Cisco Nexus 9000v ガイド、リリース 9.3(x)

初版：2019 年 7 月 20 日

最終更新：2020 年 1 月 30 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/

【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。

目 次

Trademarks ?

はじめに：

はじめに vii

対象読者 vii

表記法 vii

Cisco Nexus 9000 シリーズ スイッチの関連資料 viii

マニュアルに関するフィードバック viii

Communications, Services, and Additional Information ix

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

Cisco Nexus 9000v 3

Cisco Nexus 9000v について 3

Cisco Nexus 9000v Guidelines and Limitations 4

Cisco Nexus 9000v を使用した仮想化の利点 6

Cisco Nexus 9000v Software Functionality 6

Cisco Nexus 9000v のシステム管理の設定 10

Cisco Nexus 9000v のリソース要件 10

VMware ESXi のサポート情報 11

ESXi 6.5 での Cisco Nexus 9000v の展開に関する注意事項 11

ESXi 6.5 での古い vmdk ファイルの使用 12

KVM-QEMU のサポート情報 13

VirtualBox のサポート情報 13

VMware Fusion のサポート情報 14

Cisco Nexus 9000v のインストールと展開 14
Cisco Nexus 9000v シリーズの NX-OS ソフトウェアのアップグレードとダウングレード 14
Cisco Nexus 9000v の設定 15
中断を伴う ISSU を使用した Cisco Nexus 9000v のアップグレード 15
中断を伴う ISSU の設定 16
Cisco Nexus 9000v の展開 17
分散 OVA を使用した ESXi ハイパーバイザでの Cisco Nexus 9000v のプロビジョニング 17
ハイパーバイザの KVM または QEMU への Cisco Nexus 9000v の展開 18
KVM または QEMU 環境のネットワーキング 21
VirtualBox への Cisco Nexus 9000v の展開 21
事前にパッケージ化されたボックスを使用した VirtualBox と Vagrant への Cisco Nexus 9000v の展開 21
VM の削除 23
ネットワーク トポロジの例 23

第 3 章 **Cisco Nexus 9000v のトラブルシューティング 27**
すべてのハイパーバイザに共通の問題 27
VM が「loader >」プロンプトに落ちたときに起動する方法 27
VM が「loader >」プロンプトにドロップしないようにする方法 28
ESXi ハイパーバイザー 28
SATA コントローラを使用して Cisco Nexus 9000v の起動プロセスを高速化する方法 28
シリアル コンソールから「loader >」プロンプトにアクセスする方法 29
EFI シリアル コンソールが有効になっていない場合に ESXi 上のスイッチに接続する方法 29
Cisco Nexus 9000v が起動するとすぐに vCenter または UCS サーバーの接続が失われる 30
Cisco Nexus 9000v のデータ ポートが ESXi サーバーでトラフィックを渡していない 30
KVM または QEMU ハイパーバイザ 31
KVM または QEMU ハイパーバイザでのマルチキャスト 31
VirtualBox 31
VirtualBox または Vagrant でのネットワーキング 31
VM が VirtualBox/Vagrant で起動できない 31

L2FWDER のトラブルシューティング 32
概要 32
L2FWDER のコマンド 33
RX/TX パスのトラブルシューティング 34
MAC 学習のトラブルシューティング 34
レイヤ 2/レイヤ 3 トラフィックの l2fwder/pktmgr/netstack でのパケット ドロップのトラブルシューティング 35
VXLAN BGP EVPN のトラブルシューティング 38
VXLAN Encap/Decap のトラブルシューティング 40
コマンド 41
VM ログの収集 41

はじめに

この前書きは、次の項で構成されています。

- 対象読者 （vii ページ）
- 表記法 （vii ページ）
- Cisco Nexus 9000 シリーズ スイッチの関連資料 （viii ページ）
- マニュアルに関するフィードバック （viii ページ）
- Communications, Services, and Additional Information （ix ページ）

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

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、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこ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、角かっこで囲み、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、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこ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。角かっこ内の波かっこと縦棒は、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ないでください。引用符を使用すると、その引用符も含めて string と見なされます。

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、スクリーン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。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

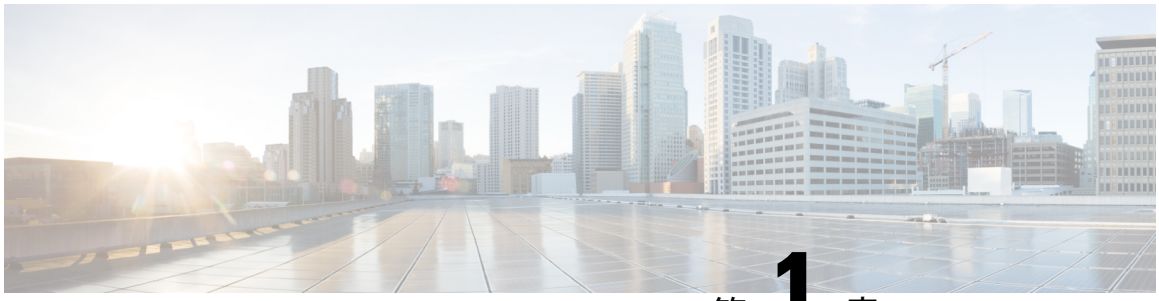
このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



第 1 章

新機能および変更された機能に関する情報

この章では、『*Cisco Nexus 9000v* ガイド *9.3(x)*』に記載されている、新機能および変更された機能に関するリリース固有の情報について説明します。

