Cisco Nexus 1000V システム管理コンフィギュレーション ガイド リリース 4.2(1)SV1(5.1)

2012 年 1 月 27 日

Text Part Number: OL-25385-01-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 システム管理コンフィギュレーション ガイド リリース 4.2(1)SV1(5.1)
© 2009-2012 Cisco Systems, Inc. All rights reserved.

Copyright © 2009–2012, 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 xiii

はじめに xv

対象読者 xv

マニュアルの構成 xv

表記法 xvi

参考資料 xvii

関連資料 xvii

マニュアルの入手方法およびテクニカル サポート xix

CHAPTER 1

システム管理の概要 1-1

CDP 1-1

ドメイン 1-1

サーバ接続 1-2

コンフィギュレーション管理 1-2

ファイル管理 1-2

ユーザ管理 1-2

NTP 1-2

ローカル SPAN および ERSPAN 1-2

SNMP 1-3

NetFlow 1-3

システム メッセージ 1-3

iSCSI マルチパス 1-3

トラブルシューティング 1-3

CHAPTER 2

CDP の設定 2-1

CDP の概要 2-1

ハイ アベイラビリティ 2-2

注意事項および制約事項 2-2

デフォルト 2-2

CDP の設定 2-3

CDP グローバル コンフィギュレーション 2-3
CDP のグローバルなイネーブルまたはディセーブル 2-3
CDP バージョンのアドバタイズ 2-4
CDP オプションの設定 2-5
CDP インターフェイス コンフィギュレーション 2-7
インターフェイス上での CDP のイネーブル化 2-7
インターフェイス上での CDP のディセーブル化 2-8
CDP のモニタリング 2-10
CDP 統計情報の消去 2-10
CDP 設定の確認 2-10
CDP のコンフィギュレーション例 2-14
その他の関連資料 2-14
関連資料 2-14
標準 2-15
CDP 機能の履歴 2-15

CHAPTER 3
ドメインの設定 3-1
ドメインについて 3-1
レイヤ 3 コントロールについて 3-1
注意事項および制約事項 3-2
デフォルト設定 3-3
ドメインの設定 3-3
ドメインの作成 3-4
レイヤ 3 トランスポートへの変更 3-6
レイヤ 2 トランスポートへの変更 3-8
レイヤ 3 コントロール用のポート プロファイルの作成 3-10
制御 VLAN の作成 3-13
パケット VLAN の作成 3-14
VSM ドメイン機能の履歴 3-16

CHAPTER 4
サーバ接続の管理 4-1
サーバ接続について 4-1
注意事項および制約事項 4-2
vCenter Server への接続 4-2
vCenter Server からの切断 4-4
vCenter Server からの DVS の削除 4-5
VSM が接続されていない場合の vCenter Server からの DVS の削除 4-5
admin ユーザまたは admin グループの設定 4-6

vCenter Server からの DVS の削除 4-7
ホスト マッピングの設定 4-7
ホスト マッピングについて 4-7
モジュールからのホスト マッピングの削除 4-7
新しいホストへのマッピング 4-9
ホスト マッピングの表示 4-10
接続の確認 4-10
ドメインの確認 4-11
設定の確認 4-11
モジュール情報の確認 4-14
サーバ接続機能の履歴 4-16

CHAPTER 5 設定の管理 5-1
コンフィギュレーション管理について 5-1
スイッチ名の変更 5-1
Message of the Day の設定 5-2
設定の確認 5-3
ソフトウェアとハードウェアのバージョンの確認 5-3
実行コンフィギュレーションの確認 5-4
スタートアップ コンフィギュレーションと実行コンフィギュレーションの比較 5-6
インターフェイス コンフィギュレーションの確認 5-7
インターフェイス コンフィギュレーションの要約の確認 5-7
インターフェイス コンフィギュレーションの詳細の確認 5-8
全インターフェイスの要約の確認 5-8
全インターフェイスの実行コンフィギュレーションの確認 5-9
コンフィギュレーションの保存 5-10
コンフィギュレーションの削除 5-10
コンフィギュレーション管理機能の履歴 5-11

CHAPTER 6 ファイルの使用 6-1
ファイルについて 6-1
ファイル システム内の移動 6-1
ファイル システムの指定 6-2
作業ディレクトリの特定 6-2
ディレクトリの変更 6-3
ファイル システム内のファイルの一覧表示 6-3
ファイルをコピーするために使用できるファイル システムの特定 6-4
タブ補完の使用 6-5

ファイルのコピーとバックアップ 6-5
ディレクトリの作成 6-7
既存のディレクトリの削除 6-7
ファイルの移動 6-8
ファイルまたはディレクトリの削除 6-9
ファイルの圧縮 6-9
ファイルの圧縮解除 6-11
コマンド出力のファイル保存 6-12
ロード前のコンフィギュレーション ファイルの確認 6-12
以前のコンフィギュレーションへのロールバック 6-13
ファイルの表示 6-13
ファイルの内容の表示 6-13
ディレクトリの内容の表示 6-14
ファイル チェックサムの表示 6-15
ファイルの最後の行の表示 6-15
ファイル管理機能の履歴 6-15

CHAPTER 7 ユーザの管理 7-1
ユーザ管理について 7-1
現在のユーザ アクセスの表示 7-1
ユーザへのメッセージ送信 7-2
ユーザ管理機能の履歴 7-2

CHAPTER 8 NTP の設定 8-1
NTP の概要 8-1
NTP ピア 8-2
ハイ アベイラビリティ 8-2
NTP の前提条件 8-2
設定時の注意事項および制限事項 8-3
デフォルト設定 8-3
NTP サーバおよびピアの設定 8-3
NTP 統計情報またはセッションのクリア 8-4
NTP の設定確認 8-4
NTP の設定例 8-5
その他の関連資料 8-5
関連資料 8-5
標準 8-5

NTP の機能の履歴 8-5

CHAPTER 9 ローカル SPAN および ERSPAN の設定 9-1
SPAN および ERSPAN について 9-1
SPAN ソース 9-1
SPAN 送信元の特性 9-2
SPAN 宛先 9-2
ローカル SPAN 宛先の特性 9-2
ERSPAN 宛先の特性 9-3
ローカル SPAN 9-3
カプセル化リモート SPAN 9-4
ネットワーク解析モジュール 9-4
SPAN セッション 9-5
SPAN 注意事項および制約事項 9-5
デフォルト設定 9-6
SPAN の設定 9-6
ローカル SPAN セッションの設定 9-7
ERSPAN ポート プロファイルの設定 9-9
ERSPAN セッションの設定 9-13
SPAN セッションのシャットダウン 9-16
SPAN セッションの再開 9-17
許可される ERSPAN フロー ID の設定 9-19
SPAN の設定確認 9-20
設定例 9-20
SPAN セッションの設定例 9-20
ERSPAN セッションの設定例 9-21
その他の関連資料 9-22
関連資料 9-22
標準 9-22
SPAN および ERSPAN 機能の履歴 9-23

CHAPTER 10 SNMP の設定 10-1
SNMP について 10-1
SNMP 機能の概要 10-1
SNMP 通知 10-2
SNMPv3 10-2
SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル 10-3
ユーザベースのセキュリティ モデル 10-4

CLI および SNMP ユーザの同期 10-4
グループベースの SNMP アクセス 10-5
ハイ アベイラビリティ 10-5
注意事項および制約事項 10-5
デフォルト設定 10-5
SNMP の設定 10-6
SNMP ユーザの設定 10-6
SNMP メッセージ暗号化の適用 10-7
SNMP コミュニティの作成 10-8
SNMP 通知レシーバーの設定 10-8
通知ターゲット ユーザの設定 10-9
SNMP 通知のイネーブル化 10-9
インターフェイスに関する linkUp/linkDown 通知のディセーブル化 10-11
TCP による SNMP のワンタイム認証のイネーブル化 10-11
SNMP スイッチのコンタクトおよびロケーション情報の指定 10-11
SNMP のディセーブル化 10-12
AAA 同期時間の変更 10-13
SNMP の設定確認 10-13
SNMP の設定例 10-13
その他の関連資料 10-14
関連資料 10-14
標準 10-14
MIB 10-15
SNMP の機能の履歴 10-16

CHAPTER 11 **NetFlow の設定** 11-1
NetFlow 情報 11-1
フローとは何か 11-2
フロー レコード定義 11-2
あらかじめ定義されたフロー レコード 11-3
NetFlow データへのアクセス 11-5
コマンドライン インターフェイス（CLI） 11-6
フロー モニタ 11-6
フロー エクスポータ 11-6
エクスポート フォーマット 11-6
NetFlow コレクタ 11-7
NetFlow コレクタ サーバへのフローのエクスポート 11-7
NetFlow データの例 11-8
ネットワーク解析モジュール 11-9

ハイ アベイラビリティ 11-9
NetFlow の前提条件 11-9
設定時の注意事項および制限事項 11-9
デフォルト設定 11-10
NetFlow 機能のイネーブル化 11-10
NetFlow の設定 11-11
フロー レコードの定義 11-12
フロー エクスポータの定義 11-15
フロー モニタの定義 11-17
フロー モニタのインターフェイスへの割り当て 11-19
ポート プロファイルへのフロー モニタの追加 11-20
NetFlow の設定確認 11-22
NetFlow のコンフィギュレーション例 11-25
その他の関連資料 11-26
関連資料 11-27
標準 11-27
NetFlow の機能の履歴 11-27

CHAPTER 12 システム メッセージ ロギングの設定 12-1
システム メッセージ ロギングの概要 12-1
システム メッセージ ロギング ファシリティ 12-2
注意事項および制約事項 12-5
デフォルト設定 12-5
システム メッセージ ロギングの設定 12-5
ターミナル セッションへのシステム メッセージ ロギングの設定 12-6
ターミナル セッションのシステム メッセージ ロギングのデフォルトの復元 12-7
モジュールのシステム メッセージ ロギングの設定 12-8
モジュールのシステム メッセージ ロギングのデフォルトの復元 12-9
ファシリティのシステム メッセージ ロギングの設定 12-9
ファシリティのシステム メッセージ ロギングのデフォルトの復元 12-11
Syslog サーバの設定 12-11
サーバのシステム メッセージ ロギングのデフォルトの復元 12-12
UNIX または Linux システムを使用したロギングの設定 12-13
ログ ファイルの表示 12-13
システム メッセージ ロギングの設定確認 12-14
システム メッセージ ロギングの設定例 12-18
その他の関連資料 12-18
関連資料 12-18

標準 12-18
システム メッセージ ロギング機能の履歴 12-18

CHAPTER 13 iSCSI マルチパスの設定 13-1
iSCSI マルチパスについて 13-1
概要 13-1
サポートされる iSCSI アダプタ 13-2
VMware スイッチの iSCSI マルチパス設定 13-3
注意事項および制約事項 13-4
前提条件 13-5
デフォルト設定 13-5
iSCSI マルチパスの設定 13-5
アップリンクのピン接続とストレージのバインド 13-5
アップリンクのピン接続とストレージのバインドのプロセス 13-6
VMkernel NIC のポート プロファイルの作成 13-6
VMkernel NIC の作成およびポート プロファイルの適用 13-9
NIC の手動ピン接続 13-10
物理 NIC の iSCSI アダプタの特定 13-11
vSphere Client の iSCSI アダプタの特定 13-12
ホスト サーバの iSCSI アダプタの特定 13-12
iSCSI アダプタへの VMkernel NIC のバインド 13-13
ハードウェアの iSCSI 設定への変換 13-14
ハードウェアの iSCSI 設定への変換のプロセス 13-14
ソフトウェアの iSCSI アダプタへのバインドの解除 13-14
DVS へのハードウェアの NIC の追加 13-15
VMkernel NIC アクセス VLAN の変更 13-15
アクセス VLAN の変更のプロセス 13-15
アクセス VLAN の変更 13-16
iSCSI マルチパスの設定の確認 13-18
ストレージ切断の検出の管理 13-19
その他の関連資料 13-21
関連資料 13-21
標準 13-21
iSCSI マルチパス機能の履歴 13-21

CHAPTER 14 VSM バックアップとリカバリの設定 14-1
VSM バックアップとリカバリに関する情報 14-1
注意事項および制約事項 14-1

VSM バックアップとリカバリの設定 14-2
VSM のバックアップ 14-2
VSM のバックアップの実行 14-2
定期的なバックアップの実行 14-8
VSM のリカバリ 14-8
バックアップ VSM VM の配置 14-8
古い設定の削除 14-16
VSM のバックアップ コンフィギュレーションの復元 14-17
その他の関連資料 14-23
関連資料 14-23
標準 14-24
VSM バックアップとリカバリの機能の履歴 14-24

CHAPTER 15 仮想化ワークロード モビリティ（DC から DC vMotion へ） 15-1
仮想化ワークロード モビリティ（DC から DC vMotion へ）の概要 15-1
ストレッチ クラスタ 15-1
スプリット クラスタ 15-2
仮想化ワークロード モビリティ（DC から DC vMotion へ）の前提条件 15-2
注意事項および制約事項 15-2
物理的なサイトの検討 15-2
Inter-Site リンク障害の処理 15-3
ヘッドレス モードの動作 15-3
VSM と VEM 間の追加の距離 / 遅延の処理 15-3
VSM の移行 15-3
ESX ホストまたは ESXi ホストでホストされている VSM の移行 15-4
仮想化ワークロード モビリティ（DC から DC vMotion へ）設定の確認 15-4
仮想化ワークロード モビリティ（DC から DC vMotion へ）のモニタリング 15-4
設定の制限値 15-4
仮想化ワークロード モビリティ（DC から DC vMotion へ）の機能の履歴 15-5

CHAPTER 16 設定の制限値 16-1

INDEX

新機能および変更された機能に関する情報

この章では、各リリースで追加または変更された情報と、その情報がこのマニュアルの中で記載されている場所を示します。

内容	説明	変更されたリリース	参照先
『Cisco Nexus 1000V システム管理コンフィギュレーション ガイド リリース 4.2(1)SV1(5.1)』には新しい情報は追加されていません			
仮想化ワークロード モビリティ（DC から DC vMotion へ）	この機能は、2 つの物理データセンター間にある Cisco Nexus 1000 に対応します。	4.2(1)SV1(4a)	第 15 章「仮想化ワークロード モビリティ（DC から DC vMotion へ）」
DVS の削除	VSM への接続がない場合に vCenter Server から DVS を削除できます。	4.2(1)SV1(4a)	「サーバ接続の管理」
VSM バックアップ	両方の VSM が HA 環境で削除されている場合に VSM を復元できます。	4.2(1)SV1(4a)	「VSM バックアップとリカバリの設定」
NetFlow 機能のイネーブル化	NetFlow 機能をイネーブルまたはディセーブルにできます。	4.2(1)SV1(4)	「NetFlow の設定」
ローカル SPAN 送信元としてのポート プロファイルの追加	ローカル SPAN モニタ トラフィックの発信元としてポート プロファイルを指定できます。	4.2(1)SV1(4)	「ローカル SPAN および ERSPAN の設定」
ERSPAN 送信元としてのポート プロファイルの追加	ERSPAN のモニタ トラフィックの送信元としてポート プロファイルを指定できます。	4.2(1)SV1(4)	「ローカル SPAN および ERSPAN の設定」
ハードウェアの iSCSI マルチパス	マルチパスにハードウェアの iSCSI アダプタを使用できます。	4.2(1)SV1(4)	「iSCSI マルチパスの設定」
追加された SNMP MIB	サポートされている MIB のリスト。	4.2(1)SV1(4)	「MIB」
ネットワーク解析モジュール（NAM）	NetFlow データソースに対する NAM サポート	4.0(4)SV1(3)	「NetFlow の設定」
	ERSPAN データソースに対する NAM サポート	4.0(4)SV1(3)	「ローカル SPAN および ERSPAN の設定」
ERSPAN タイプ III ヘッダー	ERSPAN タイプ III の拡張された形式を持つヘッダー フレームにより、ネットワーク管理、侵入検出、合法的代行受信のサポートが強化されます。	4.0(4)SV1(3)	「ローカル SPAN および ERSPAN の設定」

内容	説明	変更されたリリース	参照先
レイヤ 3 コントロール	VSM はレイヤ 3 でのアクセスが可能になり、別のレイヤ 2 ネットワークに存在するホストを制御できるようになります。	4.0(4)SV1(2)	「ドメインの設定」
iSCSI マルチパス	サーバとそのストレージ デバイスとの間に複数のルートをセットアップできるようになります。	4.0(4)SV1(2)	「iSCSI マルチパスの設定」
参考資料	Cisco Nexus 1000V の設定を行う前に読んでおくことが推奨される資料が記載されています。	4.0(4)SV1(2)	「はじめに」
設定の制限値	Cisco Nexus 1000V の設定の制限値が記載されています。	4.0(4)SV1(2)	「設定の制限値」

はじめに

システム管理のコンフィギュレーション マニュアルには、システム メッセージ ロギングの設定、コンフィギュレーション ファイルの管理、サーバ接続の管理など、システムを管理するための手順が記載されています。

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.xv）
- 「マニュアルの構成」（P.xv）
- 「表記法」（P.xvi）
- 「関連資料」（P.xvii）
- 「マニュアルの入手方法およびテクニカル サポート」（P.xix）

対象読者

本書は、次の経験および知識を持つネットワーク管理者を対象としています。

- 仮想化の知識
- VMware のツールを使用した仮想スイッチの設定

（注） VMware vNetwork 分散スイッチの知識はなくてもかまいません。

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。

章とタイトル	説明
第 1 章「システム管理の概要」	利用可能なシステム管理機能について説明します。
第 2 章「CDP の設定」	他の接続したデバイスとの情報送受信用の Cisco Discovery Protocol（CDP）を設定するための手順を説明しています。

章とタイトル	説明
第 3 章「ドメインの設定」	ドメインの作成と VLAN の割り当てを含む Cisco Nexus 1000V ドメインの設定方法について説明します。
第 4 章「サーバ接続の管理」	接続を確立してサーバに接続する方法、サーバから切断する方法、およびサーバ接続を表示する方法について説明します。
第 5 章「設定の管理」	コンフィギュレーション ファイルの管理方法について説明します。
第 6 章「ファイルの使用」	ファイルのコピーと移動を含むファイルを管理する方法を説明しています。
第 7 章「ユーザの管理」	現在のユーザの表示およびユーザへのメッセージの送信を含むシステム上でユーザを管理する方法を説明しています。
第 8 章「NTP の設定」	ネットワーク タイム プロトコル（NTP）を設定して、一連の分散したタイム サーバおよびクライアント間での計時を同期化するための手順を説明しています。この同期によって、複数のネットワーク デバイスからシステム ログおよびその他の時刻特定イベントを受信したときに、イベントを相互に関連付けることができます。
第 9 章「ローカル SPAN および ERSPAN の設定」	イーサネット スイッチド ポート アナライザ（SPAN）を設定する方法を説明しています。
第 10 章「SNMP の設定」	ユーザ、メッセージ暗号化、通知、TCP での認証などを含む SNMP を設定する方法を説明しています。
第 11 章「NetFlow の設定」	NetFlow を設定する方法を説明しています。
第 12 章「システム メッセージ ロギングの設定」	システム メッセージ ロギングの設定方法について説明します。
第 13 章「iSCSI マルチパスの設定」	サーバとそのストレージ デバイスとの間に複数のルートをセットアップするための iSCSI マルチパスを設定する方法を説明しています。
第 14 章「VSM バックアップとリカバリの設定」	ビジュアル スーパーバイザ モジュール（VSM）のバックアップとリカバリの手順を設定する方法について説明します。
第 15 章「仮想化ワークロード モビリティ（DC から DC vMotion へ）」	2 つのデータセンターに Cisco Nexus 1000 が存在する環境について説明します。
第 16 章「設定の制限値」	システム管理の設定の制限値を示します。

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。

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。
{ }	波カッコの中の要素は、必須の選択要素です。
[ ]	角カッコの中の要素は、省略可能です。

x | y | z	いずれか 1 つを選択する要素は、縦線で区切って示されます。
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	デバイスが表示するターミナル 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、注釈および注意に次の表記法を使用しています。

（注） 「*注釈*」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。

参考資料

Cisco Nexus 1000V の設定を開始する前に、次の資料を読んでおくことをお勧めします。

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

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

『*Cisco VN-Link: Virtualization-Aware Networking*』ホワイト ペーパー

関連資料

この項では、Cisco Nexus 1000 で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 Troubleshooting Guide, Release 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

システム管理の概要

この章では、次のシステム管理機能について説明します。

- 「CDP」（P.1-1）
- 「ドメイン」（P.1-1）
- 「サーバ接続」（P.1-2）
- 「コンフィギュレーション管理」（P.1-2）
- 「ファイル管理」（P.1-2）
- 「ユーザ管理」（P.1-2）
- 「NTP」（P.1-2）
- 「ローカル SPAN および ERSPAN」（P.1-2）
- 「SNMP」（P.1-3）
- 「NetFlow」（P.1-3）
- 「システム メッセージ」（P.1-3）
- 「トラブルシューティング」（P.1-3）

CDP

Cisco Discovery Protocol（CDP）は、データ リンク層の上で動作し、接続されているすべてのシスコ デバイスに情報をアドバタイズし、接続されているシスコ デバイスに関する情報を検出および表示するために使用されます。CDP は、シスコ製のすべての機器で動作します。

CDP の詳細については、第 2 章「CDP の設定」を参照してください。

ドメイン

Cisco Nexus 1000V 用のドメイン名を作成し、通信および管理用の制御 VLAN とパケット VLAN を追加する必要があります。この処理は、Cisco Nexus 1000V のソフトウェアをインストールする際の初期セットアップの一部です。ドメインを後で作成する必要がある場合は、**setup** コマンドを使用するか、第 3 章「ドメインの設定」に記載されている手順を実行します。

レイヤ 3 コントロールを VSM ドメイン内に確立すると、VSM はレイヤ 3 でのアクセスが可能になり、別のレイヤ 2 ネットワークに存在するホストを制御できるようになります。詳細については、「レイヤ 3 コントロールについて」（P.3-1）を参照してください。

サーバ接続

vCenter Server または ESX サーバに接続するには、初めに Cisco Nexus 1000V 内で接続を定義する必要があります。第 4 章「サーバ接続の管理」では、vCenter Server に接続する方法と接続を切断する方法、および接続を表示する方法を説明します。

コンフィギュレーション管理

Cisco Nexus 1000V では、スイッチ名の変更と Messages of the Day の設定や、コンフィギュレーション ファイルの表示、保存、および消去を管理者が実行できるようになっています。コンフィギュレーション管理の詳細については、第 5 章「設定の管理」を参照してください。

ファイル管理

単一のインターフェイスを使用して、次のものを含むファイル システムを管理できます。

- フラッシュ メモリ ファイル システム
- ネットワーク ファイル システム（TFTP および FTP）
- データを読み書きするためのその他のエンドポイント（実行コンフィギュレーションなど）

ファイルの使用方法の詳細については、第 6 章「ファイルの使用」を参照してください。

ユーザ管理

デバイスに現在接続されているユーザを識別し、単一のユーザまたはすべてのユーザにメッセージを送信することができます。詳細については、第 7 章「ユーザの管理」を参照してください。

NTP

NTP は、分散している一連のタイム サーバおよびクライアント間で、計時を同期させます。この同期によって、複数のネットワーク デバイスからシステム ログおよびその他の時刻特定イベントを受信したときに、イベントを相互に関連付けることができます。

NTP の詳細については、第 8 章「NTP の設定」を参照してください。

ローカル SPAN および ERSPAN

イーサネット スイッチド ポート アナライザ（SPAN）を使用すると、デバイスの入出力トラフィックをモニタしたり、送信元ポートから宛先ポートへのパケットを複製できます。

SPAN の設定については、第 9 章「ローカル SPAN および ERSPAN の設定」を参照してください。

Cisco ネットワーク解析モジュール（NAM）を使用して ERSPAN データソースをモニタし、アプリケーション パフォーマンス、トラフィック、およびパケット ヘッダーを分析することもできます。

NAM を使用して Cisco Nexus 1000V ERSPAN データソースをモニタする手順については、『*Cisco Nexus 1010 Network Analysis Module Installation and Configuration Note, 5.1*』を参照してください。

SNMP

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージ フォーマットを提供するアプリケーション層プロトコルです。SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。

SNMP の詳細については、第 10 章「SNMP の設定」を参照してください。

NetFlow

NetFlow を使用すると、送信元、宛先、タイミング、アプリケーション情報に基づいて IP トラフィックの特徴を明確にすることで、仮想スイッチを通過するトラフィックを視覚化することができます。この情報は、ネットワークの可用性とパフォーマンスの評価、法的な要求事項の満足（コンプライアンス）、トラブルシューティングに役立てることができます。

詳細については、第 11 章「NetFlow の設定」を参照してください。

Cisco ネットワーク解析モジュール（NAM）を使用して、NetFlow データソースをモニタすることもできます。詳細については、『*Cisco Nexus 1010 Network Analysis Module Installation and Configuration Note, 5.1*』を参照してください。

システム メッセージ

システム メッセージ ロギングを使用して宛先を制御し、システム プロセスが生成するメッセージの重大度をフィルタリングできます。ターミナル セッション、ログ ファイル、およびリモート システム上の Syslog サーバへのロギングを設定できます。

システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

システム メッセージの設定の詳細については、第 12 章「システム メッセージ ロギングの設定」を参照してください。

iSCSI マルチパス

iSCSI マルチパスとは、サーバとそのストレージ デバイスとの間に複数のルートをセットアップする機能です。常時接続の維持と、トラフィック負荷の分散が可能になります。

詳細については、「iSCSI マルチパスの設定」（P.13-1）を参照してください。

トラブルシューティング

ping と traceroute は、利用可能なトラブルシューティング ツールです。

詳細については、『*Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

CHAPTER 2

CDP の設定

この章では、Cisco Discovery Protocol（CDP）の設定方法について、次の内容を説明します。

- 「CDP の概要」（P.2-1）
- 「注意事項および制約事項」（P.2-2）
- 「デフォルト」（P.2-2）
- 「CDP の設定」（P.2-3）
- 「CDP のモニタリング」（P.2-10）
- 「CDP 設定の確認」（P.2-10）
- 「CDP のコンフィギュレーション例」（P.2-14）
- 「その他の関連資料」（P.2-14）

CDP の概要

Cisco Discovery Protocol（CDP）は、データ リンク層の上で動作し、接続されているすべてのシスコ デバイスに情報をアドバタイズし、接続されているシスコ デバイスに関する情報を検出および表示するために使用されます。CDP は、シスコ製のすべての機器で動作します。

CDP はネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP は、データ リンク層でのみ実行されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムが相互について認識できます。

CDP が設定された各デバイスは、マルチキャスト アドレスに定期的にアドバタイズメントを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズメントには保持時間情報も含まれます。保持時間は、受信デバイスが CDP 情報を破棄するまでに保持する時間の長さを表します。アドバタイズメントまたはリフレッシュ タイマーおよびホールド タイマーを設定できます。

CDP Version 2（CDPv2）では、接続デバイス間でネイティブ VLAN ID またはポート デュプレックス ステートが一致していないインスタンスを追跡できます。

CDP では、次の Type-Length-Value（TLV）フィールドがアドバタイズされます。

- デバイス ID
- アドレス
- ポート ID
- 機能
- バージョン

- プラットフォーム
- ネイティブ VLAN
- 全二重/半二重
- MTU
- SysName
- SysObjectID
- 管理アドレス
- 物理ロケーション

すべての CDP パケットに VLAN ID が含まれます。CDP パケットはタグなしです。したがって、パケットはネイティブ/アクセス VLAN 上で伝送され、その VLAN の情報もパケットに追加されます。

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。

ハイ アベイラビリティ

CDP ではステートレス リスタートがサポートされています。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

注意事項および制約事項

CDP 設定時の注意事項と制約事項は次のとおりです。

- 接続数が 256 のハブにポートを接続した場合、CDP はポートあたり最大 256 のネイバーを検出できます。
- インターフェイス上で CDP を設定するには、CDP がグローバルにイネーブルになっている必要があります。CDP は、デフォルトでグローバルにイネーブルになっていますが、「CDP のグローバルなイネーブルまたはディセーブル」（P.2-3）の手順を使用してディセーブルにできます。
- CDP を設定できるのは、物理インターフェイスおよびポート チャネル上に限られます。

デフォルト

表 2-1 に CDP のデフォルト設定を示します。

表 2-1　CDP のデフォルト

パラメータ	デフォルト
CDP	グローバルおよびすべてのインターフェイスでイネーブル
CDP バージョン	バージョン 2
CDP デバイス ID	システム名
CDP タイマー	60 秒
CDP ホールド タイマー	180 秒

CDP の設定

ここでは、次の内容について説明します。

- 「CDP グローバル コンフィギュレーション」（P.2-3）
- 「インターフェイス上での CDP のイネーブル化」（P.2-7）
- 「インターフェイス上での CDP のディセーブル化」（P.2-8）

CDP グローバル コンフィギュレーション

ここでは、次の内容について説明します。

- 「CDP のグローバルなイネーブルまたはディセーブル」（P.2-3）
- 「CDP バージョンのアドバタイズ」（P.2-4）
- 「CDP オプションの設定」（P.2-5）

CDP のグローバルなイネーブルまたはディセーブル

ここでは、CDP をグローバルにイネーブルまたはディセーブルにする手順を説明します。デフォルトでは CDP がグローバルにイネーブルになっていますが、ディセーブルにされたとしても、ここで説明する手順を実行すれば再度イネーブル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。
- インターフェイス上で CDP を設定するには、CDP がグローバルにイネーブルになっている必要があります。
- CDP 機能をグローバルにディセーブルにすると、すべての CDP コンフィギュレーションが削除されます。

手順の概要

1. **config t**
2. **[no] cdp enable**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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。

	コマンド	目的

ステップ 2	**[no] cdp enable**
	
	Example:
	`n1000v(config)# cdp enable`
	
	Example:
	`n1000v(config)# no cdp enable`
		CDP 機能をグローバルにイネーブルまたはディセーブルにします。

CDP バージョンのアドバタイズ

ここでは、アドバタイズするデバイスの CDP バージョンを指定する手順を説明します。

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。

- デバイス上で現在サポートされている CDP のバージョンを知っておく必要があります。
- 一度に 1 つの CDP バージョン（バージョン 1 またはバージョン 2）だけがスイッチ上のすべてのアップリンクおよびポート チャネルに対してアドバタイズされます。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. **cdp advertise {v1 | v2}**
3. （任意）**show cdp global**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**cdp advertise {v1 | v2}**
	
	Example 1:
	`n1000v(config)# cdp advertise v1`
	`n1000v(config)#`
	
	Example 2:
	`n1000v(config)# cdp advertise v2`
	`n1000v(config)#`
		アドバタイズする CDP バージョンを割り当てます。
		• CDP バージョン 1
		• CDP バージョン 2

ステップ 3	**show cdp global**	（任意）CDP コンフィギュレーションを表示します。他のデバイスにアドバタイズまたは送信されている CDP バージョンも表示されます。

コマンド	目的
Example 1: n1000v(config)# **show cdp global** Global CDP information: CDP enabled globally Sending CDP packets every 60 seconds Sending a holdtime value of 180 seconds **Sending CDPv2 advertisements is disabled** Sending DeviceID TLV in Default Format **Example 2:** n1000v(config)# **show cdp global** Global CDP information: CDP enabled globally Sending CDP packets every 60 seconds Sending a holdtime value of 180 seconds Sending CDPv2 advertisements is enabled Sending DeviceID TLV in Default Format	
ステップ 4　**copy running-config startup-config** **Example:** n1000v(config)# 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。

CDP オプションの設定

ここでは、CDP に関する次の設定を行う手順を説明します。

- 使用するデバイス ID 形式

（注）　サポートされるデバイス ID 形式は **system-name** だけです。

- ネイバー情報の最大保持時間
- 送信アドバタイズメントのリフレッシュ タイム

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。

- アップストリーム cat6k スイッチからの出力を表示するには、**show cdp neighbor** コマンドを使用すること。
- 保持時間を設定する場合、CDP がネイバー情報を保持する時間がわかっていること。
- CDP タイマーを設定する場合は、CDP がアドバタイズする頻度がわかっていること。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. （任意）**cdp format device-id system-name**
3. **show cdp neighbors** from the upstream device
4. **show cdp neighbors** from your device

5. （任意）**cdp timer** *seconds*
6. （任意）**cdp holdtime** *seconds*
7. （任意）**show cdp global**
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**cdp format device-id system-name** Example: n1000v(config)# **cdp format device-id system-name** n1000v(config)#	（任意）デバイス ID 形式としてシステム名を使用することを指定します。
ステップ 3	**show cdp neighbors**	アップストリーム デバイスから自デバイスを表示します。

Example:

```
swordfish-6k-2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

02000c000000     Gig 1/16          14             S       Soft Swit Eth 2/4
02000c000000     Gig 1/17          14             S       Soft Swit Eth 2/5
02000c000000     Gig 1/14          14             S       Soft Swit Eth 2/2
02000c000000     Gig 1/15          14             S       Soft Swit Eth 2/3
02000c000000     Gig 1/18          13             S       Soft Swit
```

ステップ 4	**show cdp neighbors**	自デバイスからアップストリーム デバイスを表示します。

```
n1000v(config)# 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         Eth2/2          169     R S I    WS-C6503-E    Gig1/14
swordfish-6k-2         Eth2/3          139     R S I    WS-C6503-E    Gig1/15
swordfish-6k-2         Eth2/4          135     R S I    WS-C6503-E    Gig1/16
swordfish-6k-2         Eth2/5          177     R S I    WS-C6503-E    Gig1/17
swordfish-6k-2         Eth2/6          141     R S I    WS-C6503-E    Gig1/18
```

ステップ 5	**cdp holdtime** *seconds* **Example:** n1000v(config)# cdp holdtime 10	（任意）CDP がネイバー情報を破棄するまでにそれを保持する最大時間を設定します。 • 範囲は 10 ～ 255 秒です。 • デフォルト値は 180 秒です。

	コマンド	目的
ステップ 6	**cdp timer** *seconds* **Example:** `n1000v(config)# cdp timer 5`	（任意）CDP がネイバーにアドバタイズメントを送信するリフレッシュ タイムを設定します。 • 範囲は 5 ～ 254 秒です。 • デフォルトは 60 秒です。
ステップ 7	**show cdp global**	グローバル CDP コンフィギュレーションを表示します。

	Example:
	`n1000v(config)# show cdp global`
	`Global CDP information:`
	`  CDP enabled globally`
	`  Sending CDP packets every 5 seconds`
	`  Sending a holdtime value of 10 seconds`
	`  Sending CDPv2 advertisements is disabled`
	`  Sending DeviceID TLV in Mac Address Format`	

ステップ 8	**copy running-config startup-config** **Example:** `n1000v(config-if)# 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。

CDP インターフェイス コンフィギュレーション

ここでは、次の手順について説明します。

- 「インターフェイス上での CDP のイネーブル化」（P.2-7）
- 「インターフェイス上での CDP のディセーブル化」（P.2-8）

インターフェイス上での CDP のイネーブル化

特定のインターフェイス上で CDP をイネーブルにするには、ここに示す手順を実行します。デフォルトでは CDP がグローバルにイネーブルになっていますが、ディセーブルにされたとしても、ここで説明する手順を実行すれば再度イネーブル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。

- CDP 機能がグローバルにイネーブルになっていること。CDP はデフォルトでグローバルにイネーブルになっていますが、再度イネーブルにするには「CDP のグローバルなイネーブルまたはディセーブル」（P.2-3）の手順を使用します。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. **interface** *interface-type number*
3. **no cdp enable**
4. **cdp enable**

5. **show cdp interface** *interface-type number*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**interface** *interface-type number* **Example:** n1000v(config)# interface port-channel 2 n1000v(config-if)#	CLI を特定のインターフェイスに対するインターフェイス コンフィギュレーション モードにします。
ステップ 3	**no cdp enable** **Example:** n1000v(config-if)# no cdp enable	このインターフェイスで CDP をディセーブルにします。
ステップ 4	**cdp enable** **Example:** n1000v(config-if)# cdp enable	このインターフェイスで CDP をイネーブルにします。
ステップ 5	**show cdp interface** *interface-type number* **Example:** n1000v(config-if)# show cdp interface mgmt0 mgmt0 is up CDP disabled on interface Sending CDP packets every 60 seconds Holdtime is 180 seconds	（任意）指定したインターフェイスの CDP 情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v(config-if)# 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。

ポート チャネル 2 で CDP をイネーブルにする例を示します。

```
n1000v# config t
n1000v(config)# interface port-channel 2
n1000v(config-if)# no cdp enable
n1000v(config-if)# cdp enable
n1000v(config-if)# copy running-config startup-config
```

インターフェイス上での CDP のディセーブル化

特定のインターフェイス上で CDP をディセーブルにするには、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。

- CDP がデバイス上で現在イネーブルになっていること。

（注）　CDP がデバイス上でディセーブルになっている場合、すべてのインターフェイスでもディセーブルになっています。

- CDP が、設定対象のインターフェイスで現在イネーブルになっていること。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. **interface** *interface-type* `number`
3. **no cdp enable**
4. （任意）**show cdp interface** *interface-type* `number`
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**interface** *interface-type number*
	
	Example:
	`n1000v(config)# interface mgmt0`
	`n1000v(config-if)#`
		指定したインターフェイスに対する CLI インターフェイス コンフィギュレーション モードにします。

ステップ 3	**no cdp enable** **Example:** `n1000v(config-if)# no cdp enable`	指定したインターフェイス上で CDP をディセーブルにします。
ステップ 4	**show cdp interface** *interface-type number* **Example:** `n1000v(config-if)# show cdp interface mgmt0`	（任意）インターフェイスの CDP 情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# 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。

次に、mgmt0 上で CDP をディセーブルにする例を示します。

```
n1000v# config t
n1000v(config)# interface mgmt0
n1000v(config-if)# no cdp enable
n1000v(config-if)# show cdp interface mgmt0
mgmt0 is up
    CDP disabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
n1000v(config-if)# copy running-config startup-config
```

CDP のモニタリング

CDP トラフィックをモニタするには、次のコマンドを使用します。

コマンド	目的
show cdp traffic interface *interface-type slot/port*	インターフェイスの CDP トラフィック統計を表示します。 例 2-7（P.2-14）を参照してください。

CDP 統計情報の消去

CDP 統計情報を消去するには、次のいずれかのコマンドを使用します。

コマンド	目的
clear cdp counters	すべてのインターフェイスの CDP 統計情報を消去します。
clear cdp counters interface *number*	指定したインターフェイスの CDP 統計情報を消去します。
clear cdp table	1 つまたはすべてのインターフェイスの CDP キャッシュを消去します。

CDP 設定の確認

CDP コンフィギュレーションを確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show cdp all	CDP がイネーブルになっているすべてのインターフェイスを表示します。 例 2-1（P.2-11）を参照してください。
show cdp entry {**all** | **name** *entry-name*}	CDP データベース エントリを表示します。 例 2-2（P.2-11）を参照してください。

コマンド	目的
show cdp global	CDP グローバル パラメータを表示します。 例 2-4（P.2-13）を参照してください。
show cdp interface *interface-type slot/port*	CDP インターフェイスのステータスを表示します。 例 2-5（P.2-13）を参照してください。
show cdp neighbors {**detail** | **interface** *interface-type slot/port*}	CDP ネイバーのステータスを表示します。 例 2-6（P.2-13）を参照してください。

例 2-1　show cdp all

```
n1000v# show cdp all
Ethernet2/2 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/3 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/4 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/5 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/6 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
mgmt0 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

例 2-2　show cdp entry *name*

```
n1000v# show cdp entry name swordfish-6k-2
----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.30.2
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/2, Port ID (outgoing port): GigabitEthernet1/14
Holdtime: 152 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team
```

例 2-3　show cdp entry all

```
n1000v# show cdp entry all
----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.30.2
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/2, Port ID (outgoing port): GigabitEthernet1/14
Holdtime: 140 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.30.2
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/3, Port ID (outgoing port): GigabitEthernet1/15
Holdtime: 129 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 7.7.8.1
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/4, Port ID (outgoing port): GigabitEthernet1/16
Holdtime: 154 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 7.7.8.1
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
```

```
Interface: Ethernet2/5, Port ID (outgoing port): GigabitEthernet1/17
Holdtime: 156 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

---------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.15.229
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/6, Port ID (outgoing port): GigabitEthernet1/18
Holdtime: 171 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1
```

例 2-4　show cdp global

```
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is disabled
    Sending DeviceID TLV in Default Format
```

例 2-5　show cdp interface

```
n1000v(config)# show cdp interface ethernet 2/3
Ethernet2/3 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

例 2-6　show cdp neighbors interface

```
n1000v(config)# show cdp neighbors interface ethernet 2/3
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         Eth2/3          173     R S I    WS-C6503-E    Gig1/15
```

例 2-7　show cdp traffic interface

```
n1000v(config)# show cdp traffic interface ethernet 2/3
----------------------------------------
Traffic statistics for Ethernet2/3
Input Statistics:
    Total Packets: 98
    Valid CDP Packets: 49
        CDP v1 Packets: 49
        CDP v2 Packets: 0
    Invalid CDP Packets: 49
        Unsupported Version: 49
        Checksum Errors: 0
        Malformed Packets: 0

Output Statistics:
    Total Packets: 47
        CDP v1 Packets: 47
        CDP v2 Packets: 0
    Send Errors: 0
```

CDP のコンフィギュレーション例

CDP 機能をイネーブルにして、リフレッシュ タイマーおよびホールド タイマーを設定する例を示します。

```
config t
cdp enable
cdp timer 50
cdp holdtime 100
```

その他の関連資料

ここでは、CDP に関する次の追加情報について説明します。

- 「関連資料」（P.2-14）
- 「標準」（P.2-15）

関連資料

関連項目	参照先
VLAN	*『Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)』*
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	*『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

CDP 機能の履歴

ここでは、CDP 機能のリリース履歴を示します。

機能名	リリース	機能情報
CDP	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 3

ドメインの設定

この章では、Cisco Nexus 1000V ドメインの設定方法について説明します。ドメインを設定するには、ドメインの作成、VLAN の割り当て、レイヤ 3 コントロールの設定などを行います。

この章では、次の事項について説明します。

- 「ドメインについて」（P.3-1）
- 「注意事項および制約事項」（P.3-2）
- 「デフォルト設定」（P.3-3）
- 「ドメインの設定」（P.3-3）
- 「VSM ドメイン機能の履歴」（P.3-16）

ドメインについて

Cisco Nexus 1000V 用のドメイン名を作成し、通信および管理用の制御 VLAN とパケット VLAN を追加する必要があります。この処理は、Cisco Nexus 1000V のソフトウェアをインストールする際の初期セットアップの一部です。ドメインを後で作成する必要がある場合は、**setup** コマンドを使用するか、この章に記載されている手順を実行します。

レイヤ 3 コントロールについて

レイヤ 3 制御、つまり IP 接続は、制御トラフィックおよびパケット トラフィック用の VSM と VEM 間でサポートされています。レイヤ 3 制御を行うと、VSM はレイヤ 3 経由でアクセス可能になり、別のレイヤ 2 ネットワークに存在するホストを制御できるようになります。ただし、その場合も、同じ VSM によって制御されるホストはすべて同じレイヤ 2 ネットワーク内に存在する必要があります。VSM は、自身が制御するレイヤ 2 ネットワークの外部にあるホストを制御することはできないので、VSM が存在するホストの制御は別の VSM が行う必要があります。

レイヤ 3 制御を実装するには、次の設定作業を行う必要があります。

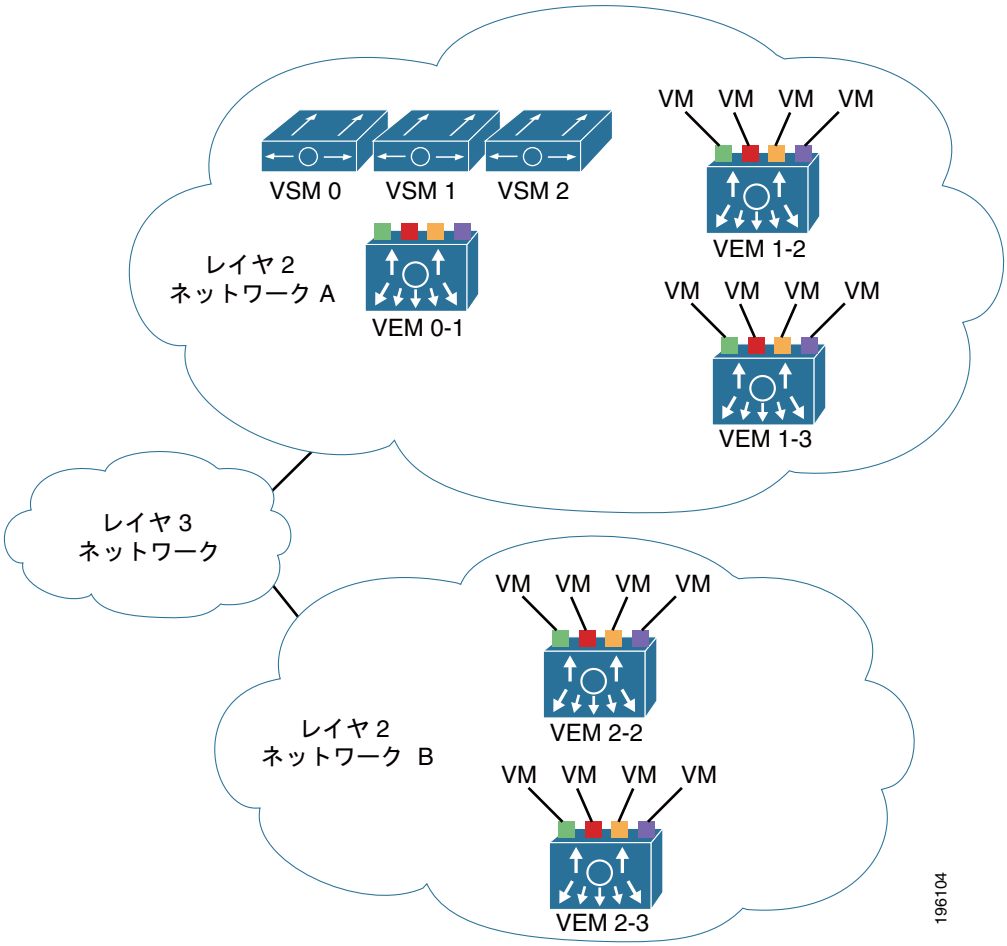
- VSM ドメイン トランスポート モードをレイヤ 3 として設定します。

  詳細については、「レイヤ 3 トランスポートへの変更」（P.3-6）の手順を参照してください。
- 「レイヤ 3 コントロール用のポート プロファイルの作成」（P.3-10）の手順を参照してポート プロファイルを設定します。
- VMware カーネル NIC インターフェイスを各ホスト上に作成し、レイヤ 3 制御ポート プロファイルを割り当てます。詳細については、VMware のマニュアルを参照してください。

図 3-1 に、レイヤ 3 コントロールの例を示します。

- VSM0 は VEM_0_1 を制御します。
- VEM_0_1 はホスト VSM1 および VSM2 を制御します。
- VSM1 および VSM2 は他のレイヤ 2 ネットワーク内の VEM を制御します。

図 3-1　　レイヤ 3 制御 IP 接続の例



注意事項および制約事項

VSM ドメインの設定時の注意事項および制約事項は、次のとおりです。

- VSM と VEM の間のレイヤ 3 の通信には UDP ポート 4785 が必要です。ネットワークにファイアウォールがあり、レイヤ 3 制御が設定されている場合は、UDP ポート 4785 がアップストリーム スイッチまたはファイアウォール デバイスで開いていることを確認します。詳細については、アップストリーム スイッチまたはファイアウォール デバイスのマニュアルを参照してください。
- レイヤ 2 ネットワークでは、トランスポート モードをレイヤ 2 とレイヤ 3 の間で切り替えることができますが、切り替えると、少しの間モジュールが使用できなくなる場合があります。
- 機能属性（レイヤ 3 コントロール）をポート プロファイルから継承することはできません。
- ホストごとに異なる VLAN をレイヤ 3 コントロールに使用することができます。

- レイヤ 3 コントロールに使用されるポート プロファイルは、アクセス ポート プロファイルであることが必要です。トランク ポート プロファイルであってはなりません。
- VMware カーネル NIC をレイヤ 3 コントロールに使用する場合は、他の目的には使用しないことを推奨します。たとえば、レイヤ 3 コントロール用の VMware カーネル NIC を VMotion や NFS マウントにも使用することは避けてください。
- コントロール VLAN、パケット VLAN、および管理 VLAN は、プライベート VLAN としてではなく通常の VLAN として設定する必要があります。

デフォルト設定

表 3-1 に、ドメイン コンフィギュレーション内のデフォルト設定を示します。

表 3-1　ドメインのデフォルト

パラメータ	デフォルト
制御 VLAN（svs-domain）	VLAN 1
パケット VLAN（svs-domain）	VLAN 1
VMware ポート グループ名（port-profile）	ポート プロファイルの名前
SVS モード（svs-domain）	レイヤ 2
スイッチポート モード（port-profile）	アクセス
ステート（port-profile）	ディセーブル
ステート（VLAN）	アクティブ
シャット ステート（VLAN）	シャットダウンなし

ドメインの設定

ここでは、次の手順について説明します。

- 「ドメインの作成」（P.3-4）
- 「レイヤ 3 トランスポートへの変更」（P.3-6）
- 「レイヤ 2 トランスポートへの変更」（P.3-8）
- 「レイヤ 3 コントロール用のポート プロファイルの作成」（P.3-10）
- 「制御 VLAN の作成」（P.3-13）
- 「パケット VLAN の作成」（P.3-14）

ドメインの作成

ここでは、VSM および VEM を特定する Cisco Nexus 1000V のドメイン名を作成してから通信および管理のための制御 VLAN とパケット VLAN を追加する手順を説明します。この処理は、Cisco Nexus 1000V のソフトウェアをインストールする際の初期セットアップの一部です。初期セットアップ後にドメインを作成する必要がある場合は、この手順を使用して作成できます。

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。

- ドメインは、2 つ以上の VSM が同じ制御 VLAN やパケット VLAN を共有している場合に、各 VSM がどの VEM を管理しているかを識別するのに役立ちます。
- EXEC モードで CLI にログインしていること。
- この Cisco Nexus 1000V インスタンスに対する一意のドメイン ID が必要です。
- 制御とパケットのトラフィックにどの VLAN を使用するかを指定する必要があります。
- 制御トラフィック用の VLAN とは別の VLAN をパケット トラフィックに使用することを推奨します。
- Cisco Nexus 1000V のインスタンスごとに（ドメインごとに）別の VLAN を使用することを推奨します。
- SVS ドメイン コンフィギュレーション モードの **svs mode** コマンドは使用されないため、このコマンドがコンフィギュレーションに影響することはありません。
- 別の VSM を追加した後のドメイン ID の変更については、『*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

手順の概要

1. **config t**
2. **svs-domain**
3. **domain id** *domain-id*
4. **control vlan** *vlan-id*
5. **packet vlan** *vlan-id*
6. **exit**
7. **show svs domain**
8. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**svs-domain** **Example:** n1000v(config)# svs-domain n1000v(config-svs-domain)#	SVS ドメイン 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	**domain id** *number* **Example:** n1000v(config-svs-domain)# domain id 100 n1000v(config-svs-domain)#	この Cisco Nexus 1000V インスタンスのドメイン ID を作成します。
ステップ 4	**control vlan** *number* **Example:** n1000v(config-svs-domain)# control vlan 190 n1000v(config-vlan)#	このドメインの制御 VLAN を割り当てます。
ステップ 5	**packet vlan** *number* **Example:** n1000v(config-vlan)# packet vlan 191 n1000v(config-vlan)#	このドメインのパケット VLAN を割り当てます。
ステップ 6	show svs domain **Example:** n1000v(config-vlan)# show svs domain	ドメイン コンフィギュレーションを表示します。
ステップ 7	**exit** **Example:** n1000v(config-vlan)# exit n1000v(config)#	CLI グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）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。

Example:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 100
n1000v(config-svs-domain)# control vlan 190
n1000v(config-svs-domain)# packet vlan 191
n1000v(config-vlan)# exit

n1000v (config)# show svs domain
SVS domain config:
  Domain id:    100
  Control vlan: 190
  Packet vlan:  191
```

```
  L2/L3 Aipc mode: L2
  L2/L3 Aipc interface: mgmt0
  Status: Config push to VC successful.

