Cisco Nexus 1000V インタークラウドシステム管理コンフィギュレーション ガイド リリース 5.2(1)IC1(1.1)

初版：2013 年 07 月 03 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-29149-01-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。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワーク トポロジ図、およびその他の図は、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および電話番号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 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: http://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)

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

ここでは、次の項について説明します。

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

このマニュアルは、次のような経験と知識を持つネットワーク管理者とサーバ管理者を対象としています。

- 仮想化の知識
- VMM ソフトウェアを使用した仮想マシンの作成と VMware vSwitch の設定
- Amazon Web Service（AWS）などのプロバイダー クラウドのアカウントを作成できること。
- VMware vNetwork Distributed Switch の知識は必要ありません。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
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。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screenフォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

表記法	説明
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

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。

Cisco Nexus 1000V InterCloud の関連資料

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

http://www.cisco.com/en/US/partner/products/ps12904/tsd_products_support_series_home.html

一般情報

『*Cisco Nexus 1000V InterCloud Release Notes*』

インストール & アップグレード

『*Cisco Nexus 1000V InterCloud Installation Guide*』

コンフィギュレーション ガイド

『*Cisco Nexus 1000V InterCloud License Configuration Guide*』

『*Cisco Nexus 1000V InterCloud High Availability and Redundancy Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Interface Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Layer 2 Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Port Profile Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Security Configuration Guide*』

『*Cisco Nexus 1000V インタークラウド システム管理コンフィギュレーション ガイド*』

リファレンス

『*Cisco Nexus 1000V InterCloud Command Reference*』

『*Cisco Nexus 1000V InterCloud Verified Scalability Reference*』

『*Cisco Nexus 1000V MIB Quick Reference*』

トラブルシューティング & アラート

『*Cisco Nexus 1000V Password Recovery Procedure*』

Cisco Nexus 1000V のマニュアル

Cisco Nexus 1000V for VMware のマニュアル

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

Cisco Prime Network Services Controller のマニュアル

http://www.cisco.com/en/US/products/ps13213/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

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 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。

第 1 章

概要

この章の内容は、次のとおりです。

システム管理の概要

ドメイン

Cisco Nexus 1000V のドメイン ID を作成することが必要です。 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 ID を後で作成する必要がある場合は、**saves-domain** コマンドを使用して設定します。

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。

サーバ接続

または ESX サーバに接続するには、まず Cisco Nexus 1000V で接続を定義する必要があります。 サーバ接続の管理では、 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。

設定管理

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。

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）。

ユーザ管理

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。

NTP

ネットワーク タイムプロトコル（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。

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 では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

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。 端末セッション、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 Nexus 1000V Series NX-OS System Messages Reference*』を参照してください。

第 2 章

ドメインの設定

この章の内容は、次のとおりです。

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 制御

レイヤ 3 制御または IP 接続は、仮想スーパーバイザ モジュール（VSM）と制御トラフィックおよびパケット トラフィック用の仮想イーサネット モジュール（VEM）との間でサポートされます。 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。 レイヤ 3 モードでは、VSM と VSM が管理するすべての VEM（ホスト）が、異なるネットワークに存在できます。

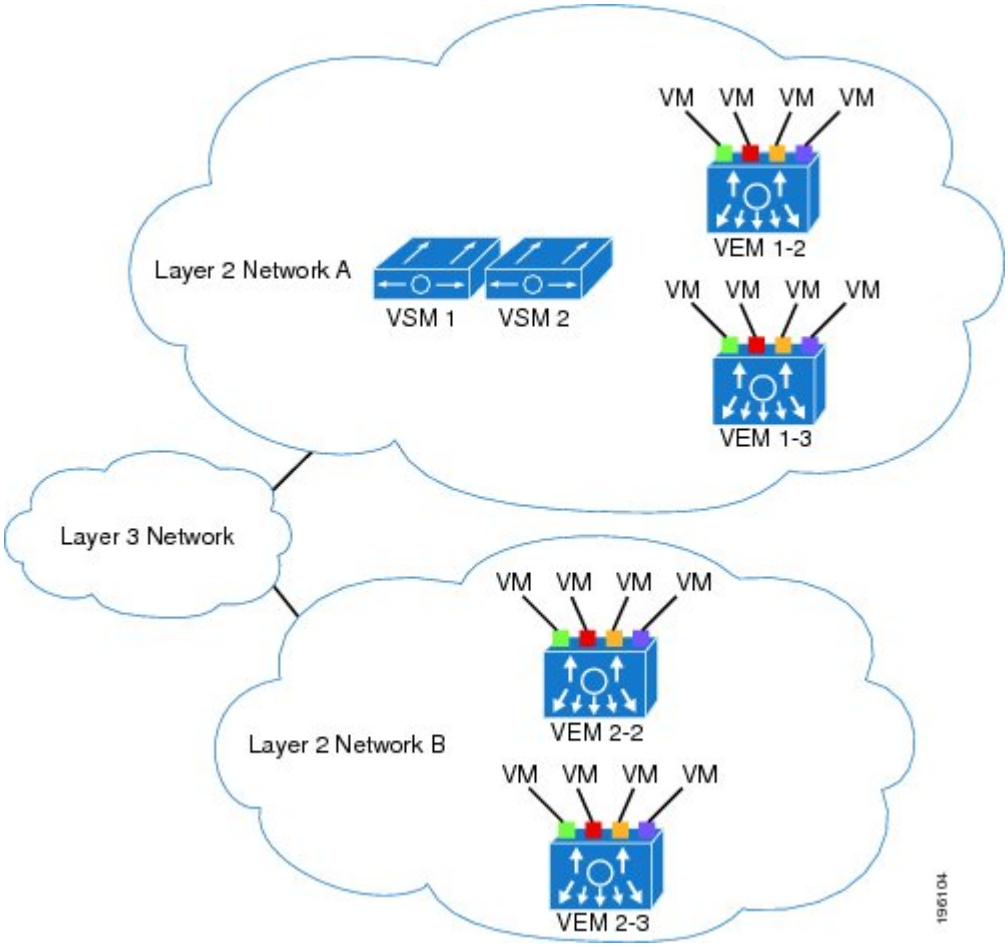
別の VSM は、自身が制御するレイヤ 2 ネットワークの外にあるホストの制御はできないので、VSM 自身が存在するホストは別の VSM によって制御する必要があります。

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。

- L3 制御モードで VSM を設定します。

この図では、VSM 1 がレイヤ 2 ネットワーク A 内の VEM を制御し、VSM 2 がレイヤ 2 ネットワーク B 内の VEM を制御します。

図 *1*：レイヤ *3* 制御 *IP* 接続の例



注意事項と制約事項

- VSM と VEM の間のレイヤ 3 通信には、UDP ポート 4785 が必要です。 ファイアウォールがあるネットワークでレイヤ 3 制御を設定する場合は、アップストリーム スイッチやファイアウォール デバイスで UDP ポート 4785 が開いていることを確認します。 詳細については、お使いのアップストリーム スイッチやファイアウォール デバイスのマニュアルを参照してください。
- 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 やネットワーク ファイル システム（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 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

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 3
スイッチポート モード（port-profile）	アクセス
ステート（port-profile）	無効
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

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 を追加できます。 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実行できます。

（注） 次の点を推奨します。

- 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します。
- Cisco Nexus 1000V の各インスタンスに別の VLAN（別のドメイン）を使用します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

次の情報を知っている必要があります。

- 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。
- この Cisco Nexus 1000V インスタンスに対する一意のドメイン ID。
- 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **config terminal**	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。
ステップ 2	switch(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	switch(config-svs-domain)# **domain id** *number*	この Cisco Nexus 1000V インスタンスに対する一意のドメイン ID を作成します。
ステップ 4	switch(config-vlan)# **show svs domain**	（任意） 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 5	switch(config-vlan)# **exit**	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 6	switch(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。

```
switch# config terminal
switch(config)# svs-domain
```

```
switch(config-svs-domain)# domain id 100

switch(config-vlan)# exit

switch(config)# show svs domain
SVS domain config:
Domain id: 211
Control vlan: NA
Packet vlan: NA
Control mode: L3
Switch guid: 20ccba13-3738-60db-b077-91a774b41eda
L3 control interface: mgmt0
Status: Config push to VC successful.
Control type multicast: No

Note: Control VLAN and Packet VLAN are not used in L3 mode
switch(config)#
switch(config)# copy run start
[########################################] 100%
switch(config)#
```

レイヤ 3 トランスポートへの変更

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。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログイン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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **show 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 が表示されます。
ステップ 2	switch# **config t**	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。
ステップ 3	switch(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 4	switch(config-svs-domain)# **no packet vlan**	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	switch(config-svs-domain)# **no control vlan**	制御 VLAN コンフィギュレーションを削除します。

	コマンドまたはアクション	目的
ステップ 6	switch(config-svs-domain)# **show svs domain**	（任意） 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	switch(config-svs-domain)# **svs mode L3 interface** { **mgmt0** | **control0** }	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。
ステップ 8	switch(config-vlan)# **show 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	switch(config-svs-domain)# **[no] control type multicast**	VSM のレイヤ 3 モードの制御タイプ マルチキャストを設定します。
ステップ 10	switch(config-vlan)# **show svs domain**	（任意） VSM のレイヤ 3 モードの制御タイプ マルチキャストのステータスを表示します。
ステップ 11	switch(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。

```
switch(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.
switch# config t
switch(config)# svs-domain
switch(config-svs-domain)# no packet vlan
switch(config-svs-domain)# no control vlan
switch(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)# svs mode l3 interface mgmt0
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.
switch(config-svs-domain)# show svs domain

switch(config-svs-domain)# control type multicast
switch(config)# show svs domain
SVS domain config:
  Domain id:    343
  Control vlan:  NA
  Packet vlan:   NA
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC successful.
  Control type multicast: Yes

switch(config-svs-domain)# no control type multicast
switch(config)# show svs domain
SVS domain config:
  Domain id:    343
  Control vlan:  NA
  Packet vlan:   NA
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC in progress.
  Control type multicast: No
  Limitation : Control type multicast is configured. It is not applicable in svs L2 mode.

switch(config-svs-domain)# copy running-config startup-config
[########################################] 100%
switch(config-svs-domain)#
```

VSM ドメイン機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
VSM ドメイン	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 3 章

サーバ接続の管理

この章の内容は、次のとおりです。

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
- vCenter Server との通信はすべて、トランスポート層セキュリティ（TLS）プロトコルでセキュリティが維持されます。

注意事項と制約事項

インタークラウド エクステンダは、トンネル インターフェイスと VSM 管理が同じサブネット内にある場合、VSM モジュールとしての接続に失敗します。

vCenter Server への接続

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

次の情報を知っている必要があります。

- データセンター名
- vCenter サーバ IP アドレスまたはホスト名

次がセットアップされていることを確認する必要があります。

- vCenter Server 管理ステーションをインストールして実行します。
- ESX サーバをインストールして実行します。
- Cisco Nexus 1000V アプライアンスがインストールされている。
- 管理ポートを設定します。
- ホスト名を使用して接続を設定する場合、DNS がすでに設定されている。
- vCenter サーバとの拡張ファイルが登録されている。 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。 vCenter Server は、拡張ファイルを使用して VSM から受信される要求の信憑性を確認します。 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*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。
ステップ 2	switch(config)# **svs connection** *name*	Cisco Nexus 1000V と特定の ESX サーバまたは vCenter Server との間にこの接続を追加するため、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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-svs-conn)# **protocol vmware-vim** [**http**]	この接続が VIM プロトコルを使用するように指定するには、**http** キーワードを使用します。 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	次のどちらかを実行します。	• IP アドレスを設定している場合は、ステップ 5 に進みます。 • ホスト名を設定している場合は、ステップ 6 に進みます。
ステップ 5	switch(config-svs-conn)# **remote ip address** *ipaddress*	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。 データセンター名を設定するには、ステップ 7 に進みます。
ステップ 6	switch(config-svs-conn)# **remote hostname** *hostname*	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	switch(config-svs-conn)# **vmware dvs datacenter-name** *name*	Cisco Nexus 1000V が分散仮想スイッチ（DVS）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	switch(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。 定義済みの接続が有効な場合は、no connect コマンドを使用して定義済みの接続を閉じるまでエラーメッセージが表示され、コマンドが拒否されます。

```
switch# config t
switch(config)# svs connection VC
switch(config-svs-conn)# protocol vmware-vim
```

```
switch(config-svs-conn)# remote ip address 192.168.0.1
switch(config-svs-conn)# vmware dvs datacenter-name Hamilton-DC
switch(config-svs-conn)# connect
switch# 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
switch#
```

