-89c5-17d7-b5a7d1a2487f  10.78.109.51
n1000v#
```

例 5-5　show running-config | include boot

```
n1000v# show running-config | include boot
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-1
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-2
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-2
n1000v#
```

例 5-6　show startup-config | include boot

```
switch# show startup-config | include boot
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-1
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mzg.4.2.1.SV1.4a.bin sup-2
boot system bootflash:/nexus-1000v-mzg.4.2.1.SV1.4a.bin sup-2
n1000v#
```

例 5-7　show svs connections

```
n1000v# show svs connections

connection vc:
    hostname: 172.23.232.139
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: Hamilton-DC
    DVS uuid: 9b dd 36 50 2e 27 27 8b-07 ed 81 89 ef 43 31 17
    config status: Enabled
    operational status: Connected
    sync status: -
    version: -
n1000v#
```

例 5-8　show svs upgrade status

```
n1000v# show svs upgrade status
Upgrade State: Start
Upgrade mgmt0 ipv4 addr: 1.1.1.1
Upgrade mgmt0 ipv6 addr:
Upgrade control0 ipv4 addr:
n1000v#
```

例 5-9　show system redundancy status

```
switch# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary

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
      Internal state:   HA standby

switch#
```

例 5-10　show vmware vem upgrade status

```
n1000v# show vmware vem upgrade status
Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201007101-BG
    DVS: VEM400-201007101-BG

n1000v#
```

CHAPTER 6

ハイ アベイラビリティ

この章では、ハイ アベイラビリティに関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「ハイ アベイラビリティについて」（P.6-1）
- 「ハイ アベイラビリティでの問題」（P.6-3）
- 「ハイ アベイラビリティのトラブルシューティング コマンド」（P.6-5）

ハイ アベイラビリティについて

ハイ アベイラビリティ（HA）の目的は、システム内で発生したハードウェアの障害およびソフトウェアのエラーの両方による影響を一定範囲内に抑えることです。Cisco NX-OS オペレーティング システムは、ネットワーク レベル、システム レベル、およびサービス レベルでのハイ アベイラビリティに向けて設計されています。

次の Cisco NX-OS 機能が、障害発生時のトラフィックの中断を防止または最小限に留めます。

- 冗長性：ソフトウェア アーキテクチャのあらゆる面での冗長性。
- プロセスの分離：1 つのプロセス内で発生したエラーで他のプロセスが中断されるのを防ぐためのソフトウェア コンポーネント間の分離。
- 再起動性：ほとんどのシステム機能およびサービスが分離されているため、エラーが発生しても、他のサービスは実行され続けている中で独立して再起動が可能。さらに、ほとんどのシステム サービスはステートフルな再起動を実行するため、その他のサービスに対して透過的に稼動を再開できます。
- スーパーバイザ ステートフル スイッチオーバー：アクティブ/スタンバイ デュアル スーパーバイザ設定。状態と設定が 2 つの仮想スーパーバイザ モジュール（VSM）の間で一貫して同期された状態が保たれ、VSM に障害が発生してもシームレスでステートフルなスイッチオーバーが提供されます。

Cisco Nexus 1000V システムは、次のコンポーネントで構成されます。

- 仮想サーバ内で実行される仮想イーサネット モジュール（VEM）。これらは、VSM 内でモジュールとして表されます。
- リモート管理コンポーネント。たとえば、VMware vCenter Server。
- 仮想マシン（VM）内で実行される 1 つまたは 2 つの VSM。

システムレベルのハイ アベイラビリティ

Cisco Nexus 1000V では、HA ペアとして実行される冗長 VSM 仮想マシン（プライマリとセカンダリ）がサポートされています。デュアル VSM は、同時にはどちらか片方の VSM しかアクティブになれず、他方はスタンバイ バックアップとして機能する、アクティブ / スタンバイ キャパシティで稼動します。状態と設定が、2 つの VSM 間で一貫して同期された状態が保たれ、アクティブな VSM に障害が発生したときにはステートフルなスイッチオーバーが提供されます。

シングルまたはデュアル スーパーバイザ

Cisco Nexus 1000V システムは、次のコンポーネントで構成されます。

- 仮想サーバ内で実行される仮想イーサネット モジュール（VEM）。これらは、VSM 内でモジュールとして表されます。
- リモート管理コンポーネント。たとえば、VMware vCenter Server。
- 仮想マシン（VM）内で実行される 1 つまたは 2 つの仮想スーパーバイザ モジュール（VSM）。

シングル VSM 運用	デュアル VSM 運用
• ステートレス：サービスはスタートアップ コンフィギュレーションから起動されます。 • ステートフル：サービスは以前の状態で再開されます。	• 1 つのアクティブな VSM と 1 つのスタンバイ VSM。 • アクティブな VSM は、すべてのシステム アプリケーションを実行し、システムを制御します。 • スタンバイ VSM では、アプリケーションはスタンバイ モードで開始され、初期化されます。また、「実行準備完了」のランタイム コンテキストを維持するために、アクティブな VSM と同期化され、最新の状態に保たれます。 • スイッチオーバーでは、スタンバイ VSM がアクティブ VSM の役目を引き継ぎます。

ネットワーク レベル ハイ アベイラビリティ

ネットワーク レベルでの Cisco Nexus 1000V HA には、ポート チャネルと Link Aggregation Control Protocol（LACP）が含まれます。ポート チャネルは、物理リンクをまとめて 1 つのチャネル グループに入れ、最大 8 つの物理リンクの帯域幅を集約した単一の論理リンクを作ります。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

さらに、LACP では最大 16 個のインターフェイスが 1 つのポート チャネルに入るように設定できます。最大 8 つのインターフェイスをアクティブにすることができ、最大 8 つのインターフェイスをスタンバイ状態に入れることができます。

ポート チャネルと LACP のその他の情報については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。

ハイ アベイラビリティでの問題

症状	考えられる原因	解決策
アクティブな VSM からスタンバイ VSM が見えない。	ロールが正しく設定されていない。 • **show system redundancy status** コマンドを使用して、2 つの VSM のロールをチェックします。	**1.** ロールがそれぞれプライマリ ロールとセカンダリ ロールになっていることを確認します。 **2.** 必要に応じて、**system redundancy role** コマンドを使用して、状況を修正します。 **3.** ロールを変更した場合は、設定を保存します。
	ネットワーク接続の問題。 • アップストリーム スイッチおよび仮想スイッチでの VSM 間の VLAN 接続の制御と管理をチェックします。	ネットワークの問題が存在する場合は、次の手順を実行します。 **1.** vSphere Client から、VSM（スタンバイ モードになっているはず）をシャットダウンします。 **2.** vSphere Client から、ネットワーク接続を復元させたあとに、スタンバイ VSM を UP にします。
アクティブ VSM がスタンバイ VSM と完全に同期化されていない。	VSM 間のバージョンの不一致。 • **show version** コマンドを使用して、プライマリ VSM とセカンダリ VSM が同じイメージ バージョンを使用しているかチェックします。	アクティブ VSM とスタンバイ VSM のソフトウェア バージョンが異なる場合は、セカンダリ VSM をプライマリ VSM で使用されているのと同じバージョンで再インストールします。
	gsync プロセス中に致命的なエラーが発生した。 • **show system internal log sysmgr gsyncctrl** コマンドを使用して gsyncctrl ログをチェックし、致命的なエラーを探します。	**reload module** *module-number* コマンドを使用して、スタンバイ VSM を再ロードします。*module-number* は、スタンバイ VSM のモジュール番号です。

症状	考えられる原因	解決策
スタンバイ VSM が周期的に再起動される。	VSM が管理インターフェイスを通じてしか接続を持っていない。 • VSM が管理インターフェイスを通じては通信できるけれでも、制御インターフェイスを通じては通信できない場合、アクティブ VSM がその状況を検出し、2 つの VSM が HA モードになって同期が取れなくなるのを防ぐために、スタンバイ VSM をリセットします。 • **show system internal redundancy info** コマンドの出力をチェックして、*degraded_mode* フラグが true に設定されていることを確認します。	プライマリ VSM とセカンダリ VSM の間の制御 VLAN 接続をチェックします。
	VSM のバージョンが異なる。 **debug system internal sysmgr all** コマンドを入力して、バージョンの不一致を示す active_verctrl エントリを探します。次のような出力が表示されます。 `2009 May  5 08:34:15.721920 sysmgr: active_verctrl: Stdby running diff version- force download the standby sup.`	スタンバイ VSM を分離してから、起動します。 **show version** コマンドを使用して、両方の VSM のソフトウェア バージョンをチェックします。 アクティブ VSM と同じバージョンのイメージをスタンバイ VSM にインストールします。

症状	考えられる原因	解決策
両方の VSM がアクティブモードになる。	ネットワーク接続の問題。 • アップストリームと仮想スイッチで、VSM 間の制御 VLAN 接続と管理 VLAN 接続を調べます。 • VSM がこの 2 つのインターフェイスのどちらを介しても通信できない場合、その両方がアクティブ VSM になろうとします。	ネットワークの問題が存在する場合は、次の手順を実行します。 **1.** vSphere Client から、VSM（スタンバイ モードになっているはず）をシャットダウンします。 **2.** vSphere Client から、ネットワーク接続を復元させたあとに、スタンバイ VSM を UP にします。
	2 つの VSM でのドメイン ID が異なる。 **show system internal redundancy info** コマンドを使用して、*domain* 値を調べます。	必要であれば、ドメイン ID を更新し、それをスタートアップ コンフィギュレーションに保存します。 • デュアル VSM システムでドメイン ID をアップグレードする場合は、決まった手順に従う必要があります。 – 正しいドメイン ID を持つ VSM を分離して、他方の VSM と通信できないようにします。 – 分離した VSM でドメイン ID を変更し、設定を保存し、VSM の電源を切ります。 – 分離した VSM を再接続し、電源を入れます。

ハイ アベイラビリティのトラブルシューティング コマンド

ここでは、ハイ アベイラビリティに関する問題のトラブルシューティングに使用できるコマンドを示します。

プロセス ログとコアのリストを表示するには、次のコマンドを使用します。

- **show cores**

```
n1000V# show cores
VDC No Module-num       Process-name      PID     Core-create-time
------ ----------       ------------      ---     ----------------
1      1                private-vlan      3207    Apr 28 13:29
```

- **show processes log [pid** *pid***]**

```
n1000V# show processes log
VDC Process          PID     Normal-exit  Stack  Core   Log-create-time
--- ---------------  ------  -----------  -----  -----  ---------------
  1 private-vlan     3207              N      Y      N  Tue Apr 28 13:29:48 2009

n1000V# show processes log pid 3207
=====================================================
Service: private-vlan
Description: Private VLAN
```

```
Started at Wed Apr 22 18:41:25 2009 (235489 us)
Stopped at Tue Apr 28 13:29:48 2009 (309243 us)
Uptime: 5 days 18 hours 48 minutes 23 seconds

Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2) <-- Reason for the process abort
Last heartbeat 46.88 secs ago
System image name: nexus-1000v-mzg.4.0.4.SV1.1.bin
System image version: 4.0(4)SV1(1) S25

PID: 3207
Exit code: signal 6 (core dumped) <-- Indicates that a cores for the process was
generated.

CWD: /var/sysmgr/work
...
```

冗長性ステータスをチェックするには、次のコマンドを使用します。

- **show system redundancy status**

```
N1000V# show system redundancy status
Redundancy role
---------------
      administrative:   primary <-- Configured redundancy role
         operational:   primary <-- Current operational redundancy role

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

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

Other supervisor (sup-2)
------------------------
    Redundancy state:   Standby <-- Redundancy state of the other VSM
    Supervisor state:   HA standby
      Internal state:   HA standby <-- The standby VSM is in HA mode and in sync
```

システム内部の冗長性ステータスをチェックするには、次のコマンドを使用します。

- **show system internal redundancy info**

```
n1000V# show system internal redundancy info
My CP:
  slot: 0
  domain: 184 <-- Domain id used by this VSM
  role:   primary <-- Redundancy role of this VSM
  status: RDN_ST_AC <-- Indicates redundancy state (RDN_ST) of the this VSM is Active
(AC)
  state:  RDN_DRV_ST_AC_SB
  intr:   enabled
  power_off_reqs: 0
  reset_reqs:     0
Other CP:
  slot: 1
  status: RDN_ST_SB <-- Indicates redundancy state (RDN_ST) of the other VSM is
Standby (SB)
  active: true
```

```
  ver_rcvd: true
  degraded_mode: false <-- When true, it indicates that communication through the
control interface is faulty
Redun Device 0: <-- This device maps to the control interface
  name: ha0
  pdev: ad7b6c60
  alarm: false
  mac: 00:50:56:b7:4b:59
  tx_set_ver_req_pkts:   11590
  tx_set_ver_rsp_pkts:   4
  tx_heartbeat_req_pkts: 442571
  tx_heartbeat_rsp_pkts: 6
  rx_set_ver_req_pkts:   4
  rx_set_ver_rsp_pkts:   1
  rx_heartbeat_req_pkts: 6
  rx_heartbeat_rsp_pkts: 442546 <-- Counter should be increasing, as this indicates
that communication between VSM is working properly.
  rx_drops_wrong_domain: 0
  rx_drops_wrong_slot:   0
  rx_drops_short_pkt:    0
  rx_drops_queue_full:   0
  rx_drops_inactive_cp:  0
  rx_drops_bad_src:      0
  rx_drops_not_ready:    0
  rx_unknown_pkts:       0
Redun Device 1: <-- This device maps to the mgmt interface
  name: ha1
  pdev: ad7b6860
  alarm: true
  mac: ff:ff:ff:ff:ff:ff
  tx_set_ver_req_pkts:   11589
  tx_set_ver_rsp_pkts:   0
  tx_heartbeat_req_pkts: 12
  tx_heartbeat_rsp_pkts: 0
  rx_set_ver_req_pkts:   0
  rx_set_ver_rsp_pkts:   0
  rx_heartbeat_req_pkts: 0
  rx_heartbeat_rsp_pkts: 0 <-- When communication between VSM through the control
interface is interrupted but continues through the mgmt interface, the
rx_heartbeat_rsp_pkts will increase.
  rx_drops_wrong_domain: 0
  rx_drops_wrong_slot:   0
  rx_drops_short_pkt:    0
  rx_drops_queue_full:   0
  rx_drops_inactive_cp:  0
  rx_drops_bad_src:      0
  rx_drops_not_ready:    0
  rx_unknown_pkts:       0
```

システム内部の sysmgr ステータスをチェックするには、次のコマンドを使用します。

- **show system internal sysmgr state**

```
N1000V# show system internal sysmgr state

The master System Manager has PID 1988 and UUID 0x1.
Last time System Manager was gracefully shutdown.
The state is SRV_STATE_MASTER_ACTIVE_HOTSTDBY entered at time Tue Apr 28 13:09:13
2009.

The '-b' option (disable heartbeat) is currently disabled.

The '-n' (don't use rlimit) option is currently disabled.
```

```
Hap-reset is currently enabled.

Watchdog checking is currently disabled.

Watchdog kgdb setting is currently enabled.


        Debugging info:

The trace mask is 0x00000000, the syslog priority enabled is 3.
The '-d' option is currently disabled.
The statistics generation is currently enabled.


        HA info:

slotid = 1    supid = 0
cardstate = SYSMGR_CARDSTATE_ACTIVE .
cardstate = SYSMGR_CARDSTATE_ACTIVE (hot switchover is configured enabled).
Configured to use the real platform manager.
Configured to use the real redundancy driver.
Redundancy register: this_sup = RDN_ST_AC, other_sup = RDN_ST_SB.
EOBC device name: eth0.
Remote addresses:  MTS - 0x00000201/3      IP - 127.1.1.2
MSYNC done.
Remote MSYNC not done.
Module online notification received.
Local super-state is: SYSMGR_SUPERSTATE_STABLE
Standby super-state is: SYSMGR_SUPERSTATE_STABLE
Swover Reason : SYSMGR_SUP_REMOVED_SWOVER <-- Reason for the last switchover
Total number of Switchovers: 0 <-- Number of switchovers
                              >> Duration of the switchover would be listed, if any.

        Statistics:

Message count:           0
Total latency:           0              Max latency:             0
Total exec:              0              Max exec:                0
```

モジュールを再ロードするには、次のコマンドを使用します。

- **reload module**

  ```
  n1000V# reload module 2
  ```

  このコマンドは、セカンダリ VSM を再ロードします。

（注）　モジュールを指定せずに **reload** コマンドを実行すると、システム全体が再ロードされます。

スタンバイ VSM コンソールに接続するには、次のコマンドを使用します。

- **attach module**

  スタンバイ VSM コンソールには、外部からはアクセスできません。アクセスするには、アクティブ VSM から **attach module** *module-number* コマンドを使用します。

  ```
  n1000V# attach module 2
  ```

  このコマンドは、セカンダリ VSM のコンソールに接続します。

CHAPTER 7

VSM および VEM モジュール

この章では、モジュールに関連する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「モジュールについて」（P.7-1）
- 「VSM にモジュールが表示されない場合のトラブルシューティング」（P.7-1）
- 「VSM の問題」（P.7-4）
- 「VSM および VEM のトラブルシューティング コマンド」（P.7-15）

モジュールについて

Cisco Nexus 1000V は、VirtualCenter で定義されたデータセンターを管理します。データセンター内の各サーバは、Nexus 1000V の 1 つのモジュールとして表され、物理的なシスコ スイッチ内のモジュールと同じように管理できます。

Cisco Nexus 1000V の実装は、次の 2 つの部分で構成されます。

- 仮想スーパーバイザ モジュール（VSM）：Cisco Nexus 1000V Distributed Virtual Switch（DVS; 分散仮想スイッチ）の制御ソフトウェア。NX-OS ソフトウェアに基づいており、仮想マシン（VM）上で実行されます。
- 仮想イーサネット モジュール（VEM）：Cisco Nexus 1000V で実際にデータ トラフィックのスイッチングを行う部分。VMware ESX 4.0 ホスト上で実行されます。複数の VEM が、1 つの VSM によって制御されます。スイッチ ドメインを形成するすべての VEM が、VMware VirtualCenter で定義されたとおりに同一の仮想データセンター内になくてはなりません。

VSM にモジュールが表示されない場合のトラブルシューティング

このセクションでは、VSM 上にモジュールが表示されない場合に使用できるプロセスについて説明します。ここでは、次の内容について説明します。

- 「モジュールのトラブルシューティングに関する注意事項」（P.7-2）
- 「モジュールのトラブルシューティングのフローチャート」（P.7-3）
- 「VSM が vCenter Server に接続されているかどうかの確認」（P.7-6）
- 「VSM が正しく設定されているかどうかの確認」（P.7-7）
- 「vCenter Server 設定の確認」（P.7-9）

- 「VSM と VEM の間のネットワーク接続の確認」（P.7-9）
- 「VEM 設定の確認」（P.7-11）
- 「ログの収集」（P.7-14）

モジュールのトラブルシューティングに関する注意事項

VSM によって制御されているモジュールのトラブルシューティング時には、次の注意事項に従ってください。

- VSM VM および VEM が起動し、動作している必要があります。
- 互換性のあるバージョンの vCenter Server および VSM が動作していることを確認します。

  詳細については、『*Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*』を参照してください。
- vCenter Server の IP アドレスを ping して、VSM と vCenter Server の間のネットワーク接続を確認します。Domain Name Service（DNS; ドメイン ネーム サービス）名を使用している場合は、その DNS 名を使用して ping します。vCenter Server の ping に失敗した場合は、ゲートウェイを ping できるかどうかを調べます。それ以外の場合は、mgmt0 インターフェイスのコンフィギュレーション設定を調べます。
- vCenter Server のファイアウォール設定がオフになっていることを確認します。ファイアウォール設定を使用する場合は、次のポートが開いているかどうかを調べます。
  - ポート 80
  - ポート 443
- 次のエラーが表示された場合は、VSM 拡張が vCenter Server から作成されているかどうかを確認します。
  - ERROR: [VMware vCenter Server 4.0.0 build-150489]
    Extension key was not registered before its use

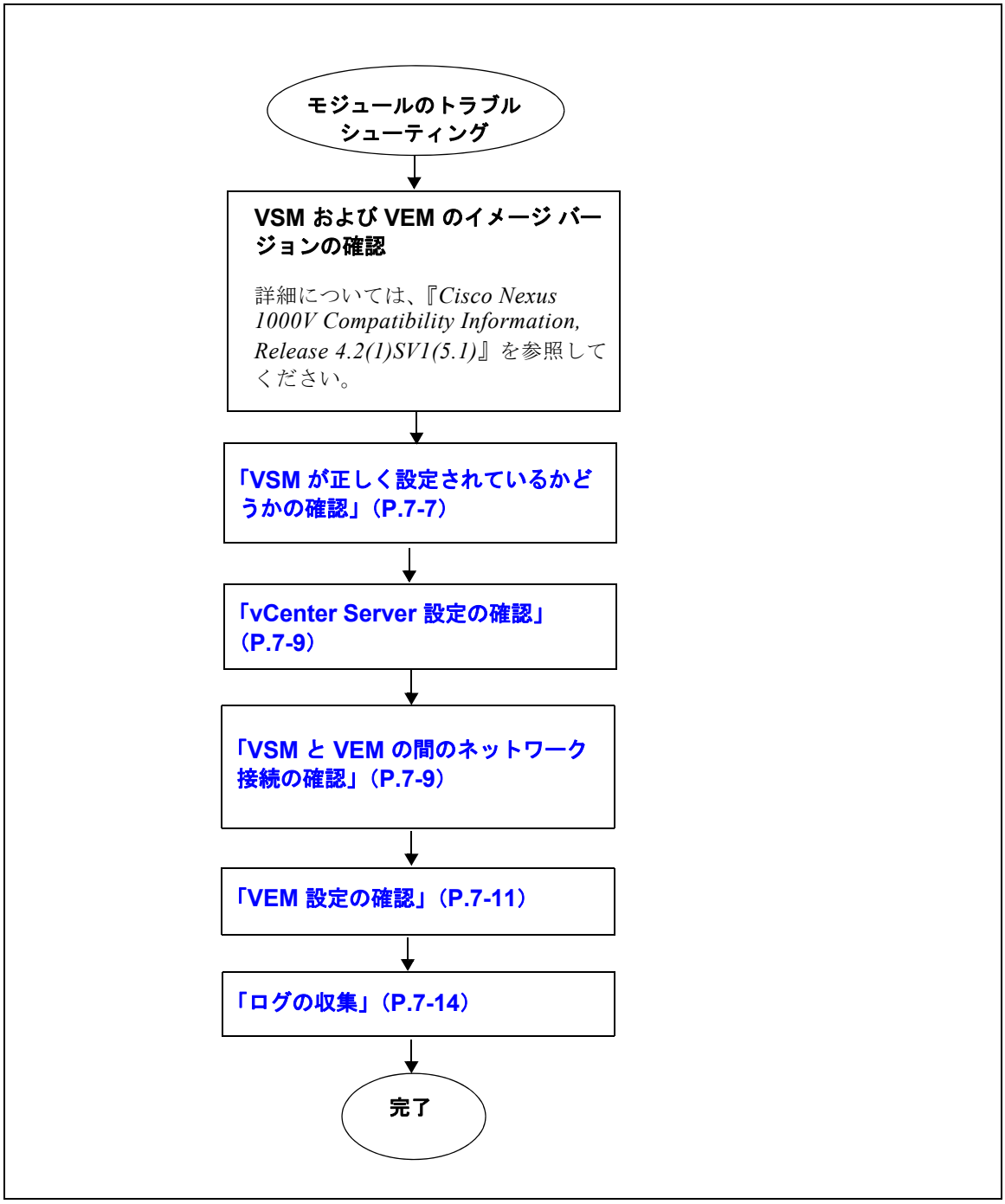
  拡張またはプラグインが作成されたことを確認するには、「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）の手順を参照してください。

  拡張キーまたはプラグインの詳細については、「拡張キーの管理」（P.3-7）を参照してください。
- 次のエラーが表示された場合は、「vCenter Server 設定の確認」（P.7-9）の手順を参照してください。
  - ERROR: Datacenter not found
- Cisco Nexus 1000V で使用される用語のリストについては、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

モジュールのトラブルシューティングのフローチャート

モジュールのトラブルシューティングには、次のフローチャートを使用します。

フローチャート：モジュールのトラブルシューティング



VSM の問題

次に、VSM の問題について現象、考えられる原因、および解決方法を示します。

表 7-1　VSM の問題

症状	考えられる原因	解決策

VSM で次のエラーが表示される。
`ERROR: [VMware vCenter Server 4.0.0 build-150489]`
`Extension key was not registered before its use`
	VSM に拡張またはプラグインが作成されていない。	**1.** 拡張またはプラグ インが作成されたことを確認します。
		「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）の手順
		2. プラグインが見つからない場合は、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』にある次の手順を使用してプラグインを作成します。
		「Creating a Cisco Nexus 1000V Plug-In on the vCenter Server」

VSM のリブート後にシステムが次のいずれかの状態で機能停止し、それ自体では回復しない。デバッグの試みが失敗する。		
ブート後に、VSM がローダー プロンプトに入る。	VSM キックスタート イメージが破損している。	**1.** CD ROM から VSM をブートします。 **2.** [CD Boot] メニューから、[Option 1, Install Nexus1000v and bring up new image] を選択します。 VSM インストール手順に従ってください。
	ブート変数が設定されていない。	**1.** CD ROM から VSM をブートします。 **2.** [CD Boot] メニューから、[Option 3, Install Nexus1000v only if the disk unformatted and bringup new image] を選択します。 **3.** VSM のブートに使用するブート変数を設定します。 **boot system bootflash:***system-boot-variable-name* **boot kickstart bootflash:***kickstart-boot-variable-name* **4.** VSM をリロードします。 **reload**
ブート後に、VSM がブート プロンプトに入る。	VSM システム イメージが破損している。	**1.** CD ROM から VSM をブートします。 **2.** [CD Boot] メニューから、[Option 1, Install Nexus1000v and bring up new image] を選択します。 **3.** VSM インストール手順に従ってください。

表 7-1　（続き）VSM の問題

症状	考えられる原因	解決策
ブート後に、VSM が再設定される。	スタートアップ コンフィギュレーションが削除されている。	次のいずれかを実行します。 • コンフィギュレーション ファイルのバックアップ コピーを保存している場合は、VSM でそのコンフィギュレーションを復元します。 **copy** *source filesystem: filename* **system:running-config** • 保存していない場合は、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』の次の項を使用して、VSM を再設定します。 ソフトウェアのセットアップ
ブート後に、VSM が「Loader Loading」で停止した。	ブート メニュー ファイルが破損している。	**1.** CD ROM から VSM をブートします。 **2.** [CD Boot] メニューから、[Option 3, Install Nexus1000v only if the disk unformatted and bringup new image] を選択します。 **3.** 次のいずれかを実行します。 • コンフィギュレーション ファイルのバックアップ コピーを保存している場合は、VSM でそのコンフィギュレーションを復元します。 **copy** *source filesystem: filename* **system:running-config** • 保存していない場合は、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』の次の項を使用して、VSM を再設定します。 ソフトウェアのセットアップ
ブート後に、セカンダリ VSM が引き続き再起動する。	コントロール VLAN またはコントロール インターフェイスがダウンする。	アクティブ VSM とスタンバイ VSM 間の制御接続をチェックします。
	アクティブ VSM およびスタンバイ VSM が同期に失敗した。	アクティブ VSM から、gsyncstats をチェックして、障害を発生させたアプリケーションを識別します。 **show logging**

VSM が vCenter Server に接続されているかどうかの確認

次の手順に従って、VSM が vCenter Server に接続されていることを確認できます。

ステップ 1　VSM と vCenter Server の間の接続を確認します。

show svs connections

出力に、動作ステータスが「**Connected**」と表示される必要があります。

例：
```
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

ステップ 2　次のいずれかを実行します。

- ステータスが「**Connected**」の場合は、「フローチャート：モジュールのトラブルシューティング」（P.7-3）に戻ります。
- 「Connected」でない場合は、次のステップに進みます。

ステップ 3　vCenter Server に接続します。

config t

svs connection *datacenter_name*

connect

例：
```
n1000v# conf t
n1000v(config)# svs connection HamiltonDC
n1000v(config-svs-conn)# connect
```

例：
```
n1000v# conf t
n1000v(config)# svs connection HamiltonDC
n1000v(config-svs-conn)# connect
ERROR: [VMWARE-VIM] Extension key was not registered before its use.
```

ステップ 4　次のいずれかを実行します。

- 拡張キーに関するエラー メッセージが表示されたら、次のステップ表 7-1 に進みます。
- 表示されない場合は、ステップ 6 に進みます。

ステップ 5　次のいずれかを行ってから、ステップ 6 に進みます。

- 「vCenter Server の拡張キーの登録解除」（P.3-13）の手順を使用して拡張キーを登録解除します。
- 『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』の次の手順を使用して、新しい拡張キーをインストールします。
  - 「*Creating a Cisco Nexus 1000V Plug-In on the vCenter Server*」

ステップ 6　VSM と vCenter Server の間の接続を確認します。

show svs connections

出力に、動作ステータスが「**Connected**」と表示される必要があります。

例：
```
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

ステップ 7　次のいずれかを実行します。

- ステータスが「**Connected**」の場合は、この手順は完了しています。
- 「Connected」でない場合は、「フローチャート：モジュールのトラブルシューティング」（P.7-3）に戻ります。

VSM が正しく設定されているかどうかの確認

ここでは、VSM 設定の確認手順について説明します。

- 「ドメイン設定の確認」（P.7-7）
- 「システム ポート プロファイル設定の確認」（P.7-8）
- 「コントロールおよびパケット VLAN の設定の確認」（P.7-8）

ドメイン設定の確認

次の手順に従って、ドメイン設定を確認できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- **show svs domain** コマンドの出力が、次のことを示している。
  - コントロール VLAN とパケット VLAN の存在。
  - ドメイン設定が正常に VC にプッシュされている。

ステップ 1　VSM で、ドメイン設定を確認します。

show svs domain

例：
```
n1000v# show svs domain
SVS domain config:
  Domain id:     682
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Control VLAN mode: L2
  L2/L3 Control VLAN interface: mgmt0
  Status: Config push to VC successful
```

システム ポート プロファイル設定の確認

次の手順に従って、ポート プロファイルの設定を確認できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- **show port-profile name** コマンドの出力が次のことを示している。
  - システム VLAN が vEthernet タイプである（デフォルト）。
  - コントロール VLAN およびパケット VLAN が割り当てられている。
  - ポート プロファイルがイネーブルになっている。
  - デフォルト以外のシステム MTU を設定している場合、適切なサイズになっている。

ステップ 1　VSM で、システム ポート プロファイル設定を確認します。

show port-profile name *system-port-profile-name*

例：

```
n1000v# show port-profile name SystemUplink
port-profile SystemUplink
  description:
  type: vethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group: SystemUplink
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    system mtu 1500
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:
```

コントロールおよびパケット VLAN の設定の確認

次の手順を使用して、コントロール VLAN とパケット VLAN が VSM に設定されていることを確認できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

- **show running-config** コマンドの出力が、設定された VLAN 間のコントロール VLAN およびパケット VLAN の ID 番号を示している。

ステップ 1　VSM で、コントロール VLAN およびパケット VLAN が存在することを確認します。

```
n1000v# show running-config vlan 260-261
version 4.0(4)SV1(3)
vlan 260
  name cp_control
vlan 261
  name cp_packet

n1000v#
. . .
```

vCenter Server 設定の確認

vSphere クライアントから次の手順に従って、vCenter Server 設定を確認できます。

ステップ 1　データセンターとそのデータセンターの Cisco Nexus 1000V DVS に、ホストが追加されていることを確認します。

ステップ 2　ホストの 1 つ以上の pnic が DVS に追加され、その pnic が **system-uplink** プロファイルに割り当てられていることを確認します。

ステップ 3　コントロール VLAN、パケット VLAN、および管理ネットワークが含まれるポート グループに 3 つの VSM vnic が割り当てられていることを確認します。

VSM と VEM の間のネットワーク接続の確認

次の手順に従って、VSM と VEM の間のレイヤ 2 ネットワーク接続を確認できます。

ステップ 1　VSM 上で、その MAC アドレスを確認します。

show svs neighbors

VSM MAC アドレスは、AIPC Interface MAC として表示されます。

ホストのユーザ VEM Agent MAC アドレスは、Src MAC として表示されます。

例：

```
n1000v# show svs neighbors

Active Domain ID: 1030

AIPC Interface MAC: 0050-568e-58b7
Inband Interface MAC: 0050-568e-2a39

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
--------------------------------------------------------------------------

0002-3d44-0602     VEM      1030         0302     261058.59
```

ステップ 2　次のいずれかを実行します。

- ステップ 1 で **show svs neighbors** コマンドの出力に VEM MAC アドレスが表示されない場合は、VSM をホストしているサーバとアップストリーム スイッチの間の接続に問題があります。VSM 設定と vCenter Server 設定をもう一度調べてください。
- それ以外の場合は、次の手順に進みます。

ステップ 3　VEM 上で、ステップ 1 で見つかった VSM MAC アドレスを使用して、vem-health スクリプトを実行します。

（注）　そのパスに vem-health スクリプトがない場合は、/usr/lib/ext/cisco/nexus/vem*/sbin/ で見つけられます。

vem-health check *vsm_mac_address*

vem-health スクリプトの出力では、接続問題の原因と、トラブルシューティングで推奨される次のステップが示されます。

例：

```
~ # vem-health check  00:50:56:a3:36:90
VSM Control MAC address: 00:50:56:a3:36:90
Control VLAN: 90
DPA MAC: 00:02:3d:40:5a:03

VSM heartbeats are not reaching the VEM.
Your uplink configuration is correct.
Recommended action:
Check if the VEM's upstream switch has learned the VSM's Control MAC.
```

ステップ 4　次のいずれかを実行します。

- ステップ 3 の VEM ヘルス チェックでアップストリーム スイッチへの接続に問題があることが示された場合は、次のステップに進んでください。
- それ以外の場合は、ステップ 7 に進みます。

ステップ 5　アップストリーム スイッチで、MAC アドレス テーブルを表示してネットワーク設定を確認します。

例：