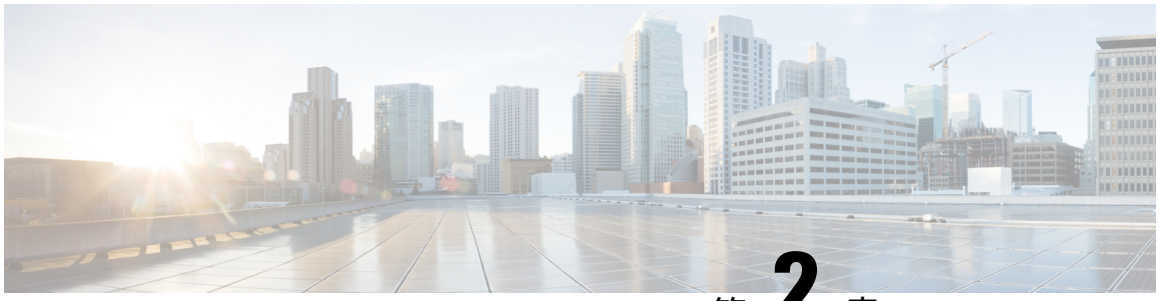
- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

表 *1*: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
Netconf、Restconf および gRPC	サポートが追加されました。	9.3(1)	Cisco Nexus 9000v Software Functionality （6 ページ）
Cisco NX-OS リリース 9.2(x) からアップデートなし)	最初の9.3(x) リリース	N/A	N/A

新機能および変更された機能に関する情報



第 2 章

Cisco Nexus 9000v

この章は、次の項で構成されています。

- Cisco Nexus 9000v について （3 ページ）
- Cisco Nexus 9000v Guidelines and Limitations, on page 4
- Cisco Nexus 9000v を使用した仮想化の利点 （6 ページ）
- Cisco Nexus 9000v Software Functionality, on page 6
- Cisco Nexus 9000v のシステム管理の設定 （10 ページ）
- Cisco Nexus 9000v のリソース要件 （10 ページ）
- VMware ESXi のサポート情報 （11 ページ）
- KVM-QEMU のサポート情報 （13 ページ）
- VirtualBox のサポート情報 （13 ページ）
- VMware Fusion のサポート情報 （14 ページ）
- Cisco Nexus 9000v のインストールと展開 （14 ページ）
- Cisco Nexus 9000v シリーズの NX-OS ソフトウェアのアップグレードとダウングレード （14 ページ）
- Cisco Nexus 9000v の設定 （15 ページ）
- 中断を伴う ISSU を使用した Cisco Nexus 9000v のアップグレード （15 ページ）
- 中断を伴う ISSU の設定 （16 ページ）
- Cisco Nexus 9000v の展開 （17 ページ）
- ネットワーク トポロジの例 （23 ページ）

Cisco Nexus 9000v について

Cisco Nexus 9000v は、Cisco Nexus 9000 ソフトウェアを実行するネットワーク要素のコントロール プレーンの側面をシミュレートするように設計された仮想プラットフォームです。Cisco Nexus 9000v には、特定のハードウェア エミュレーションは実装されていませんが、Cisco Nexus 9000 ハードウェア プラットフォームで実行されるものと同じソフトウェア イメージを共有しています。ソフトウェアが仮想マシンとして実行されている場合、ラインカード (LC) ASIC プロビジョニング、またはコントロール プレーンからハードウェア ASIC への相互作用は、Cisco Nexus 9000v ソフトウェア データ プレーンによって処理されます。

Cisco Nexus 9000 シリーズに対応する Cisco Nexus 9000v は、devops モデルを有効にし、インフラストラクチャまたはインフラストラクチャ自動化ツールへの変更を迅速にテストするための、便利なツールを提供します。これにより、顧客は、本番ネットワークに適用する前に、シミュレートされたネットワークで構成の変更を検証できます。また、一部のユーザーは、シミュレーションシステムを、機能テスト、検証、自動化ツールの開発、および展開前のテストシミュレーションで使用することにも関心を示しています。Cisco Nexus 9000v は、ソフトウェア定義ネットワーク（SDN）やネットワーク機能仮想化（NFV）ベースのソリューションを検証するための、プログラマビリティ システムとして使用できます。

Cisco Nexus 9000v Guidelines and Limitations

Cisco Nexus 9000v has the following guidelines and limitations:

- Cisco Nexus 9000v does not support the VGA console. You must provision a serial console on a VM to access the Nexus 9000v switch prompt on initial boot. See VirtualBox への Cisco Nexus 9000v の展開, on page 21 for more information.
- When N9000v VMs are created by KVM hypervisor, the following issues may occur due to the default setting on the Linux Bridge:
  - LLDP communication between the VMs: The LLDP communication is not established between N9000v. For the solution, the following Linux Bridge settings should be configured. (In the example, assume vb7af2d7ab777d0 is the Linux Bridge that is used for connecting two VMs.
    1. Stop STP running on the Linux Bridge using the **brctl setageing vb7af2d7ab777d0 0** command.
    2. Allow LLDP to be forwarded on the Linux Bridge using the **echo 0x4000 > /sys/class/net/vb7af2d7ab777d0/bridge/group_fwd_mask** command.
    3. Stop LLDP service running on Linux base host (on which the topology is running) using the **/etc/init.d/lldpd stop** command.
    4. [Optional] Disable multicast snooping using the **echo 0 > /sys/devices/virtual/net/vb7af2d7ab777d0/bridge/multicast_snooping** command.
  - LACP connection between the VMs: The LACP connection is not formed between eNXOSv. For the solution, complete the following steps:
    - The Linux kernel should be patched.
    - Group forward mask should be set up using the **echo 0x4 > /sys/class/net/vb7af2d7ab777d0/bridge/group_fwd_mask** command.
  - The multicast packet may not flow through the Linux Bridge. For the solution, use the **echo 0 > /sys/devices/virtual/net/vb7af2d7ab777d0/bridge/multicast_snooping** command.
  - Some ports may get into STP blocked port by the Linux Bridge. For the solution, disable the STP running on the Linux Bridge using the **brctl setageing vb7af2d7ab777d0 0** command.
- After initial setup of the Cisco Nexus 9000v, you must configure the booting image in your system. Otherwise, the Cisco Nexus 9000v drops to the `loader>` prompt after reload/shut down.

```
switch# configure terminal
switch(config)#  boot nxos bootflash:nxos.9.2.1.bin
switch(config)#  copy running-config startup-config
```