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

レイヤ 3 トランスポートへの変更

ここでは、VSM ドメインの制御/パケット トラフィックのトランスポート モードをレイヤ 2 からレイヤ 3 に変更する手順を説明します。

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。
- この手順では、制御 VLAN とパケット VLAN をディセーブルにする必要があります。レイヤ 3 コントロールに変更するには、あらかじめ制御 VLAN とパケット VLAN をディセーブルにする必要があります。
- レイヤ 3 インターフェイス（mgmt 0 または control 0）の設定および IP アドレスの割り当てが完了している必要があります。

  インターフェイスの設定については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

手順の概要

1. **show svs domain**
2. **config t**
3. **svs-domain**
4. **no control vlan**
5. **no packet vlan**
6. **show svs domain**
7. **svs mode L2 | svs mode L3 interface { mgmt0 | control0 }**
8. **show svs domain**
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**show svs domain**
	Example:
	`n1000v(config)# show svs domain`
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 100`
	`  Packet vlan:  101`
	`  L2/L3 Control mode: L2`
	`  L3 control interface:  NA`
	`  Status: Config push to VC successful.`
		既存のドメイン コンフィギュレーションを表示します。制御 VLAN とパケット VLAN の ID が表示されます。

ステップ 2	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 3	**svs-domain**
	Example:
	`n1000v(config)# svs-domain`
	`n1000v(config-svs-domain)#`
		CLI SVS ドメイン コンフィギュレーション モードを開始します。

ステップ 4	**no packet vlan**
	Example:
	`n1000v(config-svs-domain)# no packet vlan`
	`n1000v(config-svs-domain)#`
		パケット VLAN コンフィギュレーションを削除します。

ステップ 5	**no control vlan**
	Example:
	`n1000v(config-svs-domain)# no control vlan`
	`n1000v(config-svs-domain)#`
		制御 VLAN コンフィギュレーションを削除します。

ステップ 6	**show svs domain**
	Example:
	`n1000v(config)# show svs domain`
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 1`
	`  Packet vlan:  1`
	`  L2/L3 Control mode: L2`
	`  L2/L3 Control interface: NA`
	`  Status: Config push to VC successful.`
	`switch(config-svs-domain)#`
		既存のドメイン コンフィギュレーションを表示します。制御 VLAN とパケット VLAN のデフォルトの ID が表示されます。

ステップ 7	**svs mode L3 interface { mgmt0 | control0 }**
	Example:
	`n1000v(config-svs-domain)# svs mode l3 interface mgmt0`
	`n000v(config-svs-domain)#`
		VSM ドメインのレイヤ 3 トランスポート モードを設定します。
		レイヤ 3 トランスポートを設定する場合は、どのインターフェイスを使用するかを指定する必要があります。そのインターフェイスの IP アドレスが設定済みであることが必要です。
		この例では、management 0 インターフェイスを使用するようにレイヤ 3 トランスポートを設定する方法を示します。

	コマンド	目的

ステップ 8	**show svs domain**
	Example:
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 1`
	`  Packet vlan:  1`
	`  L2/L3 Control mode: L3`
	`  L3 control interface: mgmt0`
	`  Status: Config push to VC successful.`
	`n1000v(config-svs-domain)#`
		（任意）この VSM ドメインの新しいレイヤ 3 コントロール モード コンフィギュレーションを表示します。

ステップ 9	**copy running-config startup-config**
	Example:
	`n1000v(config-svs-domain)# copy running-config startup-config`
	`[##########################################] 100%`
	`n1000v(config-svs-domain)#`
		（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。

レイヤ 2 トランスポートへの変更

ここでは、VSM ドメインの制御/パケット トラフィックのトランスポート モードをレイヤ 2 に変更する手順を説明します。トランスポート モードはデフォルトでレイヤ 2 になっていますが、変更された場合も、この手順を使用すれば再びレイヤ 2 として設定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。
- この手順では、制御 VLAN とパケット VLAN を設定する必要があります。VSM ドメインの機能がレイヤ 3 コントロールである場合は、これらの VLAN の設定を行うことはできません。機能をレイヤ 3 コントロールに変更してから、制御 VLAN とパケット VLAN を設定します。

手順の概要

1. **show svs domain**
2. **config t**
3. **svs-domain**
4. **svs mode L2 | svs mode L3 interface { mgmt0 | control0 }**
5. **show svs domain**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**show svs domain**
	Example:
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 1`
	`  Packet vlan:  1`
	`  L2/L3 Control mode: L3`
	`  L3 control interface: mgmt0`
	`  Status: Config push to VC successful.`
	`n1000v(config-svs-domain)#`
		既存のドメイン コンフィギュレーションを表示します。制御 VLAN とパケット VLAN の ID や、レイヤ 3 インターフェイス コンフィギュレーションが表示されます。

ステップ 2	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 3	**svs-domain**
	Example:
	`n1000v(config)# svs-domain`
	`n1000v(config-svs-domain)#`
		CLI SVS ドメイン コンフィギュレーション モードを開始します。

ステップ 4	**svs mode L2**
	Example:
	`n1000v(config-svs-domain)# svs mode l2`
	`n000v(config-svs-domain)#`
		VSM ドメインのレイヤ 2 トランスポート モードを設定します。

ステップ 5	**control vlan** *vlanID* **Example:** `n1000v(config-svs-domain)# control vlan 100`	指定された VLAN ID をこの VSM ドメインの制御 VLAN として設定します。
ステップ 6	**packet vlan** *vlanID* **Example:** `n1000v(config-svs-domain)# packet vlan 101`	指定された VLAN ID をこの VSM ドメインのパケット VLAN として設定します。

ステップ 7	**show svs domain**
	Example:
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 100`
	`  Packet vlan:  101`
	`  L2/L3 Control mode: L2`
	`  L3 control interface: NA`
	`  Status: Config push to VC successful.`
	`n1000v(config-svs-domain)#`
		（任意）この VSM ドメインの新しいレイヤ 2 コントロール モード コンフィギュレーションを表示します。

ステップ 8	**copy running-config startup-config**
	Example:
	`n1000v(config-svs-domain)# copy running-config startup-config`
	`[##########################################] 100%`
	`n1000v(config-svs-domain)#`
		（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。

レイヤ 3 コントロール用のポート プロファイルの作成

ここでは、VSM と VEM の間の制御/パケット トラフィックを IP で伝送できるようにする手順を説明します。

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。
- VSM ドメインのトランスポート モードがレイヤ 3 として設定されている必要があります。詳細については、「レイヤ 2 トランスポートへの変更」（P.3-8）の手順を参照してください。
- すべての VEM が同じレイヤ 2 ドメインに属している必要があります。
- ホストを Cisco Nexus 1000V DVS に追加するときに、VEM VM カーネル NIC がこのレイヤ 3 コントロール ポート プロファイルに接続する必要があります。
- このレイヤ 3 コントロール ポート プロファイルに割り当て可能な VM カーネル NIC は、1 つのホストにつき 1 つだけです。
  - 複数の VMware カーネル NIC が同じホストに割り当てられている場合は、最後に割り当てられたものが有効になります。
  - 2 つの VMware カーネル NIC が同じホストに割り当てられている場合に、2 番目に割り当てられたものを削除しても、最初に割り当てられたものが VEM によって使用されることはありません。代わりに、VMware カーネル NIC を両方とも削除してから 1 つだけをもう一度割り当てる必要があります。
- このレイヤ 3 コントロール ポート プロファイルに追加する VLAN の VLAN ID がわかっている必要があります。
  - その VLAN は Cisco Nexus 1000V 上であらかじめ作成しておく必要があります。
  - このレイヤ 3 制御ポート プロファイルに割り当てられる VLAN は、システム VLAN でなければなりません。
  - いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN がすでに含まれている必要があります。
- ポート プロファイルは、アクセス ポート プロファイルであることが必要です。トランク ポート プロファイルであってはなりません。ここで説明する手順の中で、ポート プロファイルをアクセス ポート プロファイルとして設定します。
- 複数のポート プロファイルを **capability L3 control** として設定することができます。
- ホストごとに異なる VLAN をレイヤ 3 コントロールに使用することができます。

手順の概要

1. **config t**
2. **port-profile** *name*
3. **capability l3control**
4. **vmware port-group** [*name*]
5. **switchport mode access**
6. **switchport access vlan** *vlanID*
7. **no shutdown**

8. **system vlan** *vlanID*
9. **state enabled**
10. （任意）**show port-profile** *name*
11. （任意）copy running-config startup-config

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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*
	Example:
	`n1000v(config)# port-profile l3control-150`
	`n1000v(config-port-prof)#`
		ポート プロファイルを作成し、このポート 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。
		ポート プロファイルには最大 80 文字の名前を設定できます。ポート プロファイル名は、Cisco Nexus 1000V 上の各ポート プロファイルに対して一意である必要があります。

ステップ 3	**capability l3control**
	Example:
	`n1000v(config-port-prof)# capability l3control`
	`n1000v(config-port-prof)#`
		ポートを IP 接続に使用できるようになります。
		vCenter Server では、このレイヤ 3 コントロール ポート プロファイルが選択されて VM カーネル NIC の物理ポートに割り当てられている必要があります。

ステップ 4	**vmware port-group [***name***]**
	Example:
	`n1000v(config-port-prof)# vmware port-group`
	`n1000v(config-port-prof)#`
		ポート プロファイルを VMware ポート グループとして指定します。
		ポート プロファイルは、同じ名前の VMware ポート グループにマッピングされます。vCenter Server 接続が確立すると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。
		name：ポート グループ名。名前を指定しない場合は、ポート プロファイル名がポート グループ名となります。ポート プロファイルを別のポート グループ名にマッピングする場合は、別の名前を使用してください。

ステップ 5	**switchport mode access**]
	Example:
	`n1000v(config-port-prof)# switchport mode access`
	`n1000v(config-port-prof)#`
		インターフェイスがスイッチ アクセス ポート（デフォルト）であることを指定します。

ステップ 6	**switchport access vlan** *vlanID*
	Example:
	`n1000v(config-port-prof)# switchport access vlan 150`
	`n1000v(config-port-prof)#`
		このレイヤ 3 コントロール ポート プロファイルのアクセス ポートにシステム VLAN ID を割り当てます。

	コマンド	目的

ステップ 7	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		管理上の目的でプロファイル内のすべてのポートをイネーブルにします。

ステップ 8	**system vlan** *vlanID*
	
	Example:
	`n1000v(config-port-prof)# system vlan 150`
	`n1000v(config-port-prof)#`
		このレイヤ 3 コントロール ポート プロファイルにシステム VLAN を追加します。
		
		これで、ホストが初めて追加されたときや後で再起動されるときに、VEM が確実に VSM に到達できるようになります。いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN が含まれている必要があります。

ステップ 9	**state enabled**
	
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		レイヤ 3 コントロール ポート プロファイルをイネーブルにします。
		
		このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。

ステップ 10	**show port-profile name** *name*
	
	Example:
	`n1000v(config-port-prof)# show port-profile name l3control-150`
	`port-profile l3control-150`
	`  description:`
	`  type: vethernet`
	`  status: enabled`
	`  capability l3control: yes`
	`  pinning control-vlan: 8`
	`  pinning packet-vlan: 8`
	`  system vlans: 150`
	`  port-group: l3control-150`
	`  max ports: 32`
	`  inherit:`
	`  config attributes:`
	`  switchport mode access`
	`  switchport access vlan 150`
	`  no shutdown`
	`  evaluated config attributes:`
	`  switchport mode access`
	`  switchport access vlan 150`
	`  no shutdown`
	`  assigned interfaces:`
	
	`n1000v(config-port-prof)#`
		（任意）ポート プロファイルの現在のコンフィギュレーションを表示します。

ステップ 11	**copy running-config startup-config** **Example:** `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。

制御 VLAN の作成

ドメインに制御 VLAN を追加するには、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。
- レイヤ 3 コントロールが VSM 上で設定されている場合は、制御 VLAN を作成することはできません。まずレイヤ 3 制御をディセーブルにする必要があります。
- 必要な Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）を設定しイネーブルにしてあること（『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照）。SVI は VLAN インターフェイスとも呼ばれ、複数の VLAN 間の通信を可能にします。
- VLAN が番号付けされる方法について知っていること。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 Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*』。
- 新たに作成した VLAN は、レイヤ 2 ポートを割り当てるまで使用されないままになります。

手順の概要

1. **config t**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **state** *vlan-state*
5. **exit**
6. **show vlan id** *vlan-id*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**vlan** *30*
	
	Example:
	`n1000v(config)# vlan 30`
	`n1000v(config-vlan)#`
		制御トラフィック用の VLAN ID 30 を作成し、CLI VLAN コンフィギュレーション モードにします。
		（注） 内部的に割り当てられた VLAN に割り当て済みの VLAN ID を入力した場合、エラー メッセージが返されます。

ステップ 3	**name** *cp_control*
	
	Example:
	`n1000v(config-vlan)# name cp_control`
	`n1000v(config-vlan)#`
		説明用の名前 cp_control をこの VLAN に追加します。

	コマンド	目的
ステップ 4	**state** *active* **Example:** n1000v(config-vlan)# state active n1000v(config-vlan)#	VLAN の動作状態をアクティブに変更します。
ステップ 5	**show vlan id** *30* **Example:** n1000v(config-vlan)# show vlan id 30	VLAN ID 30 のコンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v(config-vlan)# copy running-config startup-config	（任意）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。

```
Example:
n1000v# config t
n1000v(config)# vlan 30
n1000v(config-vlan)# name cp_control
n1000v(config-vlan)# state active
n1000v(config)# show vlan id 30

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
30   cp_control                       active

VLAN Type MTU
---- -----
5    enet 1500

Remote SPAN VLAN
----------------
Disabled

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

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

パケット VLAN の作成

ドメインにパケット VLAN を追加するには、次の手順を実行します。

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。
- 『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』に従って、必要なスイッチ仮想インターフェイス（SVI）を設定しイネーブルにしてあること。SVI は VLAN インターフェイスとも呼ばれ、複数の VLAN 間の通信を可能にします。

- VLAN が番号付けされる方法について知っていること。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 Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*』。
- 新たに作成した VLAN は、レイヤ 2 ポートを割り当てるまで使用されないままになります。

手順の概要

1. **config t**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **state** *vlan-state*
5. **exit**
6. **show vlan id** *vlan-id*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**vlan** *31*
	
	Example:
	`n1000v(config)# vlan 31`
	`n1000v(config-vlan)#`
		パケット トラフィック用の VLAN ID 31 を作成し、CLI VLAN コンフィギュレーション モードにします。
		（注） 内部的に割り当てられた VLAN に割り当て済みの VLAN ID を入力した場合、エラー メッセージが返されます。

ステップ 3	**name** *cp_packet*
	
	Example:
	`n1000v(config-vlan)# name cp_packet`
	`n1000v(config-vlan)#`
		説明用の名前 cp_packet をこの VLAN に追加します。

ステップ 4	**state** *active*
	
	Example:
	`n1000v(config-vlan)# state active`
	`n1000v(config-vlan)#`
		VLAN の動作状態をアクティブに変更します。

ステップ 5	**show vlan id** *31* **Example:** `n1000v(config-vlan)# show vlan id 30`	VLAN ID 31 のコンフィギュレーションを表示します。

	コマンド	目的
ステップ 6	**exit** **Example:** n1000v(config-vlan)# exit n1000v(config)#	CLI グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）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。

```
Example:
n1000v# config t
n1000v(config)# vlan 31
n1000v(config-vlan)# name cp_packet
n1000v(config-vlan)# state active
n1000v(config-vlan)# exit
n1000v(config)# show vlan id 31

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
31   cp_packet                        active

VLAN Type MTU
---- -----
5    enet 1500

Remote SPAN VLAN
----------------
Disabled

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

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

VSM ドメイン機能の履歴

ここでは、VSM ドメイン機能のリリース履歴を示します。

機能名	リリース	機能情報
レイヤ 3 コントロール	4.0(4)SV1(2)	次の情報が追加されました。 • 「レイヤ 3 コントロールについて」（P.3-1） • 「注意事項および制約事項」（P.3-2） • 「レイヤ 2 トランスポートへの変更」（P.3-8） • 「レイヤ 3 トランスポートへの変更」（P.3-6） • 「レイヤ 3 コントロール用のポート プロファイルの作成」（P.3-10）
VSM ドメイン	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 4

サーバ接続の管理

この章では、接続を確立してサーバに接続する方法、サーバから切断する方法、およびサーバ接続を表示する方法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。

- 「サーバ接続について」（P.4-1）
- 「注意事項および制約事項」（P.4-2）
- 「vCenter Server への接続」（P.4-2）
- 「vCenter Server からの切断」（P.4-4）
- 「vCenter Server からの DVS の削除」（P.4-5）
- 「VSM が接続されていない場合の vCenter Server からの DVS の削除」（P.4-5）
- 「ホスト マッピングの設定」（P.4-7）
- 「接続の確認」（P.4-10）
- 「ドメインの確認」（P.4-11）
- 「設定の確認」（P.4-11）
- 「モジュール情報の確認」（P.4-14）
- 「サーバ接続機能の履歴」（P.4-16）

サーバ接続について

vCenter Server または ESX サーバに接続するには、初めに Cisco Nexus 1000V で接続を定義する必要があります。この定義には、次の項目が含まれます。

- 接続名
- 使用するプロトコル
- サーバの IP アドレス
- サーバの DNS 名
- データセンター名

vCenter Server との通信はすべて、TLS プロトコルによってセキュリティが維持されます。

注意事項および制約事項

サーバ接続には次の注意事項と制約事項があります。

- 1 つの VSM は一度に 1 つの vCenter Server にのみ接続できます。1 つの VSM は同時に複数の vCenter Server には接続できません。

vCenter Server への接続

この手順を使用して、接続を設定して、vCenter Server または ESX サーバに接続します。

はじめる前に

- EXEC モードで CLI にログインしていること。
- データセンターの名前がわかっている。
- vCenter Server 管理ステーションをインストールして実行します。
- vCenter Server の IP アドレスまたはホスト名がわかっている必要があります。
- ESX サーバをインストールして実行します。
- 管理ポートを設定します。
- Cisco Nexus 1000V から vCenter Server にアクセスできるようにします。
- Cisco Nexus 1000V アプライアンスをインストールします。
- ホスト名を使用して接続を設定している場合は、DNS を設定しておきます。
- 拡張ファイルが vCenter Server に登録済みであることが必要です。この拡張ファイルには、VSM 用の拡張キーとパブリック証明書が格納されています。これらは、vCenter Server が VSM から受信した要求の真正性を検証するために使用されます。拡張ファイルの追加および登録の手順については、『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

手順の概要

1. **config t**
2. **svs connection** *name*
3. **protocol vmware-vim**
4. **remote {ip address** *address A.B.C.D* **| hostname** *name***}**
5. **vmware dvs datacenter-name** *name*
6. **connect**

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	Example:
	`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	**svs connection** *name*
	
	Example:
	`n1000v (config#) svs connection VC`
	`n1000v(config-svs-conn#)`
		Cisco Nexus 1000V と特定の ESX サーバまたは vCenter Server 間にこの接続を追加するための、接続コンフィギュレーション モードに切り替えます。名前を使用して、複数接続情報をコンフィギュレーションに格納できます。

ステップ 3	**protocol vmware-vim** [http]
	
	Example:
	`n1000v(config-svs-conn#) protocol vmware-vim`
	`n1000v(config-svs-conn#)`
		この接続が VIM プロトコルを使用するように指定します。このコマンドはローカルに格納されます。
		• **http** : VIM プロトコルが HTTP で実行されるように指定します。デフォルトでは HTTP over SSL（HTTPS）を使用します。

ステップ 4	次のいずれかを実行します。 • IP アドレスを設定している場合は、ステップ 5 を参照してください。 • ホスト名を設定している場合は、ステップ 6 を参照してください。	

ステップ 5	**remote ip address** *ipaddress*
	
	Example:
	`n1000v(config-svs-conn#) remote ip address 192.168.0.1`
	`n1000v(config-svs-conn#)`
	
	ステップ 7 に進みます。
		この接続で使用する ESX サーバまたは vCenter Server の IP アドレスを指定します。このコマンドはローカルに格納されます。

ステップ 6	**remote hostname** *hostname*
	
	Example:
	`n1000v(config-svs-conn#) remote hostname vcMain`
	`n1000v(config-svs-conn#)`
		この接続で使用する ESX サーバまたは vCenter Server の DNS 名を指定します。このコマンドはローカルに格納されます。
		
		（注）　DNS はすでに設定されています。

ステップ 7	**vmware dvs datacenter-name** *name*
	
	Example:
	`n1000v(config-svs-conn#) vmware dvs datacenter-name Hamilton-DC`
	`n1000v(config-svs-conn#)`
		Cisco Nexus 1000V が Distributed Virtual Switch（DVS; 分散仮想スイッチ）として作成される vCenter Server のデータセンター名を指定します。接続前または接続後に、このコマンドを使用できます。データセンター名はローカルに格納されます。

ステップ 8	**connect** **Example:** `n1000v(config-svs-conn#) connect`	接続を開始します。この接続のユーザ名とパスワードが設定されていない場合は、ユーザ名とパスワード入力プロンプトが表示されます。 デフォルトは no connect です。一度にアクティブにできる接続は 1 つだけです。以前に定義した接続が確立している場合は、no connect を入力して以前の接続を終了するまでは、エラー メッセージが表示され、コマンドは拒否されます。

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
n1000v(config-svs-conn#) connect


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#
```

vCenter Server からの切断

この手順を使用して、vCenter Server 設定の修正後などに vCenter Server から切断します。

はじめる前に

- EXEC モードで Cisco Nexus 1000V にログインします。
- 「vCenter Server への接続」（P.4-2）の手順を参照して、Cisco Nexus 1000V 接続を設定します。
- Cisco Nexus 1000V が vCenter Server/ESX に接続されています。

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	Example:
	`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	**svs connection** *name*
	
	Example:
	`n1000v (config#) svs connection vcWest`
	`n1000v(config-svs-conn)#`
		vCenter Server に接続するために、グローバル コンフィギュレーション サブモードに切り替えます。

ステップ 3	**no connect**
	
	Example:
	`n1000v(config-svs-conn)# no connect`
	`n1000v(config-svs-conn)#`
		接続を閉じます。

vCenter Server からの DVS の削除

この手順を使用して、vCenter Server から DVS を削除します。

（注）　VSM に接続できない場合は、「VSM が接続されていない場合の vCenter Server からの DVS の削除」（P.4-5）を参照してください。

はじめる前に

- EXEC モードで CLI にログインしていること。
- 「vCenter Server への接続」（P.4-2）の手順を参照して、接続を設定します。
- Cisco Nexus 1000V が vCenter Server/ESX に接続されています。
- Server Administrator を Cisco Nexus 1000V に接続しているすべてのホストの VI クライアントから削除しておきます。詳細については、VMware のマニュアルを参照してください。

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	Example:
	`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	**svs connection** *name*
	
	Example:
	`n1000v(config#) svs connection vcWest`
	`n1000v(config-svs-conn)#`
		vCenter Server に接続するために、グローバル コンフィギュレーション サブモードに切り替えます。

ステップ 3	**no vmware dvs**
	
	Example:
	`n1000v(config-svs-conn)# no vmware dvs`
	`n1000v(config-svs-conn)#`
		指定された接続に関連付けられている DVS を vCenter Server から削除します。

VSM が接続されていない場合の vCenter Server からの DVS の削除

この手順を使用して、VSM が vCenter Server に接続されていない場合に、vCenter Server から DVS を削除します。

VSM が vCenter Server に接続されていない場合の DVS を削除する機能の設定は、2 段階のプロセスです。

1. admin ユーザまたはグループを設定します。「admin ユーザまたは admin グループの設定」（P.4-6）を参照してください。
2. vCenter Server から DVS を削除します。「vCenter Server からの DVS の削除」（P.4-7）を参照してください。

はじめる前に

- EXEC モードで CLI にログインしていること。
- vCenter Server にログインしていること。
- vCenter Server に admin ユーザまたはグループのアカウントを設定していること。

admin ユーザまたは admin グループの設定

この手順を使用して、admin ユーザまたは admin グループを設定します。

はじめる前に

- システム管理者が、DVS を管理および削除するための admin ユーザまたは admin グループを vCenter Server に作成していることを確認します。このユーザには、VM やホストの展開などの他の権限は付与できません。VSM に設定されている admin ユーザ名は、vCenter Server のユーザ名と同じである必要があります。

手順の概要

1. **config t**
2. **show svs connections**
3. **svs connection** *name*
4. **admin {user** *username* | **group** *groupname*}
5. **show svs connections**

手順の詳細

ステップ 1　DVS の名前を指定します。

```
switch# show svs connections

connection VC:
    ipaddress: 10.104.63.16
    remote port: 80
    protocol: VMware-vim https
    certificate: default
    datacenter name: N1K-DC
   admin:
    DVS uuid: a2 …
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 4.1.0 build 258902
```

ステップ 2　vCenter Server で admin ユーザを設定します。

```
switch# config t
switch(config)# svs connection VC
switch(config-svs-conn) # admin user NAuser
switch(config-svs-conn) #
```

（注）　**admin group** *groupname* コマンドを入力して、admin グループを設定することもできます。

ステップ 3　admin ユーザが作成されたことを確認します。

```
switch# show svs connections

connection VC:
    ipaddress: 10.104.63.16
    remote port: 80
    protocol: VMware-vim https
    certificate: default
    datacenter name: N1K-DC
   admin: NAuser(user)
    DVS uuid: a2 …
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 4.1.0 build 258902
```

vCenter Server からの DVS の削除

この手順を使用して、vCenter Server から DVS を削除します。

ステップ 1　admin ユーザ アカウントを使用して、VMware vSphere Client から vCenter Server にログインします。

ステップ 2　vSphere Client の左側のペインで、データセンターを選択します。

ステップ 3　[Hosts and Clusters] > [Networking] をクリックします。

ステップ 4　DVS を右クリックし、[Remove] を選択します。

ホスト マッピングの設定

ここでは、次の内容について説明します。

- 「ホスト マッピングについて」（P.4-7）
- 「モジュールからのホスト マッピングの削除」（P.4-7）
- 「新しいホストへのマッピング」（P.4-9）
- 「ホスト マッピングの表示」（P.4-10）

ホスト マッピングについて

VSM によって新しい VEM が検出されると、空きモジュール番号が自動的にその VEM に割り当てられ、このモジュール番号がホスト サーバの UUID にマッピングされます。このマッピングによって、同じホスト サーバには同じモジュール番号が割り当てられるようになります。

モジュールからのホスト マッピングの削除

ここでは、モジュールからホスト サーバへのマッピングを削除する手順を説明します。

はじめる前に

- EXEC モードで CLI にログインしていること。
- ホストはすでに vCenter 上の Cisco Nexus 1000V DVS から削除されている必要があります。

手順の概要

1. **config t**
2. **no vem** *module-number*
3. **show module vem mapping**
4. **copy running-config startup-config**

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**no vem** *module-number*
	
	Example:
	`n1000v(config)# no vem 4`
	`n1000v(config)# no vem 3`
	`cannot modify slot 3: host module is inserted`
	`n1000v((config)#`
		指定されたモジュールをソフトウェアから削除します。
		
		（注） モジュールがまだスロット内に存在している場合は、この例で示すように、コマンドは拒否されます。

ステップ 3	**show module vem mapping** **Example:** `n1000v(config)# show module vem mapping`	（任意）モジュールからホスト サーバへのマッピングを表示します。
ステップ 4	**copy running-config startup-config** **Example:** `n1000v(config-vem-slot)# 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。

例

この例は VEM のマッピングを示しています。

```
n1000v(config)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
n1000v(config)#
```

新しいホストへのマッピング

ここでは、モジュール番号を別のホスト サーバ UUID にマッピングする手順を説明します。

はじめる前に

- EXEC モードで CLI にログインしていること。
- ホストはすでに vCenter 上の Cisco Nexus 1000V DVS から「モジュールからのホスト マッピングの削除」（P.4-7）の手順を使用して削除されている必要があります。

（注）　最初に既存のホスト サーバ マッピングを削除しなかった場合は、新しいホスト サーバに別のモジュール番号が割り当てられます。

手順の概要

1. **config t**
2. **vem module** *number*
3. **host vmware id** *server-bios-uuid*
4. **show module vem mapping**
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**vem** *module number*
	
	Example:
	`n1000v(config)# vem 3`
	`n1000v((config-vem-slot)#`
		CLI VEM スロット 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	**host vmware id** *server-bios-uuid*
	
	Example:
	`n1000v(config-vem-slot)# host vmware id 6dd6c3e3-7379-11db-abcd-000bab086eb6`
	`n1000v(config-vem-slot)#`
		指定したモジュールに別のホスト サーバ UUID を割り当てます。

ステップ 4	**show module vem mapping** **Example:** `n1000v(config-vem-slot)# show module vem mapping`	（任意）モジュールからホスト サーバへのマッピングを表示します。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v(config-vem-slot)# 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。

例

この例は VEM のマッピングを示しています。

```
n1000v(config-vem-slot)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
  4          absent     6dd6c3e3-7379-11db-abcd-000bab086eb6    licensed

n1000v(config-vem-slot)#
```

ホスト マッピングの表示

ここでは、モジュールからホスト サーバへのマッピングを表示する手順を説明します。この手順は、EXEC モードで実行します。

手順の概要

1. **show module vem mapping**

手順の詳細

ステップ 1　次のコマンドを入力して、モジュールからホスト サーバへのマッピングを表示します。

```
n1000v(config)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
n1000v(config)#
```

接続の確認

ここでは、接続を表示して確認する手順を説明します。

はじめる前に

- 任意のコマンド モードで CLI にログインします。
- 「vCenter Server への接続」（P.4-2）の手順を参照して、接続設定を行います。
- Cisco Nexus 1000V が vCenter Server/ESX に接続されています。

手順の概要

手順の詳細

	コマンド	説明
ステップ 1	**show svs connections** [*name*] **Example:** n1000v# show svs connections vc Connection vc: IP address: 172.28.15.206 Protocol: vmware-vim https vmware dvs datacenter-name: HamiltonDC ConfigStatus: Enabled OperStatus: Connected n1000v#	現在の Cisco Nexus 1000V への接続を表示します。 （注）　ネットワーク接続の問題により、vCenter Server への接続がシャットダウンされる場合があります。ネットワーク接続が復元しても、Cisco Nexus 1000V では自動的に接続は復元されません。この場合、次のコマンド シーケンスを使用して、手動で接続を復元する必要があります。 no connect **connect**

ドメインの確認

ここでは、設定済みのドメインを表示して確認する手順を説明します。

はじめる前に

- 任意のコマンド モードで CLI にログインします。
- 「ドメインの作成」（P.3-4）の手順を参照して、ドメインを設定します。

手順の詳細

	コマンド	説明
ステップ 1	**show svs domain** **Example:** n1000v# **show svs domain** SVS domain config: Domain id:　98 Control vlan: 70 Packet vlan:　71 Sync state:　- n1000v#	Cisco Nexus 1000V で設定されたドメインを表示します。

設定の確認

ここでは、実行コンフィギュレーションを表示して確認する手順を説明します。

はじめる前に

- 任意のコマンド モードで CLI にログインします。

- 「vCenter Server への接続」（P.4-2）の手順を参照して、Cisco Nexus 1000V 接続を設定します。
- Cisco Nexus 1000V が vCenter Server/ESX に接続されています。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config**	現在の設定を表示します。 Cisco Nexus 1000V が vCenter Server または ESX サーバに接続していない場合は、接続関連情報だけが出力されます。

```
Example:
n1000v(config-acl)# show running-config
version 4.0(4)SV1(1)
feature port-security
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na. role network-operator
username admin password 5 $1$N1mX5tLD$daXpuxlAPcIHoz53PBhy6/ role network-admin
telnet server enable
ssh key rsa 1024 force
kernel core target 0.0.0.0
kernel core limit 1
system default switchport
ip access-list my66
  10 permit ip 1.1.1.1/32 1.1.1.2/32
snmp-server user admin network-admin auth md5 0x90f3798f3e894496a11ec42ce2efec9c priv
0x90f3798f3e894496a11ec42ce2efec9c localizedkey
snmp-server enable traps entity fru
snmp-server enable traps license
vrf context management
  ip route 0.0.0.0/0 172.28.15.1
switchname srini-cp
vlan 40-43,45-48
vdc srini-cp id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 32
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 192
  limit-resource u4route-mem minimum 32 maximum 256
  limit-resource u6route-mem minimum 16 maximum 256

interface Ethernet6/2
  inherit port-profile uplinkportprofile1

interface Ethernet6/3
  inherit port-profile uplinkportprofile2

interface Ethernet6/4
  inherit port-profile uplinportprofile3

interface Ethernet7/2
  inherit port-profile uplinkportprofile1

interface mgmt0
  ip address 172.28.15.163/24

interface Vethernet1
```

```
  inherit port-profile vm100

interface Vethernet2


  inherit port-profile vm100

interface Vethernet3


  inherit port-profile vm100

interface Vethernet4


  inherit port-profile vm100

interface Vethernet5

interface Vethernet6
boot kickstart bootflash:/svs-kickstart-mzg.4.0.1a.S1.0.82.bin sup-1
boot system bootflash:/svs-mzg.4.0.1a.S1.0.82.bin sup-1
boot system bootflash:/isan.bin sup-1
boot kickstart bootflash:/svs-kickstart-mzg.4.0.1a.S1.0.82.bin sup-2
boot system bootflash:/svs-mzg.4.0.1a.S1.0.82.bin sup-2
boot system bootflash:/isan.bin sup-2
ip route 0.0.0.0/0 172.28.15.1
port-profile uplinkportprofile1
  capability uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 1,40-43
  no shutdown
  system vlan 1,40-43
  state enabled
port-profile vm100
  vmware port-group
  switchport mode access
  switchport access vlan 43
  ip port access-group my100 out
  ip port access-group my66 in
  no shutdown
  state enabled
port-profile uplinkportprofile2
  capability uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 45-46
  no shutdown
  state enabled
port-profile uplinportprofile3
  capability uplink
  vmware port-group
  switchport trunk allowed vlan 47-48
  state enabled
port-profile uplinkportprofile3
  no shutdown
svs-domain
  domain id 163
  control vlan 41
  packet vlan 42
svs connection VCR5
  protocol vmware-vim
  remote ip address 172.28.30.83
```

```
  vmware dvs datacenter-name cisco-DC
  connect
n1000v(config-acl)#
```

モジュール情報の確認

ここでは、モジュール情報を表示して確認する手順を説明します。この情報には、Cisco Nexus 1000V からの DVS のビューも含まれます。

はじめる前に

- 任意のコマンド モードで CLI にログインします。
- 「vCenter Server への接続」（P.4-2）の手順を参照して、Cisco Nexus 1000V 接続を設定します。
- Cisco Nexus 1000V が vCenter Server/ESX に接続されています。
- Server Administrator で、Cisco Nexus 1000V を実行しているホストを、vCenter Server の DVS に追加しておきます。

手順の概要

1. **show module**
2. **show server-info**
3. **show interface brief**
4. **show interface virtual**

手順の詳細

	コマンド	説明
ステップ 1	**show module** **Example:** n1000v# **show module**	モジュール情報を表示します。
ステップ 2	**show server_info** **Example:** n1000v# **show server_info**	サーバ情報を表示します。
ステップ 3	**show interface brief** **Example:** n1000v# **show interface brief**	vCenter Server へのアップリンクを含むインターフェイス情報を表示します。
ステップ 4	**show interface virtual** **Example:** n1000v# **show interface virtual**	仮想インターフェイス情報を表示します。

```
Example
n1000v# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    1      Virtual Supervisor Module         Nexus1000V         active *
```

```
2    48     Virtual Ethernet Module                                ok
3    48     Virtual Ethernet Module                                ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    4.0(0)S1(0.82)  0.0     --
2    NA              0.0     --
3    NA              0.0     --

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

Mod  Server-IP        Server-UUID                            Server-Name
---  ---------------  -------------------------------------  --------------------
1    172.18.217.180                                          esx-1
2    172.18.117.44    487701ee-6e87-c9e8-fb62-001a64d20a20   esx-2
3    172.18.217.3     4876efdd-b563-9873-8b39-001a64644a24   esx-3

* this terminal session
```

Example

```
n1000v# show  server_info

Mod     Status          UUID
---     -----------     ----
  2      powered-up     34303734-3239-5347-4838-323130344654
  3      absent              371e5916-8505-3833-a02b-74a4122fc476
  4      powered-up     4880a7a7-7b51-dd96-5561-001e4f3a22f9
  5      absent              48840e85-e6f9-e298-85fc-001e4f3a2326
  6      powered-up     eb084ba6-3b35-3031-a6fe-255506d10cd0
n1000v#
```

Example

```
n1000v# show interface brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     172.28.15.211                           1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth2/2        1      eth  trunk  up      none                     a-1000(D) --

--------------------------------------------------------------------------------
Interface     VLAN   Type Mode   Status  Reason                   MTU
--------------------------------------------------------------------------------
```

Example

```
n1000v# show interface virtual

--------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
--------------------------------------------------------------------------------
Veth49                     R-VM-1                   2   mcs-srvr35
```

サーバ接続機能の履歴

ここでは、サーバ接続機能のリリース履歴を示します。

機能名	リリース	機能情報
DVS の削除	4.2(1)SV1(4a)	この機能が追加されました。
サーバ接続	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 5

設定の管理

この章では、次の事項について説明します。

- 「コンフィギュレーション管理について」（P.5-1）
- 「スイッチ名の変更」（P.5-1）
- 「Message of the Day の設定」（P.5-2）
- 「設定の確認」（P.5-3）
- 「コンフィギュレーションの保存」（P.5-10）
- 「コンフィギュレーションの削除」（P.5-10）
- 「コンフィギュレーション管理機能の履歴」（P.5-11）

コンフィギュレーション管理について

Cisco Nexus 1000V では、スイッチ名の変更と Messages of the Day の設定や、コンフィギュレーション ファイルの表示、保存、および消去を管理者が実行できるようになっています。

スイッチ名の変更

スイッチ名またはプロンプトをデフォルト（switch#）から別のストリングに変更するには、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。

- コンフィギュレーション モードで CLI にログインします。
- VSM が vCenter Server に接続されている場合は、この手順の中で、VSM による管理の対象の DVS も変更されます。DVS の名前を変更するときにエラーが発生した場合は、syslog が生成され、vCenter Server 上の DVS の名前は古い DVS 名のままとなります。

手順の詳細

	コマンド	目的

ステップ 1	**switchname**
	
	Example:
	`n1000v(config)# switchname metro`
	`metro(config)# exit`
	`metro#`
		スイッチ プロンプトを変更します。

Message of the Day の設定

ユーザがログインする際に端末上のログイン プロンプトの前に表示される Message of the Day（MOTD）のメッセージを設定するには、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。

- コンフィギュレーション モードで CLI にログインします。
- バナー メッセージは、最大 40 行、行あたり最大 80 文字です。
- デリミタを選ぶ際には、次のガイドラインに従ってください。
  - *メッセージストリング中ではデリミタを使用しないでください。*
  - **"** および **%** をデリミタとして使用しないでください。
- Message of the Day の中では次のトークンを使用できます。
  - `$(hostname)` を使用すると、スイッチのホスト名が表示されます。
  - `$(line)` を使用すると、vty または tty のラインまたは名前が表示されます。

手順の詳細

	コマンド	目的

ステップ 1	**banner motd [***delimiting-character message delimiting-character***]**
	
	Example:
	`n1000v(config)# banner motd #April 16, 2008 Welcome to the svs#`
	`n1000v(config)#`
		バナー Message of the Day を設定します。
		• 最大 40 行
		• 行あたり最大 80 文字
		• # などのデリミタで囲む
		• 複数行にまたがることが可能
		• トークンを使用可能

ステップ 2	**show banner motd**
	
	Example:
	`n1000v(config)# show banner motd`
	`April 16, 2008 Welcome to the Switch`
		設定されているバナー メッセージを表示します。

設定の確認

スイッチのコンフィギュレーションを表示するには、ここで説明する方法を使用します。ここでは、次の内容について説明します。

- 「ソフトウェアとハードウェアのバージョンの確認」（P.5-3）
- 「実行コンフィギュレーションの確認」（P.5-4）
- 「スタートアップ コンフィギュレーションと実行コンフィギュレーションの比較」（P.5-6）
- 「インターフェイス コンフィギュレーションの確認」（P.5-7）

ソフトウェアとハードウェアのバージョンの確認

アップグレードの前後でバージョンを確認するためなど、システム上のソフトウェアとハードウェアのバージョンを表示するには、ここに示すコマンドを使用します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show version** **Example:** n1000v# show version	現在スイッチで動作しているシステム ソフトウェアとハードウェアのバージョンを表示します。

```
Example:
n1000v# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  loader:    version 1.2(2)
  kickstart: version 4.0(4)SV1(1)
  system:    version 4.0(4)SV1(1)
  kickstart image file is:
  kickstart compile time:  4/2/2009 23:00:00
  system image file is:    bootflash:/svs.bin
  system compile time:     4/2/2009 23:00:00 [04/23/2009 09:55:29]


Hardware
```

```
  Cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU         with 1034780 kB of memory.
  Processor Board ID T5056893321

  Device name: n1000v
  bootflash:    3897832 kB

Kernel uptime is 0 day(s), 0 hour(s), 2 minute(s), 55 second(s)


plugin
  Core Plugin, Ethernet Plugin
```

実行コンフィギュレーションの確認

現在システムで動作しているコンフィギュレーションを表示するには、ここに示す方法を使用します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config** **Example:** n1000v# show running-config	現在スイッチで動作しているシステム ソフトウェアとハードウェアのバージョンを表示します。

```
Example:
n1000v# show running-config
version 4.0(4)SV1(1)
username admin password 5 $1$ouYE/pRM$/j4/2lg3RMd4PhE.1Z1S.0  role network-admin
telnet server enable
ip domain-lookup
ip host n1000v 172.23.232.141
kernel core target 0.0.0.0
kernel core limit 1
system default switchport
vem 3
  host vmware id 89130a67-e66b-3e57-ad25-547750bcfc7e
snmp-server user admin network-admin auth md5 0xb64ad6879970f0e57600c443287a79f0 priv
0xb64ad6879970f0e57600c443287a79f0 localizedkey
snmp-server enable traps license
vrf context management
  ip route 0.0.0.0/0 172.23.232.1
switchname n1000v
vlan 1,260-269
vdc n1000v id 1
  limit-resource vlan minimum 16 maximum 513
  limit-resource monitor-session minimum 0 maximum 64
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 256
  limit-resource u4route-mem minimum 32 maximum 80
  limit-resource u6route-mem minimum 16 maximum 48
```

```
port-profile Unused_Or_Quarantine_Uplink
  description "Port-group created for Nexus1000V internal usage. Do not use."
  capability uplink
  vmware port-group
  shutdown
  state enabled
port-profile Unused_Or_Quarantine_Veth
  description "Port-group created for Nexus1000V internal usage. Do not use."
  vmware port-group
  shutdown
  state enabled
port-profile system-uplink
  capability uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 260-261
  no shutdown
  system vlan 260-261
  state enabled
port-profile vm-uplink
  capability uplink
  vmware port-group
  switchport mode access
  switchport access vlan 262
  no shutdown
  state enabled
port-profile data262
  vmware port-group
  switchport access vlan 262
  no shutdown
  state enabled

interface Ethernet3/2
  inherit port-profile system-uplink

interface Ethernet3/3
  inherit port-profile vm-uplink

interface mgmt0
  ip address 172.23.232.141/24

interface control0
line vty
  session-limit 32
boot kickstart bootflash:/kick.bin sup-1
boot system bootflash:/svs.bin sup-1
boot kickstart bootflash:/kick.bin sup-2
boot system bootflash:/svs.bin sup-2
svs-domain
  domain id 141
  control vlan 260
  packet vlan 261
  svs mode L2
svs connection vc
  protocol vmware-vim
  remote hostname 172.23.231.201
  vmware dvs uuid "2c 6f 3d 50 62 f3 7f 4d-dc 00 70 e2 52 77 ca 15" datacenter-name
HamiltonDC
  connect

n1000v#
```

スタートアップ コンフィギュレーションと実行コンフィギュレーションの比較

スタートアップ コンフィギュレーションと実行コンフィギュレーションの違いを表示するには、ここに示す手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明

ステップ 1	`show running-config diff`
	
	Example:
	`n1000v# show running-config diff`
		スイッチ上の現在のスタートアップ コンフィギュレーションと実行コンフィギュレーションの差違を表示します。

例 5-1　show running-config diff のコマンド出力

```
n1000v# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1,7 ****
  version 4.0(1)
- system mem-thresholds minor 0 severe 0 critical 0
  vrf context management
    ip route 0.0.0.0/0 10.78.1.1
  switchname DCOS-112-S10
  vlan 80,110-111,150,160,170
  vdc DCOS-112-S10 id 1
--- 1,6 ----
***************
*** 116,131 ****
    ip address 10.78.1.112/24
  interface Vethernet49
    inherit port-profile vlan160
- interface Vethernet65
-   inherit port-profile vlan170
  interface Vethernet50
    inherit port-profile vlan160
  interface Vethernet66
    inherit port-profile vlan170
  ip route 0.0.0.0/0 10.78.1.1
  vlan 80-80, 110-110, 111-111, 150-150, 160-160, 170-170