```
switch# show mac address-table interface Gi3/1 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  0050.56be.7ca7   dynamic  Yes          0   Gi3/1

switch# show mac address-table interface Gi3/2 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  00:02:3d:40:0b:0c   dynamic  Yes          0   Gi3/2
```

ステップ 6　次のいずれかを実行します。

- ステップ 5 の出力に VSM の MAC アドレスが表示されない場合は、VSM をホストしているサーバとアップストリーム スイッチとの間の接続に問題があります。VSM 設定と vCenter Server 設定をもう一度調べてください。
- それ以外の場合は、次の手順に進みます。

ステップ 7　VEM 上で次のコマンドを入力して、VSM MAC がコントロール VLAN とパケット VLAN に表示されることを確認します。

config t

module vem *module_number* **execute vemcmd show l2** *control_vlan_id*

module vem *module_number* **execute vemcmd show l2** *packet_vlan_id*

VSM eth0 と eth1 の MAC アドレスが、ホスト コントロール VLAN とパケット VLAN に表示される必要があります。

例：
```
n100v# config t
n1000v(config)# module vem 3 execute vemcmd show l2 3002
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:40:0b:0c  LTL    10 pvlan     0 timeout   110

n1000v(config)# module vem 3 execute vemcmd show l2 3003
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:20:0b:0c  LTL    10 pvlan     0 timeout   110
```

ステップ 8　次のいずれかを実行します。

- VSM の MAC アドレスがステップ 7 の出力に表示されない場合は、「VEM 設定の確認」（P.7-11）の説明に従って VEM 設定を調べます。
- それ以外の場合は、この手順は完了です。

VEM 設定の確認

次の手順に従って、ESX ホストが VEM 設定を受け取り、セットアップされていることを確認できます。

ステップ 1　ESX ホスト上で次のコマンドを使用して、VEM エージェントが稼動しており、正しいホスト リンクが DVS に追加されていることを確認します。

vem status

例：
```
~ # vem status
VEM modules are loaded

Switch Name     Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0        64          3           64                1500    vmnic0
DVS Name        Num Ports   Used Ports  Configured Ports  Uplinks
n1000v          256         9           256               vmnic1 VEM Agent is running
```

ステップ 2　次のコマンドを使用して、アップリンク上の間違った MTU 値が原因で失われた接続を復元します。

vemcmd show port *port-LTL-number*

vemcmd set mtu *value* **ltl** *port-LTL-number*

例：
```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode Name
. . .
17   1a030100      1 T   304      1          32  PHYS     UP    UP    1  Trunk vmnic1
~# vemcmd set mtu 9000 ltl 17
```

（注）　これらの **vemcmd** コマンドは回復手段だけに使用して、システム アップリンクの場合はポート プロファイル設定内、システム以外のアップリンクの場合はインターフェイス設定内の MTU 値を更新します。

ステップ 3　次のコマンドを使用して、ドメイン ID、コントロール VLAN、およびパケット VLAN がホスト上に正しく設定されていることを確認します。

vemcmd show card

例：
```
~ # vemcmd show card
Card UUID type  2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: n1000v
Switch alias: DvsPortset-0
Switch uuid: 56 e0 36 50 91 1c 32 7a-e9 9f 31 59 88 0c 7f 76
Card domain: 1024
Card slot: 4
VEM Control (Control VLAN) MAC: 00:02:3d:14:00:03
VEM Packet (Inband) MAC: 00:02:3d:24:00:03
VEM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VEM SPAN MAC: 00:02:3d:34:00:03
Management IP address: 172.23.232.102
Max physical ports: 32
Max virtual ports: 216
Card control VLAN: 3002
Card packet VLAN: 3003
       Processors: 4
  Processor Cores: 4
Processor Sockets: 2
  Physical Memory: 4290351104
```

ステップ 4　次のコマンドを使用して、DVS に追加されているホストのポートが一覧表示され、各ポートがホスト上で「Access」または「Trunk」として正しく設定されていることを確認します。

vemcmd show port

例：
```
~ # vemcmd show port
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
8          0   3969       0      2           2  VIRT     UP    UP    1 Access l20
9          0   3969       0      2           2  VIRT     UP    UP    1 Access l21
10         0   3002       0      2           2  VIRT     UP    UP    1 Access l22
11         0   3968       0      2           2  VIRT     UP    UP    1 Access l23
12         0   3003       0      2           2  VIRT     UP    UP    1 Access l24
13         0      1       0      2           2  VIRT     UP    UP    0 Access l25
14         0   3967       0      2           2  VIRT     UP    UP    1 Access l26
16  1a030100      1 T     0      2           2  PHYS     UP    UP    1 Trunk vmnic1
```

出力の最後の行は、vmnic1 が Trunk モードで、CBL 値が 1 であることを示しています。ネイティブ VLAN の CBL 値は、1 である必要はありません。この値は、許可されていない場合は 0 になり、VLAN 1 で許可されていない場合は 1 になります。これは、ネイティブ VLAN がコントロール VLAN でない限り、問題にはなりません。管理状態（Admin）とポート状態（Port）は UP となります。

ステップ 5　次のコマンドを使用して、コントロール VLAN とパケット VLAN を伝送する vmnic ポートが存在することを確認します。

vemcmd show bd *control_vlan*
vemcmd show bd *packet_vlan*

例：
```
~ # vemcmd show bd 3002
BD 3002, vdc 1, vlan 3002, 2 ports
Portlist:
     10  l22
     16  vmnic1
~ # vemcmd show bd 3003
BD 3003, vdc 1, vlan 3003, 2 ports
Portlist:
     12  l24
     16  vmnic1
```

ステップ 6　**vemcmd show trunk** コマンドを使用して、次のことを確認します。

- コントロール VLAN とパケット VLAN がコマンド出力に示され、DV ポート グループが vCenter Server からホストに正常にプッシュされている。
- 正しい物理トランク ポート vmnic が使用されている。

例：
```
~ # vemcmd show trunk
Trunk port 16 native_vlan 1 CBL 1vlan(1) cbl 1, vlan(3002) cbl 1, vlan(3003) cbl 1,
```

少なくとも 1 つの物理アップリンクがコントロール VLAN とパケット VLAN を伝送している必要があります。また、複数のアップリンクがコントロール VLAN とパケット VLAN を伝送している場合、アップリンクは 1 つのポート チャネル プロファイルに属している必要があります。VEM をまだ VSM に追加していないため、ポート チャネル自体は表示されません。

ステップ 7　次のコマンドを使用して、ポートとシステム VLAN の間違った設定が原因で失われた接続を復元します。

vemcmd show port *port-ltl-number*

vemcmd set system-vlan *vlan_id* **ltl** *port-ltl-number*

例：
```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
. . .
48     1b030000     1       0     32           1 VIRT     UP  DOWN     0 Access vmk1
~ # vemcmd set system-vlan 99 ltl 48
```

（注）　これらの **vemcmd** は回復手段だけに使用して、ポート プロファイル設定を正しいシステム VLAN に更新します。

ログの収集

VEM と VSM の間のネットワーク接続を確認したら、次の手順に従ってログ ファイルを収集し、問題を識別できます。

ステップ 1　VEM 上で次のコマンドを使用して、その UUID を確認します。

vemcmd show card info

例：
```
~ # module vem 3 vemcmd show card info
Card UUID type  0: 4908a717-7d86-d28b-7d69-001a64635d18
Card name: sfish-srvr-7
Switch name: N1000v
Switch uuid: 50 84 06 50 81 36 4c 22-9b 4e c5 3e 1f 67 e5 ff
Card domain: 11
Card slot: 12
Control VLAN MAC: 00:02:3d:10:0b:0c
Inband MAC: 00:02:3d:20:0b:0c
SPAN MAC: 00:02:3d:30:0b:0c
USER DPA MAC: 00:02:3d:40:0b:0c
Management IP address: 172.28.30.56
Max physical ports: 16
Max virtual ports: 32
Card control VLAN: 3002
Card packet VLAN: 3003
```

ステップ 2　VSM 上で次のコマンドを使用して、該当する UUID エントリがマップされているモジュール番号を確認します。

show module vem mapping

例：
```
n1000v# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
60      absent          33393935-3234-5553-4538-35314e355400    unlicensed
66      powered-up      33393935-3234-5553-4538-35314e35545a    licensed
n1000v#
```

ステップ 3　ステップ 2 のモジュール番号を使用して、次のコマンドの出力を収集します。

- **show platform internal event-history module 13**
- **show module internal event-history module 13**
- **show system internal im event-history module 13**
- **show system internal vmm event-history module 13**
- **show system internal ethpm event-history module 13**

（注）　問題を解決する際に TAC に連絡する必要がある場合は、ステップ 3 に示されているコマンドの出力が必要になります。

VSM および VEM のトラブルシューティング コマンド

VSM に関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	説明
show svs neighbors	すべての svs ネイバーを表示します。 例 7-1（P.7-16）を参照してください。
show svs connections	Cisco Nexus 1000V の接続を表示します。 例 7-2（P.7-16）を参照してください。
show svs domain	ドメイン コンフィギュレーションを表示します。 例 7-3（P.7-17）を参照してください。
show port-profile name *name*	指定されたポート プロファイルの設定を表示します。 例 7-4（P.7-17）を参照してください。
show running-config vlan *vlanID*	実行コンフィギュレーションの VLAN 情報を表示します。 例 7-5（P.7-17）を参照してください。
vem-health check *vsm_**mac_address***	接続問題の原因を表示し、トラブルシューティングの次の手順を推奨します。 例 7-6（P.7-17）を参照してください。
show mac address-table interface	アップストリーム スイッチの MAC アドレス テーブルを表示し、ネットワーク設定を確認します。 例 7-7（P.7-18）を参照してください。
module vem *module_number* **execute vemcmd show l2** [*control_vlan_id* | *packet_vlan_id*]	VEM 上の VLAN 設定を表示し、VSM の MAC がコントロール VLAN およびパケット VLAN に表示されることを確認します。 例 7-8（P.7-18）を参照してください。
vem status	VEM の状態を表示して、VEM エージェントが稼動しており、正しいホスト アップリンクが DVS に追加されていることを確認します。 例 7-9（P.7-18）を参照してください。
vemcmd show card	VEM 上のカードの情報を表示して、ドメイン ID、コントロール VLAN、およびパケット VLAN がホストに正しく設定されていることを確認します。 例 7-10（P.7-18）を参照してください。
vemcmd show port [*port-LTL-number*]	VEM 上のポートの情報を表示して、DVS に追加されているホストのポートが一覧表示され、各ポートがホスト上で access または trunk として正しく設定されていることを確認します。 例 7-11（P.7-19）を参照してください。 例 7-12（P.7-19）を参照してください。

コマンド	説明
vemcmd show bd [*control_vlan_id* | *packet_vlan_id*]	VEM に設定されている情報を表示して、コントロール VLAN とパケット VLAN を伝送する VM NIC ポートが存在することを確認します。 例 7-13（P.7-19）を参照してください。
vemcmd show trunk	VEM に設定されている情報を表示して、DV ポート グループが vCenter Server からホストに正常にプッシュされること、また、適切な物理トランク ポートの VM NIC が使用されていることを確認します。 例 7-14（P.7-19）を参照してください。
show module vem mapping	VSM に接続された VEM の情報（VEM モジュール番号、ステータス、UUID、およびライセンス ステータスなど）を表示します。 例 7-15（P.7-19）を参照してください。
show platform internal event-history module *module-number*	プラットフォーム FSM イベントの情報を表示します。
show module internal event-history module *module-number*	モジュールのイベント ログを表示します。
show system internal im event-history module *module-number*	システムに関するモジュールの IM イベント ログを表示します。
show system internal vmm event-history module *module-number*	システムに関するモジュールの VMM イベント ログを表示します。
show system internal ethpm event-history module *module-number*	システムに関するモジュールのイーサネット イベント ログを表示します。
show system internal ethpm event-history int *type slot*	システムに関するイーサネット インターフェイスのログを表示します。

例 7-1　show svs neighbors

```
n1000v# show svs neighbors

Active Domain ID: 113

AIPC Interface MAC: 0050-56b6-2bd3
Inband Interface MAC: 0050-56b6-4f2d

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
--------------------------------------------------------------------------

0002-3d40-7102     VEM       113         0302     71441.12
0002-3d40-7103     VEM       113         0402       390.77

n1000v#
```

例 7-2　show svs connections

```
n1000v# show svs connections
connection vc:
    ip address: 172.23.231.223
    protocol: vmware-vim https
    certificate: user-installed
```

```
    datacenter name: hamilton-dc
    DVS uuid: 92 7a 14 50 05 11 15 9c-1a b0 f2 d4 8a d7 6e 6c
    config status: Disabled
    operational status: Disconnected
```

例 7-3　show svs domain

```
n1000v# show svs domain
SVS domain config:
  Domain id:    682
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Control VLAN mode: L2
  L2/L3 Control VLAN interface: mgmt0
  Status: Config push to VC successful
```

例 7-4　show port-profile

```
n1000v# show port-profile name SystemUplink
port-profile SystemUplink
  description:
  type: vethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: 114,115
  port-group: SystemUplink
  max ports: 32
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    system mtu 1500
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan all
    no shutdown
  assigned interfaces:
```

例 7-5　show running-configuration vlan

```
n1000v# show running-config vlan 260-261
version 4.0(4)SV1(3)
vlan 260
  name cp_control
vlan 261
  name cp_packet

n1000v#
```

例 7-6　vem-health check

```
~ # vem-health check  00:50:56:a3:36:90
VSM Control MAC address: 00:50:56:a3:36:90
Control VLAN: 90
DPA MAC: 00:02:3d:40:5a:03

VSM heartbeats are not reaching the VEM.
Your uplink configuration is correct.
```

```
Recommended action:
Check if the VEM's upstream switch has learned the VSM's Control MAC.
```

例 7-7　show mac address-table interface

```
switch# show mac address-table interface Gi3/1 vlan 3002
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Active Supervisor:
* 3002  0050.56be.7ca7   dynamic  Yes          0   Gi3/1
```

例 7-8　module vem execute vemcmd show l2

```
n100v# config t
n1000v(config)# module vem 3 execute vemcmd show l2 3002
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:40:0b:0c  LTL    10 pvlan     0 timeout   110

n1000v(config)# module vem 3 execute vemcmd show l2 3003
Bridge domain 3002 brtmax 100, brtcnt 3, timeout 120
    Dynamic MAC 00:50:56:be:7c:a7  LTL    16 pvlan     0 timeout   110
    Dynamic MAC 00:02:3d:20:0b:0c  LTL    10 pvlan     0 timeout   110
```

例 7-9　vem status

```
~ # vem status
VEM modules are loaded

Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          3           64                1500    vmnic0
DVS Name       Num Ports   Used Ports  Configured Ports  Uplinks
n1000v         256         9           256               vmnic1 VEM Agent is running
```

例 7-10　vemcmd show card

```
~ # vemcmd show card
Card UUID type  2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
Card name: sfish-srvr-1
Switch name: n1000v
Switch alias: DvsPortset-0
Switch uuid: 56 e0 36 50 91 1c 32 7a-e9 9f 31 59 88 0c 7f 76
Card domain: 1024
Card slot: 4
VEM Control (Control VLAN) MAC: 00:02:3d:14:00:03
VEM Packet (Inband) MAC: 00:02:3d:24:00:03
VEM Control Agent (DPA) MAC: 00:02:3d:44:00:03
VEM SPAN MAC: 00:02:3d:34:00:03
Management IP address: 172.23.232.102
Max physical ports: 32
Max virtual ports: 216
Card control VLAN: 3002
Card packet VLAN: 3003
       Processors: 4
  Processor Cores: 4
Processor Sockets: 2
  Physical Memory: 4290351104
```

例 7-11　vemcmd show port

```
~ # vemcmd show port
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
8          0   3969       0      2           2  VIRT     UP    UP    1 Access l20
9          0   3969       0      2           2  VIRT     UP    UP    1 Access l21
10         0   3002       0      2           2  VIRT     UP    UP    1 Access l22
11         0   3968       0      2           2  VIRT     UP    UP    1 Access l23
12         0   3003       0      2           2  VIRT     UP    UP    1 Access l24
13         0      1       0      2           2  VIRT     UP    UP    0 Access l25
14         0   3967       0      2           2  VIRT     UP    UP    1 Access l26
16  1a030100      1 T     0      2           2  PHYS     UP    UP    1 Trunk vmnic1
```

例 7-12　vemcmd show port

```
~ # vemcmd show port 48
LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode
Name  . . .
17   1a030100      1 T   304      1          32  PHYS     UP    UP    1  Trunk vmnic1
```

例 7-13　vemcmd show bd

```
~ # vemcmd show bd 3002
BD 3002, vdc 1, vlan 3002, 2 ports
Portlist:
     10  l22
     16  vmnic1
```

例 7-14　vemcmd show trunk

```
~ # vemcmd show trunk
Trunk port 16 native_vlan 1 CBL 1vlan(1) cbl 1, vlan(3002) cbl 1, vlan(3003) cbl 1,
```

例 7-15　show module vem mapping

```
n1000v# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
60      absent          33393935-3234-5553-4538-35314e355400    unlicensed
66      powered-up      33393935-3234-5553-4538-35314e35545a    licensed
n1000v#
```

CHAPTER 8

ポート

この章では、ポートに関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「ポートの概要」（P.8-1）
- 「ポート診断チェックリスト」（P.8-3）
- 「ポートの問題」（P.8-3）
- 「ポートのトラブルシューティング コマンド」（P.8-8）

ポートの概要

ここでは、次の内容について説明します。

- 「インターフェイスの特性の概要」（P.8-1）
- 「インターフェイス カウンタの概要」（P.8-2）
- 「リンク フラッピングの概要」（P.8-2）
- 「ポート セキュリティの概要」（P.8-2）

インターフェイスの特性の概要

スイッチで 1 つのデータ リンクから別のデータ リンクへのフレーム リレーを行うには、フレームが送受信されるインターフェイスの特性を定義する必要があります。設定されるインターフェイスは、イーサネット（物理）インターフェイス、仮想イーサネット インターフェイス（mgmt0）、および管理インターフェイス（mgmt0）です。

各インターフェイスには、次の設定があります。

- 管理設定

  管理設定は、修正を加えない限り変更されません。この設定には、管理モードで設定できる属性があります。

- 動作状態

  指定された属性（インターフェイス速度など）の動作状態。この状態は読み取り専用なので、変更できません。インターフェイスがダウンしているときは、一部の値（動作速度など）が有効にならない場合があります。

ポート モード、管理状態、および動作状態の詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

インターフェイス カウンタの概要

ポート カウンタは、同期問題の識別に使用されます。カウンタから、受信されたフレームと送信されたフレームの大きな差異を知ることができます。インターフェイス カウンタを表示するには、次のコマンドを使用します。

show interface ethernet *slot number* ***counters***

例 8-11（P.8-12）を参照してください。

長期間にわたってアクティブになっていたポートの場合、カウンタに格納されている値は意味を持たないことがあります。カウンタをクリアすることにより、現時点での実際のリンクの動作をより正確に把握できます。最初に、カウンタをクリアしてベースラインを作成します。

clear counters interface ethernet *slot-number*

リンク フラッピングの概要

ポートがアップとダウンを繰り返す状態をフラッピングといい、リンク フラッピングと呼ばれる場合もあります。ポートでフラッピングが発生すると、ポート状態が次の順序で変化し、一巡すると、最初の状態に戻って繰り返します。

1. Initializing：リンクを初期化しています。
2. Offline：ポートはオフライン状態です。
3. Link failure or not connected：物理層リンクが動作不能で、アクティブなデバイス接続がありません。

リンク フラッピングをトラブルシューティングするには、「リンク フラッピングの概要」（P.8-2）を参照してください。

ポート セキュリティの概要

ポート セキュリティ機能を使用すると、ポートにアクセスできる MAC アドレスを制限および識別することによってポートをセキュリティで保護できます。セキュア MAC は、手動で設定するか、ダイナミックに学習されます。

ポート セキュリティの詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ポートのタイプ	ポート セキュリティのサポートの有無
vEthernet アクセス	Yes
vEthernet トランク	Yes
vEthernet SPAN 宛先	No
スタンドアロンのイーサネット インターフェイス	No
ポート チャネル メンバー	No

ポート セキュリティの問題をトラブルシューティングするには、次の項を参照してください。

- 「VM から保護されたポートに ping できない」（P.8-6）
- 「ポート セキュリティ違反」（P.8-7）

ポート診断チェックリスト

次のチェックリストを使用して、ポート インターフェイス アクティビティを診断します。

ポート状態の詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

表 8-1　ポート診断チェックリスト

チェックリスト	例	√
モジュールがアクティブであることを確認します。 **show module**	例 8-1（P.8-10）を参照してください。	
VSM が vCenter Server に接続されていることを確認します。 **show svs connections**	例 8-3（P.8-10）を参照してください。	
vCenter Server に接続された vSphere Client で、必要なポート プロファイルが物理 NICS と仮想 NICS に割り当てられていることを確認します。		
ポートが作成されていることを確認します。 **show interface brief**	例 8-8（P.8-11）を参照してください。	
インターフェイスの状態を確認します。 **show interface ethernet**	例 8-10（P.8-12）を参照してください。	

ポートの問題

ここでは、次の現象に対して考えられる原因および解決方法について説明します。

- 「インターフェイスをイネーブルにできない」（P.8-4）
- 「ポートのリンク障害またはポートの非接続」（P.8-4）
- 「リンク フラッピング」（P.8-5）
- 「ポート errdisable」（P.8-5）
- 「VM から保護されたポートに ping できない」（P.8-6）
- 「ポート セキュリティ違反」（P.8-7）

インターフェイスをイネーブルにできない

イネーブルにできないインターフェイスをトラブルシューティングするには、次の注意事項に従ってください。

考えられる原因	解決策
レイヤ 2 ポートがアクセス VLAN に関連付けられていない、または VLAN が一時停止状態にある。	**1.** VLAN にインターフェイスが設定されていることを確認します。 **show interface brief** **2.** まだ設定されていない場合は、インターフェイスをアクセス VLAN に関連付けます。 **3.** VLAN の状態を判別します。 **show vlan brief** **4.** まだアクティブでない場合は、VLAN をアクティブとして設定します。 **config t** **vlan** *vlan-id* **state active**

ポートのリンク障害またはポートの非接続

リンク障害や非接続が解消されないポートをトラブルシューティングするには、次のガイドラインを使用してください。

表 8-2　リンク障害または非接続のポートのトラブルシューティング

考えられる原因	解決策
ポート接続が不良である。	**1.** ポートの状態を確認します。 **show system internal ethpm info** **2.** ポートをディセーブルにしてから、イネーブルにします。 **shut** **no shut** **3.** 同じモジュールまたは別のモジュール上の異なるポートに接続を移行します。 **4.** ESX 側の NIC 設定を収集します。 **vss-support**
リンクが初期化状態で停止している。または、リンクがポイントツーポイント状態になっている。	**1.** リンク障害システム メッセージがあるかどうかを確認します。 `Link Failure, Not Connected` **show logging** **2.** ポートをディセーブルにしてから、イネーブルにします。 **shut** **no shut** **3.** 同じモジュールまたは別のモジュール上の異なるポートに接続を移行します。 **4.** ESX 側の NIC 設定を収集します。 **vss-support**

リンク フラッピング

予期しないリンク フラッピングのトラブルシューティング時には、次の情報を把握することが重要です。

- リンク フラッピングを発生させたユーザ。
- リンク ダウンの実際の原因。
- リンク フラッピングの定義については、「リンク フラッピング」（P.8-5）を参照してください。

表 8-3　リンク フラッピングのトラブルシューティング

考えられる原因	解決策
ビット レートがしきい値を超えたために、ポートが errdisable ステートになっている。	ポートをディセーブルにしてから、イネーブルにします。 **shut** **no shut** ポートが通常の状態に戻ります。
ハードウェア障害または断続的なハードウェア エラーにより、スイッチでパケット ドロップが発生する。 ソフトウェア エラーにより、パケット ドロップが発生する。 制御フレームが誤ってデバイスに送信された。	外部デバイスでは、エラーが発生すると、リンクの再初期化が選択されることがあります。そのような場合、リンクを再初期化する具体的な方法はデバイスによって異なります。 **1.** MAC ドライバによって示されるリンク フラップの原因を判別します。 **2.** エンド デバイス上のデバッグ機能を使用して、問題のトラブルシューティングを行います。
ESX エラー、またはアップストリーム スイッチ上のリンク フラッピングが発生する。	ESX またはアップストリーム スイッチに関するマニュアルに記載されたトラブルシューティングの注意事項を使用してください。

ポート errdisable

errdisable ステートのポートをトラブルシューティングするには、この項のガイドラインを使用してください。

表 8-4　errdisable ステートのポートのトラブルシューティング

考えられる原因	解決策
ケーブルに欠陥または破損がある。	**1.** 物理ケーブルを確認します。 **2.** 欠陥のあるケーブルを交換または修理します。 **3.** ポートを再度イネーブルにします。 **shut** **no shut**

表 8-4　errdisable ステートのポートのトラブルシューティング （続き）

考えられる原因	解決策
同様に設定されていないポート チャネルにポートを追加しようとした。この場合、ポートは errdisabled になります。	**1.** スイッチ ログ ファイルを表示し、ポートの状態変化の一覧から正確な設定エラーを識別します。 **show logging logfile** **2.** 設定のエラーを修正し、ポート チャネルにポートを追加します。 **3.** ポートを再度イネーブルにします。 **shut** **no shut**
VSM アプリケーション エラー	**1.** ポートの起動中にエラーが発生したコンポーネントを識別します。 **show logging logfile | grep** *interface_number* 例 8-7（P.8-11）を参照してください。 **2.** エラーの遷移を識別します。 **show system internal ethpm event-history interface** *interface_number* **3.** サポート ケースを開き、上記のコマンドの出力を送信します。 詳細については、「テクニカル サポートへ問い合わせる前の準備」（P.24-1）を参照してください。

VM から保護されたポートに ping できない

VM から保護されたポートに ping できない場合、次のトラブルシューティングの注意事項を使用してください。

表 8-5　VM から保護されたポートに ping できない場合のトラブルシューティング

考えられる原因	解決策
vEthernet インターフェイスがアップになっていない。	**1.** vEthernet インターフェイスの状態を確認します。 **show interface vethernet** *number* **2.** インターフェイスがダウンしている場合は、イネーブルにします。 **shut** **no shut**
Drop on Source Miss（DSM）が設定されている。 このポートで新規の MAC アドレスを学習できない。	**1.** ポートのセキュリティ設定を確認します。 **module vem 3 execute vemcmd show portsec stats** **2.** DSM が設定されている場合、VSM の DSM ビットをクリアします。 **no port-security stop learning**

表 8-5　VM から保護されたポートに ping できない場合のトラブルシューティング （続き）

考えられる原因	解決策
パケット VLAN がポートで許可されていない。	**1.** パケット VLAN ID を識別します。 **show svs domain** **2.** パケット VLAN が VEM アップリンク ポートで許可されていることを確認します。 **show port-profile na uplink-all** **3.** パケット VLAN がアップリンク ポート プロファイルで許可されていない場合、許可された VLAN リストにそのパケット VLAN を追加します。
パケット VLAN がアップストリーム スイッチ ポートで許可されていない。	**1.** インターフェイスに接続されているアップストリーム ネイバーを識別します。 **show cdp neighbors** **2.** アップストリーム スイッチにログインして、パケット VLAN がポートで許可されていることを確認します。 **show running-config interface gigabitEthernet** *slot/port* **3.** パケット VLAN がポートで許可されていない場合、許可された VLAN リストにそのパケット VLAN を追加します。

ポート セキュリティ違反

セキュリティ違反のために vEthernet ポートがディセーブルである場合は、これらのトラブルシューティングのガイドラインを使用してください。

ポート セキュリティの詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

表 8-6　ポート セキュリティ違反のトラブルシューティング

考えられる原因	解決策
ポートに設定されている保護されたアドレスの最大数を超えている。 あるポートですでに保護されている MAC が、別のセキュア ポートで確認される。	**1.** セキュア アドレスを表示します。 **show port -security address vethernet** *number* **show port-security** **2.** セキュリティ違反したポートを識別します。 **show logging | inc "PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN"** **3.** セキュリティ違反を修正します。 **4.** インターフェイスをイネーブルにします。 **shut** **no shut**

ポートのトラブルシューティング コマンド

ポートに関する問題をトラブルシューティングするには、この項のコマンドを使用します。

表 8-7　ポートのトラブルシューティング コマンド

コマンド	目的
show module *module-number*	モジュールの状態を表示します。 例 8-1（P.8-10）を参照してください。
show svs domain	ドメイン コンフィギュレーションを表示します。 例 8-2（P.8-10）を参照してください。
show svs connections	Cisco Nexus 1000V の接続を表示します。 例 8-3（P.8-10）を参照してください。
show cdp neighbors	インターフェイスに接続しているネイバーを表示します。 例 8-4（P.8-10）を参照してください。
show port internal event-history interface	ポートの内部状態遷移の情報を表示します。 例 8-5（P.8-11）を参照してください。
show logging logfile	ログに記録されたシステム メッセージを表示します。 例 8-6（P.8-11）を参照してください。
show logging logfile |grep *interface_number*	指定のインターフェイスについてログに記録されたシステム メッセージを表示します。 例 8-7（P.8-11）を参照してください。
show interface brief	インターフェイスの状態表を表示します。 例 8-8（P.8-11）を参照してください。
show interface ethernet	次の情報を含む、指定のイーサネット インターフェイスの設定を表示します。 • 管理状態 • 速度 • トランク VLAN のステータス • 送受信されたフレームの数 • 伝送エラー（破棄、エラー、巡回冗長検査（CRC）、および不正なフレームなど） 例 8-9（P.8-11）を参照してください。 例 8-10（P.8-12）を参照してください。
show interface ethernet counters	同期問題を識別するためのポート カウンタを表示します。 カウンタについては、「インターフェイス カウンタの概要」（P.8-2）を参照してください。 例 8-11（P.8-12）を参照してください。

表 8-7　ポートのトラブルシューティング コマンド （続き）

コマンド	目的
show interface vethernet	vEthernet インターフェイス設定を表示します。 例 8-12（P.8-12）を参照してください。
show interface status	指定のインターフェイスの状態を表示します。
show interface capabilities	設定されたすべてのポート プロファイルを表形式で表示します。 例 8-13（P.8-13）を参照してください。
show interface virtual port mapping	すべての vEthernet インターフェイスの仮想ポート マッピングを表示します。 例 8-14（P.8-14）を参照してください。
show system internal ethpm errors	
show system internal ethpm event-history	
show system internal ethpm info	
show system internal ethpm mem-stats	
show system internal ethpm msgs	
show system internal vim errors	
show system internal vim event-history	
show system internal vim info	
show system internal vim mem-stats	
show system internal vim msgs	
module vem execute vemcmd show portsec status	ポートのポート セキュリティ状態を表示します。イネーブルの場合、出力には、VM ネットワーク アダプタに接続された LTL が表示されます。 例 8-15（P.8-14）を参照してください。
show port-security	システムで保護されている MAC アドレスの情報を表示します。 例 8-16（P.8-15）を参照してください。
show port-security interface veth	セキュアな vEthernet インターフェイスを表示します。
show port -security address vethernet	インターフェイス上のセキュア アドレスの情報を表示します。 例 8-17（P.8-15）を参照してください。
show system internal port-security msgs	
show system internal port-security errors	
show system internal l2fm msgs	
show system internal l2fm errors	
show system internal l2fm info detail	
show system internal pktmgr interface brief	
show system internal pktmgr client detail	

show コマンド出力の詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

例

例 8-1　show module

```
n1000v# show mod 3
Mod  Ports  Module-Type                       Model              Status
---  -----  -------------------------------- ------------------ ------------
3    248    Virtual Ethernet Module                             ok

Mod  Sw              Hw
---  --------------  ------
3    NA              0.0

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  ------------------------------------ --------------------
3    192.168.48.20    496e48fa-ee6c-d952-af5b-001517136344 frodo
```

例 8-2　show svs domain

```
n1000v# show svs domain
SVS domain config:
  Domain id:    559
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Aipc mode: L2
  L2/L3 Aipc interface: mgmt0
  Status: Config push to VC successful.
n1000v#
```

例 8-3　show svs connections

```
n1000v# show svs connections
connection VC:
    ip address: 192.168.0.1
    protocol: vmware-vim https
    certificate: default
    datacenter name: Hamilton-DC
    DVS uuid: ac 36 07 50 42 88 e9 ab-03 fe 4f dd d1 30 cc 5c
    config status: Enabled
    operational status: Connected
n1000v#
```

例 8-4　show cdp neighbors

```
n1000V#show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
swordfish-6k-2         Eth3/2        149    R S I       WS-C6506-E    Gig1/38
n1000V#
```

例 8-5　show port internal event-history interface

```
n1000v# show port internal event-history interface e1/7
>>>>FSM: <e1/7> has 86 logged transitions<<<<<
1) FSM:<e1/7> Transition at 647054 usecs after Tue Jan  1 22:44..
    Previous state: [PI_FSM_ST_IF_NOT_INIT]
    Triggered event: [PI_FSM_EV_MODULE_INIT_DONE]
    Next state: [PI_FSM_ST_IF_INIT_EVAL]
2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan  1 22:43..
    Previous state: [PI_FSM_ST_IF_INIT_EVAL]
    Triggered event: [PI_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
    Next state: [PI_FSM_ST_IF_DOWN_STATE]
```

例 8-6　show logging logfile

```
n1000v# show logging logfile
 . . .
Jan  4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 7 created
Jan  4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel 7
is down (No operational members)
Jan  4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: e1/8 added to port-channel 7
Jan  4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface e1/7 is down (Admnistratively
down)
Jan  4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible
Jan 4 06:55:56 switch%PORT_CHANNEL-5-PORT_ADDED: e1/7 added to port-channel 7
n1000v#
```

例 8-7　show logging logfile | grep interface_number

```
n1000v# show logging logfile | grep Vethernet3626
2011 Mar 25 10:56:03 n1k-bl %VIM-5-IF_ATTACHED: Interface Vethernet3626
is attached to Network Adapter 8 of gentoo-pxe-520 on port 193 of module
13 with dvport id 6899
2011 Mar 25 11:10:06 n1k-bl %ETHPORT-2-IF_SEQ_ERROR: Error ("Client data
inconsistency") while communicating with component MTS_SAP_ACLMGR for
opcode MTS_OPC_ETHPM_PORT_PRE_CFG (RID_PORT: Vethernet3626)
2011 Mar 25 11:10:06 n1k-bl %ETHPORT-2-IF_DOWN_ERROR_DISABLED: Interface
Vethernet3626 is down (Error disabled. Reason:Client data inconsistency)
```

例 8-8　show interface brief

```
n1000v# show int brief
--------------------------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------------------------
mgmt0 -- up 172.23.232.141 1000 1500
--------------------------------------------------------------------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
Eth3/2 1 eth trunk up none 1000(D) --
Eth3/3 1 eth access up none 1000(D) --
n1000v#
```

例 8-9　show interface ethernet

```
n1000v# show interface e1/14
e1/7 is down (errDisabled)
```

例 8-10　show interface ethernet

例：