- Cisco Nexus 9000v does not support VGA console. You must provision the serial console on any VM to access the Cisco Nexus 9000v switch prompt on initial boot.
- Cisco Nexus 9000v chassis node can be managed using the Cisco Network Manager, such as SNMP.
- The Cisco Nexus 9000v uses vNICs that are entered from the KVM/QEMU command line or from the GUI on ESXi for networking either externally or internally within a hypervisor server. The first NIC is always used as the Cisco Nexus 9000v management interface. The subsequence NICs are used as data ports as e1/1, e1/2, ... e1/9. Maximum 128 interfaces can be supported on the Cisco Nexus 9000v VM depending on the hypervisor capability. Since currently, only KVM/Qemu hypervisor has this maximum capability, total 129 NICs are required

Note A maximum of 128 data ports (e1/1, e1/2, ... e1/128) are supported.

Connect only the first NIC for the Cisco Nexus 9000v VM as the management interface to your LAN physical switch or vSwitch (VM Network) connecting directly to a physical switch. Do not connect any data port vNIC to any physical switch that conflicts with your server management connectivity.

- Cisco Nexus 9000v only supports the ESXi standard vSwitch when VMs are interconnected within a hypervisor or an external physical switch.
- The vSwitch mapping to data port interface is required to have Promiscuous Mode as the Accept mode in order to pass traffic between VMs.
- The Cisco Nexus 9000v operates as a bridge that generates BPDU packets on its Ethernet interfaces as it participates in Spanning Tree Protocol (STP). It also forwards broadcast, unknown unicast, and multicast traffic as expected by classic bridging logic. Do not connect the Cisco Nexus 9000v data plane interfaces to the upstream network in a manner that would create bridging loops or interfere with upstream STP operation.
- Cisco Nexus 9000v is supported in the Virtual Internet Routing Lab (VIRL) and the Cisco Modeling Lab (CML) environment running as a VM.
- VXLAN BGP EVPN is supported on Cisco Nexus 9000v. For details on VXLAN configuration, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide .
- Beginning with Cisco NX-OS Release 9.2(1), VXLAN EVPN multi-site is supported on Cisco Nexus 9000v. For details on VXLAN EVPN multi-site configuration, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide.
- When you configure the supported Cisco Nexus 9000 features on Cisco Nexus 9000v, it is necessary that you configure the TCAM carving. For example, when configuring ARP suppression with BGP-EVPN, use the **hardware access-list tcam region arp-ether** *size* **double-wide** command to accommodate ARP in this region. (You must decrease the size of an existing TCAM region before using this command.)
- Beginning with Cisco NX-OS Release 9.3(5), the **show interface counters** is supported for analyzing packet-flow on network topology. The users can use CLI or any SNMP query to get traffic flow counters on a N9Kv device.

- Statistics for Routed packet and Multicast packets are not supported.
-

Cisco Nexus 9000v を使用した仮想化の利点

この仮想プラットフォームは、クラウド環境でこれらの仮想化の利点を提供します。ハードウェアのタイプやその他のリソースに限定されません。

利点	説明
ハードウェアからの独立	この仮想プラットフォームは、クラウド環境でこれらの仮想化の利点を提供します。ユーザーはハードウェアやその他のリソースに限定されません。 （注） Cisco Nexus 9000v ベースの VM の最小 RAM/メモリ要件は 5GB です
リソースの共有	Cisco Nexus 9000v で使用されるリソースはハイパーバイザによって管理されており、VM 間で共有できます。VM サーバーが特定の VM に割り当てたハードウェア リソースの量は、サーバー上の別の VM に再割り当てできます。
展開の柔軟性	VM はあるサーバーから別のサーバーに容易に移動できます。したがって、ある物理的な場所にあるサーバーから別の物理的な場所にあるサーバーへ、ハードウェア リソースを移動せずにCisco Nexus 9000v を移動できます。
ダイナミックなネットワーキング	ユーザーは、物理的な配線を行わなくても、数分でネットワーク接続と構成を変更できます。

Cisco Nexus 9000v Software Functionality

Supported Features

The following table displays specific Layer 2 and Layer 3 software feature support based on branch/lineup.