--- 115,130 ----
    ip address 10.78.1.112/24

  interface Vethernet49
    inherit port-profile vlan160
```

```
  interface Vethernet50
    inherit port-profile vlan160

+ interface Vethernet65
+   inherit port-profile vlan170
+
  interface Vethernet66
    inherit port-profile vlan170
  ip route 0.0.0.0/0 10.78.1.1
  vlan 80-80, 110-110, 111-111, 150-150, 160-160, 170-170

n1000v#
```

インターフェイス コンフィギュレーションの確認

ここでは、次の手順について説明します。

- 「インターフェイス コンフィギュレーションの要約の確認」（P.5-7）
- 「インターフェイス コンフィギュレーションの詳細の確認」（P.5-8）
- 「全インターフェイスの要約の確認」（P.5-8）
- 「全インターフェイスの実行コンフィギュレーションの確認」（P.5-9）

インターフェイスの表示の詳細については、『*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 コンフィギュレーションの要約の確認

インターフェイス コンフィギュレーションの要約を表示するには、ここに示す手順を実行します。

はじめる前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show interface** {*type*} {*name*} **brief**	指定したインターフェイス コンフィギュレーションに関する要約情報を表示します。

```
Example:
n1000v# show interface mgmt 0 brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     10.78.1.63                              1000     1500
n1000v#
```

インターフェイス コンフィギュレーションの詳細の確認

インターフェイス コンフィギュレーションの詳細を表示するには、ここに示す手順を実行します。

はじめる前に

ここに示すコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show interface** {*type*} {*name*}	指定したインターフェイス コンフィギュレーションに関する詳細を表示します。

```
Example:
n1000v# show interface mgmt 0
mgmt0 is up
  Hardware: Ethernet, address: 0050.5689.3321 (bia 0050.5689.3321)
  Internet Address is 172.23.232.141/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    4961 packets input, 511995 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    245 packets output, 35853 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors

n1000v#
```

全インターフェイスの要約の確認

システム上で設定されているすべてのインターフェイスの要約を表示するには、ここに示す手順を実行します。

はじめる前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show interface brief**	システム上の全インターフェイス コンフィギュレーションの要約を表示します。

```
Example:
n1000v# show interface 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        262    eth  access up      none                     1000(D) --
--------------------------------------------------------------------------------
Interface     VLAN   Type Mode   Status  Reason                   MTU
--------------------------------------------------------------------------------
Veth81        630    virt access up      none                     1500
Veth82        630    virt access up      none                     1500
Veth224       631    virt access up      none                     1500
Veth225       1      virt access nonPcpt nonParticipating         1500
n1000v#
```

全インターフェイスの実行コンフィギュレーションの確認

システム上の全インターフェイスの実行コンフィギュレーションを表示するには、ここに示す手順を実行します。

はじめる前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。
- コマンド **show running-config interface** の出力は、コマンド **show interface** の出力と異なります。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config interface**	システム上の全インターフェイスの実行コンフィギュレーションを表示します。

```
Example:
n1000v# show running-config interface
version 4.0(1)

interface Ethernet3/2
  switchport
  inherit port-profile sftrunk

interface Ethernet3/6
  switchport
  inherit port-profile vmuplink

interface Ethernet6/2
  switchport
```

```
  inherit port-profile alluplink

interface mgmt0
  ip address 10.78.1.63/24

interface Vethernet81
  inherit port-profile vm630

interface Vethernet82
  inherit port-profile vm630

interface Vethernet224
  inherit port-profile vm631

interface Vethernet225

n1000v#
```

コンフィギュレーションの保存

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保存するには、ここに示す手順を実行します。これにより、コンフィギュレーション ファイルに変更内容が保存され、次回システムを起動したときに有効になります。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**copy running-config startup-config**	新しいコンフィギュレーションを不揮発性ストレージに保存します。これにより、実行コンフィギュレーションとスタートアップ コンフィギュレーションが同じになります。

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

コンフィギュレーションの削除

スタートアップ コンフィギュレーションを削除するには、ここに示す手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

注意　**write erase** コマンドを実行すると、スタートアップ コンフィギュレーション全体（ローダ機能、ライセンス コンフィギュレーション、および証明書拡張ファイル コンフィギュレーションを除く）が削除されます。

- CLI にログインしていること。
- このコマンドでは次のパラメータが使用されます。
  - boot：ブート変数と mgmt0 IP コンフィギュレーションを削除します。
  - debug：デバッグ コンフィギュレーションを削除します。

手順の詳細

	コマンド	説明
ステップ 1	**write erase** [boot | debug]	既存のスタートアップ コンフィギュレーションが完全に削除され、すべての設定が工場出荷時のデフォルトに戻ります。 実行コンフィギュレーションに影響はありません。

コンフィギュレーション管理機能の履歴

ここでは、コンフィギュレーション管理機能のリリース履歴を示します。

機能名	リリース	機能情報
コンフィギュレーション管理	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 6

ファイルの使用

ここでは、次の内容について説明します。

- 「ファイルについて」（P.6-1）
- 「ファイル システム内の移動」（P.6-1）
- 「ファイルのコピーとバックアップ」（P.6-5）
- 「ディレクトリの作成」（P.6-7）
- 「既存のディレクトリの削除」（P.6-7）
- 「ファイルの移動」（P.6-8）
- 「ファイルまたはディレクトリの削除」（P.6-9）
- 「ファイルの圧縮」（P.6-9）
- 「ファイルの圧縮解除」（P.6-11）
- 「コマンド出力のファイル保存」（P.6-12）
- 「ロード前のコンフィギュレーション ファイルの確認」（P.6-12）
- 「以前のコンフィギュレーションへのロールバック」（P.6-13）
- 「ファイルの表示」（P.6-13）
- 「ファイル管理機能の履歴」（P.6-15）

ファイルについて

Cisco Nexus 1000V のファイル システムは、スイッチによって使用される次のようなファイル システムすべてに対するインターフェイスとなります。

- フラッシュ メモリ ファイル システム
- ネットワーク ファイル システム（TFTP および FTP）
- データを読み書きするためのその他のエンドポイント（実行コンフィギュレーションなど）

ファイル システム内の移動

ここでは、ファイル システム内の移動方法について説明します。具体的な内容は次のとおりです。

- 「ファイル システムの指定」（P.6-2）
- 「作業ディレクトリの特定」（P.6-2）

- 「ディレクトリの変更」（P.6-3）
- 「ファイル システム内のファイルの一覧表示」（P.6-3）
- 「ファイルをコピーするために使用できるファイル システムの特定」（P.6-4）
- 「タブ補完の使用」（P.6-5）

ファイル システムの指定

ファイル システムを指定するための構文は、`<file system name>`:[//*server*/] です。表 6-1 にファイル システムの構文を示します。

表 6-1　ファイル システムの構文の構成要素

ファイル システム名	サーバ	説明
bootflash	sup-active sup-local sup-1 module-1	アクティブ スーパーバイザにある内部メモリ。システム イメージ、コンフィギュレーション ファイル、およびその他のファイルの格納に使用されます。Cisco Nexus 1000V CLI でのデフォルトは bootflash: ファイル システムです。
	sup-standby sup-remote sup-2 module-2	スタンバイ スーパーバイザにある内部メモリ。システム イメージ、コンフィギュレーション ファイル、およびその他のファイルの格納に使用されます。
volatile	—	スーパーバイザ モジュールにある、一時的または保留中の変更のために使用される Volatile Random-Access Memory（VRAM）。

作業ディレクトリの特定

CLI の現在のディレクトリ名を表示するには、ここに示す手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的

ステップ 1	**pwd**
	
	Example:
	`n1000v# pwd`
	`bootflash:`
		現在の作業ディレクトリを表示します。

ディレクトリの変更

CLI で、あるディレクトリまたはファイル システムから別のディレクトリまたはファイル システムに場所を変更するには、ここに示す手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。
- Cisco Nexus 1000V CLI でのデフォルトは bootflash: ファイル システムです。

ヒント volatile: ファイル システムに保存されたファイルは、スイッチのリブート時にすべて消去されます。

手順の詳細

手順	コマンド	目的

ステップ 1	**pwd**
	
	Example:
	`n1000v# pwd`
	`volatile:`
	`n1000v#`
		CLI の現在のディレクトリ名を表示します。

ステップ 2	**cd** *directory name*	CLI の場所を指定したディレクトリに変更します
	Example: `n1000v# cd bootflash:`	CLI の場所を、bootflash: ファイル システムのルート ディレクトリに変更します。
	Example: `n1000v# cd bootflash:mydir`	CLI の場所を、bootflash: ファイル システムの mydir ディレクトリに変更します。
	Example: `n1000v# cd mystorage`	CLI の場所を、現在のディレクトリの中にある mystorage ディレクトリに変更します。 現在のディレクトリが bootflash: mydir だった場合、このコマンドを実行すると、現在のディレクトリが bootflash: mydir/mystorage に変更されます。

ファイル システム内のファイルの一覧表示

ディレクトリまたはファイルの内容を表示するには、ここに示す手順を実行します。

手順の詳細

手順	コマンド	目的
ステップ 1	**dir** [*directory* | *filename*]	ディレクトリまたはファイルの内容を表示します。

Example:

```
DCOS-112-R5# dir lost+found/
      49241     Jul 01 09:30:00 2008  diagclient_log.2613
      12861     Jul 01 09:29:34 2008  diagmgr_log.2580
         31     Jul 01 09:28:47 2008  dmesg
       1811     Jul 01 09:28:58 2008  example_test.2633
         89     Jul 01 09:28:58 2008  libdiag.2633
      42136     Jul 01 16:34:34 2008  messages
         65     Jul 01 09:29:00 2008  otm.log
        741     Jul 01 09:29:07 2008  sal.log
         87     Jul 01 09:28:50 2008  startupdebug

Usage for log://sup-local
   51408896 bytes used
  158306304 bytes free
  209715200 bytes total
DCOS-112-R5#
```

ファイルをコピーするために使用できるファイル システムの特定

コピー先またはコピー元として使用できるファイル システムを特定するには、ここに示す手順を実行します。

はじめる前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。

手順の詳細

手順	コマンド	目的
ステップ 1	**copy ?**	copy コマンドで使用できるコピー元ファイル システムを表示します。
ステップ 2	**copy filename ?** **Example:** 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 nvram: Select source filesystem running-config Copy running configuration to destination scp: Select source filesystem sftp: Select source filesystem startup-config Copy startup configuration to destination system: Select source filesystem tftp: Select source filesystem volatile: Select source filesystem	copy コマンドで特定のファイルに対して使用できるコピー先ファイル システムを表示します。

タブ補完の使用

CLI でコマンド中の部分的なファイル名を補完するには、次に示す手順を実行します。

	コマンド	目的
ステップ 1	**show file** *filesystem name: partial filename* <Tab> **Example:** n1000v# show file bootflash:nexus-1000v-bootflash:nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin bootflash:nexus-1000v-mzg.4.0.4.SV1.0.42.bin bootflash:nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin	部分的なファイル名を入力して Tab キーを押すと、入力した文字が単一のファイルに一致する場合、CLI によりファイル名が補完されます。 一致しない場合は、入力した文字に一致するファイル名の選択肢の一覧が表示されます。 その後、ファイル名が一意になるような十分な文字を入力することで、CLI によりファイル名が補完されます。
ステップ 2	**show file bootflash:c** <Tab> **Example:** n1000v# show file bootflash:c<Tab> -----BEGIN RSA PRIVATE KEY----- MIICXgIBAAKBgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j ... ... n1000v#	CLI によりファイル名が補完されます。

ファイルのコピーとバックアップ

保存のためや別の場所で再利用するために、コンフィギュレーション ファイルなどのファイルをコピーするには、ここに示す手順を実行します。内部ファイル システムが壊れると、コンフィギュレーションが失われるおそれがあります。コンフィギュレーション ファイルは定期的に保存およびバックアップしてください。また、新しいソフトウェア コンフィギュレーションをインストールしたり、新しいソフトウェア コンフィギュレーションに移行する前に、既存のコンフィギュレーション ファイルをバックアップしてください。

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。

- Telnet または SSH 接続を通じて CLI にログインしていること。
- 離れた場所にコピーする場合は、デバイスから宛先に到達できるルートがあること。サブネット間でトラフィックをルーティングするルータまたはデフォルト ゲートウェイがない場合は、使用デバイスとリモートのコピー先が同じサブネットワーク内にあることが必要です。
- ping コマンドを使用して、デバイスがコピー先に接続できること。
- コピー元のコンフィギュレーション ファイルがリモート サーバ上の正しいディレクトリにあること。
- コピー元ファイルのアクセス権が正しく設定されていること。ファイルのアクセス権は、誰でも読み取り可能に設定されている必要があります。

（注）　**dir** コマンドを使用して、コピー先のファイル システムに十分なスペースがあることを確認してください。十分な領域が残っていない場合は、**delete** コマンドを使用して不要なファイルを削除します。

ファイル システム	サーバ	ファイル名
bootflash	sup-active sup-standby sup-1 または module-1 sup-2 または module-2 sup-local sup-remote	ユーザ指定
volatile	—	ユーザ指定
system	—	running-config
tftp[1]	IPv4 アドレス、IPv6 アドレス、または DNS 名	ユーザ指定
ftp		
scp（secure copy）		
sftp		
core	*slot-number*	プロセス識別番号

1. ファイルのダウンロードとアップロードを行う際には、TFTP の制限により、TFTP クライアントではファイル サイズが 32 MB に制限され、一部の TFTP サーバでは 16 MB に制限されます。

手順の詳細

手順	コマンド	目的
ステップ 1	**copy** [*source filesystem*:] *filename* [*destination filesystem*:] *filename*	指定したコピー元から指定したコピー先にファイルをコピーします。
	Example: `n1000v# copy system:running-config tftp://10.10.1.1/home/configs/switch3-run.cfg`	実行コンフィギュレーションのコピーをリモートのスイッチに保存します。
	Example: `n1000v# copy bootflash:system_image bootflash://sup-2/system_image`	アクティブ スーパーバイザ モジュールのブートフラッシュから、スタンバイ スーパーバイザ モジュールのブートフラッシュにファイルをコピーします。
	Example: `n1000v# copy system:running-config bootflash:my-config`	実行コンフィギュレーションを bootflash: ファイル システムにコピーします。
	Example: `n1000v# copy scp://user@10.1.7.2/system-image bootflash:system-image`	IPv4 アドレスで識別される SCP サーバからシステム イメージ ファイルをブートフラッシュにコピーします。
	Example: `n1000v# copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt`	IPv4 アドレスで識別される SFTP サーバからスクリプト ファイルを volatile: ファイル システムにコピーします。
	Example: `n1000v# copy system:running-config bootflash:my-config`	実行コンフィギュレーションのバックアップ コピーを bootflash: ファイル システムに格納します（ASCII ファイル）。

手順	コマンド	目的
	Example: `n1000v# copy bootflash:samplefile bootflash:mystorage/samplefile`	samplefile という名前のファイルを、bootflash: ファイル システムのルート ディレクトリから mystorage ディレクトリにコピーします。
	Example: `n1000v# copy samplefile mystorage/samplefile`	現在のファイル システム内でファイルをコピーします。
	Example: `n1000v# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config`	コピー元ファイルをスイッチの実行コンフィギュレーションにコピーします。ファイルは行単位で解析され、スイッチが設定されます。

ディレクトリの作成

現在のディレクトリ レベルまたは指定したディレクトリ レベルにディレクトリを作成するには、次の手順を実行します。

手順	コマンド	目的
ステップ 1	**mkdir** *directory name* **dir** *filename*	現在のディレクトリ レベルにディレクトリを作成します。

	example:
	`n1000v# mkdir bootflash:test`
	`n1000v#`
		test という名前のディレクトリを bootflash: ディレクトリに作成します。

	example:
	`n1000v# mkdir test`
	`n1000v#`
		test という名前のディレクトリを現在のディレクトリ レベルに作成します。現在のディレクトリが bootflash:mydir の場合、このコマンドを実行すると、bootflash:mydir/test というディレクトリが作成されます。

既存のディレクトリの削除

フラッシュ ファイル システムから既存のディレクトリを削除するには、次の手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。
- このコマンドは、フラッシュ ファイル システムでだけ有効であること。
- ディレクトリを削除するには、ディレクトリが空であること。

手順の詳細

手順	コマンド	目的
ステップ 1	**rmdir** {bootflash: | debug: | volatile:} *directory*	ディレクトリを削除します。
	example: n1000v# rmdir bootflash:test n1000v#	bootflash ディレクトリ内の test という名前のディレクトリを削除します。
	example: n1000v# rmdir test n1000v#	現在のディレクトリ レベルにある test という名前のディレクトリを削除します。カレント ディレクトリが bootflahs:mydir である場合、このコマンドでは bootflash:mydir/test ディレクトリが削除されます。

ファイルの移動

ある場所から別の場所にファイルを移動するには、次の手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。
- 移動先のディレクトリに十分なスペースがない場合、コピーは完了しないこと。

注意　宛先ディレクトリに同名のファイルがすでに存在する場合は、そのファイルは移動対象のファイルによって上書きされます。

手順の詳細

手順	コマンド	目的
ステップ 1	**move** {*source path and filename*}　{*destination path and filename*}	ディレクトリを削除します。
	Example: n1000v# move bootflash:samplefile bootflash:mystorage/samplefile	あるディレクトリから同じファイル システム（bootflash:）内の別のディレクトリにファイルを移動します。
	Example: n1000v# move samplefile mystorage/samplefile	現在のファイル システム内であるディレクトリから別のディレクトリにファイルを移動します。

ファイルまたはディレクトリの削除

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、ここに示す手順を実行します。

はじめる前に

注意　削除する際にファイル名の代わりにディレクトリ名を指定すると、ディレクトリとその内容がすべて削除されます。

- ファイルを削除する場合、ソフトウェアによってファイルが消去されます。
- 環境変数 CONFIG_FILE または BOOTLDR で指定されているコンフィギュレーション ファイルまたはイメージを削除しようとすると、削除を確認するプロンプトが表示されます。
- BOOT 環境変数で指定されている最後の有効なシステム イメージを削除しようとすると、削除を確認するプロンプトが表示されます。

手順の詳細

手順	コマンド	目的
ステップ 1	**delete** [**bootflash:** | **debug:** | **log:** | **volatile:**] *filename or directory name* **Example:** `n1000v# delete bootflash:dns_config.cfg`	指定したファイルまたはディレクトリを削除します。
	Example: `n1000v# delete dns_config.cfg`	指定したファイルを現在の作業ディレクトリから削除します。
	Example: `n1000v# delete bootflash:my-dir`	指定したディレクトリとその内容を削除します。

ファイルの圧縮

LZ77 符号化を使用して指定したファイルを圧縮（zip）するには、ここに示す手順を実行します。

はじめる前に

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的
ステップ1	**show** *command* > [*path*] *filename* **Example:** n1000v# show system internal l2fm event-history errors n1000v#	show コマンドの出力をファイルに保存します。
ステップ2	dir **Example:** n1000v# dir	最初の手順で作成した新しいファイルを含め、現在のディレクトリの内容を表示します。
ステップ3	**gzip** [*path*] *filename* **Example:** n1000v# gzip bootflash:errorsfile n1000v#	指定したファイルを圧縮します。
ステップ4	dir **Example:** n1000v# dir	新たに圧縮したファイルを含め、指定したディレクトリの内容を表示します。新たに圧縮したファイルのファイル サイズの違いを表示します。

```
Example:
n1000v# show system internal l2fm event-history errors >errorsfile
n1000v# dir
      2687     Jul 01 18:17:20 2008  errorsfile
     16384      Jun 30 05:17:51 2008  lost+found/
      4096      Jun 30 05:18:29 2008  routing-sw/
        49      Jul 01 17:09:18 2008  sample_test.txt
   1322843      Jun 30 05:17:56 2008  nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin
  21629952      Jun 30 05:18:02 2008  nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
  39289400      Jun 30 05:18:14 2008  nexus-1000v-mzg.4.0.4.SV1.0.42.bin

Usage for bootflash://
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
n1000v# gzip bootflash:errorsfile
n1000v# dir
      1681      Jun 30 05:21:08 2008  cisco_svs_certificate.pem
       703      Jul 01 18:17:20 2008  errorsfile.gz
     16384      Jun 30 05:17:51 2008  lost+found/
      4096      Jun 30 05:18:29 2008  routing-sw/
        49      Jul 01 17:09:18 2008  sample_test.txt
   1322843      Jun 30 05:17:56 2008  nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin
  21629952      Jun 30 05:18:02 2008  nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
  39289400      Jun 30 05:18:14 2008  nexus-1000v-mzg.4.0.0.S1.0.34.bin

Usage for bootflash://
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
n1000v#
```

ファイルの圧縮解除

LZ77 符号化を使用して圧縮された、指定したファイルを圧縮解除（unzip）するには、ここに示す手順を実行します。

はじめる前に

- CLI にログインしていること。

手順の詳細

手順　コマンド	目的
ステップ1 **gunzip** [path] *filename*	指定したファイルを圧縮解除します。
ステップ2 **dir**	新たに圧縮解除したファイルを含め、ディレクトリの内容を表示します。

```
Example:
n1000v# gunzip bootflash:errorsfile.gz
n1000v# dir bootflash:
       2687     Jul 01 18:17:20 2008  errorsfile
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  nexus-1000v-dplug-mzg.4.0.0.SV1.0.42.bin
   21629952     Jun 30 05:18:02 2008  nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
   39289400     Jun 30 05:18:14 2008  nexus-1000v-mzg.4.0.0.SV1.0424.bin

Usage for bootflash://sup-local
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
DCOS-112-R5#
```

コマンド出力のファイル保存

コマンド出力をファイルに保存するには、次の手順を実行します。

手順の詳細

手順	コマンド	目的
ステップ1	**show running-config >** [*path* | *filename*]	コマンド **show running-config** の出力を、指定したパスおよびファイル名に保存します。
	Example: `n1000v# show running-config > volatile:switch1-run.cfg`	コマンド **show running-config** の出力を、volatile: ファイル システム上のファイル switch1-run.cfg に保存します。
	Example: `n1000v# show running-config > bootflash:switch2-run.cfg`	コマンド **show running-config** の出力を、ブートフラッシュ上のファイル switch2-run.cfg に保存します。
	Example: `n1000v# show running-config > tftp://10.10.1.1/home/configs/switch3-run.cfg`	コマンド **show running-config** の出力を、TFTP サーバ上のファイル switch3-run.cfg に保存します。
	Example: `n1000v# show interface > samplefile`	コマンド show interface の出力を、ブートフラッシュなど、同じディレクトリ レベルのファイル samplefile に保存します。

ロード前のコンフィギュレーション ファイルの確認

イメージをロードする前にその完全性を確認するには、ここに示す手順を実行します。このコマンドは、システム イメージとキックスタート イメージの両方に使用できます。

手順の詳細

手順	コマンド	目的
ステップ1	**copy** *source path and file* **system:running-config** **Example:** `n1000v# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config`	コピー元ファイルをスイッチの実行コンフィギュレーションにコピーします。ファイルは行単位で解析され、スイッチが設定されます。

ステップ2	**show version image** [bootflash: | modflash: |volatile:]
	
	Example:
	`n1000v# show version image bootflash:isan.bin`
	`  image name: nexus-1000v-mz.4.0.4.SV1.1.bin`
	`  bios:  version unavailable`
	`  system:  version 4.0(4)SV1(1)`
	`  compiled:  4/2/2009 23:00:00 [04/23/2009 09:55:29]`
	`n1000v#`
		指定したイメージを検証します。

以前のコンフィギュレーションへのロールバック

以前保存したコンフィギュレーションからコンフィギュレーションを復元するには、ここに示す手順を実行します。

はじめる前に

（注）　**copy running-config startup-config** コマンドを実行するたびに、バイナリ ファイルが作成され、ASCII ファイルが更新されます。有効なバイナリ コンフィギュレーション ファイルを使用すると、ブート全体の時間が大幅に短縮されます。バイナリ ファイルはアップロードできませんが、その内容を使用して既存のスタートアップ コンフィギュレーションを上書きできます。**write erase** コマンドを実行すると、バイナリ ファイルが消去されます。

手順の詳細

手順	コマンド	目的

ステップ 1	`copy running-config bootflash: {filename}`
	
	Example:
	`n1000v# copy running-config bootflash:June03-Running`
		以前保存した実行コンフィギュレーションのスナップショット コピー（バイナリ ファイル）に戻します。

	copy bootflash: {*filename*} startup-config **Example:** `n1000v# copy bootflash:my-config startup-config`	bootflash: ファイル システムに以前保存したコンフィギュレーションのコピー（ASCII ファイル）に戻します。

ファイルの表示

ここでは、ファイルに関する情報の表示方法について説明します。具体的には次の手順について説明します。

- 「ファイルの内容の表示」（P.6-13）
- 「ディレクトリの内容の表示」（P.6-14）
- 「ファイル チェックサムの表示」（P.6-15）
- 「ファイルの最後の行の表示」（P.6-15）

ファイルの内容の表示

指定したファイルの内容を表示するには、次の手順を実行します。

はじめる前に

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的
ステップ 1	**show file [bootflash: | debug: | volatile:]** *filename* **Example:** n1000v# show file bootflash:sample_test.txt config t Int veth1/1 no shut end show int veth1/1 n1000v#	指定したファイルの内容を表示します。

ディレクトリの内容の表示

ディレクトリまたはファイル システムの内容を表示するには、ここに示す手順を実行します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順	コマンド	目的
ステップ 1	**pwd** **Example:** n1000v# pwd bootflash:	現在の作業ディレクトリを表示します。
ステップ 2	**dir**	ディレクトリの内容を表示します。

```
Example:
n1000v# pwd
bootflash:
n1000v# dir

Usage for volatile://
          0 bytes used
   20971520 bytes free
   20971520 bytes total
n1000v#
```

ファイル チェックサムの表示

ファイルの完全性を確認するためにチェックサムを表示するには、次の手順を実行します。

手順	コマンド	目的
ステップ 1	**show file** *filename* [**cksum | md5sum**] **Example:** n1000v# **s**how file bootflash:cisco_svs_certificate.pem cksum 266988670	元のファイルと比較するために、ファイルのチェックサムまたは Message-Digest Algorithm 5（MD5）チェックサムを表示します。
	Example: n1000v# show file bootflash:cisco_svs_certificate.pem md5sum d3013f73aea3fda329f7ea5851ae81ff n1000v#	ファイルの Message-Digest Algorithm 5（MD5）チェックサムを表示します。MD5 はファイルの電子的なフィンガープリントです。

ファイルの最後の行の表示

指定したファイルの最後の行（末尾）を表示するには、ここに示すコマンドを使用します。

はじめる前に

- EXEC モードで CLI にログインしていること。

手順の詳細

手順	コマンド	目的
ステップ 1	**tail** {*path*}[*filename*] {*Number of lines*}	指定したファイルの末尾から、要求された数の行を表示します。 行数に指定できる範囲は 0 ～ 80 です。

```
Example:
n1000v# tail bootflash:errorsfile 5

20) Event:E_DEBUG, length:34, at 171590 usecs after Tue Jul  1 09:29:05 2008
    [102] main(326): stateless restart


n1000v#
```

ファイル管理機能の履歴

ここでは、ファイル管理機能のリリース履歴を示します。

機能名	リリース	機能情報
ファイル管理	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 7

ユーザの管理

ここでは、次の手順について説明します。

- 「ユーザ管理について」（P.7-1）
- 「現在のユーザ アクセスの表示」（P.7-1）
- 「ユーザへのメッセージ送信」（P.7-2）
- 「ユーザ管理機能の履歴」（P.7-2）

ユーザ管理について

管理者は、デバイスに現在接続しているユーザを特定することができます。また、ユーザの 1 人または全員にメッセージを送信することができます。

ユーザ ロールを割り当てる方法については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

現在のユーザ アクセスの表示

この手順を使用して、現在スイッチにアクセスしているすべてのユーザを表示します。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順の詳細

	コマンド	説明
ステップ 1	**show users**	現在システムにアクセスしているユーザのリストを表示します。

```
Example:
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    pts/0        Jul  1 04:40 03:29        2915 (::ffff:64.103.145.136)
admin    pts/2        Jul  1 10:06 03:37        6413 (::ffff:64.103.145.136)
```

```
admin    pts/3        Jul  1 13:49   .          8835 (171.71.55.196)*
n1000v#
```

ユーザへのメッセージ送信

このコマンドを使用して、現在システムを使用しているすべてのアクティブな CLI ユーザにメッセージを送信できます。

はじめる前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順の詳細

	コマンド	説明
ステップ 1	**send** {session *device*} *line*	現在システムにログインしているユーザにメッセージを送信します。 • **session**：指定された pts または tty デバイス タイプにメッセージを送信します。 • *line*：メッセージ（最長 80 文字の英数字）。

```
Example:
n1000v# send Hello. Shutting down the system in 10 minutes.

Broadcast Message from admin@switch
        (/dev/pts/34) at 8:58 ...

Hello. Shutting down the system in 10 minutes.


n1000v#
```

ユーザ管理機能の履歴

ここでは、ユーザ管理機能のリリース履歴を示します。

機能名	リリース	機能情報
ユーザ管理	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 8

NTP の設定

この章では、Network Time Protocol（NTP; ネットワーク タイム プロトコル）の設定方法について説明し、次の内容が含まれます。

- 「NTP の概要」（P.8-1）
- 「NTP の前提条件」（P.8-2）
- 「設定時の注意事項および制限事項」（P.8-3）
- 「デフォルト設定」（P.8-3）
- 「NTP サーバおよびピアの設定」（P.8-3）
- 「NTP の設定確認」（P.8-4）
- 「NTP の設定例」（P.8-5）
- 「その他の関連資料」（P.8-5）
- 「NTP の機能の履歴」（P.8-5）

NTP の概要

NTP は、分散している一連のタイム サーバおよびクライアント間で、計時を同期させます。この同期によって、複数のネットワーク デバイスからシステム ログおよびその他の時刻特定イベントを受信したときに、イベントを相互に関連付けることができます。

NTP ではトランスポート プロトコルとして、ユーザ データグラム プロトコル（UDP）を使用します。すべての NTP 通信で Universal Time Coordinated（UTC; 協定世界時）規格を使用します。NTP サーバは通常、タイム サーバに接続されたラジオ クロック、アトミック クロックなど、信頼できる時刻源から時刻を受信します。NTP はネットワークにこの時刻を配信します。NTP はきわめて効率的です。毎分 1 パケット以下で、2 台のマシンが相互に 1 ミリ秒以内で同期します。

NTP では層（stratum）を使用して、ネットワーク デバイスが正規の時刻源から NTP ホップ カウントにしてどれだけ離れているかを表します。Stratum 1 タイム サーバは、正規の時刻源（アトミック クロックなど）が直接接続されています。Stratum 2 の NTP サーバは、Stratum 1 NTP サーバから NTP を使用して時刻を受信し、それによって正規の時刻源に接続します。

NTP は正確な時刻を維持している可能性のあるネットワーク デバイスへの同期を回避します。また、NTP は順番どおりに同期しないシステムには、同期しません。NTP は複数のネットワーク デバイスから伝えられた時刻を比較し、時刻が他と大きく異なっているネットワーク デバイスには、下位の層であっても同期しません。

Cisco NX-OS は Stratum 1 サーバとして動作しません。したがって、ラジオ クロックまたはアトミック クロックには接続できません。インターネット上で利用できる、パブリックな NTP サーバに由来するタイム サービスをネットワークに使用することを推奨します。

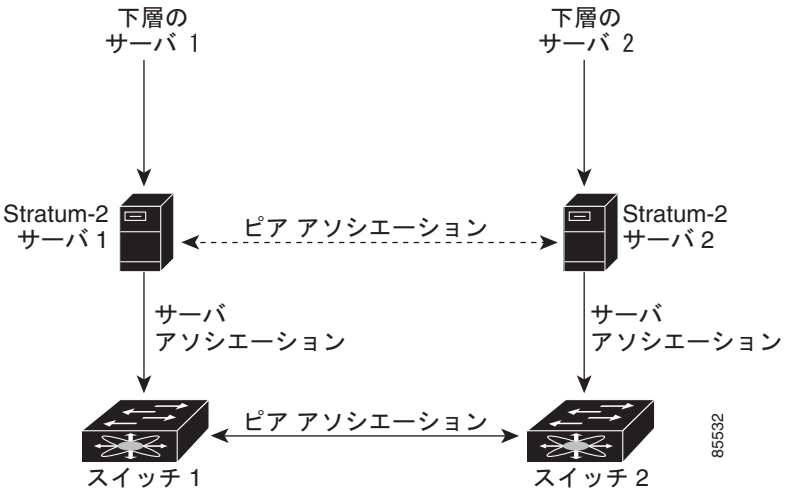
ネットワークがインターネットから切り離されている場合、Cisco NX-OS ではネットワーク デバイスが実際には他の方法で時刻を決定している場合でも、NTP によって同期しているものとして動作するように、ネットワーク デバイスを設定できます。その後、NTP を使用して、そのネットワーク デバイスに他のネットワーク デバイスを同期させることができます。

NTP ピア

NTP を使用すると、2 つのネットワーキング デバイス間にピア関係を設定できます。ピアはそのままで時刻を提供することも、または NTP サーバに接続することもできます。ローカル デバイスとリモート ピアの両方がそれぞれ異なる NTP サーバに接続すると、NTP サービスの信頼性が高くなります。ローカル デバイスはピアから得た時刻を使用することによって、接続先の NTP サーバに障害が発生した場合でも、正確な時刻を維持できます。

図 8-1 に、2 つの NTP ストラタム 2 サーバおよび 2 つのスイッチを含むネットワークを示します。

図 8-1　NTP のピアおよびサーバ アソシエーション



この構成では、スイッチ 1 とスイッチ 2 は NTP ピアになっています。スイッチ 1 は Stratum-2 サーバ 1 を使用し、スイッチ 2 は Stratum-2 サーバ 2 を使用します。Stratum-2 サーバ 1 に障害が発生すると、サーバ 1 はスイッチ 2 に関連付けられたピア経由で正しい時刻を維持します。

ハイ アベイラビリティ

NTP はステートレス リスタートをサポートします。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

NTP ピアを設定すると、NTP サーバ障害の発生時に冗長性が得られます。

NTP の前提条件

NTP を設定する場合は、NTP が動作している 1 つ以上のサーバに接続できなければなりません。

設定時の注意事項および制限事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

- 別のデバイスとの間にピア アソシエーションを設定できるのは、使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバのクライアントである場合）に限られます。
- ピアだけが設定されている場合、そのピアがサーバの役割を引き受け、バック アップとして使用される必要があります。サーバが 2 台ある場合、一部のデバイスが一方のサーバに接続し、残りのデバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピア アソシエーションを設定すると、信頼性の高い NTP 構成になります。
- サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定する必要があります。
- 設定できる NTP エンティティ（サーバおよびピア）は最大 64 です。

デフォルト設定

次のテーブルは、CDP および NTP パラメータのデフォルト設定をリスト表示しています。

パラメータ	デフォルト
NTP	イネーブル

NTP サーバおよびピアの設定

この手順を使用して、NTP サーバとピアを設定します。

はじめる前に

- NTP を設定するには、IPv4 アドレスまたはドメイン ネーム サーバ（DNS）名を使用します。

手順の概要

1. **config t**
2. **ntp server** {*ip-address* | *dns-name*}
3. **ntp peer** {*ip-address* | *dns-name*}
4. **show ntp peers**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**ntp server** {*ip-address* | *dns-name*} **Example:** n1000v(config)# ntp server 192.0.2.10	1 つのサーバと 1 つのサーバ アソシエーションを形成します。
ステップ 3	**ntp peer** {*ip-address* | *dns-name*} n1000v(config)# ntp peer 2001:0db8::4101	1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。
ステップ 4	**show ntp peers** **Example:** n1000v(config)# show ntp peers	（任意）設定済みのサーバおよびピアを表示します。 **（注）**　ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。
ステップ 5	**copy running-config startup-config** **Example:** n1000v(config-if)# 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。

次に、NTP サーバとピアを設定する例を示します。

```
n1000v# config t
n1000v(config)# ntp server 192.0.2.10
n1000v(config# ntp peer 2001:0db8::4101
```

NTP 統計情報またはセッションのクリア

NTP 統計情報またはセッションをクリアするには、次のコマンドを使用します。

コマンド	目的
clear ntp statistics	NTP 統計をクリアします。
clear ntp session	NTP セッションをクリアします。

NTP の設定確認

NTP の設定情報を表示するには、次のコマンドのいずれかを使用します。

コマンド	目的
show ntp peer-status	すべての NTP サーバおよびピアのステータスを表示します。

コマンド	目的
show ntp peers	すべての NTP ピアを表示します。
show ntp statistics {**io** | **local** | **memory** | **peer** {*ip-address* | *dns-name*}	NTP 統計を表示します。

NTP の設定例

NTP サーバの設定例を示します。