```
n1000v# show interface eth3/2
Ethernet3/2 is up
  Hardware: Ethernet, address: 0050.5653.6345 (bia 0050.5653.6345)
  MTU 1500 bytes, BW -598629368 Kbit, DLY 10 usec,
     reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned off
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
    Rx
    18775 Input Packets 10910 Unicast Packets
    862 Multicast Packets 7003 Broadcast Packets
    2165184 Bytes
    Tx
    6411 Output Packets 6188 Unicast Packets
    216 Multicast Packets 7 Broadcast Packets 58 Flood Packets
    1081277 Bytes
    1000 Input Packet Drops 0 Output Packet Drops
    1 interface resets
n1000v#
```

例 8-11　show interface ethernet counters

```
n1000v# show interface eth3/2 counters

--------------------------------------------------------------------------------
Port                InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Eth3/2             2224326         11226           885          7191

--------------------------------------------------------------------------------
Port               OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
Eth3/2             1112171          6368           220             7
```

例 8-12　show interface vEthernet

```
n1000v# show interface veth1
Vethernet1 is up
    Port description is gentoo1, Network Adapter 1
    Hardware is Virtual, address is 0050.56bd.42f6
    Owner is VM "gentoo1", adapter is Network Adapter 1
    Active on module 33
    VMware DVS port 100
    Port-Profile is vlan48
    Port mode is access
    Rx
    491242 Input Packets 491180 Unicast Packets
    7 Multicast Packets 55 Broadcast Packets
    29488527 Bytes
    Tx
    504958 Output Packets 491181 Unicast Packets
    1 Multicast Packets 13776 Broadcast Packets 941 Flood Packets
    714925076 Bytes
    11 Input Packet Drops 0 Output Packet Drops
```

```
n1000v#
```

例 8-13　show interface capabilities

```
n1000v# show interface capabilities
mgmt0
  Model:                 --
  Type:                  --
  Speed:                 10,100,1000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               no
  Broadcast suppression: none
  Flowcontrol:           rx-(none),tx-(none)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  yes
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

port-channel1
  Model:                 unavailable
  Type:                  unknown
  Speed:                 10,100,1000,10000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  no
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

port-channel2
  Model:                 unavailable
  Type:                  unknown
  Speed:                 10,100,1000,10000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  no
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
```

```
  Port Group Members:    none

port-channel12
  Model:                 unavailable
  Type:                  unknown
  Speed:                 10,100,1000,10000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  no
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

control0
  Model:                 --
  Type:                  --
  Speed:                 10,100,1000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               no
  Broadcast suppression: none
  Flowcontrol:           rx-(none),tx-(none)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  yes
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

n1000v#
```

例 8-14　show interface virtual port-mapping

```
n1000v# show interface virtual port-mapping

--------------------------------------------------------------------------------
Port    Hypervisor Port    Binding Type    Status    Reason
--------------------------------------------------------------------------------
Veth1   DVPort5747         static          up        none
Veth2   DVPort3361         static          up        none
n1000v#
```

例 8-15　module vem execute vemcmd show portsec status

```
n1000V# module vem 3 execute vemcmd show portsec stats
  LTL   if_index  cp-cnt  Max         Aging   Aging     DSM  Sticky   VM
                          Secure      Time    Type      Bit  Enabled  Name
                          Addresses
   47   1b020000       0          1       0   Absolute  Clr       No  VM-Pri.eth1
n1000V#
```

例 8-16　show port security

```
n1000V# show port-security
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

--------------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------------
Vethernet1            1              0              0              Shutdown
===================================================================================
```

例 8-17　show port security address interface vethernet

```
n1000v#show port-security address interface vethernet 1
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

-----------------------------------------------------------------------
                    Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining age
                                                                (mins)
----    -----------            ------            -----     ---------------
  65    0050.56B7.7DE2        DYNAMIC        Vethernet1        0
=======================================================================
```

CHAPTER 9

ポート プロファイル

この章では、ポート プロファイルに関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「ポート プロファイルについて」（P.9-1）
- 「ポート プロファイルの問題」（P.9-2）
- 「ポート プロファイルのログ」（P.9-6）
- 「ポート プロファイルのトラブルシューティング コマンド」（P.9-6）

ポート プロファイルについて

ポート プロファイルを使用してインターフェイスを設定します。1 つのポート プロファイルを複数のインターフェイスを割り当てることで、すべてのインターフェイスを同じ設定にすることができます。ポート プロファイルに対する変更は、そのポート プロファイルに割り当てられているすべてのインターフェイスの設定に自動的に伝播されます。

VMware vCenter Server では、ポート プロファイルはポート グループとして表されます。vCenter Server では、vEthernet インターフェイスやイーサネット インターフェイスは、次の目的でポート プロファイルに割り当てられます。

- ポリシーによってポート設定を定義する。
- 単一ポリシーを多数のポートに適用する。
- vEthernet ポートとイーサネット ポートをサポートする。

vEthernet ポート プロファイルは、サーバ管理者によって物理ポート（VMNIC または PNIC）に割り当てることができます。vEthernet として設定されていないポート プロファイルは、VM 仮想ポートに割り当てられます。

（注） 手動インターフェイス設定でポート プロファイルの設定を上書きすることもできますが、この方法は推奨できません。手動インターフェイス設定は、たとえば、すばやく変更をテストする場合や、継承されたポート プロファイルを変更する必要なくポートをディセーブルにすることを許可する場合だけ使用します。

物理ポートまたは仮想ポートへのポート プロファイルの割り当ての詳細については、VMware のマニュアルを参照してください。

プロファイルが予期したとおりに物理ポートまたは仮想ポートに割り当てられていることを確認するには、次の show コマンドを使用してください。

- **show port-profile virtual usage**
- **show running-config interface** *interface-id*

ポート プロファイルの継承を確認するには、次のコマンドを使用します。

- **show running-config interface** *interface-id*

（注）継承されたポート プロファイルは、Cisco Nexus 1000V CLI を使用して変更したり、インターフェイスから削除したりできません。このような操作は、vCenter Server からのみ実行できます。

（注）ポートがホストに接続されている場合、継承されたポート プロファイルは Cisco Nexus 1000V によって自動設定されます。これは、システム管理者によって割り当てられた VMware ポート グループを作成元のポート プロファイルと比較することによって行います。

ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ポート プロファイルの問題

次に、ポート プロファイルの問題について現象、考えられる原因、および解決方法を示します。

表 9-1　ポート プロファイルの問題

症状	考えられる原因	解決策
vCenter Server にポート グループが表示されない。または、次のメッセージが表示される。 `Warning: Operation succeeded locally but update failed on vCenter server. Please check if you are connected to vCenter Server.`	vCenter Server への接続がダウンしている。	**1.** vCenter Server への接続が Enabled および Connected であることを確認します。 **show svs connections** **2.** vCenter Server に再接続します。 詳細な手順については、『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』に記載された「*Connecting to vCenter Server*」の手順を参照してください。
	ドメイン設定が vCenter Server に正常にプッシュされなかった。	**1.** ドメイン設定が vCenter Server に正常にプッシュされたことを確認します。 **show svs domain** **2.** ドメイン設定の問題を修正します。 ドメインを設定する方法の詳細については、『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
	ポート プロファイルの設定に誤りがある。	**1.** ポート プロファイルに **vmware port-group** が設定されていることと、ポート プロファイルがイネーブルになっていることを確認します。 **show port profile name** *name* **2.** 『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』に記載された手順を使用して、ポート プロファイルを修正します。
ポートの設定がインターフェイスに適用されない。	vCenter Server と VSM 間の管理接続で、ポート プロファイルの割り当ての送受信が防止されている。	**1.** ポート プロファイルの使用状況をインターフェイス別に表示します。 **show port-profile virtual usage** **2.** インターフェイス レベルの設定によってポート プロファイルの設定が上書きされていないことを確認します。 **show run** **show port-profile expand-interface** **3.** show コマンドの出力に誤りがある場合は、vCenter Server でポート グループをインターフェイスに再割り当てします。

表 9-1　ポート プロファイルの問題 （続き）

症状	考えられる原因	解決策
イーサネット インターフェイスまたは vEthernet インターフェイスが管理上のダウン状態になっている。 次のようなシステム メッセージがログに記録されている。 `%VMS-3-DVPG_NICS_MOVED: '1' nics have been moved from port-group 'Access483' to 'Unused_Or_Quarantine_Veth'.`	インターフェイスが検疫ポート プロファイルを継承している。 VSM をリブートする前に設定が保存されず、設定が失われ、インターフェイスが次のいずれかのポート プロファイルに移動された。 • Unused_Or_Quarantine_Uplink（イーサネット タイプの場合） • Unused_Or_Quarantine_Veth（vEhternet タイプの場合）	**1.** ポート プロファイルとインターフェイスのマッピングを確認します。 **show port-profile virtual usage** **2.** VMNIC または PNIC を非検疫ポート グループに再割り当てすることで、インターフェイスがアップになり、トラフィックを転送できるようにします。これには、vCenter Server 上のポート グループを変更する必要があります。
ポート プロファイルを適用した後、オンライン インターフェイスが検疫される。 次のようなシステム メッセージがログに記録されている。 `%PORT-PROFILE-2-INTERFACE_QUARANTINED: Interface Ethernet3/3 has been quarantined due to Cache Overrun`	割り当て済みのポート プロファイルの設定に誤りがある。ポート プロファイルがインターフェイスに適用されるときに、誤りのあるコマンドは失敗します。 特定のコマンドが失敗しても、ポート プロファイルとインターフェイスのマッピングが作成される。	**1.** 失敗したコマンドを識別します。 **show accounting log | grep FAILURE** **2.** インターフェイスが検疫されたことを確認します。 **show port-profile sync-status** **3.** ポート プロファイルとインターフェイスのマッピングを確認します。 **show port-profile virtual usage** **4.** 『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』に記載された手順を使用して、ポート プロファイルのエラーを修正します。 **5.** インターフェイスを検疫から戻します。 **no shutdown** インターフェイスがオンラインに戻ります。 **6.** リターン シャットダウン制御がポート プロファイルに戻ります。 **default shutdown**

表 9-1　ポート プロファイルの問題 （続き）

症状	考えられる原因	解決策
ポート プロファイルを修正した後で、割り当てられたオフライン インターフェイスが検疫される。 次のようなシステム メッセージがログに記録されている。 `%PORT-PROFILE-2-INTERFACE_QUARANTINED: Interface Ethernet4/3 has been quarantined due to Cache Overrun`	インターフェイスが DVS から削除されている。	インターフェイスをオンラインに戻すには、「検疫されたオフライン インターフェイスの回復」（P.9-5）の手順を使用します。

モジュールと、関連付けられたすべてのインターフェイスがオフラインになっている。
次のようなシステム メッセージがログに記録されている。
`2011 Mar 2 22:28:50 n1000v %VEM_MGR-2-VEM_MGR_REMOVE_NO_HB: Removing VEM 3 (heartbeats lost)`
`2011 Mar 2 22:29:00 n1000v %VEM_MGR-2-MOD_OFFLINE: Module 3 is offline`
	システム VLAN を伝送しているモジュールのインターフェイスが、次のいずれかの理由でダウンしている。
	• システム インターフェイスが vCenter Server 上の DVS から削除された。
	• モジュールの電源がダウンした。
	• モジュールへの一般的な接続損失がある。
		モジュールをオンラインに戻すには、VEM のトラブルシューティング ガイドに従ってください。
		インターフェイスをオンラインに戻すには、「検疫されたオフライン インターフェイスの回復」（P.9-5）の手順を使用します。

検疫されたオフライン インターフェイスの回復

次の手順に従って、検疫されたオフライン インターフェイスを回復させ、オンラインにすることができます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の詳細

ステップ 1　インターフェイスが検疫されたことを確認します。show コマンドの出力にインターフェイスが表示されます。

show port-profile sync-status

ステップ 2　vCenter Server で、PNIC をポート プロファイル（元のポート プロファイルまたは別のポート プロファイル）に追加するか、関連付けます。

インターフェイスがオンラインに戻ります。

ステップ 3　インターフェイスがオンラインに戻ったことを確認します。

show interface brief

ステップ 4　ポート プロファイルとインターフェイスのマッピングを確認します。

show port-profile virtual usage

ステップ 5　インターフェイスが検疫から自動的に戻ったことを確認します。インターフェイスは、show コマンドの出力に表示されなくなります。

show port-profile sync-status

ステップ 6　リターン シャットダウン制御がポート プロファイルに戻ります。

default shutdown

ポート プロファイルのログ

ポート プロファイルに関する詳細なログをイネーブルにして収集するには、次のコマンドを使用します。

- **debug port-profile trace**
- **debug port-profile error**
- **debug port-profile all**
- **debug msp all**

デバッグ ログをイネーブルにした後、後続のポート プロファイル設定の結果はログ ファイルにキャプチャされます。

ポート プロファイルのトラブルシューティング コマンド

ポート プロファイルに関する問題をトラブルシューティングするには、この項のコマンドを使用できます。

コマンド	目的
show port-profile	ポート プロファイルの設定を表示します。 例 9-1（P.9-7）を参照してください。
show port-profile name *name*	指定されたポート プロファイルの設定を表示します。 例 9-2（P.9-8）を参照してください。
show port-profile brief	設定されたすべてのポート プロファイルを表形式で表示します。 例 9-3（P.9-9）を参照してください。
show port-profile expand-interface	割り当てられているインターフェイスを包含するように展開された、設定済みのすべてのポート プロファイルを表示します。 例 9-4（P.9-9）を参照してください。
show port-profile expand-interface name *name*	割り当てられているインターフェイスを包含するように展開された、指定のポート プロファイルを表示します。 例 9-5（P.9-11）を参照してください。

コマンド	目的
show port-profile-role [**name** ***port-profile-role-name***]	ロール名、説明、割り当てられたユーザ、および割り当てられたグループなど、ポート プロファイルのロール設定を表示します。 例 9-7（P.9-12）を参照してください。
show running-config port-profile [*profile-name*]	ポート プロファイルの設定を表示します。 例 9-6（P.9-12）を参照してください。
show port-profile-role	ポート プロファイルのロール設定を表示します。 例 9-7（P.9-12）を参照してください。
show port-profile-role users	使用可能なユーザおよびグループを表示します。 例 9-8（P.9-12）を参照してください。
show port-profile sync-status [**interface** *if-name*]	ポート プロファイルと同期しないインターフェイスを表示します。 例 9-9（P.9-12）を参照してください。
show port-profile virtual usage [**name** *profile-name*]	ポート プロファイルの使用状況をインターフェイス別に表示します。 例 9-10（P.9-13）を参照してください。
show msp internal info	vCenter Server 上のポート プロファイルのマッピングと、設定されているロールを表示します。 例 9-11（P.9-13）を参照してください。
show system internal port-profile profile-fsm	継承や設定などの遷移を含む、Cisco Nexus 1000V でのポート プロファイルのアクティビティを表示します。次のように表示される場合は、すべての継承が処理されています。 `Curr state: [PPM_PROFILE_ST_SIDLE]` 例 9-12（P.9-17）を参照してください。
show system internal port-profile event-history msgs	Cisco Nexus 1000V 内のポート プロファイル イベントについてログに記録されたメッセージを表示します。 例 9-13（P.9-17）を参照してください。

show コマンド出力の詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

例

例 9-1　show port-profile

```
n1000v# show port-profile
port-profile vEthProfile1
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
```

```
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on mac-pinning
  evaluated config attributes:
    channel-group auto mode on mac-pinning
  assigned interfaces:
port-profile vEthProfile2
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group cdp
  evaluated config attributes:
    channel-group auto mode on sub-group cdp
  assigned interfaces:
port-profile vEthProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:n1000v#
```

例 9-2　show port-profile name profile_name

```
n1000v# show port-profile name vEthProfile3
port-profile vEthProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:
n1000v#
```

例 9-3　show port-profile brief

```
n1000v# show port-profile brief
--------------------------------------------------------------------------------
Port                          Profile    Profile  Conf   Eval    Assigned  Child
Profile                       Type       State    Items  Items   Intfs     Profs
--------------------------------------------------------------------------------
AccessProf                    Vethernet  0        0      0       0         0
PP1027                        Vethernet  1        0      0       0         0
PP1028                        Vethernet  1        0      0       0         0
Unused_Or_Quarantine_Uplink   Ethernet   1        1      0       0         0
Unused_Or_Quarantine_Veth     Vethernet  1        1      0       0         0
accessprof                    Vethernet  0        3      3       0         0
portp1                        Vethernet  0        0      0       0         0
--------------------------------------------------------------------------------
Profile    Total
Type       Intfs
--------------------------------------------------------------------------------
Vethernet  8
Ethernet   10
n1000v#
```

例 9-4　show port-profile expand-interface

```
n1000v# show port-profile expand-interface
port-profile AccessProf
  id: 1
  capability: 0x0
  state: 0x0
  type: 0x0
  system vlan mode: -
  system vlans:
  port-binding: static
  bind_opts: 0
  max ports: 32
  min ports: 32
  used ports: 0
  vmware config information
    pg name: AccessProf
    dvs:  (ignore)
    reserved ports: 32
  port-profile role:
  alias information:
port-profile PP1027
  id: 4
  capability: 0x0
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  bind_opts: 1
  max ports: 64
  min ports: 32
  used ports: 0
  vmware config information
    pg name: PP1027
    dvs:  (ignore)
    reserved ports: 16
  port-profile role:
  alias information:
    pg id: PP1027
    dvs uuid:
```

```
    type: 1
    pg id: dvportgroup-3180
    dvs uuid: 12 98 0e 50 6b 78 6f c5-74 af b2 3a 16 6e 45 10
    type: 2
port-profile PP1028
  id: 3
  capability: 0x0
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: dynamic
  bind_opts: 1
  max ports: 64
  min ports: 32
  used ports: 0
  vmware config information
    pg name: PP1028
    dvs:  (ignore)
    reserved ports: 16
  port-profile role:
  alias information:
    pg id: PP1028
    dvs uuid:
    type: 1
    pg id: dvportgroup-3181
    dvs uuid: 12 98 0e 50 6b 78 6f c5-74 af b2 3a 16 6e 45 10
    type: 2
port-profile Unused_Or_Quarantine_Uplink
  id: 6
  capability: 0x1
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: dynamic
  bind_opts: 1
  max ports: 32
  min ports: 32
  used ports: 0
  vmware config information
    pg name: Unused_Or_Quarantine_Uplink
    dvs:  (ignore)
    reserved ports: 0
  port-profile role:
  alias information:
    pg id: Unused_Or_Quarantine_Uplink
    dvs uuid:
    type: 1
    pg id: dvportgroup-3182
    dvs uuid: 12 98 0e 50 6b 78 6f c5-74 af b2 3a 16 6e 45 10
    type: 2
port-profile Unused_Or_Quarantine_Veth
  id: 7
  capability: 0x0
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: dynamic
  bind_opts: 1
  max ports: 32
  min ports: 32
  used ports: 0
```

```
  vmware config information
    pg name: Unused_Or_Quarantine_Veth
    dvs:  (ignore)
    reserved ports: 32
  port-profile role:
  alias information:
    pg id: Unused_Or_Quarantine_Veth
    dvs uuid:
    type: 1
    pg id: dvportgroup-3183
    dvs uuid: 12 98 0e 50 6b 78 6f c5-74 af b2 3a 16 6e 45 10
    type: 2
port-profile accessprof
  id: 5
  capability: 0x0
  state: 0x0
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: dynamic
  bind_opts: 1
  max ports: 32
  min ports: 32
  used ports: 0
  vmware config information
    pg name: accessprof
    dvs:  (ignore)
    reserved ports: 32
  port-profile role:
  alias information:
    pg id: accessprof
    dvs uuid:
    type: 1
port-profile portp1
  id: 2
  capability: 0x0
  state: 0x0
  type: 0x0
  system vlan mode: -
  system vlans:
  port-binding: static
  bind_opts: 0
  max ports: 32
  min ports: 32
  used ports: 0
  vmware config information
    pg name: portp1
    dvs:  (ignore)
    reserved ports: 32
  port-profile role:
  alias information:
pending binds:
n1000v#
```

例 9-5　show port-profile expand-interface name UplinkProfile1

```
n1000v# show port-profile expand-interface name UplinkProfile1
port-profile EthProfile1
Ethernet2/2
    switchport mode trunk
    switchport trunk allowed vlan 110-119
    no shutdown
n1000v#
```

例 9-6　show running-config port-profile

```
n1000v# show running-config port-profile
port-profile type ethernet UplinkProfile1
  description "Profile for critical system ports"
  vmware port-group
  switchport mode access
  switchport access vlan 113
  switchport trunk native vlan 113
  channel-group auto mode on
  no shutdown
port-profile type vethernet vEthProfile2
  vmware port-group
  vmware max-ports 5
  switchport mode trunk
  switchport trunk native vlan 112
  channel-group auto mode on sub-group cdp
  no shutdown
n1000v#
```

例 9-7　show port-profile-role

```
n1000v# show port-profile-role name adminUser

Name: adminUser
Description: adminOnly
Users:
    hdbaar (user)
Assigned port-profiles:
    allaccess2
n1000v#
```

例 9-8　show port-profile-role users

```
switch# show port-profile-role users
Groups:
  Administrators
  TestGroupB
Users:
  hdbaar
  fgreen
  suchen
  mariofr
switch#
```

例 9-9　show port-profile sync-status

```
n1000v# show port-profile sync-status interface ethernet 3/2
Ethernet3/2
 port-profile: uplink
 interface status: quarantine
 sync status: out of sync
 cached commands:
 errors:
    command cache overrun
 recovery steps:
    bring interface online
n1000v#
```

例 9-10　show port-profile virtual usage

```
n1000v# show port-profile virtual usage
--------------------------------------------------------------------------------
Port Profile                Port        Adapter        Owner
--------------------------------------------------------------------------------
n1kv-uplink0                Po1
                            Eth3/2      vmnic1         localhost.
                            Eth3/3      vmnic2         localhost.
vlan1767                    Veth7       Net Adapter 1  all-tool-7
                            Veth8       Net Adapter 1  all-tool-8
aipc1765                    Veth4       Net Adapter 1  bl-h-s
inband1766                  Veth6       Net Adapter 3  bl-h-s
mgmt1764                    Veth5       Net Adapter 2  bl-h-s
vpc-mac-uplink              Po7
                            Eth5/2      vmnic1         localhost.
                            Eth5/3      vmnic2         localhost.
ch-vpc-mac-uplink           Po2
                            Po3
                            Eth4/2      vmnic1         VDANIKLNCOS
                            Eth4/3      vmnic2         VDANIKLNCOS
ch-aipc1765                 Veth1       Net Adapter 1  bl-h-p
ch-mgmt1764                 Veth2       Net Adapter 2  bl-h-p
ch-inband1766               Veth3       Net Adapter 3  bl-h-p
n1000v#
```

例 9-11　show msp internal info

```
n1000v# show msp internal info
port-profile Access484
  id: 5
  capability: 0x0
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  max ports: 256
  vmware config information
    pg name: Access484
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: Access484
    dvs uuid:
    type: 1
    pg id: dvportgroup-3285
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
    pg id: dvportgroup-3292
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
port-profile Unused_Or_Quarantine_Uplink
  id: 1
  capability: 0x1
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  max ports: 32
  vmware config information
    pg name: Unused_Or_Quarantine_Uplink
```

```
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: Unused_Or_Quarantine_Uplink
    dvs uuid:
    type: 1
    pg id: dvportgroup-2444
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
port-profile Unused_Or_Quarantine_Veth
  id: 2
  capability: 0x0
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  max ports: 32
  vmware config information
    pg name: Unused_Or_Quarantine_Veth
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: Unused_Or_Quarantine_Veth
    dvs uuid:
    type: 1
    pg id: dvportgroup-2445
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
port-profile eth-break-deinherit
  id: 10
  capability: 0x1
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  max ports: 32
  vmware config information
    pg name: eth-break-deinherit
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: eth-break-deinherit
    dvs uuid:
    type: 1
    pg id: dvportgroup-3286
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
    pg id: dvportgroup-3293
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
port-profile eth-break-inherit
  id: 9
  capability: 0x1
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  max ports: 32
  vmware config information
    pg name: eth-break-inherit
    dvs:  (ignore)
```

```
    port-profile role:
    alias information:
      pg id: eth-break-inherit
      dvs uuid:
      type: 1
      pg id: dvportgroup-3287
      dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
      type: 2
      pg id: dvportgroup-3294
      dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
      type: 2
  port-profile uplink
    id: 3
    capability: 0x3
    state: 0x1
    type: 0x1
    system vlan mode: trunk
    system vlans: 480-481
    port-binding: static
    max ports: 32
    vmware config information
      pg name: uplink
      dvs:  (ignore)
    port-profile role:
    alias information:
      pg id: uplink
      dvs uuid:
      type: 1
      pg id: dvportgroup-3283
      dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
      type: 2
  port-profile uplink-quar
    id: 12
    capability: 0x1
    state: 0x1
    type: 0x1
    system vlan mode: -
    system vlans:
    port-binding: static
    max ports: 32
    vmware config information
      pg name: uplink-quar
      dvs:  (ignore)
    port-profile role:
    alias information:
      pg id: uplink-quar
      dvs uuid:
      type: 1
      pg id: dvportgroup-3288
      dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
      type: 2
      pg id: dvportgroup-3295
      dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
      type: 2
  port-profile veth-break-deinherit
    id: 8
    capability: 0x0
    state: 0x1
    type: 0x1
    system vlan mode: -
    system vlans:
    port-binding: static
    max ports: 256
    vmware config information
```

```
    pg name: veth-break-deinherit
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: veth-break-deinherit
    dvs uuid:
    type: 1
    pg id: dvportgroup-3289
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
    pg id: dvportgroup-3296
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
port-profile veth-break-inherit
  id: 7
  capability: 0x0
  state: 0x1
  type: 0x1
  system vlan mode: -
  system vlans:
  port-binding: static
  max ports: 256
  vmware config information
    pg name: veth-break-inherit
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: veth-break-inherit
    dvs uuid:
    type: 1
    pg id: dvportgroup-3290
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
    pg id: dvportgroup-3297
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
port-profile vpc-uplink
  id: 6
  capability: 0x3
  state: 0x1
  type: 0x1
  system vlan mode: trunk
  system vlans: 480-481
  port-binding: static
  max ports: 32
  vmware config information
    pg name: vpc-uplink
    dvs:  (ignore)
  port-profile role:
  alias information:
    pg id: vpc-uplink
    dvs uuid:
    type: 1
    pg id: dvportgroup-3291
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
    pg id: dvportgroup-3298
    dvs uuid: 44 dc 3b 50 53 11 b7 ac-ef ed ef 46 ee df c2 d5
    type: 2
pending binds:
port-profile-role adfd
  id: 0
  desc:
  num users: 1
```

```
    group GROUP

n1000v#
```

例 9-12　show system internal port-profile profile-fsm

```
n1000v# show system internal port-profile profile-fsm
>>>>FSM: <PROFILE_FSM:1> has 4 logged transitions<<<<<

1) FSM:<PROFILE_FSM:1> Transition at 856903 usecs after Tue Mar  8 19:11:47 2011
    Previous state: [PPM_PROFILE_ST_SIDLE]
    Triggered event: [PPM_PROFILE_EV_EIF_STATUS_CHANGE]
    Next state: [PPM_PROFILE_ST_SIDLE]

2) FSM:<PROFILE_FSM:1> Transition at 858442 usecs after Tue Mar  8 19:11:47 2011
    Previous state: [PPM_PROFILE_ST_SIDLE]
    Triggered event: [PPM_PROFILE_EV_ELEARN]
    Next state: [PPM_PROFILE_ST_SIF_CREATE]

3) FSM:<PROFILE_FSM:1> Transition at 842710 usecs after Tue Mar  8 19:12:04 2011
    Previous state: [PPM_PROFILE_ST_SIF_CREATE]
    Triggered event: [PPM_PROFILE_EV_EACKNOWLEDGE]
    Next state: [FSM_ST_NO_CHANGE]

4) FSM:<PROFILE_FSM:1> Transition at 873872 usecs after Tue Mar  8 19:12:04 2011
    Previous state: [PPM_PROFILE_ST_SIF_CREATE]
    Triggered event: [PPM_PROFILE_EV_ESUCCESS]
    Next state: [PPM_PROFILE_ST_SIDLE]

    Curr state: [PPM_PROFILE_ST_SIDLE]
n1000v#
```

例 9-13　show system internal port-profile event-history msgs

```
n1000v# show system internal port-profile event-history msgs
1) Event:E_MTS_RX, length:60, at 538337 usecs after Tue Mar  8 19:13:02 2011
    [NOT] Opc:MTS_OPC_IM_IF_CREATED(62467), Id:0X0000B814, Ret:SUCCESS
    Src:0x00000101/175, Dst:0x00000101/0, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:120
    Payload:
    0x0000:  00 00 00 02 00 00 00 02 00 00 00 0c 00 00 00 29

2) Event:E_MTS_RX, length:60, at 515030 usecs after Tue Mar  8 19:13:02 2011
    [NOT] Opc:MTS_OPC_LC_ONLINE(1084), Id:0X0000B7E8, Ret:SUCCESS
    Src:0x00000101/744, Dst:0x00000101/0, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:234
    Payload:
    0x0000:  02 00 00 03 00 00 00 00 00 00 03 02 03 02 00 00

3) Event:E_MTS_RX, length:60, at 624319 usecs after Tue Mar  8 19:12:05 2011
    [NOT] Opc:MTS_OPC_PPM_INTERFACE_UPDATE(152601), Id:0X00003908, Ret:SUCCESS
    Src:0x00000101/489, Dst:0x00000101/0, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:107
    Payload:
    0x0000:  00 00 00 02 00 00 00 02 00 00 00 0c 00 00 00 26

4) Event:E_MTS_RX, length:60, at 624180 usecs after Tue Mar  8 19:12:05 2011
    [NOT] Opc:MTS_OPC_PPM_INTERFACE_UPDATE(152601), Id:0X00003905, Ret:SUCCESS
    Src:0x00000101/489, Dst:0x00000101/0, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:107
    Payload:
    0x0000:  00 00 00 02 00 00 00 02 00 00 00 0c 00 00 00 26
```

```
5) Event:E_MTS_RX, length:60, at 624041 usecs after Tue Mar  8 19:12:05 2011
    [NOT] Opc:MTS_OPC_PPM_INTERFACE_UPDATE(152601), Id:0X00003903, Ret:SUCCESS
    Src:0x00000101/489, Dst:0x00000101/0, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:107
    Payload:
    0x0000:  00 00 00 02 00 00 00 02 00 00 00 0c 00 00 00 26
...
```

CHAPTER 10

ポート チャネルおよびトランキング

この章では、ポート チャネルとトランキングのトラブルシューティングについて説明します。

この章では、次の事項について説明します。

- 「概要」（P.10-1）
- 「トラブルシューティングの初期チェックリスト」（P.10-2）
- 「非対称ポート チャネル（APC）のトラブルシューティング」（P.10-3）
- 「ポート チャネルが作成できない」（P.10-4）
- 「新しく追加したインターフェイスがポート チャネル内でオンラインにならない」（P.10-4）
- 「VLAN トラフィックがトランクを通過しない」（P.10-6）

概要

ここでは、次の内容について説明します。

- 「ポート チャネルの概要」（P.10-1）
- 「トランキングの概要」（P.10-2）

ポート チャネルの概要

ポート チャネルは、物理的に複数のインターフェイスをまとめて 1 つの論理インターフェイスにすることで、より広い帯域幅やより優れたロード バランシング、リンク冗長性を提供します。

ポート チャネルは、次の機能を実行します。

- そのチャネル内にあって機能するすべてのリンクにトラフィックを分散させることにより、リンク上の帯域幅の集約を向上させます。
- 複数のリンクに負荷を分散させて、最適な帯域幅利用を維持します。
- 高い可用性を提供します。いずれか 1 つのリンクに障害が発生したら、それまでそのリンクで伝送されていたトラフィックが残りのリンクに切り替えられます。ポート チャネル内の 1 つのリンクが停止しても、上位プロトコルにはそれは認識されません。上位プロトコルにとっては、帯域幅が減るだけで、リンクはまだそこにあります。MAC アドレス テーブルは、リンクの障害による影響を受けません。

ポート チャネルの制限

ポート チャネルの制限は、次のとおりです。

- ポート チャネルは ACL をサポートしない。
- ポート チャネルは NetFlow をサポートしない。

トランキングの概要

トランキングは、「VLAN トランキング」とも呼ばれ、複数の VLAN 内で、同一の物理リンクを介して、ポートが相互接続してフレームを送受信することを可能にします。

トランキングとポート チャネルは、次のように機能します。

- ポート チャネルが、複数の物理リンクを結合して 1 つのまとまった論理リンクにすることを可能にします。
- トランキングが、1 つのリンクで複数の VAN トラフィックを伝送する（トランキングする）ことを可能にします。

トラブルシューティングの初期チェックリスト

次のチェックリストを使用して、ポート チャネルとトランキングの問題のトラブルシューティングを開始してください。

チェックリスト	√
show port-channel compatibility-parameters CLI コマンドを使用して、ポート チャネルの要件を調べます。	
ポート チャネル内のすべてのインターフェイスが、LACP チャネルについて同一の宛先デバイスを持つことを確認します。Nexus 1000V で Asymmetric Port Channel（APC; 非対称ポート チャネル）機能を使用することにより、ON モード チャネルのポートを 2 つの異なる宛先デバイスに接続できます。 **（注）** APC は、ON モード チャネルでしかサポートされていません。LACP チャネルにはサポートされていません。	
ポート チャネルのどちらかの側が同じ数のインターフェイスに接続されていることを確認します。	
各インターフェイスが反対側で同じタイプのインターフェイスに接続されていることを確認します。	
トランク ポート上の必要なすべての VLAN が、許可されている VLAN リストに入っていることを確認します。	
1 つのポート チャネルを形成しようとするすべてのメンバーが同一モジュール上にあることを確認します。	
物理ポートによって使用されるプロファイルにポート チャネルの設定が入っていることを確認します。	

チェックリスト	√
ポートが異なるアップストリーム スイッチに接続されている場合は、APC を設定します。	
アップストリーム スイッチでポート チャネルがサポートされていない場合は、必ずプロファイル内で APC を設定してください。さらに、APC 内にあるポートが多くても 2 つであることを確認します。	

次のコマンドが、ポート チャネルとトランキングのトラブルシューティングに役立ちます。

- **show port-channel summary**
- **show port-channel internal event-history interface port-channel** *channel-number*
- **show port-channel internal event-history interface ethernet** *slot-number*
- **show system internal ethpm event-history interface port-channel** *channel-number*
- **show system internal ethpm event-history interface ethernet** *slot-number*
- **show vlan internal trunk interface ethernet** *slot-number*
- **show vlan internal trunk interface port-channel** *channel-number*
- **debug port-channel error**
- **module vem** *module-number* **execute vemcmd show port**
- **module vem** *module-number* **execute vemcmd show pc**
- **module vem** *module-number* **execute vemcmd show trunk**

例 10-1 に、**show port-channel summary** コマンドの出力を示します。

例 10-1　show port-channel summary コマンド