ホスト マッピングの設定

この項では、次のトピックについて取り上げます。

- ホスト マッピングについて
- モジュールからのホスト マッピングの削除
- 新しいホストへのマッピング
- ホスト マッピングの表示

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 サーバの汎用固有識別子（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

はじめる前に

この手順を開始する前に、次のことを確認してください。

- EXEC モードで Cisco Nexus 1000V にログインしていること。
- ホストを vCenter の Cisco Nexus 1000V DVS から削除してあること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **no vem** *module-number*	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	switch(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	switch(config)# **copy running-config startup-config**	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# configure terminal
switch(config)# no vem 4
switch(config)# no vem 3
cannot modify slot 3: host module is inserted
switch(config)# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3      powered-up     93312881-309e-11db-afa1-0015170f51a8    licensed
switch(config-vem-slot)# copy running-config startup-config
```

新しいホストへのマッピング

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- ホストを vCenter の Cisco Nexus 1000V DVS から削除してあること。

（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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **vem** *module number*	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	switch(config-vem-slot)# **host vmware id** *server-bios-uuid*	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	switch(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	switch(config-vem-slot)# **copy running-config startup-config**	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# config t
switch(config)# vem 3
switch(config-vem-slot)# host vmware id 6dd6c3e3-7379-11db-abcd-000bab086eb6
switch(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

switch(config-vem-slot)# copy running-config startup-config
```

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

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。**show module vem mapping**

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

ドメインの確認

設定されたドメインを確認するには、次のコマンドを使用します。

コマンド	説明
show svs domain	Cisco Nexus 1000V で設定されたドメインを表示します。

```
n1000v# show svs domain
SVS domain config:
Domain id: 98
Control vlan: 70
Packet vlan: 71
Sync state: -
n1000v#
```

設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	説明
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。
show svs domain	Cisco Nexus 1000V で設定されたドメインを表示します。
show module	モジュール情報を表示します。
show server_info	サーバ情報を表示します。
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。
show interface virtual	仮想インターフェイス情報を表示します。
show module vem mapping	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。

モジュール情報の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	説明
show module	モジュール情報を表示します。
show server_info [*name*]	サーバ情報を表示します。
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。
show interface virtual	仮想インターフェイス情報を表示します。

サーバ接続機能の履歴

機能名	リリース	機能情報
サーバ接続	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 4 章

設定の管理

この章の内容は、次のとおりです。

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。

VSM が vCenter Server に接続されている場合、この手順では、その VSM が管理している Dynamic Vectoring and Streaming（DVS）エンジンも変更します。 DVS の名前変更時にエラーを出した場合、syslog が生成され、vCenter Server 上の DVS は古い DVS の名前を使用し続けます。

はじめる前に

この手順を開始する前に、コンフィギュレーション モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **switchname**	スイッチプロンプトを変更します。

```
switch(config)# switchname metro
metro(config)# exit
metro#
```

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。

- 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。

はじめる前に

この手順を開始する前に、コンフィギュレーション モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **banner motd** [*delimiting-character message delimiting-character*]	次の特徴を持つ Message of the Day バナーを設定します: • 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

	コマンドまたはアクション	目的
		• トークンを使用可能
ステップ 2	switch(config)# **show banner motd**	設定されているバナー メッセージを表示します。

```
switch(config)# banner motd #April 16, 2011 Welcome to the svs#
switch(config)# show banner motd
April 16, 2011 Welcome to the Switch
```

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。 この項では、次のトピックについて取り上げます。

- ソフトウェアとハードウェアのバージョンの確認
- 実行コンフィギュレーションの確認
- 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
- インターフェイス コンフィギュレーションの確認

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などに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確認するには、次のコマンドを使用します。

コマンド	説明
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。

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確認するには、次のコマンドを使用します。

コマンド	説明
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。

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

はじめる前に

この手順を開始する前に、任意のコマンド モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	swtich# **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。

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確認するには、次のコマンドを使用します。

コマンド	説明
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。

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

設定されたドメインを確認するには、次のコマンドを使用します。

コマンド	説明
show interface {*type*} {*name*}	指定したインターフェイス設定に関する詳細を表示します。

全インターフェイスの要約の確認

すべてのインターフェイスの要約を確認するには、次のコマンドを使用します。

コマンド	説明
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。

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確認するには、次のコマンドを使用します。

コマンド	説明
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。

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

この手順を開始する前に、任意のコマンド モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ **1**	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を永続的に保存します。

```
switch# copy run start
[########################################] 100%
switch#
```

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。

⚠

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

はじめる前に

この手順を開始する前に、任意のコマンド モードで CLI にログインする必要があります。

-

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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。 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。

```
switch# write erase debug
```

コンフィギュレーション管理機能の履歴

機能名	リリース	機能情報
設定管理	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 5 章

ファイルの使用

この章の内容は、次のとおりです。

ファイルについて

Cisco Nexus 1000V ファイル システムは、Cisco Nexus 1000V スイッチが使用するすべてのファイル システムに単一のインタフェースを提供します。次のシステムが含まれます。

- 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
- 作業ディレクトリの特定
- ディレクトリの変更
- ファイル システム内のファイルの一覧表示
- 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
- タブ補完の使用

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。 次の表に、ファイル システムの構文を示します。

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 1000VCLI のデフォルトでは、bootflash: ファイル システムになります
	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揮発性 RAM（VRAM）。

作業ディレクトリの特定

現在の CLI 位置のディレクトリ名を表示できます。

はじめる前に

この手順を開始する前に、任意のコマンド モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **pwd**	現在の作業ディレクトリを表示します。

```
switch# pwd
bootflash:
```

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できます。

Cisco Nexus 1000VCLI のデフォルトでは、bootflash: ファイル システムになります。

（注） 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。

はじめる前に

この手順を開始する前に、任意のコマンド モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **pwd**	CLI の現在のディレクトリ名を表示します。
ステップ 2	switch# **cd directory name** • switch# **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。	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。

	コマンドまたはアクション	目的
	• switch# **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。 • switch# **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。	

```
switch# pwd
volatile:
switch# cd bootflash:

switch# pwd
volatile:
switch# cd bootflash:mydir
switch# pwd
volatile:
switch# cd mystorage
```

ファイル システム内のファイルの一覧表示

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

```
switch# 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
switch#
```

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

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch# **copy filename ?**	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。

```
switch# 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
```

タブ補完の使用

CLI を使用してコマンド内の部分的なファイル名を補完できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show file** *filesystem name: partial filename* <Tab>	部分的なファイル名を入力したときに Tab キーを押すと、入力した文字が単一のファイルにのみ一致する場合、ファイル名を補完します。 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。

	コマンドまたはアクション	目的
ステップ 2	switch# **show file bootflash:c** <Tab>	ファイル名を補完します

```
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
n1000v# show file bootflash:c<Tab>
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j
...
...
n1000v#
```

ファイルのコピーとバックアップ

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し、保存するか、または別の場所で再利用することができます。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。

（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。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- Telnet または SSH 接続を通じて CLI にログインしていること。
- リモートの場所にコピーする場合、デバイスからコピー先へのルートがある。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。
- デバイスからコピー先への接続がある。確認には、**ping** コマンドを使用します。
- 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。
- コピー元のファイルに対するアクセス権が正しく設定されている。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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **copy** [*source filesystem:*] *filename* [*destination filesystem*:] *filename* • switch# **copy system:running-config** *system* **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。 • switch# **copy bootflash:** *system_image* **bootflash:**//*sup-standby/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。 • switch# **copy system:running-config bootflash:***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。 • switch# **copy scp:**[//[*username@*]*server*][/*path*]/*filename* セキュア シェル（SSH）をサポートし、Secure Copy Protocol（SCP）を使用してファイルのコピーを受け入れるネットワーク サーバのコピー元またはコピー先の URL をコピーします。 • switch# **copy sftp:**[//[*username@*]*server*][/*path*]/*filename*/// SSH FTP（SFTP）ネットワーク サーバのコピー元またはコピー先の URL をコピーします。 • switch# **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）。 • switch# **copy bootflash:** *filename* **bootflash:***directory*/*filename* 指定されたファイルを、bootflash: ファイル システムのルート ディレクトリから指定されたディレクトリにコピーします。 • switch# **copy** *filename directory*/*filename* 現在のファイル システム内でファイルをコピーします。 • switch# **copy tftp:**[//*server*[:*port*]][/*path*]/*filename* 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。	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。

```
switch# copy system:running-config tftp://10.10.1.1/home/configs/switch3-run.cfg
switch# copy bootflash:system_image bootflash://sup-2/system_image
switch# copy system:running-config bootflash:my-config
switch# copy scp://user@10.1.7.2/system-image bootflash:system-image
switch# copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt
switch# copy system:running-config bootflash:my-config
switch# copy bootflash:samplefile bootflash:mystorage/samplefile
```

```
switch# copy samplefile mystorage/samplefile
switch# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config
```

ディレクトリの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **mkdir** *directory name* • **mkdir** {**bootflash:** | **debug:** | **volatile:**} 選択したディレクトリ名を指定します。 ◦ bootflash: ◦ debug: ◦ volatile: • switch# **mkdir bootflash:***directory name* bootflash: ディレクトリに名前を指定してディレクトリを作成します。	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。

```
switch# mkdir test
switch# mkdir bootflash:test
```

既存のディレクトリの削除

このコマンドは、フラッシュ ファイル システムだけで有効です。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI にログインしていること。
- 削除するディレクトリが空であること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **rmdir** [**filesystem:**[//**module**/]]*directory* • switch# **rmdir** *directory* 現在のディレクトリ レベルにある、指定されたディレクトリを削除します。 • switch# **rmdir** {**bootflash:** | **debug:** | **volatile:**} *directory* ファイル システムからディレクトリを削除します。	ディレクトリを削除します。 ディレクトリ名では、大文字と小文字が区別されます。

```
switch# rmdir test
switch# rmdir bootflash:test
```

ファイルの移動

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。

移動先のディレクトリに十分なスペースがない場合、移動は完了しません。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **move** {*source path and filename*} {*destination path and filename*} • switch# **move** *filename path/filename* 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。	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。

```
switch# move bootflash:samplefile bootflash:mystorage/samplefile
switch# move samplefile mystorage/samplefile
```

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できます。

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。

はじめる前に

次のことを理解しておく必要があります。

- 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

	コマンドまたはアクション	目的
ステップ 1	switch# **delete** [**bootflash:** | **debug:** | **log:** | **volatile:**] *filename* or *directory name* • switch# **delete** *filename* 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。 • switch# **delete bootflash:***directory name* 指定したディレクトリとその内容を削除します。	指定したファイルまたはディレクトリを削除します。

```
switch# delete bootflash:dns_config.cfg
switch# delete dns_config.cfg
```

ファイルの圧縮

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show** *command* > [*path*] *filename*	**show** コマンドの出力をファイルに保存します。
ステップ 2	switch# **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	switch# **gzip** [*path*] *filename*	指定したファイルを圧縮します。
ステップ 4	switch# **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。

```
switch# show system internal l2fm event-history errors >errorsfile
switch# 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
switch# gzip bootflash:errorsfile
switch# 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
switch#
```