```
config t
ntp server 192.0.2.10
```

その他の関連資料

NTP に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.8-5）
- 「標準」（P.8-5）

関連資料

関連項目	参照先
インターフェイス	*『Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)』*
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	*『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

NTP の機能の履歴

ここでは、NTP 機能のリリース履歴を示します。

機能名	リリース	機能情報
NTP	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 9

ローカル SPAN および ERSPAN の設定

この章では、ローカルおよびカプセル化リモート（ER）スイッチド ポート アナライザ（SPAN）機能を設定して、トラフィックをモニタする方法を説明します。また、次の内容が含まれます。

- 「SPAN および ERSPAN について」（P.9-1）
- 「SPAN 注意事項および制約事項」（P.9-5）
- 「デフォルト設定」（P.9-6）
- 「SPAN の設定」（P.9-6）
- 「SPAN の設定確認」（P.9-20）
- 「設定例」（P.9-20）
- 「その他の関連資料」（P.9-22）
- 「SPAN および ERSPAN 機能の履歴」（P.9-23）

SPAN および ERSPAN について

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ます）では、Cisco SwitchProbe やその他のリモート モニタリング（RMON）プローブなどのネットワーク アナライザを使用して、ネットワーク トラフィックを分析できます。

SPAN では、1 つ以上のポートまたは 1 つ以上の VLAN 上のトラフィックをモニタして、ネットワーク アナライザが接続されている 1 つ以上の宛先ポートに、モニタされたトラフィックを送信できます。

ここでは、次の内容について説明します。

- 「SPAN ソース」（P.9-1）
- 「SPAN 宛先」（P.9-2）
- 「SPAN セッション」（P.9-5）

SPAN ソース

トラフィックをモニタできるモニタ元インターフェイスのことを SPAN ソースと呼びます。これには、イーサネット、仮想イーサネット、ポートチャネル、ポート プロファイル、および VLAN が含まれます。VLAN が SPAN ソースとして指定されている場合は、VLAN 内でサポートされているすべてのインターフェイスが SPAN ソースになります。ポート プロファイルが SPAN 送信元として指定されてい

る場合、ポート プロファイルを継承するすべてのポートが SPAN 送信元になります。トラフィックのモニタは、イーサネットおよび仮想イーサネットのソース インターフェイスの受信方向、送信方向、双方向のいずれでも行えます。

- 受信ソース（Rx）：このソース ポートを介してスイッチに入ってくるトラフィックが、SPAN 宛先ポートにコピーされます。
- 送信ソース（Tx）：このソース ポートを介してスイッチから出て行くトラフィックが、SPAN 宛先ポートにコピーされます。

SPAN 送信元の特性

ローカル SPAN 送信元には次の特性があります。

- ポート タイプは、イーサネット、仮想イーサネット、ポート チャネル、ポート プロファイル、VLAN のいずれでもかまいません。
- 宛先ポートまたはポート プロファイルにはできません。
- モニタするトラフィックの方向を、受信、送信、両方のいずれかに設定できます。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- VLAN の SPAN 送信元では、送信元 VLAN のすべてのアクティブ ポートが送信元ポートとして含まれます。
- ローカル SPAN 送信元は、宛先ポートと同じホスト（VEM）上にある必要があります。
- ポート プロファイル送信元の場合、ポート プロファイルに接続しているすべてのアクティブ インターフェイスが送信元ポートとして含まれます。

SPAN 宛先

SPAN 宛先とは、送信元ポートをモニタするインターフェイスを指します。ここでは、次の内容について説明します。

- 「ローカル SPAN 宛先の特性」（P.9-2）
- 「ERSPAN 宛先の特性」（P.9-3）

ローカル SPAN 宛先の特性

各ローカル SPAN セッションが、ソース ポートまたはソース VLAN から送られてくるトラフィックのコピーを受信する少なくとも 1 つの宛先ポート（モニタリング ポートとも呼ばれます）を持っていなければなりません。宛先ポートの特性は、次のとおりです。

- 物理または仮想イーサネット ポート、ポート チャネル、ポート プロファイルのいずれでもかまいません。
- 送信元ポートまたはポート プロファイルにはできません。
- いずれかの SPAN セッションの送信元 VLAN または送信元ポート プロファイルに属する場合、送信元リストから除外され、モニタされません。
- 同じ VEM モジュールのすべてのモニタ対象送信元ポートの送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ型の場合、輻輳が発生する可能性があります。輻輳が発生すると、1 つまたは複数の送信元ポートでのトラフィック転送に影響を及ぼす可能性があります。
- プライベート VLAN モードには設定できません。

- 宛先ポートは同じホスト（VEM）上の送信元のみモニタできます。図 9-1、「ローカル SPAN」を参照してください。
- アクセス モードの宛先ポートは、すべての VLAN のモニタ対象トラフィックを受信します。
- トランク モードの宛先ポートは、トランク設定で許可されている VLAN のモニタ対象トラフィックのみ受信します。

ERSPAN 宛先の特性

- ERSPAN 宛先は、IP アドレスによって指定されます。
- ERSPAN では、送信元 SPAN インターフェイスと宛先 SPAN インターフェイスは、IP ネットワークで相互接続された異なるデバイス上にある場合があります。ERSPAN トラフィックは GRE によってカプセル化されています。図 9-2、「ERSPAN」を参照してください。

ローカル SPAN

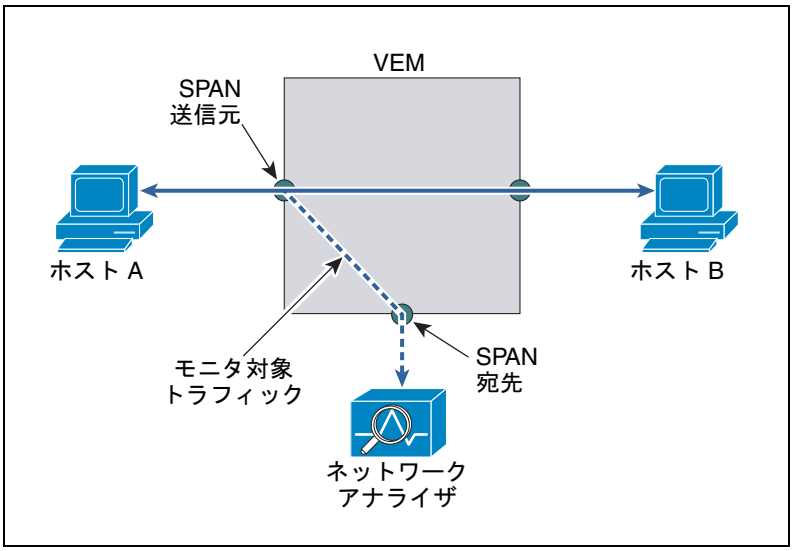
ローカル SPAN では、送信元インターフェイスと宛先インターフェイスは同じ VEM 上にあります。ネットワーク アナライザは、SPAN 宛先ポートに直接接続しています。SPAN 送信元は、ポート、VLAN インターフェイス、またはポート プロファイルのいずれかです。宛先は、ポートまたはポート プロファイルのいずれかです。

図 9-1 では、ホスト A から送信されたトラフィックが、SPAN 送信元インターフェイスで受信されます。トラフィック（ACL、QoS など）は、通常どおり処理されます。その後、トラフィックが複製されます。元のパケットは、ホスト B に対して転送されます。複製されたパケットは、モニタが接続されている宛先 SPAN インターフェイスに送信されます。

ローカル SPAN は、1 つ以上の宛先ポートに複製できます。トラフィックをフィルタリングできるため、必要なトラフィックだけが宛先 SPAN インターフェイスを送信します。

ローカル SPAN は、BPDU を含む送信元インターフェイスで受信されるすべてのトラフィックをモニタできます。

図 9-1　ローカル SPAN

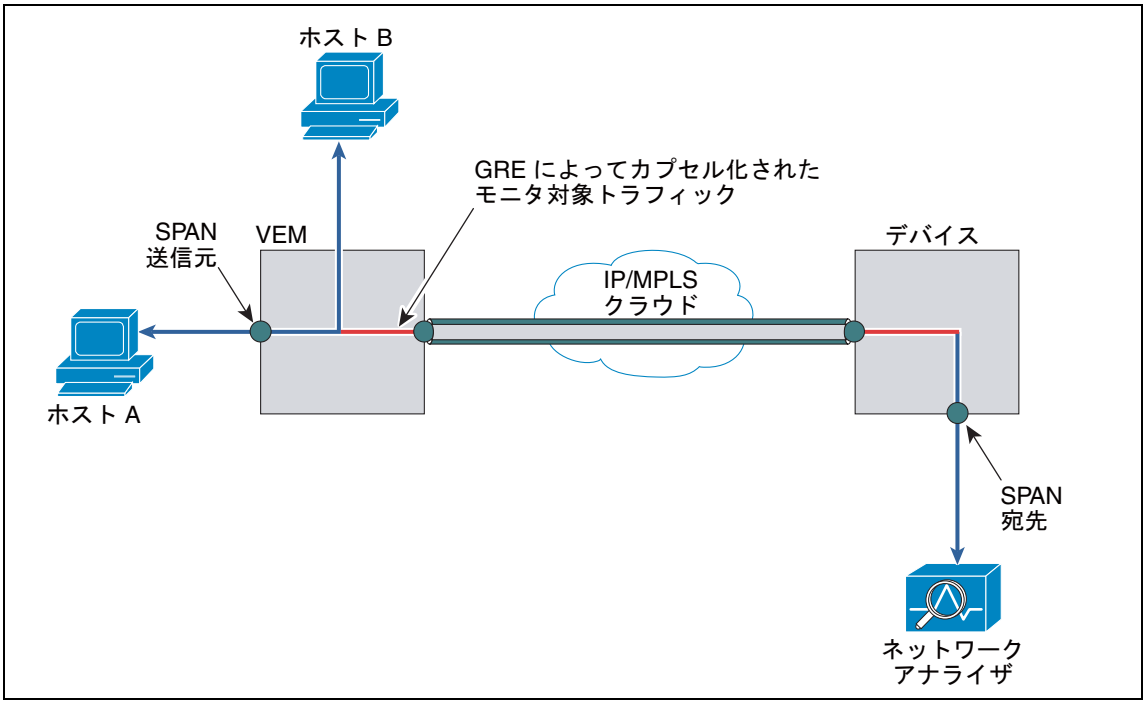


カプセル化リモート SPAN

カプセル化リモート（ER）SPAN は、IP ネットワーク全体の複数のネットワーク デバイスのトラフィックをモニタし、カプセル化エンベロープにあるトラフィックを宛先アナライザに送信します。これとは対照的に、ローカル SPAN は、IP ネットワーク経由でトラフィックを転送できません。ERSPAN を使用して、リモートでトラフィックをモニタできます。ERSPAN 送信元は、ポート、VLAN、またはポート プロファイルのいずれかです。

図 9-2 では、ホスト A の入出力トラフィックが ERSPAN によってモニタされています。カプセル化された ERSPAN パケットは、ルーティングされたネットワーク経由で、ホスト A から宛先デバイスにルーティングされます。宛先デバイスではパケットのカプセルが解除されて、接続しているネットワーク アナライザに転送されます。宛先は送信元と同じ L2 ネットワークにすることもできます。

図 9-2　ERSPAN



ネットワーク解析モジュール

Cisco ネットワーク解析モジュール（NAM）を使用して ERSPAN データソースをモニタし、アプリケーション パフォーマンス、トラフィック、およびパケット ヘッダーを分析することもできます。

NAM を使用して Cisco Nexus 1000V ERSPAN データソースをモニタする手順については、『*Cisco Nexus 1010 Network Analysis Module Installation and Configuration Note, 5.1*』を参照してください。

SPAN セッション

VEM には最大 64 の SPAN セッション（ローカル SPAN と ERSPAN の合計）を作成できます。

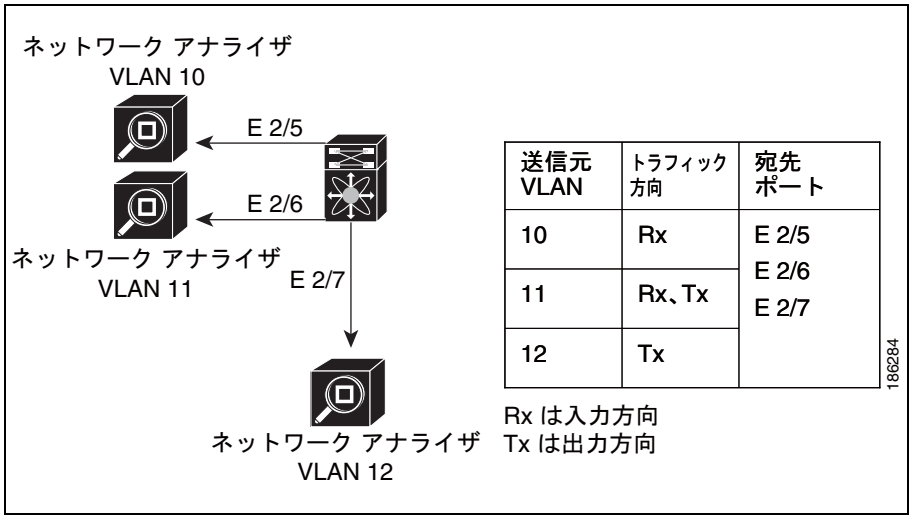
管理者は、終端ボックス側でのトラフィックの ERSPAN ストリームを区別するために、カプセル化されたフレームの ERSPAN ヘッダーに追加される ERSPAN セッション ID を設定する必要があります。フロー ID 番号の範囲を設定することもできます。詳細については、「許可される ERSPAN フロー ID の設定」（P.9-19）を参照してください。

トランク ポートが SPAN 送信元および宛先として設定されている場合、許可された中から宛先ポートに送信する VLAN をフィルタリングできます。送信元と宛先の両方を VLAN を許可するように設定する必要があります。

図 9-3 は、トラフィックが 3 つの VLAN から指定された 3 つの宛先ポートにコピーされる VLAN ベースの SPAN 設定の例を示しています。各宛先ポートで許可する VLAN を選択して、トラフィックの送信を制限できます。図 9-3 では、デバイスは各宛先ポートの 1 つの VLAN からパケットを送信します。この例の宛先は、許可 VLAN が設定されたトランクです。

（注）　VLAN ベースの SPAN セッションでは、パケットが宛先で必要かどうかに関係なく、すべての送信元パケットがすべての宛先にコピーされます。VLAN トラフィック フィルタリングは、送信宛先ポートで実行されます。

図 9-3　VLAN ベースの SPAN の設定例



SPAN 注意事項および制約事項

SPAN に関する設定時の注意事項および制約事項は、次のとおりです。

- 最大 64 の SPAN セッション（ローカル SPAN と ERSPAN）を VSM で設定できます。
- 最大 32 の送信元 VLAN がセッションで許可されます。
- 最大 32 の宛先がローカル SPAN セッションで許可されます。
- 最大 128 の送信元インターフェイスがセッションで許可されます。

注意　**過負荷の可能性**
アップリンク ポートの過負荷を回避するには、ERSPAN の設定、特に送信元 VLAN の設定時には注意が必要です。

- ポートは最大 4 つの SPAN セッションで設定できます。
- 1 つの SPAN セッションで使用される宛先ポートは、別の SPAN セッションの宛先ポートとしても使用できません。
- ポートを送信元ポートと宛先ポートの両方として設定することはできません。
- SPAN セッションでは、送信元ポートが受信したパケットは、そのポートで送信されるものではなくても複製される可能性があります。たとえば、次のような場合です。
  - 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
- 送受信の両方が設定された同じ VLAN でスイッチされる VLAN SPAN セッションの場合、宛先ポートから 2 つのパケット（受信から 1 つ、送信から 1 つ）が転送されます。

デフォルト設定

表 9-1 に、SPAN のデフォルト設定を示します。

表 9-1　SPAN のデフォルト

パラメータ	デフォルト
State	SPAN セッションはシャット ステートで作成されます。
Description	ブランク
Traffic direction for source interface or port profile	両方
Traffic direction for source VLAN	受信（入力または RX）

SPAN の設定

この項では、SPAN を設定する方法を説明し、次の手順が含まれています。

- 「ローカル SPAN セッションの設定」（P.9-7）
- 「ERSPAN ポート プロファイルの設定」（P.9-9）
- 「ERSPAN セッションの設定」（P.9-13）
- 「SPAN セッションのシャットダウン」（P.9-16）
- 「SPAN セッションの再開」（P.9-17）
- 「SPAN の設定確認」（P.9-20）

ローカル SPAN セッションの設定

この手順を使用して、SPAN セッションを設定します。

（注）　ERSPAN を設定している場合は、「ERSPAN セッションの設定」（P.9-13）の手順を参照してください。

はじめる前に

- EXEC モードで CLI にログインしていること。
- 設定する SPAN セッションの数を確認します。
- 送信元および宛先ポートは、アクセスまたはトランク モードで設定しておきます。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。
- デフォルトでは、SPAN セッションはシャット ステートで作成されます。
- 既存の SPAN セッションを作成する場合は、追加の設定がセッションに追加されます。確実にセッションの以前の設定をクリアするには、まず、セッションを削除する必要があります（ステップ 2 の **no monitor session** を参照）。
- この手順では、SPAN セッションをモニタ コンフィギュレーション モードで作成してから、許可される VLAN をインターフェイス コンフィギュレーション モードで設定します。許可される VLAN の設定は省略可能です。

手順の概要

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number*
4. **description** *description*
5. **source** {**interface** {*type*} {*id* | *range*} | **vlan** {*id* | *range*} | **port-profile** {*name*}} [**rx** | **tx** | **both**]
6. （任意）ステップ 5 を繰り返して、追加の SPAN 送信元を設定します。
7. （任意）**filter vlan** {*number* | *range*}
8. （任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。
9. **destination** {**interface** {*type*} {*id* } | **port-profile** {*name*}}
10. （任意）ステップ 9 を繰り返して、すべての SPAN 宛先ポートを設定します。
11. **no shut**
12. （任意）**exit**
13. （任意）**show monitor session** *session-number*
14. （任意）`show interface` {*type*} {*id*} **switchport**
15. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**no monitor session** *session-number* **Example:** `n1000v(config)# no monitor session 3`	指定されたセッションをクリアします。

ステップ 3	**monitor session** *session-number*
	
	Example:
	`n1000v(config)# monitor session 3`
	`n1000v(config-monitor)#`
		任意のセッション番号でセッションを作成して、CLI モニタ コンフィギュレーション モードに切り替え、セッションを設定します。

ステップ 4	**description** *description* **Example:** `n1000v(config-monitor)# description my_span_session_3`	指定された SPAN セッションの場合は、説明を追加します。 • description：最大 32 文字の英数字 デフォルト = ブランク（説明なし）

ステップ 5	**source** {**interface** {*type*} {*id*} |
	vlan {*id* | *range*} |
	port-profile {*name*}} [**rx** | **tx** | **both**]
	
	Example 1:
	`n1000v(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	Example 2:
	`n1000v(config-monitor)# source interface port-channel 2`
	
	Example 3:
	`n1000v(config-monitor)# source interface vethernet 12 both`
	
	Example 4:
	`n1000v(config-monitor)# source vlan 3, 6-8 tx`
	
	Example 5:
	`n1000v(config-monitor)# source port-profile my_port_profile`
		指定されたセッションの場合は、モニタするトラフィックの送信元と方向を設定します。
		• type：インターフェイス タイプ（イーサネットまたは vEthernet）を指定します。
		• ID：モニタする vEthernet 番号、イーサネット スロット/ポート、または VLAN ID を指定します。
		• range：モニタする VLAN の範囲を指定します。
		• name：既存のポート プロファイルの名前を指定します。このポート プロファイルは、「ERSPAN ポート プロファイルの設定」（P.9-9）で定義されている IP ネットワークを介して ERSPAN パケットを伝送するために作成されているポート プロファイルとは異なります。
		• traffic direction：トラフィック モニタリングの方向を指定します。
		– 受信（rx）（VLAN デフォルト）
		– 送信（tx）
		– 両方（デフォルト）

ステップ 6	（任意）ステップ 5 を繰り返して、追加の SPAN 送信元を設定します。	
ステップ 7	**filter vlan** {*id* | *range*} **Example:** `n1000v(config-monitor)# filter vlan 3-5, 7`	（任意）指定された SPAN セッションの場合、送信元 VLAN の中からフィルタを設定します。
ステップ 8	（任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。	

	コマンド	目的
ステップ 9	**destination** {**interface** {*type*} {*id* | *range*} | **port-profile** {*name*}} **Example:** `n1000v(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	指定された SPAN セッションの場合は、コピーされた送信元パケットの宛先を設定します。 • type：インターフェイス タイプ（イーサネットまたは vEthernet）を指定します。 • ID：モニタする vEthernet 番号、またはイーサネット スロット/ポートを指定します。 • name：モニタするポート プロファイルの名前を指定します。 （注）　SPAN 宛先ポートはアクセスまたはトランク ポートとして設定しておく必要があります。
ステップ 10	（任意）ステップ 9 を繰り返して、すべての SPAN 宛先ポートを設定します。	
ステップ 11	**no shut** **Example:** `n1000v(config-monitor)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。

ステップ 12	**exit**
	
	Example:
	`n1000v(config-monitor)# exit`
	`n1000v(config)#`
		（任意）モニタ コンフィギュレーション モードを終了して、CLI コンフィギュレーション モードに切り替えます。

ステップ 13	**show monitor session** *session-number* **Example:** `n1000v(config-if)# show monitor session 3`	（任意）設定済みのモニタ セッションを表示します。
ステップ 14	**show interface** {*type*} {*id*} **switchport** **Example:** `n1000v(config-if)# show interface ethernet 2/5 switchport`	（任意）許可 VLAN を含む、設定済みのポートを表示します。
ステップ 15	**copy running-config startup-config** **Example:** `n1000v(config-if)# 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。

ERSPAN ポート プロファイルの設定

この手順を使用して、VSM 上のポート プロファイルを設定し、ERSPAN パケットを IP ネットワーク経由で、リモート宛先アナライザに転送します。

はじめる前に

- EXEC モードで CLI にログインしていること。
- vCenter Server のすべてのホストに対して、この設定を完了する必要があります。
- このポート プロファイルに使用する名前を確認します。

（注）　ポート プロファイル名は、VMKNIC を設定するために使用されます。VMKNIC は、ERSPAN カプセル化 IP パケットを送信するために各 ESX ホストで必要であり、ERSPAN 宛先 IP アドレスへの IP 接続が必要です。

- このプロファイルをマッピングする VMware ポート グループ名を確認します。
- 新しい仮想アダプタを追加するための VMware マニュアルを手元に用意します。
- ERSPAN 宛先に IP トラフィックを送信するシステム VLAN をすでに作成していること、およびこの設定で使用される VLAN ID を確認します。

  システム 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。
- ERSPAN に使用するポート プロファイルは、レイヤ 3 コントロール用に設定する必要があります。この手順には、この設定を行うステップも含まれています。
- このレイヤ 3 コントロール ポート プロファイルに割り当て可能な VM カーネル NIC は、1 つのホストにつき 1 つだけです。
  - 複数の VMware カーネル NIC が同じホストに割り当てられている場合は、最初に割り当てられたものが有効になります。2 番目はレイヤ 3 制御 VMware カーネル NIC とは見なされません。
  - 2 つの VMware カーネル NIC が同じホストに割り当てられている場合に、2 番目に割り当てられたものを削除しても、最初に割り当てられたものが VEM によって使用されることはありません。代わりに、VMware カーネル NIC を両方とも削除してから 1 つだけをもう一度割り当てる必要があります。
- ポート プロファイルは、アクセス ポート プロファイルであることが必要です。トランク ポート プロファイルであってはなりません。ここで説明する手順の中で、ポート プロファイルをアクセス ポート プロファイルとして設定します。
- レイヤ 3 制御ポート プロファイルの作成方法の詳細については、「レイヤ 3 コントロール用のポート プロファイルの作成」（P.3-10）の手順を参照してください。

手順の概要

1. **config t**
2. **port-profile** *name*
3. **capability l3control**
4. **vmware port-group** *name*
5. **switchport mode access**
6. **switchport access vlan** *id*
7. **no shutdown**
8. **system vlan** *id*
9. **state enabled**
10. （任意）**show port-profile name** *name*
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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** *port_profile_name*
	
	Example:
	`n1000v(config)# port-profile erspan_profile`
	`n1000v(config-port-prof)#`
		ポート プロファイルを作成し、指定されたポート プロファイルの CLI グローバル コンフィギュレーション モードに切り替えます。実行コンフィギュレーションに、ポート プロファイルを保存します。
		
		ポート プロファイル名は最大 80 文字で指定し、Cisco Nexus 1000V のポート プロファイルごとに一意である必要があります。

ステップ 3	**capability l3control**
	
	Example:
	`n1000v(config-port-prof)# capability l3control`
	`n1000v(config-port-prof)#`
		ポート プロファイルを設定して、ERSPAN トラフィックを転送し、実行コンフィギュレーションに保存します。

ステップ 4	**vmware port-group** *name*
	
	Example:
	`n1000v(config-port-prof)#vmware port-group erspan`
	`n1000v(config-port-prof)#`
		ポート プロファイルを VMware ポート グループとして指定し、このプロファイルがマッピングする VMware ポート グループ名を追加します。実行コンフィギュレーションに、設定を保存します。
		
		ポート プロファイルは、同じ名前の VMware ポート グループにマッピングされます。vCenter Server 接続が確立すると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。
		
		• **name** : ポート グループ名。名前を指定しない場合は、ポート プロファイル名がポート グループ名となります。ポート プロファイルを異なるポート グループ名にマッピングする場合は、name オプションの後に別の名前を続けます。

ステップ 5	**switchport mode access**
	
	Example:
	`n1000v(config-port-prof)# switchport mode access`
	`n1000v(config-port-prof)#`
		インターフェイスがスイッチ アクセス ポート（デフォルト）であることを指定します。

ステップ 6	**switchport access vlan** *id*
	
	Example 1:
	`n1000v(config-port-prof)# switchport access vlan 2`
	`n1000v(config-port-prof)#`
		VLAN ID をこのポート プロファイルのアクセス ポートに割り当て、実行コンフィギュレーションに設定を保存します。
		
		この VLAN が ERSPAN 宛先に IP トラフィックを送信するために使用されます。

	コマンド	目的

ステップ 7	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		実行コンフィギュレーションのインターフェイスをイネーブルにします。

ステップ 8	**system vlan** *id*
	
	Example:
	`n1000v(config-port-prof)# system vlan 2`
	`n1000v(config-port-prof)#`
		システム VLAN ID をポート プロファイルに関連付け、実行コンフィギュレーションに保存します。
		アクセス ポートに割り当てられた VLAN ID と一致しなければなりません。一致しない場合は、次のエラー メッセージが表示されます。
		ERROR: System vlan being set does not match the switchport access vlan 2

ステップ 9	**state enabled**
	
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		実行コンフィギュレーションで、ポート プロファイルをイネーブルにします。
		これで、このポート プロファイルは、ERSPAN 送信元を持つすべての ESX ホストの ERSPAN パケットを送信できます。

ステップ 10	**show port-profile name** *port_profile_name*
	
	Example:
	`n1000v(config-port-prof)# show port-profile name erspan`
	`port-profile erspan`
	`  description:`
	`  status: enabled`
	`  capability uplink: no`
	`  capability l3control: yes`
	`  system vlans: 2`
	`  port-group: access`
	`  max-ports: 32`
	`  inherit:`
	`  config attributes:`
	`  switchport access vlan 2`
	`  no shutdown`
	`  evaluated config attributes:`
	`  switchport access vlan 2`
	`  no shutdown`
	`  assigned interfaces:`
	
	`n1000v(config-port-prof)#`
		（任意）指定されたポート プロファイルの設定を、実行コンフィギュレーションにあるとおりに表示します。

ステップ 11	**copy running-config startup-config**
	
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		（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。

ステップ 12	VMware のマニュアルを参照して、vSphere Client で、各 ESX ホストの VMKNIC を ERSPAN カプセル化パケットを送信するように設定します。必ず**新しい仮想アダプタ**として、VMKNIC がこのポート プロファイルを参照するようにします。この VMKNIC は ERSPAN 宛先 IP アドレスに IP 接続できる必要があります。	

ERSPAN セッションの設定

この手順を使用して、ERSPAN セッションを設定します。

（注）　ローカル SPAN を設定している場合は、「ローカル SPAN セッションの設定」（P.9-7）の手順を参照してください。

はじめる前に

- EXEC モードで CLI にログインしていること。
- 設定する SPAN セッションの数を確認します。
- 「ERSPAN ポート プロファイルの設定」（P.9-9）の手順を参照して、VSM の ERSPAN 対応ポートプロファイルを設定しておきます。
- 新しい仮想アダプタを追加するための VMware マニュアルを使用して、各 ESX ホスト上に必要な VMKNIC を設定しておきます。VMKNIC は ERSPAN カプセル化パケットを送信するために、ERSPAN 宛先 IP アドレスに IP 接続できる必要があります。
- デフォルトでは、SPAN セッションはシャット ステートで作成されます。
- 既存の SPAN セッションを作成する場合は、追加の設定がセッションに追加されます。確実にセッションの以前の設定をクリアするには、まず、セッションを削除する必要があります（ステップ 2 の **no monitor session** を参照）。
- この手順には、ERSPAN 送信元コンフィギュレーション モード（config-erspan-source）での SPAN セッションの作成が含まれます。

手順の概要

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number* **type erspan-source**
4. **description** *description*
5. **source** {**interface** ***type*** {*number* | *range*} | **vlan** {*number* | *range*} | **port-profile** *name*}} [**rx** | **tx** | **both**]
6. （任意）ステップ 5 を繰り返して、追加の ERSPAN 送信元を設定します。
7. （任意）**filter vlan** {*number* | *range*}
8. （任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。
9. **destination ip** *ip_address*
10. （任意）**ip ttl** *ttl_value*
11. （任意）**ip prec** *ipp_value*
12. （任意）**ip dscp** *dscp_value*
13. （任意）**mtu** *mtu_value*
14. （任意）**header-type** *value*
15. **erspan-id** *flow_id*
16. **no shut**

17.（任意）**show monitor session session_id**

18.（任意）**exit**

19.（任意）copy running-config startup-config

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**no monitor session** *session-number* **Example:** `n1000v(config)# no monitor session 3`	指定されたセッションをクリアします。

ステップ 3	**monitor session** *session-number* **type erspan-source**
	
	Example:
	`n1000v(config)# monitor session 3 type erspan`
	`n1000v(config-erspan-source)#`
		任意のセッション番号でセッションを作成し、CLI ERSPAN 送信元コンフィギュレーション モードに切り替えます。この設定は、実行コンフィギュレーションに保存されます。

ステップ 4	**description** *description*
	Example:
	`n1000v(config-erspan-src)# description my_erspan_session_3`
	`n1000v(config-erspan-src)#`
		指定された ERSPAN セッションの場合、説明を追加して、実行コンフィギュレーションに保存します。
		• description：最大 32 文字の英数字
		デフォルト = ブランク（説明なし）

ステップ 5	**source** {**interface** *type* {*number* | *range*} | **vlan** {*number* | *range*} | **port-profile** *name*}} [**rx** | **tx** | **both**]
	
	Example 1:
	`n1000v(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	Example 2:
	`n1000v(config-erspan-src)# source interface port-channel 2`
	
	Example 3:
	`n1000v(config-erspan-src)# source interface vethernet 12 both`
	
	Example 4:
	`n1000v(config-erspan-src)# source vlan 3, 6-8 tx`
	
	Example 5:
	`n1000v(config-erspan-src)# source port-profile my_port_profile`
		指定されたセッションの場合、モニタする送信元とトラフィックの方向を設定し、実行コンフィギュレーションに保存します。
		• type：インターフェイス タイプ（イーサネット、ポートチャネル、仮想イーサネット）を指定します。
		• number：モニタするインターフェイス スロットおよびポートまたはポート範囲、VLAN 番号または VLAN 範囲を指定します。
		• name：既存のポート プロファイルの名前。
		• traffic direction：次の方向のいずれかになるように、トラフィック モニタを指定します。
		– 受信（rx）（VLAN デフォルト）
		– 送信（tx）
		– 両方（インターフェイスおよびポート プロファイルのデフォルト値）

ステップ 6	（任意）ステップ 5 を繰り返して、追加の ERSPAN 送信元を設定します。	

	コマンド	目的
ステップ 7	**filter vlan** {*number* | *range*} **Example:** `n1000v(config-erspan-src)# filter vlan 3-5, 7`	（任意）指定された ERSPAN セッションの場合、モニタする VLAN、VLAN リスト、VLAN 範囲のいずれかを設定して、実行コンフィギュレーションに保存します。 モニタ ポート上では、VLAN フィルタ リストと一致する VLAN からのトラフィックだけが宛先に複製されます。
ステップ 8	（任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。	

ステップ 9	**destination ip** *ip_address*
	
	Example:
	`n1000v(config-erspan-src)# destination ip 10.54.54.1`
	`n1000v(config-erspan-src)#`
		このモニタ セッションでカプセル化されたトラフィックが送信されるホストの IP アドレスを設定し、実行コンフィギュレーションに保存します。

ステップ 10	**ip ttl** *ttl_value*
	
	Example:
	`n1000v(config-erspan-src)# ip ttl 64`
	`n1000v(config-erspan-src)#`
		（任意）このモニタ セッションでの ERSPAN パケットの IP 存続可能時間の値（1 ～ 255）を指定し、実行コンフィギュレーションに保存します。
		
		デフォルトは 64 です。

ステップ 11	**ip prec** *precedence_value*
	
	Example:
	`n1000v(config-erspan-src)# ip prec 1`
	`n1000v(config-erspan-src)#`
		（任意）このモニタ セッションでの ERSPAN パケットの IP Precedence 値（0 ～ 7）を指定し、実行コンフィギュレーションに保存します。
		
		デフォルト値は 0 です。

ステップ 12	**ip dscp** *dscp_value*
	
	Example:
	`n1000v(config-erspan-src)# ip dscp 24`
	`n1000v(config-erspan-src)#`
		（任意）このモニタ セッションでの ERSPAN パケットの IP DSCP 値（0 ～ 63）を指定し、実行コンフィギュレーションに保存します。
		
		デフォルトは 0 です。

ステップ 13	**mtu** *mtu_value*
	
	Example:
	`n1000v(config-erspan-src)# mtu 1000`
	`n1000v(config-erspan-src)#`
		（任意）このモニタ セッションでの ERSPANed パケットの MTU サイズ（50 ～ 1500）を指定し、実行コンフィギュレーションに保存します。1500 の MTU サイズの制限には、ERSPAN によってモニタ対象パケットに追加される 50 バイトのオーバーヘッドが含まれます。このサイズより大きいパケットは切り捨てられます。
		
		デフォルト値は 1500 です。

ステップ 14	**header-type** *value*
	
	Example:
	`n1000v(config-erspan-src)# header-type 2`
	`n1000v(config-erspan-src)#`
		（任意）このモニタ セッションの ERSPAN のカプセル化に使用される ERSPAN ヘッダー タイプ（2 または 3）を指定します。
		• 2 = ERPSPANv2 ヘッダー タイプ（デフォルト）
		• 3 = ERSPANv3 ヘッダー タイプ（NAM 設定で使用されます。他のタイプの宛先は、デフォルト v2 ヘッダーでのみ動作します）。

	コマンド	目的
ステップ 15	**erspan-id** *flow_id* **Example:** `n1000v(config-erspan-src)# erspan-id 51`	ERSPAN ID（1 ～ 1023）をセッション設定に追加して、実行コンフィギュレーションに保存します。 セッション ERSPAN ID を、カプセル化されたフレームの ERSPAN ヘッダーに追加し、終端ボックスで使用して、さまざまなトラフィックの ERSPAN ストリームを識別できます。

ステップ 16	`no shut`
	
	Example:
	`n1000v(config-erspan-src)# no shut`
		ERSPAN セッションをイネーブルにし、実行コンフィギュレーションに保存します。
		デフォルトでは、セッションはシャット ステートで作成されます。

ステップ 17	**show monitor session** *session_id* **Example:** `n1000v(config-erspan-src)# show monitor session 3`	（任意）実行コンフィギュレーションにあるとおりに、ERSPAN セッション設定を表示します。
ステップ 18	**copy running-config startup-config** **Example:** `n1000v(config-erspan-src)# 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。

SPAN セッションのシャットダウン

この手順を使用して、SPAN セッションのパケットのコピーを中止します。1 つの送信元および宛先からのパケットのコピーを中止し、別の送信元および宛先で再開できます。

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。
- シャットダウンする SPAN セッションを確認します。
- グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、SPAN セッションをシャットダウンできます。

手順の概要

グローバル コンフィギュレーション モードから：

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**} **shut**
3. **show monitor**
4. **copy running-config startup-config**

モニタ コンフィギュレーション モードから：

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**} **[type erspan-source]**

3. **shut**
4. **show monitor**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**monitor session** {session-number | session-range | **all**} **shut** **Example:** n1000v(config)# monitor session 3 shut n1000v(config)# **Example:** n1000v(config)# monitor session 3 n1000v(config-monitor)# shut	グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、指定された SPAN モニタ セッションをシャットダウンします。 • session-number : 特定の SPAN セッション番号を指定します。 • session range : SPAN セッションの範囲を指定します（許可されている範囲は 1 ～ 64）。 • all : すべての SPAN モニタ セッションを指定します。
ステップ 3	**show monitor** **Example:** n1000v(config-monitor)# show monitor	（任意）SPAN セッションの状況を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config-monitor)# 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。

SPAN セッションの再開

この手順を使用して、SPAN セッションのパケットのコピーを再開します。1 つの送信元および宛先からのパケットのコピーを中止し、別の送信元および宛先で再開できます。

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。
- 設定する SPAN セッションを確認します。
- グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、SPAN セッションを再開できます。

手順の概要

グローバル コンフィギュレーション モードから：

1. **config t**
2. **no monitor session** {*session-number* | *session-range* | **all**} **shut**
3. **show monitor**
4. **copy running-config startup-config**

モニタ コンフィギュレーション モードから：

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**} **[type erspan-source]**
3. **no shut**
4. **show monitor**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	[**no**] **monitor session** {*session-number* *session-range* | **all**} **shut**
	
	Example:
	`n1000v(config)# no monitor session 3 shut`
	`n1000v(config)#`
	
	Example:
	`n1000v(config)# monitor session 3`
	`n1000v(config-monitor)# no shut`
		グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、指定された SPAN モニタ セッションを開始します。
		• session-number：特定の SPAN セッション番号を指定します。
		• session range：SPAN セッションの範囲を指定します（許可されている範囲は 1 ～ 64）。
		• all：すべての SPAN モニタ セッションを指定します。

ステップ 3	**show monitor** **Example:** `n1000v(config-monitor)# show monitor`	（任意）確認のために、すべての設定済み SPAN セッションのステータスを表示します。
ステップ 4	**show monitor session** *session-id* **Example:** `n1000v(config-monitor)# show monitor session 3`	（任意）確認のために、特定の SPAN セッションの詳細な設定およびステータスを表示します。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v(config-monitor)# 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。

許可される ERSPAN フロー ID の設定

ここでは、ERSPAN セッションに割り当て可能なフロー ID の範囲を限定する手順を説明します。

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。
- 許容される ERSPAN フロー ID の範囲がわかっている必要があります。
- 使用可能な ERSPAN フロー ID は 1 ～ 1023 です。この手順を使用すると、使用可能な ID の範囲を制限できます。

手順の概要

1. **config t**
2. **[no] limit-resource erspan-flow-id minimum** *min_val* **maximum** *max_val*
3. **show running monitor**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**[no] limit-resource erspan-flow-id minimum** *min_val* **maximum** *max_val*
	
	Example:
	`n1000v(config)# limit-resource erspan-flow-id minimum 20 maximum 40`
	`n1000v(config)#`
	
	Example:
	`n1000v(config)# no limit-resource erspan-flow-id`
	`n1000v(config)#`
		割り当て可能な ERSPAN フロー ID の範囲を限定します。
		• 有効な範囲 = 1 ～ 1023
		• デフォルト：
		　– min_val = 1
		　– max_val = 1023
		このコマンドの no バージョンは設定値を削除し、デフォルト値に戻します。

ステップ 3	**show running monitor** **Example:** `n1000v(config-monitor)# show monitor session 3`	（任意）確認のために、デフォルトの limit-resource erspan-flow-id 値に対する変更を表示します。
ステップ 4	**copy running-config startup-config** **Example:** `n1000v(config-monitor)# 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。

SPAN の設定確認

SPAN 設定を確認するには、次のコマンドを使用します。

コマンド	目的
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	SPAN セッションの設定を表示します。
show monitor	イーサネット SPAN 情報を表示します。
module vem *module-number* **execute vemcmd show span**	VEM モジュールで設定された SPAN セッションを表示します。
show port-profile name *port_profile_name*	ポート プロファイルを表示します。

設定例

この項には、次の設定例が含まれています。

- 「SPAN セッションの設定例」（P.9-20）
- 「ERSPAN セッションの設定例」（P.9-21）

SPAN セッションの設定例

SPAN セッションを設定する手順は、次のとおりです。

ステップ 1　アクセス モードまたはトランク モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

```
n1000v# config t
  n1000v(config)# interface ethernet 2/5
    n1000v(config-if)# switchport
    n1000v(config-if)# switchport mode trunk
    n1000v(config-if)# no shut
    n1000v(config-if)# exit
  n1000v(config)#
```

ステップ 2　SPAN セッションを設定します。

```
  n1000v(config)# no monitor session 1
  n1000v(config)# monitor session 1
    n1000v(config-monitor)# source interface ethernet 2/1-3
    n1000v(config-monitor)# source interface port-channel 2
    n1000v(config-monitor)# source port-profile my_profile_src
    n1000v(config-monitor)# source vlan 3, 6-8 tx
    n1000v(config-monitor)# filter vlan 3-5, 7
    n1000v(config-monitor)# destination interface ethernet 2/5
    n1000v(config-monitor)# destination port-profile my_profile_dst
    n1000v(config-monitor)# no shut
    n1000v(config-monitor)# exit
  n1000v(config)# show monitor session 1
  n1000v(config)# copy running-config startup-config

n1000v(config)# show monitor session 1
   session 1
```

```
---------------
type              : local
state             : up
source intf       :
    rx            : Eth2/1 Eth2/2 Eth2/3
    tx            : Eth2/1 Eth2/2 Eth2/3
    both          : Eth2/1 Eth2/2 Eth2/3
source VLANs      :
    rx            :
    tx            : 3,6,7,8
    both          :
source port-profile :
    rx            : my_profile_src
    tx            : my_profile_src
    both          : my_profile_src
filter VLANs      : 3,4,5,7
destination ports : Eth2/5
destination port-profile : my_profile_dst

n1000v# module vem 3 execute vemcmd show span

VEM SOURCE IP NOT CONFIGURED.

HW SSN ID   ERSPAN ID   HDR VER   DST LTL/IP
        1                 local   49,51,52,55,56
```

ERSPAN セッションの設定例

次の例では、Cisco Nexus 1000V の送信元イーサネット インターフェイスおよび宛先 IP アドレスに対する ERSPAN セッションを作成する方法を示します。宛先 IP に到達するパケットは、ヘッダーの ID 999 で特定されます。

```
monitor session 2 type erspan-source
source interface ethernet 3/3
source port-profile my_profile_src
destination ip 10.54.54.1
erspan-id 999
mtu 1000
no shut

show monitor session 2
   session 2
---------------
type              : erspan-source
state             : up
source intf       :
    rx            : Eth3/3
    tx            : Eth3/3
    both          : Eth3/3
source VLANs      :
    rx            :
    tx            :
    both          :
source port-profile :
    rx            : my_profile_src
    tx            : my_profile_src
    both          : my_profile_src
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
ERSPAN Header Type: 2

module vem 3 execute vemcmd show span

VEM SOURCE IP: 10.54.54.10

HW SSN ID   ERSPAN ID   HDR VER   DST LTL/IP
        1                 local   49,51,52,55,56
        2         999         2   10.54.54.1
```

その他の関連資料

SPAN の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.9-22）
- 「標準」（P.9-22）

関連資料

関連項目	参照先
ポート プロファイルの設定	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』
インターフェイス コンフィギュレーション	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

SPAN および ERSPAN 機能の履歴

ここでは、SPAN および ERSPAN 機能のリリース履歴を示します。

機能名	リリース	機能情報
ローカル SPAN および ERSPAN 送信元としてのポート プロファイル	4.2(1)SV1(4)	ローカル SPAN および ERSPAN モニタ トラフィックの送信元としてのポート プロファイルを指定できます。
ERSPAN データソースに対する NAM サポート	4.0(4)SV1(3)	NAM サポートが追加されました。
ERSPAN タイプ III ヘッダー	4.0(4)SV1(3)	ERSPAN タイプ III ヘッダー形式が追加されました。
SPAN および ERSPAN	4.0(4)SV1(1)	SPAN および ERSPAN が追加されました。

SPAN および ERSPAN 機能の履歴

CHAPTER 10

SNMP の設定

この章では、ユーザ、メッセージ暗号化、通知、TCP での認証などを含む SNMP を設定する方法を説明します。

この章は、次の内容で構成されています。

- 「SNMP について」（P.10-1）
- 「注意事項および制約事項」（P.10-5）
- 「デフォルト設定」（P.10-5）
- 「SNMP の設定」（P.10-6）
- 「SNMP の設定確認」（P.10-13）
- 「SNMP の設定例」（P.10-13）
- 「その他の関連資料」（P.10-14）
- 「SNMP の機能の履歴」（P.10-16）

SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージ フォーマットを提供するアプリケーション層プロトコルです。SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。

ここでは、次の内容について説明します。

- 「SNMP 機能の概要」（P.10-1）
- 「SNMP 通知」（P.10-2）
- 「SNMPv3」（P.10-2）
- 「ハイ アベイラビリティ」（P.10-5）

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスの動作を制御およびモニタするためのシステム。

- SNMP エージェント：管理デバイス内部のソフトウェア コンポーネントで、デバイスに関するデータを維持し、必要に応じてこれらのデータを管理システムに伝えます。Cisco Nexus 1000V はエージェントと MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。
- Managed Information Base（MIB; 管理情報ベース）：SNMP エージェント上の管理対象オブジェクトのコレクション。

SNMP は、RFC 3411 ～ 3418 で規定されています。

（注）　SNMP Role Based Access Control（RBAC）はサポートされていません。

SNMPv1、SNMPv2c、および SNMPv3 です。SNMPv1 および SNMPv2c の両方により、コミュニティベースのセキュリティ形式の使用がサポートされています。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知によって、不正なユーザ認証、再起動、接続の終了、隣接ルータとの接続切断、またはその他の重要イベントを示すことができます。

SNMP 通知は、トラップまたは応答要求として生成されます。トラップは、エージェントからホスト レシーバ テーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。応答要求は、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても Acknowledgment（ACK; 確認応答）を送信しないからです。Cisco Nexus 1000V では、トラップを受信したかどうかを判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージの受信を確認します。応答を受信しなかった場合、Cisco Nexus 1000V は再度インフォーム要求を送信できます。

複数のホスト レシーバーに通知を送信するよう Cisco Nexus 1000V を設定できます。ホスト レシーバーの詳細については、「SNMP 通知レシーバーの設定」（P.10-8）を参照してください。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージの送信元が有効かどうかを判別します。
- 暗号化：許可されていない送信元により判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルは、セキュリティ モデル内で許可されたセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

ここでは、次の内容について説明します。

- 「SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル」（P.10-3）

- 「ユーザベースのセキュリティ モデル」（P.10-4）
- 「CLI および SNMP ユーザの同期」（P.10-4）
- 「グループベースの SNMP アクセス」（P.10-5）

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル
- authPriv：認証と暗号化両方を実行するセキュリティ レベル

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

表 10-1 に、セキュリティ モデルとセキュリティ レベルの組み合わせの意味を示します。

表 10-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	No	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）メッセージ ダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。Data Encryption Standard（DES; データ暗号規格）の 56 ビット暗号化、および Cipher Block Chaining（CBC; 暗号ブロック連鎖）DES（DES-56）標準に基づいた認証を提供します。

ユーザベースのセキュリティ モデル

SNMPv3 User-Based Security Model（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないこと、データ シーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

Cisco Nexus 1000V は、次の 2 つの SNMPv3 認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco Nexus 1000V は、SNMPv3 メッセージ暗号化用プライバシー プロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES を選択できます。**priv** オプションを **aes-128** トークンと併用すると、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合は、大文字と小文字を区別して、最大 64 文字の英数字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注）外部 AAA（認証、認可、アカウンティング）サーバを使用する SNMPv3 動作の場合は、外部 AAA サーバ上のユーザ コンフィギュレーションで、プライバシー プロトコルとして AES を使用する必要があります。

CLI および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中化できます。この中央集中型ユーザ管理により、Cisco Nexus 1000V の SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

Cisco Nexus 1000V は、次のようにユーザ設定を同期化します。

- **snmp-server user** コマンドで指定された認証パスフレーズが CLI ユーザのパスワードになります
- **username** コマンドで指定されたパスワードが SNMP ユーザの認証およびプライバシー パスフレーズになります。
- SNMP または CLI を使用してユーザを削除すると、SNMP と CLI の両方でユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- CLI から行ったロール変更（削除または変更）は、SNMP と同期します。

（注）　パスフレーズ/パスワードをローカライズド キー/暗号化形式で設定すると、Cisco Nexus 1000V はパスワードを同期化しません。

Cisco NX-OS はデフォルトで、同期したユーザ設定を 60 分間維持します。このデフォルト値の変更方法については、「AAA 同期時間の変更」（P.10-13）を参照してください。

グループベースの SNMP アクセス

（注）　グループが業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは読み取りアクセス権または読み取りと書き込みアクセス権を指定して定義します。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

ハイ アベイラビリティ

SNMP ではステートレス リスタートがサポートされています。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションを適用します。

注意事項および制約事項

SNMP に関する設定時の注意事項および制約事項は、次のとおりです。

- 一部の SNMP MIB に対する読み取り専用アクセスがサポートされています。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポート リストを参照してください。

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- SNMP Role Based Access Control（RBAC）はサポートされていません。
- SNMP 設定コマンドは、次の Cisco MIB でサポートされます。
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB

デフォルト設定

表 10-2 に、SNMP パラメータのデフォルト設定を示します。

表 10-2　デフォルトの SNMP パラメータ

パラメータ	デフォルト
ライセンス通知	イネーブル

SNMP の設定

ここでは、次の内容について説明します。

- 「SNMP ユーザの設定」（P.10-6）
- 「SNMP メッセージ暗号化の適用」（P.10-7）
- 「SNMP コミュニティの作成」（P.10-8）
- 「SNMP 通知レシーバーの設定」（P.10-8）
- 「通知ターゲット ユーザの設定」（P.10-9）
- 「SNMP 通知のイネーブル化」（P.10-9）
- 「インターフェイスに関する linkUp/linkDown 通知のディセーブル化」（P.10-11）
- 「TCP による SNMP のワンタイム認証のイネーブル化」（P.10-11）
- 「SNMP スイッチのコンタクトおよびロケーション情報の指定」（P.10-11）
- 「SNMP のディセーブル化」（P.10-12）
- 「AAA 同期時間の変更」（P.10-13）

（注）　この機能に対応する Cisco NX-OS コマンドは、Cisco IOS で使用されているコマンドと異なる場合があるので注意してください。

SNMP ユーザの設定

この手順を使用して、SNMP のユーザを設定します。

はじめる前に

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. **show snmp user**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(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	**snmp-server user** *name* [auth {**md5** | **sha**} *passphrase* [auto] [**p**riv [aes-128] *passphrase*] [engineID *id*] [localizedkey]] **Example:** switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh	認証およびプライバシー パラメータのある SNMP ユーザを設定します。パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字を区別します。**localizekey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	**show snmp user** **Example:** switch(config-callhome)# show snmp user	（任意）1 人または複数の SNMP ユーザに関する情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# 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。

次の例では、SNMP のコンタクトおよびロケーション情報を設定する方法を示します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを強化する場合、Cisco Nexus 1000V は noAuthoNoPriv または authNoPriv の securityLevel パラメータを使用している SNMPv3 PDU 要求に、authorizationError で応答します。

SNMP メッセージの暗号化をユーザに強制するには、グローバル 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。

コマンド	目的
snmp-server user *name* enforcePriv **Example:** switch(config)# snmp-server user Admin enforcePriv	このユーザに対して SNMP メッセージ暗号化を適用します。

SNMP メッセージの暗号化をすべてのユーザに強制するには、グローバル 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。

コマンド	目的
snmp-server globalEnforcePriv **Example:** switch(config)# snmp-server globalEnforcePriv	すべてのユーザに対して SNMP メッセージ暗号化を適用します。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

SNMP コミュニティ ストリングを作成するには、グローバル 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。

コマンド	目的
snmp-server community *name* {**ro** | **rw**} **Example:** switch(config)# snmp-server community public ro	SNMP コミュニティ ストリングを作成します。

SNMP 通知レシーバーの設定

複数のホスト レシーバに対して SNMP 通知を作成するように、Cisco Nexus 1000V を設定できます。

SNMPv1 トラップのホスト レシーバを設定するには、グローバル 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。

コマンド	目的
snmp-server host *ip-address* **traps version 1** *community* [**udp_port** *number*] **Example:** switch(config)# snmp-server host 192.0.2.1 traps version 1 public	SNMPv1 トラップのホスト レシーバを設定します。community には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

SNMPv2c トラップまたは応答要求のホスト レシーバを設定するには、グローバル 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。

コマンド	目的
snmp-server host *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*] **Example:** switch(config)# snmp-server host 192.0.2.1 informs version 2c public	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。community には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

SNMPv3 トラップまたは応答要求のホスト レシーバを設定するには、グローバル 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。

コマンド	目的
snmp-server host *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。username には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

（注）　SNMP マネージャは SNMPv3 メッセージを認証して解読するために、Cisco Nexus 1000V デバイスの SNMP engineID に基づいてユーザ クレデンシャル（authKey/PrivKey）を調べる必要があります。

通知ターゲット ユーザの設定

通知ホスト レシーバに SNMPv3 応答要求通知を送信するには、デバイス上で通知ターゲット ユーザを設定する必要があります。

Cisco Nexus 1000V は通知ターゲット ユーザのクレデンシャルを使用して、設定された通知ホスト レシーバへの SNMPv3 応答要求通知メッセージを暗号化します。

（注）　受信した INFORM PDU を認証して解読する場合、Cisco Nexus 1000V で設定されているのと同じ、応答要求を認証して解読するユーザ クレデンシャルが通知ホスト レシーバに必要です。

通知ターゲット ユーザを設定するには、グローバル 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。

コマンド	目的
snmp-server user *name* [auth {md5 | sha} *passphrase* [auto] [**priv** [aes-128] *passphrase*] [engineID *id*] **Example:** `switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	通知ホスト レシーバに対応した、指定した engineID を持つ通知ターゲット ユーザを設定します。engineID の形式は、12 桁のコロンで区切った 10 進数字です。

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco Nexus 1000V は通知をすべてイネーブルにします。

表 10-3 には、Cisco Nexus 1000V MIB に関する通知をイネーブルにする、CLI コマンドを示します。

（注）　**snmp-server enable traps** コマンドを使用すると、設定されている通知ホスト レシーバに応じて、トラップおよび応答要求の両方がイネーブルになります。

表 10-3　SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB	**snmp-server enable traps entity**
CISCO-ENTITY-FRU-CONTROL-MIB	**snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

ライセンス通知は、デフォルトではイネーブルです。他の通知はすべて、デフォルトではディセーブルです。

指定した通知をイネーブルにするには、グローバル 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。

コマンド	目的
snmp-server enable traps **Example:** `switch(config)# snmp-server enable traps`	すべての SNMP 通知をイネーブルにします。
snmp-server enable traps aaa [**server-state-change**] **Example:** `switch(config)# snmp-server enable traps aaa`	AAA SNMP 通知をイネーブルにします。
snmp-server enable traps entity [**fru**] **Example:** `switch(config)# snmp-server enable traps entity`	ENTITY-MIB SNMP 通知をイネーブルにします。
snmp-server enable traps license **Example:** `switch(config)# snmp-server enable traps license`	ライセンス SNMP 通知をイネーブルにします。
snmp-server enable traps link **Example:** `switch(config)# snmp-server enable traps link`	リンク SNMP 通知をイネーブルにします。

コマンド	目的
snmp-server enable traps port-security **Example:** `switch(config)# snmp-server enable traps port-security`	ポート セキュリティ SNMP 通知をイネーブルにします。
snmp-server enable traps snmp [**authentication**] **Example:** `switch(config)# snmp-server enable traps snmp`	SNMP エージェント通知をイネーブルにします。

インターフェイスに関する linkUp/linkDown 通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。フラッピング インターフェイス（Up と Down の間を頻繁に切り替わるインターフェイス）で、この制限通知を使用できます。

インターフェイスに関する linkUp/linkDown 通知をディセーブルにするには、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。

コマンド	目的
no snmp trap link-status **Example:** `switch(config-if)# no snmp trap link-status`	インターフェイスの SNMP リンクステート トラップをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

TCP による SNMP のワンタイム認証のイネーブル化

TCP セッションでの 1 回限りの SNMP 認証をイネーブルにできます。

TCP による SNMP のワンタイム認証をイネーブルにするには、グローバル 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。

コマンド	目的
snmp-server tcp-session [**auth**] **Example:** `switch(config)# snmp-server tcp-session`	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。デフォルトはディセーブルです。

SNMP スイッチのコンタクトおよびロケーション情報の指定

32 文字までの長さで（スペースを含まない）のスイッチ コンタクト情報を指定できます。さらに、スイッチ ロケーションを指定できます。

はじめる前に

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **snmp-server contact** *name*
3. **snmp-server location** *name*
4. **show snmp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(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	**snmp-server contact** *name* **Example:** switch(config)# snmp-server contact Admin	SNMP コンタクト名である sysContact を設定します。
ステップ 3	**snmp-server location** *name* **Example:** switch(config)# snmp-server location Lab-7	SNMP ロケーションである sysLocation を設定します。
ステップ 4	**show snmp** **Example:** switch(config)# show snmp	（任意）1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config)# 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。

次の例では、SNMP のコンタクトおよびロケーション情報を設定する方法を示します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

SNMP のディセーブル化

デバイスの SNMP プロトコルをディセーブルにできます。

SNMP プロトコルをディセーブルにするには、グローバル 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。

コマンド	目的
no snmp-server protocol enable **Example:** `switch(config)# no snmp-server protocol enable`	SNMP プロトコルをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

AAA 同期時間の変更

同期したユーザ設定を Cisco NX-OS に維持させる時間の長さを変更できます。

AAA 同期時間を変更するには、グローバル 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。

コマンド	目的
snmp-server aaa-user cache-timeout *seconds* **Example:** `switch(config)# snmp-server aaa-user cache-timeout 1200.`	ローカル キャッシュで AAA 同期ユーザ設定を維持する時間を設定します。指定できる範囲は 1 ～ 86400 秒です。デフォルト値は 3600 です。

SNMP の設定確認

SNMP 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config snmp [**all**]	SNMP の実行コンフィギュレーションを表示します。
show snmp	SNMP のステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show snmp context	SNMP コンテキスト マッピングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp session	SNMP セッションを表示します。
show snmp trap	イネーブルまたはディセーブルである SNMP 通知を表示します。
show snmp user	SNMPv3 ユーザを表示します。

SNMP の設定例

Blue VRF を使用してある通知ホスト レシーバに Cisco linkUp/linkDown 通知を送信するように設定し、Admin と NMS という 2 つの SNMP ユーザを定義する例を示します。