```
n1000v# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      NONE      Eth3/4(P)
2     Po2(SU)     Eth      NONE      Eth3/2(P)    Eth3/6(P)
```

非対称ポート チャネル（APC）のトラブルシューティング

非対称ポート チャネルのトラブルシューティングは、次のガイドラインに従って行います。

- メンバーが 2 つの異なるアップストリーム スイッチに接続されているポート チャネルを設定する場合は、APC を使用します。
- APC は、Cisco Discovery Protocol（CDP）に依存しています。VSM 上およびアップストリーム スイッチ上で CDP が有効になっていることを確認してください。
- アップストリーム スイッチから受信した CDP 情報に基づいて、APC 内の物理ポートにサブグループ ID が割り当てられます。

- ユーザが、インターフェイス コンフィギュレーション サブモードから手動でサブグループ ID を設定できます。
- ポート プロファイルまたはポート チャネル インターフェイスのいずれかで、必ずサブグループ CDP を設定してください。
- APC 内のポートは、手動でまたは CDP を通じてサブループ ID が割り当てられている場合にだけ UP になります。
- VSM に対して **show cdp neighbors** コマンドを実行して、出力を確認します。
- ポートが UP になったら、VEM に対して **module vem** *module-number* **execute vemcmd show pc** コマンドを実行して、ポートが正しいサブグループに入っていることを確認します。
- **debug port-channel trace** コマンドを使用して、情報を収集します。

ポート チャネルが作成できない

症状	考えられる原因	解決策
ポート チャネルが作成できない。	システムのポート チャネルの最大数に達した。	コマンド **show port-channel summary** を使用して、すでに設定されているポート チャネルの数を確認します。Cisco Nexus 1000V 上では、最大 256 個のポート チャネルを持てます。

新しく追加したインターフェイスがポート チャネル内でオンラインにならない

症状	考えられる原因	解決策
新しく追加したインターフェイスがポート チャネル内でオンラインにならない。	ポート チャネル モードがオンになっている。	**1.** そのインターフェイスで使用されるポート プロファイル（ポート グループ）にポート チャネルの設定があることを確認します。 **2.** 同じポート プロファイルを使用するモジュール上にすでにポート チャネルが存在するかどうかを確認します。存在する場合は、そのポート チャネルの実行コンフィギュレーションと新しく追加したインターフェイスを確認します。ポート チャネルの設定が違っていると、インターフェイスは UP になりません。 **3.** ポート チャネルの設定が違う場合は、違う部分を新しく追加したインターフェイスに適用してください。ポートを削除して、追加し直します。
	インターフェイス パラメータが、既存ポートのものと互換性がない。	「ポート チャネルの特性をインターフェイスに強制する」（P.10-5）の手順に従って、物理インターフェイスに強制的にポート チャネルのパラメータを取らせます。この手順を行うのは、ポート プロファイルを通じてではなく、手動でポート チャネルを設定したい場合だけにしてください。

ポート チャネルの特性をインターフェイスに強制する

この手順を使用して、物理インターフェイスに強制的にポート チャネルの特性を取らせます。この手順を行うのは、ポート プロファイルを通じてではなく、手動でポート チャネルを設定したい場合だけにしてください。

はじめる前に

- コンフィギュレーション モードで CLI にログインします。
- 強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。

手順の詳細

ステップ 1　CLI コンフィギュレーション モードで、次のコマンドを入力します。

interface ethernet *slot/port*

これにより、インターフェイス コンフィギュレーション モードに入ります。

例：
```
switch(config)# interface ethernet 1/4
switch(config-if)
```

ステップ 2　次のコマンドを入力します。

channel-group ***channel-number*** **force**

互換性のない設定を持つ物理インターフェイスが、強制的にチャネル グループに追加されます。

例：
```
switch(config-if)# channel-group 5 force
switch(config-if)
```

ポート チャネルの設定の確認

この手順を使用して、ポート プロファイルを通じて、ポート チャネルの設定をデバッグします。

はじめる前に

- コンフィギュレーション モードで CLI にログインします。

手順の詳細

ステップ 1　**show port-profile name** *profile-name* コマンドを実行して、プロファイル内でポート チャネルが設定されていることを確認します。

ステップ 2　**show port-channel summary** コマンドを実行します。

ステップ 3　**debug port-channel trace** コマンドを実行します。

VLAN トラフィックがトランクを通過しない

症状	考えられる原因	解決策
VLAN トラフィックがトランクを通過しない。	VLAN が VLAN リスト内で許可されていない。	VLAN を許可される VLAN のリストに追加します。そのインターフェイスによって使用されるプロファイル内で、**switchport trunk allowed vlan add** *vlan-id* コマンドを使用します。

CHAPTER 11

レイヤ 2 スイッチング

この章では、レイヤ 2 スイッチングに関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「レイヤ 2 イーサネット スイッチングについて」（P.11-1）
- 「ポート モデル」（P.11-1）
- 「レイヤ 2 スイッチングの問題」（P.11-4）
- 「レイヤ 2 スイッチングの確認」（P.11-7）
- 「Microsoft NLB ユニキャスト モードのトラブルシューティング」（P.11-12）

レイヤ 2 イーサネット スイッチングについて

Nexus1000V は、多数の仮想ホストにまたがって広がる分散したレイヤ 2 仮想スイッチを提供します。これは、次の 2 つのコンポーネントから成ります。

- 仮想スーパーバイザ モジュール（VSM）。コントロール プレーン（CP）とも呼ばれ、スーパーバイザとして機能し、Cisco CLI、コンフィギュレーション、および高レベルの機能を含みます。
- 仮想イーサネット モジュール（VEM）。データ プレーン（DP）とも呼ばれ、ライン カードとして機能し、各仮想サーバ内で実行されてパケット転送やその他のローカライズ機能を処理します。

ポート モデル

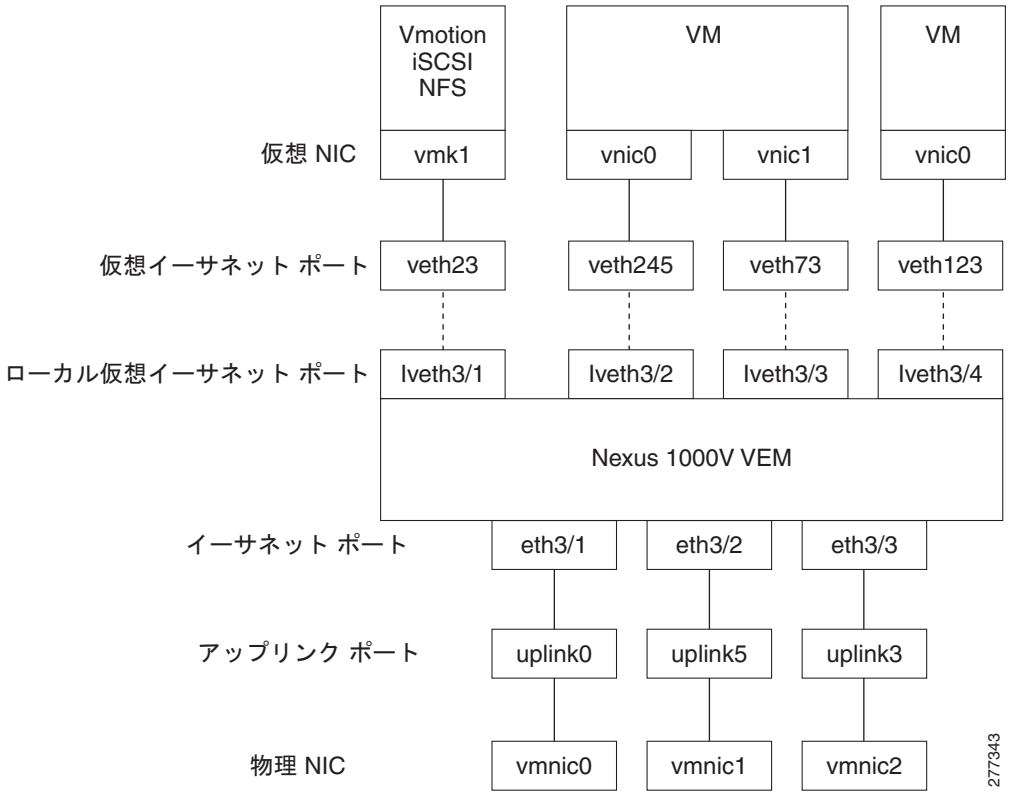
このセクションでは、次の観点からポートについて説明します。

- 「VEM から見たポート」（P.11-2）
- 「VSM から見たポート」（P.11-3）。

VEM から見たポート

Nexus1000V では、各 VEM での仮想ポートと物理ポートが区別されます。図 11-1 は、Nexus1000V スイッチ上のポートが VEM 内の物理 VMware ポートと仮想 VMware ポートにどのようにバインドされるかを示します。

図 11-1　VEM から見たポート



スイッチの仮想側には、一緒にマッピングされる次の 3 つのポート レイヤがあります。

- 仮想 NIC：VMware 内には 3 タイプの仮想 NIC があります。仮想 NIC（vnic）は、VM の一部であり、スイッチに接続されたホストの物理ポートを表します。仮想カーネル NIC（vmknic）は、管理のハイパーバイザ、VMotion、iSCSI、NFS、およびカーネルに必要とされるその他のネットワーク アクセスによって使用されます。このインターフェイスは、ハイパーバイザ自体の IP アドレスを伝送し、仮想イーサネット ポートにもバインドされます。vswif（示されていない）は、COS ベースのシステムにしか現れず、VMware 管理ポートとして使用されます。これらの各タイプが、Nexus1000V 内の Veth ポートにマッピングされます。
- 仮想イーサネット ポート（VEth）: VEth ポートは、Cisco Nexus 1000V Distributed Virtual Switch（DVS; 分散仮想スイッチ）上のポートです。Cisco Nexus 1000V は、VEth ポート 0 ～ N のフラットな空間を持ちます。仮想ケーブルは、VM を実行するホストに移動されるこれらの VEth ポートに接続されます。

  VEth ポートは、ポート グループに割り当てられます。
- ローカル仮想イーサネット ポート（lveth）：各ホストが、いくつものローカル VEth ポートを持ちます。これらのポートは、ホスト上で必要とされる VEth ポート用に動的に選択されます。

これらのローカル ポートは、移動することはなく、モジュール - ポート番号方式によってアドレス指定可能です。

スイッチの物理側では、下から上に向かって次のようになっています。

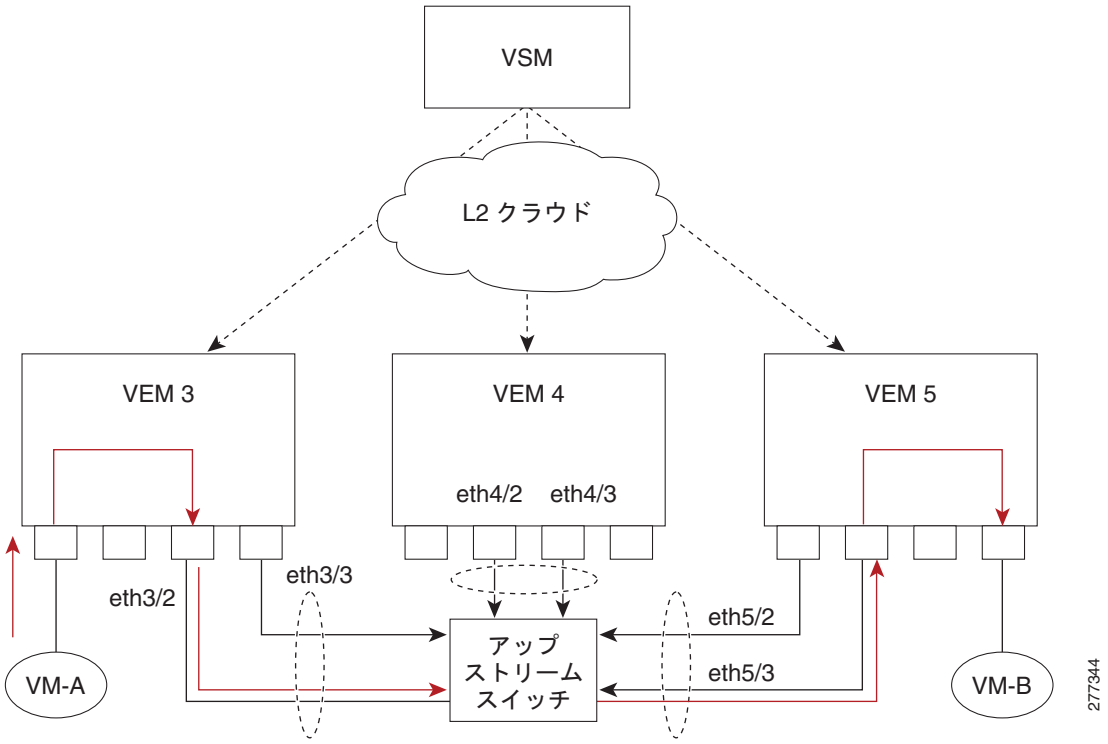
- VMware 内の各物理 NIC は、vmnic と呼ばれるインターフェイスによって表されます。vmnic 番号は、VMware のインストール時または新しい物理 NIC がインストールされたときに割り当てられ、ホストの寿命を通じて同じまま保たれます。
- ホスト上の各アップリンク ポートは、物理インターフェイスを表します。これは、lveth ポートと非常によく似た動作をしますが、物理ポートはホスト間で移動しないため、マッピングはアップリンク ポートと vmnic の間で 1:1 です。
- Nexus1000V スイッチに追加された各物理ポートが、ハードウェア ベースのスイッチ上にあるのとまったく同じように、物理イーサネット ポートとして現れます。

  アップリンク ポートの概念は、完全に VMware によって扱われ、ポート設定を vmnics に関連付けるために使用されます。アップリンクの番号と vmnic の番号の間には固定した関係はありません。これらは、ホストごとに異なっていてもかまわず、ホストの寿命を通じて変更可能です。VSM 上では、イーサネット インターフェイス番号（イーサネット 2/4 など）は、アップリンクの番号ではなく vmnic の番号から導出されます。

VSM から見たポート

図 11-2 に、VSM から見たポートを示します。

図 11-2　VSM から見たポート



ポート タイプ

次のタイプのポートを使用できます。

- Veth（仮想イーサネット インターフェイス）は、次のいずれか 1 つと関連付けできます。
  - ESX ホスト上の仮想マシンの VNIC
  - ESX ホストの VMKNIC
  - ESX COS ホストの VSWIF
- Eth（物理イーサネット インターフェイス）：ESX ホスト上の物理 NIC に対応します。
- Po（ポート チャネル インターフェイス）：ESX ホストの物理 NIC は、まとめて 1 つの論理インターフェイスにすることができます。この論理バンドルが、ポート チャネル インターフェイスと呼ばれます。

レイヤ 2 スイッチングの詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

レイヤ 2 スイッチングの問題

ここでは、レイヤ 2 の問題をトラブルシューティングする方法を説明し、トラブルシューティング コマンドの一覧を示します。ここでは、次の内容について説明します。

- 「VEM ポート間の接続の確認」（P.11-4）
- 「VEM 間の接続の確認」（P.11-5）
- 「トラフィック中断の特定」（P.11-6）
- 「レイヤ 2 スイッチングの確認」（P.11-7）

VEM ポート間の接続の確認

VEM 上の VEth ポート間の接続を確認するには、次の手順を実行します。

ステップ 1　VSM 上で、**show vlan** コマンドを入力して、ポートに関連付けられている VLAN の状態を確認します。ポートに関連付けられている VLAN がアクティブでない場合は、ポートはおそらくダウンしています。この場合は、VLAN を作成して、アクティブにする必要があります。

ステップ 2　VSM 上のポートの状態を見るには、**show interface brief** コマンドを入力します。

ステップ 3　**module vem** *module-number* **execute vemcmd show port** コマンドを実行して、VEM 上に現れているポートと、そのローカル インターフェイス インデックス、VLAN、タイプ（物理か仮想か）、CBL 状態、ポート モード、およびポート名を表示します。

出力の中で注目する必要のある主要項目は、次のとおりです。

- ポートの状態。
- CBL。
- モード。
- 接続されているデバイスの名前。

- トラブルシューティングしようとしているポートの LTL。この情報は、インターフェイス名が表示されないような他の VEM コマンドでインターフェイスをすばやく見つけるのに役立ちます。
- ポートの状態が UP になっていることの確認。UP になっていない場合は、VSM 上のポートの設定を確認してください。

ステップ 4　特定の VEM 上にある VLAN およびそのポートのリストを表示するには、**module vem** *module-number* **execute vemcmd show bd** コマンドを次のように使用します。

```
n1000V# module vem 5 execute vemcmd show bd
```

ポートが特定の VLAN に属していることを確認しようとしている場合は、必ずその VLAN のポートリスト内のポート名または LTL を見てください。

VEM 間の接続の確認

2 つの個別の VEM 上にある VEth ポート間の接続を確認するには、次の手順を実行します。

ステップ 1　**show vlan** コマンドを実行して、ポートに関連付けられている VLAN が VSM 上に作成されているか確認します。

ステップ 2　**show interface brief** コマンドを実行して、ポートが VSM 内で UP になっていることを確認します。

ステップ 3　VEM 上で、**module vem 3 execute vemcmd show port** コマンドを実行して、2 つのポートの CBL の状態が転送用の値である 1（アクティブ）に設定されているか確認します。

ステップ 4　VEM 上で、**module vem 3 execute vemcmd show bd** コマンドを実行して、2 つの VEth ポートが、それらが通信しようとしている相手 VLAN のフラッディング リストに入っているか確認します。

ステップ 5　VEM が接続されているアップリンク スイッチが、ポートの属している VLAN を伝送していることを確認します。

ステップ 6　アップストリーム スイッチのポートから、VEM 上の pnic（VLAN を伝送するはずのもの）が接続されているポートを探します。

```
n1000v# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device ID              Local Intrfce   Hldtme Capability  Platform      Port ID
swordfish-6k-2         Eth5/2        168    R S I       WS-C6506-E    Gig1/38
```

PNIC（Eth 5/2）は、ポート Gig1/38 上の swordfish-6k-2 に接続されています。

ステップ 7　アップストリーム スイッチにログインして、ポートが、探している VLAN を許可するように設定されていることを確認します。

```
n1000v#show running-config interface gigabitEthernet 1/38
Building configuration...

Current configuration : 161 bytes
!
interface GigabitEthernet1/38
 description Srvr-100:vmnic1
 switchport
 switchport trunk allowed vlan 1,60-69,231-233
```

```
 switchport mode trunk
end
```

この出力では、VLAN 1、60 ～ 69、231 ～ 233 がポート上で許可されています。注目している VLAN が許可されている VLAN のリストに入っていない場合は、それをポートの許可される VLAN リストに追加してください。

トラフィック中断の特定

次の手順を使用して、異なる複数の VEM 上の VM 間でトラフィックが伝送されなくなった原因を特定します。

ステップ 1　**show port-profile name** コマンドの出力から、次の情報を確認します。

- 設定したコントロール VLAN とパケット VLAN が存在する（例では、3002 と 3003 が該当）。
- 設定での物理 NIC が VM の VLAN を伝送する場合に、その VLAN も許可されている VLAN リストに入っている。

```
n1000v#show port-profile name alluplink
port-profile alluplink
  description:
  status: enabled
  system vlans: 3002,3003
  port-group: alluplink
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 1,80,3002,610,620,630-650
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 1,80,3002,3003,610,620,630-650
    no shutdown
  assigned interfaces:
    Ethernet2/2
```

ステップ 2　VM 内で、次のコマンドを使用して、イーサネット インターフェイスが UP になっていることを確認します。

ifconfig –a

UP になっていない場合は、その NIC を VM から削除し、別の NIC を追加することを検討します。

ステップ 3　任意の sniffer ツールを使用して、ARP 要求とその応答が VM インターフェイス上で受信されることを確認します。

ステップ 4　アップストリーム スイッチ上で、次のコマンドを使用して、IP と MAC アドレスの関連付けを探します。

debug arp
show arp

例：

```
n1000v_CAT6K# debug arp
ARP packet debugging is on
11w4d: RARP: Rcvd RARP req for 0050.56b7.3031
11w4d: RARP: Rcvd RARP req for 0050.56b7.3031
11w4d: RARP: Rcvd RARP req for 0050.56b7.4d35
11w4d: RARP: Rcvd RARP req for 0050.56b7.52f4
11w4d: IP ARP: rcvd req src 10.78.1.123 0050.564f.3586, dst 10.78.1.24 Vlan3002
```

```
11w4d: RARP: Rcvd RARP req for 0050.56b7.3031
n1000v_CAT6K#
```

例：

```
n1000v_CAT6K# sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.78.1.72             -   001a.6464.2008  ARPA
Internet  7.114.1.100            -   0011.bcac.6c00  ARPA   Vlan140
Internet  41.0.0.1               -   0011.bcac.6c00  ARPA   Vlan410
Internet  7.61.5.1               -   0011.bcac.6c00  ARPA   Vlan1161
Internet  10.78.1.5              -   0011.bcac.6c00  ARPA   Vlan3002
Internet  7.70.1.1               -   0011.bcac.6c00  ARPA   Vlan700
Internet  7.70.3.1               -   0011.bcac.6c00  ARPA   Vlan703
Internet  7.70.4.1               -   0011.bcac.6c00  ARPA   Vlan704
Internet  10.78.1.1              0   0011.bc7c.9c0a  ARPA   Vlan3002
Internet  10.78.1.15             0   0050.56b7.52f4  ARPA   Vlan3002
Internet  10.78.1.123            0   0050.564f.3586  ARPA   Vlan3002
```

ステップ 5　これで手順は完了です。

レイヤ 2 スイッチングの確認

レイヤ 2 MAC アドレス設定を表示し、検証するには、次のコマンドを使用します。

コマンド	目的
show mac address-table	MAC アドレス テーブルを表示し、VSM によって制御されている全 VEM の MAC アドレスをすべて確認します。 例 11-1（P.11-8）を参照してください。
show mac address-table module *module-number*	すべての MAC アドレスを指定された VEM 上に表示します。
show mac address-table static *HHHH.WWWW.HHHH*	MAC アドレス テーブルのスタティック エントリを表示します。 例 11-2（P.11-9）を参照してください。
show mac address-table address *HHHH.WWWW.HHHH*	MAC アドレスが指定されているインターフェイスが学習または設定されているかどうかを表示します。 • ダイナミック MAC の場合、同じ MAC が複数のインターフェイスに現れる場合は、そのそれぞれが個別に表示されます。 • スタティック MAC で同じ MAC が複数のインターフェイスに表れる場合は、設定されているインターフェイス上のエントリだけが表示されます。
show mac address-table static | inc veth	VEM 物理ポートがダイナミック MAC を学習し、パケット ソースが同じ VSM 上の別の VEM にある場合、vEthernet インターフェイスのスタティック MAC アドレスを表示します。 例 11-3（P.11-9）を参照してください。

コマンド	目的
show running-config vlan <vlan-id>	実行コンフィギュレーションに VLAN 情報を表示します。
show vlan [**all-ports** | **brief** | **id** <*vlan-id*> | **name** <*name*> | **dot1q tag native**]	VLAN 情報を指定されたとおりに表示します。 例 11-4（P.11-9）を参照してください。
show vlan summary	VLAN 情報の要約を表示します。
show interface brief	インターフェイスの状態表を表示します。 例 11-5（P.11-10）を参照してください。
module vem *module-number* **execute vemcmd show port**	VEM 上で、特定の VEM のポート状態を表示します。 このコマンドは、VEM からに限って実行できます。 例 11-6（P.11-10）を参照してください。
module vem *module-number* **execute vemcmd show bd** コマンド	指定された VEM について、その VLAN とそれらのポート リストを表示します。 例 11-7（P.11-11）を参照してください。
module vem *module-number* **execute vemcmd show trunk**	指定された VEM について、トランク ポート上の VLAN の状態を表示します。 • VLAN がポート上で転送している（アクティブな）場合、その CBL 状態は 1 になります。 • VLAN がブロックされている場合は、その CBL 状態は 0 です。 例 11-8（P.11-11）を参照してください。
module vem *module-number* execute vemcmd show l2 *vlan-id*	指定された VEM について、指定された VLAN の VLAN 転送テーブルを表示します。 例 11-9（P.11-12）を参照してください。
show interface *interface_id* **mac**	インターフェイスの MAC アドレスとバーンドイン MAC アドレスを表示します。

例 11-1　　show mac address-table

（注）　Cisco Nexus 1000V の MAC アドレス テーブルに、マルチキャスト MAC アドレスは表示されません。

ヒント　モジュールは、この MAC が表示される VEM を示します。

N1KV Internal Port は、VEM 上で作成された内部ポートを表します。このポートは、VEM の制御と管理に使用され、パケットの転送には使用されません。

```
n1000v# show mac address-table
VLAN      MAC Address       Type    Age       Port                          Module
---------+-----------------+-------+---------+-----------------------------+---------
1         0002.3d11.5502    static  0         N1KV Internal Port            3
1         0002.3d21.5500    static  0         N1KV Internal Port            3
1         0002.3d21.5502    static  0         N1KV Internal Port            3
1         0002.3d31.5502    static  0         N1KV Internal Port            3
1         0002.3d41.5502    static  0         N1KV Internal Port            3
```

```
1         0002.3d61.5500    static  0         N1KV Internal Port            3
1         0002.3d61.5502    static  0         N1KV Internal Port            3
1         0002.3d81.5502    static  0         N1KV Internal Port            3
3         12ab.47dd.ff89    static  0         Eth3/3                        3
342       0002.3d41.5502    static  0         N1KV Internal Port            3
342       0050.568d.5a3f    dynamic 0         Eth3/3                        3
343       0002.3d21.5502    static  0         N1KV Internal Port            3
343       0050.568d.2aa0    dynamic 9         Eth3/3                        3
Total MAC Addresses: 13
n1000v#
```

例 11-2　show mac address-table address

ヒント このコマンドは、MAC が動的に学習されたすべてのインターフェイスを表示します。この例では、同じ MAC が Eth3/3 と Eth4/3 の両方に現れています。

```
n1000v# show mac address-table address 0050.568d.5a3f
VLAN      MAC Address       Type    Age       Port                          Module
---------+-----------------+-------+---------+-----------------------------+---------
342       0050.568d.5a3f    dynamic 0         Eth3/3                        3
342       0050.568d.5a3f    dynamic 0         Eth4/3                        4
Total MAC Addresses: 1
n1000v#
```

例 11-3　show mac address-table static | inc veth

```
n1000v# show mac address-table static | inc veth
460       0050.5678.ed16    static  0         Veth2                         3
460       0050.567b.1864    static  0         Veth1                         4
n1000v#
```

例 11-4　show vlan

ヒント このコマンドは、VSM 上で作成された各 VLAN の状態を表示します。

```
n1000v# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Eth3/3, Eth3/4, Eth4/2, Eth4/3
110  VLAN0110                         active
111  VLAN0111                         active
112  VLAN0112                         active
113  VLAN0113                         active
114  VLAN0114                         active
115  VLAN0115                         active
116  VLAN0116                         active
117  VLAN0117                         active
118  VLAN0118                         active
119  VLAN0119                         active
800  VLAN0800                         active
801  VLAN0801                         active
802  VLAN0802                         active
803  VLAN0803                         active
804  VLAN0804                         active
805  VLAN0805                         active
```

```
806  VLAN0806                          active
807  VLAN0807                          active
808  VLAN0808                          active
809  VLAN0809                          active
810  VLAN0810                          active
811  VLAN0811                          active
812  VLAN0812                          active
813  VLAN0813                          active
814  VLAN0814                          active
815  VLAN0815                          active
816  VLAN0816                          active
817  VLAN0817                          active
818  VLAN0818                          active
819  VLAN0819                          active
820  VLAN0820                          active
VLAN Name                              Status    Ports
---- -------------------------------- --------- -------------------------------
---- -------------------------------- --------- -------------------------------

Remote SPAN VLANs
-------------------------------------------------------------------------------

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
```

例 11-5　show interface brief

```
n1000v# show int brief

--------------------------------------------------------------------------------
Port      VRF          Status IP Address                     Speed    MTU
--------------------------------------------------------------------------------
mgmt0     --            up     172.23.232.143                 1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/4        1      eth  trunk  up      none                       1000(D) --
Eth4/2        1      eth  trunk  up      none                       1000(D) --
Eth4/3        1      eth  trunk  up      none                       1000(D) --
```

例 11-6　module vem *module-number* execute vemcmd show port

ヒント　ポートの状態を検出します。

```
~ # module vem 3 execute vemcmd show port
  LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
    8          0   3969       0      2           2  VIRT     UP    UP    1 Access 120
    9          0   3969       0      2           2  VIRT     UP    UP    1 Access 121
   10          0    115       0      2           0  VIRT     UP    UP    1 Access 122
   11          0   3968       0      2           2  VIRT     UP    UP    1 Access 123
   12          0    116       0      2           0  VIRT     UP    UP    1 Access 124
   13          0      1       0      2           2  VIRT     UP    UP    0 Access 125
   14          0   3967       0      2           2  VIRT     UP    UP    1 Access 126
   16   1a030100      1 T     0      0           2  PHYS     UP    UP    1 Trunk
vmnic1
```

```
   17   1a030200      1 T     0      2           2  PHYS     UP    UP    1 Trunk
vmnic2
```

例 11-7　module vem *module-number* execute vemcmd show bd

ヒント ポートが特定の VLAN に属している場合は、ポート名または LTL がその VLAN のポート リストに表示されます。

```
~ # module vem 5 execute vemcmd show bd
Number of valid BDS: 8
BD 1, vdc 1, vlan 1, 2 ports
Portlist:
16 vmnic1
17 vmnic2
BD 100, vdc 1, vlan 100, 0 ports
Portlist:
BD 110, vdc 1, vlan 110, 1 ports
Portlist:
16 vmnic1
BD 111, vdc 1, vlan 111, 1 ports
Portlist:
16 vmnic1
BD 112, vdc 1, vlan 112, 1 ports
Portlist:
16 vmnic1
BD 113, vdc 1, vlan 113, 1 ports
Portlist:
16 vmnic1
BD 114, vdc 1, vlan 114, 1 ports
Portlist:
16 vmnic1
BD 115, vdc 1, vlan 115, 2 ports
Portlist:
10 l22
16 vmnic1
```

例 11-8　module vem *module-number* execute vemcmd show trunk

ヒント VLAN がポート上でアクティブな場合、その CBL 状態は 1 になります。
VLAN がブロックされている場合は、その CBL 状態は 0 です。

```
~ # module vem 5 execute vemcmd show trunk
Trunk port 16 native_vlan 1 CBL 1
vlan(1) cbl 1, vlan(110) cbl 1, vlan(111) cbl 1, vlan(112) cbl 1, vlan(113) cbl 1,
vlan(114) cbl 1,vlan(115) cbl 1, vlan(116) cbl 1, vlan(117) cbl 1, vlan(118) cbl 1,
vlan(119) cbl 1,
Trunk port 17 native_vlan 1 CBL 0
vlan(1) cbl 1, vlan(117) cbl 1,
~ #
```

例 11-9　module vem *module-number* execute vemcmd show l2

```
Bridge domain 115 brtmax 1024, brtcnt 2, timeout 300
Dynamic MAC 00:50:56:bb:49:d9 LTL 16 timeout 0
Dynamic MAC 00:02:3d:42:e3:03 LTL 10 timeout 0
```

Microsoft NLB ユニキャスト モードのトラブルシューティング

Microsoft Network Load Balancing（MS-NLB）は、Windows サーバのオペレーティング システムの一部として Microsoft 社から提供されるクラスタリング テクノロジーです。クラスタリングは、アベイラビリティの改善、管理の簡素化、スケーラビリティの向上のために、1 つのシステムとして管理する独立したサーバのグループをイネーブルにします。

Microsoft Network Load Balancing の詳細については、次の URL を参照してください。

http://technet.microsoft.com/en-us/library/bb742455.aspx

（注）このマニュアル内で示されているサードパーティ Web サイトへのアクセスは、お客様に便宜を図ることのみを目的として提供されています。シスコおよびその関連会社は、サードパーティ Web サイトの動作の保証についていかなる責任も負いません。また、サードパーティ Web サイトを通じてアクセスしたソフトウェア プログラム等のダウンロード、パフォーマンス、品質、動作、サポートについても一切責任を負いません。さらに、サードパーティ Web サイトまたはそれらを通じてアクセスしたプログラム等により発生したいかなる損害、修理、修正、費用についても一切の責任を負いません。シスコのエンド ユーザ ライセンス契約書は、サードパーティ Web サイトおよびそれらの Web サイトを通じてアクセスされるソフトウェア プログラムの使用条件に適用されるものではありません。

制限事項と制約事項

MS-NLB の自動スタティック MAC 学習をディセーブルにしようとした際に次のいずれかのコンフィギュレーションが存在する場合は、これらの機能をサポートしていないため、Syslog が生成されます。

- PVLAN ポート
- 不明なユニキャスト フラッド ブロッキング（UUFB）で設定されているポート
- switchport port-security mac-address sticky で設定されているポート

vEthernet 上での自動スタティック MAC 学習のディセーブル化

vEthernet（vEth）を正常に設定するには、事前に自動スタティック MAC 学習をディセーブルにしておく必要があります。

インターフェイス コンフィギュレーション モードで、次のコマンドを使用します。

```
switch(config)# int veth 1
switch(config-if)# no mac auto-static-learn
```

ポート プロファイル コンフィギュレーション モードで、次のコマンドを使用します。

```
switch(config)# port-profile type vethernet ms-nlb
```

```
switch(config-port-prof)# no mac auto-static-learn
```

VSM のステータスの確認

NLB のユニキャスト モード設定が機能しない場合は、仮想スーパーバイザ モジュール（VSM）のステータスを確認します。

vEth またはポート プロファイル ポート プロファイル コンフィギュレーションまたはその両方で、**no mac auto-static-learn** がリストされていることを確認します。

VSM のステータスを生成するには、インターフェイス コンフィギュレーション モードで、次のコマンドを使用します。

switch(config-if)# show running-config int veth1

```
interface Vethernet1
  inherit port-profile vm59
  description Fedora117, Network Adapter 2
  no mac auto-static-learn
  vmware dvport 32 dvswitch uuid "ea 5c 3b 50 cd 00 9f 55-41 a3 2d 61 84 9e 0e c4"
```

VSM のステータスを生成するには、ポート プロファイル コンフィギュレーション モードで、次のコマンドを使用します。

switch(config-if)# show running-config port-profile ms-nlb