ファイルの圧縮解除

LZ77 コーディングを使用して、圧縮済みの指定したファイルを圧縮解除（unzip）できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **gunzip** [*path*] *filename*	指定したファイルを圧縮解除します。 ファイル名では、大文字と小文字が区別されます。
ステップ 2	switch# **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。

```
switch# gunzip bootflash:errorsfile.gz
switch# 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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show running-config >** [*path* | *filename*] • switch# **show running-config > volatile:***filename* 揮発性ファイルシステムの指定されたファイル名にコマンド **show running-config** の出力を送信します。 • switch# **show running-config > bootflash:***filename* コマンド **show running-config** の出力を、ブートフラッシュ上の指定されたファイルに送信します。 • switch# **show running-config > tftp:**// *ipaddress*/*filename* コマンド **show running-config** の出力を、TFTP サーバ上の指定されたファイルに送信します。 • switch# **show interface >** *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送信します。

	コマンドまたはアクション	目的
	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 レベルの指定されたファイルに送信します。	

```
switch# show running-config > volatile:switch1-run.cfg
switch# show running-config > bootflash:switch2-run.cfg
switch# show running-config > tftp://10.10.1.1/home/configs/switch3-run.cfg
switch# show interface > samplefile
```

ロード前のコンフィギュレーション ファイルの確認

ロード前にシステムまたはキックスタートイメージの完全性を確認するには、次のコマンドを使用します。

コマンド	説明
copy *source path* and *file* **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。
show version image [**bootflash:** | **modflash:** |**volatile:**]	指定したイメージを検証します。 bootflash: : ディレクトリ名として bootflash を指定します。 volatile: : ディレクトリ名として volatile を指定します。 modflash: : ディレクトリ名として modflash を指定します。

```
switch# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config
 switch# 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]
```

以前のコンフィギュレーションへのロールバック

以前保存したバージョンからコンフィギュレーションを復元できます。

（注） **copy running-config startup-config** コマンドを使用するたびに、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

	コマンドまたはアクション	目的
ステップ 1	switch# **copy running-config bootflash:** {*filename*}	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。
ステップ 2	switch# **copy bootflash:** {*filename*} **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。

```
switch# copy running-config bootflash:June03-Running
switch# copy bootflash:my-config startup-config
```

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。

- ファイル内容の表示
- ディレクトリの内容の表示
- ファイル チェックサムの表示
- ファイルの最終行の表示

ファイル内容の表示

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show file** [**bootflash:** | **debug**: | **volatile:**] *filename*	指定されたファイルの内容を表示します。

```
switch# show file bootflash:sample_test.txt
config t
Int veth1/1
no shut
end
show int veth1/1

switch#
```

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できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **pwd**	現在の作業ディレクトリを表示します。
ステップ 2	switch# **dir**	ディレクトリの内容を表示します。

```
switch# pwd
bootflash:
switch# dir

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

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のチェックサムを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show file** *filename* [**cksum** | **md5sum**]**show file** {**bootflash:** | **volatile:** | **debug:**} *filename* [**cksum** | **md5sum**]	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。 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。

```
switch# show file bootflash:cisco_svs_certificate.pem cksum
266988670
switch# show file bootflash:cisco_svs_certificate.pem md5sum
d3013f73aea3fda329f7ea5851ae81ff
```

ファイルの最終行の表示

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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。 行数の範囲は 0 ～ 80 です。

```
switch# 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
```

ファイル管理機能の履歴

機能名	リリース	機能情報
ファイル管理	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 6 章

ユーザの管理

この章の内容は、次のとおりです。

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 ロールの割り当てに関する詳細については、『『*Cisco Nexus 1000V InterCloud Security Configuration Guide*』.』を参照してください。

現在のユーザ アクセスの表示

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できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

```
switch# 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)*
switch#
```

ユーザへのメッセージ送信

システムを現在使用しているすべてのアクティブ CLI ユーザにメッセージを送信できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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* 引数は、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。 • *device* 引数は、デバイス タイプを指定します。 • *line* 引数は、メッセージです（最長 80 文字の英数字）。

```
switch# 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.


switch#
```

ユーザ管理機能の履歴

機能名	リリース	機能情報
ユーザ管理	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 7 章

NTP の設定

この章の内容は、次のとおりです。

NTP の概要

ネットワーク タイムプロトコル（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 通信で協定世界時（UTC）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 はこの時刻をネットワーク全体に配信します。 NTP はきわめて効率的で、毎分 1 パケット以下で 2 台のマシンを相互に 1 ミリ秒以内に同期します。

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。

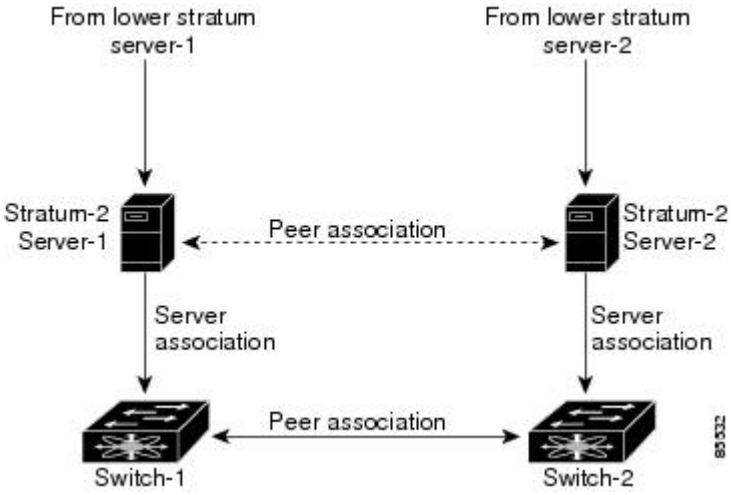
ネットワークがインターネットから切り離されている場合、Cisco NX-OS ではネットワーク デバイスが実際には他の方法で時刻を決定している場合でも、NTP によって同期しているものとして動作するように、ネットワーク デバイスを設定できます。 その後、NTPを使用して、そのネットワーク デバイスに他のネットワーク デバイスを同期させることができます。

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。

次の図に、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 *2* : *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 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。

NTP の注意事項と制限事項

- 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。
- 単独で設定したピアは、サーバの役割を担いますが、バックアップとして使用する必要があります。 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。

NTP のデフォルト設定

パラメータ	デフォルト
NTP	有効

NTP サーバおよびピアの設定

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。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。
ステップ 2	switch(config)# **ntp server** {*ip-address* | *dns-name*}	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	switch(config)# **ntp peer** {*ip-address* | *dns-name*}	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	switch(config)# **show ntp peers**	（任意） 設定された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	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。

```
switch# configure terminal
switch(config)# ntp server 192.0.2.10
switch(config# ntp peer 2001:0db8::4101
```

NTP セッションのクリア

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

NTP 統計情報のクリア

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

NTP の設定確認

次のいずれかのコマンドを使用して、設定を確認します。

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。
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 統計情報を表示します。

NTP の設定例

NTP サーバの設定例を示します。

手順

ステップ 1 switch# **configure terminal**
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 192.0.2.10**
NTP サーバを設定します。

NTP 機能の履歴

機能名	リリース	機能情報
NTP	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 8 章

SNMP の設定

この章の内容は、次のとおりです。

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。

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 デバイスのアクティビティを制御し、モニタリングするシステム。

- SNMP エージェント：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。 Cisco NX-OS はエージェントおよび 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。
- 管理情報ベース（MIB）：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。

Cisco NX-OS は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。 SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。

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、ネイバー 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。

Cisco NX-OS は、トラップまたはインフォームとして SNMP 通知を生成します。 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。 このため、トラップが受信されたかどうかを Cisco NX-OS が判断できません。 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。 Cisco NX-OS が応答を受信しない場合、インフォーム要求を再度送信できます。

複数のホスト レシーバーに通知を送信するように Cisco Nexus NX-OS を設定できます。

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：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソース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 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。 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 レベルとは、セキュリティ モデル内で許可される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。

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。

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

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（Community string）	いいえ（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（Community string）	いいえ（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（Username）	いいえ（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	いいえ（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。

モデル	レベル	認証	暗号化	結果
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。 データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）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ず、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 NX-OS は SNMPv3 に 2 種類の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 NX-OS は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして高度暗号化規格（AES）を使用し、RFC 3826 に準拠しています。

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、許可、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。

コマンドライン インターフェイス（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 NX-OS 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 NX-OS は次のようにユーザ設定を同期します。

- **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） パスフレーズまたはパスワードをローカライズしたキーおよび暗号形式で設定した場合、Cisco NX-OS はユーザ情報（パスワードやロールなど）を同期させません。

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, （61 ページ）を参照してください。

グループベースの SNMP アクセス

（注） グループは業界全体で使用されている標準的な SNMP 用語なので、SNMP に関する説明では、「ロール」ではなく「グループ」を使用します。

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。

SNMP の注意事項および制約事項

- 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 でサポートされています。
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB
- 推奨される SNMP ポーリングのインタビュー時間は 5 分です。

SNMP のデフォルト設定

パラメータ	デフォルト
ライセンス通知	enabled

SNMP の設定

この項では、次のトピックについて取り上げます。

- SNMP の設定
- SNMP メッセージ暗号化の適用ユーザ
- SNMP コミュニティの作成
- SNMP 通知レシーバーの設定
- 通知対象ユーザの設定
- SNMP 通知のイネーブル化
- インターフェイスに関する linkUp/linkDown 通知のディセーブル化

- TCP による SNMP のワンタイム認証のイネーブル化
- 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
- SNMP のディセーブル化
- AAA 同期時間の変更

SNMP ユーザの設定

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。
ステップ 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	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。 *passphrase* 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。 **localizedkey** キーワードを使用する場合は、*passphrase* 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。 *name* 引数は、SNMP エンジンにアクセスできるユーザの名前です。 **auth** キーワードは TCP セッションでの 1 回限りの SNMP 認証をイネーブルにします。 この選択は任意です。 **md5** キーワードは、認証に HMAC MD5 アルゴリズムを指定します。 この選択は任意です。 **sha** キーワードは、認証に HMAC SHA アルゴリズムを指定します。 この選択は任意です。 **priv** キーワードはユーザの暗号化パラメータを指定します。この選択は任意です。 **aes-128** キーワードは、プライバシーに 128 バイト AES アルゴリズムを指定します。 この選択は任意です。 **engineID** キーワードは、通知ターゲット ユーザを設定する engineID を指定します（V3 informs 用）。 この選択は任意です。 *id* は、12 桁のコロンで区切った 10 進数字です。

	コマンドまたはアクション	目的
ステップ 3	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	switch(config-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。

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

すべてのユーザに対する SNMP メッセージ暗号化の適用

手順

	コマンドまたはアクション	目的
ステップ 1	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。

```
switch(config)# snmp-server globalEnforcePriv
```

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。

はじめる前に

グローバル コンフィギュレーション モードである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **snmp-server community** *name* {**ro** | **rw**}	SNMP コミュニティ ストリングを作成します。

```
switch(config)# snmp-server community public ro
```

SNMP 通知レシーバーの設定

通知対象ユーザの設定

SNMPv3 インフォーム通知を通知ホスト レシーバに送信するには、デバイスに通知ターゲット 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。

はじめる前に

グローバル コンフィギュレーション モードである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*]	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。 *id* は、12 桁のコロンで区切った 10 進数字です。

```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:10:20:15:10:03
```

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 はすべての通知をイネーブルにします。

次の表に、Cisco Nexus 1000V MIB の通知をイネーブルにする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。

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。

はじめる前に

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ある必要があります

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **snmp-server enable traps**	すべての SNMP 通知をイネーブルにします。
ステップ 2	switch(config)# **snmp-server enable traps aaa** [**server-state-change**]	AAA SNMP 通知をイネーブルにします。
ステップ 3	switch(config)# **snmp-server enable traps entity** [**fru**]	ENTITY-MIB SNMP 通知をイネーブルにします。
ステップ 4	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。
ステップ 5	switch(config)# **snmp-server enable traps link**	リンク SNMP 通知をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	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
ステップ 7	switch(config)# **snmp-server enable traps snmp** [**authentication**]	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。

はじめる前に

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 モードである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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なっています。

```
switch(config-if)# no snmp trap link-status
```

TCP による SNMP のワンタイム認証のイネーブル化

はじめる前に

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 モードである必要があります

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **snmp-server tcp-session** [**auth**]	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。 デフォルトではディセーブルになっています。

```
switch(config)# snmp-server tcp-session
```