```
config t
 snmp-server contact Admin@company.com
```

```
 snmp-server user Admin auth sha abcd1234 priv abcdefgh
 snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
 snmp-server host 192.0.2.1 informs version 3 auth NMS
 snmp-server host 192.0.2.1 use-vrf Blue
 snmp-server enable traps link cisco
```

その他の関連資料

SNMP の実装に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.10-14）
- 「標準」（P.10-14）
- 「MIB」（P.10-15）

関連資料

関連項目	参照先
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』
MIB	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

表 10-4　サポートされている MIB

MIB	MIB のリンク
• CISCO-TC • SNMPv2-MIB • SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • ENTITY-MIB • IF-MIB • CISCO-ENTITY-EXT-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-VIRTUAL-NIC-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB • NOTIFICATION-LOG-MIB • IANA-ADDRESS-FAMILY-NUMBERS-MIB • IANAifType-MIB • IANAiprouteprotocol-MIB • HCNUM-TC	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
• CISCO-VLAN-MEMBERSHIP-MIB • CISCO-SYSTEM-MIB • CISCO-SYSTEM-EXT-MIB • CISCO-IMAGE-MIB • CISCO-IMAGE-UPGRADE-MIB • CISCO-BRIDGE-MIB • CISCO-CONFIG-COPY-MIB • CISCO-SYSLOG-EXT-MIB • CISCO-PROCESS-MIB • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB • CISCO-COMMON-ROLES-MIB • CISCO-COMMON-MGMT-MIB	

SNMP の機能の履歴

ここでは、SNMP 機能のリリース履歴を示します。

機能名	リリース	機能情報
SNMP	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 11

NetFlow の設定

この章では、NetFlow を設定して、送信元、宛先、タイミング、アプリケーション情報に基づいて、IP トラフィックを特徴付けます。これによって、ネットワークの可用性とパフォーマンスを評価します。

この章は、次の内容で構成されています。

- 「NetFlow 情報」（P.11-1）
- 「NetFlow の前提条件」（P.11-9）
- 「設定時の注意事項および制限事項」（P.11-9）
- 「デフォルト設定」（P.11-10）
- 「NetFlow 機能のイネーブル化」（P.11-10）
- 「NetFlow の設定」（P.11-11）
- 「NetFlow の設定確認」（P.11-22）
- 「NetFlow のコンフィギュレーション例」（P.11-25）
- 「その他の関連資料」（P.11-26）
- 「NetFlow の機能の履歴」（P.11-27）

NetFlow 情報

NetFlow は IP トラフィックを評価し、IP トラフィックがフローする方法と場所を把握できます。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。

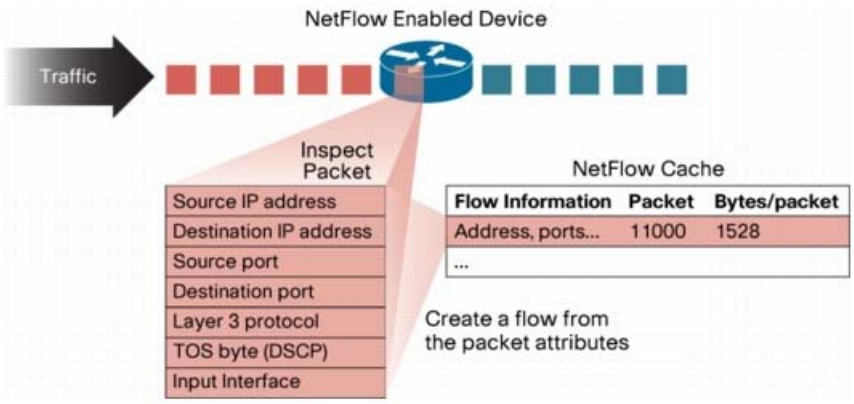
ここでは、次の内容について説明します。

- 「フローとは何か」（P.11-2）
- 「フロー レコード定義」（P.11-2）
- 「NetFlow データへのアクセス」（P.11-5）
- 「NetFlow コレクタ サーバへのフローのエクスポート」（P.11-7）
- 「NetFlow データの例」（P.11-8）
- 「ハイ アベイラビリティ」（P.11-9）

フローとは何か

フローとは、送信元インターフェイス（またはサブインターフェイス）に到着する一方向のパケットストリームであり、一連の条件と一致します。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。

図 11-1　NetFlow キャッシュでのフローの作成



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。フローは NetFlow キャッシュに格納されます。

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 レコード定義

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 レコードを定義するか、あらかじめ定義された Cisco Nexus 1000V フロー レコードを使用できます。

レコードを作成するには、「フロー レコードの定義」（P.11-12）の手順を参照してください。

次の表では、フロー レコードで定義される条件を説明します。

フロー レコード条件	説明
Match	フロー レコードのコレクションと一致する情報を定義します。 • **ip**：フロー レコードで収集されるデータは、次の IP オプションのいずれかと一致します。 – プロトコル – tos（タイプ オブ サービス） • **ipv4**：フロー レコードで収集されるデータは、次の ipv4 アドレス オプションのいずれかと一致します。 – 送信元アドレス – 宛先アドレス • **transport**：フロー レコードで収集されるデータは、次のトランスポート オプションのいずれかと一致します。 – 宛先ポート – 送信元ポート
Collect	フロー レコードが情報を収集する方法を定義します。 • **counter**：次のフォーマットのいずれかで、フロー レコード情報を収集します。 – bytes：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 – packets：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 • **timestamp sys-uptime**：フローの先頭または最終パケットに関するシステム稼動時間を収集します。 • **transport tcp flags**：フローのパケットの TCP トランスポート層フラグを収集します。

あらかじめ定義されたフロー レコード

Cisco Nexus 1000V には、次のあらかじめ定義されたフロー レコードが含まれます。

- 「例 11-1Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow-Original」（P.11-3）
- 「例 11-2Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Original-Input」（P.11-4）
- 「例 11-3Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Original-Output」（P.11-5）
- 「例 11-4Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow Protocol-Port」（P.11-5）

例 11-1　Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow-Original

```
n1000v# show flow record netflow-original
Flow record netflow-original:
```

```
    Description: Traditional IPv4 input NetFlow with origin ASs
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
n1000v#
```

（注）　**show flow record** コマンドによる出力結果には、次の行が表示されますが、基になるコマンドは現在 Cisco Nexus 1000V ではサポートされていません。これらのコマンドを使用しても、コンフィギュレーションには影響はありません。

```
collect routing source as
collect routing destination as
collect routing next-hop address ipv4
```

例 11-2　Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Original-Input

```
n1000v# show flow record netflow ipv4 original-input
Flow record ipv4 original-input:
    Description: Traditional IPv4 input NetFlow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
n1000v#
```

例 11-3　Cisco Nexus 1000V であらかじめ定義されたフロー レコード : Netflow IPv4 Original-Output

```
switch# show flow record netflow ipv4 original-output
Flow record ipv4 original-output:
    Description: Traditional IPv4 output NetFlow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

例 11-4　Cisco Nexus 1000V であらかじめ定義されたフロー レコード : Netflow Protocol-Port

```
switch# show flow record netflow protocol-port
Flow record ipv4 protocol-port:
    Description: Protocol and Ports aggregation scheme
    No. of users: 0
    Template ID: 0
    Fields:
        match ip protocol
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

NetFlow データへのアクセス

NetFlow データには、主に 2 つの方法を使用してアクセスできます。

- 「コマンドライン インターフェイス（CLI）」（P.11-6）
- 「NetFlow コレクタ」（P.11-7）

コマンドライン インターフェイス（CLI）

現在のネットワーク状態を調べるには、CLI を使用します。利用可能な show コマンドを表示するには、「NetFlow の設定確認」（P.11-22）を参照してください。

CLI は次のツールを使用して、フロー レコードを取得して、Netflow コレクタにエクスポートします。

- 「フロー モニタ」（P.11-6）
- 「フロー エクスポータ」（P.11-6）

フロー モニタ

フロー モニタは、次の NetFlow コンポーネント間のアソシエーションを作成します。

- フロー レコード：マッチングおよび収集条件から構成されます。
- フロー エクスポータ：エクスポート条件から構成されます。

このフロー モニタ アソシエーションによって、レコードとエクスポータから構成されるセットを一度だけ定義して何度も再利用することが可能になります。さまざまなニーズに合わせて、複数のフロー モニタを作成できます。フロー モニタは、特定の方向の、特定のインターフェイスに適用されます。

「フロー モニタの定義」（P.11-17）の手順および「フロー モニタのインターフェイスへの割り当て」（P.11-19）の手順を参照してください。

フロー エクスポータ

フロー エクスポータを使用して、キャッシュから NetFlow コレクタと呼ばれるレポーティング サーバに、フロー レコードが送信される場所と時間を定義します。

エクスポータ定義には、次の内容が含まれます。

- 宛先 IP アドレス
- 送信元インターフェイス
- UDP ポート番号（コレクタが待機するところ）
- エクスポート フォーマット

（注）NetFlow エクスポート パケットでは、送信元インターフェイスに割り当てられた IP アドレスを使用します。送信元インターフェイスに IP アドレスが割り当てられていない場合、エクスポータはアクティブになりません。

「フロー エクスポータの定義」（P.11-15）の手順を参照してください。

エクスポート フォーマット

Cisco Nexus 1000V は、NetFlow バージョン 9 エクスポート フォーマットをサポートしています。

（注）Cisco Nexus 1000V は、モニタごとに最大 2 つのエクスポータにデータをエクスポートするトランスポート プロトコルとして、UDP をサポートしています。

NetFlow コレクタ

Cisco Nexus 1000V NetFlow キャッシュから、NetFlow コレクタと呼ばれるレポーティング サーバに、NetFlow をエクスポートできます。NetFlow コレクタは、エクスポートされたフローを再構成し、フローを組み合わせて、トラフィックおよびセキュリティ分析で使用するレポートを生成します。SNMP ポーリングとは異なり、NetFlow エクスポートは定期的に、情報を NetFlow レポーティング コレクタにプッシュします。NetFlow キャッシュには常にフローが入ってきます。Cisco Nexus 1000V はキャッシュ内の終了または期限切れになったフローを検索し、NetFlow コレクタ サーバにエクスポートします。ネットワーク通信が終了すると、フローも終了します。つまり、パケットには、TCP FIN フラグが含まれます。

次は、NetFlow データ レポーティングを実装する手順です。

- NetFlow が収集する情報を定義するように、NetFlow レコードを設定します。
- NetFlow キャッシュへのフロー レコードを取得するように、Netflow モニタを設定します。
- フローをコレクタに送信するように、NetFlow エクスポートを設定します。
- Cisco Nexus 1000V は、NetFlow キャッシュ内の終了したフローを検索し、NetFlow コレクタ サーバにエクスポートします。
- フローは UDP エクスポート パケットで利用可能なスペース、またはエクスポート タイマーに基づいてまとめられます。
- NetFlow コレクタ ソフトウェアは、データからリアルタイムのレポートまたは履歴レポートを作成します。

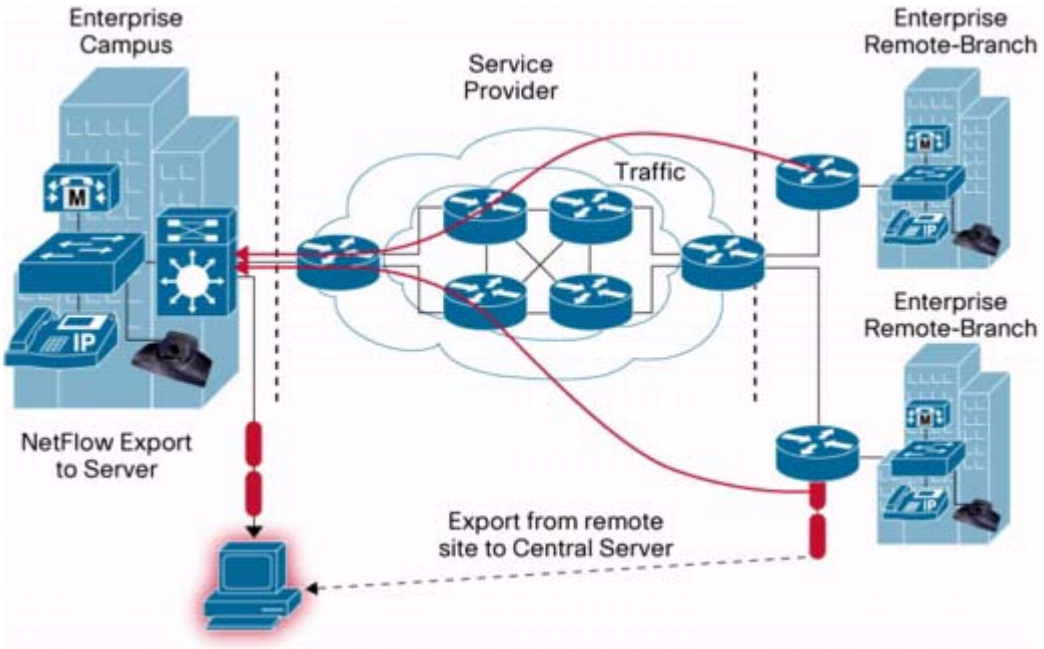
NetFlow コレクタ サーバへのフローのエクスポート

タイマーは、フローが NetFlow コレクタ サーバにエクスポートされるタイミングを判断します。

次のいずれかが発生するときに、フローのエクスポートが可能になります。

- フローが一定時間非アクティブとなり、その間、フローで新しいパケットを受信していない場合。
- 長時間の FTP ダウンロードなど、フローがアクティブなタイマーより長く存在している場合。
- TCP フラグが、フローが終了したことを示している場合。つまり、FIN または RST フラグが表示されている場合です。
- フロー キャッシュが満杯で、一部の古いフローを削除して、新しいフローのための領域を作成する必要がある場合。

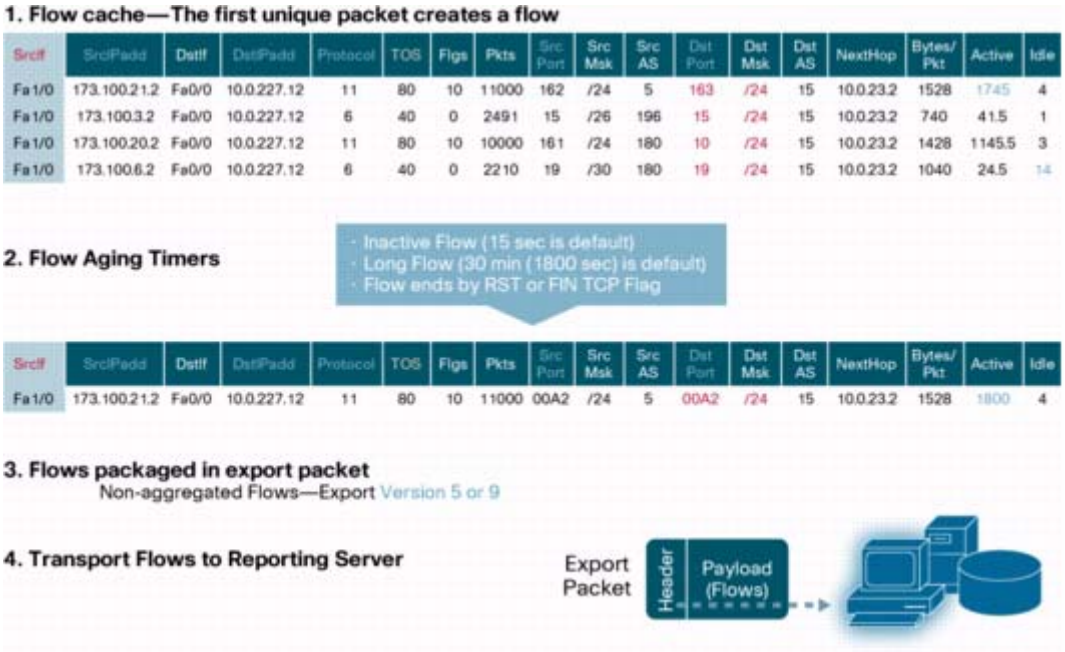
図 11-2　「NetFlow コレクタ サーバへのフローのエクスポート」



NetFlow データの例

次の図は、NetFlow データの例を示しています。

図 11-3　NetFlow キャッシュの例



SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	163	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

ネットワーク解析モジュール

Cisco ネットワーク解析モジュール（NAM）を使用して、NetFlow データソースをモニタすることもできます。NAM を使用すると、ホスト、アプリケーション、対話、VLAN、QoS などのトラフィック分析の表示およびレポート作成が可能になります。

NAM を使用して Cisco Nexus 1000V NetFlow データソースをモニタする手順については、『*Cisco Nexus 1010 Network Analysis Module Installation and Configuration Note, 5.1*』を参照してください。

ハイ アベイラビリティ

Cisco Nexus 1000V は、NetFlow のステートレス リスタートをサポートします リブートまたはスーパーバイザ スイッチオーバーの後に、Cisco Nexus 1000V は実行コンフィギュレーションを適用します。

NetFlow の前提条件

- NetFlow は追加メモリと CPU リソースを消費するため、リソース要件に注意する必要があります。
- メモリと CPU リソースは、フロー モニタ インターフェイスをホスティングする VEM が提供します。リソースは VEM 上の CPU コアの数によって、制限されています。

設定時の注意事項および制限事項

NetFlow に関する設定時の注意事項および制約事項は、次のとおりです。

- 送信元インターフェイスが設定されていない場合、NetFlow エクスポータはディセーブルの状態のままです。
- Cisco Nexus 1000V では、デフォルトで、エクスポータの送信元インターフェイスとして、Mgmt0 インターフェイスが設定されます。必要に応じて、送信元インターフェイスを変更できます。
- Cisco Nexus 1000V には、次のあらかじめ定義されたフロー レコードが含まれているため、新しいフロー レコードを作成する代わりに、これを使用できます。詳細については、「フロー レコード定義」（P.11-2）を参照してください。
  - netflow-originalCisco Nexus 1000V のあらかじめ定義された、起点 AS を含む従来の IPv4 入力 NetFlow

    （注）　このあらかじめ定義されたフロー レコード内のルーティング関連のフィールドは無視されます。

  - netflow ipv4 original-inputCisco Nexus 1000V のあらかじめ定義された従来の IPv4 入力 NetFlow
  - netflow ipv4 original-outputCisco Nexus 1000V のあらかじめ定義された従来の IPv4 出力 NetFlow
  - netflow protocol-portCisco Nexus 1000V のあらかじめ定義されたプロトコル ポート集約方式

- DVS あたり最大 256 個の NetFlow インターフェイスが許可されます。
- ホストあたり最大 32 個の NetFlow インターフェイスが許可されます。
- 1 方向あたり 1 インターフェイスにつき最大 1 個のフロー モニタが許可されます。
- VEM あたり最大 8 個のフロー モニタが許可されます。
- モニタあたり最大 2 個のフロー エクスポータが許可されます。
- DVS あたり最大 32 個の NetFlow ポリシーが許可されます。
- ホストあたり最大 8 個の NetFlow ポリシーが許可されます。
- NetFlow は、ポート チャネルではサポートされていません。

デフォルト設定

表 11-1 に、NetFlow パラメータのデフォルト設定をリスト表示します。

表 11-1　デフォルトの NetFlow パラメータ

パラメータ	デフォルト
NetFlow version	9
source interface	mgmt0
match	方向とインターフェイス（着信 / 発信）
flow monitor active timeout	1800
flow monitor inactive timeout	15
flow monitor cache size	4096
flow exporter UDP port **transport udp** command	9995
DSCP	デフォルト /best-effort（0）
VRF	デフォルト

NetFlow 機能のイネーブル化

NetFlow 機能をイネーブルにするには、こ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。

手順の概要

1. **config t**
2. **feature netflow**
3. **show feature**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`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	**feature netflow**
	Example:
	`n1000v(config)# feature netflow`
	`n1000v(config)#`
		NetFlow 機能をイネーブルにします。

ステップ 3	**show feature** **Example:** `n1000v(config)# show feature`	（任意）使用可能な機能、およびそれらの機能がイネーブルかどうかを表示します。
ステップ 4	**copy running-config startup-config** **Example:** `n1000v(config-flow-exporter)# 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。

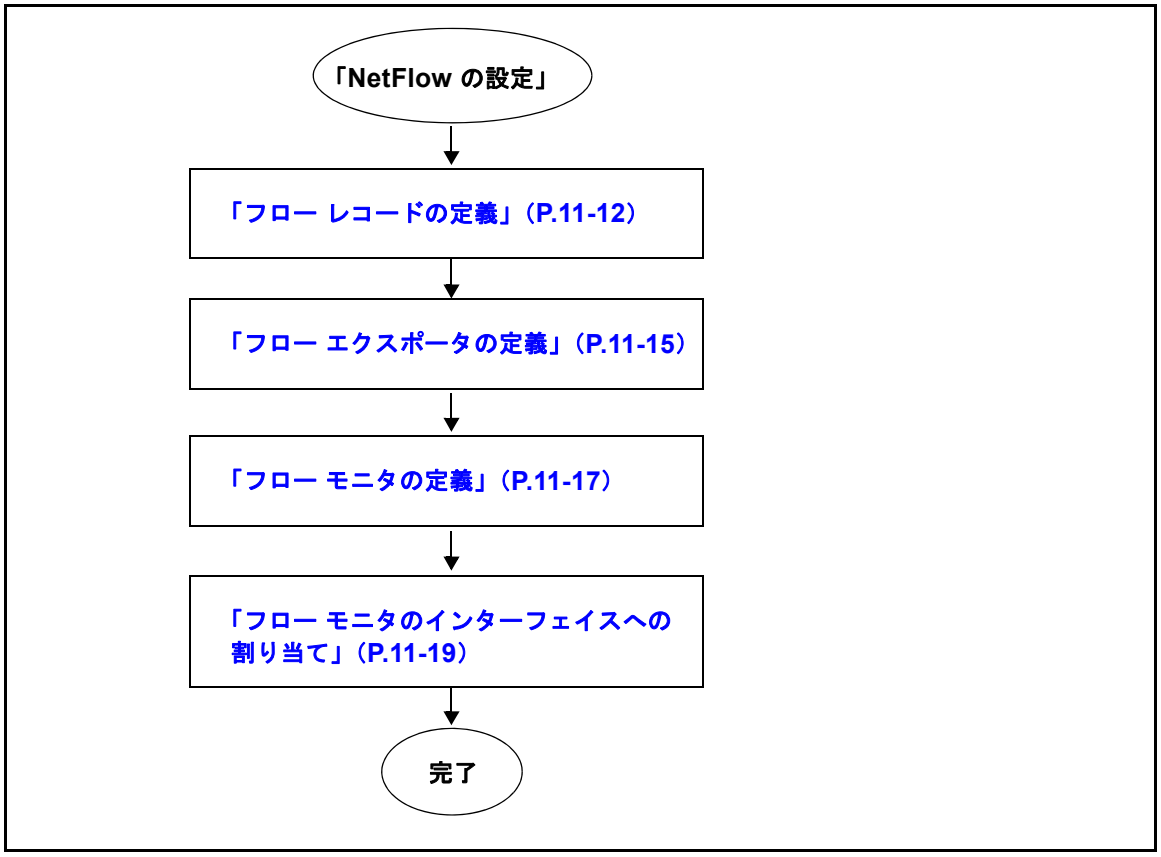
次に、NetFlow 機能をイネーブルにする例を示します。

```
n1000v# config t
n1000v(config)# feature netflow
```

NetFlow の設定

次のフロー チャートは、NetFlow コンフィギュレーション プロセスを案内するために作成されています。各手順を完了したらこのフロー チャートに戻り、すべての必要な手順を正しい順序で完了したことを確認してください。

フロー チャート：「NetFlow の設定」



フロー レコードの定義

この手順を使用して、フロー レコードを作成します。

（注）　任意で、「フロー レコード定義」（P.11-2）で説明されている Cisco Nexus 1000V のあらかじめ定義されたレコードを使用できます。「フロー モニタの定義」（P.11-17）を参照して、あらかじめ定義されたレコードを、フロー モニタに適用します。

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。

- このフロー レコードが一致するオプションを確認します。
- このフロー レコードが収集するオプションを確認します。

  詳細については、「フロー レコード定義」（P.11-2）を参照してください。

（注）　**show flow record** コマンドによる出力結果には、次の行が表示されますが、基になるコマンドは現在 Cisco Nexus 1000V ではサポートされていません。これらのコマンドを使用しても、コンフィギュレーションには影響はありません。

collect routing source as
collect routing destination as
collect routing next-hop address ipv4

手順の概要

1. **config t**
2. **flow record** *name*
3. **description** *string*
4. **match {ip {protocol | tos} | ipv4 {destination address | source address} | transport {destination-port | source-port}}**
5. **collect {counter {bytes [long] | packets [long]} | timestamp sys-uptime | transport tcp flags}**
6. **show flow record** [*name*]
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	***config t***
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**flow record** *name*
	Example:
	`n1000v(config)# flow record RecordTest`
	`n1000v(config-flow-record)#`
		名前ごとにフロー レコードを作成し、特定のレコードで、CLI フロー レコード コンフィギュレーション モードに切り替えます。

ステップ 3	**description** *string* **Example:** `n1000v(config-flow-record)# description Ipv4Flow`	（任意）63 文字以内の説明をこのフロー レコードに追加し、実行コンフィギュレーションに保存します。
ステップ 4	**match** {**ip**{**protocol**| **tos**}|**ipv4**{**destination address**|**source address**}|**transport** {**destination-port**|**source-port**}} **Example:** `n1000v(config-flow-record)# match ipv4 destination address`	次のいずれかに一致するフロー レコードを定義し、実行コンフィギュレーションに保存します。 • **ip**：次の IP オプションのいずれかと一致します。 – プロトコル – tos（タイプ オブ サービス） • **ipv4**：次の ipv4 アドレス オプションのいずれかと一致します。 – 送信元アドレス – 宛先アドレス • **transport**：次のトランスポート オプションのいずれかと一致します。 – 宛先ポート – 送信元ポート

	コマンド	目的
ステップ 5	**collect {counter {bytes [long] | packets [long]} | timestamp sys-uptime | transport tcp flags}** **Example:** `n1000v(config-flow-record)# collect counter packets`	収集オプションを指定して、フロー レコードで収集する情報を定義し、実行コンフィギュレーションに保存します。 • **counter**：次のフォーマットのいずれかで、フロー レコード情報を収集します。 – bytes：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 – packets：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 • **timestamp sys-uptime**：フローの先頭または最終パケットに関するシステム稼動時間を収集します。 • **transport tcp flags**：フローのパケットの TCP トランスポート層フラグを収集します。
ステップ 6	**show flow record** [*name*] **Example:** `n1000v(config-flow-exporter)# show flow record RecordTest`	（任意）フロー レコード情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** `n1000v(config-flow-exporter)# 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。

次に、フロー レコードを作成する例を示します。

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# description Ipv4flow
n1000v(config-flow-record)# match ipv4 destination address
n1000v(config-flow-record)# collect counter packets
n1000v(config-flow-record)# show flow record RecordTest
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

フロー エクスポータの定義

この手順を使用して、フロー レコードが NetFlow コレクタ サーバにエクスポートされる場所と方法を定義する、フロー エクスポータを作成します。

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。

- 最大 2 つのフロー エクスポータを、各モニタに対して許可します。
- NetFlow コレクタ サーバの宛先 IP アドレスを確認します。
- フロー レコードが送信される送信元インターフェイスを確認します。
- コレクタがリッスンしているトランスポート UDP を確認します。
- エクスポート フォーマット バージョン 9 がサポートされているバージョンです。

手順の概要

1. **config t**
2. **flow exporter** *name*
3. **description** *string*
4. **destination** {*ipv4-address* | *ipv6-address*}
5. **dscp** *value*
6. **source mgmt** *interface_number*
7. **transport udp** *port-number*
8. `version 9`
9. **option {exporter-stats | interface-table} timeout** *seconds*
10. **template data timeout** *seconds*
11. **show flow exporter** [*name*]
12. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**flow exporter** *name*
	Example:
	`n1000v(config)# flow exporter ExportTest`
	`n1000v(config-flow-exporter)#`
		フロー エクスポータを作成して、実行コンフィギュレーションに保存します。次に、CLI フロー エクスポータ コンフィギュレーション モードに切り替えます。

ステップ 3	**description** *string*
	Example:
	`n1000v(config-flow-exporter)#`
	`description ExportV9`
		63 文字以内の説明をこのフロー エクスポータに追加し、実行コンフィギュレーションに保存します。

	コマンド	目的
ステップ 4	**destination** {*ipv4-address* | *ipv6-address*} **Example:** `n1000v(config-flow-exporter)# destination 192.0.2.1`	このフロー エクスポータの宛先インターフェイスの IP アドレスを指定し、実行コンフィギュレーションに保存します。
ステップ 5	**dscp** *value* **Example:** `n1000v(config-flow-exporter)# dscp 0`	このフロー エクスポータの DiffServ コードポイント値を 0 ～ 63 の範囲で指定して、実行コンフィギュレーションに保存します。
ステップ 6	**source mgmt** *interface_number* **Example:** `n1000v(config-flow-exporter)# source mgmt 0`	フロー レコードが NetFlow コレクタ サーバに送信されるインターフェイスと数を指定して、実行コンフィギュレーションに保存します。
ステップ 7	**transport udp** *port-number* **Example:** `n1000v(config-flow-exporter)# transport udp 200`	NetFlow コレクションに到達するために使用する宛先 UDP ポートを、0 ～ 65535 の範囲で指定して、実行コンフィギュレーションに保存します。

ステップ 8	**version** {**9**}
	Example:
	`n1000v(config-flow-exporter)# version 9`
	`n1000v(config-flow-exporter-version-9)#`
		NetFlow エクスポート バージョン 9 を指定して、実行コンフィギュレーションに保存します。次に、エクスポート バージョン 9 コンフィギュレーション モードに切り替えます。

ステップ 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout** *value* **Example:** `n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	次のバージョン 9 のエクスポータ再送タイマーと値のいずれかを、1 ～ 86400 秒の範囲で指定して、実行コンフィギュレーションに保存します。 • **exporter-stats** • **interface-table** • **sampler-table**
ステップ 10	**template data timeout** *seconds* **Example:** `n1000v(config-flow-exporter-version-9)# template data timeout 1200`	テンプレート データ再送タイマーと値を、1 ～ 86400 秒の範囲で設定して、実行コンフィギュレーションに保存します。
ステップ 11	**show flow exporter** [*name*] **Example:** `n1000v(config-flow-exporter)# show flow exporter`	（任意）フロー エクスポータに関する情報を表示します。
ステップ 12	**copy running-config startup-config** **Example:** `n1000v(config-flow-exporter)# 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。

次に、フロー エクスポータを作成する例を示します。

```
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
n1000v(config-flow-exporter)# destination 192.0.2.1
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)# source mgmt 0
n1000v(config-flow-exporter)# transport udp 200
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200
n1000v(config-flow-exporter-version-9)# template data timeout 1200
```

```
n1000v(config-flow-exporter-version-9)# show flow exporter ExportTest
Flow exporter ExportTest:
    Description: ExportHamilton
    Destination: 192.0.2.1
    VRF: default (1)
    Destination UDP Port 200
    Source Interface Mgmt0
    DSCP 2
    Export Version 9
        Exporter-stats timeout 1200 seconds
        Data template timeout 1200 seconds
    Exporter Statistics
        Number of Flow Records Exported 0
        Number of Templates Exported 0
        Number of Export Packets Sent 0
        Number of Export Bytes Sent 0
        Number of Destination Unreachable Events 0
        Number of No Buffer Events 0
        Number of Packets Dropped (No Route to Host) 0
        Number of Packets Dropped (other) 0
        Number of Packets Dropped (LC to RP Error) 0
        Number of Packets Dropped (Output Drops) 1
        Time statistics were last cleared: Never
n1000v(config-flow-exporter-version-9)#
```

フロー モニタの定義

この手順を使用して、フロー モニタを作成し、フロー レコードとフロー エクスポータを作成したフロー モニタに関連付けます。

はじめる前に

- 最大 1 つのフロー モニタを、各方向の各インターフェイスに対して許可します。
- このフロー モニタを関連付ける既存のフロー エクスポータ名を確認します。
- このフロー モニタを関連付ける既存のフロー レコード名を確認します。以前に作成したフロー レコードまたは次の Cisco Nexus 1000V のあらかじめ定義されたフロー レコードのいずれかを使用できます。
  - netflow-original
  - netflow ipv4 original-input
  - netflow ipv4 original-output
  - netflow protocol-port

  フロー レコードの詳細については、「フロー レコード定義」（P.11-2）を参照してください。

手順の概要

1. **config t**
2. **flow monitor** *name*
3. **description** *string*
4. **exporter** *name*
5. **record** *name*
6. **timeout** {**active** *value* | **inactive** *value*}

7. **cache** {**size** *value*}
8. **show flow monitor** [*name*]
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**flow monitor** *name*
	Example:
	`n1000v(config)# flow monitor MonitorTest`
	`n1000v(config-flow-monitor)#`
		名前ごとにフロー モニタを作成し、実行コンフィギュレーションに保存します。次に、CLI フロー モニタ コンフィギュレーション モードに切り替えます。

ステップ 3	**description** *string* **Example:** `n1000v(config-flow-monitor)# description Ipv4Monitor`	（任意）指定されたフロー モニタの場合は、63 文字以下の英数字で説明用の文字列を追加し、実行コンフィギュレーションに保存します。
ステップ 4	**exporter** *name* **Example:** `n1000v(config-flow-monitor)# exporter Exportv9`	指定されたフロー モニタの場合は、既存のフロー エクスポータを追加し、実行コンフィギュレーションに保存します。

ステップ 5	**record** {*name* | **netflow** {**ipv4**}}
	Example using Cisco Nexus 1000V pre-defined record:
	`n1000v(config-flow-monitor)# record netflow-original`
	Example using user-defined record:
	`n1000v(config-flow-monitor)# record RecordTest`
		指定されたフロー モニタの場合は、既存のフロー レコードを追加し、実行コンフィギュレーションに保存します。
		• **name**：以前に作成したフロー レコード名、またはシスコが提供しているあらかじめ定義されたフロー レコード名。
		• **netflow**：従来の NetFlow 収集方式
		　– **ipv4**：従来の IPv4 NetFlow 収集方式

ステップ 6	**timeout** {**active** *value* | **inactive** *value*} **Example:** `n1000v(config-flow-monitor)# timeout inactive 600`	（任意）指定されたフロー モニタの場合、古いタイマーとキャッシュからの古いエントリの値を指定し、実行コンフィギュレーションに保存します。 • **active**：アクティブ、ロング、またはタイムアウト。許可されている値は、60 ～ 4092 秒の範囲です。デフォルト値は 1800 秒です。 • **inactive**：非アクティブまたは通常のタイムアウト。許可されている値は、15 ～ 4092 秒の範囲です。デフォルト値は 15 秒です。
ステップ 7	**cache** {**size** *value*} **Example:** `n1000v(config-flow-monitor)# cache size 15000`	（任意）指定されたフロー モニタのキャッシュ サイズを 256 ～ 16384 エントリの範囲で指定し、実行コンフィギュレーションに保存します。デフォルト値は 4096 です。 **（注）** このオプションは、モニタ キャッシュのメモリとパフォーマンスへの影響を抑えます。

	コマンド	目的
ステップ 8	**show flow monitor** [*name*] **Example:** `n1000v(config-flow-monitor)# show flow monitor Monitor Test`	（任意）既存のフロー モニタに関する情報を表示します。
ステップ 9	**copy running-config startup-config** **Example:** `n1000v(config-flow-monitor)# 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。

次に、フロー エクスポータを作成する例を示します。

```
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
n1000v(config-flow-monitor)# exporter ExportTest
n1000v(config-flow-monitor)# record RecordTest
n1000v(config-flow-monitor)# cache size 15000
n1000v(config-flow-monitor)# timeout inactive 600
n1000v(config-flow-monitor)# show flow monitor MonitorTest
Flow Monitor monitortest:
    Use count: 0
    Inactive timeout: 600
    Active timeout: 1800
    Cache Size: 15000
n1000v(config-flow-monitor)#
```

フロー モニタのインターフェイスへの割り当て

この手順を使用して、フロー モニタをインターフェイスに割り当てます。

はじめる前に

- インターフェイスに使用するフロー モニタ名を確認します。
- インターフェイス タイプと数を確認します。

手順の概要

1. **config t**
2. **interface** *interface-type interface-number*
3. **ip flow monitor** *name* {**input** | **output**}
4. **show flow** *interface-type interface-number*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**interface** *interface-type interface-number*
	Example:
	`n1000v(config)# interface veth 2`
	`n1000v(config-if)#`
		指定されたインターフェイスの CLI インターフェイス コンフィギュレーション モードに切り替えます。

ステップ 3	**ip flow monitor** *name* {**input** | **output**} **Example:** `n1000v(config-if)# ip flow monitor MonitorTest output`	指定されたインターフェイスの場合は、入出力パケット用にフロー モニタを割り当て、実行コンフィギュレーションに保存します。
ステップ 4	**show flow** *interface-type interface-number* **Example:** `n1000v(config-if# show flow interface veth 2`	（任意）指定されたインターフェイスの場合、NetFlow 設定が表示されます。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# 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。

次に、フロー モニタをインターフェイスに割り当てる例を示します。

```
n1000v(config)# interface veth 2
n1000v(config-if)# ip flow monitor MonitorTest output
n1000v(config-if)# show flow interface veth 2
Interface veth 2:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

ポート プロファイルへのフロー モニタの追加

この手順を使用して、フロー モニタをポート プロファイルに追加できます。

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。
- 「フロー モニタの定義」（P.11-17）の手順を使用して、フロー モニタをすでに作成していること。
- 既存のポート プロファイルを使用する場合は、ポート プロファイルをすでに作成していて、その名前がわかっていること。
- 新しいポート プロファイルを作成する場合は、インターフェイスのタイプ（イーサネットまたは vEthernet）を理解し、ポート プロファイルに付ける名前を知っていること。

- 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。

手順の概要

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *name*
3. **ip flow monitor** *name* {input | output}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明
ステップ 1	**config t** **Example:** 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** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	名前付きポート 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	**ip flow monitor** *name* {**input** | **output**} **Example:** n1000v(config-port-prof)# ip flow monitor allaccess4 output n1000v(config-port-prof)#	受信（**input**）または送信（**output**）トラフィックのポート プロファイルに指定のフロー モニタを適用します。
ステップ 4	**show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*] **Example:** 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** **Example:** 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。

例

次に、ポート プロファイルにフロー モニタを追加する例を示します。

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# ip flow monitor allacces4 output
n1000v(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
```

```
pinning packet-vlan: -
system vlans: none
port-group:
max ports: 32
inherit:
config attributes:
  ip flow monitor allaccess4 output
evaluated config attributes:
  ip flow monitor allaccess4 output
assigned interfaces:n1000v(config-port-prof)#
```

NetFlow の設定確認

NetFlow 設定を確認するには、表 11-2 で説明されているコマンドを使用します。

表 11-2　NetFlow の設定確認

コマンド	目的
show flow exporter [*name*]	NetFlow のフロー エクスポータ マップ情報を表示します。 例 11-5（P.11-22）を参照してください。
show flow interface [*interface-type number*]	NetFlow インターフェイスに関する情報を表示します。 例 11-6（P.11-23）を参照してください。
show flow monitor [*name* [**cache module** ***number*** |**statistics module** ***number***]]	NetFlow フロー モニタに関する情報を表示します。 （注）　**show flow monitor cache** コマンドは、キャッシュ エントリも表示するという点で、**show flow monitor statistics** コマンドとは異なります。各プロセッサには独自のキャッシュがあるため、これらのコマンドのすべての出力内容は、サーバ（モジュールまたはホストとも呼ばれます）のプロセッサ数に基づいています。複数のプロセッサを使用して、1 つのフローのパケットを処理している場合、同じフローが各プロセッサに表示されます。 次の例を参照してください。 • 「例 11-7Show flow monitor」（P.11-23） • 「例 11-8Show flow monitor cache module」（P.11-23） • 「例 11-9Show flow monitor statistics module」（P.11-24）
show flow record [*name*]	NetFlow のフロー レコード情報を表示します。

例 11-5　Show flow exporter

```
n1000v(config-flow-exporter-version-9)# show flow exporter ExportTest
```

```
Flow exporter ExportTest:
    Description: ExportHamilton
    Destination: 192.0.2.1
    VRF: default (1)
    Destination UDP Port 200
    Source Interface 2
    DSCP 2
    Export Version 9
        Exporter-stats timeout 1200 seconds
        Data template timeout 1200 seconds
    Exporter Statistics
        Number of Flow Records Exported 0
        Number of Templates Exported 0
        Number of Export Packets Sent 0
        Number of Export Bytes Sent 0
        Number of Destination Unreachable Events 0
        Number of No Buffer Events 0
        Number of Packets Dropped (No Route to Host) 0
        Number of Packets Dropped (other) 0
        Number of Packets Dropped (LC to RP Error) 0
        Number of Packets Dropped (Output Drops) 1
        Time statistics were last cleared: Never
n1000v(config-flow-exporter-version-9)#
```

例 11-6　Show flow interface

```
n1000v(config-if)# show flow interface VEth2
Interface veth2:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

例 11-7　Show flow monitor

```
n1000v(config)# show flow monitor
Flow Monitor MonitorTest:
    Description: Ipv4Monitor
    Use count: 1
    Flow Record: test
    Flow Exporter: ExportTest
    Inactive timeout: 15
    Active timeout: 1800
    Cache Size: 15000
Flow Monitor MonitorIpv4:
    Description: exit
    Use count: 70
    Flow Record: RecordTest
    Flow Exporter: ExportIpv4
    Inactive timeout: 15
    Active timeout: 1800
    Cache Size: 4096
n1000v(config)#
```

例 11-8　Show flow monitor cache module

```
n1000v# show flow monitor test_mon cache module 5
Cache type:                          Normal
Cache size (per-processor):          4096
High Watermark:                      2
Flows added:                         102
Flows aged:                          099
```

```
    - Active timeout                0
    - Inactive timeout              099
    - Event aged                    0
    - Watermark aged                0
    - Emergency aged                0
    - Permanent                     0
    - Immediate aged                0
    - Fast aged                     0

Cache entries on Processor0
    - Active Flows:                 2
    - Free Flows:                   4094

  IPV4 SRC ADDR    IPV4 DST ADDR  IP PROT            INTF INPUT           INTF OUTPUT  FLOW DIRN
===============  ===============  =======  ====================  ====================  =========
        0.0.0.0  255.255.255.255  17                      Veth1                            Input
   7.192.192.10      7.192.192.2  1                       Veth1                Eth5/2      Input

Cache entries on Processor1
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor2
    - Active Flows:                 1
    - Free Flows:                   4095

  IPV4 SRC ADDR    IPV4 DST ADDR  IP PROT            INTF INPUT           INTF OUTPUT  FLOW DIRN
===============  ===============  =======  ====================  ====================  =========
   7.192.192.10      7.192.192.1  1                       Veth1                Eth5/2      Input

Cache entries on Processor3
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor4
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor5
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor6
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor7
    - Active Flows:                 0
    - Free Flows:                   4096
```

例 11-9　Show flow monitor statistics module

```
NX-1000v# show flow monitor test_mon statistics module 5
Cache type:                          Normal
Cache size (per-processor):          4096
High Watermark:                      2
Flows added:                         105
Flows aged:                          103
    - Active timeout                 0
    - Inactive timeout               103
    - Event aged                     0
    - Watermark aged                 0
```

```
    - Emergency aged                0
    - Permanent                     0
    - Immediate aged                0
    - Fast aged                     0

Cache entries on Processor0
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor1
    - Active Flows:                 1
    - Free Flows:                   4095

Cache entries on Processor2
    - Active Flows:                 1
    - Free Flows:                   4095

Cache entries on Processor3
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor4
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor5
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor6
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor7
    - Active Flows:                 0
    - Free Flows:                   4096
```

例 11-10　Show flow record

```
n1000v(config-flow-record)# show flow record RecordTest
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

NetFlow のコンフィギュレーション例

次に、新しいフロー レコードを使用し、インターフェイスに適用してフロー モニタを設定する例を示します。

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# description Ipv4flow
```

```
n1000v(config-flow-record)# match ipv4 destination address
n1000v(config-flow-record)# collect counter packets
n1000v(config-flow-record)# exit
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
n1000v(config-flow-exporter)# destination 192.0.2.1
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)# source mgmt 0
n1000v(config-flow-exporter)# transport udp 200
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200
n1000v(config-flow-exporter-version-9)# template data timeout 1200
n1000v(config-flow-exporter-version-9)# exit
n1000v(config-flow-exporter)# exit
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
n1000v(config-flow-monitor)# exporter ExportTest
n1000v(config-flow-monitor)# record RecordTest
n1000v(config-flow-monitor)# exit
n1000v(config)# interface veth 2/1
n1000v(config-if)# ip flow monitor MonitorTest output
n1000v(config-if)# show flow interface veth 2
Interface veth 2:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

次に、あらかじめ定義されたレコードを使用し、インターフェイスに適用してフロー モニタを設定する例を示します。

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
n1000v(config-flow-exporter)# destination 192.0.2.1
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)# source mgmt 0
n1000v(config-flow-exporter)# transport udp 200
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200
n1000v(config-flow-exporter-version-9)# template data timeout 1200
n1000v(config-flow-exporter-version-9)# exit
n1000v(config-flow-exporter)# exit
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
n1000v(config-flow-monitor)# exporter ExportTest
n1000v(config-flow-monitor)# record netflow-original
n1000v(config-flow-monitor)# exit
n1000v(config)# interface veth 2/1
n1000v(config-if)# ip flow monitor MonitorTest output
n1000v(config-if)# show flow interface veth 2
Interface veth 2:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

その他の関連資料

NetFlow の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.11-27）

- 「標準」（P.11-27）

関連資料

関連項目	参照先
Cisco NetFlow の概要	http://cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
ポート プロファイル	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』
Cisco Nexus 1000V のすべてのコマンドのコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意事項、および例。	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

NetFlow の機能の履歴

ここでは、NetFlow 機能のリリース履歴を示します。

機能名	リリース	機能情報
NetFlow データソースに対する NAM サポート	4.0(4)SV1(3)	NetFlow データソースに対する NAM サポートが追加されました。
NetFlow	4.0(4)SV1(1)	NetFlow が追加されました。

CHAPTER 12

システム メッセージ ロギングの設定

この章では、システム メッセージ ロギングを設定する方法を説明します。

この章では、次の事項について説明します。

- 「システム メッセージ ロギングの概要」（P.12-1）
- 「システム メッセージ ロギング ファシリティ」（P.12-2）
- 「注意事項および制約事項」（P.12-5）
- 「デフォルト設定」（P.12-5）
- 「システム メッセージ ロギングの設定」（P.12-5）
- 「システム メッセージ ロギングの設定確認」（P.12-14）
- 「システム メッセージ ロギングの設定例」（P.12-18）
- 「その他の関連資料」（P.12-18）
- 「システム メッセージ ロギング機能の履歴」（P.12-18）

システム メッセージ ロギングの概要

システム メッセージ ロギングを使用して宛先を制御し、システム プロセスが生成するメッセージの重大度をフィルタリングできます。ターミナル セッション、ログ ファイル、およびリモート システム上の Syslog サーバへのロギングを設定できます。

システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

デバイスはデフォルトで、ターミナル セッションにメッセージを出力します。ターミナル セッションへのロギングの設定については、「ターミナル セッションへのシステム メッセージ ロギングの設定」（P.12-6）を参照してください。

表 12-1 に、システム メッセージで使用する重大度を示します。重大度を設定する場合、システムはそのレベル以下のメッセージを出力します。

表 12-1　システム メッセージの重大度

レベル	説明
0：緊急	システムが使用不可
1：アラート	即時処理が必要
2：クリティカル	クリティカル状態

表 12-1　システム メッセージの重大度 （続き）

レベル	説明
3：エラー	エラー状態
4：警告	警告状態
5：通知	正常だが注意を要する状態
6：情報	単なる情報メッセージ
7：デバッグ	デバッグ実行時にのみ表示

デバイスは、重大度 0、1、または 2 のメッセージのうち、最新の 100 個をログに記録します。

メッセージを生成したファシリティと重大度に基づいて記録するシステム メッセージを設定できます。ファシリティについては、「システム メッセージ ロギング ファシリティ」（P.12-2）を参照してください。モジュールおよびファシリティごとの重大度の設定については、「モジュールのシステム メッセージ ロギングの設定」（P.12-8）を参照してください。

Syslog サーバは、Syslog プロトコルに基づいてシステム メッセージを記録するよう設定されたリモート システムで稼動します。最大で 3 台の Syslog サーバを設定できます。Syslog サーバの設定については、「Syslog サーバの設定」（P.12-11）を参照してください。

（注）　最初のデバイス初期化時に、メッセージが Syslog サーバに送信されるのは、ネットワークの初期化後です。

システム メッセージ ロギング ファシリティ

表 12-2 に、システム メッセージ ロギング コンフィギュレーションで使用できるファシリティの一覧を示します。

表 12-2　システム メッセージ ロギング ファシリティ

ファシリティ	説明
aaa	AAA マネージャ
aclmgr	ACL マネージャ
adjmgr	隣接マネージャ
all	すべてのファシリティを表すキーワード
arbiter	アービター マネージャ
arp	ARP マネージャ
auth	許可システム
authpriv	プライベート許可システム
bootvar	Bootvar
callhome	Call home マネージャ
capability	MIG ユーティリティ デーモン
cdp	CDP マネージャ
cert-enroll	証明書登録デーモン
cfs	CFS マネージャ

表 12-2　システム メッセージ ロギング ファシリティ （続き）

ファシリティ	説明
clis	CLIS マネージャ
cmpproxy	CMP プロキシ マネージャ
copp	CoPP マネージャ
core	コア デーモン
cron	cron および at スケジューリング サービス
daemon	システム デーモン
dhcp	DHCP マネージャ
diagclient	GOLD 診断クライアント マネージャ
diagmgr	GOLD 診断マネージャ
eltm	ELTM マネージャ
ethpm	イーサネット PM マネージャ
evmc	EVMC マネージャ
evms	EVMS マネージャ
feature-mgr	Feature マネージャ
fs-daemon	Fs デーモン
ftp	ファイル転送システム
glbp	GLBP マネージャ
hsrp	HSRP マネージャ
im	IM マネージャ
ipconf	IP コンフィギュレーション マネージャ
ipfib	IP FIB マネージャ
kernel	OS カーネル
l2fm	L2 FM マネージャ
l2nac	L2 NAC マネージャ
l3vm	L3 VM マネージャ
license	ライセンス マネージャ
local0	Local use daemon
local1	Local use daemon
local2	Local use daemon
local3	Local use daemon
local4	Local use daemon
local5	Local use daemon
local6	Local use daemon
local7	Local use daemon
lpr	ライン プリンタ システム
m6rib	M6RIB マネージャ
mail	メール システム
mfdm	MFDM マネージャ

表 12-2　システム メッセージ ロギング ファシリティ （続き）

ファシリティ	説明
module	モジュール マネージャ
monitor	イーサネット SPAN マネージャ
mrib	MRIB マネージャ
mvsh	MVSH マネージャ
news	USENET ニュース
nf	NF マネージャ
ntp	NTP マネージャ
otm	GLBP マネージャ
pblr	PBLR マネージャ
pfstat	PFSTAT マネージャ
pixm	PIXM マネージャ
pixmc	PIXMC マネージャ
pktmgr	パケット マネージャ
platform	プラットフォーム マネージャ
pltfm_config	PLTFM コンフィギュレーション マネージャ
plugin	プラグイン マネージャ
port-channel	ポート チャネル マネージャ
port_client	ポート クライアント マネージャ
port_lb	診断ポート ループバック テスト マネージャ
qengine	Q エンジン マネージャ
radius	RADIUS マネージャ
res_mgr	リソース manager
rpm	RPM マネージャ
security	セキュリティ マネージャ
session	セッション マネージャ
spanning-tree	スパニング ツリー マネージャ
syslog	内部 syslog マネージャ
sysmgr	システム マネージャ
tcpudp	TCP および UDP マネージャ
u2	U2 マネージャ
u6rib	U6RIB マネージャ
ufdm	UFDM マネージャ
urib	URIB マネージャ
user	ユーザ プロセス
uucp	UNIX 間コピー システム
vdc_mgr	VDC マネージャ
vlan_mgr	VLAN マネージャ
vmm	VMM マネージャ

表 12-2　システム メッセージ ロギング ファシリティ （続き）

ファシリティ	説明
vshd	VSHD マネージャ
xbar	XBAR マネージャ
xbar_client	XBAR クライアント マネージャ
xbar_driver	XBAR ドライバ マネージャ
xml	XML エージェント

注意事項および制約事項

システム メッセージは、デフォルトでコンソールおよびログ ファイルに記録されます。

デフォルト設定

表 12-3 に、システム メッセージ ロギングのデフォルト設定を示します。

表 12-3　システム メッセージ ロギングのデフォルト

パラメータ	デフォルト
コンソール ロギング	重大度 2 でイネーブル
モニタ ロギング	重大度 5 でイネーブル
ログ ファイル ロギング	重大度 5 でログ メッセージをイネーブル
モジュール ロギング	重大度 5 でイネーブル
ファシリティ ロギング	イネーブル。重大度については「システム メッセージ ロギング ファシリティ」（P.12-2）を参照
タイムスタンプ単位	秒
Syslog サーバ ロギング	ディセーブル
Syslog サーバ設定の配布	ディセーブル

システム メッセージ ロギングの設定

ここでは、次の内容について説明します。

- 「ターミナル セッションへのシステム メッセージ ロギングの設定」（P.12-6）
- 「ターミナル セッションのシステム メッセージ ロギングのデフォルトの復元」（P.12-7）
- 「モジュールのシステム メッセージ ロギングの設定」（P.12-8）
- 「モジュールのシステム メッセージ ロギングのデフォルトの復元」（P.12-9）
- 「ファシリティのシステム メッセージ ロギングの設定」（P.12-9）
- 「ファシリティのシステム メッセージ ロギングのデフォルトの復元」（P.12-11）

- 「Syslog サーバの設定」（P.12-11）
- 「サーバのシステム メッセージ ロギングのデフォルトの復元」（P.12-12）
- 「UNIX または Linux システムを使用したロギングの設定」（P.12-13）
- 「ログ ファイルの表示」（P.12-13）

（注）　NX-OS コマンドは Cisco IOS コマンドと異なる場合があることに注意してください。

ターミナル セッションへのシステム メッセージ ロギングの設定

重大度に基づいて、コンソール、Telnet、および SSH セッションにメッセージを記録するには、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しておく必要があります。

- デフォルトでは、ターミナル セッションでロギングはイネーブルです。

手順の概要

1. **terminal monitor**
2. **config t**
3. **logging console** [*severity-level*]
4. **show logging console**
5. **logging monitor** [*severity-level*]
6. **show logging monitor**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**terminal monitor**
	
	Example:
	`n1000v# terminal monitor`
	`n1000v#`
		デバイスがコンソールにメッセージを記録できるようにします。

ステップ 2	**config t**
	
	Example:
	`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 3	**logging console** [*severity-level*]
	
	Example:
	`n1000v(config)# logging console 2`
	`n1000v(config)#`
		指定された重大度とそれより上位の重大度のメッセージをコンソール セッションに記録するように、デバイスを設定します。重大度は 0 ～ 7 で、表 12-1 に示します。重大度が指定されていない場合、デフォルトの 2 が使用されます。

	コマンド	目的
ステップ 4	**show logging console**	（任意）コンソール ロギング設定を表示します。
ステップ 5	**logging monitor** [*severity-level*] **Example:** n1000v(config)# logging monitor 3 n1000v(config)#	デバイスが指定された重大度とそれより上位の重大度のメッセージをモニタに記録できるようにします。この設定は、Telnet および SSH セッションに適用されます。重大度は 0 ～ 7 で、表 12-1 に示します。重大度が指定されていない場合、デフォルトの 2 が使用されます。
ステップ 6	**show logging monitor**	（任意）モニタ ロギング設定を表示します。
ステップ 7	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）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。