```
port-profile type vethernet ms-nlb
  vmware port-group
  switchport mode access
  switchport access vlan 59
  no mac auto-static-learn
  no shutdown
  state enabled
```

VEM のステータスの確認

NLB のユニキャスト モード設定が機能しない場合は、仮想イーサネット モジュール（VEM）のステータスを確認します。次の点をチェックします。

- MS-NLB veths がディセーブルであることを確認します。
- MS-NLB shared-MAC（02:BF で開始）がレイヤ 2（L2）MAC テーブルにリストされていないことを確認します。

VEM のステータスを生成するには、次のコマンドを使用します。

~ # vemcmd show port auto-smac-learning

```
  LTL   VSM Port  Auto Static MAC Learning
   49      Veth4   DISABLED
   50      Veth5   DISABLED
   51      Veth6   DISABLED
```

VLAN59 の L2 MAC テーブルを生成するには、次のコマンドを使用します。

~ # vemcmd show l2 59

```
Bridge domain   15 brtmax 4096, brtcnt 6, timeout 300

VLAN 59, swbd 59, ""

Flags:  P - PVLAN  S - Secure  D - Drop

       Type         MAC Address   LTL   timeout   Flags    PVLAN
```

```
Dynamic   00:15:5d:b4:d7:02   305         4
Dynamic   00:15:5d:b4:d7:04   305        25
Dynamic   00:50:56:b3:00:96    51         4
Dynamic   00:50:56:b3:00:94   305         5
Dynamic   00:0b:45:b6:e4:00   305         5
Dynamic   00:00:5e:00:01:0a    51         0
```

CHAPTER 12

VLAN

この章では、VLAN の実装時に発生する可能性がある問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「VLAN について」（P.12-1）
- 「トラブルシューティングの初期チェックリスト」（P.12-2）
- 「VLAN を作成できない」（P.12-3）

VLAN について

VLAN では、物理的には同じネットワークに接続されていても、論理的には相互に認識する必要のない、異なる LAN に位置すると見なされるデバイスを分離できます。

VLAN 名では次の文字だけを使用することを推奨します。

- a ～ z または A ～ Z
- 0 ～ 9
- -（ハイフン）
- _（アンダースコア）

VLAN については、次のガイドラインを考慮してください。

- ユーザ トラフィックを管理 VLAN から切り離し、管理 VLAN をユーザ データから分離します。

（注） プライベート VLAN を設定する場合、スティッキ Address Resolution Protocol（ARP; アドレス解決プロトコル）をイネーブルにすることを推奨します。レイヤ 3 プライベート VLAN インターフェイスで学習される ARP エントリは、スティッキ ARP エントリになります。セキュリティ上の理由から、プライベート VLAN ポートのスティッキ ARP エントリには期限切れがありません。

- IGMP は、プライマリ VLAN 上でだけ実行され、すべてのセカンダリ VLAN にプライマリ VLAN の設定が使用されます。
- セカンダリ VLAN 内の IGMP 加入要求は、プライマリ VLAN で受信されたものとして処理されます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN ポートを SPAN 送信元ポートとして設定できます。
  - VLAN ベースの SPAN（VSPAN）はプライマリ VLAN、独立 VLAN、およびコミュニティ VLAN で使用できます。また、出力または入力トラフィックを別々にモニタするために、1 つの VLAN でだけ SPAN を使用できます。

- プライベート VLAN ホストまたは混合ポートは、SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定すると、ポートは非アクティブになります。
- 宛先 SPAN ポートは、独立ポートにしないでください（ただし、ソース SPAN ポートは独立ポートにできます）。
- SPAN は、プライマリ VLAN またはセカンダリ VLAN の両方にまたがるように設定できます。またはユーザが入力トラフィックか出力トラフィックにだけ関係する場合は、いずれか 1 つを補うように設定できます。
- セカンダリ VLAN で学習された MAC アドレスは、プライマリ VLAN の共有テーブルに追加されます。セカンダリ VLAN がプライマリ VLAN に関連付けられると、セカンダリ VLAN の MAC アドレス テーブルは単一の共有 MAC テーブルにマージされます。

トラブルシューティングの初期チェックリスト

VLAN の問題のトラブルシューティングでは、個々のデバイスおよびネットワーク全体の設定と接続に関する情報を収集する必要があります。VLAN の場合は、次のようにしてトラブルシューティング作業を開始します。

チェックリスト	√
問題のあるポートまたは VLAN の物理接続を確認します。	
両方のエンド デバイスが同じ VLAN にあることを確認します。	

次の CLI コマンドを使用して、VLAN 情報を表示します。

- **show system internal private-vlan info**
- **show system internal private-vlan event-history errors**
- **show system internal private-vlan event-history traces**
- **show vlan id** *vlan-id*
- **show vlan private-vlan**
- **show vlan all-ports**
- **show vlan private-vlan type**
- **show vlan internal bd-info vlan-to-bd 1**
- **show vlan internal errors**
- **show vlan internal info**
- **show vlan internal event-history errors**

VLAN を作成できない

症状	考えられる原因	解決策
VLAN を作成できない。	予約された VLAN ID を使用している。	VLAN 3968 ～ 4047 および 4094 は内部使用のために予約されており、変更できません。

CHAPTER 13

プライベート VLAN

この章では、プライベート VLAN に関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「プライベート VLAN について」（P.13-1）
- 「トラブルシューティングのガイドライン」（P.13-2）
- 「プライベート VLAN トラブルシューティング コマンド」（P.13-2）

プライベート VLAN について

プライベート VLAN（PVLAN）は、レイヤ 2 ISP トラフィックを分離して、単一のルータ インターフェイスへと伝送するのに使用されます。PVLAN は、レイヤ 2 は分離したうえで、エンド デバイスが同一の IP サブネットを共有することを可能にするレイヤ 2 転送制約を適用することによって、デバイス分離を実現します。したがって、より大きいサブネットを使用すると、アドレス管理のオーバーヘッドが低減します。接続されている各エンドポイントが同一プライベート VLAN ドメイン内のその他の接続エンドポイントと通信できるかどうかを制御する独自の一連のルールをそれぞれで持っている 3 つの独立したポート指定が使用されます。

プライベート VLAN ドメイン

プライベート VLAN ドメインは、1 つまたは複数の VLAN ペアから成ります。プライマリ VLAN がドメインを形成し、各 VLAN ペアがサブドメインを形成します。ペアになっている VLAN は、プライマリ VLAN とセカンダリ VLAN と呼ばれます。1 つのプライベート VLAN 内の VLAN ペアはすべて、同一のプライマリ VLAN を持ちます。セカンダリ VLAN ID が、サブドメイン間を区別するためのものです。

複数のスイッチのスパニング

プライベート VLAN は、通常の VLAN とまったく同じように、複数のスイッチにまたがることができます。スイッチ間リンク ポートは、特殊な VLAN タイプを認識する必要がなく、これらの VLAN でタグ付けされたフレームもその他のフレームとまったく同じように伝送します。プライベート VLAN は、1 つのスイッチ内の独立ポートからのトラフィックが、スイッチ間リンクを伝送されたあと、別のスイッチ内の他の独立ポートまたはコミュニティ ポートに到達しない状態を確保します。VLAN レベルでの分離情報を埋め込み、それをパケットと一緒に伝送することにより、ネットワーク全体での一貫した動作の維持が可能になります。このため、レイヤ 2 通信を同一スイッチ内の 2 つの独立ポート間に限定するメカニズムが、2 つの異なるスイッチ内の 2 つの独立ポート間へのレイヤ 2 通信の限定も行います。

プライベート VLAN ポート

プライベート VLAN ドメイン内には、3 つの独立したポート指定があります。各ポート指定が独自の一連のルールを持っており、これが、1 つのエンドポイントが同一プライベート VLAN ドメイン内にある他の接続エンドポイントと通信する能力を制御します。次に示すのが、その 3 つのポート指定です。

- promiscuous
- isolated
- community

プライベート VLAN の詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

トラブルシューティングのガイドライン

プライベート VLAN の問題をトラブルシューティングする際には、次のガイドラインに従ってください。

- **show vlan** *private-vlan* コマンドを使用して、プライベート VLAN が正しく設定されていることを確認します。
- **show interface** *slot-port* コマンドを使用して、インターフェイスが UP になっていることを確認します。
- **module vem** *module-number* **execute vemcmd show port** コマンドを使用して、VEM が正しく設定されていることを確認します。

プライベート VLAN トラブルシューティング コマンド

ここに挙げるコマンドが、プライベート VLAN 関連の問題のトラブルシューティングに使用できます。

プライベート VLAN が正しく設定されていることを確認するには、次のコマンドを使用します。

- **show vlan private-vlan**

```
n1000V# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
152      157        community
152      158        isolated
156      153        community
156      154        community
156      155        isolated
```

プライベート VLAN トランク無差別モードの物理イーサネット インターフェイスが UP になっていることを確認するには、次のコマンドを使用します。

- **show interface**

```
n1000V# show int eth3/4
Ethernet3/4 is up
  Hardware: Ethernet, address: 0050.565a.ca50 (bia 0050.565a.ca50)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA
  Port mode is Private-vlan trunk promiscuous
  full-duplex, 1000 Mb/s
  Beacon is turned off
```

```
  Auto-Negotiation is turned off
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
    Rx
    158776 Input Packets 75724 Unicast Packets
    76 Multicast Packets 82976 Broadcast Packets
    13861581 Bytes
    Tx
    75763 Output Packets 75709 Unicast Packets
    3 Multicast Packets 51 Broadcast Packets 0 Flood Packets
    7424670 Bytes
    5507 Input Packet Drops 0 Output Packet Drops
  2 interface resets
```

プライベート VLAN ホスト モードの仮想イーサネット インターフェイスが UP になっていることを確認するには、次のコマンドを使用します。

- **show interface**

```
n1000V# show int v3
Vethernet3 is up
    Hardware is Virtual, address is 0050.56bb.6330
    Owner is VM "fedora9", adapter is Network Adapter 1
    Active on module 3
    VMware DVS port 10
    Port-Profile is pvlancomm153
    Port mode is Private-vlan host
    Rx
    14802 Input Packets 14539 Unicast Packets
    122 Multicast Packets 141 Broadcast Packets
    1446568 Bytes
    Tx
    15755 Output Packets 14492 Unicast Packets
    0 Multicast Packets 1263 Broadcast Packets 0 Flood Packets
    1494886 Bytes
    45 Input Packet Drops 0 Output Packet Drops
```

VEM が正しく設定されていることを確認するには、次のコマンドを使用します。

- **module vem** *module-number* **execute vemcmd show port**

```
n1000V# module vem 3 execute vemcmd show port
  LTL    IfIndex   Vlan    Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode   Name
    8          0   3969       0      2           2  VIRT     UP    UP    4 Access l20
    9          0   3969       0      2           2  VIRT     UP    UP    4 Access l21
   10          0    150       0      2           2  VIRT     UP    UP    4 Access l22
   11          0   3968       0      2           2  VIRT     UP    UP    4 Access l23
   12          0    151       0      2           2  VIRT     UP    UP    4 Access l24
   13          0      1       0      2           2  VIRT     UP    UP    0 Access l25
   14          0   3967       0      2           2  VIRT     UP    UP    4 Access l26
   16   1a020100      1 T     0      2           2  PHYS     UP    UP    4  Trunk
vmnic1
   18   1a020300      1 T     0      2           2  PHYS     UP    UP    4  Trunk
vmnic3
        pvlan promiscuous trunk port
            153 --> 156
            154 --> 156
            155 --> 156
            157 --> 152
            158 --> 152
   19   1a020400      1 T     0      2           2  PHYS     UP    UP    4  Trunk
vmnic4
        pvlan promiscuous trunk port
            153 --> 156
```

```
            154 --> 156
            155 --> 156
            157 --> 152
            158 --> 152
   47   1b020000    154       0      2           0  VIRT     UP    UP    4 Access
fedora9.eth0
        pvlan community 156 153
```

シスコ テクニカル サポートがプライベート VLAN の問題をトラブルシューティングするためにその他の情報が必要な場合は、次のコマンドを使用します。

- **show system internal private-vlan info**
- **show system internal private-vlan event-history traces**

CHAPTER 14

NetFlow

この章では、Netflow に関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「NetFlow 情報」（P.14-1）
- 「NetFlow トラブルシューティング コマンド」（P.14-2）
- 「NetFlow の一般的な問題」（P.14-3）

NetFlow 情報

NetFlow は、IP トラフィックを評価し、IP トラフィックがどこでどのようにして流れているかを理解することを可能にするテクノロジーです。NetFlow は、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングで使用できるデータを収集します。

フローとは、ソース インターフェイス（またはサブインターフェイス）に到達し、一連の基準に一致するパケットの一方向ストリームです。同じ送信元/宛先 IP アドレス、送信元/宛先ポート、プロトコル インターフェイス、サービス クラスを持つすべてのパケットがグループ化されて 1 つのフローに入れられ、パケットとバイトが集計されます。これにより、大量のネットワーク情報が NetFlow キャッシュと呼ばれるデータベースに凝縮されます。

フローは、収集する基準を定義することにより作成します。フロー情報から、次の情報がわかります。

- 送信元アドレスから、誰がトラフィックを送信したかがわかります。
- 宛先アドレスから、誰がトラフィックを受信するかがわかります。
- ポートは、トラフィックを使用するアプリケーションの特性を示します。
- サービス クラスからは、トラフィックの優先度がわかります。
- デバイス インターフェイスから、トラフィックがネットワーク デバイスによってどのように使用されるかがわかります。
- 集約されたパケットとバイトは、トラフィックの量を示します。

フロー レコードは、フロー内のパケット、フローごとに収集されるカウンタのタイプなどの NetFlow が収集する情報を定義します。新しいフロー レコードを自分で定義することもできれば、定義済みの Nexus 1000V フロー レコードを使用することもできます。

NetFlow 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。

NetFlow トラブルシューティング コマンド

ここに挙げるコマンドは、NetFlow 関連の問題のトラブルシューティングに使用できるものです。

- **debug logfile *filename***：このコマンドは、次のデバッグ コマンドの出力をブートフラッシュ内に保存されるファイルにリダイレクトします。
  - **debug nfm all**
  - **debug sf_nf_srv all**
- **vemdebug netflow dump policy :** このコマンドでは、VEM 上のインターフェイスに正しいポリシーがインストールされているかどうかを検証できます。このコマンドの出力は、vemlog 内部バッファに送られます。出力に通常どおりのキャッシュ タイプが表示され、正しいキャッシュ サイズとキャッシュ タイマー値が表示されることを確認してください。

```
Apr 14 12:20:51.504410        19   2    2  16   Debug Port 49 has 1
monitors for dir INPUT traffic IPV4
Apr 14 12:20:51.504412        20   2    2  16   Debug Flow Monitor fm1:
Apr 14 12:20:51.504413        21   2    2  16   Debug   Description:
fm1
Apr 14 12:20:51.504413        22   2    2  16   Debug   Monitor ID:
3
Apr 14 12:20:51.504413        23   2    2  16   Debug   Cache:
Apr 14 12:20:51.504414        24   2    2  16   Debug     Type:
normal
Apr 14 12:20:51.504414        25   2    2  16   Debug     Status:
allocated
Apr 14 12:20:51.504415        26   2    2  16   Debug     Size:
256 entries
Apr 14 12:20:51.504415        27   2    2  16   Debug     Inactive
Timeout:  15 secs
Apr 14 12:20:51.504416        28   2    2  16   Debug     Active
Timeout:    1800 secs
```

- **vemdebug netflow dump pakstore :** このコマンドは、インターフェイス上のポリシーについて、pakstore の使用状況をダンプします。出力は、vemlog 内部バッファに送られます。出力に正しいモニタ名とインターフェイスが表示されることを確認してください。

```
Apr 14 12:25:30. 29787       260   0    2  16   Debug Pak Store for
Client: fm1
Apr 14 12:25:30. 29793       266   0    2  16   Debug Pak Store for
Client: LTL49
```

- **vemlog debug sfnetflow_cache all**
- **vemlog debug sfnetflow_config all**
- **vemlog debug sfnetflow_flowapi all**

  これらのコマンドで、VEM 上のポリシー インストールの NetFlow デバッグが行えます。DPA からの要求を開いて、検証し、コミットするすべての PDL セッションについて、デバッグ メッセージが出力されます。
- **vemlog debug sfnetflow all**

  このコマンドで、VEM 上の Netflow ポリシーのパケット パスのデバッグが行えます。NetFlow ポリシーにヒットしたすべてのパケットについて、デバッグ メッセージが出力されます。このコマンドの使用に当たっては、十分注意してください。多数のデバッグ メッセージで大量のトラフィックが発生する場合があります。

次のコマンドでは、NFM プロセス ランタイム設定エラーに関する情報が収集できます。

- **show flow internal event-history errors**

- **show flow internal event-history msgs**
- **show flow internal ddb b**
- **show flow internal mem-stats**（メモリの使用状況とリークのデバッグのために）

次のコマンドでは、sf_nf_srv プロセス ラインタイム情報が収集できます。

- **show system internal sf_nf_srv event-history errors**
- **show system internal sf_nf_srv event-history msgs**
- **show system internal sf_nf_srv pdl detailed**
- **show system internal sf_nf_srv mem-stats**（メモリの使用状況とリークのデバッグのために）

NetFlow の一般的な問題

VSM 上での NetFlow の設定に関する一般的な問題は、次のような操作を行おうとしたときに発生します。

- 未定義のレコード、エクスポータ、サンプラー、またはモニタを使用した。
- 無効なレコード、エクスポータ、サンプラー、またはモニタを使用した。
- レコード、エクスポータ、サンプラー、またはモニタをインターフェイスに適用したあとに修正した。
- インターフェイス上のモニタを設定し、それが VEM のメモリ不足を発生させ、検証エラーが発生した。
- NetFlow をポート チャネルで使用した。NetFlow は、ポート チャネルでサポートされていません。

さらに、エクスポータで設定されている UDP ポートと NetFlow Collector でのリッスンが有効になっているポートが一致しない場合にも設定エラーが発生します。

ポリシー検証エラーのデバッグ

VSM 上での何らかの処理が原因で発生したポリシー検証の失敗をデバッグするには、次の手順を実行します。

ステップ 1　**debug nfm all** コマンドを実行します。

ステップ 2　**debug sf_nf_srv_all** コマンドを実行します。

ステップ 3　Telnet SSH セッション バッファをファイルに保存します。

ステップ 4　**ip flow mon** *monitor name direction* コマンドを実行します。

コマンドがもう一度実行され、デバッグ トレースがコンソールに出力されます。

ポリシー検証手順を使用して、フロー レコードの定義やエクスポータ機能のトレースなどの操作のログを収集することもできます。

統計情報エクスポートのデバッグ

NetFlow 統計情報のエクスポートに関する問題をデバッグする際には、次のガイドラインに従ってください。

- 宛先 IP アドレスが VSM から到達できることを確認します。
- エクスポータに設定されている UDP が NetFlow Collector によって使用されるものと一致していることを確認します。
- **show flow exporter** コマンドを実行して、エクスポータの統計情報を表示し、VSM 上でドロップが発生していないか確認します。

CHAPTER 15

ACL

この章では、アクセス コントロール リスト（ACL）に関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「アクセス コントロール リスト（ACL）について」（P.15-1）
- 「ACL 設定の制限事項」（P.15-2）
- 「ACL の制限事項」（P.15-2）
- 「ACL のトラブルシューティング」（P.15-2）
- 「VEM での ACL ポリシーの表示」（P.15-3）
- 「ポリシー検証に関する問題のデバッグ」（P.15-3）

アクセス コントロール リスト（ACL）について

ACL は、トラフィックをフィルタリングするための順番に並べられた一連のルールです。デバイスは、パケットを適用する ACL を決定する際に、パケットをルールに対してテストしていきます。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するルールがない場合は、そのデバイスでのデフォルト ルールが適用されます。デバイスは、許可されたパケットは処理し、拒否されたパケットは廃棄します。

ACL は、ネットワークおよび特定のホストを不必要なトラフィックや望ましくないトラフィックから保護します。たとえば、ACL を使用して、セキュリティの高いネットワークからインターネットへの HTTP は許可しないようにしたりできます。ACL では、サイトの IP アドレスを使用して IP ACL 内でサイトを識別することにより、特定のサイトへの HTTP トラフィックだけを許可するといったこともできます。

トラフィックのフィルタリングに、次のタイプの ACL がサポートされています。

- IP ACL：IP ACL は IP トラフィックにだけ適用されます。
- MAC ACL：MAC ACL は非 IP トラフィックにだけ適用されます。

ACL ルールを使用してネットワーク トラフィックを設定する方法の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ACL 設定の制限事項

ACL には、次の設定上の制限事項が適用されます。

- 1 つの ACL に入れられるルールは 128 個までです。
- 1 つの VEM 内に 10,000 個を超える ACL を持つことはできません（すべての ACL にわたって拡散）。

ACL の制限事項

ACL には次の制限事項が適用されます。

- インターフェイス上の各方向に 1 つの IP ACL と 1 つの MAC ACL よりも多くの ACL を適用することはできません。
- MAC ACL は、レイヤ 2 パケットにしか適用されません。
- VLAN ACL はサポートされていません。
- ACL ルールでは IP フラグメントはサポートされていません。
- 非初期フラグメントは、ACL ルックアップの対象になりません。
- TCP フラグを指定するために制定されたオプションは、サポートされていません。
- 同一ルール内に 2 つの neq（等しくない）演算子を入れることはできません。
- ACL は、ポート チャネルでサポートされていません。

ACL のトラブルシューティング

ここに挙げるコマンドは、インターフェイスに対して設定され適用されているポリシーを見るために VSM 上で使用できるものです。

次のコマンドは、設定済みの ACL を表示するために使用できます。

- **show access-list summary**

次のコマンドは、設定エラーの中での ACLMGR および ACLCOMP のランタイム情報を表示したり、ACLMGR プロセス ランタイム情報設定エラーを収集したりするために VSM 上で使用できます。

- **show system internal aclmgr event-history errors**
- **show system internal aclmgr event-history msgs**
- **show system internal aclmgr ppf**
- **show system internal aclmgr mem-stats**（メモリの使用状況とリークのデバッグのために）
- **show system internal aclmgr status**
- **show system internal aclmgr dictionary**

次のコマンドは、ACLCOMP プロセス ランタイム情報設定エラーの収集に使用できます。

- **show system internal aclcomp event-history errors**
- **show system internal aclcomp event-history msgs**
- **show system internal aclcomp pdl detailed**
- **show system internal aclcomp mem-stats**（メモリの使用状況とリークのデバッグのために）

VEM での ACL ポリシーの表示

ここに挙げるコマンドは、VEM 上の設定済み ACL ポリシーの表示に使用できます。

次のコマンドは、そのサーバにインストールされている ACL のリストを表示します。

```
~ # module vem 3 execute vemcmd show acl
Acl-id Ref-cnt  Type Numrules  Stats
    1      1    IPv4      1    disabled
```

Acl-id は、この VEM のローカル ACLID です。Ref-cnt は、この VEM 内のこの ACL のインスタンスの数です。

次のコマンドは、ACL がインストールされているインターフェイスのリストを表示します。

```
~ # module vem 3 execute vemcmd show acl pinst
LTL   Acl-id    Dir
 16       1    ingress
```

ポリシー検証に関する問題のデバッグ

ポリシー検証のエラーをデバッグするには、次の手順を実行します。

ステップ 1　VSM で、**debug logfile** *filename* コマンドを入力して、出力をブートフラッシュ内のファイルにリダイレクトします。

ステップ 2　**debug aclmgr all** コマンドを入力します。

ステップ 3　**debug aclcomp all** コマンドを入力します。

ポリシーが置かれているか、または対象となっている VEM に対して、VSM から次の手順を実行します。出力は、コンソールに表示されます。

ステップ 4　**module vem** *module-number* **execute vemdpalog debug sfaclagent all** コマンドを入力します。

ステップ 5　**module vem** *module-number* **execute vemdpalog debug sfpdlagent all** コマンドを入力します。

ステップ 6　**module vem** *module-number* **execute vemlog debug sfacl all** コマンドを入力します。

ステップ 7　**module vem** *module-number* **execute vemlog start** コマンドを入力します。

ステップ 8　**module vem** *module-number* **execute vemlog start** コマンドを入力します。

ステップ 9　検証エラーを発生させたポリシーを設定します。

ステップ 10　**module vem** *module-number* **execute vemdpalog show all** コマンドを入力します。

ステップ 11　**module vem** *module-number* **execute vemlog show all** コマンドを入力します。

Telnet または SSH セッションのバッファをファイルに保存します。ブートフラッシュ内に作成されたログファイルをコピーします。

CHAPTER 16

Quality of Service

この章では、Quality of Service（QoS）に関連する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「QoS について」（P.16-1）
- 「QoS 設定の制限事項」（P.16-2）
- 「QoS トラブルシューティング コマンド」（P.16-2）
- 「VEM のトラブルシューティング」（P.16-3）
- 「ポリシング検証エラーのデバッグ」（P.16-4）

QoS について

QoS は、ネットワーク トラフィックを分類して、輻輳を防ぐようにポリシングおよびプライオリティ付けすることを可能にします。トラフィックは、ユーザが指定した分類方法とユーザが設定した QoS ポリシーに基づいて処理されます。分類、マーキング、およびポリシングが、QoS の 3 つの主要機能です。

- トラフィックの分類：定義された基準に基づいてネットワーク トラフィックをグループ化します。
- トラフィックのマーキング：クラスごとに DSCP、COS、Precedence などのトラフィック属性を変更します。
- ポリシング：特定のクラスのトラフィックについて、データ速度とバースト サイズをモニタします。ネットワークでの QoS ポリシングは、ネットワーク トラフィックが指定したプロファイル（規約）内にあるかどうかを決定します。

QoS の詳細については、『*Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

QoS 設定の制限事項

表 16-1 と 表 16-2 に、QoS の設定上の制限事項の一覧を示します。

表 16-1　QoS 設定の制限事項

項目	DVS 制限値	サーバごとの制限値
クラス マップ	1000	64（ポリシー付き）
ポリシー マップ	128	16
サービス ポリシー	–	128

表 16-2　QoS 設定の制限事項

項目	制限
クラス マップごとの一致基準	32
ポリシー マップごとのクラス マップ数	64

QoS トラブルシューティング コマンド

ここに挙げるコマンドは、インターフェイスに対して設定され適用されているポリシーを見るために VSM 上で使用できるものです。

次のコマンドで、設定済みのポリシーとクラス マップを表示できます。

- **Show policy-map [policy-map-name]**
- **Show class-map [class-map-name]**

次のコマンドで、インストールされているポリシーを表示できます。

- **Show policy-map interface brief**

次のコマンドを VSM で使用して、設定エラーの発生中に QOSMGR および ACLCOMP のランタイム情報を表示できます。

QOSMGR プロセス ランタイム情報設定エラーを収集するコマンドは、次のとおりです。

- **show system internal ipqos event-history errors**
- **show system internal ipqos event-history msgs**
- **show system internal ipqos port-node**
- **show system internal ipqos mem-stats**（メモリの使用状況とリークのデバッグのために）
- **show system internal ipqos status**
- **show system internal ipqos log**（中止されたプラン情報を表示するために）
- **show system internal ipqos**

ACLCOMP プロセス ランタイム情報設定エラーを収集するコマンドは、次のとおりです。

- **show system internal aclcomp event-history errors**
- **show system internal aclcomp event-history msgs**

- **show system internal aclcomp pdl detailed**
- **show system internal aclcomp mem-stats**（メモリの使用状況とリークのデバッグのために）

VEM のトラブルシューティング

ここに挙げるコマンドは、VEM 上で設定されている QoS ポリシーを表示するためのものです。

次のコマンドで、サーバ上で使用中のすべてのクラス マップおよびポリシーのリストを表示できます。

- **module vem** *module-number* **execute vemcmd show qos node**

```
~ # module vem 3 execute vemcmd show qos node
nodeid   type     details
-------- -------- --------
       0   policer
                  cir:50 pir:50
                  bc:200000 be:200000
                  cir/pir units 1 bc/be units 3 flags 2
       1    class   op_AND
                      DSCP
       2    class op_DEFAULT
```

次のコマンドで、サーバ上で使用中のすべてのインストール済みポリシー マップのリストを表示できます。

- **module vem** *module-number* **execute vemcmd show qos policy**

```
~ # module vem 3 execute vemcmd show qos policy
policyid classid policerid set_type value
-------- -------- -------- -------- --------
       0        1       -1             dscp        5
                 2        0              dscp        0
```

次のコマンドで、サーバ上にインストールされているすべてのサービス ポリシーのリストを表示できます。

- **module vem** *module-number* **execute vemcmd show qos pinst**

```
~ # module vem 3 execute vemcmd show qos pinst


id       type
-------- --------
      17  Ingress
            class        bytes matched         pkts matched
         -------- -------------------- --------------------
                1                    0                    0

                2                85529                  572
                0
                  policer stats: conforming (85529, 572)
                  policer stats: exceeding (0, 0)
                  policer stats: violating (0, 0)
```

ポリシング検証エラーのデバッグ

VSM 上で処理することにより、ポリシー検証に失敗した原因をデバッグするには、次の手順を実行します。

ステップ 1　ポリシーが ACL を参照している場合は、**debug aclmgr all** コマンドを入力します。

ステップ 2　**debug ipqos all** コマンドを入力します。

ステップ 3　**debug aclcomp all** コマンドを入力します。

ステップ 4　デバッグ トレースをコンソールに出力しながらもう一度コマンドを実行する **service-policy** コマンドを入力します。このコマンドでは、すべての操作のログを収集できます。

ステップ 5　Telnet SSH セッション バッファをファイルに保存します。

ポート プロファイルのポリシーをデバッグしている場合は、おそらく、まずそれをインターフェイスに直接インストールした方が簡単です。

VEM 上でのポリシー検証の失敗をデバッグするには、次の手順を実行します。

ステップ 1　**module vem** *module-number* **execute vemdpalog clear** コマンドを入力します。

ステップ 2　**module vem** *module-number* **execute vemdpalog sfqosagent all** コマンドを入力します。

ステップ 3　**module vem** *module-number* **execute vemdpalog start** コマンドを入力します。

ステップ 4　DPA デバッグ トレースを vemdpalog に出力しながらもう一度コマンドを実行する **service-policy** コマンドを入力します。

ステップ 5　**module vem** *module-number* **execute vemdpalog stop** コマンドを入力します。

ステップ 6　**module vem** *module-number* **execute vemdpalog show all** コマンドを入力して、コンソールに表示されたログを見ます。

次のような出力が表示されます。

```
calling add policy 81610ac len 220 classmaps 3- --> Session actions
…
Adding classmap 1 (108) with op 1 and 2 filters
…
Adding classmap 2 (116) with op 2 and 2 filters
…
Adding classmap 3 (56) with op 0 and 0 filters
…
init pinst ltl 11 policy id 0 if_index 1a020200 --> Service-policy being applied
installing pinst type 0 17 for policy 0
dpa_sf_qos_verify returned 0
…
Session commit complete and successful --> Session ending
```

CHAPTER 17

SPAN

この章では、SPAN に関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「SPAN に関する情報」（P.17-1）
- 「SPAN の問題」（P.17-2）
- 「SPAN のトラブルシューティング コマンド」（P.17-3）

SPAN に関する情報

スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためのネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe でもその他のリモート モニタリング（RMON）プローブでもかまいません。

Cisco Nexus 1000V は、次の 2 タイプの SPAN をサポートしています。

- ホスト内または VEM 内のソースをモニタできる SPAN（ローカル SPAN）。
- モニタ対象トラフィックを IP 送信先に送信できる Encapsulated Remote SPAN（ERSPAN）。

ローカル SPAN または ERSPAN を設定する方法の詳細については、『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

SPAN セッションのガイドライン

SPAN セッションのガイドラインは、次のとおりです。

- SPAN セッションに複数の送信ソース ポートが含まれている場合、それらのポートが受信するパケットは、ポート上で送信されなくても複製される場合があります。例には次のようなものがあります。
  - フラッディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック
- 受信と送信の両方が設定されている VLAN SPAN セッションについては、パケットが同一 VLAN 上でスイッチされた場合、2 つのパケット（1 つは受信から、1 つは送信から）が宛先ポートから転送されます。
- VMotion 後：
  - ソース ポートと宛先ポートが分離されると、セッションが停止します。

  - ソース ポートと宛先ポートが同一ホスト上に落ち着けば、セッションが再開します。
- 実行中の SPAN セッションには、次のことが必要です。
  - SPAN セッション数 64 という制限を超えていない。
  - 動作可能なソースが 1 つ以上設定されている。
  - 動作可能な宛先が 1 つ以上設定されている。
  - 設定済みのソースと宛先が、同一ホスト上にある。
  - セッションが、**no shut** コマンドでイネーブルにされている。
- 次のいずれかが発生すると、セッションは停止します。
  - すべてのソース ポートがダウンしたか、または削除された。
  - すべての宛先ポートがダウンしたか、または削除された。
  - すべてのソース ポートおよび宛先ポートが VMotion によって分離されている。
  - セッションが **shut** コマンドによってディセーブルにされた。

SPAN の問題

症状	考えられる原因	解決策
イーサネットの宛先を持つセッションを設定したあとに、VM トラフィックで問題が発生した。	—	イーサネットの宛先が同じアップリンク スイッチに接続されていないことを確認します。SPAN パケットがアップリンク スイッチ上の IP テーブル、MAC テーブル、またはその両方で問題を発生させており、それが通常のトラフィックに問題を発生させている場合があります。
セッションの状態は UP になっているのに、パケットが宛先ポートで受信されない。	—	トランク宛先ポート上で正しい VLAN が許可されているか確認します。
セッションでエラーが表示される。	—	**1.** NX-OS VEM 接続が正常に機能していることを確認します。 **2.** VEM でセッションを強制的に再プログラミングします。 **shut** **no shut**

症状	考えられる原因	解決策
ERSPAN セッションは UP になっているのに、宛先でパケットが見えない。	ERSPAN ID が設定されていません。	ERSPAN ID が宛先として設定されていることを確認します。
	ERSPAN 対応の VMKernel NIC がホストまたは VEM 上で設定されていません。	ERSPAN 用に設定されたポート プロファイルを使用するホストの VMKernel NIC が作成されていることを確認します。
	ERSPAN 対応の VMKernel NIC が適切な IP またはゲートウェイ、またはその両方で設定されていません。	ホストの VMKernel NIC から ERSPAN IP 宛先を ping します。 **vmkping** *dest-id*

SPAN のトラブルシューティング コマンド

SPAN に関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	目的
show monitor	SPAN セッションのステータスを表示します。 例 17-1（P.17-3）を参照してください。
show monitor session	現在の SPAN セッションの状態、ダウンしている理由、およびセッションの設定を表示します。 例 17-2（P.17-3）を参照してください。
module vem *module-number* **execute vemcmd show span**	VEM 送信元 IP および SPAN 設定を表示します。 例 17-3（P.17-4）を参照してください。
show monitor internal errors	
show monitor internal event-history msgs	
show monitor internal info global-info	
show monitor internal mem-stats	

例 17-1　show monitor