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

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **snmp-server contact** *name*	SNMP コンタクト名として sysContact を設定します。
ステップ 3	switch(config)# **snmp-server location** *name*	SNMP ロケーションとして sysLocation を設定します。
ステップ 4	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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を永続的に保存します。

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

```
switch(config)# show snmp
switch(config)# copy running-config startup-config
```

SNMPv1 トラップのホスト レシーバの設定

はじめる前に

グローバル コンフィギュレーション モードである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **snmp-server host** *ip-address* **traps version 1** *community* [**udp_port** *number*]	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。

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
```

SNMP のディセーブル化

はじめる前に

デバイスの 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 モードである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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なっています。

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

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。

はじめる前に

グローバル コンフィギュレーション モードである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **snmp-server aaa-user cache-timeout** *seconds*	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。 値の範囲は 1 ～ 86400 秒です。 デフォルト値は 3600 です。

```
switch(config)# snmp-server aaa-user cache-timeout 1200
```

SNMP の設定確認

次のいずれかのコマンドを使用して、設定を確認します。

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 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

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

```
switch# configure terminal
 switch(config)# snmp-server contact Admin@company.com
 switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
 switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
 switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
 switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
 switch(config)# snmp-server enable traps link cisco
```

SNMP の関連資料

関連項目	マニュアル タイトル
MIB	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MIB

• 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 の機能履歴

機能名	リリース	機能情報
SNMP	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 9 章

システム メッセージ ロギングの設定

この章の内容は、次のとおりです。

システム メッセージ ロギングについて

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。 端末セッション、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、端末セッションにメッセージを出力します。

次の表に、システム メッセージで使用されてい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。

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

レベル	説明
2：クリティカル	クリティカル状態
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。

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 システムで稼働します。 最大で 3 台の Syslog サーバを設定できます。

（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

次の表に、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を示します。

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

ファシリティ	説明
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
cert-enroll	証明書登録デーモン
cfs	CFS マネージャ
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
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

ファシリティ	説明
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	ローカル使用デーモン
local1	ローカル使用デーモン
local2	ローカル使用デーモン
local3	ローカル使用デーモン
local4	ローカル使用デーモン
local5	ローカル使用デーモン
local6	ローカル使用デーモン
local7	ローカル使用デーモン
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
module	モジュール マネージャ
mrib	MRIB マネージャ

ファシリティ	説明
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_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 マネージャ
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

ファシリティ	説明
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
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

システムメッセージロギングの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。

デフォルトのシステム メッセージ ロギングの設定

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

パラメータ	デフォルト
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 のメッセージ ロギングがイネーブル
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	有効
タイムスタンプ単位	Seconds
Syslog サーバ ロギング	無効
Syslog サーバ設定の配布	無効

システム メッセージ ロギングの設定

この項では、次のトピックについて取り上げます。

- 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
- 端末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
- 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 ロギングの設定
- 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
- syslog サーバの設定
- 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
- UNIX または Linux システムを使用したロギングの設定
- ログ ファイルの表示

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できます。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

	コマンドまたはアクション	目的
ステップ 1	switch# **terminal monitor**	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	switch# **configure terminal**	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	switch(config)# **logging console** [*severity-level*]	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。 デフォルトの重大度は 2 です。
ステップ 4	switch(config)# **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	switch(config)# **logging monitor** [*severity-level*]	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。 デフォルトの重大度は 2 です。
ステップ 6	switch(config)# **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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を永続的に保存します。

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging console 2
switch(config)# show logging console
Logging console:                enabled (Severity: critical)
switch(config)# logging monitor 3
switch(config)# show logging monitor
Logging monitor:                enabled (Severity: errors)
switch(config)# copy running-config startup-config
switch(config)#
```

端末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

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て、端末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できます。

コマンド	説明
no logging console [*severity-level*]	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*]	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

モジュールが記録するメッセージの重大度およびタイムスタンプの単位を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **logging module** [*severity-level*]	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	switch(config)# **show logging module**	
ステップ 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	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	switch(config)# 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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を永続的に保存します。

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。

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
Logging linecard:                enabled (Severity: errors)
switch(config)# logging timestamp microseconds
switch(config)# show logging timestamp
```

```
Logging timestamp:              Microseconds
switch(config)# copy running-config startup-config
switch(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

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て、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できます。

コマンド	説明
no logging module [*severity-level*]	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**}	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **logging module** [*severity-level*]	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	switch(config)# **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	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	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	switch(config)# **show logging timestamp**	（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。

	コマンドまたはアクション	目的
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を永続的に保存します。

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。

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
Logging linecard:                enabled (Severity: errors)
switch(config)# logging timestamp microseconds
switch(config)# show logging timestamp
Logging timestamp:               Microseconds
switch(config)# copy running-config startup-config
switch(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

次のコマンドを使用して、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できます。

コマンド	説明
no logging level [*facility severity-level*]	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**}	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]	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の範囲です。 デフォルトの発信ファシリティはlocal7です。
ステップ 3	switch(config)# **show logging server**	（任意）Syslogサーバ設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、ファシリティ local7 のすべてのメッセージを転送する例を示します。

```
switch# configure terminal
switch(config)# logging server 10.10.2.2 7
switch(config)# show logging server
Logging server:                 enabled
{10.10.2.2}
        server severity:        debugging
        server facility:        local7
switch(config)# copy running-config startup-config
switch(config)#
```

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

ここに示す手順を実行して、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できます。

コマンド	説明
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

はじめる前に

次の UNIX または Linux フィールドを syslog 用に設定する必要があります。

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

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

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

	コマンドまたはアクション	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。

```
switch# 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
switch#
```

システム メッセージ ロギングの設定確認

次のいずれかのコマンドを使用して、設定を確認します。

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。
show logging info	ロギング設定を表示します。
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。
show logging level [*facility*]	show logging level [facility]
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging server	Syslog サーバ設定を表示します。

コマンド	目的
show logging session	ロギング セッションのステータスを表示します。
show logging status	ロギング ステータスを表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。

システム メッセージ ロギングの機能履歴

機能名	リリース	機能情報
システム メッセージ ロギング	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 10 章

VSM バックアップとリカバリの設定

この章は、次の項で構成されています。

VSM のバックアップおよびリカバリに関する情報

VSM のバックアップおよびリカバリ手順を使用して、ハイ アベイラビリティ（HA）環境で両方の VSM に障害が発生した場合に VSM を再作成するための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。 詳しくは、「定期的なバックアップの実行」を参照してください。

注意事項と制約事項

VSM バックアップ/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 のバックアップには、ネットワーク管理者とサーバ管理者間の調整が必要になります。
- これらの手順は、アップグレードおよびダウングレード用ではありません。
- これらの手順では、バックアップが作成されたのと同じリリースの VSM でリストアが実行される必要があります。
- 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

この項では、次のトピックについて取り上げます。

- VSM のバックアップの実行
- 定期的なバックアップの実行
- VSM のリカバリ

（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

この項では、次のトピックについて取り上げます。

- VSM のバックアップの実行
- 定期的なバックアップの実行

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。

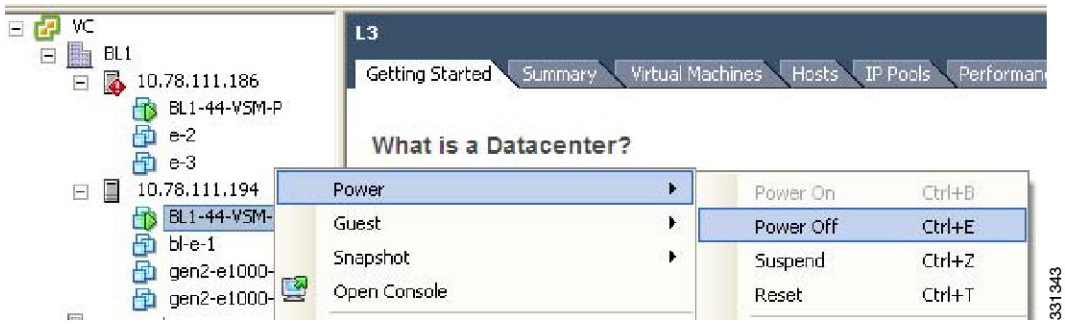
- VSM が仮想イーサネット モジュール（VEM）ホスト上にある場合、システム VLAN として管理 VLAN を設定する必要があります。
- この手順を開始する前に、VSM で、**copy running-config startup-config** コマンドを入力します。

手順

ステップ 1 [vSphere Client] を開きます。

次の図に示すように、[vSphere Client] ウィンドウが開きます。

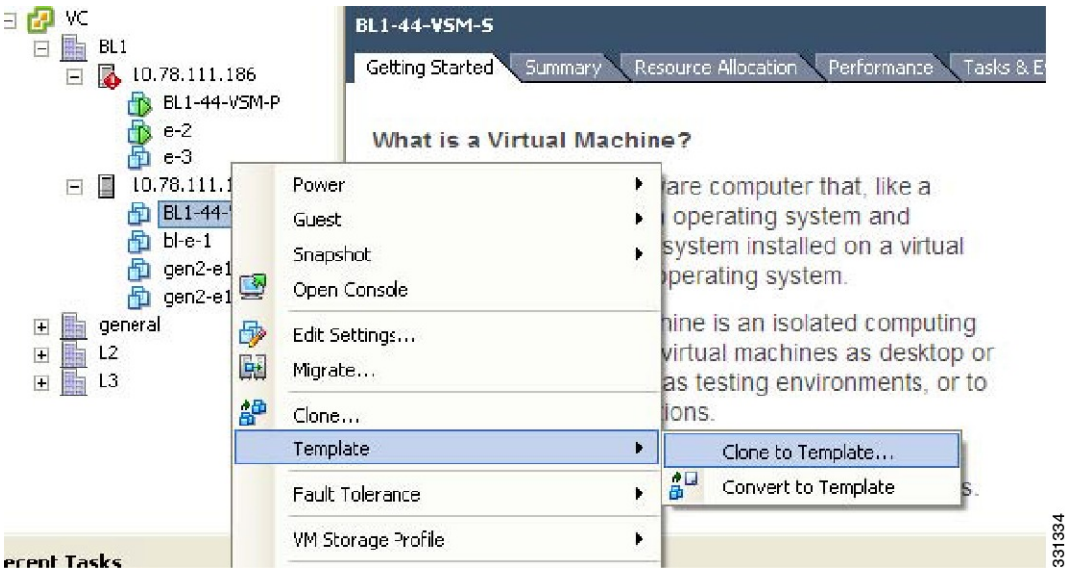
図 3：***[vSphere Client]*** ウィンドウ



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]と選択します。
操作は、[Clone to Template] ウィンドウに表示されます。