```
Example:
n1000v# terminal monitor
n1000v# config t
n1000v(config)# logging console 2
n1000v(config)# show logging console
Logging console:                enabled (Severity: critical)
n1000v(config)# logging monitor 3
n1000v(config)# show logging monitor
Logging monitor:                enabled (Severity: errors)
n1000v(config)#
n1000v(config)# copy running-config startup-config
```

ターミナル セッションのシステム メッセージ ロギングのデフォルトの復元

ターミナル セッションのシステム メッセージ ロギングのデフォルト設定を復元するには、CLI グローバル コンフィギュレーション モードで次のコマンドを実行します。

コマンド	説明
no logging console [*severity-level*] **Example:** n1000v(config)# no logging console n1000v(config)#	デバイスによるコンソールへのメッセージのロギングをディセーブルにします。
no logging monitor [*severity-level*] **Example:** n1000v(config)# no logging monitor 3 n1000v(config)#	Telnet および SSH セッションへのメッセージのロギングをディセーブルにします。

モジュールのシステム メッセージ ロギングの設定

モジュールごとに記録されるメッセージの重大度とタイムスタンプ ユニットを設定するには、ここに示す手順を実行します。

手順の概要

1. **config t**
2. **logging module** [*severity-level*]
3. **show logging module**
4. **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}
5. **show logging timestamp**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**logging module** [*severity-level*] **Example:** `n1000v(config)# logging module 3`	指定された重大度またはそれ以上の重大度であるモジュール ログ メッセージをイネーブルにします。重大度は 0 ～ 7 で、表 12-1 に示します。重大度が指定されていない場合、デフォルトの 5 が使用されます。
ステップ 3	**show logging module**	（任意）モジュール ロギング設定を表示します。
ステップ 4	**logging timestamp** {**microseconds** | **milliseconds** | **seconds**} **Example:** `n1000v(config)# logging timestamp microseconds`	ロギング タイムスタンプ単位を設定します。デフォルトの単位は秒です。
ステップ 5	**show logging timestamp**	（任意）設定されたロギング タイムスタンプ単位を表示します。
ステップ 6	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	（任意）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。

次に、モジュールのシステム メッセージ ロギングを設定する例を示します。

```
n1000v# config t
```

```
n1000v(config)# logging module 3

n1000v(config)# show logging module
Logging linecard:                enabled (Severity: errors)
n1000v(config)# logging timestamp microseconds
n1000v(config)# show logging timestamp
Logging timestamp:               Microseconds
n1000v(config)# copy running-config
```

モジュールのシステム メッセージ ロギングのデフォルトの復元

モジュールのシステム メッセージ ロギングのデフォルト設定を復元するには、CLI グローバル コンフィギュレーション モードで次のコマンドを実行します。

コマンド	説明
no logging module [*severity-level*] **Example:** n1000v(config)# no logging module 3 n1000v(config)#	モジュールのシステム メッセージ ロギングのデフォルトの重大度を復元します。
no logging timestamp {**microseconds** | **milliseconds** | **seconds**} **Example:** n1000v(config)# no logging timestamp milliseconds	ロギング タイムスタンプ ユニットをデフォルトの秒にリセットします。

ファシリティのシステム メッセージ ロギングの設定

ファシリティごとに記録されるメッセージの重大度とタイムスタンプ ユニットを設定するには、ここに示す手順を実行します。

手順の概要

1. **config t**
2. **logging level** *facility severity-level*
3. **show logging level** [*facility*]
4. **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}
5. **show logging timestamp**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**logging level** *facility severity-level* **Example:** n1000v(config)# logging level aaa 3 n1000v(config)#	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。ファシリティについては、「システム メッセージ ロギング ファシリティ」（P.12-2）を参照してください。重大度は 0 ～ 7 で、表 12-1 に示します。同じ重大度をすべてのファシリティに適用するには、**all** ファシリティを使用します。デフォルト値については、**show logging level** コマンドを参照してください。
ステップ 3	**show logging level** [*facility*] **Example:** n1000v(config)# show logging level aaa	（任意）ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。ファシリティを指定しなかった場合は、すべてのファシリティのレベルが表示されます。
ステップ 4	**logging timestamp** {**microseconds** | **milliseconds** | **seconds**} **Example:** n1000v(config)# logging timestamp microseconds	ロギング タイムスタンプ単位を設定します。デフォルトの単位は秒です。
ステップ 5	**show logging timestamp**	（任意）設定されたロギング タイムスタンプ単位を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）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。

ファシリティのシステム メッセージ ロギングの設定例を示します。

```
n1000v# config t
n1000v(config)# logging level aaa 3
n1000v(config)# show logging level aaa
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
logging timestamp microseconds
n1000v(config)# show logging timestamp
Logging timestamp:              Microseconds
copy running-config startup-config
```

ファシリティのシステム メッセージ ロギングのデフォルトの復元

ファシリティのシステム メッセージ ロギングのデフォルトを復元するには、次のコマンドを使用します。

コマンド	説明

no logging level [*facility severity-level*]
 	
Example:
`n1000v(config)# no logging level aaa 3`
`n1000v(config)#`
	指定したファシリティのデフォルトのロギング重大度を復元します。ファシリティおよび重大度を指定しなかった場合、すべてのファシリティがそれぞれのデフォルト重大度にリセットされます。

no logging timestamp {**microseconds** | **milliseconds** | **seconds**} **Example:** `n1000v(config)# no logging timestamp milliseconds`	ロギング タイムスタンプ ユニットをデフォルトの秒にリセットします。

Syslog サーバの設定

システム メッセージ ロギングのための syslog サーバを設定するには、ここに示す手順を実行します。

手順の概要

1. **config t**
2. **logging server** *host* [*severity-level* [**use_vrf** *vrf-name*]]
3. **show logging server**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** 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	**logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]] **Example:** n1000v(config)# **logging server 10.10.2.2 7**	指定されたホスト名、あるいは IPv4 または IPv6 アドレスで Syslog サーバを設定します。**use_vrf** キーワードを使用すると、メッセージ ロギングを特定の VRF に限定できます。重大度は 0 ～ 7 で、表 12-1 に示します。デフォルトの発信ファシリティは local7 です。 この例では、ファシリティ local 7 のすべてのメッセージを転送します。
ステップ 3	**show logging server** **Example:** n1000v(config)# **show logging server** Logging server: enabled {10.10.2.2} server severity: debugging server facility: local7	（任意）Syslog サーバ設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）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。

サーバのシステム メッセージ ロギングのデフォルトの復元

サーバのシステム メッセージ ロギングのデフォルトを復元するには、ここに示す手順を実行します。

コマンド	説明
no logging server *host* **Example:** n1000v(config)# no logging server host	指定されたホストのロギング サーバを削除します。

UNIX または Linux システムを使用したロギングの設定

UNIX または Linux システムでメッセージ ロギングを設定するには、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、次の点を理解または実行しておく必要があります。

- 次に示すのは、syslog 用に設定する UNIX または Linux のフィールドです。

フィールド	説明
Facility	メッセージの作成者。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7 です。アスタリスク（*）を使用するとすべてを指定します。これらのファシリティ指定により、発信元に基づいてメッセージの宛先を制御できます。 **（注）**　ローカル ファシリティを使用する前に設定をチェックします。
Level	メッセージを記録する最小重大度。debug、info、notice、warning、err、crit、alert、emerg です。アスタリスク（*）を使用するとすべてを指定します。none を使用するとファシリティをディセーブルにできます。
Action	メッセージの宛先。ファイル名、前にアット マーク（@）が付いたホスト名、カンマで区切られたユーザ リストです。アスタリスク（*）を使用するとすべてのログイン ユーザを指定します。

手順の詳細

ステップ 1　UNIX または Linux システムで、次の内容をファイル /var/log/myfile.log に追加します。

```
facility.level <five tab characters> action
```

```
Example:
debug.local7            /var/log/myfile.log
```

ステップ 2　シェル プロンプトで次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

ステップ 3　次のコマンドを入力して、システム メッセージ ロギング デーモンが myfile.log をチェックして、新しい変更を取得するようにします。

```
$ kill -HUP ~cat /etc/syslog.pid~
```

ログ ファイルの表示

ログ ファイル中のメッセージを表示するには、ここに示す手順を実行します。

手順の概要

1. **show logging last** *number-lines*

手順の概要

	コマンド	目的
ステップ 1	**show logging last** *number-lines*	ロギング ファイルの最終行番号を表示します。最終行番号には 1 ～ 9999 を指定できます。

次に、ログ ファイル内の最後の 5 行を表示する例を示します。

```
n1000v#  show logging last 5
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
n1000v#
```

システム メッセージ ロギングの設定確認

システム メッセージ ロギングの設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show logging console	コンソール ロギング設定を表示します。 例 12-1（P.12-15）を参照してください。
show logging info	ロギング設定を表示します。 例 12-2（P.12-15）を参照してください。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。 例 12-3（P.12-16）を参照してください。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。 例 12-4（P.12-16）を参照してください。
show logging module	モジュール ロギング設定を表示します。 例 12-5（P.12-17）を参照してください。
show logging monitor	モニタ ロギング設定を表示します。 例 12-6（P.12-17）を参照してください。
show logging server	Syslog サーバ設定を表示します。 例 12-7（P.12-17）を参照してください。
show logging session	ロギング セッションのステータスを表示します。 例 12-8（P.12-17）を参照してください。

コマンド	目的
show logging status	ロギング ステータスを表示します。 例 12-9（P.12-17）を参照してください。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。 例 12-10（P.12-17）を参照してください。

例 12-1　　show logging console

```
n1000v# show logging console
Logging console:                disabled
n1000v#
```

例 12-2　　show logging info

```
n1000v# show logging info

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: notifications)
Logging linecard:               enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - g/external/messages: Severity - notifications Size - 4194304

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
cdp                     2                       2
cert_enroll             2                       2
cfs                     3                       3
confcheck               2                       2
cron                    3                       3
daemon                  3                       3
diagclient              2                       2
diagmgr                 2                       2
eth_port_channel        5                       5
ethpm                   5                       5
evmc                    5                       5
evms                    2                       2
feature-mgr             2                       2
ftp                     3                       3
ifmgr                   5                       5
igmp_1                  3                       3
ip                      2                       2
ipv6                    2                       2
kern                    6                       6
l2fm                    2                       2
licmgr                  6                       6
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
```

```
local6                  3                       3
local7                  3                       3
lpr                     3                       3
mail                    3                       3
mfdm                    2                       2
module                  5                       5
monitor                 7                       7
msp                     2                       2
mvsh                    2                       2
news                    3                       3
ntp                     2                       2
otm                     3                       3
pblr                    2                       2
pixm                    2                       2
pixmc                   2                       2
platform                5                       5
portprofile             5                       5
private-vlan            3                       3
radius                  2                       2
res_mgr                 2                       2
rpm                     2                       2
sal                     2                       2
securityd               2                       2
sksd                    3                       3
stp                     3                       3
syslog                  3                       3
sysmgr                  3                       3
ufdm                    2                       2
urib                    3                       3
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
vim                     5                       5
vlan_mgr                2                       2
vms                     5                       5
vshd                    5                       5
xmlma                   3                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
n1000v$
```

例 12-3　　show logging last

```
n1000v# show logging last 5
2008 Jul 29 17:52:42 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/5 is up in mode access
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/2 is up in mode trunk
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/4 is up in mode access
2008 Jul 29 17:53:04 S22-DCOS %SYSMGR-3-BASIC_TRACE: process_cfg_write: PID 1858 with
message rcvd cfg_action from
sap 0x545 for vdc 1 at time 1217353984 .
2008 Jul 29 17:53:04 S22-DCOS clis[2558]: CLI-3-NVDB: Batched send failed for component:
clic
n1000v#
```

例 12-4　　show logging level aaa

```
n1000v# show logging level aaa
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2
```

```
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
n1000v#
```

例 12-5　show logging module

```
n1000v# show logging module
Logging linecard:               enabled (Severity: notifications)
n1000v#
```

例 12-6　show logging monitor

```
n1000v# show logging monitor
Logging monitor:                enabled (Severity: errors)
n1000v#
```

例 12-7　show logging server

```
n1000v# show logging server
Logging server:                 enabled
{10.10.2.2}
        server severity:        debugging
        server facility:        local7
n1000v#
```

例 12-8　show logging session status

```
n1000v# show logging session status
Last Action Time Stamp     : Fri Nov 18 11:28:55 1910
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
n1000v#
```

例 12-9　show logging status

```
n1000v# show logging status
Fabric Distribute     : Enabled
Session State         : IDLE
n1000v#
```

例 12-10　show logging timestamp

```
n1000v# show logging timestamp
Logging timestamp:              Seconds
n1000v#
```

システム メッセージ ロギングの設定例

次に、システム メッセージ ロギングを設定する例を示します。

```
config t
  logging console 3
  logging monitor 3
  logging logfile my_log 6
  logging module 3
  logging level aaa 2
  logging timestamp milliseconds
  logging distribute
  logging server 172.28.254.253
  logging server 172.28.254.254 5 local3
  logging commit
  copy running-config startup-config
```

その他の関連資料

システム メッセージ ロギングの実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.12-18）
- 「標準」（P.12-18）

関連資料

関連項目	参照先
システム メッセージ	*『Cisco NX-OS System Messages Reference』*
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	*『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

システム メッセージ ロギング機能の履歴

ここでは、システム メッセージ ロギング機能のリリース履歴を示します。

機能名	リリース	機能情報
システム メッセージ ロギング	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 13

iSCSI マルチパスの設定

この章では、サーバとそのストレージ デバイス間の複数のルートのために iSCSI マルチパスを設定する方法について説明します。次の内容が含まれます。

- 「iSCSI マルチパスについて」（P.13-1）
- 「注意事項および制約事項」（P.13-4）
- 「前提条件」（P.13-5）
- 「デフォルト設定」（P.13-5）
- 「iSCSI マルチパスの設定」（P.13-5）
- 「iSCSI マルチパスの設定の確認」（P.13-18）
- 「ストレージ切断の検出の管理」（P.13-19）
- 「その他の関連資料」（P.13-21）
- 「iSCSI マルチパス機能の履歴」（P.13-21）

iSCSI マルチパスについて

ここでは、次の内容について説明します。

- 「概要」（P.13-1）
- 「サポートされる iSCSI アダプタ」（P.13-2）
- 「VMware スイッチの iSCSI マルチパス設定」（P.13-3）

概要

iSCSI マルチパスとは、サーバとそのストレージ デバイスとの間に複数のルートをセットアップする機能です。常時接続の維持と、トラフィック負荷の分散が可能になります。マルチパス ソフトウェアによって、すべての入力/出力要求が処理され、要求は最善のパスを通して送信されます。ホスト サーバから共有ストレージへのトラフィックの伝送には、iSCSI プロトコルが使用されます。この iSCSI プロトコルによって、SCSI コマンドが iSCSI パケットにパッケージ化され、このパケットがイーサネット ネットワーク上で伝送されます。

iSCSI マルチパスは、パス フェールオーバーを可能にします。パスまたはそのコンポーネントのいずれかで障害が発生した場合、サーバは別の使用可能なパスを選択します。パス フェールオーバーに加えて、マルチパスは、複数の物理パス間でストレージの負荷を分散することで潜在的なボトルネックを低減、またはなくします。

Cisco Nexus 1000V DVS は iSCSI ターゲットに関係なく、iSCSI マルチパスを実行します。ESX サーバの iSCSI デーモンは、ホスト上の 2 つ以上の VMkernel NIC を使用して複数のセッションの iSCSI ターゲットと通信し、それらを Cisco Nexus 1000V の物理 NIC にピン接続します。アップリンクのピン接続は、Cisco Nexus 1000V によって提供されるマルチパスの唯一の機能です。ストレージのバインド、パス選択、パス フェールオーバーなどの他のマルチパス機能は、VMkernel で実行される VMware コードによって提供されます。

iSCSI マルチパスを設定するには、次の手順を実行します。

1. アップリンクのピン接続

   iSCSI アクセス用に作成された VMkernel の各ポートは、1 つの物理 NIC にピン接続されます。

   これは、NIC チーミング ポリシーまたはポート バンドリング ポリシーを無効にします。VMkernel ポートからのトラフィックはすべて、アップストリーム スイッチに到達するためにピン接続されたアップリンクのみ使用します。

2. ストレージのバインド

   VMkernel の各ポートは、VMkernel ポートがピン接続される物理 NIC に関連付けられた VMware iSCSI ホスト バス アダプタ（VMHBA）にピン接続されます。

   ESX または ESXi ホストは物理 NIC 用に次の VMHBA を作成します。

   - ソフトウェアの iSCSI では、すべての物理 NIC に対して VMHBA が 1 つだけ作成されます。
   - ハードウェアの iSCSI では、ハードウェアの iSCSI オフロードをサポートする物理 NIC ごとに VMHBA が 1 つ作成されます。

iSCSI ストレージ エリア ネットワーク（SAN）とともに VMware ESX および VMware ESXi のシステムを使用する方法の詳細については、『*iSCSI SAN Configuration Guide*』を参照してください。

サポートされる iSCSI アダプタ

この項では、使用可能な VMware iSCSI ホスト バス アダプタ（VMHBA）の一覧、および Cisco Nexus 1000V によってサポートされるものを示します。

VMware iSCSI ホスト バス アダプタ（VMHBA）	VSM のサポート対象か。	説明	VMkernel ネットワーキングが必要か。
ソフトウェア	Yes	標準の NIC が IP ネットワーク上のリモート iSCSI ターゲットにホストを接続できるようにします。	Yes
依存するハードウェア	Yes	サードパーティのアダプタはホストからの iSCSI およびネットワーク処理をオフロードしますが、iSCSI 制御処理はオフロードしません。	Yes
独立したハードウェア	No	サードパーティのアダプタはホストからの iSCSI 制御およびネットワーク処理をオフロードします。vSphere Client から直接設定されるため、VSM で設定を行う必要はありません。	No

VMware スイッチの iSCSI マルチパス設定

マルチパスをイネーブルにするか、または設定する前に、ソフトウェアまたはハードウェアの iSCSI アダプタのネットワーキングを設定する必要があります。この設定には、iSCSI アダプタと物理 NIC 間のトラフィック用の VMkernel iSCSI ポートの作成が含まれます。

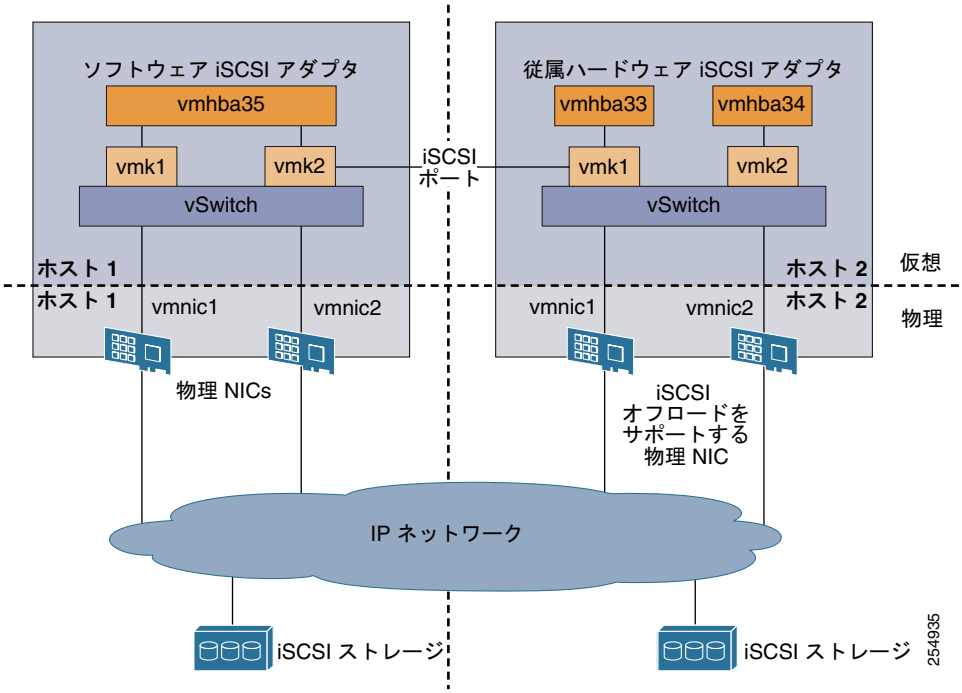
vSwitch では、アップリンクのピン接続は、管理者の手動により、vSphere Client 上で行われます。

ストレージのバインドも、管理者の手動により、ESX ホスト上で直接行われるか、または RCLI を使用して行われます。

ソフトウェアの iSCSI の場合、全体の実装に VMHBA が 1 つだけ必要です。VMkernel のすべてのポートは、このアダプタにバインドされます。たとえば、図 13-1（P.13-3）では、vmk1 と vmk2 の両方が VMHBA35 にバインドされています。

ハードウェアの iSCSI の場合、NIC ごとに別々のアダプタが必要です。VMkernel の各ポートは、ピン接続されている物理 VM NIC のアダプタにバインドされます。たとえば、図 13-1（P.13-3）では、vmk1 は、vmnic1 と関連付けられていて、vmk1 がピン接続されている iSCSI アダプタである VMHBA33 にバインドされています。同様に vmk2 は VMHBA34 にバインドされています。

図 13-1　VMware 仮想スイッチの iSCSI マルチパス



次の表は図 13-1に示されているハードウェアおよびソフトウェアの iSCSI マルチパスの設定で使用されるアダプタおよび NIC を示しています。

ソフトウェア HBA	VMkernel NIC	VM NIC
VMHBA35	1	1
	2	2
ハードウェア HBA		
VMHBA33	1	1
VMHBA34	2	2

注意事項および制約事項

iSCSI マルチパス機能に関する注意事項および制約事項は、次のとおりです。

- vEthernet タイプのポート プロファイルのみ、**capability iscsi-multipath** を指定して設定できます。
- iSCSI マルチパスに使用されるポート プロファイルは、トランク ポート プロファイルではなくアクセス ポート プロファイルである必要があります。
- **capability iscsi-multipath** を指定して設定したポート プロファイルでは、次のことはできません。
  - **capability l3 control** を指定してポート プロファイルを設定することもできません。
  - ポート プロファイルが VMkernel NIC によって継承される場合のシステム VLAN の変更。
  - ポート プロファイルが VMkernel NIC によって継承される場合のアクセス VLAN の変更。
  - ポート モードからトランク モードへの変更。
- VMkernel NIC ポートのみ **capability iscsi-multipath** を指定して設定されているポート プロファイルを継承できます。
- Cisco Nexus 1000V のアップリンクの自動ピン接続を無効にしようとする場合、次の制限が適用されます。
  - VMkernel ポートは、1 つの物理 NIC にのみピン接続できます。
  - ソフトウェア物理 NIC には VMkernel の複数のポートをピン接続できます。
  - ハードウェア物理 NIC には VMkernel の 1 つのポートのみピン接続できます。
- iSCSI イニシエータとストレージがすでに動作可能である必要があります。
- ESX 4.0 Update1 以降ではソフトウェアの iSCSI マルチパスのみサポートされます。
- ESX 4.1 以降ではソフトウェアとハードウェアの iSCSI マルチパスの両方がサポートされます。
- ソフトウェアまたはハードウェアの iSCSI でマルチパスをイネーブルにする、または設定する前に VMkernel ポートを作成する必要があります。
- VMkernel ネットワーキングが iSCSI トラフィックに対して機能している必要があります。
- アクティブな VMkernel NIC がピン接続されているアップリンクを DVS から取り外す前に、VMkernel NIC とその VMHBA 間のバインドを解除する必要があります。次のシステム メッセージは警告として表示されます。

  ```
  vsm# 2010 Nov 10 02:22:12 sekrishn-bl-vsm %VEM_MGR-SLOT8-1-VEM_SYSLOG_ALERT: sfport
  : Removing Uplink Port Eth8/3 (ltl 19), when vmknic lveth8/1 (ltl 49) is pinned to
  this port for iSCSI Multipathing
  ```

- ハードウェアの iSCSI は、Cisco Nexus 1000V Release 4.2(1)SV1(5.1) の新機能です。以前のリリースでソフトウェアの iSCSI マルチパスを設定している場合は、アップグレード後も次の内容が維持されます。
  - マルチパス
  - ソフトウェアの iSCSI アップリンクのピン接続
  - VMHBA アダプタのバインド
  - iSCSI ストレージへのホスト アクセス

  ハードウェア オフロードが可能な NIC を ESX 4.1 で利用するには、「ハードウェアの iSCSI 設定への変換」（P.13-14）の手順を参照してください。
- iSCSI ターゲットとイニシエータは同じサブネットにある必要があります。

前提条件

iSCSI マルチパス機能を使用するための前提条件は次のとおりです。

- VMware iSCSI SAN ストレージ仮想化について理解している。iSCSI ストレージ エリア ネットワーク（SAN）とともに VMware ESX および VMware ESXi のシステムを使用する方法の詳細については、『*iSCSI SAN Configuration Guide*』を参照してください。
- iSCSI イニシエータを VMware ESX/ESXi ホストでセットアップする方法を理解している。
- ホストが次のいずれかですでに機能している。
  - VMware ESX 4.0.1 Update 01（ソフトウェアの iSCSI の場合）
  - VMware ESX 4.1 以降（ソフトウェアとハードウェアの iSCSI の場合）
- iSCSI マルチパス化およびパス フェールオーバーについて理解している。
- VMware カーネル NIC が SAN 外部ストレージにアクセスするように設定されている。

デフォルト設定

表 13-1 に、iSCSI マルチパス コンフィギュレーション内のデフォルト設定を示します。

表 13-1　iSCSI マルチパスのデフォルト

パラメータ	デフォルト
タイプ（port-profile）	vEthernet
説明（port-profile）	なし
VMware ポート グループ名（port-profile）	ポート プロファイルの名前
スイッチポート モード（port-profile）	アクセス
ステート（port-profile）	ディセーブル

iSCSI マルチパスの設定

iSCSI マルチパスを設定するには、次の手順を使用します。

- 「アップリンクのピン接続とストレージのバインド」（P.13-5）の手順
- 「ハードウェアの iSCSI 設定への変換」（P.13-14）の手順
- 「VMkernel NIC アクセス VLAN の変更」（P.13-15）の手順

アップリンクのピン接続とストレージのバインド

ここでは、システム VLAN を使用して設定されている iSCSI マルチパス ポート プロファイルに vEthernet インターフェイスを割り当てることで、iSCSI プロトコルを介してホストとターゲット間に iSCSI マルチパスを設定する方法を説明します。

アップリンクのピン接続とストレージのバインドのプロセス

ステップ 1　「VMkernel NIC のポート プロファイルの作成」（P.13-6）の手順。

ステップ 2　「VMkernel NIC の作成およびポート プロファイルの適用」（P.13-9）の手順。

ステップ 3　次のいずれかを実行します。

- NICS の自動ピン接続を無効にする場合は、「NIC の手動ピン接続」（P.13-10）の手順に進みます。
- そうでない場合は、ストレージのバインドを続行します。

アップリンクのピン接続を完了しました。ストレージのバインドの次のステップに進みます。

ステップ 4　「物理 NIC の iSCSI アダプタの特定」（P.13-11）の手順

ステップ 5　「iSCSI アダプタへの VMkernel NIC のバインド」（P.13-13）の手順

ステップ 6　「iSCSI マルチパスの設定の確認」（P.13-18）の手順

VMkernel NIC のポート プロファイルの作成

VMkernel NIC のポート プロファイルを作成するには、こ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。

- 2 つ以上の物理 NIC が含まれる 1 つのポート チャネルを持つホストを設定済みです。
- マルチパス化をインターフェイス上で設定する必要があります。設定するには、この手順を使用して iSCSI マルチパス ポート プロファイルを作成し、そのポート プロファイルにインターフェイスを割り当てます。
- EXEC モードで CLI にログインしていること。
- この iSCSI マルチパス ポート プロファイルに追加する VLAN の VLAN ID がわかっている必要があります。
  - その VLAN は Cisco Nexus 1000V 上であらかじめ作成しておく必要があります。
  - この iSCSI マルチパス ポート プロファイルに割り当てる VLAN は、システム VLAN であることが必要です。
  - いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN がすでに含まれている必要があります。
- ポート プロファイルは、アクセス ポート プロファイルであることが必要です。トランク ポート プロファイルであってはなりません。ここで説明する手順の中で、ポート プロファイルをアクセス ポート プロファイルとして設定します。

手順の概要

1. **config t**
2. **port-profile type vethernet** *name*
3. **vmware port-group [***name***]**
4. **switchport mode access**

5. **switchport access vlan** *vlanID*
6. **no shutdown**
7. （任意）**system vlan** *vlanID*
8. **capability iscsi-multipath**
9. **state enabled**
10. （任意）**show port-profile** *name*
11. （任意）copy running-config startup-config

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 type vethernet** *name*
	Example:
	`n1000v(config)# port-profile type vethernet VMK-port-profile`
	`n1000v(config-port-prof)#`
		指定したポート プロファイルの CLI 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。
		• **type**：ポート プロファイルを Ethernet タイプまたは vEthernet タイプとして定義します。この設定を後で変更することはできません。デフォルトは vEthernet タイプです。
		（注）　ポート プロファイルを Ethernet タイプとして設定すると、VMware 仮想ポートの設定には使用できなくなります。
		• *name*：ポート プロファイル名の長さは最大 80 文字です。Cisco Nexus 1000V 上の各ポート プロファイルの名前は一意でなければなりません。

ステップ 3	**description** *profile description*
	Example:
	`n1000v(config-port-prof)# description "Port Profile for iSCSI multipath"`
	`n1000v(config-port-prof)#`
		ポート プロファイルに説明を追加します。この説明は、自動的に vCenter Server にプッシュされます。
		profile description：最大 80 の ASCII 文字
		（注）　説明にスペースが含まれる場合、引用符で囲む必要があります。

ステップ 4	**vmware port-group [***name***]**
	Example:
	`n1000v(config-port-prof)# vmware port-group VMK-port-profile`
	`n1000v(config-port-prof)#`
		ポート プロファイルを VMware ポート グループとして指定します。
		ポート プロファイルは、同じ名前の VMware ポート グループにマッピングされます。vCenter Server 接続が確立すると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。
		name：VMware ポート グループ名。ポート プロファイルを別のポート グループ名にマッピングする場合は、別の名前を使用してください。

	コマンド	目的

ステップ 5	**switchport mode access**
	Example:
	`n1000v(config-port-prof)# switchport mode access`
	`n1000v(config-port-prof)#`
		インターフェイスがスイッチ アクセス ポート（デフォルト）であることを指定します。

ステップ 6	**switchport access vlan** *vlanID*
	Example:
	`n1000v(config-port-prof)# switchport access vlan 254`
	`n1000v(config-port-prof)#`
		システム VLAN ID を、このポート プロファイルのアクセス ポートに割り当てます。
		（注） この iSCSI ポート プロファイルに割り当てられる VLAN は、システム VLAN でなければなりません。

ステップ 7	**no shutdown**
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		管理上の目的でプロファイル内のすべてのポートをイネーブルにします。

ステップ 8	**system vlan** *vlanID*
	Example:
	`n1000v(config-port-prof)# system vlan 254`
	`n1000v(config-port-prof)#`
		システム VLAN を、このポート プロファイルに追加します。
		これで、ホストが初めて追加されたときや後で再起動されるときに、VEM が確実に VSM に到達できるようになります。いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN が含まれている必要があります。

ステップ 9	**capability iscsi-multipath**
	Example:
	`n1000v(config-port-prof)# capability iscsi-multipath`
	`n1000v(config-port-prof)#`
		ポートを iSCSI マルチパス化に使用できるようになります。
		vCenter Server で、iSCSI マルチパス ポート プロファイルが選択され、VMkernel NIC ポートに割り当てられている必要があります。

ステップ 10	**state enabled**
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		ポート プロファイルをイネーブルにします。
		このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。

ステップ 11	**show port-profile name** *name*
	Example:
	`n1000v(config-port-prof)# show port-profile name multipath-profile`
	`n1000v(config-port-prof)#`
		（任意）ポート プロファイルの現在のコンフィギュレーションを表示します。

ステップ 12	**copy running-config startup-config** **Example:** `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。
ステップ 13	「アップリンクのピン接続とストレージのバインドのプロセス」（P.13-6）	

VMkernel NIC の作成およびポート プロファイルの適用

この手順を使用して、VMkernel NIC を作成し、それらにポート プロファイルを適用することができます。適用すると、VMkernel NIC が物理 NIC に自動的にピン接続されます。

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。

- 「VMkernel NIC のポート プロファイルの作成」（P.13-6）の手順を使用してポート プロファイルをすでに作成しており、このポート プロファイルの名前を知っている必要があります。
- VMkernel ポートが、vSphere Client 上に直接作成されている必要があります。
- iSCSI VLAN を伝送する物理 NIC ごとに VMkernel NIC を 1 つ作成します。ストレージ デバイスへのパスの数が、作成した VMkernel NIC の数と同じである必要があります。
- この手順の 2 を行うと、VMkernel NIC が物理 NIC に自動的にピン接続されます。そのため、自動ピン接続に関する次のルールを理解しておく必要があります。
  - VMkernel NIC とアップリンクが同じ VLAN を伝送する場合のみ、VMkernel NIC はアップリンクにピン接続されます。
  - iSCSI VLAN を伝送する物理 NIC が多数ある場合は、ハードウェアの iSCSI NIC が最初に選択されます。
  - ソフトウェアの iSCSI NIC は、使用可能なハードウェアの iSCSI NIC がない場合にのみ選択されます。
  - 2 つの VMkernel NIC が同じハードウェアの iSCSI NIC にピン接続されることはありません。
  - 2 つの VMkernel NIC を同じソフトウェアの iSCSI NIC にピン接続できます。

ステップ 1　iSCSI VLAN を伝送する物理 NIC ごとに VMkernel NIC を 1 つ作成します。

たとえば、2 つのパスを設定する場合は、Cisco Nexus 1000V DVS に 2 つの物理 NIC を作成して iSCSI VLAN を伝送します。2 つの物理 NIC は、他の VLAN を伝送する場合があります。2 つのパス用の VMkernel NIC を 2 つ作成します。

ステップ 2　**capability iscsi-multipath** を指定して設定したポート プロファイルを VMkernel ポートに適用します。

Cisco Nexus 1000V は、VMkernel NIC を物理 NIC に自動的にピン接続します。

ステップ 3　ESX ホストで、自動ピン接続の設定を表示して確認します。

~ # vemcmd show iscsi pinning

Example:

```
~ # vemcmd show iscsi pinning
Vmknic    LTL      Pinned_Uplink    LTL
vmk6      49       vmnic2           19
vmk5      50       vmnic1           18
```

ステップ 4　これで手順は完了です。「アップリンクのピン接続とストレージのバインドのプロセス」（P.13-6）に戻ってください。

NIC の手動ピン接続

この手順を使用して、Cisco Nexus 1000V によって行われる NIC の自動ピン接続を無効にして、VMkernel NIC を物理 NIC に手動でピン接続できます。

（注）　Cisco Nexus 1000V によって自動的に行われたピン接続が最適ではない場合、またはピン接続を変更する場合は、この手順で説明されている、ESX ホストで vemcmd を使用してピン接続を無効にする方法を参照してください。

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 ホストにログインしている。
- VMkernel NIC をすでに作成していて、ポート プロファイルを適用している場合は、「VMkernel NIC の作成およびポート プロファイルの適用」（P.13-9）の手順を使用します。
- ピン接続を変更する前に、iSCSI VMkernel NIC と VMHBA 間のバインドを解除する必要があります。この手順には、解除のステップも含まれています。
- 手動のピン接続は、ESX ホストのリブート後も維持されます。VMkernel NIC を DVS から vSwitch に移動して戻した場合、手動のピン接続は失われます。

ステップ 1　各 VMHBA のバインドを表示して、解除するバインドを特定します（iSCSI VMkernel NIC から VMHBA）。

esxcli swiscsi nic list -d vmhba*nn*

```
Example:
esxcli swiscsi nic list -d vmhba33
vmk6
    pNic name: vmnic2
    ipv4 address: 169.254.0.1
    ipv4 net mask: 255.255.0.0
    ipv6 addresses:
    mac address: 00:1a:64:d2:ac:94
    mtu: 1500
    toe: false
    tso: true
    tcp checksum: false
    vlan: true
    link connected: true
    ethernet speed: 1000
    packets received: 3548617
    packets sent: 102313
    NIC driver: bnx2
    driver version: 1.6.9
    firmware version: 3.4.4
vmk5
    pNic name: vmnic3
    ipv4 address: 169.254.0.2
    ipv4 net mask: 255.255.0.0
    ipv6 addresses:
    mac address: 00:1a:64:d2:ac:94
    mtu: 1500
    toe: false
    tso: true
    tcp checksum: false
    vlan: true
```

```
link connected: true
ethernet speed: 1000
packets received: 3548617
packets sent: 102313
NIC driver: bnx2
driver version: 1.6.9
firmware version: 3.4.4
```

ステップ 2　iSCSI VMkernel NIC と VMHBA 間のバインドを解除します。

Example:

```
esxcli swiscsi nic remove --adapter vmhba33 --nic vmk6
esxcli swiscsi nic remove --adapter vmhba33 --nic vmk5
```

（注）　アクティブな iSCSI セッションがホストとターゲットの間に存在する場合、iSCSI ポートは接続解除できません。

ステップ 3　EXS のホストで自動ピン接続の設定を表示します。

~ # vemcmd show iscsi pinning

Example:

```
~ # vemcmd show iscsi pinning
Vmknic    LTL      Pinned_Uplink    LTL
vmk6      49       vmnic2           19
vmk5      50       vmnic1           18
```

ステップ 4　VMkernel NIC を物理 NIC に手動でピン接続して、自動ピン接続の設定を無効にします。

~ # vemcmd set iscsi pinning *vmk-ltl vmnic-ltl*

Example:

~ # vemcmd set iscsi pinning 50 20

ステップ 5　手動のピン接続を確認します。

~ # vemcmd show iscsi pinning

Example:

```
~ # vemcmd show iscsi pinning
Vmknic    LTL      Pinned_Uplink    LTL
vmk6      49       vmnic2           19
vmk5      50       vmnic3           20
```

ステップ 6　これで手順は完了です。「アップリンクのピン接続とストレージのバインドのプロセス」（P.13-6）に戻ってください。

物理 NIC の iSCSI アダプタの特定

次の手順のいずれかを使用して、物理 NIC に関連付けられている iSCSI アダプタを特定できます。

- 「vSphere Client の iSCSI アダプタの特定」（P.13-12）の手順
- 「ホスト サーバの iSCSI アダプタの特定」（P.13-12）の手順

vSphere Client の iSCSI アダプタの特定

vSphere Client でこの手順を使用して、物理 NIC に関連付けられている iSCSI アダプタを特定できます。

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。

- vSphere Client にログインしている。

ステップ 1　[Inventory] パネルでホストを選択します。

ステップ 2　[Configuration] タブをクリックします。

ステップ 3　[Hardware] パネルの [Storage Adapters] をクリックします。

依存するハードウェアの iSCSI アダプタが、ストレージ アダプタのリストに表示されます。

ステップ 4　アダプタを選択し、[Properties] をクリックします。

iSCSI イニシエータの [Properties] ダイアログボックスには、iSCSI 名および iSCSI エイリアスを含むアダプタに関する情報が表示されます。

ステップ 5　iSCSI アダプタに関連付けられている物理 NIC の名前を探します。

デフォルトの iSCSI エイリアスは次の形式になります。*driver_name-vmnic #*、*vmnic #* は、iSCSI アダプタに関連付けられている NIC です。

ステップ 6　これで手順は完了です。「アップリンクのピン接続とストレージのバインドのプロセス」（P.13-6）に戻ってください。

ホスト サーバの iSCSI アダプタの特定

ESX または ESXi ホストでこの手順を使用して、物理 NIC に関連付けられている iSCSI アダプタを特定できます。

はじめる前に

この手順を開始する前に、次のことを実行する必要があります。

- サーバ ホストにログインする。

ステップ 1　サーバのストレージ アダプタを一覧表示します。

esxcfg-scsidevs –a

```
Example:
esxcfg-scsidevs -a
vmhba33 bnx2i unbound   iscsi.vmhba33 Broadcom iSCSI Adapter
vmhba34 bnx2i online    iscsi.vmhba34 Broadcom iSCSI Adapter
```

ステップ 2　アダプタごとに、バインドされている物理 NIC を表示します。

esxcli swiscsi vmnic list –d *adapter-name*

```
Example:
esxcli swiscsi vmnic list -d vmhba33 | grep name
    vmnic name: vmnic2
```

```
esxcli swiscsi vmnic list -d vmhba34 | grep name
    vmnic name: vmnic3
```

ソフトウェアの iSCSI アダプタの場合、サーバのすべての物理 NIC が一覧表示されます。

ハードウェアの iSCSI アダプタごとに、1 つの物理 NIC が表示されます。

ステップ 3　これで手順は完了です。次に示されている項に戻ります。

- 「アップリンクのピン接続とストレージのバインドのプロセス」（P.13-6）。
- 「ハードウェアの iSCSI 設定への変換のプロセス」（P.13-14）。
- 「アクセス VLAN の変更のプロセス」（P.13-15）。

iSCSI アダプタへの VMkernel NIC のバインド

この手順を使用して、ピン接続されている物理 NIC に対応する iSCSI アダプタに物理 VMkernel NIC を手動でバインドできます。

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。

- ESX ホストにログインしている。
- 「物理 NIC の iSCSI アダプタの特定」（P.13-11）の手順 で確認した、物理 NIC と関連付けられている iSCSI アダプタがわかっている。

ステップ 1　VEM が VMkernel NIC にピン接続されている物理 NIC を見つけます。

Example:

```
Vmknic LTL Pinned_Uplink LTL
vmk2   48  vmnic2        18
vmk3   49  vmnic3        19
```

ステップ 2　「物理 NIC の iSCSI アダプタの特定」（P.13-11）の手順 で確認した iSCSI アダプタに物理 NIC をバインドします。

Example:

```
esxcli swiscsi nic add --adapter vmhba33 --nic vmk2
```

Example:

```
esxcli swiscsi nic add --adapter vmhba34 --nic vmk3
```

ステップ 3　これで手順は完了です。次に示されている項に戻ります。

- 「アップリンクのピン接続とストレージのバインドのプロセス」（P.13-6）。
- 「ハードウェアの iSCSI 設定への変換のプロセス」（P.13-14）。
- 「アクセス VLAN の変更のプロセス」（P.13-15）。

ハードウェアの iSCSI 設定への変換

ESX 4.1 ホストでこの項の手順を使用して、ソフトウェアの iSCSI からハードウェアの iSCSI に変換できます。

はじめる前に

ここに示す手順を開始する前に、次の点を理解または実行しておく必要があります。

- この変換用のメンテナンス時間をスケジュールしている。ソフトウェアからハードウェアの iSCSI への設定の変換には、ストレージの更新が含まれます。

ハードウェアの iSCSI 設定への変換のプロセス

次の手順を使用して、ハードウェアの iSCSI 設定に変換できます。

ステップ 1　vSphere Client で、iSCSI NIC で行ったストレージ設定を解除します。

ステップ 2　iSCSI ターゲットへのパスを削除します。

ステップ 3　「ソフトウェアの iSCSI アダプタへのバインドの解除」（P.13-14）の手順 を使用して、VMkernel NIC と iSCSI アダプタ間のバインドを解除します。

ステップ 4　VMkernel NIC を Cisco Nexus 1000V DVS から vSwitch に移動します。

ステップ 5　ESX ホストにハードウェアの NIC をインストールします（まだインストールされていない場合）。

ステップ 6　次のいずれかを実行します。

- ハードウェアの NIC がすでに Cisco Nexus 1000V DVS に存在する場合は、次のステップに進みます。
- ハードウェアの NIC がまだ Cisco Nexus 1000V DVS に存在しない場合は、「DVS へのハードウェアの NIC の追加」（P.13-15）の手順に進みます。

ステップ 7　VMkernel NIC を vSwitch から Cisco Nexus 1000V DVS に戻します。

ステップ 8　「物理 NIC の iSCSI アダプタの特定」（P.13-11）の手順 を使用して iSCSI アダプタを検索します。

ステップ 9　「iSCSI アダプタへの VMkernel NIC のバインド」（P.13-13）の手順 を使用して NIC をアダプタにバインドします。

ステップ 10　「iSCSI マルチパスの設定の確認」（P.13-18）の手順 を使用して iSCSI マルチパス設定を確認します。

ソフトウェアの iSCSI アダプタへのバインドの解除

この手順を使用して、iSCSI VMkernel NIC とソフトウェアの iSCSI アダプタ間のバインドを解除できます。

ステップ 1　VMHBA への iSCSI VMkernel NIC のバインドを解除します。