Table 2: Supported Layer 2 and Layer 3 Features (Software)

Technology	Nexus Feature Name	Support Statement
OS Infra	Bash Shell	Supported

Technology	Nexus Feature Name	Support Statement
	Guest Shell	Supported
	SSH	Supported
	RPM Installation	Supported
	POAP	Supported
Programmability	NXAPI	Supported
	Ansible	Supported
	Puppet Integration (Guest Shell)	Supported
	Chef Integration (Guest Shell)	Supported
	NETCONF	Supported
	RESTCONF	Supported
	gRPC	Supported
	Docker	Supported (Kubernetes API Server) For information on the Docker support, see Cisco Nexus 9000 Series NX-OS Programmability Guide
L3 Features	L3 SVI	Supported
	BGP v4	Supported (No BFD, EVPN)
	BGP v6	Supported (No BFD, EVPN)
	OSPFv2	Supported (No BFD, EVPN)
	OSPFv3	Supported (No BFD, EVPN)
	EIGRP	Supported
	RIP	Supported
L2 Features	L2 Switching Unicast	Supported
	L2 Switching Broadcast	Supported
	CDP	Supported
	LLDP	Supported

Technology	Nexus Feature Name	Support Statement
	L2 Switching Multicast	Supported as Broadcast (not explicit Mcast) , No PIM or Mcast Group support
	ARP Suppression	Supported
	MAC learning	Supported
	Static/Router MAC	Supported
	Switchport	Supported
	802.1q VLAN Trunk/Access	Supported
	STP	Supported
	Subinterfaces	Supported
	VXLAN and VXLAN EVPN	Supported
	VXLAN EVPN Multi-Site	Supported (with non-vPC on border-leafs).
	vPC	Supported
	Port channel	Supported
	SNMP	Supported

Note The Cisco Nexus 9000v features in this table have been verified to operate only with the Cisco devices mentioned in this document.

If a networking or system feature is not identified as a supported feature in this document, it should be considered as unsupported despite that it may seem to work correctly. Unsupported features did not have any level of regression testing on Cisco Nexus 9000v.

Table 3: NX-OS Features Not Supported (Not Tested)

NX-OS Features	Limitations
QoS	Not supported on Cisco Nexus 9000v.
BFD	Not supported on Cisco Nexus 9000v.
ACL	Not supported on Cisco Nexus 9000v.
Policy maps	Not supported on Cisco Nexus 9000v.
SPAN	Not supported on Cisco Nexus 9000v.
IGMP Snooping	Not supported on Cisco Nexus 9000v.

NX-OS Features	Limitations
AMT	Not supported on Cisco Nexus 9000v.

The following list (not comprehensive) contains known system limitations.

Table 4: NX-OS System Limitations

System Capabilities	Limitations
MAC Address	Cisco Nexus 9000v does not integrate the L2FM module and L2FDWR data plane. It maintains its own MAC Table. Therefore the behavior of the MAC address related CLIs will be different from the physical platform.
Statistics	Cisco Nexus 9000v does not sure interface statistics.
Consistency Checker	The consistency checker has a hardware dependency and hence is not supported on Cisco Nexus 9000v. All ‘show’ and ‘exec’ commands will result with appropriate error/warnings.
Network Throughput	Low data plane performance. Additional rate limiter is in place to limit the total amount of traffic received by Cisco Nexus 9000v to 4M.
TOR-ISSU	TOR-ISSU is not supported.
Link Status	Cisco Nexus 9000v virtual interfaces serve as the ‘Ethernet Ports’. The link status of these links within the NX-OS is dependent on the Hypervisor’s capability.
Link-down	Connectivity between the two ends of the interface link is simulated, hence it is important that you shut the interface in both the ends, followed by no shut at both the ends of the interface link.

Cisco Nexus 9000v Feature UI/CLI Difference From Hardware Platform

Feature enablement in the Cisco Nexus 9000v virtual platform is the same as Cisco Nexus 9000 hardware platform.

For example, the following features can be enabled:

- **feature telnet**
- **feature bash-shell**
- **feature ospf**
- **feature bgp**
- **feature interface-vlan**
- **feature nv overlay**

However, not all commands are available for Cisco Nexus 9000v, such as hardware data plane specific commands. Some of these commands exist in the command parse chain, but these commands might not display correct output information. It is not possible for the virtual platform to verify all commands on Cisco Nexus 9000v that exist for the Cisco Nexus 9000 hardware platform.

A few commands are critical for Cisco Nexus 9000v to display Layer 2/Layer 3 information, but are not provided for the Cisco Nexus 9000v platform. The following displays substitute commands:

NX-OS Hardware Platform Commands	Substitute for Cisco Nexus 9000v
show mac address-table	**show system internal l2fwder mac**
clear mac address-table	**clear mac address-table datapath static|dynamic**

Cisco Nexus 9000v のシステム管理の設定

Cisco Nexus 9000v は、コントロール プレーンの面で、Nexus 9000 シリーズ TOR ハードウェア プラットフォームと同じソフトウェアを実行します。該当するすべての CLI は、ハードウェア プラットフォームのものと同じになります。このリリースでは、Nexus 9000v シャーシ管理用のシンプル ネットワーク管理プロトコル（SNMP）が追加されています。Nexus 9000v SNMP ソフトウェアは、Nexus 9000 シリーズ ハードウェア プラットフォームに固有の基本的な SNMP インフラストラクチャです。システム管理設定は、Cisco Nexus 9000 シリーズのドキュメントに従って実施する必要があります。ただし、管理エンティティには、Nexus 9000v プラットフォーム固有の制限が適用されます。たとえば、Nexus 9000v プラットフォームにはインターフェイスの統計情報がないため、そのようなデータはどの管理要求でも使用できません。サポートされている機能の詳細については、Cisco Nexus 9000v Software Functionality （6 ページ）を参照してください。