図 4：***[Clone to Template]*** ウィンドウ

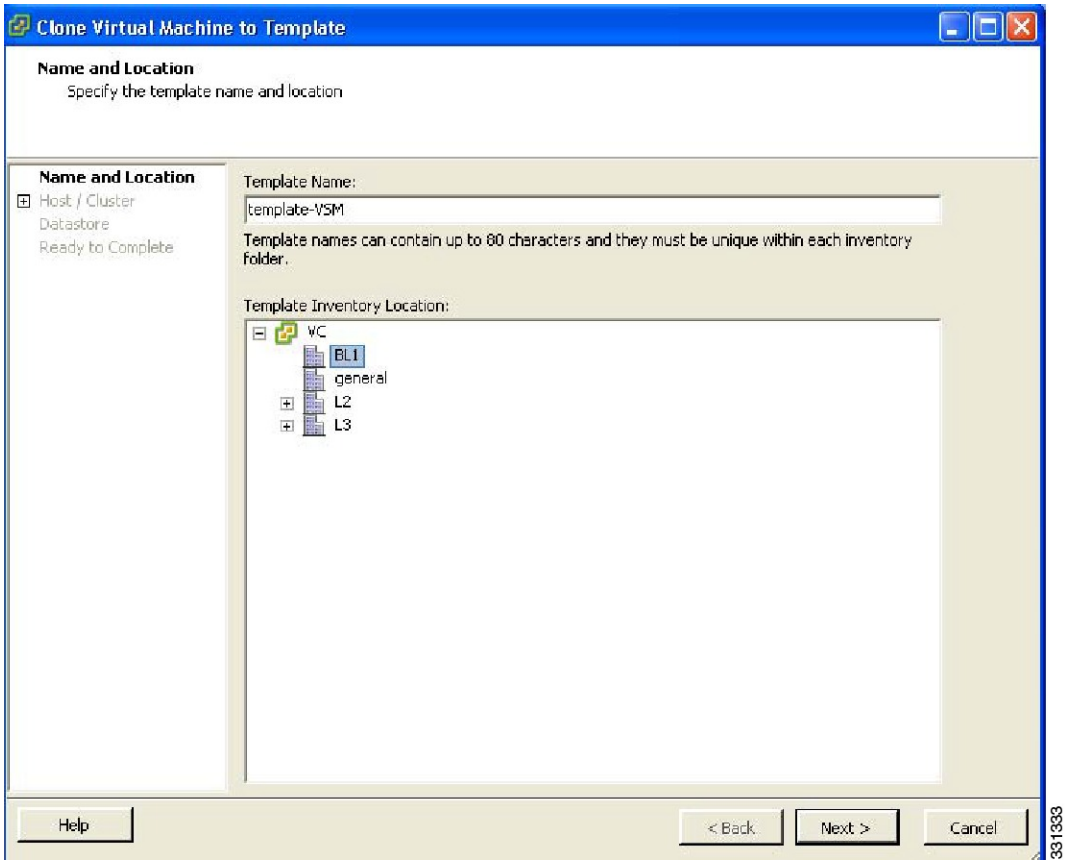


ステップ 4　左側のナビゲーション ペインで、スタンバイ VSM を右クリックします。
ドロップダウン リストが表示されます。

ステップ 5　[Template] > [Clone to Template] と選択します。

[Clone Virtual Machine to Template] ウィンドウが開きます。

図 5：*[Clone Virtual Machine to Template]* ウィンドウ



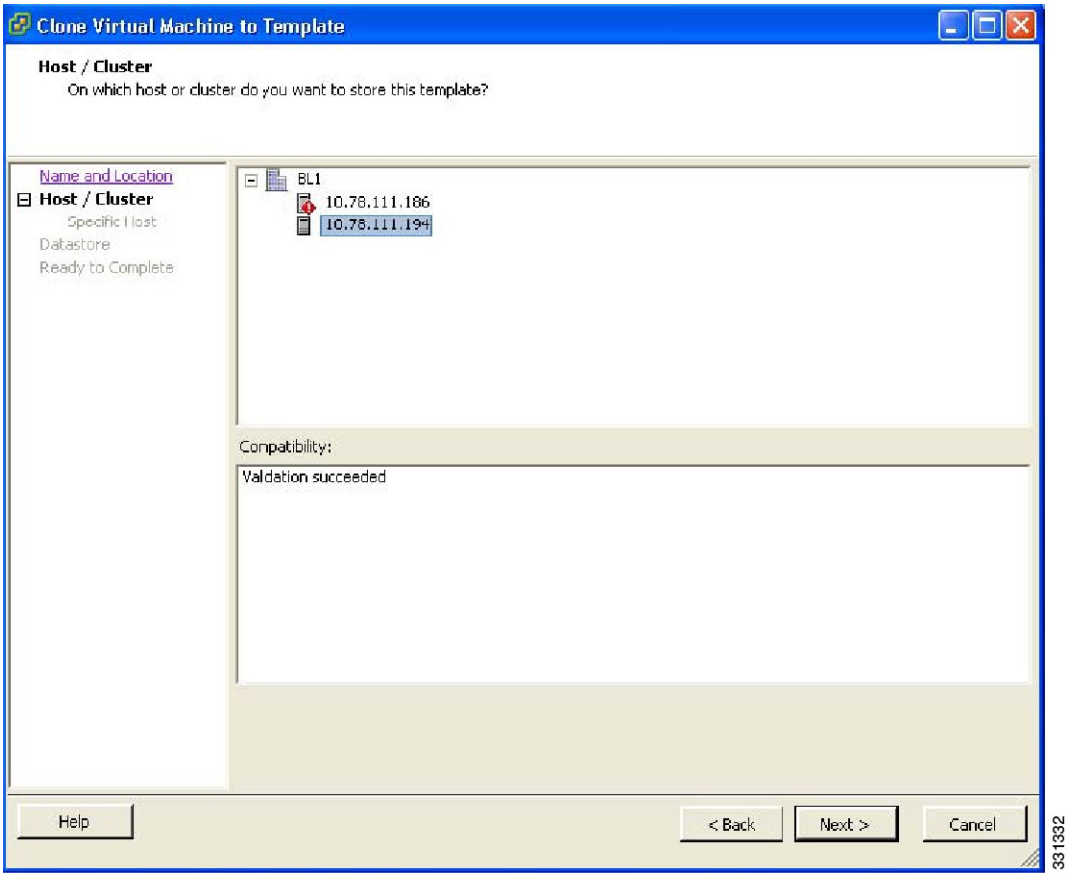
ステップ 6　[Template Name] フィールドに名前を入力します。

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] ウィンドウが開きます。

図 *6* : *[Host]* ウィンドウ

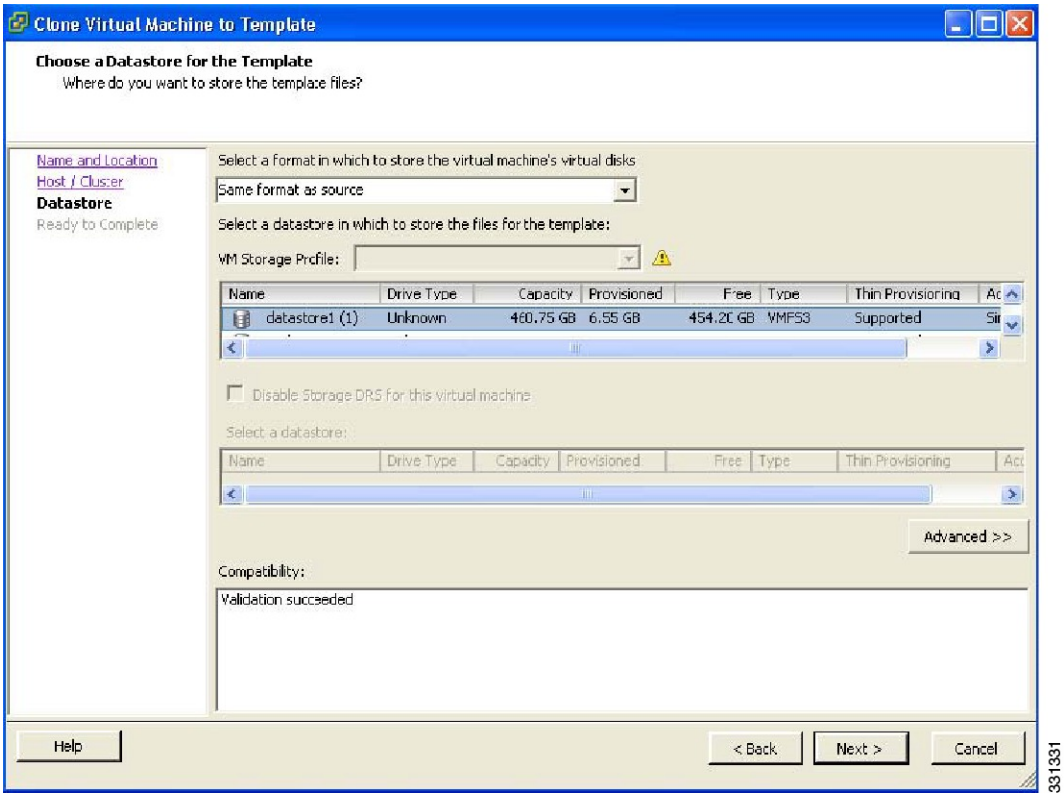


ステップ 9　テンプレートを格納するホストを選択します。

ステップ 10　[Next] をクリックします。

[Choosing a Datastore] ウィンドウが開きます。

図 *7* : ***[Choosing a Datastore]*** ウィンドウ



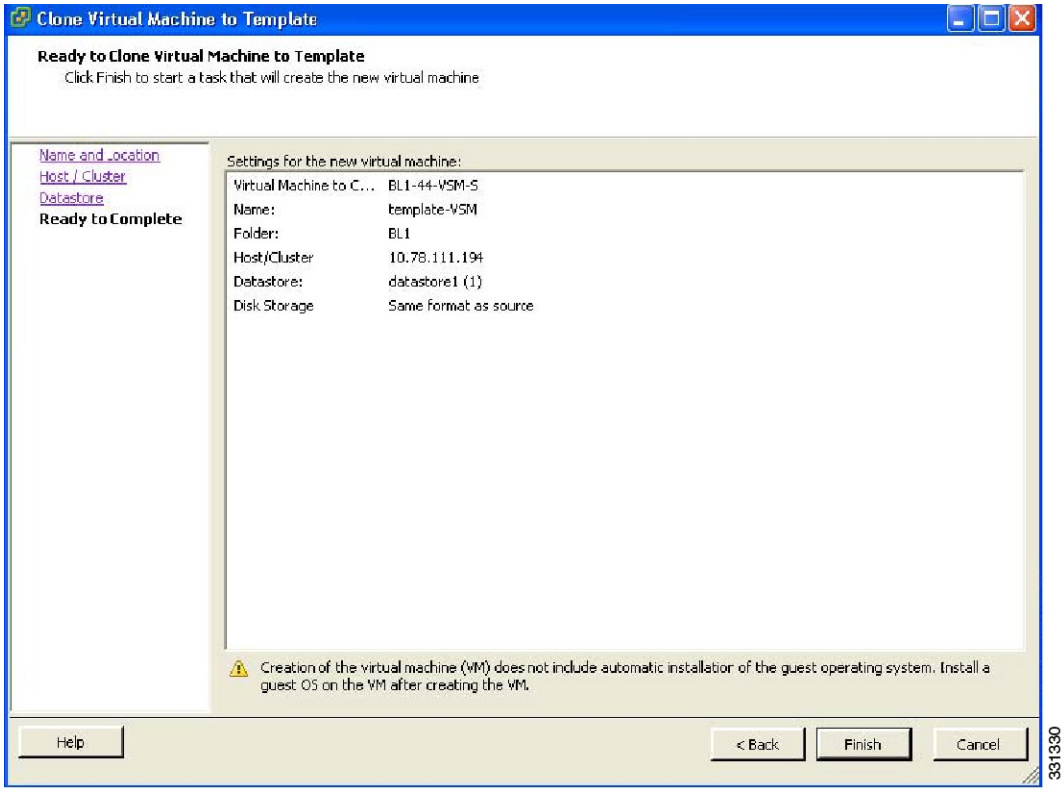
ステップ 11 [Select a format in which to store the virtual machine's virtual disks] ドロップダウン リストで、[Same format as source] を選択します。

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 the Settings] ウィンドウが開きます。

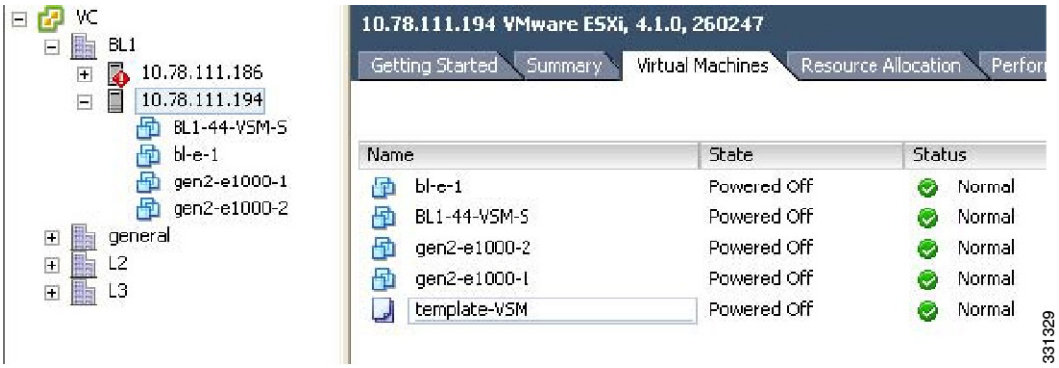
図 *8*：*[Confirming the Settings]* ウィンドウ



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 テンプレートが作成され、[Virtual Machines] タブに表示されます。