```
Example:
esxcli swiscsi nic remove --adapter vmhba33 --nic vmk6
esxcli swiscsi nic remove --adapter vmhba33 --nic vmk5
```

ステップ 2　これで手順は完了です。「ハードウェアの iSCSI 設定への変換のプロセス」（P.13-14）に戻ってください。

DVS へのハードウェアの NIC の追加

この手順を使用して、ハードウェアの NIC が Cisco Nexus 1000V DVS にない場合に、vSphere Client を使用して DVS にアップリンクを追加できます。

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。

- vSphere Client にログインしている。
- この手順では、サーバのリブートが必要です。

ステップ 1　[Inventory] パネルでサーバを選択します。

ステップ 2　[Configuration] タブをクリックします。

ステップ 3　[Configuration] パネルで、[Networking] をクリックします。

ステップ 4　[vNetwork Distributed Switch] をクリックします。

ステップ 5　[Manage Physical Adapters] をクリックします。

ステップ 6　ハードウェア NIC に使用するポート プロファイルを選択します。

ステップ 7　[Click to Add NIC] をクリックします。

ステップ 8　[Unclaimed Adapters] で、物理 NIC を選択し、[OK] をクリックします。

ステップ 9　[Manage Physical Adapters] ウィンドウで [OK] をクリックします。

ステップ 10　vSwitch から Cisco Nexus 1000V DVS に iSCSI VMkernel NIC を移動します。

VMkernel NIC は、ハードウェアの NIC に自動的にピン接続されます。

ステップ 11　これで手順は完了です。「ハードウェアの iSCSI 設定への変換のプロセス」（P.13-14）に戻ってください。

VMkernel NIC アクセス VLAN の変更

この項の手順を使用して、iSCSI VMkernel のアクセス VLAN、またはネットワーキング設定を変更できます。

アクセス VLAN の変更のプロセス

次の手順を使用して、VMkernel NIC アクセス VLAN を変更できます。

ステップ 1　vSphere Client で、iSCSI NIC で行ったストレージ設定を解除します。

ステップ 2　iSCSI ターゲットへのパスを削除します。

ステップ 3　「ソフトウェアの iSCSI アダプタへのバインドの解除」（P.13-14）の手順 を使用して、VMkernel NIC と iSCSI アダプタ間のバインドを解除します。

ステップ 4　VMkernel NIC を Cisco Nexus 1000V DVS から vSwitch に移動します。

ステップ 5　「アクセス VLAN の変更」（P.13-16）の手順 を使用してアクセス VLAN を変更します。

ステップ 6　VMkernel NIC を vSwitch から Cisco Nexus 1000V DVS に戻します。

ステップ 7　「物理 NIC の iSCSI アダプタの特定」（P.13-11）の手順 を使用して iSCSI アダプタを検索します。

ステップ 8　「iSCSI アダプタへの VMkernel NIC のバインド」（P.13-13）の手順 を使用して NIC をアダプタにバインドします。

ステップ 9　「iSCSI マルチパスの設定の確認」（P.13-18）の手順 を使用して iSCSI マルチパス設定を確認します。

アクセス VLAN の変更

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 ホストにログインしている。
- iSCSI マルチパス ポート プロファイルのアクセス VLAN は、VMkernel NIC によって継承されている場合は変更できません。継承を確認するには、**show port-profile name** *profile-name* コマンドを使用します。

ステップ 1　vSphere Client から iSCSI ターゲットへのパスを削除します。

ステップ 2　各 VMHBA のバインドを表示して、解除するバインドを特定します（iSCSI VMkernel NIC から VMHBA）。

esxcli swiscsi nic list -d vmhba*nn*

```
Example:
esxcli swiscsi nic list -d vmhba33
vmk6
    pNic name: vmnic2
    ipv4 address: 169.254.0.1
    ipv4 net mask: 255.255.0.0
    ipv6 addresses:
    mac address: 00:1a:64:d2:ac:94
    mtu: 1500
    toe: false
    tso: true
    tcp checksum: false
    vlan: true
    link connected: true
    ethernet speed: 1000
    packets received: 3548617
    packets sent: 102313
    NIC driver: bnx2
    driver version: 1.6.9
    firmware version: 3.4.4
vmk5
    pNic name: vmnic3
    ipv4 address: 169.254.0.2
    ipv4 net mask: 255.255.0.0
    ipv6 addresses:
```

```
mac address: 00:1a:64:d2:ac:94
mtu: 1500
toe: false
tso: true
tcp checksum: false
vlan: true
link connected: true
ethernet speed: 1000
packets received: 3548617
packets sent: 102313
NIC driver: bnx2
driver version: 1.6.9
firmware version: 3.4.4
```

ステップ 3　VMHBA への iSCSI VMkernel NIC のバインドを解除します。

Example:

```
esxcli swiscsi nic remove --adapter vmhba33 --nic vmk6 esxcli swiscsi nic remove --adapter
vmhba33 --nic vmk5
```

ステップ 4　ポート プロファイルから **capability iscsi-multipath** の設定を削除します。

no capability iscsi-multipath

Example:

```
n1000v# config t
n1000v(config)# port-profile type vethernet VMK-port-profile
n1000v(config-port-prof)# no capability iscsi-multipath
```

ステップ 5　システム VLAN を削除します。

no system vlan *vlanID*

Example:

```
n1000v# config t
n1000v(config)# port-profile type vethernet VMK-port-profile
n1000v(config-port-prof)# no system vlan 300
```

ステップ 6　ポート プロファイルのアクセス VLAN を変更します。

switchport access vlan *vlanID*

Example:

```
n1000v# config t
n1000v(config)# port-profile type vethernet VMK-port-profile
n1000v(config-port-prof)# switchport access vlan 300
```

ステップ 7　システム VLAN を追加します。

system vlan *vlanID*

Example:

```
n1000v# config t
n1000v(config)# port-profile type vethernet VMK-port-profile
n1000v(config-port-prof)# system vlan 300
```

ステップ 8　ポート プロファイルに **capability iscsi-multipath** の設定を追加し直します。

capability iscsi-multipath

Example:

```
n1000v# config t
n1000v(config)# port-profile type vethernet VMK-port-profile
n1000v(config-port-prof)# capability iscsi-multipath
```

ステップ 9　これで手順は完了です。「アクセス VLAN の変更のプロセス」（P.13-15）に戻ってください。

iSCSI マルチパスの設定の確認

この項のコマンドを使用して、iSCSI マルチパスの設定を確認できます。

コマンド	目的
`~ # vemcmd show iscsi pinning`	VMkernel NIC の自動ピン接続を表示します 例 13-1（P.13-18）を参照してください。
esxcli swiscsi nic list -d vmhba33	VMkernel NIC の iSCSI アダプタのバインドを表示します。 例 13-2（P.13-18）を参照してください。
show port-profile [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	ポート プロファイルの設定を表示します。 例 13-3（P.13-18）を参照してください。

例 13-1　~ # vemcmd show iscsi pinning

```
~ # vemcmd show iscsi pinning
Vmknic    LTL       Pinned_Uplink     LTL
vmk6      49        vmnic2            19
vmk5      50        vmnic1            18
```

例 13-2　esxcli swiscsi nic list -d vmhbann

```
esxcli swiscsi nic list -d vmhba33
vmk6
    pNic name: vmnic2
    ipv4 address: 169.254.0.1
    ipv4 net mask: 255.255.0.0
    ipv6 addresses:
    mac address: 00:1a:64:d2:ac:94
    mtu: 1500
    toe: false
    tso: true
    tcp checksum: false
    vlan: true
    link connected: true
    ethernet speed: 1000
    packets received: 3548617
    packets sent: 102313
    NIC driver: bnx2
    driver version: 1.6.9
    firmware version: 3.4.4
```

例 13-3　show port-profile name iscsi-profile

```
n1000v# show port-profile name iscsi-profile
port-profile iscsi-profile
 type: Vethernet
 description:
 status: enabled
```

```
 max-ports: 32
 inherit:
 config attributes:
 evaluated config attributes:
 assigned interfaces:
 port-group:
 system vlans: 254
 capability l3control: no
 capability iscsi-multipath: yes
 port-profile role: none
 port-binding: static
n1000v#
```

ストレージ切断の検出の管理

ここでは、ストレージ接続の切断を検出する設定を行い、ストレージの切断が検出されたときにサポートを提供するコマンドについて説明します。VSM が NFS または iSCSI などのリモート ストレージ システムでホストされている場合、ストレージの接続が失われる可能性があります。この接続の切断によって予期しない VSM 動作が生じることがあります。

ストレージの切断の検出を設定するには、次のコマンド構文を使用します。

system storage-loss { log | reboot } [time <interval>] | no system storage-loss [{ log | reboot }] [time <interval>]

時間間隔値は、VSM がストレージ接続のステータスをチェックする間隔です。ストレージの切断が検出されると、Syslog が表示されます。デフォルトの間隔は 30 秒です。30 ～ 600 秒の間で間隔を設定できます。このコマンドのデフォルト設定は次のとおりです。

system storage-loss log time 30

（注）　このコマンドは EXEC モードで設定します。コンフィギュレーション モードは使用しないでください。

次に、このコマンドがストレージの切断の検出を管理する方法について説明します。

- ログのみ：ストレージの切断が発生したことを示す Syslog メッセージが表示されます。管理者は予期せぬ VSM 状態にならないようにただちにアクションを取る必要があります。
- リセット：ストレージの切断が検出された VSM が予期せぬ VSM 状態にならないように自動的にリロードされます。
  - アクティブ VSM のストレージの切断：アクティブ VSM がリロードされます。スタンバイ VSM がアクティブになり、ホストを制御します。
  - スタンバイ VSM のストレージの切断：スタンバイ VSM がリロードされます。アクティブ VSM がホストを制御し続けます。

（注）　ストレージの切断が VSM の動作に影響を与えないように、同じリモート ストレージにアクティブ VSM とスタンバイ VSM を設定しないでください。

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。

手順の概要

1. **system storage-loss** *{time <interval>}*
2. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**system storage-loss log time 30** **Example:** n1000v# system storage-loss log time 30 n1000v#	秒単位の時間間隔を設定してストレージ接続をチェックし、ステータスを記録します。デフォルトの間隔は 30 秒です。
ステップ 2	**copy running-config startup-config** **Example:** n1000v# copy run start n1000v#	持続性メモリ内のスタートアップ コンフィギュレーションに実行コンフィギュレーションの設定の変更を保存します。

例

次のコマンドは、storage-loss のチェックをディセーブルにします。VSM がローカル ストレージにインストールされている場合は常に、これが推奨の設定です。

```
n1000v# no system storage-loss
```

（注）　両方の VSM がローカル ストレージにある場合は、ストレージの切断のチェックをディセーブルにします。

次のコマンドは、アクティブまたはスタンバイ VSM のストレージの切断の検出時間間隔をイネーブルにし、ストレージの切断に関する Syslog メッセージを表示します。この例では、VSM のストレージの切断は 60 秒ごとにチェックされます。管理者は、ストレージを回復するためのアクションを取り、矛盾した VSM 状態にならないようにする必要があります。

```
n1000v# system storage-loss log time 60
```

以下のコマンドにより、50 秒ごとにストレージの切断の検出が実行されます。

```
n1000v# system storage-loss log time 50
```

次の例は、ストレージの切断が検出された場合にだけログを記録するように設定するために使用するコマンドを示しています。

```
n1000v# system storage-loss log time 60
n1000v# copy run start
```

次の例は、ストレージの切断が検出された場合にリブートするように VSM を設定するために使用するコマンドを示しています。

```
n1000v# system storage-loss reboot time 60
n1000v# copy run start
```

次の例は、ストレージの切断のチェックをディセーブルにするために使用するコマンドを示しています。

```
n1000v# no system storage-loss
n1000v# copy run start
```

その他の関連資料

iSCSI マルチパスの実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.13-21）
- 「標準」（P.13-21）

関連資料

関連項目	参照先
VMware SAN 設定	『VMware SAN Configuration Guide』
ポート プロファイルの設定	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』
インターフェイス コンフィギュレーション	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』
Cisco Nexus 1000V のすべてのコマンドのコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、および例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

iSCSI マルチパス機能の履歴

表 13-2 に、iSCSI マルチパス機能のリリース履歴を示します。

表 13-2　iSCSI マルチパス機能の履歴

機能名	リリース	機能情報
ハードウェアの iSCSI マルチパス	4.2(1)SV1(4)	ハードウェアの iSCSI マルチパスのサポートが追加されました。
iSCSI マルチパス	4.0(4)SV1(2)	iSCSI マルチパス機能が追加されました。

CHAPTER 14

VSM バックアップとリカバリの設定

この章では、仮想スーパーバイザ モジュール（VSM）のバックアップとリカバリの手順を設定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。

- 「VSM バックアップとリカバリに関する情報」（P.14-1）
- 「注意事項および制約事項」（P.14-1）
- 「VSM バックアップとリカバリの設定」（P.14-2）
- 「その他の関連資料」（P.14-23）
- 「VSM バックアップとリカバリの機能の履歴」（P.14-24）

VSM バックアップとリカバリに関する情報

VSM バックアップとリカバリの手順を使用して、ハイ アベイラビリティ（HA）環境にある両方の VSM で障害が発生した場合に、VSM を再作成できるテンプレートを作成できます。

（注） 初期バックアップ後に定期的にバックアップを実行して、最新の設定を保持できるようにすることを推奨します。「定期的なバックアップの実行」（P.14-8）を参照してください。

注意事項および制約事項

VSM バックアップとリカバリには次の注意事項と制約事項があります。

- VSM のバックアップはワンタイム タスクです。
- VSM をバックアップするには、ネットワーク管理者とサーバ管理者間で調整をする必要があります。
- 次の手順は Release 4.0(4)SV1(3) 以降のリリースに当てはまります。
- これらの手順は、アップグレードやダウングレード用ではありません。
- これらの手順では、バックアップを作成したものと同じリリースの VSM で復元を実行する必要があります。
- コンフィギュレーション ファイルには VSM を再作成するための十分な情報はありません。

VSM バックアップとリカバリの設定

ここでは、次の内容について説明します。

- 「VSM のバックアップの実行」（P.14-2）
- 「定期的なバックアップの実行」（P.14-8）
- 「VSM のリカバリ」（P.14-8）

（注）　Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があることに注意してください。

VSM のバックアップ

ここでは、次の内容について説明します。

- 「VSM のバックアップの実行」（P.14-2）
- 「定期的なバックアップの実行」（P.14-8）

VSM のバックアップの実行

ここでは、VSM のバックアップを作成する方法について説明します。

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。

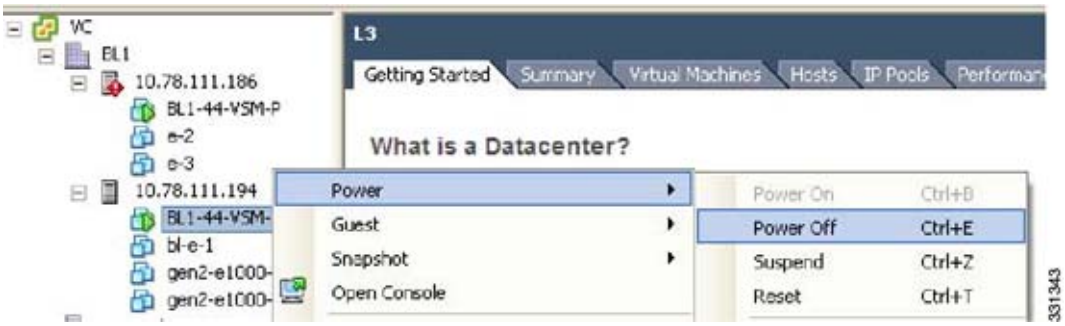
- VSM が仮想イーサネット モジュール（VEM）ホストにある場合、システム VLAN として管理 VLAN を設定する必要があります。
- この手順を開始する前に、VSM で、**copy running-config startup-config** コマンドを入力します。

手順

ステップ 1　vSphere Client を開きます。

[vSphere Client] ウィンドウが開きます。図 14-1 を参照してください。

図 14-1　[vSphere Client] ウィンドウ

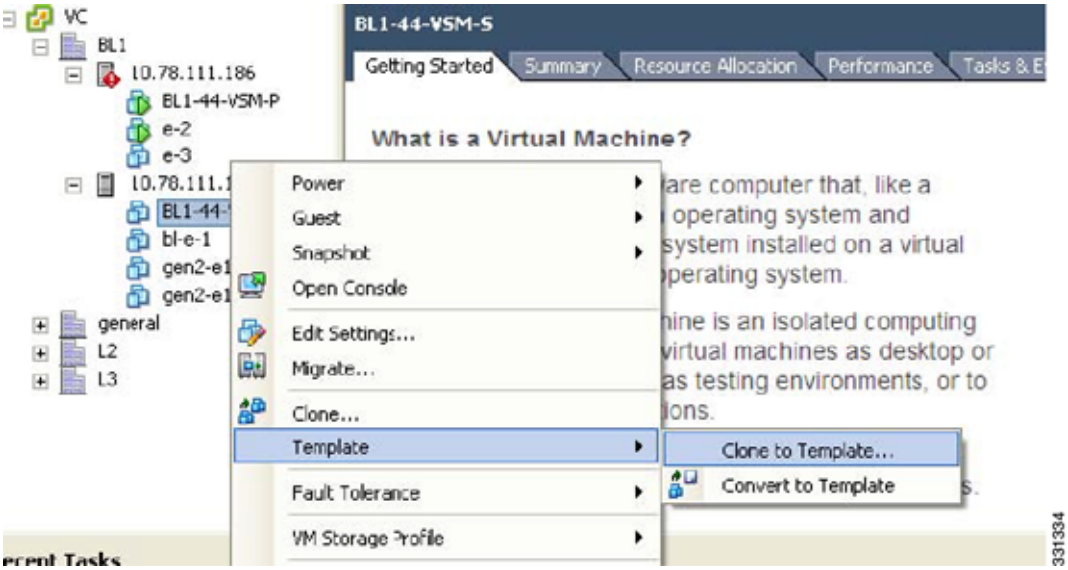


ステップ 2　左側のナビゲーション ペインで、スタンバイ VSM を右クリックします。

ドロップダウン リストが表示されます。

ステップ 3　[Power] > [Power Off] を選択します。

図 14-2　[Clone to Template] ウィンドウ



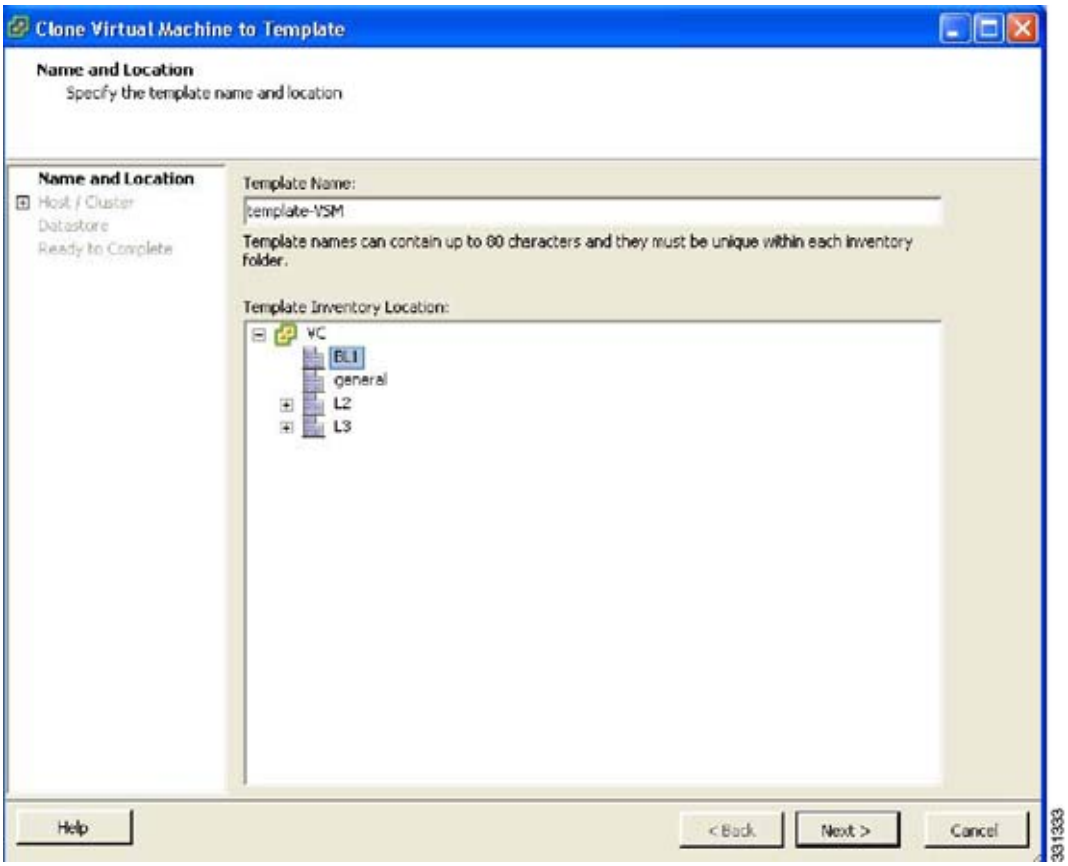
ステップ 4　左側のナビゲーション ペインで、スタンバイ VSM を右クリックします。

ドロップダウン リストが表示されます。

ステップ 5　[Template] > [Clone to Template] を選択します。

[Clone Virtual Machine to Template] 画面が開きます。図 14-3 を参照してください。

図 14-3　[Clone Virtual Machine to Template] 画面



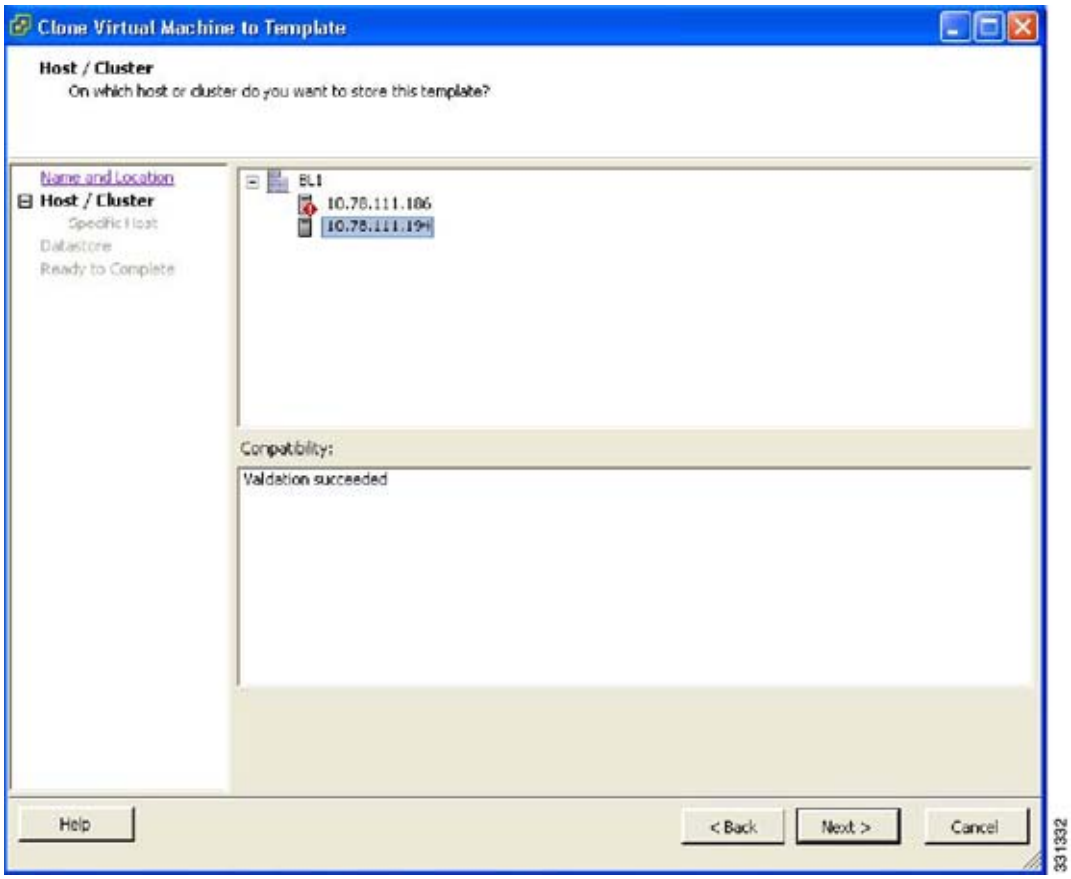
ステップ 6　[Template Name] フィールドに名前を入力します。

ステップ 7　[Template Inventory Location] ペインで、テンプレートの場所を選択します。

ステップ 8　[Next] をクリックします。

[Choosing the Host] 画面が開きます。図 14-4 を参照してください。

図 14-4　[Choosing the Host] 画面

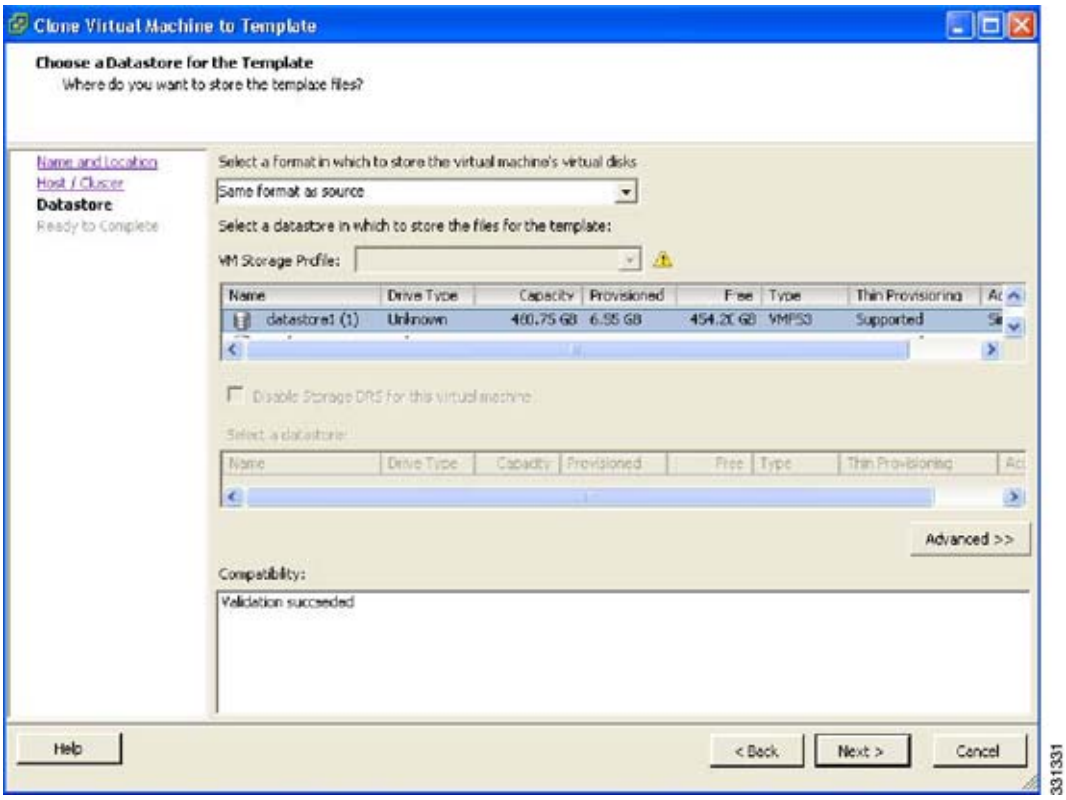


ステップ 9　テンプレートを格納するホストを選択します。

ステップ 10　[Next] をクリックします。

[Choosing a Datastore] 画面が開きます。図 14-5 を参照してください。

図 14-5　[Choosing a Datastore] 画面



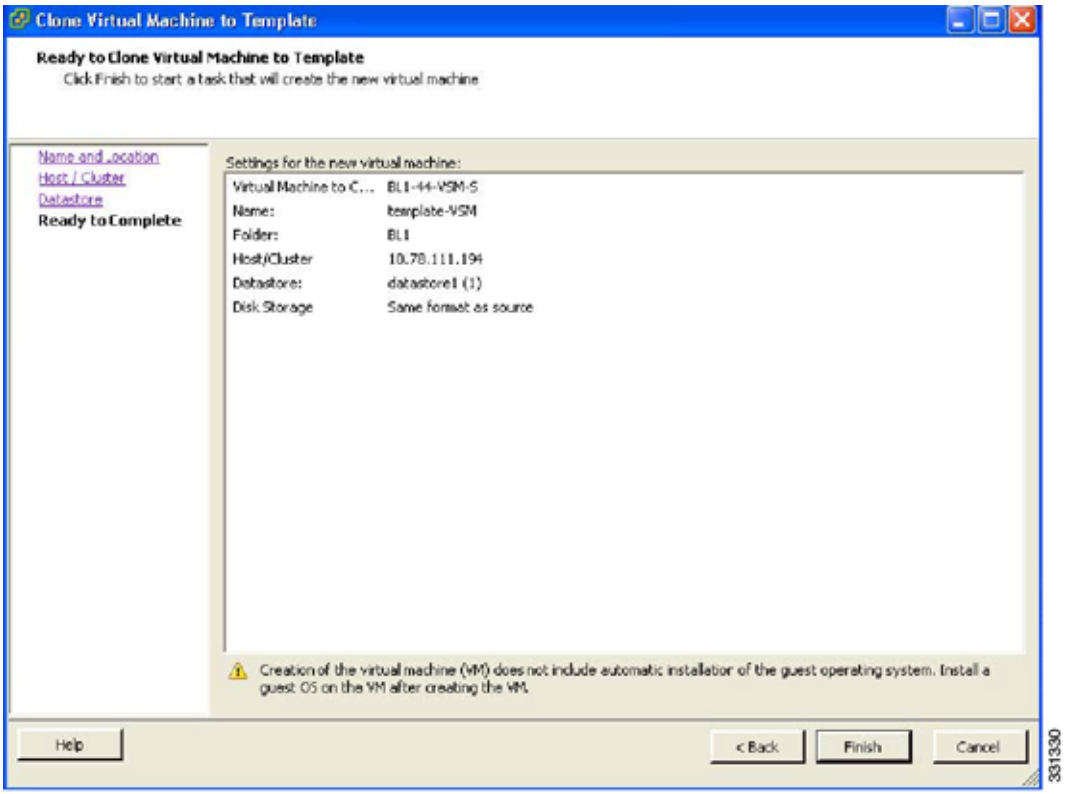
ステップ 11　[Select a format in which to store the virtual machine's virtual disks] ドロップダウン リストで、[Same format as source] を選択します。

ステップ 12　データストアを選択します。

ステップ 13　[Next] をクリックします。

[Confirming Settings] 画面が開きます。図 14-6 を参照してください。

図 14-6　[Confirming Settings] 画面

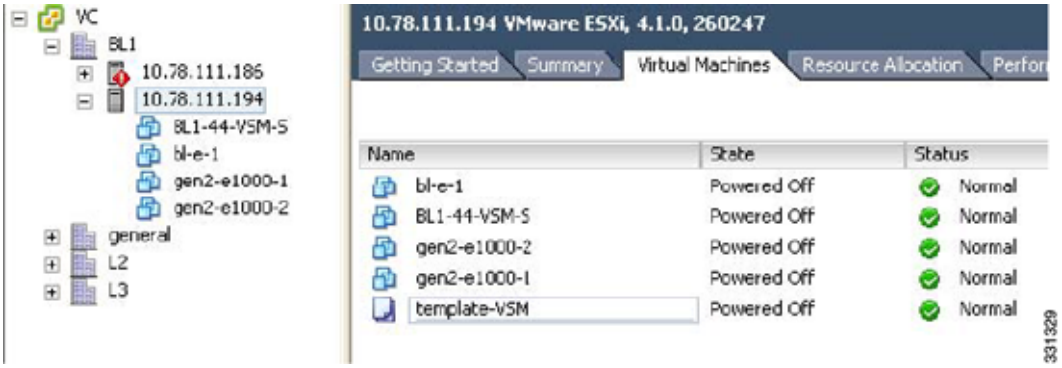


ステップ 14　新しい仮想マシンの設定を確認し、[Finish] をクリックします。

バックアップのテンプレートが作成され、[Virtual Machines] タブに表示されます。

[Template Virtual Machine] ウィンドウが開きます。図 14-7 を参照してください。

図 14-7　[Template Virtual Machine] ウィンドウ



これで、テンプレートの作成が完了しました。

定期的なバックアップの実行

ここでは、スタンバイ VSM の初期バックアップ実行後に、アクティブ VSM をバックアップする方法について説明します。

この手順を実行する必要がある事例をいくつか示します。

- アップグレードを実行した。
- 設定に大幅な変更を加えた。

手順

ステップ 1　次のようなコマンドを入力して、VSM をバック アップします。

```
switch# copy running-config scp://root@10.78.19.15/tftpboot/config/
Enter destination filename: [switch-running-config]
Enter vrf (If no input, current vrf 'default' is considered):
The authenticity of host '10.78.19.15 (10.78.19.15)' can't be established.
RSA key fingerprint is 29:bc:4c:26:e3:6f:53:91:d4:b9:fe:d8:68:4a:b4:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.78.19.15' (RSA) to the list of known hosts.
root@10.78.19.15's password:
switch-running-config 100% 6090 6.0KB/s 00:00
switch#
```

VSM のリカバリ

この項では、バックアップのテンプレートを使用して VSM を配置する方法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。

- 「バックアップ VSM VM の配置」（P.14-8）
- 「古い設定の削除」（P.14-16）
- 「VSM のバックアップ コンフィギュレーションの復元」（P.14-17）

手順

ステップ 1　バックアップした VSM VM を配置するには、「バックアップ VSM VM の配置」（P.14-8）を参照してください。

ステップ 2　古い設定を削除するには、「古い設定の削除」（P.14-16）を参照してください。

ステップ 3　バックアップ設定を復元するには、「VSM のバックアップ コンフィギュレーションの復元」（P.14-17）を参照してください。

バックアップ VSM VM の配置

ここでは、プライマリおよびセカンダリ VSM が存在しない場合にバックアップ VSM VM を配置する方法について説明します。

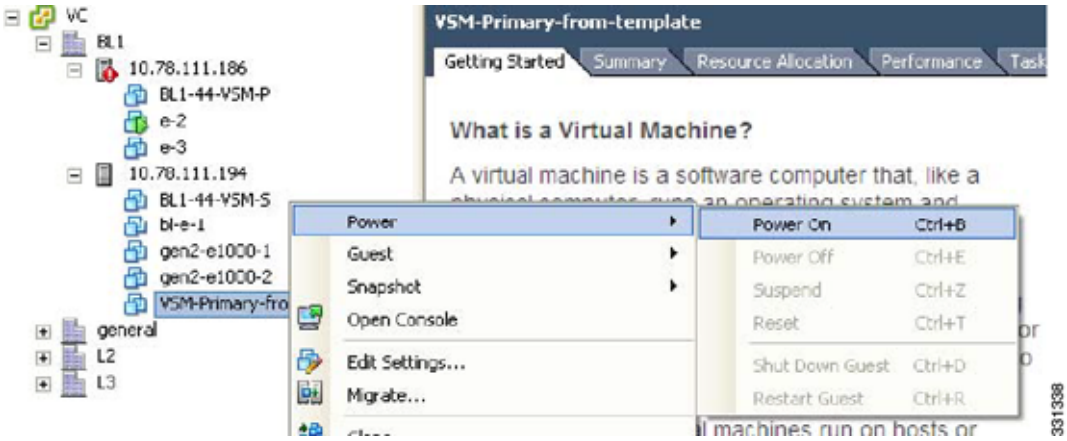
（注）　VSM VM の配置時には、その電源をオンにしないでください。

手順

ステップ 1　vSphere Client を開きます。

[vSphere Client] ウィンドウが開きます。図 14-8 を参照してください。

図 14-8　[vSphere Client] ウィンドウ



ステップ 2　左側のナビゲーション ペインで、スタンバイ VSM のホストを選択します。

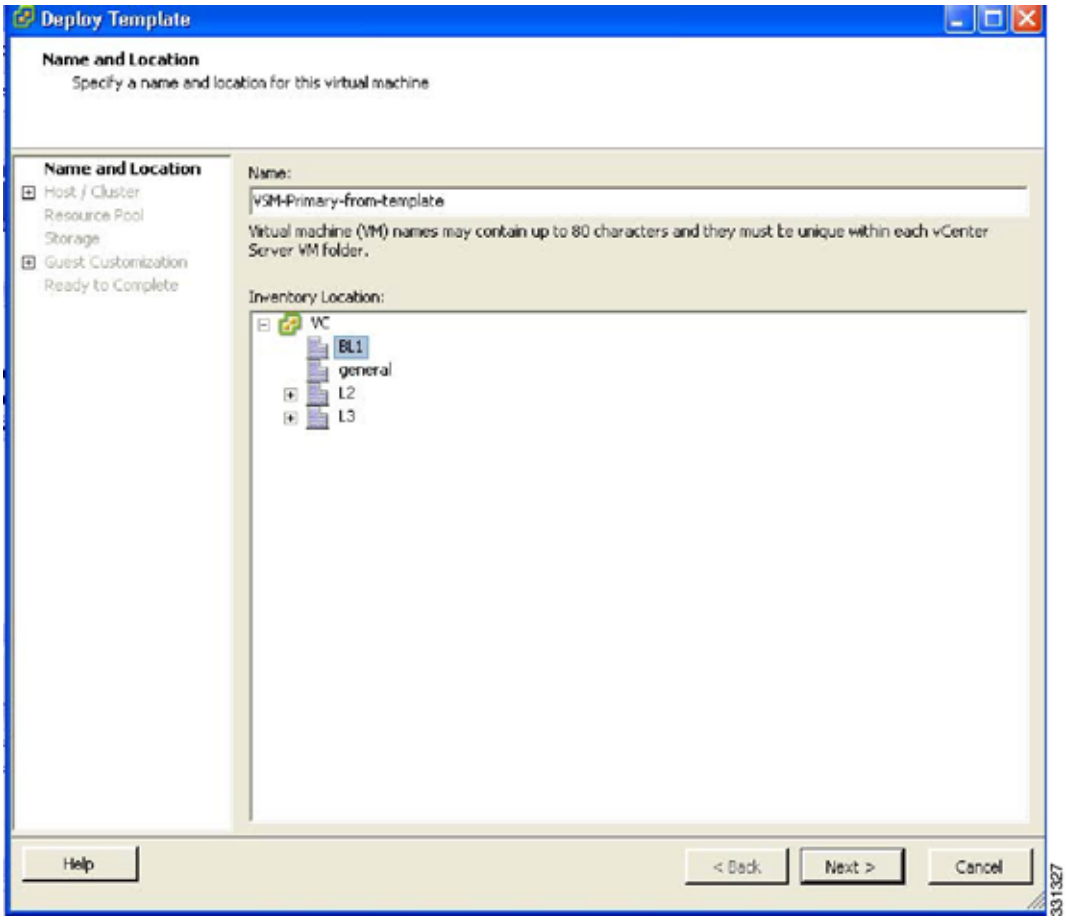
ステップ 3　[Virtual Machines] タブをクリックします。

ステップ 4　[template_VSM] を右クリックします。

ステップ 5　[Deploy Virtual Machine from this Template] を選択します。

[Deploy Template Wizard] 画面が開きます。図 14-9 を参照してください。

図 14-9　[Deploy Template Wizard] 画面



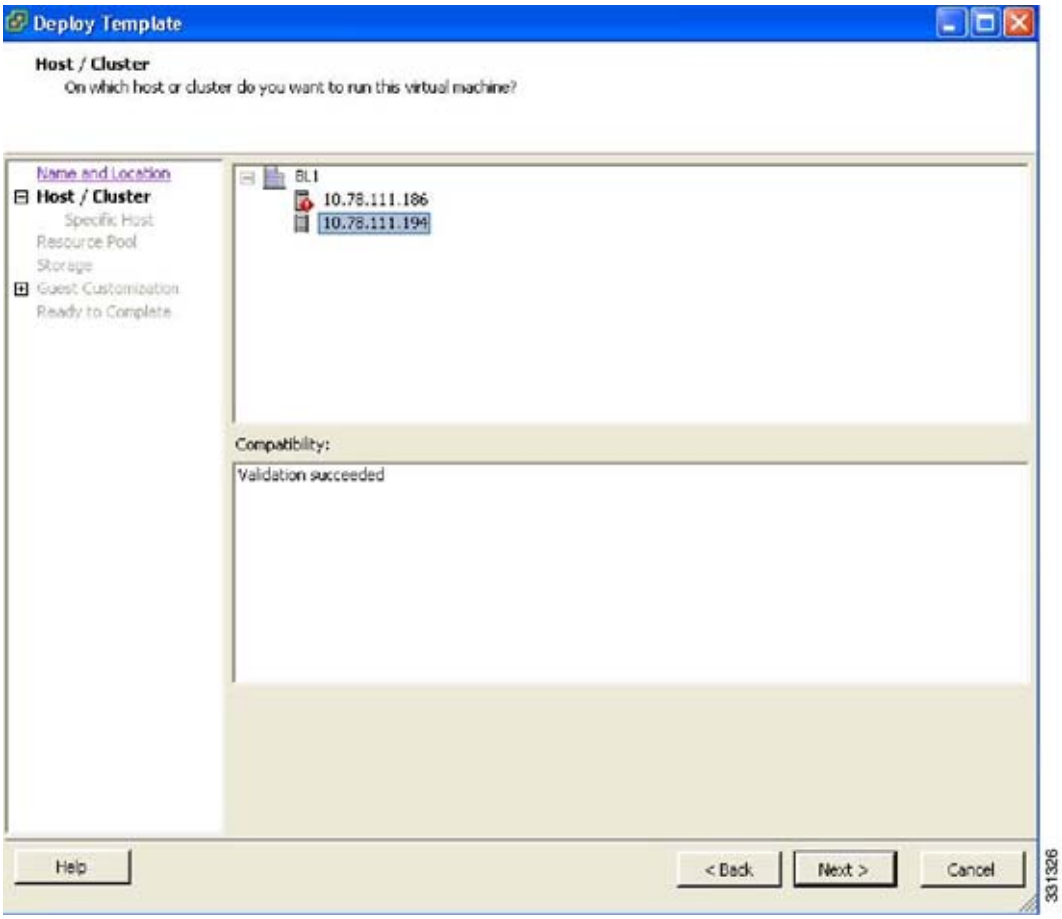
ステップ 6　[Name] フィールドに VSM の名前を入力します。

ステップ 7　[Inventory Location] ペインでクラスタを選択します。

ステップ 8　[Next] をクリックします。

[Choosing a Host] 画面が開きます。図 14-10 を参照してください。

図 14-10　[Choosing a Host] 画面

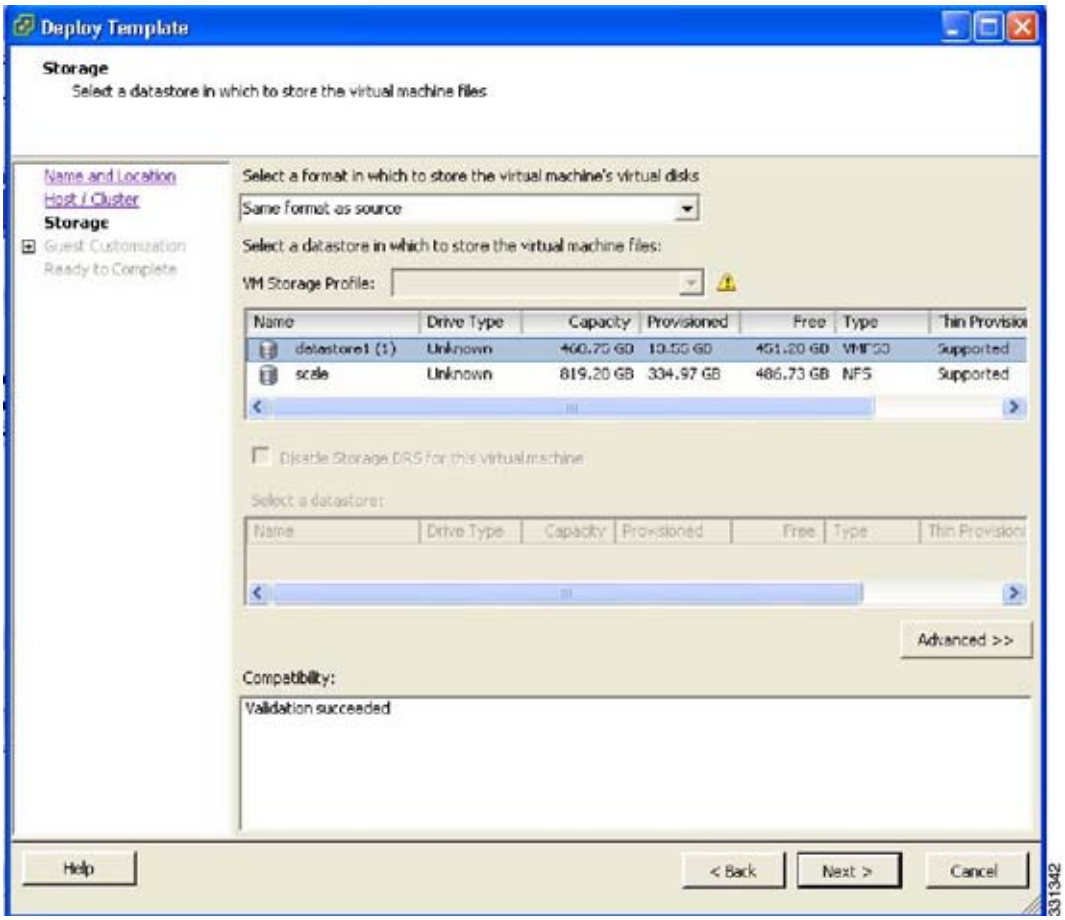


ステップ 9　ホストを選択します。

ステップ 10　[Next] をクリックします。

[Choosing a Datastore] 画面が開きます。図 14-11 を参照してください。

図 14-11　[Choosing the Datastore] 画面



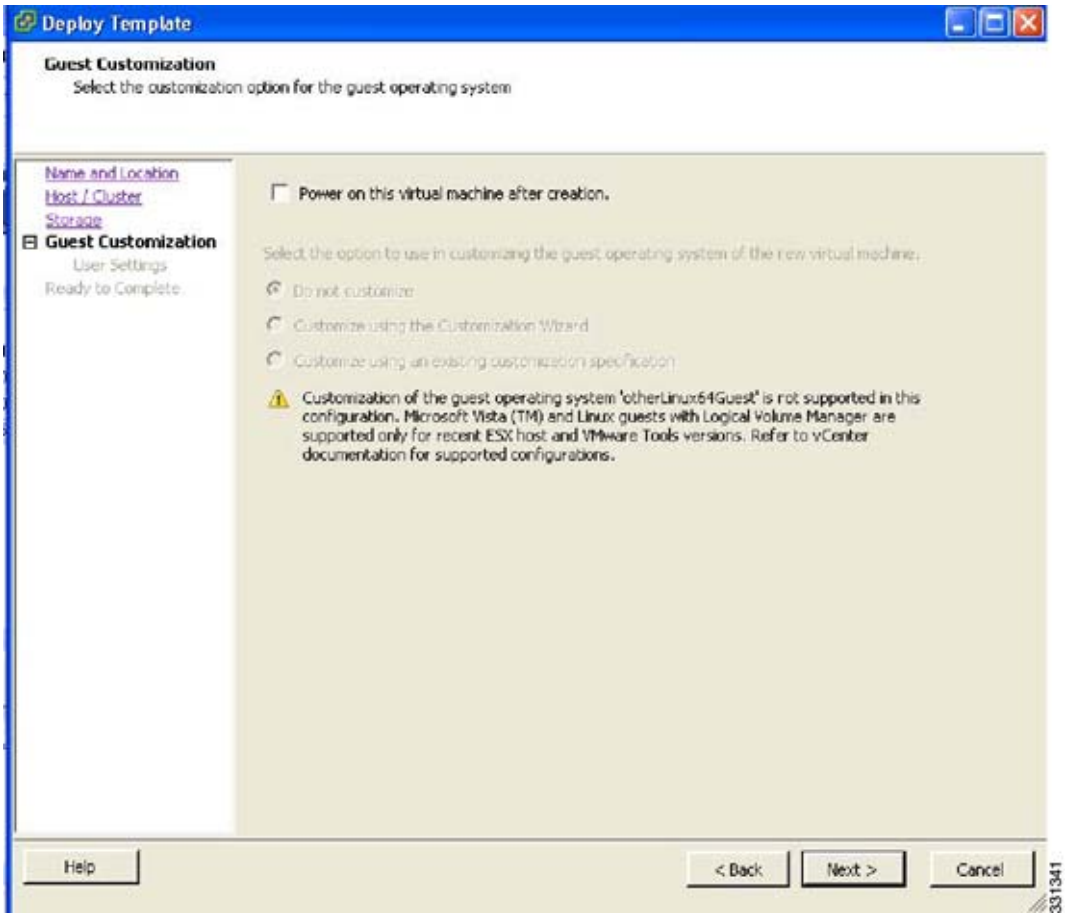
ステップ 11　[Select a format in which to store the virtual machine's virtual disks] ドロップダウン リストで、[Same format as source] を選択します。

ステップ 12　データストアを選択します。

ステップ 13　[Next] をクリックします。

[Guest Customization] 画面が開きます。図 14-12 を参照してください。

図 14-12　[Guest Customization] 画面

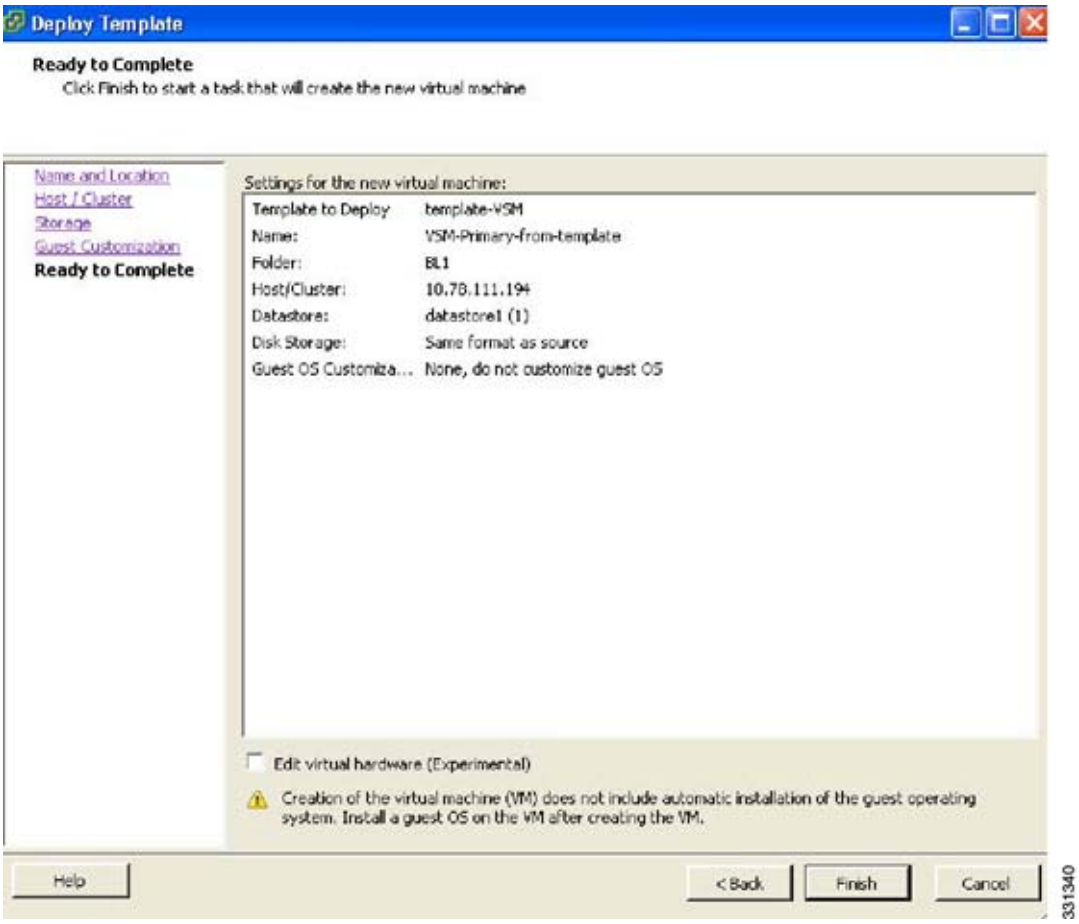


（注）　[Power on this virtual machine after creation] チェックボックスがオフになっていることを確認します。

ステップ 14　[Next] をクリックします。

[Deploy Template - Ready to Complete] 画面が開きます。図 14-13 を参照してください。

図 14-13　[Deploy Template - Ready to Complete] 画面



ステップ 15　新しい仮想マシンの設定を確認し、[Finish] をクリックします。

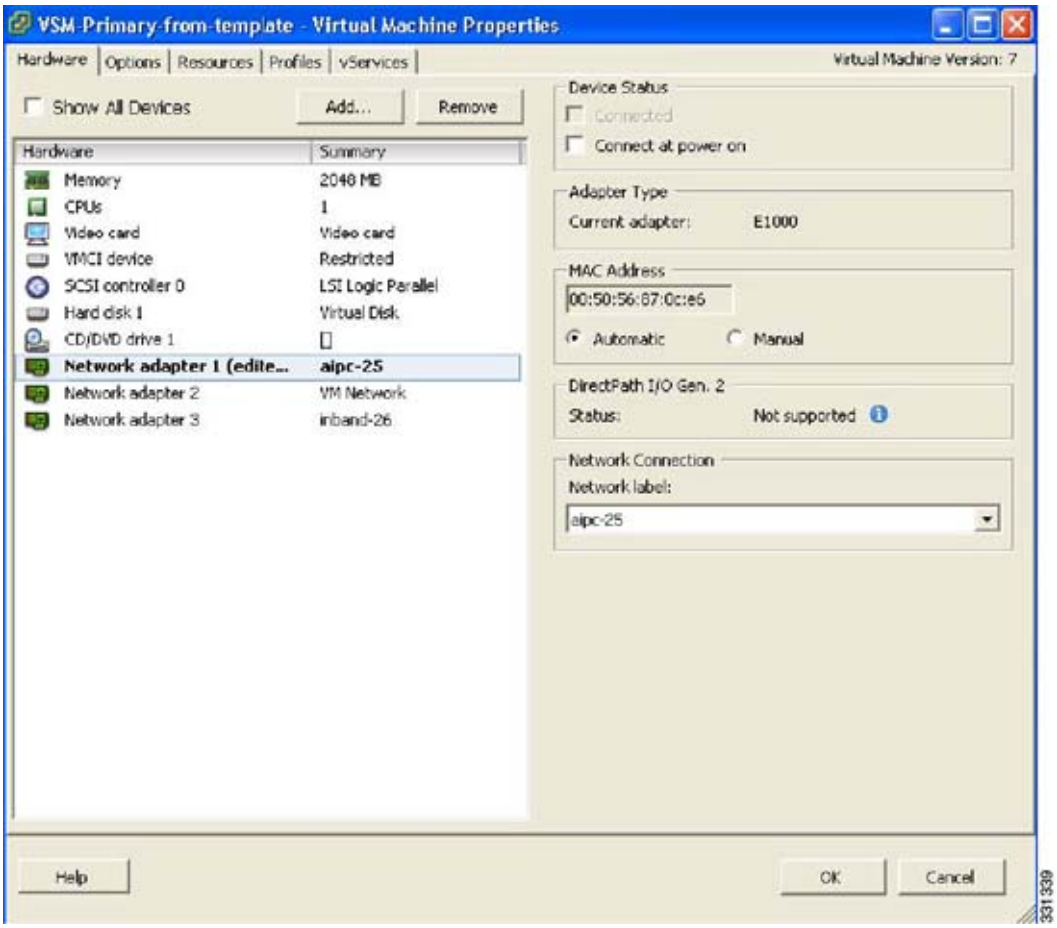
（注）　VEM で管理 VLAN を使用できない場合は、vSwitch に管理インターフェイスを追加する必要があります。

ステップ 16　新たに配置した VM を右クリックします。

ステップ 17　[Edit Settings] を選択します。

[Virtual Machine Properties] ウィンドウが開きます。図 14-14 を参照してください。

図 14-14　[Virtual Machine Properties] ウィンドウ



ステップ 18　[Hardware / Summary] ペインで、[Network adapter 1] を選択します。

ステップ 19　[Hardware / Summary] ペインで、[Connect at power on] チェックボックスをオフにします。

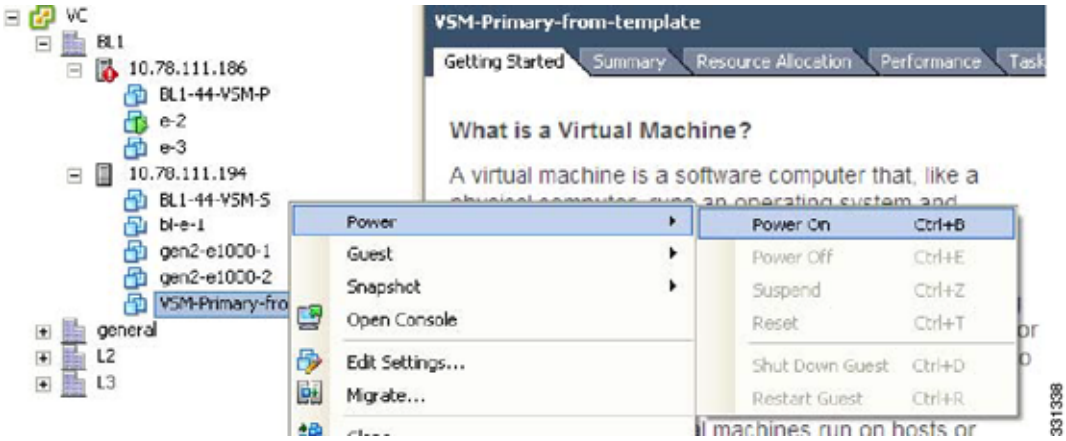
ステップ 20　[Hardware / Summary] ペインで、[Network adapter 2] を選択します。

ステップ 21　[Device Status] 領域で、[Connect at power on] チェックボックスをオフにします。

ステップ 22　[OK] をクリックします。

[Power On] ウィンドウが開きます。図 14-15 を参照してください。

図 14-15　[Power On] ウィンドウ



ステップ 23　新たに配置した VSM を右クリックします。

ドロップダウン リストが表示されます。

ステップ 24　[Power] > [Power On] を選択します。

これで、バックアップ VSM VM の配置が完了しました。

古い設定の削除

ここでは、新たに配置した VSM のスタートアップ コンフィギュレーションを削除する方法について説明します。

手順

ステップ 1　新たに配置した VSM の仮想マシンのコンソールを起動します。

ステップ 2　次のコマンドを入力して、プライマリに冗長ロールを設定します。