Cisco Nexus 9000v SNMP シャーシ管理は、次のエンティティ MIB をサポートします。ただし、このプラットフォームから取得できるのは、適用可能で意味のある属性のみです。

- CISCO エンティティ アセット MIB
- ceEXTEntityLEDTable
- ciscoEntityExtMIB
- ciscoRFMIB
- ciscoTSMIB
- ciscoEntityFRUControlMIB
- ciscoSyslogMIB

Cisco Nexus 9000v のリソース要件

Cisco Nexus 9000v は、Cisco Nexus 9000 シリーズ ハードウェアのソフトウェア イメージを使用します。次のリストに示す最小限のリソースが必要です。これらのリソースは、通常、どのサーバーでもオーバーサブスクライブされません。

- 8Gメモリ

- 最低 5G。複雑なトポロジに対応し、機能を有効化するには、8G の VM 構成をお勧めします。
- 最低 6G。複雑なトポロジに対応し、機能を有効化するには、8G の VM 構成をお勧めします。
- 1 ～ 4 個の vCPU
- 8G のハードディスク
- 1 x シリアル ポート
- 1 x ネットワーク インターフェイス カード（NIC）

サーバー ソフトウェアの要件

Cisco Nexus 9000v は、VMware ESXi 5.1（Post Build 1065491/ESXi 5.5）または Ubuntu Linux 14.04LTS 以降のバージョンと KVM-QEMU 2.5 の組み合わせをサポートする Cisco Unified Computing System (UCS) サーバーまたは主要ベンダーのサーバーで実行できます。

スタンドアロンの Cisco Nexus 9000v ノードのみが必要な場合は、仮想ボックス ハイパーバイザを備えた（および基本的なリソース要件を満たしている）ラップトップまたは Apple Mac Pro に展開することもできます。

VMware ESXi のサポート情報

仮想マシン（VM）は、VMware vSphere ハイパーバイザ上で稼働します。一連の VM を実行するとき、同じ VMware vSphere ハイパーバイザを使用することができます。VM を作成して管理するには、VMware vSphere Client GUI を使用します。

VMware vSphere Client が VMware vCenter Server VM を作成、構成、管理するためのアプリケーションです。Cisco CSR 9000v は、データ ストアにある仮想ディスクからブートできます。VMware vSphere Client を使用して Cisco CSR 9000v の開始と停止など、基本的な管理作業を実行できます。

VMware vCenter Server は、vSphere 環境を管理し、単一のコンソールからデータセンターのすべてのホストと VM を統合管理できます。

Cisco と VMware の連携の詳細については、https://www.vmware.com/partners/global-alliances/cisco.htmlを参照してください。

VMware の機能と操作の詳細については、https://www.vmware.com/support/pubs/を参照してください。

ESXi 6.5 での Cisco Nexus 9000v の展開に関する注意事項

VMware ESXi 6.5 に Cisco Nexus 9000v を展開する場合は、次のことを確認してください。

- ブート プロセスを高速化するために、VMware ESXi 6.5 サーバーで SATA コントローラを使用して Cisco Nexus 9000v VM を展開することをお勧めします。

- 展開環境に正しい VMware ESXi 6.5 サーバーおよびホスト ライセンスがあることを確認します。ライセンスが無効だと、展開環境が不安定になる可能性があります。不安定性の問題は VM に関連するもので、VM シリアル コンソールにアクセスできない、Cisco Nexus 9000v スイッチプロンプトにアクセスできない、誤ったエラー メッセージなどが含まれます。
- Mac 環境に展開する場合は、Opera ブラウザの使用をお勧めします。http://www.opera.com
- EFI のデフォルト ファームウェア オプション：Cisco Nexus 9000v には EFI ファームウェア ブートが必要です。http://software.cisco.com から配布されている ova ファイルをダウンロードします。VM をパワーオンする前に、[仮想マシンの編集（Edit Virtual Machine ）] 設定メニューから [EFI] を選択します。

（注） Windows で以前に vSphere クライアントを使用して Cisco Nexus 9000v を展開していた場合は、これを実行する必要はありません。

- http://software.cisco.com からダウンロードした分散 vmdk ファイルは、ESXi 6.5 リリース形式と互換性がありません。古い vmdk ファイルを使用するには、ESXi 6.5 での古い vmdk ファイルの使用 （12 ページ） を参照してください。
- VM 設定で vNIC を追加するときは、vNIC アダプタ タイプをデフォルト値の E1000E から E1000 に変更することが重要です。これは、E1000 だけが Cisco Nexus 9000v でサポートされているためです。

ESXi 6.5 での古い vmdk ファイルの使用

手順

ステップ 1 分散 vmdk フォーマットを ESXi ネイティブ ディスク フォーマットに変換し、SATA コントローラを使用します。

（注） ESXi 6.5 サーバーは、分散モノリス VMDK フォーマットを ESXi ネイティブ ディスク フォーマットに変換する **vmkfstools** ツールを提供します。この変換プロセスは、どの ESXI 6.5 サーバーでも実行できます。変換後、SATA ディスク コントローラーを使用して VM を作成できます。

```
nexus9000v-user@fe-ucs-dt13:vmkfstools -i nxosv-final.9.2.1vmdk nxos-final.9.2.1.esx.vmdk
```