ステップ 15　[Template Virtual Machine] ウィンドウが開きます。
これで、テンプレートの作成が完了しました。

図 *9*：*[Template Virtual Machine]* ウィンドウ



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。

はじめる前に

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。
- 設定を大幅に変更した。

手順

コマンド **copy running-config scp://root@10.78.19.15/tftpboot/config/** を入力し、VSM をバックアップします。

例：

```
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

ここでは、バックアップ 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。 この項では、次のトピックについて取り上げます。

- バックアップ VSM VM の配置
- 古い設定の削除
- VSM のバックアップ コンフィギュレーションの復元

バックアップ VSM VM の配置

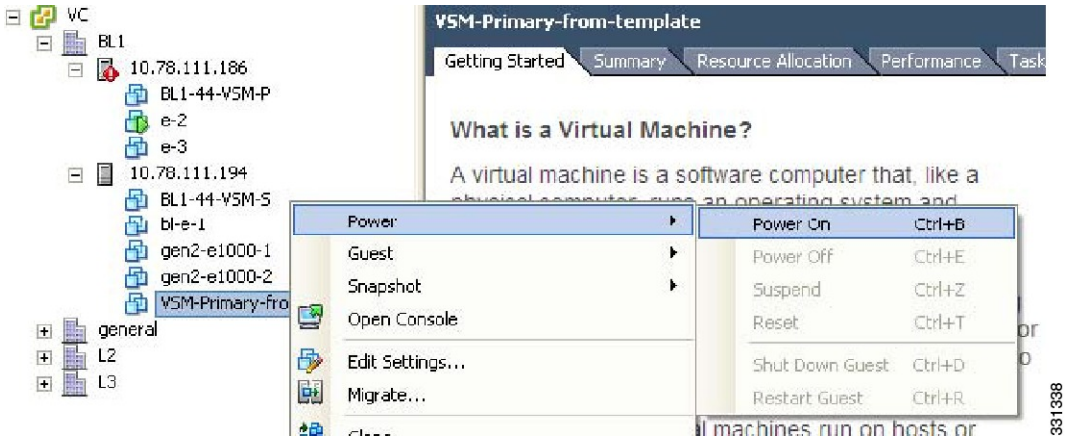
ここでは、プライマリおよびセカンダリ VSM が存在しない場合にバックアップ VSM VM を配置する方法について説明します。

（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。
次の図に示すように、[vSphere Client] ウィンドウが開きます。

図 10：***[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。

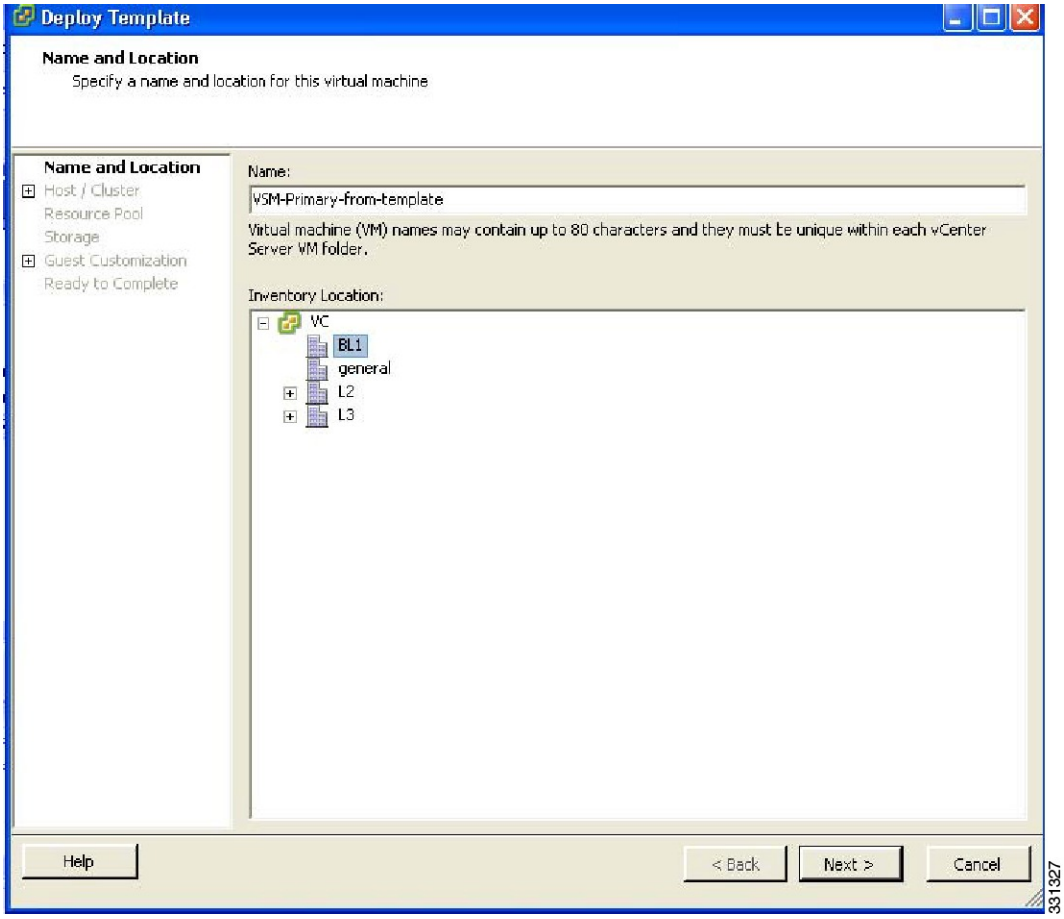
ステップ 3 [Virtual Machines] タブをクリックします。

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] ウィンドウが開きます。

図 *11*：*[Deploy Template Wizard]* ウィンドウ



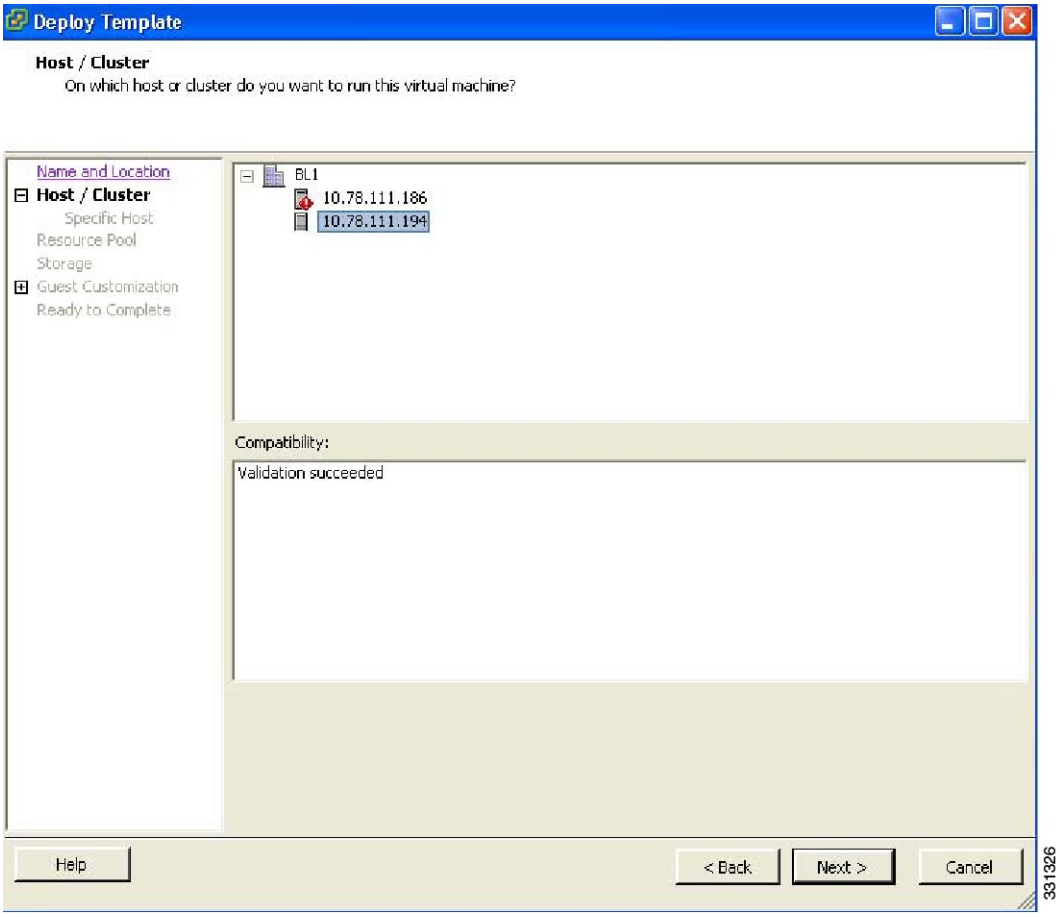
ステップ 6　[Name] フィールドに VSM の名前を入力します。

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] ウィンドウが開きます。

図 *12*：*[Choosing a Host]* ウィンドウ



ステップ 9　ホストを選択します。

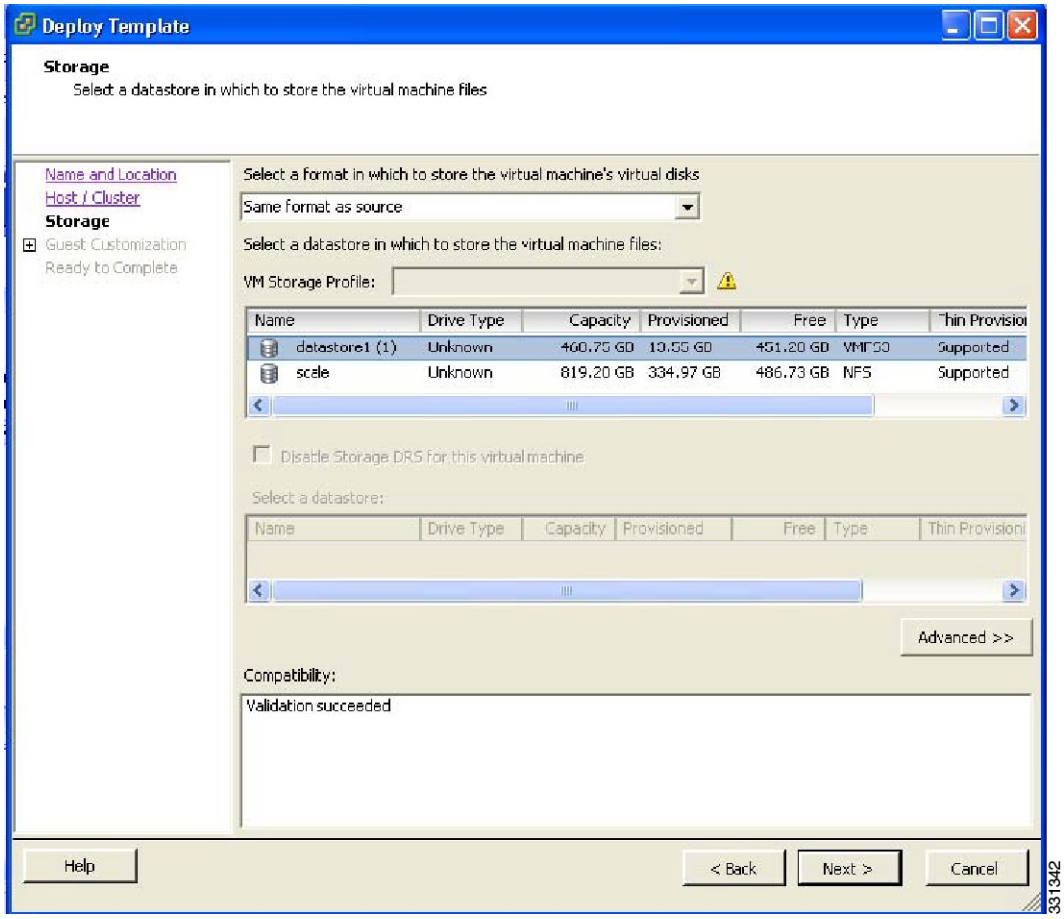
ステップ 10

例：

[Next] をクリックします。