```
n1000v# show monitor
Session  State        Reason                   Description
-------  -----------  -----------------------  ---------------------------------
17       down         Session admin shut       folio
```

例 17-2　show monitor session

```
n1000v(config)# show monitor session 1
   session 1
---------------
type               : erspan-source
state              : up
source intf        :
    rx             : Eth3/3
    tx             : Eth3/3
    both           : Eth3/3
source VLANs       :
```

```
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
destination IP    : 10.54.54.1
ERSPAN ID         : 999
ERSPAN TTL        : 64
ERSPAN IP Prec.   : 0
ERSPAN DSCP       : 0
ERSPAN MTU        : 1000
```

例 17-3　module vem execute vemcmd show span

```
n1000v# module vem 3 execute vemcmd show span
VEM SOURCE IP: 10.54.54.10
HW SSN ID DST LTL/IP ERSPAN ID
0 10.54.54.1 999
1 48 local
```

CHAPTER 18

マルチキャスト IGMP

この章では、マルチキャスト インターネット グループ管理プロトコル（IGMP）スヌーピングに関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「マルチキャストに関する情報」（P.18-1）
- 「マルチキャスト IGMP スヌーピング」（P.18-1）
- 「マルチキャスト IGMP スヌーピングの問題」（P.18-2）

マルチキャストに関する情報

IP マルチキャストは、ネットワーク内の複数のホストに同じ IP パケット セットを転送する機能です。マルチキャストは、IPv4 ネットワークと IPv6 ネットワークの両方で使用でき、複数の宛先への効率のよいデータ配信を提供します。

マルチキャストは、マルチキャスト データの配信機能と、送信元および受信者の検出機能からなり、マルチキャスト データは、グループと呼ばれる IP マルチキャスト アドレス宛に送信されます。多くの場合、グループおよび送信元 IP アドレスを含むマルチキャスト アドレスは、チャネルと呼ばれます。

マルチキャスト IGMP スヌーピング

IGMP スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッディングを回避します。IGMP スヌーピング機能は、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバーシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。

基本的に、IGMP スヌーピングは次のように機能します。

- イーサネット スイッチ（Cisco Catalyst 6000 スイッチなど）が、すべての IGMP パケットを解析および傍受し、プロトコル処理のために CPU（スーパーバイザ モジュールなど）に転送します。
- ルータのポートが、IGMP クエリーを使用して学習されます。スイッチは、IGMP クエリーを返し、クエリーがどのポートから送られてきたかを記憶し、そのポートをルータ ポートとしてマークします。
- IGMP メンバーシップが、IGMP レポートを使用して学習されます。スイッチが、IGMP メンバーシップを追跡するために、IGMP レポート パケットを解析し、パケットを報告し、そのマルチキャスト転送テーブルを更新します。

- スイッチは、マルチキャスト トラフィックを受信したら、そのマルチキャスト テーブルをチェックし、そのトラフィックを受け取るべきポートだけにトラフィックを転送します。
- IGMP クエリーは、全 VLAN にフラッディングされます。
- IGMP レポートは、アップリンク ポート（ルータ ポート）に転送されます。
- マルチキャスト データ トラフィックは、アップリンク ポート（ルータ ポート）に転送されます。

マルチキャスト IGMP スヌーピングの問題

マルチキャスト IGMP スヌーピングの操作は、アップリンク スイッチが正しく設定されていないとうまく機能しません。IGMP プロセスは、どのアップストリーム ポートが IGMP ルーティングをサポートするルータに接続されているかを知る必要があるため、**ip multicast-routing** コマンドを実行して、アップストリーム スイッチ上の IP マルチキャスト ルーティングを有効にしておく必要があります。

次の例は、グローバルなマルチキャスト ルーティングを有効にし、SVI インターフェイスを設定し、PIM ルーティング プロトコルを有効にする方法を示します。

```
switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip multicast-routing
switch(config)# end

switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# int vlan159
switch(config-if)# ip pim dense-mode
switch(config-if)# end
```

トラブルシューティングのガイドライン

マルチキャスト IGMP の問題をトラブルシューティングする際には、次のガイドラインに従ってください。

- **show ip igmp snooping** コマンドを使用して、IGMP スヌーピングがイネーブルになっていることを確認します。
- アップストリーム スイッチの IGMP が設定されていることを確認します。
- **show ip igmp snooping groups** コマンドを使用して、Nexus 1000V スイッチが正しく設定され、マルチキャスト トラフィックを転送できる状態になっていることを確認します。表示されたコマンド出力のポート見出しの下で、R という文字を探します。R は、VSM がアップストリーム スイッチによって送信された IGMP クエリーからアップリンク ルータ ポートを学習したということを示しており、Nexus 1000V がマルチキャスト トラフィックを転送できる状態になっているということを意味します。

トラブルシューティング コマンド

マルチキャスト IGMP スヌーピングに関する問題をトラブルシューティングするには、次のコマンドを使用できます。

- **show cdp neighbor**

  IGMP はパケット VLAN を使用して IGMP パケットを VSM に転送していますが、これは Cisco Discovery Protocol（CDP; シスコ検出プロトコル）が使用するメカニズムと同じであるため、このトラブルシューティングにも **show cdp neighbor** コマンドを使用できます。ただし、アップストリーム スイッチで **no cdp enable** コマンドを使用して CDP プロトコルをディセーブルにしていた場合は、**show cdp neighbor** コマンドを実行しても何も情報は表示されません。

例 18-1　show cdp neighbor コマンド

```
n1000V# show cdp neighbor
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID              Local Intrfce   Hldtme  Capability  Platform    Port ID
n1000V         Eth3/2            179    R S I       WS-C6506-E    Gig5/16
n1000V         Eth3/4            179    R S I       WS-C6506-E    Gig5/23
```

- **show ip igmp groups**

  show ip igmp groups コマンドでは、VLAN 上で IGMP スヌーピングがイネーブルになっていることを確認できます。

例 18-2　show ip igmp snooping vlan コマンド

```
n1000V# show ip igmp snooping vlan 159
IGMP Snooping information for vlan 159
  IGMP snooping enabled     <-- IGMP SNOOPING is enabled for vlan 159
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled (initializing, time-left: 00:03:20)
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0show ip igmp snooping
```

- **show ip igmp snooping groups**
- **debug ip igmp snooping vlan**

例 18-3　debug ip igmp snooping vlan コマンド

```
n1000V(config)# debug ip igmp snooping vlan
2008 Sep  2 13:29:36.125661 igmp: SNOOP: <vlan 159> Process a valid IGMP packet
2008 Sep  2 13:29:36.126005 igmp: SNOOP: <vlan 159> Received v2 report: group
224.0.0.251 fro 7.159.159.54 on Vethernet3
2008 Sep  2 13:29:36.126086 igmp: SNOOP: <vlan 159> Added oif Vethernet3 for (*,
224.0.0.251) entry
2008 Sep  2 13:29:36.126157 igmp: SNOOP: <vlan 159> Forwarding report for (*,
224.0.0.251) came on Vethernet3
```

```
2008 Sep  2 13:29:36.126225 igmp: SNOOP: <vlan 159> Forwarding the packet to
router-ports
2008 Sep  2 13:29:36.126323 igmp: SNOOP: <vlan 159> Forwarding packet to router-port
Ethernet3/6 (iod 42)
```

VSM 上で、次のコマンドを使用します。

- **module vem** *module-number* **execute vemcmd show vlan**

  例 18-4 の出力では、LTL 18 が vmnic3 に対応し、LTL 47 が VM fedora8, interface eth0 に対応することがわかります。

  224.1.2.3 のマルチキャスト グループ テーブルは、VEM がグループ 224.1.2.3 のマルチキャスト トラフィックを受信したときに転送先とするインターフェイスを示します。fedora8 がその eth0 インターフェイス上にマルチキャスト グループ 224.1.2.3 を持つ場合、LTL 47 が 224.1.2.3 のマルチキャスト グループ テーブルに入っている必要があります。

  LTL 18 は、マルチキャスト グループ 224.1.2.3 内にもあります。これは、LTL 18 が VM であり、224.1.2.3 へのマルチキャスト トラフィックを生成するということを意味します。トラフィックは、アップストリーム スイッチへのアップリンクである vmnic3 に転送されます。

  0.0.0.0 のマルチキャスト グループ テーブル エントリは、デフォルト ルートを提供します。どのマルチキャスト グループにも一致しないマルチキャスト グループ トラフィックがあった場合、そのアドレスにはデフォルト ルートが使用されます。つまり、この場合、トラフィックは vmnic3 を介してアップストリーム スイッチに転送されます。

例 18-4　　module vem *module-number execute* **vemcmd show vlan コマンド**

```
n1000V# module vem 3 execute vemcmd show vlan 159
BD 159, vdc 1, vlan 159, 3 ports
Portlist:
     18  vmnic3
     47  fedora8.eth0

Multicast Group Table:
Group 224.1.2.3 RID 1 Multicast LTL 4408
    47
    18
Group 0.0.0.0 RID 2 Multicast LTL 4407
    18
```

現象、原因、および解決方法

症状	考えられる原因	解決策
VM がマルチキャスト トラフィックを受け取る必要があるのに、マルチキャスト トラフィックを受信していない。	—	**debug ip igmp snooping vlan** コマンドを使用して、IGMP スヌーピングが期待されるとおりに機能しているかどうかを調べます。出力を見て、ポートが IGMP レポートを受信しているか、およびインターフェイスが VM のマルチキャスト トラフィック インターフェイス リストに追加されているかを調べます。
	—	**module vem** *module-number* **execute vemcmd show vlan** コマンドを使用して、VEM 内のマルチキャスト分散テーブルに正しい情報が格納されていることを確認します。
	—	**module vem** *module-number* **execute vemcmd show port** コマンドを使用して、ポート テーブルを見ます。テーブルに正しい情報が格納されていることを確認します。トランク ポートとアクセス ポートの状態が UP/UP になっていることを確認します。

CHAPTER 19

DHCP、DAI、および IPSG

この章では、次のセキュリティ機能に関する問題を識別して解決する方法について説明します。

- Dynamic Host Configuration Protocol（DHCP）スヌーピング
- Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）
- IP Source Guard（IPSG; IP ソース ガード）

この章は、次の内容で構成されています。

- 「DHCP スヌーピングの概要」（P.19-1）
- 「ダイナミック ARP インスペクションに関する情報」（P.19-2）
- 「IP ソース ガードの概要」（P.19-2）
- 「トラブルシューティングの注意事項と制約事項」（P.19-2）
- 「DHCP スヌーピングの問題」（P.19-3）
- 「ドロップされた ARP 応答のトラブルシューティング」（P.19-4）
- 「IP ソース ガードの問題」（P.19-5）
- 「ログの収集と評価」（P.19-5）
- 「DHCP、DAI、および IPSG のトラブルシューティング コマンド」（P.19-6）

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような役割を果たします。具体的には、次の処理を実行します。

- 信頼できない発信元からの DHCP メッセージを検証するとともに、DHCP サーバからの無効な応答メッセージを除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。

DHCP スヌーピングの設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ダイナミック ARP インスペクションに関する情報

DAI は、ARP の要求と応答を検証するための機能です。具体的には、次のような処理を実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- ARP キャッシュの更新やパケットの転送を行う前に、そのパケットに対応する有効な IP-to-MAC バインディングが存在することを確認します。
- 無効な ARP パケットはドロップします。

DAI によって ARP パケットの有効性を判断するときの基準となる有効な IP-to-MAC バインディングは、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースに保存されています。このデータベースは、VLAN とデバイスに対して DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピング機能によって構築されます。このデータベースには、管理者が作成したスタティック エントリが格納されていることもあります。

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

IP ソース ガードの概要

IP ソース ガードとは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング テーブル内のダイナミックまたはスタティック IP ソース エントリの IP-MAC アドレス バインディングと一致する場合にのみ、IP トラフィックを許可します。

IP ソース ガードの設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

トラブルシューティングの注意事項と制約事項

DHCP スヌーピング、ダイナミック ARP インスペクション、または IP ソース ガードをトラブルシューティングするときは、次の注意事項と制約事項が適用されます。

- 最大 2000 の DHCP エントリを DVS 内のシステム全体でスヌーピングまたは学習できます。これは、動的に学習されたエントリと、静的に設定されたエントリの両方を組み合わせた合計です。
- DHCP サーバに接続している VSD SVM ポートまたは vEthernet ポートなどの信頼できるインターフェイスについては、インターフェイスのレート制限値を高めに設定する必要があります。

これらの機能の設定に使用する詳細な注意事項および制約事項については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

DHCP スヌーピングの問題

次に、DHCP スヌーピングに関する問題の現象、考えられる原因、および解決方法を示します。

症状	考えられる原因	解決策
スヌーピングが設定された状態では、DHCP クライアントはサーバから IP アドレスを取得できません。	IP アドレスがバインディング データベースに追加されていない。 DHCP サーバとクライアント間の接続の障害。	**1.** DHCP サーバと、クライアントに接続されているホスト間の接続を確認します。 **vmkping** **2.** DHCP サーバとホスト間の接続が切断された場合は、次の手順を実行します。 – たとえば、VLAN が許可されているかなど、アップストリーム スイッチで設定を確認します。 – サーバ自体がアップし、稼動していることを確認します。
	VM として DVS に接続している DHCP サーバのインターフェイスが信頼できない。	**1.** VSM で、インターフェイスが信頼できることを確認します。 **show ip dhcp snooping** **2.** VSM で、サーバに接続している vEthernet インターフェイスが信頼できることを確認します。 **module vem** *mod#* **execute vemcmd show dhcps interfaces**
	VM からの DHCP 要求がサーバに到達せず、肯定応答を得られない。	DHCP サーバで、ログインしてパケット キャプチャ ユーティリティを使用し、パケットの要求および確認応答を確認します。
	DHCP 要求と肯定応答が Cisco Nexus 1000V に到達していない。	• クライアント vEthernet インターフェイスから、パケットを SPAN で解析して、パケットがクライアントに到達していることを確認します。 • クライアントに接続されているホストで、VEM パケット キャプチャをイネーブルにし、パケットの着信要求および確認応答を確認します。
	Cisco Nexus 1000V が、パケットをドロップしている。	VSM で、DHCP 統計情報を確認します。 **show ip dhcp snooping statistics** **module vem** *mod#* **execute vemcmd show dhcps stats**

ドロップされた ARP 応答のトラブルシューティング

次に、ドロップされた ARP 応答の原因、および解決方法を示します。

考えられる原因	解決策
ARP インスペクションが VSM に設定されていない。	VSM で、ARP インスペクションが予期したとおりに設定されていることを確認します。 **show ip arp inspection** DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
DHCP スヌーピングが VSM でグローバルにイネーブルにならず、VLAN でもイネーブルにならない。	VSM で、DHCP スヌーピングの設定を確認します。 **show ip dhcp snooping** DHCP をイネーブルにして、DAI を設定する方法の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
DHCP スヌーピングが VEM でイネーブルにならず、VLAN でもイネーブルにならない。	**1.** VSM から、VEM の DHCP スヌーピングの設定を確認します。 **module vem** *mod#* **execute vemcmd show dhcps vlan** **2.** 次のいずれかを実行します。 – VSM の DHCP 設定のエラーを修正します。詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。 – VSM の設定に誤りが見つからないが、VEM でエラーになる場合は、VSM と VEM の両方からエラー ログをキャプチャして分析し、エラーの理由を識別します。
スヌーピングがディセーブルである場合、バインディング エントリがバインディング テーブルに静的に設定されない。	**1.** VSM で、バインディング テーブルを表示します。 **show ip dhcp snooping binding** **2.** スタティック バインディング テーブルのエラーを修正します。 テーブルからのエントリのクリア、DHCP のイネーブル化、および DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
ARP 応答を送信している VM に対応するバインディングが、バインディング テーブルに存在しない。	**1.** VSM で、バインディング テーブルを表示します。 **show ip dhcp snooping binding** **2.** スタティック バインディング テーブルのエラーを修正します。 テーブルからのエントリのクリア、DHCP のイネーブル化、および DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。 **3.** どの設定にも誤りがない場合は、DAI または IPSG の前に DHCP スヌーピングをオンにしていることを確認します。これによって、Cisco Nexus 1000V はスヌーピング データベースにバインディングを追加するのに十分な時間を取ることができます。 詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

IP ソース ガードの問題

次に、IP ソース ガードの問題について現象、考えられる原因、および解決方法を示します。

症状	考えられる原因	解決策
トラフィックの中断	ARP インスペクションが VSM に設定されていない。	VSM で、IP ソース ガードが予期したとおりに設定されていることを確認します。 **show port-profile name** *profile_name* **show running interface** *if_ID* **show ip verify source** IP ソース ガードの設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
	vEthernet インターフェイスに対応する IP アドレスがスヌーピング バインディング テーブルにない。	**1.** VSM で、バインディング テーブルを表示します。 **show ip dhcp snooping binding** **2.** 欠落しているスタティック エントリを設定するか、VM でリースを更新します。 **3.** VSM で、バインディング テーブルを再表示して、エントリが適切に追加されていることを確認します。 **show ip dhcp snooping binding**

ログの収集と評価

DHCP、DAI、および IP ソース ガードに関するログを収集し、表示するには、VSM からこの項のコマンドを使用します。

- 「VSM ロギング」（P.19-5）
- 「ホスト ロギング」（P.19-6）

VSM ロギング

DHCP、DAI、および IP ソース ガードに関するログを収集し、表示するには、VSM からこの項のコマンドを使用します。

VSM コマンド	説明
debug dhcp all	dhcp 設定フラグに対するすべてのデバッグをイネーブルにします。
debug dhcp errors	エラーのデバッグをイネーブルにします。
debug dhcp mts-errors	mts エラーのデバッグをイネーブルにします。
debug dhcp mts-events	mts イベントのデバッグをイネーブルにします。
debug dhcp pkt-events	pkt イベントのデバッグをイネーブルにします。

VSM コマンド	説明
debug dhcp pss-errors	pss エラーのデバッグをイネーブルにします。
debug dhcp pss-events	pss イベントのデバッグをイネーブルにします。

ホスト ロギング

DHCP、DAI、および IP ソース ガードに関するログを収集し、表示するには、ESX ホストからこの項のコマンドを使用します。

ESX ホスト コマンド	説明
echo "logfile enable" > /tmp/dpafifo	DPA デバッグ ロギングをイネーブルにします。 ログは、/var/log/vemdpa.log ファイルに出力されます。
echo "debug sfdhcpsagent all" > /tmp/dpafifo	DPA DHCP エージェント デバッグ ロギングをイネーブルにします。 ログは、/var/log/vemdpa.log ファイルに出力されます。
vemlog debug sfdhcps all	データパス デバッグ ロギングをイネーブルにして、クライアントとサーバ間で送信されたデータパケットに関するログをキャプチャします。
vemlog debug sfdhcps_config all	データパス デバッグ ロギングをイネーブルにして、VSM からの設定に関するログをキャプチャします。
vemlog debug sfdhcps_binding_table all	データパス デバッグ ロギングをイネーブルにして、バインディング データベースの変更に対応するログをキャプチャします。

DHCP、DAI、および IPSG のトラブルシューティング コマンド

DHCP スヌーピング、DAI、および IP ソース ガードに関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	説明
show running-config dhcp	DHCP スヌーピング、DAI、および IP ソース ガードの設定を表示します。 例 19-1（P.19-7）を参照してください。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。 例 19-2（P.19-7）を参照してください。

コマンド	説明
show ip dhcp snooping binding	DHCP スヌーピング バインディング テーブルの内容を表示します。 例 19-3（P.19-8）を参照してください。
show feature	DHCP などの使用可能な機能と、それらがイネーブルかどうかを表示します。 例 19-4（P.19-8）を参照してください。
show ip arp inspection	DAI のステータスを表示します。 例 19-5（P.19-8）を参照してください。
show ip arp inspection interface vethernet *interface-number*	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。 例 19-6（P.19-9）を参照してください。
show ip arp inspection vlan *vlan-ID*	特定の VLAN の DAI 設定を表示します。 例 19-7（P.19-9）を参照してください。
show ip verify source	IP ソース ガードがイネーブルであるインターフェイスと、IP-MAC アドレス バインディングを表示します。 例 19-8（P.19-9）を参照してください。

例 19-1　show running-config dhcp

```
n1000v# show running-config dhcp

!Command: show running-config dhcp
!Time: Wed Feb 16 14:20:36 2011

version 4.2(1)SV1(4)
feature dhcp

no ip dhcp relay

n1000v#
```

例 19-2　show ip dhcp snooping

```
n1000v# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
vEthernet 3           Yes

n1000v#
```

例 19-3　show ip dhcp snooping binding

```
n1000v# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type        VLAN  Interface
-----------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33  10.3.2.2         infinite  static      13    vEthernet 6
0f:00:60:b3:23:35  10.2.2.2         infinite  static      100   vEthernet 10
n1000v#
```

例 19-4　show feature

```
n1000v# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         enabled
http-server           1         enabled
ippool                1         enabled
lacp                  1         enabled
lisp                  1         enabled
lisphelper            1         enabled
netflow               1         disabled
port-profile-roles    1         enabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
n1000v#
```

例 19-5　show ip arp inspection

```
n1000v# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan : 1
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 5
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 100
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 101
-----------
Configuration          : Disabled
Operation State        : Inactive
n1000v#
```

例 19-6　show ip arp inspection interface

```
n1000v# show ip arp inspection interface vethernet 6

 Interface        Trust State
 -------------    -----------
 vEthernet 6        Trusted
n1000v#
```

例 19-7　show ip arp inspection vlan

```
n1000v# show ip arp inspection vlan 13

Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

n1000v#
```

例 19-8　show ip verify source

```
n1000v# show ip arp inspection vlan 13
IP source guard is  enabled on the following interfaces:
---------------------------------------------------------------------------
     Vethernet1

Interface         Filter-mode     IP-address     Mac-address       Vlan
------------      -----------     ----------     --------------    ----
Vethernet11      active           25.0.0.128     00:50:56:88:00:20  25
```

CHAPTER 20

仮想サービス ドメイン

この章では、仮想サービス ドメイン（VSD）に関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「仮想サービス ドメインの概要」（P.20-1）
- 「仮想サービス ドメインの問題」（P.20-1）
- 「ログの収集と評価」（P.20-2）
- 「仮想サービス ドメインのトラブルシューティング コマンド」（P.20-3）

仮想サービス ドメインの概要

仮想サービス ドメイン（VSD）は、共通のサービス VM（SVM）によって管理されるインターフェイスの論理グループです。VSD が設定された Cisco Nexus 1000V では、vShield などのサードパーティ アプライアンスをサポートできます。

VSD を使用することで、ファイアウォールやトラフィック モニタリングなどのネットワーク サービスに対するトラフィックを分類し、区別することができます。

複数の VSD を 1 つのホストに共存させることができ、各 VSD は SVM によって管理されます。

詳細情報、VSD の設定方法、設定例、および設定に関する制約事項については、『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

仮想サービス ドメインの問題

次に、VSD の問題について現象、考えられる原因、および解決方法を示します。

症状	考えられる原因	解決策
SVM がオンラインにならない。	1 台のホストの 1 つの VSD に対して複数の SVM が存在する。 1 台のホストの 1 つの VSD に対して 1 つの SVM のみ存在できます。別の SVM がアップになろうとすると、SVM ポートが errdisable になります。	**1.** 1 台のホストの 1 つの VSD に対して複数の SVM がないかどうかを調べます。 **show virtual-service-domain interface** 出力が **Invalid SVM interface** を示している場合は、1 台のホストの 1 つの VSD に対して複数の SVM が存在します。 **2.** SVM の 1 つを消去または再配置します。

症状	考えられる原因	解決策
ループが発生する。	SVM ポートが内部および外部ポート プロファイルに正しく接続されていない。	**1.** SVM ルーピング機能または SVM 自体をオフにします。 **2.** ポート プロファイルに接続しているインターフェイスを表示します。 **show port-profile usage** **3.** 設定エラーを修正します。 VSD 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。

ログの収集と評価

この項のコマンドを VSM から使用して、VSM からキャプチャされた VSD に関する次のログを収集し、表示することができます。

- VSM のログ：/var/log/external/startupdebug
- VEM の DPA のログ：/var/log/vemdpa.log

コマンド	説明
module vem *module_number* **execute vemdpalog writelogs** **module vem** *module_number* **execute vemdpalog debug sfvsimagent all**	DPA のログをイネーブルにして、vemdpa.log に書き込みます。
module vem *module_number* **execute vemdpalog start** **module vem** *module_number* **execute vemdpalog stop**	表示用の DPA のロギングを開始および停止します。
module vem *module_number* **execute vemdpalog show all**	DPA のログを表示します。
module vem *module_number* **execute vemlog debug sfvsim all**	DP のログをイネーブルにします。
module vem *module_number* **execute vemlog start** **module vem** *module_number* **execute vemlog stop**	表示用の DP のロギングを開始および停止します。
module vem *module_number* **execute vemlog show all**	DPA のログを表示します。

例 20-1　　VSM のログ

```
2011 Feb 17 10:14:01 vsm vsim: <{vsim}> [DBG]==============ZONES===============
2011 Feb 17 10:14:01 vsm vsim: <{vsim}>[DBG]Zone_id: 1, name: vsd1, is_in_use? 1,
default_action: (DROP), member_cnt: 5
2011 Feb 17 10:14:01 vsm vsim: <{vsim}> [DBG]==============INTFS===============
```

```
2011 Feb 17 10:14:01 vsm vsim: <{vsim}>[DBG]Ifindex 0x1c000000, zoneid 1, status ATTACHED,
type SVM_MEMBER (2)
2011 Feb 17 10:14:01 vsm vsim: <{vsim}>[DBG]Ifindex 0x1c000010, zoneid 1, status ATTACHED,
type SVM_MEMBER (2)
2011 Feb 17 10:14:01 vsm vsim: <{vsim}>[DBG]Ifindex 0x1c000020, zoneid 1, status ATTACHED,
type SVM_MEMBER (2)
2011 Feb 17 10:14:01 vsm vsim: <{vsim}>[DBG]Ifindex 0x1c000030, zoneid 1, status ATTACHED,
type SVM_MEMBER (2)
```

例 20-2　　VEM の DPA のログ

```
Feb 17 16:11:02.645378: sfvsimagent: PDL Lite :Opening new session
Feb 17 16:11:02.723186: sfvsimagent: PDL Lite :Add policy callback
Feb 17 16:11:02.727281: sfvsimagent: PDL Lite :Add policy node callback
Feb 17 16:11:02.727293: sfvsimagent: sf_vsim_add_vzone: Entered
Feb 17 16:11:02.727303: sfvsimagent: sf_vsim_dpa_vzone_init: Entered
Feb 17 16:11:02.727324: sfvsimagent: MTS Opcode: 142337
```

例 20-3　　VEM のログ

```
Feb 17 15:58:42.924322      4411   1    1  16   Debug sfvsimsrc: Reached vsim stage src
ltl 18 dst ltl 10
Feb 17 15:58:42.924337      4412   1    1  16   Debug sfvsimsrc: Reached vsim stage src
ltl 9 dst ltl 8
Feb 17 15:58:43.038065      4413   1    1  16   Debug sfvsimsrc: Reached vsim stage src
ltl 18 dst ltl 10
Feb 17 15:58:43.038087      4414   1    1  16   Debug sfvsimsrc: Reached vsim stage src
ltl 9 dst ltl 8
Feb 17 15:58:43.038128      4415   2    1  16   Debug sfvsimsrc: Reached vsim stage src
ltl 8 dst ltl 4282
Feb 17 15:58:43.038152      4416   1    1  16   Debug sfvsimsrc: Reached vsim stage src
ltl 10 dst ltl 18
Feb 17 15:58:43.038156      4417   2    0  0         Suspending log
```

仮想サービス ドメインのトラブルシューティング コマンド

VSD に関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	説明
show system internal ethpm event-history interface	要求/応答の事前設定されたイベントを表示します。ポートが errdisable ステートのときに役立ちます。 例 20-4（P.20-4）を参照してください。
show system internal vsim event-history msgs	VSIM によって処理された MTS イベントのログを表示します。 例 20-5（P.20-4）を参照してください。
module vem *mod-number* **execute vemcmd show port**	VEM のポート状態を表示します。インターフェイス上のトラフィック フローをデバッグするのに役立ちます。 例 20-6（P.20-5）を参照してください。
show virtual-service-domain name *vsd-name*	特定の VSD の設定を表示します。 例 20-7（P.20-5）を参照してください。

コマンド	説明
show virtual-service-domain brief	すべての VSD 設定の要約を表示します。 例 20-8（P.20-5）を参照してください。
show virtual-service-domain interface	すべての VSD のインターフェイス設定を表示します。 例 20-9（P.20-6）を参照してください。
module vem *module_number* **execute vemcmd show vsd**	VEM の VSD 設定を表示するために、リモートの Cisco Nexus 1000V から VEM にコマンドを送信します。 例 20-10（P.20-6）を参照してください。
module vem *module_number* **execute vemcmd show vsd ports**	VEM の VSD ポート設定を表示するために、リモートの Cisco Nexus 1000V から VEM にコマンドを送信します。 例 20-11（P.20-6）を参照してください。
show port-profile name *profile-name*	ポート プロファイルの設定を表示します。 ～を参照してください。

例 20-4　show system internal ethpm event-history interface vethernet 1

```
n1000v# show system internal ethpm event-history interface vethernet 1
...
 18) Event:ESQ_REQ length:34, at 725272 usecs after Thu Feb 17 15:42:13 2011
    Instance:469762048, Seq Id:0x1, Ret:success
    [E_MTS_TX] Dst:MTS_SAP_VSIM(716), Opc:MTS_OPC_ETHPM_PORT_PRE_CFG(61441)

19) Event:ESQ_RSP length:34, at 739984 usecs after Thu Feb 17 15:42:13 2011
    Instance:469762048, Seq Id:0x1, Ret:success
    [E_MTS_RX] Src:MTS_SAP_VSIM(716), Opc:MTS_OPC_ETHPM_PORT_PRE_CFG(61441)
...
n1000v#
```

例 20-5　show system internal vsim event-history msgs

```
n1000v# show system internal vsim event-history msgs
1) Event:E_MTS_RX, length:60, at 215249 usecs after Thu Feb 17 10:16:53 2011
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X000C14C4, Ret:SUCCESS
    Src:0x00000101/2282, Dst:0x00000101/716, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x000C14C4, Sync:UNKNOWN, Payloadsize:216
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 32 34

2) Event:E_MTS_TX, length:60, at 833885 usecs after Thu Feb 17 10:14:01 2011
    [NOT] Opc:MTS_OPC_FSMUTILS_SYNC_PSS_TO_STDBY(1523), Id:0X000C05B3, Ret:SUCCESS
    Src:0x00000101/716, Dst:0x00000101/0, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:380
    Payload:
    0x0000:  00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 01

3) Event:E_FU_UNLOCK, length:36, at 820289 usecs after Thu Feb 17 10:14:01 2011
    Status: 0x0
    Gwrap: 0x80fa09c  Cat: 0x0
      Opc:MTS_OPC_VSH_CMD_TLV_SYNC(7682)
      Msg id: 0X000C05A5
```

```
    Lock type: 0
    RID Size: 8
      Val   :
      0x0000:  01 00 00 00 00 00 00 01
4) Event:E_FU_UNLOCK, length:36, at 818291 usecs after Thu Feb 17 10:14:01 2011
    Status: 0x0
    Gwrap: 0x80fa09c  Cat: 0x0
      Opc:MTS_OPC_VSH_CMD_TLV_SYNC(7682)
      Msg id: 0X000C05A5
    Lock type: 0
    RID Size: 8
      Val   :
      0x0000:  00 00 00 1c 00 00 00 02
5) Event:E_FU_UNLOCK, length:36, at 816421 usecs after Thu Feb 17 10:14:01 2011
    Status: 0x0
    Gwrap: 0x80fa09c  Cat: 0x0
      Opc:MTS_OPC_VSH_CMD_TLV_SYNC(7682)
      Msg id: 0X000C05A5
    Lock type: 0
    RID Size: 8
      Val   :
      0x0000:  10 00 00 1c 00 00 00 02
n1000v#
```

例 20-6　module vem # execute vemcmd show port

```
n1000v# module vem 3 execute vemcmd show port
  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port
   18     Eth3/2     UP   UP    F/B*      0        vmnic1
   49      Veth1     UP   UP    FWD       0        New Virtual Machine.eth0
   50      Veth2     UP   UP    FWD       0        New Virtual Machine.eth1
   51      Veth3     UP   UP    FWD       0        New Virtual Machine.eth2
   52      Veth4     UP   UP    FWD       0        New Virtual Machine.eth3

* F/B: Port is BLOCKED on some of the vlans.
 Please run "vemcmd show port vlans" to see the details.
n1000v#
```

例 20-7　show virtual-service-domain name *vsd_name*

```
n1000v# show virtual-service-domain name vsd1
Default Action: drop
____________________________
Interface        Type
____________________________
Vethernet1       Member
Vethernet2       Member
Vethernet3       Member
Vethernet6       Member
Vethernet7       Inside
Vethernet8       Outside

n1000v#
```

例 20-8　show virtual-service-domain brief

```
n1000v# show virtual-service-domain brief
Name   vsd-id    default action    in-ports   out-ports   mem-ports    Modules with
                                                                       VSD Enabled
zone    1         forward           1          1           2            4
n1000v#
```

例 20-9　show virtual-service-domain interface

```
n1000v# sho virtual-service-domain interface
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Name             Interface            Type      Status
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
vsd1             Vethernet1           Member    Active
vsd1             Vethernet2           Member    Active
vsd1             Vethernet3           Member    Active
vsd1             Vethernet6           Member    Active
vsd1             Vethernet7           Inside    Active
vsd1             Vethernet8           Outside   Active
vsd2             Vethernet9           Inside    Active
vsd2             Vethernet10          Outside   Active
```

例 20-10　module *module_number* execute vemcmd show vsd

```
n1000v# module vem 4 execute vemcmd show vsd
ID Def_Act ILTL OLTL NMLTL State Member LTLs
1 FRWD 51 50 1 ENA 49
n1000v#
```

例 20-11　module *module_number* execute vemcmd show vsd ports

```
n1000v# module vem 4 execute vemcmd show vsd ports
LTL IfIndex VSD_ID VSD_PORT_TYPE
49 1c000010 1 REGULAR
50 1c000040 1 OUTSIDE
51 1c000030 1 INSIDE
n1000v#
```

例 20-12　show port-profile name UpLinkProfile