ステップ 2 VM の作成中に、互換性の選択の手順で ESXi 5.5 以降を選択します。

ステップ 3 SATA コントローラを追加します。

ステップ 4 既存のハードディスクを追加し、1 で作成した nxos-final.7.0.3.I6.1.esx.vmdk を選択します。

ステップ 5 IDE の代わりに新しい SATA コントローラを選択します。

KVM-QEMU のサポート情報

カーネルベース仮想マシン（KVM）は、仮想化拡張機能を搭載した x86 ハードウェア上の Linux 向けの、オープンソース完全仮想化ソリューションです。コア仮想化インフラストラクチャを提供するロード可能カーネル モジュール（kvm.ko）と、プロセッサ固有のモジュール（kvm-intel.ko または kvm-amd.ko）で構成されています。

クイック エミュレータ（QEMU）は、ハードウェア仮想化を実現する無料のオープンソース ソフトウェア製品です。KVM がインストールされている Cisco UCS サーバーでは、QEMU を実行することができます。Cisco Nexus 9000v リファレンス プラットフォームの QEMU の推奨バージョンは、バージョン 2.2.0 以降です。

128 interfaces are supported for Cisco Nexus 9000v switches only on KVM hypervisor. このサポートは、Ubuntu 14.04.4 LTS および 16.04.3 LTS 環境に適用されます。QEMU のファイルは qemu-2.10.0-rc3.tar.xz です。

Cisco Nexus 9000v は、最大 128+1 のインターフェイスをサポートします（128 個のデータ ポート、たとえば、e1/1、e1/2..、e1/128 に加え、管理インターフェイス）。128 のインターフェースが必要ない場合でも、悪影響はありません。入力した vNIC ユーザーと同じ数が、適切なインターフェイス状態で表示されます。関連付けられた vNIC のない他のすべてのインターフェイスには、**link not connected**状態が表示されます。

インターフェイスがスムーズに機能するには、次の基準が満たされていることを確認してください。

- 128 のインターフェイスを利用可能にするには、KVM ハイパーバイザーのコマンド ラインからの合計 129 の vNIC（データ用に 128、管理用に 1）が必要です。
- VM resources must be sufficient in terms of memory and vCPUs based on the enabled features and interfaces.
- カーネルの起動時に PCI スキャンに時間がかかるため、システムの起動には 3 分余分にかかります。VM の起動時間を短縮するには、Qemu 2.9.93 (テスト済みバージョン) をお勧めします。Typical VM boot up time is proximately 5–6 minutes for all 128 data port interfaces to be able to pass the traffic in a large topology system. Qemu の古いリリース バージョンでは、VM の起動に時間がかかる場合があります。
- 128 の接続インターフェイスを使用するには、8G+ のメモリ フットプリントが必要です。

VirtualBox のサポート情報

VirtualBox は、エンタープライズおよびホーム ユーザー向けの強力な x86 および AMD64/Intel 64 仮想化製品です。これは、GNU General Public License (GPL) バージョン 2 の条件の下でオープン ソース ソフトウェアとして入手できるフリー ソフトウェアであり、https://www.virtualbox.org/ Web サイトから詳細情報を入手したりダウンロードしたりできます。

VMware Fusion のサポート情報

VMware Fusion は、エンタープライズおよび PC ユーザー向けの強力な仮想化製品でもあります。

Cisco Nexus 9000v のインストールと展開

Cisco Nexus 9000v は現在、virtio ブロック ディスクをサポートしていません。パフォーマンスを最適化するには、特定のハイパーバイザーで特定の仮想アーティファクトフォーマットを使用することをお勧めします。

ハイパーバイザ	仮想アーティファクト形式
EXSi	オープン仮想アプライアンス（ova） （注） 9.3 (1) Ova 仮想アーティファクトは、ESXI 6.5 バージョンでのみ検証およびサポートされています。
KVM/Qemu	QEMU コピー オン ライト（qcow2）、オープン仮想アプライアンス（ova）
Virtual Box	パッケージ化されたボックス
VMware Fusion	オープン仮想アプライアンス（ova）

Cisco Nexus 9000v シリーズの NX-OS ソフトウェアのアップグレードとダウングレード

Cisco Nexus 9000v のソフトウェアのアップグレードとダウングレードは、通常のハードウェアプラットフォームの手順に従いません。Cisco Nexus 9000v の一般的なアップグレード方法は、新しいイメージをブートフラッシュに tftp または scp で転送し、loader> プロンプトから新しいイメージを起動するか、「config t; boot nxos bootflash:new_image.bin」でブートイメージを設定することです。同様のアプローチがダウングレードにも使用されます。

（注） このアプローチでは、別のイメージを保持するための十分なブートフラッシュディスク領域が必要です。そのため、nxos.7.0.3.I2.2aイメージは新しいリリースにアップグレードできません。この場合、nxosv-final.7.0.3.I2.2d リリースに基づいて新しい VM を作成し、その後で新しいリリースにアップグレードします。

Cisco Nexus 9000v の設定

Cisco Nexus 9000v は、シスコ仮想アプライアンス構成（CVAC）をサポートしています。このアウトオブバンド構成メカニズムは、パワーオン自動プロビジョニング（POAP）自動構成に似ていますが、POAP のようにネットワーク経由で構成をダウンロードする代わりに、CVAC は CD-ROM で Cisco Nexus 9000v 環境に挿入される構成を受け取ります。 この構成は、起動時に検出されて適用されます。