[Choosing a Datastore] ウィンドウが開きます。

図 *13*：*[Choosing a Datastore]* ウィンドウ



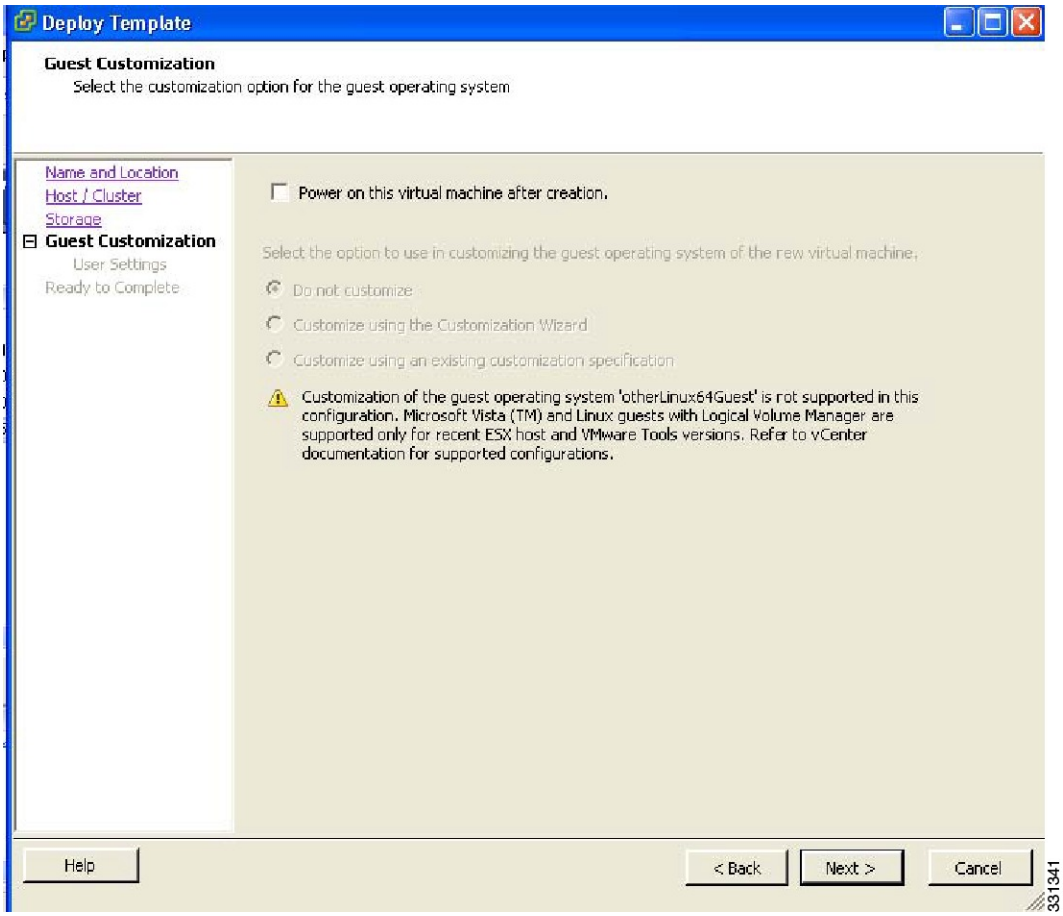
ステップ 11 [Select a format in which to store the virtual machine's virtual disks] ドロップダウン リストで、[Same format as source] を選択します。

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] ウィンドウが開きます。 [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。

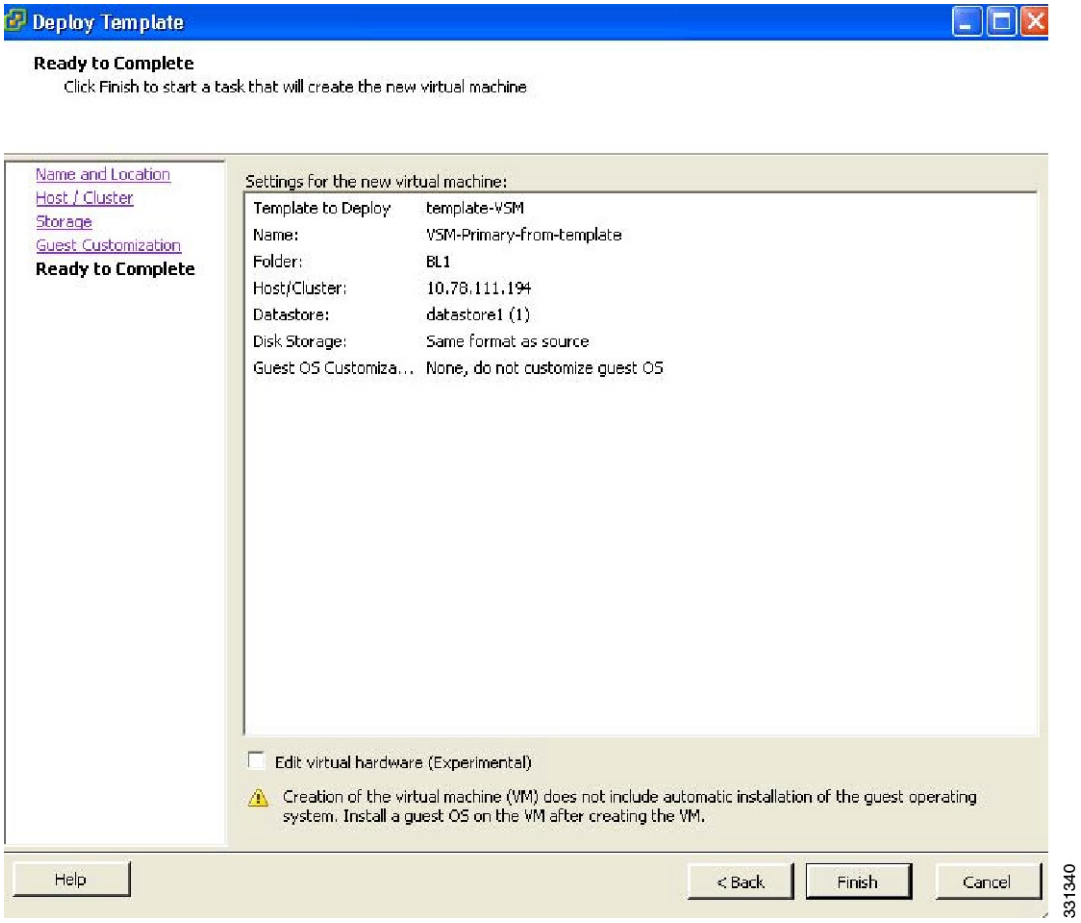
図 *14*：*[Guest Customization]* ウィンドウ



ステップ 14　[Next] をクリックします。

[Deploy Template - Ready to Complete] ウィンドウが開きます。

図 *15*：*[Guest Customization]* ウィンドウ



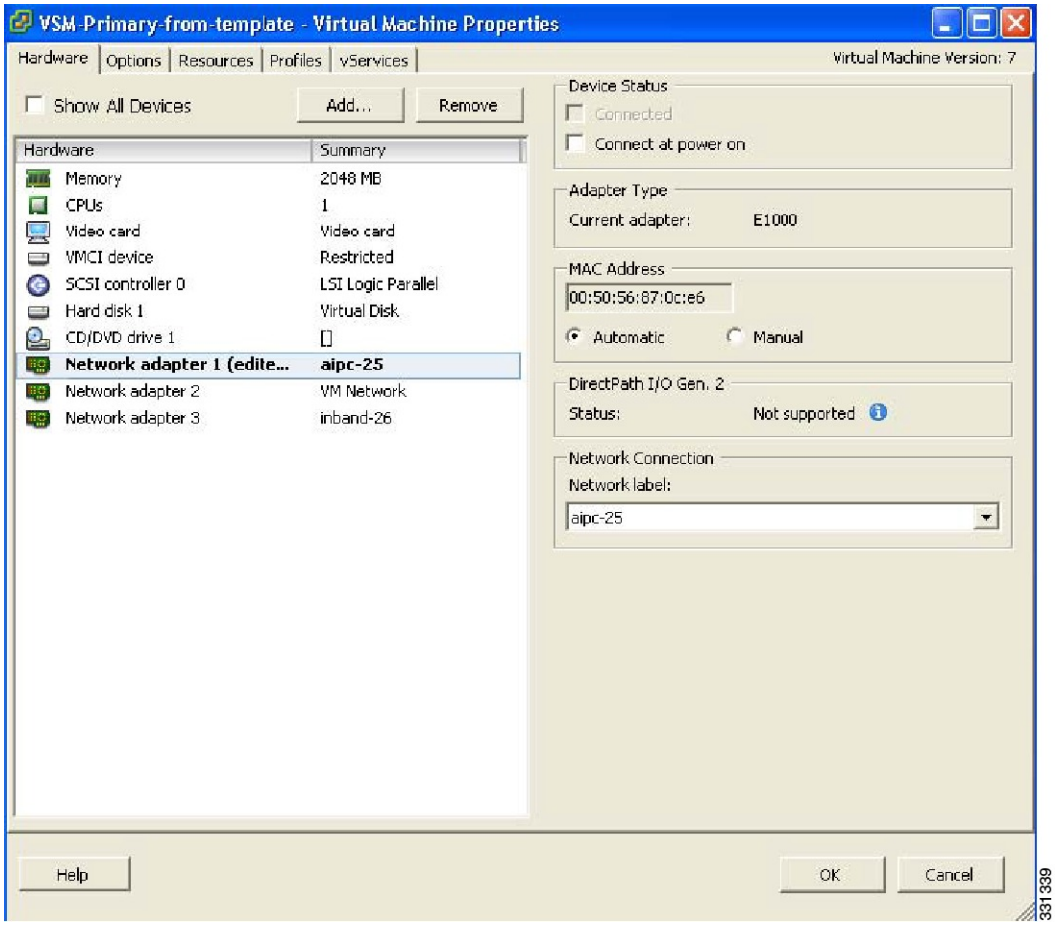
ステップ 15　新しい仮想マシンの設定を確認し、[Finish] をクリックします。 VEM で管理 VLAN を使用できない場合は、vSwitch に管理インターフェイスを追加する必要があります。

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 *16*：*[Guest Customization]* 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　[Connect at power on] チェックボックスをオフにします。

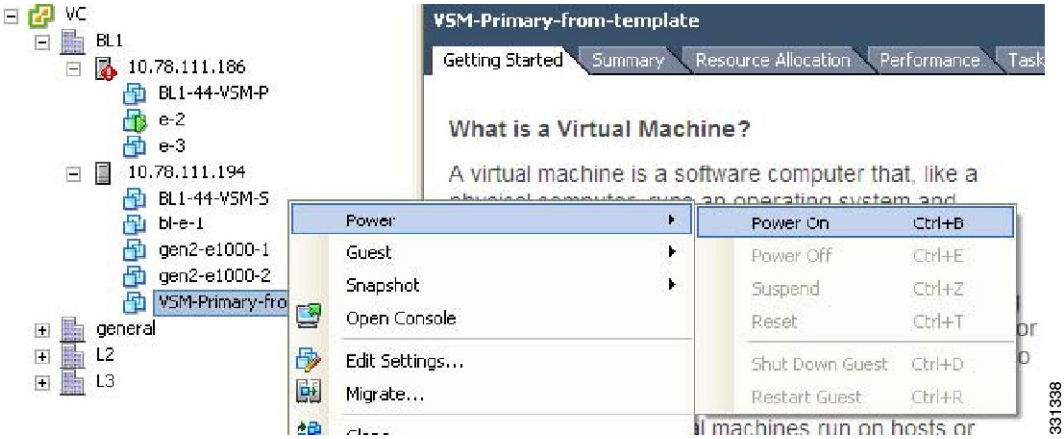
ステップ 20　[Network Adapter 2] を選択します。

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 *17* : *[Guest Customization]* 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セットします:

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。

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。

ステップ 5 次のコマンドを入力して、プライマリおよびセカンダリ VSM を再起動します。

この例では、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