```
switch# system redundancy role primary
Setting will be activated on next reload
switch#
```

ステップ 3　次のコマンドを入力して、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。

```
switch# copy running-config startup-config
scp:        sftp:           startup-config
[####################################] 100%
switch#
```

ステップ 4　次のコマンドを入力して、スタートアップ コンフィギュレーションを削除します。

```
switch# write erase
Warning: The command will erase the startup-configurations.
Do you wish to proceed anyway? (y/n) [n] y
```

ステップ 5　次のコマンドを入力して、プライマリ VSM とセカンダリ VSM をリブートします。

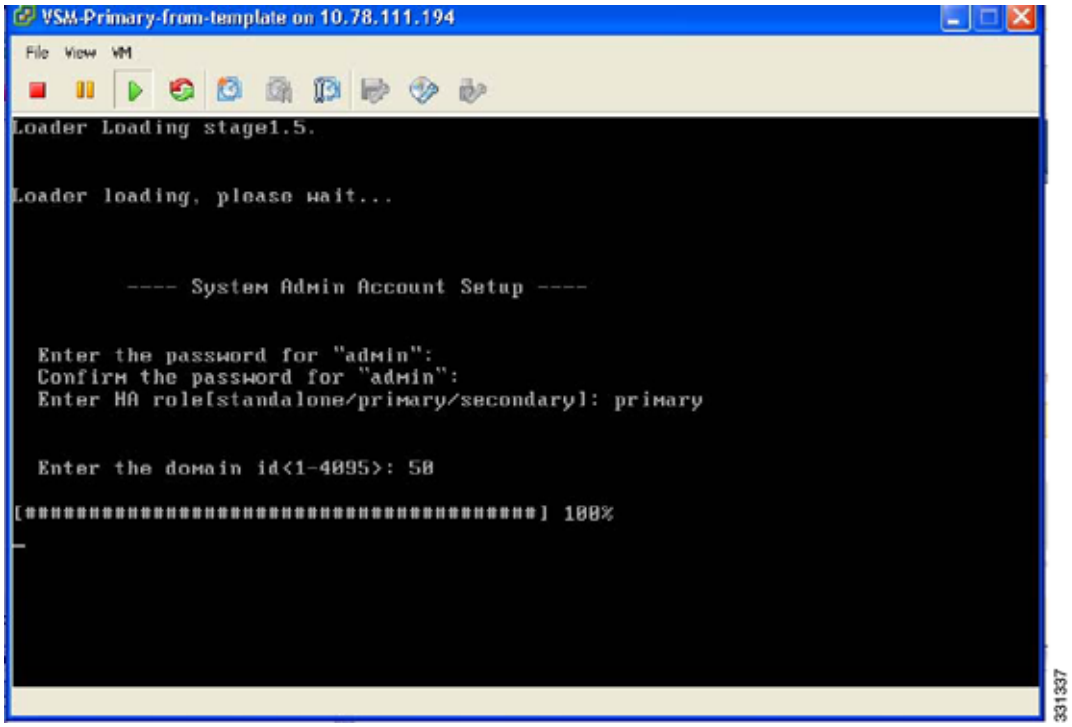
```
switch# reload
This command will reboot the system. (y/n)? [n] y
```

VSM のバックアップ コンフィギュレーションの復元

ここでは、VSM のバックアップ コンフィギュレーションを復元する方法について説明します。

ステップ 1　VSM をリブートすると、[System Admin Account Setup] ウィンドウが開きます。図 14-16 を参照してください。

図 14-16　[System Admin Account Setup] ウィンドウ



ステップ 2　管理者パスワードを入力し、確認します。

```
---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":
```

ステップ 3　ドメイン ID を入力します。

```
Enter the domain id<1-4095>: 50
```

ステップ 4　HA ロールを入力します。

ロールを指定しない場合は、スタンドアロン ロールがデフォルトで割り当てられます。

```
Enter HA role[standalone/primary/secondary]: primary


[##########################################] 100%

          ---- Basic System Configuration Dialog ----
```

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

ステップ 5　基本設定ダイアログボックスを開始するように求められたら、yes を入力します。

```
Would you like to enter the basic configuration dialog (yes/no): yes
```

ステップ 6　別のログイン アカウントを作成するように求められたら、no を入力します。.

```
Create another login account (yes/no) [n]: no
```

ステップ 7　読み取り専用の SNMP コミュニティ ストリングを設定するように求められたら、no を入力します。

```
Configure read-only SNMP community string (yes/no) [n]: no
```

ステップ 8　読み取り / 書き込みの SNMP コミュニティ ストリングを設定するように求められたら、no を入力します。

```
Configure read-write SNMP community string (yes/no) [n]: no
```

ステップ 9　スイッチの名前を入力します。

```
Enter the switch name:
```

ステップ 10　アウトオブバンド管理を設定するように求められたら、yes を入力し、mgmt0 IPv4 アドレスとサブネット マスクを入力します。

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: yes
Mgmt0 IPv4 address: 172.28.15.152
Mgmt0 IPv4 netmask: 255.255.255.0
```

ステップ 11　デフォルト ゲートウェイを設定するように求められたら、no を入力します。

```
Configure the default-gateway: (yes/no) [y]: no

    IPv4 address of the default gateway : 172.23.233.1
```

ステップ 12　Telnet サービスをイネーブルにするように求められたら、yes を入力します。

```
Enable the telnet service? (yes/no) [y]: yes
```

ステップ 13　SSH サービスをイネーブルにするように求められたら、yes を入力して、キー タイプとキー ビット数を入力します。
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。

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of key bits <768-2048> : 1024
```

ステップ 14　HTTP サーバをイネーブルにするように求められたら、yes を入力します。

```
Enable the http-server? (yes/no) yes
```

ステップ 15　NTP サーバを設定するように求められたら、no を入力します。

```
Configure NTP server? (yes/no) [n]: no
```

ステップ 16　VEM 機能レベルを設定するように求められたら、no を入力します。

Do you want to reconfigure?(yes/no) [n] **no**

これで、設定全体がまとめられ、編集するように求められます。

```
The following configuration will be applied:
 interface Mgmt0
ip address 172.28.15.152 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 10.78.111.11
  no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  feature http-server
  svs-domain
    svs mode L2
    control vlan 1
    packet vlan 1
    domain id 1
```

ステップ 17　設定を編集するかどうか尋ねられたら、no を入力します。

```
Would you like to edit the configuration? (yes/no) [n]: no

Enter SVS Control mode (L2 / L3) : L2
Enter control vlan <1-3967, 4048-4093> : 100
Enter packet vlan <1-3967, 4048-4093> : 101
```

ステップ 18　この設定を使用し、保存するように求められたら、yes を入力します。

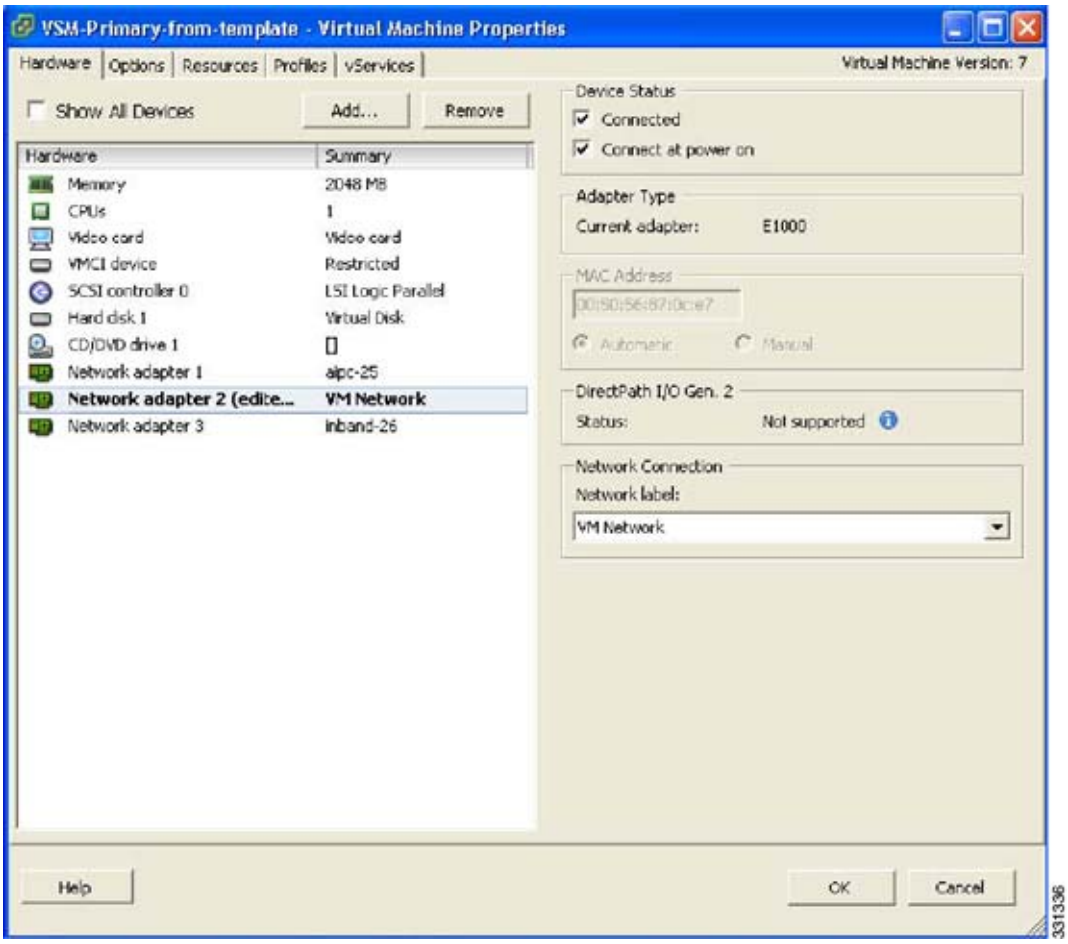
注意　ここで設定を保存しておかないと、次回のスイッチ起動時に設定が更新されません。新しい設定を保存するには、**yes** と入力します。これによって、キックスタート イメージとシステム イメージも自動的に設定されます。

```
Use this configuration and save it? (yes/no) [y]: yes
[########################################] 100%
```

ステップ 19　vSphere Client で、VSM を右クリックし、[Edit Settings] を選択します。

[VSM Virtual Machine Properties] ウィンドウが開きます。図 14-17 を参照してください。

図 14-17　[VSM Virtual Machine Properties] ウィンドウ



ステップ 20　[Hardware / Summary] ペインで、[Network adapter 2] を選択します。

ステップ 21　[Connect at power on] チェックボックスをオンにします。

ステップ 22　VSM にログインします。

ステップ 23　次のコマンドを入力して、VSM のブートフラッシュにバックアップ コンフィギュレーションをコピーします。

```
switch# copy scp://root@10.78.19.15/tftpboot/backup/VSM-Backup-running-config
bootflash:
Enter vrf (If no input, current vrf 'default' is considered):
The authenticity of host '10.78.19.15 (10.78.19.15)' can't be established.
RSA key fingerprint is 29:bc:4c:26:e3:6f:53:91:d4:b9:fe:d8:68:4a:b4:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.78.19.15' (RSA) to the list of known hosts.
root@10.78.19.15's password:
switch-running-config 100%
6090 6.0KB/s 00:00
switch#
```

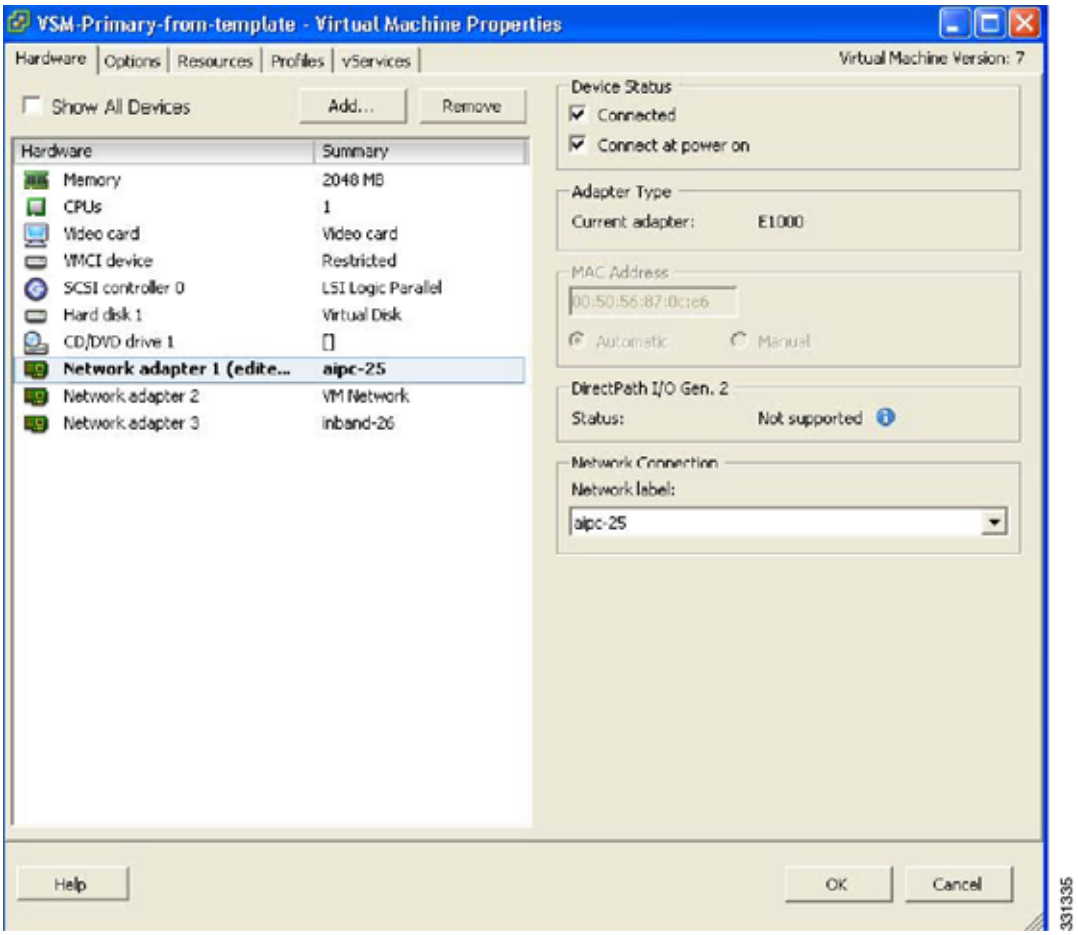
ステップ 24　次のコマンドを入力して、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

```
switch# copy bootflash:VSM-Backup-running-config running-config
Disabling ssh: as its enabled right now:
Can't disable ssh for key generation:Current user is logged in through ssh
```

```
Please do a "copy running startup" to ensure the new setting takes effect
on next reboot
LACP Offload Status can be verified using "show lacp offload status"
Change in LACP Offload Status takes effect only on the next VSM Reboot
This can potentially cause modules with LACP uplinks to flap
Syntax error while parsing 'limit-resource m4route-mem minimum 58 maximum 58'
Syntax error while parsing 'limit-resource m6route-mem minimum 8 maximum 8'
Syntax error while parsing 'interface Ethernet3/2'
Syntax error while parsing 'inherit port-profile uplink-cdp'
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
command failed. Invalid ip address.
Syntax error while parsing 'log-level '
Syntax error while parsing 'no ip dhcp relay'
switch#
```

（注）　構文エラーが表示されることがあります。構文エラーは無視できます。

図 14-18　[Virtual Machine Properties] ウィンドウ



ステップ 25　[Hardware / Summary] ペインで、[Network adapter 1] を選択します。

ステップ 26　[Device Status] 領域で、[Connect at power on] チェックボックスをオンにします。

ステップ 27 次のコマンドを入力して、VEM が VSM に接続されていることを確認します。

```
switch# show module
Mod Ports Module-Type Model Status
--- ----- ------------------------------- ------------------ ------------
1 0 Virtual Supervisor Module Nexus1000V active *
3 248 Virtual Ethernet Module NA ok
Mod Sw Hw
--- ---------------- ------------------------------------------------
1 4.2(1)SV1(4a) 0.0
3 4.2(1)SV1(4a) VMware ESXi 4.0.0 Releasebuild-261974 (1.20)
Mod MAC-Address(es) Serial-Num
--- -------------------------------------- ----------
1 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 10.78.111.20 NA NA
3 10.78.111.186 0e973f80-e804-11de-956e-4bc311a28ede VEM-186-KLU2
* this terminal session
switch#
```

ステップ 28 すべての VEM を接続した後で、次のコマンドを入力して、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

```
switch# copy bootflash:VSM-Backup-running-config running-config
Disabling ssh: as its enabled right now:
Can't disable ssh for key generation:Current user is logged in through ssh
2011 Apr 26 12:21:22 switch %KERN-3-SYSTEM_MSG: redun_platform_ioctl :
Entered - kernel
2011 Apr 26 12:21:22 switch %KERN-3-SYSTEM_MSG: redun_platform_ioctl : Host
name is set switch - kernel
2011 Apr 26 12:21:22 switch %KERN-3-SYSTEM_MSG: redun_platform_ioctl :
Entered - kernel
2011 Apr 26 12:21:22 switch %KERN-3-SYSTEM_MSG: redun_platform_ioctl : Host
name is set switch - kernel
ERROR: Flow Record: Record is in use. Remove from all clients before modifying.
ERROR: Flow Record: Record is in use. Remove from all clients before modifying.
ERROR: Flow Record: Record is in use. Remove from all clients before modifying.
Please do a "copy running startup" to ensure the new setting takes effect
on next reboot
LACP Offload Status can be verified using "show lacp offload status"
Change in LACP Offload Status takes effect only on the next VSM Reboot
This can potentially cause modules with LACP uplinks to flap
2011 Apr 26 12:21:23 switch %VMS-5-DVS_NAME_CHANGE: Changed dvswitch
name to 'switch' on the vCenter Server.
Syntax error while parsing 'limit-resource m4route-mem minimum 58 maximum 58'
Syntax error while parsing 'limit-resource m6route-mem minimum 8 maximum 8'
ERROR: Port-channel interface has non-zero members!
2011 Apr 26 12:21:34 switch %MSP-5-DOMAIN_CFG_SYNC_DONE: Domain config
successfully pushed to the management server.
ERROR: Cannot change connection configuration in 'Enabled' state.
ERROR: Cannot change connection configuration in 'Enabled' state.
ERROR: Cannot change the data-center name in connected state.
command failed. Invalid ip address.
Syntax error while parsing 'log-level '
Syntax error while parsing 'no ip dhcp relay'
switch# 2011 Apr 26 12:21:35 switch last message repeated 3 times
2011 Apr 26 12:21:35 switch %ETHPORT-5-SPEED: Interface port-channel1,
operational speed changed to 1 Gbps
2011 Apr 26 12:21:35 switch %ETHPORT-5-IF_DUPLEX: Interface port-channel1,
operational duplex mode changed to Full
2011 Apr 26 12:21:35 switch %ETHPORT-5-IF_RX_FLOW_CONTROL: Interface portchannel1,
operational Receive Flow Control state changed to on
```

```
2011 Apr 26 12:21:35 switch %ETHPORT-5-IF_TX_FLOW_CONTROL: Interface portchannel1,
operational Transmit Flow Control state changed to on
VSM backup and Recovery Procedure EDCS-1017832
Cisco Systems Pvt Ltd Internal Document April-27-2011
2011 Apr 26 12:21:35 switch %ETH_PORT_CHANNEL-5-PORT_UP: port-channel1:
Ethernet3/2 is up
2011 Apr 26 12:21:35 switch %ETH_PORT_CHANNEL-5-FOP_CHANGED: portchannel1:
first operational port changed from none to Ethernet3/2
2011 Apr 26 12:21:35 switch %ETHPORT-5-IF_UP: Interface Ethernet3/2 is up in
mode trunk
2011 Apr 26 12:21:35 switch %ETHPORT-5-IF_UP: Interface port-channel1 is up in
mode trunk
switch#
```

（注）　このステップは、イーサネット インターフェイスにインターフェイス コンフィギュレーション モードで直接機能が設定されている場合や、ERSPAN/NFM のような機能がある場合に、実行する必要があります。

ステップ 29　次のコマンドを入力して、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。

```
switch# copy running-config startup-config
[########################################] 100%
switch#
```

ステップ 30　OVA/OVF ファイルを使用してスタンバイ VSM を作成し、HA ペアを形成します。『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』の「Installing the Software from an OVA or OVF Image」を参照してください。

- Release 4.2(1)SV1(4) 以降のリリースでは、VMware vSphere Client から OVF テンプレートを展開し、[Configuration] ドロップダウン リストから [Nexus 1000V Secondary] を選択します。
- Release 4.0(4)SV1(2) ～ Release 4.0(4)SV1(3d) では、[Configuration] ドロップダウン リストから [Manual Install of Nexus 1000V] を選択し、VSM の [System Admin Setup] にセカンダリの HA ロールを割り当てます。

これで回復が完了しました。

その他の関連資料

システム メッセージ ロギングの実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.14-23）
- 「標準」（P.14-24）

関連資料

関連項目	参照先
システム メッセージ	『*Cisco NX-OS System Messages Reference*』
すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

VSM バックアップとリカバリの機能の履歴

ここでは、VSM バックアップとリカバリ機能のリリース履歴を示します。

機能名	リリース	機能情報
VSM バックアップとリカバリ	4.2(1)SV1(4a)	この機能が導入されました。

CHAPTER 15

仮想化ワークロード モビリティ（DC から DC vMotion へ）

この章では、Cisco Nexus 1000 の仮想化ワークロード モビリティ（DC から DC vMotion へ）機能について説明します。この機能は、2 つの物理データセンター間にある Cisco Nexus 1000 に対応します。

この章は、次の内容で構成されています。

- 「仮想化ワークロード モビリティ（DC から DC vMotion へ）の概要」（P.15-1）
- 「仮想化ワークロード モビリティ（DC から DC vMotion へ）の前提条件」（P.15-2）
- 「注意事項および制約事項」（P.15-2）
- 「仮想化ワークロード モビリティ（DC から DC vMotion へ）設定の確認」（P.15-4）
- 「仮想化ワークロード モビリティ（DC から DC vMotion へ）のモニタリング」（P.15-4）
- 「仮想化ワークロード モビリティ（DC から DC vMotion へ）の機能の履歴」（P.15-5）

仮想化ワークロード モビリティ（DC から DC vMotion へ）の概要

この項では、仮想化ワークロード モビリティ（DC から DC vMotion へ）の設定について説明します。次の項目を取り上げます。

- 「ストレッチ クラスタ」（P.15-1）
- 「スプリット クラスタ」（P.15-2）
- 「物理的なサイトの検討」（P.15-2）

ストレッチ クラスタ

（注） ストレッチ クラスタは、物理的に異なる場所に ESX/ESXi ホストがあるクラスタです。

同じ Cisco Nexus 1000 インスタンスが 2 つのデータセンターにまたがる環境では、この設定により、異なるデータセンターの仮想イーサネット モジュール（VEM）を同じ vCenter Server クラスタの一部として設定できます。

この設定を選択することで、2 つのデータセンター環境におけるいずれかのデータセンターの VEM を、同じ Dynamic Resource Scheduling（DRS）/VMware ハイ アベイラビリティ（VMW HA）/ 耐障害性（FT）ドメインの一部とすることができ、複数のパラレル仮想マシン（VM）移行イベントが可能になります。

スプリット クラスタ

スプリット クラスタ設定はストレッチ クラスタ配置の代替設定です。この設定の配置は、複数のデータセンターの VEM を含む、クラスタのないいずれかの物理サイトの 1 つ以上のクラスタで構成されます。この設定では物理データセンター間の VM 移行が可能ですが、移行イベントは、DRS によっては自動的にスケジュールされません。

仮想化ワークロード モビリティ（DC から DC vMotion へ）の前提条件

仮想化ワークロード モビリティ（DC から DC vMotion へ）には次の前提条件があります。

- VSM ペアが 1 つのサイトに限定されるように DRS アフィニティ ルールを設定する必要があります。
- DCI リンクを介した 2 つの物理データセンター間にレイヤ 2 拡張が必要です。

注意事項および制約事項

仮想化ワークロード モビリティ（DC から DC vMotion へ）には次の注意事項と制約事項があります。

- VSM HA ペアは、それぞれのストレージおよびアクティブな vCenter Server と同じサイトにある必要があります。
- レイヤ 3 コントロール モードが優先されます。
- VEM の Link Aggregation Control Protocol（LACP）を使用している場合は、LACP オフロードを使用します。
- DCI リンクを介した制御トラフィックの Quality of Service の帯域幅が保証されます。
- 物理データセンターの数は 2 つに制限されます。
- VSM-VEM 制御トラフィックに対して 5 ミリ秒の最大遅延がサポートされます。

2 つのデータセンター環境の設定の制限値については、「設定の制限値」（P.15-4）を参照してください。

物理的なサイトの検討

物理的なサイトを設計する場合は、次の注意事項に従ってください。

- 仮想スーパーバイザ モジュール（VSM）と VEM 間の平均および最大遅延を確認します。
- 手順に従い、通常の運用で行う予定のアクションを実行します。たとえば、VSM 移行を実行します。

- データセンター インターコネクト（DCI）リンク障害のために VEM がヘッドレス モードで動作する必要がある、可能性が高い VSM-VEM 通信障害を処理するようシステムを設計します。

Inter-Site リンク障害の処理

DCI リンクまたはレイヤ 2 拡張メカニズムで障害が発生すると、一連の VEM モジュールは最後の既知の設定でしばらく動作することがあります。

ヘッドレス モードの動作

VSM と VEM が通信できない間、VEM は最後の既知の設定で引き続き動作します。DCI リンク接続が復元し、VSM-VEM の通信が再確立されたら、システムは前の動作状態に戻る必要があります。

このモード タイプはデータセンターでのヘッドレス モードの動作モードと同じですが、ヘッドレス VEM には次の制約事項があります。

- 新しいポートはヘッドレス VEM では起動できません（新しい VM が起動するか、または vMotion 後に VM が起動します）。
- NetFlow データ エクスポートはありません。
- VSM が再接続するまで DHCPS/DAI のレート制限が自動的に起動しないため、ポートがシャットダウンします。
- セキュア MAC アドレスのエージングまたはラーニング、ポート セキュリティ違反からのシャットダウン/復旧などのポート セキュリティ オプションは、VSM が再接続されるまで使用できません。
- Cisco Discovery Protocol（CDP）は、切断されている VEM に対しては機能しません。
- IGMP Join/Leave は、VSM が再接続するまで処理されません。
- VSM で処理される BRIDGE および IF-MIB のクエリーは、ヘッドレス モードでのホストの最後の既知のステータスを返します。

VSM と VEM 間の追加の距離/遅延の処理

VSM と VEM 間にかなりの距離があるネットワークでは、遅延が重要な要因になります。

VSM と VEM 間の制御トラフィックはデータセンター内でサブミリ秒の遅延が生じるため、遅延は距離によっては数ミリ秒まで増えることがあります。

ラウンドトリップ時間が増えることで、VSM と VEM 間の通信時間が長くなります。VEM および vEthernet インターフェイスを追加すると、多数のタスクがシリアル化されるため、コンフィギュレーション コマンド、モジュールの挿入、ポートの起動、および **show** コマンドなどのアクションの実行にかかる時間が延びます。

VSM の移行

この項では、物理的なサイト間で VSM を移行する方法について説明します。

（注）　Cisco Nexus 1010 の VSM を移行する場合は、『*Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(3)*』を参照してください。

ESX ホストまたは ESXi ホストでホストされている VSM の移行

ESX ホストまたは ESXi ホストでホストされている VSM をローカル データセンターからリモート データセンターに移行するには、次の手順を実行します。

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。

- VSM が別のデータセンターのリモート ストレージで動作する時間を短縮する。
- 移行されている VSM に対応する VEM でホストされている新しい VM または vMotion VM を起動しない。

（注）vMotion またはストレージ vMotion の詳細については、VMware のマニュアルを参照してください。

手順

ステップ 1　バックアップ サイトにスタンバイ VSM を移行します。

ステップ 2　スタンバイ VSM ストレージのストレージ vMotion を実行します。

ステップ 3　**system switchover** コマンドを入力します。

```
switch # system switchover
```

ステップ 4　バックアップ サイトに元のアクティブな VSM を移行します。

ステップ 5　元のアクティブな VSM ストレージのストレージ vMotion を実行します。

仮想化ワークロード モビリティ（DC から DC vMotion へ）設定の確認

```
switch# show module
```

```
switch# show interface
```

仮想化ワークロード モビリティ（DC から DC vMotion へ）のモニタリング

```
switch# show module
```

```
switch# show interface
```

設定の制限値

Cisco Nexus 1000V に関するこの情報については、第 16 章「設定の制限値」を参照してください。

仮想化ワークロード モビリティ（DC から DC vMotion へ）の機能の履歴

表 15-1 は、この機能のリリースの履歴です。

表 15-1　仮想化ワークロード モビリティ（DC から DC vMotion へ）の機能の履歴

機能名	リリース	機能情報
仮想化ワークフロー モビリティ（DC から DC vMotion へ）	4.2(1)SV1(4a)	この機能が導入されました。

CHAPTER 16

設定の制限値

表 16-1　Cisco Nexus 1000V の設定の制限値

コンポーネント	同じデータセンターにある Cisco Nexus 1000V のサポート制限値		2 つのデータセンター間にある Cisco Nexus 1000V のサポート制限値	
最大モジュール数	66		34	
仮想イーサネット モジュール（VEM）	64		32	
仮想スーパーバイザ モジュール（VSM）	HA ペアに 2 つ（同じデータセンターでホストされているアクティブ / スタンバイ）		HA ペアに 2 つ（同じデータセンターでホストされているアクティブ / スタンバイ）	
VSM あたりの vCenter Server データセンター	1		1	
ホスト	64		32	
アクティブな VLAN の数（すべての VEM の合計）	2048		1024	
VEM あたりの MAC	32000		32000	
VEM あたりの VLAN ごとの MAC	4000		4000	
ポート プロファイルあたりの vEthernet インターフェイス	1024		1024	
PVLAN	512		128	
VMware vCloud Director（VCD）がある vCenter ごとの分散仮想スイッチ（DVS）	12		12	
VMware vCloud Director（VCD）がない vCenter ごとの分散仮想スイッチ（DVS）	32		32	
vCenter Server 接続	VSM HA ペアあたり 1[1]		VSM HA ペア[1] あたり 1	
VSM と VEM 間の最大遅延	—		5 ミリ秒	
	DVS あたり	**ホストあたり**	**DVS あたり**	**ホストあたり**
Virtual Service Domain（VSD）	64	6	32	3

表 16-1　Cisco Nexus 1000V の設定の制限値 （続き）

コンポーネント	同じデータセンターにある Cisco Nexus 1000V のサポート制限値		2 つのデータセンター間にある Cisco Nexus 1000V のサポート制限値	
VSD インターフェイス	2048	216	1024	108
vEthernet インターフェイス	2048	216	1024	108
ポート プロファイル	2048	—	1024	—
システム ポート プロファイル	32	32	16	16
ポート チャネル	256	8	128	4
物理トランク	512	—	256	—
物理 NIC	—	32	—	16
vEthernet トランク	256	8	128	4
ACL	128	16[2]	64	8[2]
ACL あたりの ACE	128	128[2]	64	64[2]
ACL インターフェイス	2048	256	1024	128
NetFlow ポリシー	32	8	16	4
NetFlow インターフェイス	256	32	128	16
SPAN/ERSPAN セッション	64	64	32	32
QoS ポリシー マップ	128	128	64	64
QoS クラス マップ	1024	1024	512	512
QoS インターフェイス	2048	256	1024	128
ポート セキュリティ	2048	216	1024	108
MultiCast グループ	512	512	256	256

1. vCenter Server に同時に許可される接続は 1 つだけです。
2. VEM の空きメモリの大きさが十分ならば、この数を超えてもかまいません。

INDEX

C

capability コマンド　3-11, 13-8

D

description コマンド　13-7

E

ERSPAN
- NAM のモニタリング　9-4
- 概要　9-4
- 実装　9-4
- セッションの設定　9-13

H

HA ロール
- CLI セットアップ　14-17

HTTP
- CLI セットアップ　14-18

I

ip flow monitor コマンド　11-21

IP 接続　3-10

M

mgmt0
- CLI セットアップ　14-18

mgmt0 インターフェイス
- デフォルト設定　2-2, 8-3, 9-6, 11-10, 12-5

MIB
- SNMP　10-15
- 説明　10-2
- ダウンロード元　10-15

N

NAM
- ERSPAN データソース　9-4
- NetFlow データソース　11-9

NetFlow　11-20
- NAM のモニタリング　11-9
- エクスポータ　11-6
- モニタ　11-6

no shutdown コマンド　3-12, 13-8

NTP
- CLI セットアップ　14-18
- 設定　2-3 ～ 2-10

P

pg-name オプション　3-11, 9-11, 13-7

port-profile コマンド　3-11

S

show コマンド
- show interface brief　4-14
- show interface virtual　4-14
- show module　4-14
- show running-config　4-11
- show server-info　4-14

show svs connections 4-10
show svs-domain 4-11
SNMP
CLI とユーザの同期 10-4
engineID の形式 10-7
MIB 10-2
RFC 10-2
暗号化の強制 10-7
エージェント 10-2
グループベースのアクセス 10-5
コミュニティの作成 10-8
コンタクトの指定 10-11
コンフィギュレーション例 10-13
サポート対象の MIB 10-15
制限事項 10-5
設定の確認 10-13
説明 10-1 ～ ??
注意事項 10-5
通知
LinkUp/LinkDown 通知の設定 10-11
応答要求 10-2
個々の通知のイネーブル化 10-9
説明 10-2
通知ターゲット ユーザの設定 10-9
通知レシーバの設定 10-8
トラップ 10-2
デフォルト設定 3-3, 10-5, 13-5
認証 10-4
バージョン
SNMPv3 10-2
USM 10-4
セキュリティのモデルおよびレベル 10-3
ハイ アベイラビリティ 10-5
プロトコルのディセーブル化 10-12
マネージャ 10-1
ユーザの設定 10-6
ロケーションの指定 10-11
ワンタイム認証のイネーブル化 10-11
SPAN
出力送信元 9-2
SPAN セッション
再開 9-17, 9-19
シャットダウン 9-16
説明 9-5
SPAN 送信元
出力 9-2
SSH
CLI セットアップ 14-18
state enabled コマンド 3-12, 13-8
SVI
VLAN インターフェイス 3-13, 3-14
switchport access vlan コマンド 3-11, 13-8
switchport mode コマンド 3-11, 13-8
system vlan コマンド 3-12, 13-8

T

Telnet
CLI セットアップ 14-18

V

vCenter Server
Nexus 1000V を削除 4-5
接続 4-2
接続の切断 4-4
VEM
機能レベル
CLI セットアップ 14-18
VLAN
SVI 3-13, 3-14
VLAN インターフェイス
VLAN 間の通信 3-13, 3-14
vmware port-group コマンド 3-11
volatile:
スイッチのリブート 6-3
VSM
クレデンシャル

CLI セットアップ 14-17

い

一致基準の制限 16-1
イネーブル
プロファイル内のポート 3-12, 13-8
ポート プロファイル 3-12, 13-8
インターフェイス
デフォルト設定 2-2, 8-3, 9-6, 11-10, 12-5

か

簡易ネットワーク管理プロトコル。「SNMP」を参照
管理インターフェイス
デフォルト設定 2-2, 8-3, 9-6, 11-10, 12-5
関連資料 xvii, xix

き

機能、レイヤ 3 コントロール 3-11, 13-8

く

クラスマップの制限値 16-1

け

現在のディレクトリ
表示 6-2
変更 6-3

こ

コピー、ファイル 6-5
コマンド
出力をファイルに保存 6-12
コンフィギュレーション
以前へのロールバック 6-13
表示 5-3
コンフィギュレーション ファイル
コピー 6-5
削除 6-9
ダウンロード 6-5
バックアップ 6-5

さ

サービス ポリシーの制限値 16-1
削除、Nexus1000V を vCenter Server から 4-5
作成、VLAN
デフォルト ステート 3-13, 3-15

す

スイッチ名
CLI セットアップ 14-18
ストレージ切断の検出 13-19

せ

制御 VLAN
CLI セットアップ 14-19
制限値、設定 16-1
接続、vCenter Server へ 4-2
接続、表示 4-10
切断、vCenter Server との接続 4-4
設定
クリア 5-10
保存 5-10
設定されたドメイン
表示 4-11
設定の制限値 16-1
設定、表示 4-11

て

ディレクトリ
現在の表示 6-2
削除 6-7, 6-9
作成 6-7
ファイルの一覧表示 6-3
ファイルの移動 6-8
デフォルト ゲートウェイ
CLI セットアップ 14-18
デフォルト設定
SNMP 3-3, 10-5, 13-5

と

ドメイン
CLI セットアップ 14-19
ドメイン ID、VSM
CLI セットアップ 14-17
トラップ。「SNMP」を参照

ね

ネットワーク解析モジュール
ERSPAN データソース 9-4
NetFlow データソース 11-9

は

ハイ アベイラビリティ
SNMP 10-5
パケット VLAN
CLI セットアップ 14-19
バックアップ、ファイル 6-5
バナー メッセージ
設定 5-2

ひ

表示、スイッチ設定 4-11

ふ

ファイバ チャネル インターフェイス
デフォルト設定 2-2, 8-3, 9-6, 11-10, 12-5
ファイル
圧縮 6-9
圧縮解除 6-9
移動 6-8
コピーまたはバックアップ 6-5
削除 6-9
チェックサムの表示 6-15
内容の表示 6-13
末尾の表示 6-15
ファイル システム
現在のディレクトリの表示 6-2
指定 6-2
ディレクトリの削除 6-7
ディレクトリの作成 6-7
ディレクトリの変更 6-3
ファイルの一覧表示 6-3
フロー エクスポータ 11-6
フロー モニタ 11-6

へ

変更、VLAN
許容されるパラメータ 3-13, 3-15

ほ

ポート プロファイル
IP 接続 3-10
NetFlow 11-20
レイヤ 3 コントロール 3-10
ポリシー マップの制限値 16-1

ま

マニュアル
追加資料 xvii

も

モジュール、表示 4-14

ゆ

ユーザ
表示 7-1
メッセージの送信 7-2

れ

レイヤ 3 接続 3-10

ろ

ローカル SPAN
概要 9-3
実装 9-3
セッションの設定 9-7