```
n1000v# show port-profile name UpLinkProfile3
port-profile UpLinkProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:
n1000v#
```

CHAPTER 21

システム

この章では、Nexus 1000V システムに関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「システムについて」（P.21-1）
- 「vCenter Server の基本的な制限事項」（P.21-2）
- 「DVS の回復」（P.21-2）
- 「VSM と vCenter Server 接続に関連した問題」（P.21-5）
- 「ESX の再起動後の接続の失敗」（P.21-6）
- 「VSM の作成」（P.21-9）
- 「ポート プロファイル」（P.21-9）
- 「ホストでの問題」（P.21-10）
- 「VM トラフィックでの問題」（P.21-11）
- 「VEM トラブルシューティング コマンド」（P.21-11）
- 「VEM ログ コマンド」（P.21-12）
- 「エラー メッセージ」（P.21-12）

システムについて

Cisco Nexus 1000V は、仮想化されたサーバ環境で、レイヤ 2 スイッチング機能を提供します。Nexus 1000V は、ESX Server 内の仮想スイッチを置き換えて、ユーザが Cisco NX-OS コマンドライン インターフェイスを使用して仮想スイッチの設定とモニタを行うことを可能にします。Nexus 1000V により、ESX Server のネットワーク コンポーネントに対する可視性、およびネットワーク上の仮想スイッチへのアクセスも得られます。

Nexus 1000V は、vCenter Server で定義されたデータセンターを管理します。データセンター内の各サーバは、Nexus 1000V ではラインカードとして表され、物理的な Cisco スイッチ内のラインカードであるかのように管理できます。Nexus 1000V の実装は、次の 2 つのコンポーネントで構成されます。

- Virtual Supervisor Module（VSM; 仮想スーパーバイザ モジュール）: Nexus 1000V Distributed Virtual Switch（DVS; 分散仮想スイッチ）の制御ソフトウェア。NX-OS に基づいており、Virtual Machine（VM; 仮想マシン）上で実行されます。

- Virtual Ethernet Module（VEM; 仮想イーサネット モジュール）：Cisco Nexus 1000V で実際にデータ トラフィックのスイッチングを行う部分。VMware ESX 4.0 ホスト上で実行されます。複数の VEM が、1 つの VSM によって制御されます。スイッチ ドメインを形成するすべての VEM が、VMware vCenter Server で定義されたとおりに同一の仮想データセンター内になくてはなりません。

Nexus 1000V が VMware ESX ソフトウェアでどのように機能するかの詳細については、『*Cisco Nexus 1000V Getting Started Guide*』を参照してください。

vCenter Server の基本的な制限事項

vCenter Server に関する問題のトラブルシューティングを行う際には、次の制限事項に注意してください。

- 分散仮想スイッチ（DVS）の名前は、データセンター全体にわたって一意でなければなりません。
- DVS は、ネットワーク フォルダ内に作成します。
- DBS フォルダまたは下層の DVS を削除しない限り、データセンターを削除することはできません。
- DVS を削除できるのは、config-svs-conn モードで **no vmware dvs** コマンドを使用して VSM の助けを得た場合だけです。
- no vmware dvs コマンドが正常に実行できるのは、DVS ポート グループを使用している VM がない場合だけです。
- vCenter Server 上のポート グループを削除できるのは、それに関連付けられているインターフェイスがない場合だけです。
- **connect** コマンドと一緒に同期操作を実行すると、VSM の vCenter Server との同期が保たれます。
- 各 VSM が、一意の拡張キーを使用して vCenter Server と通信し、DVS 上で操作を実行します。

拡張キー

VSM では、vCenter Server と通信する際に拡張キーが使用されます。各 VSM が独自の一意の拡張キーを持ちます（Cisco_Nexus_1000V_32943215 など）。

VSM の拡張キーを調べるには、**show vmware vc extension-key** コマンドを使用します。拡張キーは、.xml ファイルでも調べることができます。

vCenter Server 上で登録されている拡張キーは、MOB を通じて見つかります。詳細については、「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）の手順を参照してください。

同じ拡張キーを使用して、vCenter Server 上で複数の DVS を作成することはできません。

DVS の回復

DVS の作成に使用された VSM VM が失われた場合、またはその VSM VM を置き換える必要がある場合、次の手順に従って DVS を回復できます。ここでは、次の手順について説明します。

- 「VSM のコピーが保存されている場合の DVS の回復」（P.21-3）
- 「VSM のコピーが保存されていない場合の DVS の回復」（P.21-4）

VSM のコピーが保存されている場合の DVS の回復

VSM 設定ファイルのバックアップ コピーをあらかじめ保存していた場合は、次の手順に従って DVS を回復できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- VSM 設定ファイルのバックアップ コピーをあらかじめ保存していた場合は、この手順に従います。バックアップ コピーを保存していなかった場合は、「VSM のコピーが保存されていない場合の DVS の回復」（P.21-4）の手順を参照してください。
- VSM VM スイッチ名が、vCenter Server 上の DVS スイッチ名と同じであることを確認します。スイッチ名が同じであれば、VSM 設定は、vCenter Server 上の正しい DVS と同期されます。

  VSM スイッチ名を変更するには、**switchname** *newname* コマンドを使用します。

ステップ 1　MOB から、DVS 拡張キーを見つけます。
詳細については、「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）の手順を参照してください。

ステップ 2　VSM 上で、ステップ 1 で見つけた DVS 拡張キーを追加します。

この拡張キーにより、VSM は vCenter Server にログインできるようになります。

例：
```
n1000v# config t
n1000v(config)# vmware vc extension-key Cisco_Nexus_1000V_32943215
```

ステップ 3　MOB から、ステップ 1 で見つけた拡張キーを登録解除します。

詳細については、「vCenter Server の拡張キーの登録解除」（P.3-13）の手順を参照してください。

ステップ 4　VC クライアントから、VSM の拡張（プラグイン）を登録します。

詳細については、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』にある次の手順を参照してください。

- 「Creating a Cisco Nexus 1000V Plug-In on the vCenter Server」

ステップ 5　VSM 上で、あらかじめ保存しておいた VSM 設定ファイルのコピーを使用して設定を復元します。

copy *path/filename* **running-config**

例：
```
n1000v# copy sftp://user1@172.22.36.10/backup/hamilton_cfg running-config
```

ステップ 6　次のいずれかを実行します。

- vCenter Server 接続が、あらかじめ保存しておいた設定に含まれていない場合は、次のステップに進みます。
- それ以外の場合は、ステップ 8 に進みます。

ステップ 7　VSM 上で、vCenter Server 接続の設定を復元します。

例：
```
n1000v# config t
n1000v (config)# svs connection VC
n1000v(config-svs-conn#) protocol vmware-vim
n1000v(config-svs-conn#) remote ip address 192.168.0.1
n1000v(config-svs-conn#) vmware dvs datacenter-name Hamilton-DC
```

ステップ 8　vCenter Server に接続します。

例：
```
n1000v(config-svs-conn#) connect
```

これで、古い DVS を使用することも削除することもできます。

VSM のコピーが保存されていない場合の DVS の回復

VSM 設定ファイルのバックアップ コピーを保存していなかった場合は、次の手順に従って DVS を回復できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- VSM が存在するフォルダは次を満たす必要があります。
  - 存在するデータセンターのルート レベルにあること。
    別のフォルダに組み込むことはできません。
  - VSM と同じ名前であること。

  フォルダがこの条件を満たしていない場合、vCenter サーバへの接続が「*the VSM already exists*」というエラーにより失敗します。
- VSM 設定ファイルのバックアップ コピーを保存していなかった場合は、この手順に従います。バックアップ コピーをあらかじめ保存していた場合は、「VSM のコピーが保存されている場合の DVS の回復」（P.21-3）の手順を参照してください。
- VSM 設定ファイルのバックアップ コピーを保存していなかった場合は、VC に接続する前に、古いポート プロファイルの再作成を試してみることができます。この手順には、ポート プロファイルを再作成するためのステップが含まれています。VC に接続する前にこれらを再作成しなければ、VC 上に存在するポート グループはすべて削除され、使用中のすべてのポートが検疫ポート グループに移動されます。
- VSM VM スイッチ名が、vCenter Server 上の DVS スイッチ名と同じであることを確認します。スイッチ名が同じであれば、VSM 設定は、vCenter Server 上の正しい DVS と同期されます。

  VSM スイッチ名を変更するには、**switchname** *newname* コマンドを使用します。

ステップ 1　MOB から、DVS 拡張キーを見つけます。
詳細については、「特定の DVS に結び付けられた拡張キーの確認」（P.3-9）の手順を参照してください。

ステップ 2　VSM 上で、ステップ 1 で見つけた DVS 拡張キーを追加します。

この拡張キーにより、VSM は vCenter Server にログインできるようになります。

例：
```
n1000v# config t
n1000v(config)# vmware vc extension-key Cisco_Nexus_1000V_32943215
```

ステップ 3　MOB から、ステップ 1 で見つけた拡張キーを登録解除します。

詳細については、「vCenter Server の拡張キーの登録解除」（P.3-13）の手順を参照してください。

ステップ 4　VC クライアントから、VSM の拡張（プラグイン）を登録します。

詳細については、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』にある次の手順を参照してください。

- 「Creating a Cisco Nexus 1000V Plug-In on the vCenter Server」

ステップ 5　前の設定から古いポート プロファイルを手動で再作成します。

詳細については、『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(5.1)*』にある次の手順を参照してください。

- 「Configuring the System Port Profile for VSM-VEM Communication」
- 「Configuring the Uplink Port Profile for VM Traffic」
- 「Configuring the Data Port Profile for VM Traffic」

（注）　ポート プロファイルを手動で再作成しなかった場合、VSM が接続するときに、vCenter Server 上のすべてのポート グループが削除されます。

ステップ 6　VSM 上で、vCenter Server 接続の設定を復元します。

例：
```
n1000v# config t
n1000v (config)# svs connection VC
n1000v(config-svs-conn#) protocol vmware-vim
n1000v(config-svs-conn#) remote ip address 192.168.0.1
n1000v(config-svs-conn#) vmware dvs datacenter-name Hamilton-DC
```

ステップ 7　vCenter Server に接続します。

例：
```
n1000v(config-svs-conn#) connect
```

これで、古い DVS を使用することも削除することもできます。

VSM と vCenter Server 接続に関連した問題

症状	解決策
Release 4.0(4)SV1(3a) VSM と VMware vCenter Server 5.0 の間の接続がサポートされていない。	対応したバージョンの Cisco Nexus 1000V ソフトウェアにアップグレードしてください。
vCenter Server 接続が正常に見えるのに、正常でない。	ドメイン ID が正しく設定されていることを確認します。
svs connection コマンドが失敗する。	**svs connection** コマンドのすべてのパラメータを設定しているか確認します。
	vCenter Server の IP アドレスを ping できるか確認します。
	proxy.xml ファイルの IP アドレスと長さが両方とも正しいことを確認します。
	vCenter Server を再起動します。

症状	解決策
ESX の再起動後に接続が失敗する。	「ESX の再起動後の接続の失敗」（P.21-6）の手順
[Add host to DVS] 画面にホストが表示されない。	ホストのインストールに使用された VMware Enterprise Plus ライセンスに分散仮想スイッチ機能が含まれていることを確認します。
[Add host to DVS] でエラーが返される。	VEM ソフトウェアが ESX Server 上にインストールされていることを確認します。
show module コマンドの出力のサーバ名の列に IP アドレスが示される。	サーバ名は、ホスト名か IP アドレスのうち、vCenter Server 上の DVS へのホストの追加に使用された方で表示されます。

例 21-1 に、**show vms internal event-history errors** コマンドを示します。このコマンドは、VC エラーの詳細を検証するのに便利です。この出力から、エラーが VSM（クライアント）とサーバのどちらによって発生したかがわかります。

例 21-1　　show vms internal event-history error コマンド

```
n1000v# show vms internal event-history errors

Event:E_DEBUG, length:239, at 758116 usecs after Tue Feb  3 18:21:58 2009
    [102] convert_soap_fault_to_err(1179): SOAP 1.1 fault: "":ServerFaultCode [VMWARE-VIM]
A DVS n1000v with spec.name as n1000v already exists, cannot create DVS n1000v. A
specified parameter was not correct.spec.name

Event:E_DEBUG, length:142, at 824006 usecs after Tue Feb  3 18:18:30 2009
    [102] convert_soap_fault_to_err(1179): SOAP 1.1 fault: SOAP-ENV:Client [VMWARE-VIM]
Operation could not be completed due to connection failure.

Event:E_DEBUG, length:134, at 468208 usecs after Tue Feb  3 18:15:37 2009
    [102] convert_soap_fault_to_err(1179): SOAP 1.1 fault: "":ServerFaultCode [VMWARE-VIM]
Extension key was not registered before its use.
```

ESX の再起動後の接続の失敗

VSM と VEM の間の接続が失われるのを防ぎ、ESX のリブートを経由する物理 NIC にデフォルト以外の MTU 設定を維持するには、システム ポート プロファイルでシステム MTU を設定する必要があります。

Cisco Nexus 1000V に接続されている物理 NIC に対して 1500（デフォルト）以外の MTU を使用している場合、ESX が再起動すると、VMware カーネル NIC MTU との不一致、および VSM と VEM 障害が発生することがあります。たとえば、ジャンボ フレームを使用しているネットワーク内で、手動で 1500 以外の MTU を設定したとします。電源を再投入すると、ESX は再起動し、物理 NIC の MTU はデフォルトの 1500 に戻りますが、VMware カーネル NIC は戻りません。

MTU の不一致による接続の損失を防止するには、「システム MTU の設定」（P.21-7）の手順を参照してください。

システム アップリンク ポート プロファイルでシステム MTU を設定していない場合に接続を回復するには、～を参照してください。

システム MTU の設定

既存のシステム アップリンク ポート プロファイルでシステム MTU を設定するには、次の手順を使用します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- システム ポート プロファイルがすでに設定されており、アップリンク プロファイル名がわかっていること。

  詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
- ポート プロファイルで **system mtu** に設定する MTU サイズは、インターフェイスで設定した **system jumbomtu** のサイズより小さくする必要があります。

  インターフェイスでの MTU の設定の詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
- システム ポート プロファイルにシステム MTU を設定すると、その MTU がインターフェイスに設定した MTU よりも優先されます。
- 対応する PNIC の ESX MTU の設定を確認するには、**esxcfg-nics -l** コマンドを使用します。

手順の概要

1. **config t**
2. **port-profile** *profilename*
3. **system mtu** *mtu value*
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profilename*]
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**port-profile** *name*
	
	例：
	`n1000v(config)# port-profile AccessProf`
	`n1000v(config-port-prof)#`
		名前付きシステム アップリンク ポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。

ステップ 3	**system mtu** *mtu-size*
	
	例：
	`n1000v(config-port-prof)# system mtu 4000`
	`n1000v(config-port-prof)#`
		MTU サイズを指定します。
		• 1500 ～ 9000 の範囲の偶数である必要があります。
		• インターフェイスの **system jumbomtu** のサイズよりも小さくする必要があります。

	コマンド	説明
ステップ 4	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] 例： n1000v(config-port-prof)# show port-profile name AccessProf	（任意）確認のためにコンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： n1000v(config-port-prof)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

MTU の不一致によって失われた接続の回復

ESX のリブート後に、物理 NIC と VMware カーネル NIC 間の MTU の不一致によって失われた接続を回復するには、ここに示す手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 対応する PNIC の ESX MTU の設定を確認するには、**esxcfg-nics -l** コマンドを使用します。

（注）　**vemcmd** コマンドは回復手段だけに使用して、システム アップリンクの場合はポート プロファイル設定内、システム以外のアップリンクの場合はインターフェイス設定内の MTU 値を更新します。

手順の概要

1. **config t**
2. **module vem** *module_number* **execute vemcmd show port** *port-LTL-number*
3. **module vem** *module_number* **execute vemcmd set mtu** *size* **ltl** *port-LTL-number*

手順の詳細

	コマンド	説明
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**module vem** *module_number* **execute vemcmd show port** *port-LTL-number*	ステップ 3 に必要な LTL 番号を含むポート設定を表示します。

コマンド	説明

例：
`n1000v(config)# module vem 3 execute vemcmd show port 48`
`LTL  IfIndex  Vlan  Bndl  SG_ID Pinned_SGID  Type  Admin State  CBL Mode  Name`
`17  1a030100  1 T  304  1  32  PHYS  UP  UP  1 Trunk  vmnic1`
`n1000v(config)#`	

ステップ 3　**module vem** *module_number* **execute vemcmd set mtu** *size* **ltl** *port-LTL-number*
 	
例：
`n1000v(config)# module vem 3 execute vemcmd set mtu 9000 ltl 17`
`n1000v(config)#`
	ステップ 2 で取得した LTL 番号を使用して、ポートの MTU サイズを指定します。

VSM の作成

症状	考えられる原因	解決策
VSM VM が boot プロンプトで止まる。	—	e1000 NIC が 3 つあることを確認します。
VSM VM が自分に ping できない。	—	mgmt0 インターフェイスを設定します。
VSM VM が自分には ping できるが、ゲートウェイに ping できない。	—	NIC の順序が正しいことを確認します。正しい順序は、control、mgmt、inband です。
VSM VM がゲートウェイには ping できるが、外部サブネットに ping できない。	—	vrf コンテキスト管理を設定します。

ポート プロファイル

ポート プロファイルを作成する際には、次のコマンドを使用して、vCenter Server 上に対応するポートグループを作成します。

- **vmware port-group**
- **state enabled**

システム VLAN の設定を持つプロファイルは、VEM の VSM との通信を許可します。

システム ポート プロファイルが正しいシステム VLANS で定義されていることを確認してください。

必要な基本情報を収集するには、**show port-profile** コマンドと **show port-profile usage** コマンドを使用します。

ポート プロファイルの問題

症状	考えられる原因	解決策
「Possible failure in communication with vCenter Server.」というエラー メッセージが表示される。	VSM が vCenter Server に接続されていない。	**svs connection vc** コマンドを実行して、vCenter Server に接続します。
	ポート グループ名が一意でない。	ポート グループ名は、vCenter Server データセンター内で一意でなければなりません。
ポート プロファイルまたはポート グループが vCenter Server に表示されない。	—	必ず **vmware port-group** コマンドと **state enable** コマンドを実行してください。

ホストでの問題

症状	解決策
「DVS Operation failed for one or more members.」というエラー メッセージが表示される。	**vem status -v** コマンドを実行して、ホスト上で VEM が実行されていることを確認します。
	vem unload コマンドを実行して、VEM をアップロードします。
	vSphere Client で、次の手順を実行して、古くなった DVS を削除します。 **1.** [Host] タブに移動します。[Networking] -> [Configuration] -> Distributed Virtual Switch **2.** [Remove] をクリックします。
ホストが vCenter Server 上に表示されるが、VSM には表示されない。	**vemcmd show trunk** コマンドを実行して、制御 VLAN を伝送するアップリンクがあることを確認します。アップリンクに適用されるプロファイルは、制御 VLAN をシステム VLAN として持つシステム プロファイルでなければなりません。
	アップストリーム スイッチ ポート内の制御 VLAN と VSM VM へのパスを確認します。制御 VLAN を伝送するのは 1 つのアップリンクだけであるか、または制御 VLAN を伝送するすべてのアップリンクとアップストリーム ポートがポート チャネル内にあることを確認します。
モジュール フラップが発生する。	VSM が過負荷になっている。vCenter Server 上の VSM VM に 1GB のメモリと CPU シェアがあることを確認します。

VM トラフィックでの問題

ホスト内 VM トラフィックでの問題をトラブルシューティングする際には、次のガイドラインに従ってください。

- 少なくとも 1 つの VMware 仮想 NIC が正しい DVS ポート グループ上に存在し、接続されていることを確認します。
- VMware 仮想 NIC がダウンしている場合は、OS で設定されている MAC アドレスと VMware によって割り当てられている MAC アドレスの間に矛盾がないか調べます。割り当てられている MAC アドレスは、vmx ファイルで確認できます。

ホスト内 VM トラフィックでの問題をトラブルシューティングする際には、次のガイドラインに従ってください。

- VLAN を VMware 仮想 NIC と共有しているアップリンクは 1 つしかないことを確認します。2 つ以上ある場合は、それらがポート チャネルでなければなりません。
- **show intX counters** コマンドを使用して、アップストリーム スイッチ上の SVI を ping します。

VEM トラブルシューティング コマンド

次のコマンドを使用して、VEM 情報を表示します。

- **vemlog**：VEM カーネル ログの表示と制御を行います。
- **vemcmd**：設定とステータス情報を表示します。
- **vem-support all**：サポート情報を収集します。
- **vem status**：ステータス情報を収集します。
- **vem version**：バージョン情報を収集します。
- **vemlog show last** *number-of-entries*：循環バッファを表示します。

例 21-2　vemlog show last コマンド

```
[root@esx-cos1 ~]# vemlog show last 5
Timestamp                  Entry CPU  Mod Lv         Message
Oct 13 13:15:52.615416      1095   1    1  4 Warning vssnet_port_pg_data_ …
Oct 13 13:15:52.620028      1096   1    1  4 Warning vssnet_port_pg_data_ …
Oct 13 13:15:52.630377      1097   1    1  4 Warning svs_switch_state …
Oct 13 13:15:52.633201      1098   1    1  8    Info vssnet new switch …
Oct 13 13:16:24.990236      1099   1    0  0         Suspending log
```

- **vemlog show info**：ログ内のエントリに関する情報を表示します。

例 21-3　vemcmd show info コマンド

```
[root@esx-cos1 ~]# vemlog show info
          Enabled: Yes
    Total Entries: 1092
  Wrapped Entries: 0
     Lost Entries: 0
  Skipped Entries: 0
Available Entries: 6898
 Stop After Entry: Not Specified
```

- **vemcmd help**：表示できる情報の種類を表示します。

例 21-4　vemcmd help コマンド

```
[root@esx-cos1 ~]# vemcmd help
show card              Show the card's global info
show vlan [vlan]       Show the VLAN/BD table
show bd [bd]           Show the VLAN/BD table
show l2 <bd-number>    Show the L2 table for a given BD/VLAN
show l2 all            Show the L2 table
show port [priv|vsm]   Show the port table
show pc                Show the port channel table
show portmac           Show the port table MAC entries
show trunk [priv|vsm]  Show the trunk ports in the port table
show stats             Show port stats
```

VEM ログ コマンド

次のコマンドで、vemlog を制御できます。

- **vemlog stop**：ログを停止します。
- **vemlog clear**：ログをクリアします。
- **vemlog start** *number-of-entries*：ログを開始し、指定したエントリ数に達したところでログを停止します。
- **vemlog stop** *number-of-entries*：これから指定したエントリ数に達したところでログを停止します。
- **vemlog resume**：ログを開始しますが、停止値のクリアは行いません。

エラー メッセージ

vSphere Client では、最近のタスクが表示されるタブでエラー メッセージを確認できます。エラーの詳しい説明は、[Tasks and Events] タブで確認できます。同じメッセージが、VSM にも伝播されます。

表 21-1 に、VSM で表示される可能性のあるエラー メッセージを示します。

表 21-1　VSM でのエラー メッセージ

エラー	説明
ERROR: [VMWARE-VIM] Extension key was not registered before its use	このエラーは、VSM 拡張キーが登録されていないことを示します。
ERROR: [VMWARE-VIM] A DVS n1000v with spec.name as n1000v already exists, cannot create DVS n1000v.A specified parameter was not correct.spec.name.	このエラーは、初めて **connect** コマンドを入力したあとに表示されるエラーで、同じ名前の DVS がすでに存在することを示します。
ERROR: [VMWARE-VIM] A DVS n1000v with spec.extensionKey as Cisco_Nexus_1000V_2055343757 already exists, cannot create DVS new-n1000v.A specified parameter was not correct.spec.extensionKey	このエラーは、VSM がスイッチ名を変更したあとに別の DVS を作成しようとしたときに表示されます。

表 21-1　VSM でのエラー メッセージ （続き）

エラー	説明
ERROR: [VMWARE-VIM] A DVS n1000v with name as n1000v already exists, cannot reconfigure DVS test.A specified parameter was not correct.Spec.name	このエラーは、同じ名前の DVS がすでに存在することを示します。
Warning: Operation succeeded locally but update failed on vCenter server.[VMWARE-VIM] DVPortgroup test port 0 is in use.The resource vim.dvs.DistributedVirtualPort 0 is in use.	この警告は、VSM がポート プロファイルを削除しようとしたときに、VSM がポート グループに割り当てられている NIC を認識できなかった場合に表示されます。

CHAPTER 22

Network Segmentation Manager

この章では、NSM に関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

- 「Network Segmentation Manager に関する情報」（P.22-1）
- 「Network Segmentation Manager の問題」（P.22-2）
- 「Network Segmentation Manager のトラブルシューティング コマンド」（P.22-7）

Network Segmentation Manager に関する情報

詳細については、『*Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

Network Segmentation Manager の問題

ここでは、Network Segmentation Manager（NSM）の次の問題について考えられる原因、および解決方法について説明します。問題の大半のシステム メッセージは、vShield Manager または vCloud Director に記録されます。

表 22-1　Network Segmentation Manager の問題

症状	考えられる原因	確認およびソリューション
Network Segmentation Manager での vShield Manager の登録失敗 システム メッセージは、vShield Manager に記録されます。	vShield Manager が Network Segmentation Manager に到達できない。	Cisco Nexus 1000V と VMware vShield Manager の間の接続がイネーブルであることを確認します。 vShield Manager が Cisco Nexus 1000V に ping 可能であることを確認します。 そうでない場合は、vShield Manger と Cisco Nexus 1000V との間の L2 または L3 接続を再確立します。詳細については、『*Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
	vShield Manager が Network Segmentation Manager で認証を行えない。	VSM システム ログをチェックして、ユーザ名とパスワードが正確であるかどうかを確認します。ユーザ名とパスワードが正しくない場合、次のシステム ログが表示されます。 **2012 Jan 20 00:49:59 switch %USER-3-SYSTEM_MSG: VALIDATE: user: admin, Authentication failure - validate** そうでない場合は、vShield Manager のネットワーキング設定のユーザ名とパスワードを置き換えます。
	NSM 機能が Cisco Nexus 1000V でイネーブルになっていない。	Cisco Nexus 1000V でイネーブルになっているかどうかを確認します。 **show feature** そうでない場合は、NSM 機能をイネーブルにします。 **feature network-segmentation-manager**
	HTTPS が Cisco Nexus 1000V でイネーブルになっていない。	ブラウザが https://<vsm-ip>/? に接続できるかどうかを確認します。 そうでない場合は、VSM 上で HTTPS サーバをイネーブルにします。 **feature http-server**

表 22-1　Network Segmentation Manager の問題 （続き）

症状	考えられる原因	確認およびソリューション
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to create network segment`	vCloud Director が、ネットワークに関連付けられた VLAN を作成できない。	**1.** VLANS の既存の番号をチェックして、リソースが VLAN を作成できることを確認します。 **show vlan summary** 既存の VLAN の数がサポートされる VLAN の数（つまり 2048）を超える場合は、システムから削除できる VLAN があるかどうかを評価します。 **2.** vCloud Director の VLAN プールに使用可能な 2048 を超える VLAN が含まれていないことを確認します。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Template could not be inherited on port-profile`	ネットワーク用に作成されたポート プロファイル上でネットワーク セグメント ポリシーに関連付けられたポート プロファイルを継承できない。	**1.** ポート プロファイルがあるかどうかを確認します。 **show running-config port-profile** *name* ポート プロファイルの名前を識別するには、ネットワークが使用しようとしていたネットワーク セグメント ポリシーを決定する必要があります。これらの値が設定された対応するネットワーク セグメント ポリシーを見つけるには、テナント / 組織 UUID およびネットワークが作成されたネットワーク プールのタイプ（VXLAN または VLAN）に関する情報が必要になります。ネットワーク セグメントのポリシーでこれらの値が設定されていない場合、ポート プロファイルの名前を識別するには、デフォルトのネットワーク セグメント ポリシーを使用します。 **2.** Network Segmentation Manager によって報告されたポート プロファイルの継承の障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set max-ports`	ポート プロファイルで最大ポート数を設定できない。	Network Segmentation Manager によって報告された最大ポート数の障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Network already exists`	同じ名前のネットワークが vCloud Director にすでに存在する。	**1.** 同じ名前の既存のネットワークを削除します。 **no port-profile** *network name* **2.** 同じ名前のブリッジ ドメイン（存在する場合）を削除します。 **no bridge-domain** *name*

表 22-1　Network Segmentation Manager の問題 （続き）

症状	考えられる原因	確認およびソリューション
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to create port-profile`	Cisco Nexus 1000V がネットワークに必要なポート プロファイルを作成できない。	Network Segmentation Manager によって報告されたポート プロファイルの障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Template does not exist`	ネットワークに関連付けられたネットワーク セグメント ポリシーに関連付けられたポート プロファイルを見つけることができない。	**1.** ポート プロファイルがあるかどうかを確認します。 **show running-config port-profile** *name* ポート プロファイルの名前を識別するには、ネットワークが使用しようとしていたネットワーク セグメント ポリシーを決定する必要があります。これらの値が設定された対応するネットワーク セグメント ポリシーを見つけるには、テナント/組織 UUID およびネットワークが作成されたネットワーク プールのタイプ（VXLAN または VLAN）に関する情報が必要になります。ネットワーク セグメントのポリシーでこれらの値が設定されていない場合、ポート プロファイルの名前を識別するには、デフォルトのネットワーク セグメント ポリシーを使用します。 **2.** Network Segmentation Manager によって報告されたポート プロファイルの障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Alias ID not found`	ネットワーク用に作成されたポート プロファイルに関連付けられたポート グループ ID を取得できない。	Verify that the Virtual Supervisor Module（VSM）にアクティブ SVS 接続があることを確認します。 **show svs connection** コマンドを入力したときに、出力に次が表示される必要があります。 **operational status: connected**
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set port-binding`	ネットワークに関連付けられたポート ファイルにポート バインディングを設定できない。	Network Segmentation Manager によって報告されたポート バインディングの障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set vlan`	ネットワークに関連付けられたポート プロファイル上のアクセス VLAN を設定できない。	Network Segmentation Manager によって報告された VLAN 設定の障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

表 22-1　Network Segmentation Manager の問題 （続き）

症状	考えられる原因	確認およびソリューション
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set vmware port-group`	ポート プロファイルの Vmware ポート グループ プロパティを設定できない。	Network Segmentation Manager によって報告されたポート グループ プロパティの障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set state enabled`	イネーブルにするポート プロファイルのプロパティ ステートを設定できない。	Network Segmentation Manager によって報告されたステート イネーブル プロパティ障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to collect svs configuration`	コマンドを実行できない **show svs connection**	Verify that the Virtual Supervisor Module（VSM）にアクティブ SVS 接続があることを確認します。 **show svs connection** コマンドを入力したときに、出力に次が表示される必要があります。 **operational status: connected**
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Operational status is missing`	SVS 接続で動作ステータスを検出できない。	**1.** Verify that the Virtual Supervisor Module（VSM）にアクティブ SVS 接続があることを確認します。 **show svs connection** コマンドを入力したときに、出力に次が表示される必要があります。 **operational status: connected** **2.** 動作ステータスの障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `SVS connection is disconnected`	SVS 接続が切断される。	Verify that the Virtual Supervisor Module（VSM）にアクティブ SVS 接続があることを確認します。 **show svs connection** コマンドを入力したときに、出力に次が表示される必要があります。 **operational status: connected**

表 22-1　Network Segmentation Manager の問題 （続き）

症状	考えられる原因	確認およびソリューション
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to create bridge domain`	ネットワークに関連付けられたブリッジの dmain を作成できない。	セグメンテーション機能がイネーブルになっていることを確認します。 **show feature** そうでない場合は、セグメンテーション機能をイネーブルにします。 **feature segmentation**
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set segment ID`	ネットワークに関連付けられたセグメント ID を設定できない。	セグメント ID がすでに別のブリッジ ドメインで使用されていないことを確認します。 **show bridge-domain** システム ログのエラー メッセージを確認し、セグメント ID を取得します。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set group IP`	ネットワークに関連付けられたグループ IP を設定できない。	Network Segmentation Manager で報告された無効な IP アドレス エラー メッセージのシステム ログを確認し、グループ ID が有効なマルチキャスト IP アドレスを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの作成が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to set port-profile description`	ネットワークに関連付けられたポート プロファイルの説明を設定できない。	Network Segmentation Manager によって報告されたポート プロファイルの説明の障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vCloud Directors からトリガーされたネットワークの削除が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to delete interface using the port-profile`	ポート プロファイルを継承するインターフェイスを削除できない。	**1.** インターフェイスを手動で削除します。 **2.** vCenter Server で、vApp に関連付けられた VM の電源が切断されるようにします。 **3.** VSM でコマンドを実行します。 **no interface vethernet** *vethernet number*

表 22-1　Network Segmentation Manager の問題 （続き）

症状	考えられる原因	確認およびソリューション
vCloud Directors からトリガーされたネットワークの削除が失敗する。次のようなシステム メッセージが vCloud Director に記録されます。 `Failed to delete the port-profile`	ネットワークに関連付けられたポート プロファイルを削除できない。	**1.** ポート プロファイルを手動で削除します。 **2.** Network Segmentation Manager によって報告されたポート プロファイルの削除の障害メッセージのシステム ログを確認します。詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
vEthernet インターフェイスが管理上ダウンしている。インターフェイスは、**NoPortProfile** 状態になります。	vEthernet インターフェイスが検疫状態である。	**1.** インターフェイスが検疫されたことを確認します。 **show port-profile sync-status** **2.** インターフェイスを検疫から戻します。 **no shutdown** インターフェイスがオンラインに戻ります。 **3.** インターフェイスがオンラインかどうかを確認します。 **show interface vethernet**

Network Segmentation Manager のトラブルシューティング コマンド

ポートに関する問題をトラブルシューティングするには、この項のコマンドを使用します。

表 22-2　ポートのトラブルシューティング コマンド

コマンド	目的
show network-segment manager switch	NSM で設定されている Cisco Nexus 1000V を表示します。
show running-config port-profile	ポート プロファイルの設定を表示します。
show running-config network-segment policy	NSM ポリシー設定を表示します。
show network-segment policy usage	ネットワークによるネットワーク セグメンテーション ポリシーの使用状況を表示します。
show network-segment network	ネットワーク セグメンテーション ポリシーに関連付けられたネットワークを表示します。
show network-segment network id *id*	ネットワーク セグメンテーション ポリシーに関連付けられたネットワーク ID を表示します。
show network-segment network name *name*	ネットワーク セグメンテーション ポリシーに関連付けられたネットワークの名前を表示します。
show logging logfile | grep NSMGR	Network Segmentation Manager からのシステム ログを表示します。

show コマンド出力の詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

CHAPTER 23

VXLAN

この章では、Virtual Extensible Local Area Network（VXLAN）の実装時に発生する可能性がある問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「VXLAN に関する情報」（P.23-1）
- 「VXLAN のトラブルシューティング コマンド」（P.23-3）
- 「VEM パケット パスのデバッグ」（P.23-6）
- 「VEM マルチキャストのデバッグ」（P.23-7）
- 「VXLAN Datapath のデバッグ」（P.23-7）

VXLAN に関する情報

- 「概要」（P.23-1）
- 「VXLAN の VEM L3 IP インターフェイス」（P.23-2）
- 「フラグメンテーション」（P.23-2）
- 「スケーラビリティ」（P.23-3）
- 「サポートされる機能」（P.23-3）

概要

VXLAN は、IP カプセル化で MAC とオーバーレイ アプローチを使用することによって、LAN セグメントを作成します。カプセル化は、仮想イーサネット モジュール（VEM）内で、カプセル化される元の仮想マシン（VM）からオリジナル レイヤ 2（L2）フレームを伝送します。ネットワークで送信する MAC フレームをカプセル化する際に、送信元 IP アドレスとして使用する IP アドレスが各 VEM に割り当てられます。このカプセル化されたトラフィックの送信元として使用する VEM ごとに、複数の vmknics を設定できます。カプセル化は、ペイロード フレームの MAC アドレスのスコープに使用される VXLAN 識別子を伝送します。

接続された VXLAN は vNIC のポート プロファイル コンフィギュレーション内で指定され、VM の接続時に適用されます。各 VXLAN は、割り当てられた IP マルチキャスト グループを VXLAN セグメント内でのブロードキャスト トラフィックの伝送に使用します。

VM が VEM に接続する際、VEM 上の特定の VXLAN セグメントに参加する 1 番目の VM の場合、IGMP の参加は VXLAN の割り当てられたマルチキャスト グループに対して発行されます。VM がネットワーク セグメントのパケットを送信する際、ルックアップはフレームの宛先 MAC および

VXLAN 識別子を使用して L2 テーブルで行われます。結果がヒットの場合、L2 テーブル エントリには、フレームをカプセル化するようにリモート IP アドレスが含まれ、フレームは、リモート IP アドレス宛ての IP パケットに格納されて送信されます。結果が失敗（ブロードキャスト/マルチキャストまたは不明なユニキャストは、このバケットになります）の場合、フレームはセグメントの割り当てられた IP マルチキャスト グループに設定される宛先 IP アドレスでカプセル化されます。

カプセル化されたパケットをネットワークから受信すると、カプセル化が解除され、内部フレームおよび VXLAN ID の送信元 MAC アドレスがルックアップ キーとして L2 テーブルに追加され、カプセル化ヘッダーの送信元 IP アドレスは、テーブル エントリのリモート IP アドレスとして追加されます。

VXLAN の VEM L3 IP インターフェイス

VXLAN に接続している vEthernet インターフェイスが VEM にある場合、VEM は少なくとも 1 つの IP/MAC ペアで VXLAN パケットを終端させる必要があります。このため、VEM は IP ホストとして機能します。この目的で、VEM によりサポートされるのは IPv4 アドレッシングだけです。

VEM レイヤ 3（L3）コントロールの設定方法と同様に、VXLAN に使用する IP アドレスは、**capability vxlan** コマンドを持つ vmknic にポート プロファイルを割り当てることによって設定されます。

vPC-HM MAC-Pinning が必要なサーバ コンフィギュレーションで複数のアップリンク、またはサブグループ上の VXLAN トラフィックの伝送をサポートするには、最大 4 つの vmknics と **capability vxlan** を設定できます。同じ ESX/ESXi ホスト内のすべての VXLAN vmknics は、**capability vxlan** パラメータを持つ必要がある同じポート プロファイルに割り当てることを推奨します。

ローカル vEthernet インターフェイスによってソースされた VXLAN トラフィックは、フレームの送信元 MAC アドレスに基づいてこれらの vmknics 間で分散されます。VEM は自動的に複数の VXLAN vmknics を別々のアップリンクにピン接続します。アップリンクに障害が発生すると、VEM は自動的に vmknic を動作アップリンクに再ピン接続します。

カプセル化されたトラフィックが異なるサブネットに接続されている VEM に送られる際、VEM は VMware ホストのルーティング テーブルを使用しません。代わりに、vmknic はリモート VEM IP アドレスに対して ARP を開始します。アップストリーム ルータは、プロキシ ARP 機能を使用して応答するように設定する必要があります。

フラグメンテーション

VXLAN カプセル化のオーバーヘッドは 50 バイトです。フラグメンテーションによるパフォーマンスの低下を回避するには、VXLAN パケットを交換するすべての VEM 間のインターコネクト インフラストラクチャ全体を、VM VNIC が送信するように設定されているよりも 50 バイト多く伝送するように設定する必要があります。たとえば、デフォルト VNIC 設定の 1500 バイトを使用している場合、VEM アップリンク ポート プロファイル、アップストリーム物理スイッチ ポート、およびスイッチ間リンクとルータ（存在する場合）は、少なくとも 1550 バイトの MTU を伝送するように設定する必要があります。これが不可能な場合、ゲスト VM 内の MTU を 50 バイト小さく、たとえば、1450 バイトに設定すること推奨します。

これが設定されていない場合、VEM は Path MTU（PMTU）Discovery を実行するかどうかを VM に通知しようとします。VM が小さい MTU でパケットを送信しない場合、VM は IP パケットをフラグメント化します。フラグメンテーションは、IP レイヤだけで行われます。伝送に大きすぎるフレームを VM が送信する場合、VXLAN カプセル化を追加した後、およびフレームに IP パケットを含まない場合、フレームはドロップされます。

スケーラビリティ

VXLAN の最大数

Cisco Nexus 1000V は、合計 2048 の VLAN または VXLAN または 2048 を超えない任意の組み合わせをサポートします。この番号は、Cisco Nexus 1000V のポートの最大数と一致します。これにより、各ポートが異なる VLAN または VXLAN に接続できるようにします。

サポートされる機能

ここでは、次の項目について説明します。

- 「ジャンボ フレーム」（P.23-3）
- 「VXLAN 機能のグローバルなディセーブル化」（P.23-3）

ジャンボ フレーム

ジャンボ フレームは、VXLAN カプセル化のオーバーヘッドに対応するための空き容量が少なくとも 50 バイトあり、物理スイッチ/ルータ インフラストラクチャがこれらのジャンボ サイズの IP パケットを転送できる限り、でサポートされます。

VXLAN 機能のグローバルなディセーブル化

安全策として、**no feature segmentation** コマンドは、VXLAN のポート プロファイルに関連付けられたポートがある場合は許可されません。この機能をディセーブルにする前に、すべてのアソシエーションを削除する必要があります。**no feature segmentation** コマンドは、上のすべての VXLAN ブリッジドメイン設定をクリーンアップします。

VXLAN のトラブルシューティング コマンド

VXLAN 属性を表示するには、次のコマンドを使用します。

ここでは、次の項目について説明します。

- 「VSM コマンド」（P.23-3）
- 「VEM コマンド」（P.23-5）

VSM コマンド

特定のセグメントに属しているポートを表示する方法