```
switch# system redundancy role primary
Setting will be activated on next reload
```

```
switch# copy running-config startup-config
scp:        sftp:           startup-config
[####################################] 100%
switch# write erase
Warning: The command will erase the startup-configurations.
Do you wish to proceed anyway? (y/n) [n] y
switch# reload
This command will reboot the system. (y/n)? [n] y
switch# reload
This command will reboot the system. (y/n)? [n] y
```

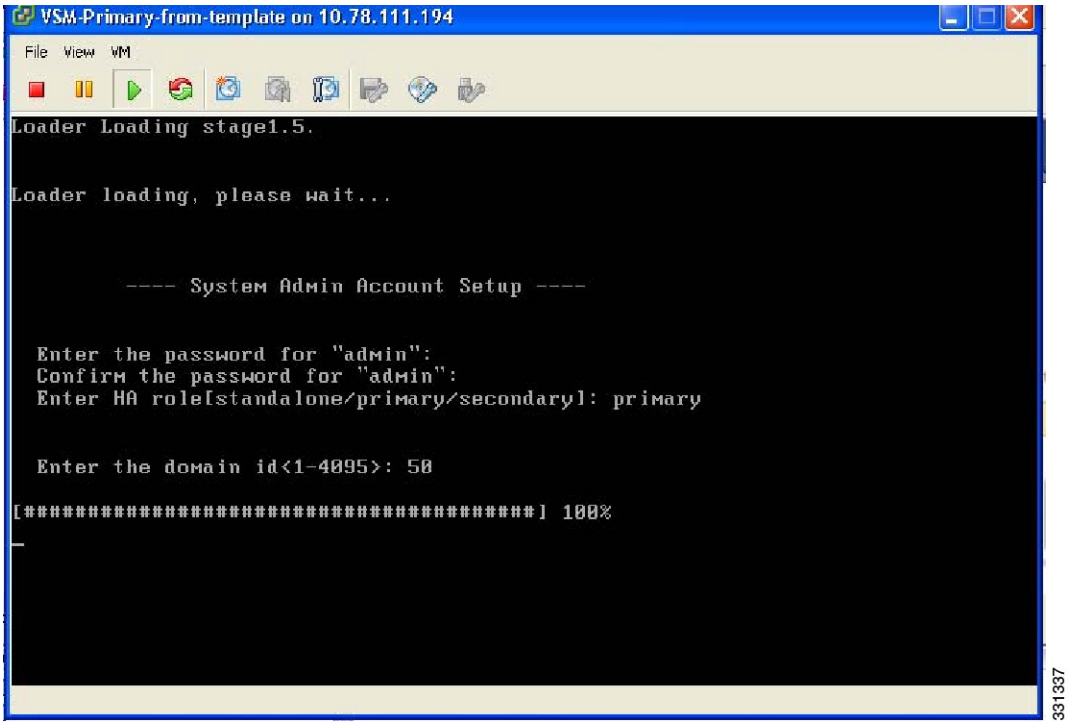
VSM のバックアップ コンフィギュレーションの復元

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。

手順

ステップ 1 VSM がリブートすると、[System Admin Account Setup] ウィンドウが開きます。

図 *18*：*[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て確認します。

例：

```
---- 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。

例：
```
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。

例：
```
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。

例：
```
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。

例：
```
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。

例：
```
Configure read-only SNMP community string (yes/no) [n]: no
```

ステップ 8 読み取り/書き込み 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。

例：
```
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。

例：
```
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。

例：
```
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。

例：
```
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。

例：
```
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 InterCloud Security Configuration Guide*』を参照してください。

例：
```
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。

例：
```
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。

例：
```
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。

例：
```
Vem feature level will be set to 4.2(1)SV1(4a).
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。

例：
```
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。

例：
```
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。

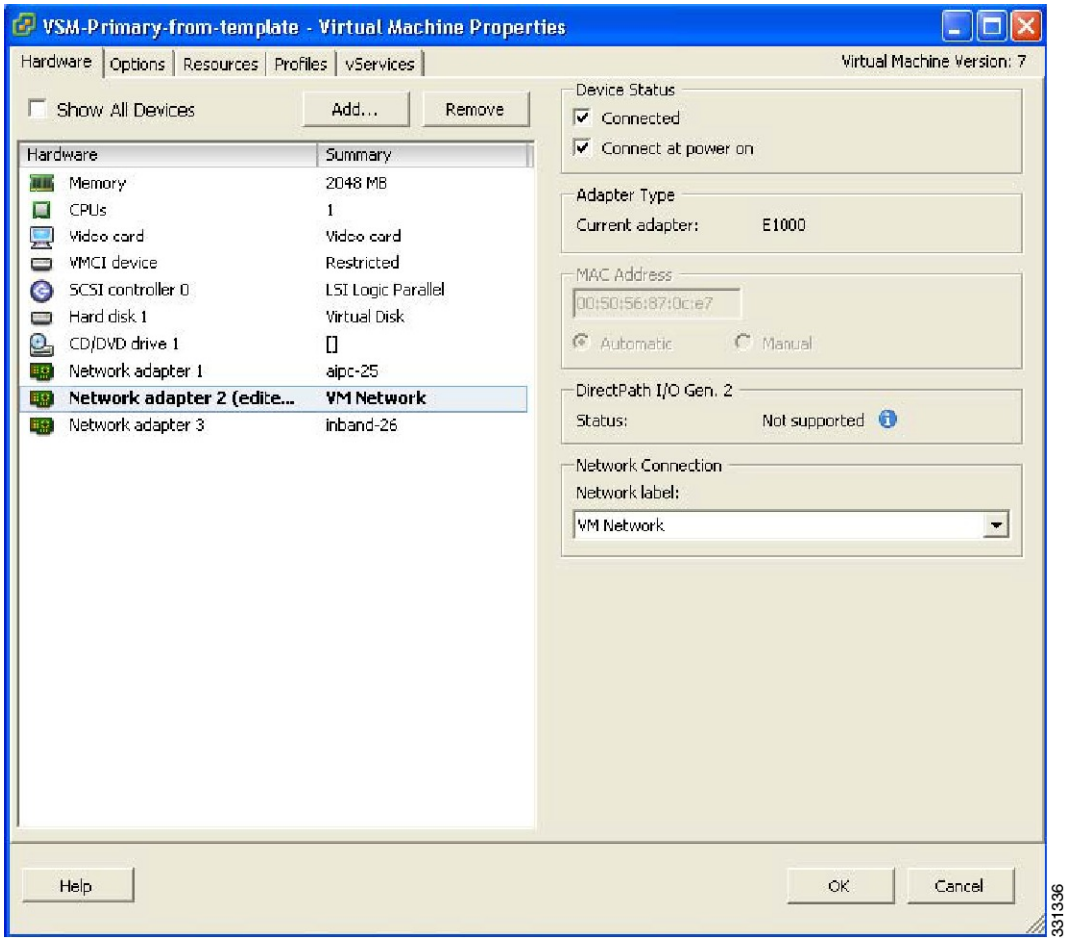
例：

```
Use this configuration and save it? (yes/no) [y]: yes
[########################################] 100%
```

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。

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 *19*：*[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。

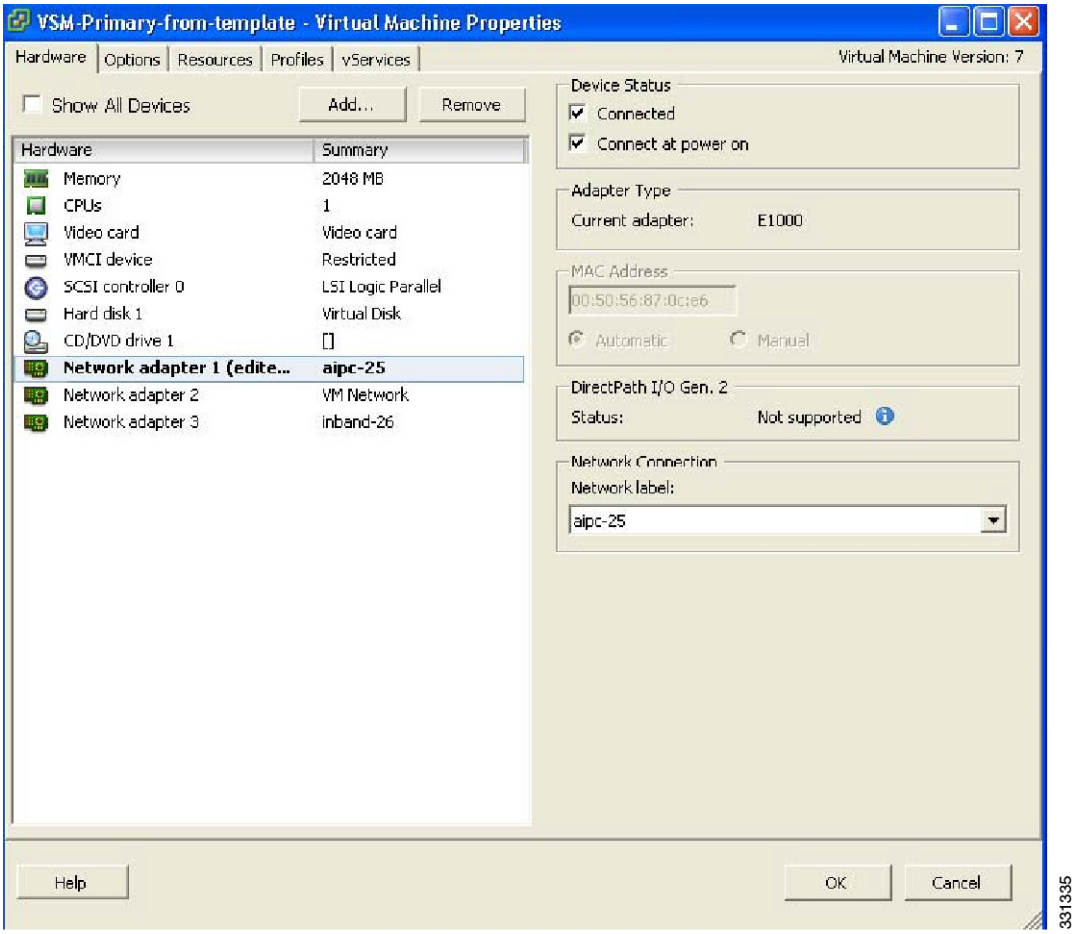
ステップ 23 次のコマンドを入力して、VSM のブートフラッシュにバックアップ コンフィギュレーションをコピーします。

例：

```
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 [Virtual Machine Properties] ウィンドウが表示されます。

図 *20*：*[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 コマンド **show module** を入力して、VEM が VSM に接続されていることを確認します。

ステップ 28 コマンド **copy bootflash:VSM-Backup-running-config running-config** を入力して、バックアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
この手順は ERSPAN/NFM などの機能に必要です。

ステップ 29 Cisco Nexus 1000V InterCloud VSM を Cisco Prime Network Services Controllerに登録します。 Cisco Nexus 1000V InterCloud VSM CLI で、次のコマンドを入力します。

```
switch# configure terminal
switch(config)#  nsc-policy-agent
switch(config-nsc-policy-agent)#   no policy-agent-image
switch(config-nsc-policy-agent)#  no shared-secret
switch(config-nsc-policy-agent)#   shared-secret Example_Secret123
switch(config)#  policy-agent-image bootflash:///vsmcpa.3.0.1c.bin
switch(config)# exit
```

ステップ 30 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。

例：

```
switch# copy running-config startup-config
[########################################] 100%
switch#
```

ステップ 31 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。 **show module**

ステップ 32 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。

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の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	Release 5.2(1)IC1(1.1)	この機能が導入されました。