CVAC は、ブートストラップ構成（Telnet、RESTful API、またはその他の標準メカニズムを使用した後続の構成に適した、スイッチを到達可能な状態にするのに十分なだけの構成を提供）または完全構成(別のルーターの構成全体を取得して複製し、新しく起動されたプラットフォーム VM に挿入）に使用できます。構成は、nxos_config.txt というプレーン テキスト ファイルに記載します。次のコマンドを使用して、構成ファイルを CD-ROM にパッケージ化できます。

```
mkisofs -output nxosconfig.iso -l --relaxed-filenames --iso-level 2 <file(s) to add>
```

システムが CVAC 構成を検出しない場合、POAP プロセスが開始され、POAP インターフェイスが初期インストールのプロンプトを表示します。新しく設置されたるスイッチの POAP については、*NX-OS Fundamentals Configuration Guide*を参照してください。

Cisco Cisco Nexus 9000v は、Cisco Nexus 9000 シリーズ ハードウェア プラットフォームでサポートされているものと同じコントロール プレーン機能と設定をサポートします。コントロール プレーン機能の設定コマンドは、Cisco Nexus 9000 シリーズ スイッチと同じ構文に従います。

中断を伴う ISSU を使用した Cisco Nexus 9000v のアップグレード

ISSU（インサービス ソフトウェア アップグレード）は、Cisco Nexus 9000 プラットフォーム スイッチのソフトウェア アップグレード手順です。Cisco Nexus 9000 プラットフォーム スイッチの ISSU 手順には、次の 2 種類があります。

- 高速リロードは ISSU 手順であり、次の手順が実行されます。
  - スイッチは、NX-OS ソフトウェア イメージをロードし、カーネルをアップグレードします。すべてのアプリケーションはステートレス コールド リブートされ、スタートアップ コンフィギュレーションを介して再起動します。
  - コントロール プレーンが中断されます。
  - データ プレーンも中断されます。
- 拡張 ISSU：Cisco Nexus 9000v は、中断を伴う ISSU をサポートします。
  - 中断を伴うアップグレード モード：基本的な拡張 ISSU の基準（たとえば、16G のメモリおよびハード ディスク要件）を満たさない Cisco Nexus 9000 プラットフォーム スイッチは、デフォルトで中断を伴うアップグレード手順を引き続き使用します。新

しいソフトウェア リリースをアクティブ化するには、スイッチを再起動する必要があります。中断を伴う ISSU は、プログラマビリティの観点でのみサポートされます。

- ISSUD（ISSU ダウングレード） は常に中断を伴います。

中断を伴う ISSU の設定

ISSU と ISSUD は同じ手順であり、どちらも中断を伴います。ISSU のアップグレード手順に特別な VM 設定は必要ありません。

中断を伴う ISSU 手順を実行するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show install all impact nxos bootflash:***image***.bin**	実際にアップグレードを実行する前に、ソフトウェアのアップグレードの影響を確認します。
ステップ 2	**show file bootflash:***image***.bin sha256sum**	ファイルの SHA256 チェックサムを表示して、オペレーティング システムの整合性を検証し、ダウンロードしたイメージを安全にインストールし、使用できるかを確認ます。
ステップ 3	show install all status	アップグレード プロセス全体を表示します。
ステップ 4	show version	必要なソフトウェア バージョンがデバイスで実行されていることを確認します。
ステップ 5	**install all nxos bootflash:***image***.bin**	Cisco NX-OS ソフトウェアをアップグレードします。

Cisco Nexus 9000v の展開

分散 OVA を使用した ESXi ハイパーバイザでの Cisco Nexus 9000v のプロビジョニング

始める前に

次の状態を確認してください。

- ESXi ハイパーバイザーをインストールしたこと。
- 配布された OVA ファイルがデスクトップにダウンロードされていること。

手順

ステップ 1 ESXi vCenter にログインします。

ステップ 2 ホストを右クリックして **[OVF テンプレートの展開 (Deploy OVF Template)]** を選択します。

（注） 表示される後続の画面でセルフガイドの指示を実行します。

ステップ 3 **[名前が必要（Need name）]** 画面で、**[ローカル ファイル（Local file）]** を選択し、**[参照（Browse）]** をクリックします。デスクトップからダウンロードした配布 OVA ファイルを選択します。

ステップ 4 **[名前が必要（Need name）]** 画面で、データセンター（またはフォルダ）を選択し、VM 名を入力します。

ステップ 5 **[名前が必要（Need name）]** 画面で、仮想マシンを展開する ESXi サーバーを選択し、検証後に **[完了（Finish）]** をクリックします。

ステップ 6 **[名前が必要（Need name）]** 画面で、詳細を確認し、**[次へ（Next）]** をクリックします。

ステップ 7 **[構成（Configure）]** 画面で、**[次へ（Next）]** をクリックします。

ステップ 8 **[ストレージの選択（Select Storage）]** 画面で、データストアを選択し、**[次へ（Next）]** をクリックします。

ステップ 9 **[ネットワークの選択（Select Networks）]** 画面で、次の値が選択されていることを確認します。

- 送信元ネットワーク名：mgmt 0
- 宛先ネットワーク：ラボ管理 LAN vSwitch

ラボ管理 LAN vSwitch として他の vNIC 宛先が選択されていないことが重要です。そうでないと、Cisco Nexus 9000v データ ポートが物理スイッチと競合するため、管理接続の問題が発生します。

ステップ 10 **[完了の準備（Ready to Complete）]** 画面で、**[完了（Finish）]** をクリックし、プロセスが完了するまで待ちます。

ステップ 11 **[仮想ハードウェア（Virtual Hardware）]** タブで、**[ネットワークの使用（Use Network）]** パネルを選択し、次のオプションを選択します。