```
switch(config)# show system internal seg_bd info segment 10000
Bridge-domain: A
Port Count: 11
Veth1
Veth2
Veth3
```

vEthernet ブリッジ ドメインの設定を表示する方法

```
switch(config)# show system internal seg_bd info port vethernet 1
Bridge-domain: A
segment_id = 10000
Group IP: 225.1.1.1
```

vEthernet ブリッジ設定と ifindex を引数として表示する方法

```
switch(config)# show system internal seg_bd info port ifindex 0x1c000050
Bridge-domain: A
segment_id = 10000
Group IP: 225.1.1.1
```

ブリッジ ドメイン ポートの合計数を表示する方法

```
switch(config)# show system internal seg_bd info port_count
Number of ports: 11
```

ブリッジ ドメイン内部コンフィギュレーションを表示する方法

```
switch(config)# show system internal seg_bd info bd vxlan-home

Bridge-domain vxlan-home (2 ports in all)
Segment ID: 5555 (Manual/Active)
Group IP: 235.5.5.5
State: UP               Mac learning: Enabled
is_bd_created: Yes
current state: SEG_BD_FSM_ST_READY
pending_delete: 0
port_count: 2
action: 4
hwbd: 28
pa_count: 0
Veth2, Veth5
switch(config)#
```

VXLAN vEthernet インターフェイスの情報を表示する方法

```
switch# show system internal seg_bd info port
if_index = <0x1c000010>
Bridge-domain vxlan-pepsi
rid = 216172786878513168
swbd = 4098

if_index = <0x1c000040>
Bridge-domain vxlan-pepsi
rid = 216172786878513216
swbd = 4098

switch#
```

追加の **show** コマンド：

show system internal seg_bd info {pss | sdb | global | all}

show system internal seg_bd {event-history | errors | mem-stats | msgs}

VEM コマンド

VXLAN vEthernet プログラミングの確認手順

```
~ # vemcmd show port segments
                          Native  Seg
  LTL   VSM Port  Mode    SegID   State
   50      Veth5   A       5555   FWD
   51      Veth9   A       8888   FWD
~ #
```

VXLAN vmknic プログラミングの確認手順

```
~ # vemcmd show vxlan interfaces
LTL           IP       Seconds since Last
                       IGMP Query Received
(* Interface on which IGMP Joins are sent)
-----------------------------------------
 49        10.3.3.3        50         *
 52        10.3.3.6        50
~ #
```

vmknics が適切なトランスポート VLAN にあるかどうか確認するには、“vemcmd show port vlans” を使用してください。

VEM ブリッジ ドメインの作成の確認手順

```
~ # vemcmd show bd  bd-name vxlan-home
BD 31, vdc 1, segment id 5555, segment group IP 235.5.5.5, swbd 4098, 1 ports,
"vxlan-home"
Portlist:
     50  RedHat_VM1.eth0

~ #
```

リモート IP の学習の確認手順

```
~ # vemcmd show l2 bd-name vxlan-home
Bridge domain   31 brtmax 4096, brtcnt 2, timeout 300
Segment ID 5555, swbd 4098, "vxlan-home"
Flags:  P - PVLAN  S - Secure  D - Drop
       Type         MAC Address   LTL   timeout   Flags    PVLAN    Remote IP
    Dynamic   00:50:56:ad:71:4e   305         2                      10.3.3.100
     Static   00:50:56:85:01:5b    50         0                       0.0.0.0

~ #
```

統計情報を表示する方法

```
~ # vemcmd show vxlan-stats
  LTL  Ucast   Mcast   Ucast   Mcast    Total
       Encaps  Encaps  Decaps  Decaps   Drops
   49       5   14265       4      15       0
   50       6   14261       4      15     213
   51       1      15       0       0      10
   52       0      11       0       0      15

~ #
```

VXLAN vEthernet/vmknic のポート単位の詳細な統計情報を表示する方法

```
~ # vemcmd show vxlan-stats ltl 51
```

すべてのブリッジ ドメインの VXLAN vmknic のポート単位ブリッジ単位の詳細なドメイン統計情報を表示する方法

```
~ # vemcmd show vxlan-stats ltl <vxlan_vmknic_ltl> bd-all
```

指定したブリッジ ドメインの VXLAN vmknic のポート単位ブリッジ単位の詳細なドメイン統計情報を表示する方法

```
~ # vemcmd show vxlan-stats ltl vxlan_vmknic_ltl bd-name bd-name
```

VEM パケット パスのデバッグ

VEM1 の VM から VEM2 の VM への VXLAN トラフィックをデバッグするには、次のコマンドを使用します。

- VEM1：パケットがセグメント vEthernet からスイッチに着信していることを確認します。

  ```
  vempkt capture ingress ltl vxlan_veth
  ```

- VEM1：VXLAN のカプセル化を確認します。

  ```
  vemlog debug sflisp all
  vemlog debug sfvnsegment all
  ```

- VEM1：リモート IP が学習されたことを確認します。

  ```
  vemcmd show l2 bd-name segbdname
  ```

  リモート IP が学習されていない場合、パケットはマルチキャストにカプセル化されて送信されます。たとえば、VM からの最初の ARP 要求はこの方法で送信されます。

- VEM1：カプセル化されたパケットがアップリンク送信されることを確認します。

  どのアップリンクが使用されるかを調べるには、**vemcmd show vxlan-encap ltl** *ltl* コマンドまたは **vemcmd show l2lisp-encap mac** *mac* を使用します。

  ```
  vempkt capture egress ltl uplink
  ```

- VEM1：任意の障害の統計情報を確認します。

  ```
  vemcmd show vxlan-stats all
  vemcmd show vxlan-stats ltl veth/vxlanvmknic
  ```

- VEM2：カプセル化されたパケットがアップリンクに到達していることを確認します。

  ```
  vempkt capture ingress ltl uplink
  ```

- VEM2：VXLAN カプセル開放を確認します。

  ```
  "vemlog debug sflisp all"
  "vemlog debug sfvnsegment all"
  ```

- VEM2：VXLAN vEthernet で送信されるカプセル解放されたパケットを確認します。

  ```
  vempkt capture egress ltl vxlan_veth
  ```

- VEM2：任意の障害の統計情報を確認します。

  ```
  vemcmd show vxlan-stats all
  vemcmd show vxlan-stats ltl veth/vxlanvmknic
  ```

VEM マルチキャストのデバッグ

VEM マルチキャストをデバッグするには、次のコマンドを使用します。

- VEM の IGMP ステート：

  vemcmd show igmp *vxlan_transport_vlan* **detail**

（注）このコマンドは、セグメント マルチキャスト グループの出力を表示しません。マルチキャスト テーブル スペースを節約するため、セグメントのグループは、VEM 上の IGMP スヌーピングによって追跡されません。

- IGMP クエリー：

vemcmd show vxlan interfaces コマンドを使用して、IGMP クエリーが受信されていることを確認します。

- vmknic からの IGMP Join:

VMware スタックが Join を送信しているかどうかを確認するには、**vempkt capture ingress ltl** *first_vxlan_vmknic_ltl* コマンドを使用します。

Join がアップストリーム ポートに送信されているかどうかを確認するには、**vempkt capture egress ltl** *uplink_ltl* コマンドを使用します。

VXLAN Datapath のデバッグ

ここに挙げるコマンドは、VXLAN 関連の問題のトラブルシューティングに使用できるものです。

ここでは、次の項目について説明します。

- 「Vemlog デバッグ」（P.23-7）
- 「HR」（P.23-8）
- 「Vempkt」（P.23-8）
- 「統計情報」（P.23-8）
- 「show コマンド」（P.23-9）

Vemlog デバッグ

ブリッジ ドメインのセットアップまたは設定をデバッグするには、次のコマンドを使用します。

```
vemlog debug sfbd all
```

ポート設定/CBL/vEthernet LTL ピン接続をデバッグするには、次のコマンドを使用します。

```
vemlog debug sfporttable all
```

（encap/decap の設定と決定）

```
vemlog debug sfvnsegment all
```

実際のパケット編集、VXLAN のインターフェイス処理、およびマルチキャストの処理をデバッグするには、次のコマンドを使用します。

```
vemlog debug sflisp all
```

DPA ソケットのマルチキャストの出入りをデバッグするには、次のコマンドを使用します。

```
echo "debug dpa_allplatform all" > /tmp/dpafifo
```

ブリッジ ドメイン設定をデバッグするには、次のコマンドを使用します。

```
echo “debug sfl2agent all” > /tmp/dpafifo
```

ポート設定をデバッグするには、次のコマンドを使用します。

```
echo “debug sfportagent all” > /tmp/dpafifo
```

capability l2-lisp のヒットレス再接続（HR）をデバッグするには、次のコマンドを使用します。

```
echo “debug sfportl2lisp_cache all” > /tmp/dpafifo
```

CBL のプログラミングをデバッグします。

```
echo “debug sfpixmagent all” > /tmp/dpafifo
```

HR

HR のセグメント情報をデバッグするには、次のコマンドを使用します。

```
echo “debug sfsegment_cache all” > /tmp/dpafifo (to debug segment info HR)
```

（キャッシュされたおよび一時セグメント情報リストの詳細がある場合）

```
echo "show vsm cache vsm control mac" > /tmp/dpafifo
```

Vempkt

Vempkt で VLAN/SegmentID が表示されるようになりました。VEM を通過するパケット パスを追跡するには、vempkt を使用します。

- Encap：Seg-VEth LTL の入力 – アップリンクの出力をキャプチャします。
- Decap：アップリンクの入力 – Seg-VEth LTL の出力をキャプチャします。

統計情報

ポート単位の統計情報の要約を表示するには、次のコマンドを使用します。

```
vemcmd show vxlan-stats
```

VXLAN vmknic のポート単位の詳細な統計情報を表示するには、次のコマンドを使用します。

```
vemcmd show vxlan-stats ltl vxlan_vmknic_ltl
```

VXLAN の vEthernet のポート単位の詳細な統計情報を表示するには、次のコマンドを使用します。

```
vemcmd show vxlan-stats ltl vxlan_veth_ltl
```

すべてのブリッジ ドメインの VXLAN vmknic のポート単位ブリッジ単位の詳細なドメイン統計情報を表示するには、次のコマンドを使用します。

```
vemcmd show vxlan-stats ltl vxlan_vmknic_ltl bd-all
```

指定したブリッジ ドメインの VXLAN vmknic のポート単位ブリッジ単位の詳細なドメイン統計情報を表示するには、次のコマンドを使用します。

vemcmd show vxlan-stats ltl *vxlan_vmknic_ltl* **bd-name** *bd-name*

ポート上で学習したスタティック MAC について、カプセル化およびその後のアップリンク PC へのピン接続に使用する VXLAN vmknic を表示するには、次のコマンドを使用します。

vemcmd show vxlan-encap ltl *vxlan_veth_ltl*

カプセル化およびその後のアップリンク PC へのピン接続に使用する VXLAN vmknic を表示するには、次のコマンドを使用します。

vemcmd show vxlan-encap mac *vxlan_vm_mac*

show コマンド

表 23-1 は、使用可能な **vemcmd show** コマンドのリストです。

表 23-1　vemcmd Show コマンド

コマンド	結果
vemcmd show vxlan interfaces	VXLAN カプセル化インターフェイスを表示します。
vemcmd show port vlans	ブリッジ ドメインのポート プログラミングと CBL 状態を確認します。
vemcmd show bd	ポートの SegmentID/ グループ / リストを表示します。
vemcmd show bd bd-name *bd-name-string*	1 セグメント ブリッジ ドメインを表示します。
vemcmd show l2 all	学習されているリモート IP を表示します。
vemcmd show l2 bd-name *bd-name-string*	1 セグメント ブリッジ ドメインのレイヤ 2 テーブルを表示します。
vemcmd show arp all	外部でカプセル化されたヘッダーの IP-MAC マッピングを表示します。

CHAPTER 24

テクニカル サポートへ問い合わせる前の準備

この章では、テクニカル サポートに問い合わせる前に従う手順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。

- 「シスコのサポート コミュニティ」（P.24-1）
- 「テクニカル サポートへ問い合わせるための情報の収集」（P.24-1）
- 「コア メモリ情報のファイルの取得」（P.24-3）
- 「ファイルのコピー」（P.24-3）

（注） シスコのサポートをシスコのリセラーからご購入された場合は、リセラーに直接お問い合わせください。サポートをシスコから直接購入された場合には、次の URL にアクセスしてシスコのテクニカル サポートにお問い合わせください。
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtm

シスコのサポート コミュニティ

詳細については、次のいずれかのサポート コミュニティにアクセスしてください。

- Cisco Support Community for Server Networking
- Cisco Communities : Nexus 1000V

テクニカル サポートへ問い合わせるための情報の収集

追加の支援を受けるために、カスタマー サポート担当者または Cisco TAC への問い合わせが必要になることがあります。ここでは、次のレベルのサポートに問い合わせる前に実行する必要がある手順の概要について説明します。この手順に従うことにより、問題の解決にかかる時間が短縮されます。

（注） 少なくとも次のステップ 1 が完了するまでは、モジュールやスイッチをリロードしないでください。一部のログとカウンタは揮発性ストレージに保持されているので、リロードを実行すると消去されてしまいます。

テクニカル サポート担当者に問い合わせる前に必要な準備を行うには、次の手順に従います。

ステップ 1　スイッチの情報とコンフィギュレーションを収集します。この作業は、問題解決の前と後で行う必要があります。

Telnet または SSH アプリケーションを設定して、画面出力をテキスト ファイルに記録します。**terminal length 0** コマンドライン インターフェイス（CLI）コマンドを実行し、続いて **show tech-support details** CLI コマンドを実行します。

ステップ 2　次のいずれかのコマンドを使用して、CLI に表示されている正確なエラー コードをメッセージ ログにキャプチャします。

- **show logging log** CLI（エラー メッセージを表示する）
- **show logging last *number***（ログの最後の行数を表示する）

ステップ 3　テクニカル サポートに問い合わせる前に、次の質問に回答します。

- どのスイッチまたはポートで問題が発生しているか。
- ファブリック内の Cisco Nexus 1000V ソフトウェア、ドライバのバージョン、オペレーティング システムのバージョン、およびストレージ デバイスのファームウェア。
- 実行している ESX Server および vCenter Server ソフトウェア。
- どのようなネットワーク トポロジが使用されているか。
- このイベントの発生前または発生時に、環境に変更（VLAN、モジュールの追加、アップグレード）が加えられたか。
- 同様の設定がされた他のデバイスで、この問題が発生したか。
- 問題の発生したデバイスの接続先はどこか（どのスイッチまたはインターフェイスか）。
- この問題が最初に発生したのはいつか。
- この問題が最後に発生したのはいつか。
- この問題の発生頻度はどの程度か。
- 何台のデバイスでこの問題が発生していたか。
- 問題発生時にキャプチャした出力のトレースまたはデバッグを行ったか。どのようなトラブルシューティングの手順を試みたか。次のどのツールを使用したか（使用した場合）。
  - Ethanalyzer、ローカルまたはリモート SPAN
  - CLI デバッグ コマンド
  - traceroute、ping

ステップ 4　問題はソフトウェアをアップグレードしようとしたことに関係していますか。

- Cisco Nexus 1000V の元のバージョンは何であったか。
- Cisco Nexus 1000V の新しいバージョンは何か。

コア メモリ情報のファイルの取得

シスコのカスタマー サポート担当者は、ユーザ システムのファイルを分析用に使用することがあります。このようなファイルの 1 つに、コア ダンプと呼ばれる、メモリ情報が含まれるファイルがあります。このファイルは、TFTP サーバ、またはローカル スイッチの slot0: にあるフラッシュ カードに送信されます。カスタマー サポート担当者の指導に基づいて、このファイルが生成されるようにスイッチをセットアップし、サポート担当者に E メールで送信できるように、生成されたファイルを TFTP サーバへ送信する必要があります。

コア メモリ情報のファイル（コア ダンプ）を生成するには、次の例に示すコマンドを使用します。

```
n1000v# system cores tftp://10.91.51.200/jsmith_cores
n1000v# show system cores
Cores are transferred to tftp://10.91.51.200/jsmith_cores
```

（注）　ファイル（この例では jsmith_cores）が TFTP サーバのディレクトリ内に存在する必要があります。

ファイルのコピー

ファイルをスイッチとの間で移動することが必要になる場合もあります。このようなファイルには、ログ ファイル、コンフィギュレーション ファイル、ファームウェア ファイルなどがあります。

Cisco Nexus 1000V は、常にクライアントとして動作します。つまり、ftp、scp、tftp セッションは常にスイッチで発生し、ファイルは外部システムにプッシュされるか、外部システムからプルされます。

```
File Server: 172.22.36.10
File to be copied to the switch: /etc/hosts
```

copy CLI コマンドは、4 つの転送プロトコルと 12 の異なるファイル ソースをサポートしています。

```
n1000v# copy ?
    bootflash: Select source filesystem
    core: Select source filesystem
    debug: Select source filesystem
    ftp: Select source filesystem
    licenses Backup license files
    log: Select source filesystem
    modflash: Select source filesystem
    nvram: Select source filesystem
    running-config Copy running configuration to destination
    scp: Select source filesystem
    sftp: Select source filesystem
    slot0: Select source filesystem
    startup-config Copy startup configuration to destination
    system: Select source filesystem
    tftp: Select source filesystem
    volatile: Select source filesystem
```

転送メカニズムとしてセキュアなコピー（scp）を使用するには、次の構文を使用します。

```
"scp:[//[username@]server][/path]"
```

ユーザ `user1` を使用して 172.22.36.10 から `/etc/hosts` をコピーする（コピー先は `hosts.txt`）には、次のコマンドを使用します。

```
n1000v# copy scp://user1@172.22.36.10/etc/hosts bootflash:hosts.txt
user1@172.22.36.10's password:
hosts 100% |****************************| 2035 00:00
```

スタートアップ コンフィギュレーションを sftp サーバにバックアップするには、次のコマンドを使用します。

```
n1000v# copy startup-config sftp://user1@172.22.36.10/test/startup-configuration.bak1
Connecting to 172.22.36.10...
User1@172.22.36.10's password:
n1000v#
```

ヒント　サーバへのスタートアップ コンフィギュレーションのバックアップは、毎日および変更を行う前に実施する必要があります。コンフィギュレーションの保存およびバックアップを行う短いスクリプトを記述して、Cisco Nexus 1000V 上で実行することもできます。このスクリプトには、**copy running-configuration startup-configuration** と **copy startup-configuration tftp:**//***server/name*** の 2 つのコマンドだけを含める必要があります。スクリプトを実行するには、**run-script** filename コマンドを使用します。

INDEX

A

ACL
- VEM での ACL ポリシーの表示 15-3
- 制限事項 15-2
- 設定の制限事項 15-2
- 説明 15-1
- トラブルシューティングのためのコマンド 15-2
- ポリシー検証のデバッグ 15-3

C

CLI
- ping コマンド 2-2
- traceroute コマンド 2-2

CPU ステータス
- モニタリング 2-2

D

DHCP
- ログ、収集と評価 19-5

DHCP スヌーピング
- DHCP バインディングの表示 19-7
- 問題の現象と解決方法 19-3

DVS
- 回復 21-2
- 拡張キーの確認 3-9

G

GUI のアップグレード
- 問題の現象と解決方法 5-7

H

HA
- システム レベルのサポート 6-2
- 説明 6-1
- トラブルシューティングのためのコマンド 6-5
- ネットワーク レベルのサポート 6-2
- 問題の現象と解決方法 6-3

I

IGMP スヌーピング
- 説明 18-1
- トラブルシューティングのガイドライン 18-2
- トラブルシューティングのためのコマンド 18-3
- 問題の現象と解決方法 18-5

IP ARP インスペクション
- 問題の現象と解決方法 19-4

IP ソース ガード
- 問題の現象と解決方法 19-5

ISSU のアップグレード
- 問題の現象と解決方法 5-1

M

MAC アドレス テーブル
- 検証 11-7

MAC 学習 11-12

MS-NLB 11-12

MTU 設定、ジャンボ フレームを使用 21-6

N

NetFlow
設定に関する問題 14-3
説明 14-1
トラブルシューティングのためのコマンド 14-2
Nexus 1000V
システムの概要 21-1
Nexus 1000V スイッチ
との間でのファイルのコピー 24-3
プラグイン 3-7
NLB 11-12

Q

QoS
VEM 上での QoS ポリシーのトラブルシューティング 16-3
設定の制限事項 16-2
説明 16-1
トラブルシューティングのためのコマンド 16-2
ポリシー検証エラーのデバッグ 16-4
Quality of Service。「QoS」を参照

R

RADIUS
アカウンティング ログ 2-5

S

show port-profile sync-status コマンド 9-7
show port-profile virtual usage コマンド 9-7
SPAN
セッションの要件 17-2
設定時の注意事項 17-1
説明 17-1
トラブルシューティングのためのコマンド 17-3
問題の現象と解決方法 17-2
Switched Port Analyzer（スイッチド ポート アナライザ）。「SPAN」を参照
syslog
「システム メッセージ」を参照

V

vCenter Server
VSM との接続の確認 7-6
VSM の削除 3-12
VSM の登録解除 3-13
制限事項 21-2
接続のリフレッシュ 3-4
設定が正しいかの確認 7-9
VEM
vemlog のためのコマンド 21-12
仮想ポート 11-2
ステータス 11-13
設定が正しいかの確認 7-11
ドメイン パラメータ 3-4
トラブルシューティングのためのコマンド 21-11
物理ポート 11-2
ポートのビュー 11-2
VEM ステータスのチェック 11-13
VEM のアップグレード
問題の現象と解決方法 5-5
VLAN
作成できない 12-3
説明 12-1
トラフィックがトランクを通過しない 10-6
トラブルシューティングのチェックリスト 12-2
VM
トラフィックでの問題 21-11
パフォーマンスの向上 3-4
vmnic
番号の割り当て 11-3
VSD
トラブルシューティングのためのコマンド 5-18, 19-6, 20-3

問題の現象と解決方法 20-1
ログの収集と評価 20-2
VSM
拡張キーの識別 3-13
作成 21-9
ステータス 11-13
設定が正しいかの確認 7-7
ドメイン パラメータ 3-4
トラブルシューティングのためのコマンド 7-15
ポートのビュー 11-3
ホストの削除 3-12
VSM ステータスのチェック 11-13
vSphere Client
エラー メッセージ 21-12
VXLAN
VEM L3 IP インターフェイス 23-2
概要 23-1
最大数 23-3
スケーラビリティ 23-3
フラグメンテーション 23-2

あ

アクセス コントロール リスト。「ACL」を参照。
アップグレード
GUI の問題の現象と解決方法 5-7
ISSU の問題の現象と解決方法 5-1
VEM の問題の現象と解決方法 5-5

い

インストール
インストール フローチャートの再作成 3-4, 3-11
インターネット グループ管理プロトコル スヌーピング。「IGMP スヌーピング」を参照

え

エラー メッセージ
vSphere Client 21-12

お

オンライン サポート コミュニティ 1-7, 24-1

か

概要
VXLAN 23-1
拡張キー
vCenter Server での登録解除 3-13
確認、特定の DVS に結び付けられた 3-9
拡張キーの登録解除 3-13
カスタマー サポート
シスコまたは VMware への連絡 1-8
情報の収集 24-1
仮想 NIC 11-2
仮想イーサネット ポート（veth） 11-2
仮想イーサネット モジュール。「VEM」を参照。
仮想スーパーバイザ モジュール。「VSM」を参照。
関連資料 xv, ii-xv, ii-xvii

き

キー、拡張 3-9

け

検証
MAC アドレス テーブル 11-7

こ

コア ダンプ 24-3

さ

最大数
VXLAN 23-3
サポート コミュニティへのリンク 1-7, 24-1
サポートされる機能
ジャンボ フレーム 23-3

し

シスコのサポート コミュニティ 1-7, 24-1
システム プロセス
モニタリング 2-2
システム メッセージ
CLI の使用 1-6
Sslog サーバ 1-6
概要 1-5, 2-5
説明と推奨処置 1-5
ログ レベル 2-5, 2-6
自動スタティック MAC 学習 11-12
自動スタティック MAC 学習のディセーブル化 11-12
ジャンボ フレームおよび MTU 21-6

す

スケーラビリティ
VXLAN 23-3
スタティック MAC 学習 11-12
ステータス、VEM 11-13
ステータス、VSM 11-13

せ

接続
vCenter Server 3-6
VSM と vCenter Server に関する問題の現象と解決方法 21-5
VSM と vCenter Server の間の接続確認 3-5
VSM と VEM の間の接続確認 7-9
確認 1-3

そ

ソフトウェア
コア ダンプ 24-3

た

ダイナミック ARP インスペクション
DHCP スヌーピング バインディング データベース 19-2

て

ディセーブル化
VXLAN 機能をグローバルで 23-3

と

同期の問題 8-2, 8-8
ドメイン パラメータ 3-4
トラブルシューティング プロセス
一般的な CLI コマンド 1-3
一般的なプロセスの手順 1-2
ガイドライン 1-2
概要 1-1
ベスト プラクティス 1-1
トランキング
概要 10-2
初期チェックリスト 10-2

ね

ネットワーク アダプタ 3-5
ネットワーク ロード バランシング 11-12

は

ハイ アベイラビリティ。「HA」を参照

ふ

プライベート VLAN
説明 13-1
トラブルシューティングのガイドライン 13-2
トラブルシューティングのためのコマンド 13-2
フラグメンテーション
VXLAN 23-2

ほ

ポート
errdisable 8-5
インターフェイス記述 8-1
概要 8-1
確認 1-3
トラブルシューティングのチェックリスト 8-3
フラッピング 8-5
ポート インターフェイスがイネーブルにできない 8-4
ポートがイネーブルになっており、ポート セキュリティが ErrDisabled になっている 8-7
ポート カウンタ 8-2, 8-8
ポート状態の表示 8-8
ポート セキュリティに関する問題 8-2
ポート セキュリティのアドレス カウント超過違反 8-7
ポート タイプ 11-4
ポートの状態がリンク障害または接続なしになっている 8-4
ポート グループ
VSM VM への割り当て 3-5
仮想インターフェイス 3-5
ポート チャネル
インターフェイスがオンラインにならない 10-4
初期チェックリスト 10-2
説明 10-1
トラブルシューティングのためのコマンド 10-3
トラブルシューティングのチェックリスト 10-2
非対称 10-3
ポート チャネルの設定の確認 10-5
ポート チャネルの特性をインターフェイスに強制する 10-5
ポート チャネルを作成できない 10-4
ポート プロファイル
vCenter Server 上での対応するポート グループの作成 21-9
概要情報 9-1
説明 9-1
デバッグ ログ 9-6
トラブルシューティングのためのコマンド 4-4, 9-6
問題の現象と解決方法 9-3
ホスト
問題の現象と解決方法 21-9, 21-10

ま

マニュアル
追加資料 xv, ii-xv
表記法 xiv
マルチキャスト
説明 18-1

も

モジュール
VSM に表示されない 7-1
仮想イーサネット モジュール（VEM） 7-1
仮想スーパーバイザ モジュール（VSM） 7-1
ライセンス付き 4-1
ライセンスなし 4-1

ら

ライセンス

Cisco Nexus N1000V ライセンス パッケージ 4-1
Cisco Nexus N1000V ライセンス ファイルの内容 4-2
VMware Enterprise Plus 3-2
トラブルシューティングのチェックリスト 4-2
ライセンス付きモジュール 4-1
ライセンスなしモジュール 4-1

り

リンク アグリゲーション制御プロトコル（LACP） 6-2

れ

レイヤ 2 スイッチング
VEM 間 ping 11-4
VEM 内 ping 11-5
概要 11-1
トラフィック中断 11-6
問題の現象と解決方法 11-7

ろ

ログ 1-7
ログ レベル 2-6