- 方向：サーバー
- ポート URL：telent://0.0.0.0:1000。1000 はこのサーバーの一意のポート番号です。

ステップ 12 **[仮想ハードウェア（Virtual Hardware）]** タブで、**[ファームウェア（Firmware）]** パネルを選択し、**[EFI]** を選択します。

ステップ 13 **[仮想ハードウェア（Virtual Hardware）]** タブで、**[詳細（Advance）]** パネルを選択し、**[構成の編集（Edit Configuration）]** 画面で、対応するフィールドに次の値を入力します。

- 名前：efi.serialconsole.enabled
- 列：TRUE

[OK] をクリックします。これにより、VGA とシリアル コンソール モードの両方で起動プロセスを表示できます。

ステップ 14 仮想マシンの電源をオンにします。

ハイパーバイザの KVM または QEMU への Cisco Nexus 9000v の展開

Cisco Nexus 9000v は、KVM または QEMU ハイパーバイザで起動できます。次の表に、KVM または QEMU での Cisco Nexus 9000v 展開でサポートされるパラメータを示します。

パラメータ	例	説明
/path_to/qemu	/usr/bin/qemu-system-x86_64	QEMU の実行可能ファイルへのパス。（QEMU ソフトウェアは、http://wiki.qemu.org/download からさまざまなバージョンをダウンロードできます）。
-nographic	-nographic	推奨。Cisco Nexus 9000v は VGA をサポートしていないからです。

パラメータ	例	説明
-bios file	-bios bios.bin	必須。Cisco Nexus 9000v は EFI ブートを使用するため、動作には互換性のある BIOS イメージが必要です。 ディスク操作のパフォーマンスを向上させるには、SATA コントローラで最新の OVMF BIOS ファイルを使用することをお勧めします。SATA コントローラでは QEMU 2.6 を推奨します。Linux マシンでこの rpm パッケージから bios ファイルを抽出するには、次のコマンドを入力します：`rpm2cpio edk2.git-ovmf-x64-0-20191016.1281.g1bcc65b9a1.noarch.rpm | cpio -idmv` 次のディレクトリにある bios ファイルを探します：./usr/share/edk2.git/ovmf-x64/OVMF-pure-efi.fd
-smp	-smp 4	Cisco Nexus 9000v は 1 ～ 4 個の vCPU をサポートしますが、2 ～ 4 個を推奨します。
-m memory	-m 8096	メモリ（MB）。
-serial telnet:host:port,server,nowait	-serial telnet:localhost:8888,server,nowait または -serial telnet:server_ip:8888,server,nowait	少なくとも 1 つを指定します。

パラメータ	例	説明
-net ... -net ... または -netdev ... -device ...	-net socket,vlan=x,name=n1_s0,listen=localhost:12000 -net nic, vlan=x,model=e1000,macaddr=aaa.bbb.ccc -netdev socket,listen=localhost:12000,id=eth_s_f -device e1000,addr=s.f,netdev=eth_s_f, mac=aaa.bbb.ccc,multifunction=on,romfile= または -netdev tap,ifname=tap_s_f,script=no, downscript=no,id=eth_s_f -device e1000,addr=s.f,netdev=eth_s_f, mac=aaa.bbb.ccc,multifunction=on,romfile=	net/net または netdev/device のペアは、仮想ネットワーク インターフェイス カード（vNIC）をネットワーク化するためのものです。 _s_f は、PCI スロット番号と機能番号を表します。QEMU 2.0 以降には、少なくとも 20 本の PCI スロットと 4 つの機能をプラグインする機能があり、合計で約 80 個の vNIC に対応します。スロットの範囲は 3 ～ 19、機能番号の範囲は 0 ～ 3 です。 mac= オプションは、各 vNIC MAC アドレスの MAC アドレスを VM インターフェイスに渡します。最初の -netdev は、VM の mgmt0 インターフェイスに自動的にマップされます。2 番目の -netdev は e1/1 インターフェースにマップされ、65 番目の e1/64 まで同様にマップされます。これらの MAC アドレスがネットワーク デバイスごとに一意であることを確認してください。
-enable-kvm	-enable-kvm	このフラグは、Cisco Nexus 9000v に必要です。
-drive ... -device ... (SATA コントローラの場合)	-device ahci, id=ahci0,bus=pci.0 -drive file=img.qcow2, if=none,id=drive-sata-disk0, format=qcow2 -device ide-drive, bus=ahci0.0, drive=drive-sata-disk0, id=drive-sata-disk0	SATA コントローラを使用できるようフォーマットします。QEMU 2.6.0 では SATA コントローラを使用することをお勧めします。これは、このコントローラが IDE コントローラよりも優れたパフォーマンスを提供するためです。ただし、SATA コントローラをサポートしていない QEMU の以前のバージョンを使用している場合は、IDE コントローラを使用できます。

パラメータ	例	説明
-drive ... media=cdrom	-drive file=cfg.iso,media=cdrom	Cisco Nexus 9000v の起動後に適用されるスイッチ コンフィギュレーション ファイルを含む CD-ROM ディスク。 1. テキスト ファイルに名前を付けます（nxos_config.txt）。 2. Linux の mkisofs -o cfg.iso -l --iso-level 2 nxos_config.txt コマンドを使用して、cfg.iso を作成します。

KVM または QEMU 環境のネットワーキング

VirtualBox への Cisco Nexus 9000v の展開

VirtualBox への Cisco Nexus 9000v の展開では、Vagrant ソフトウェアとともに事前パッケージ化された Box を使用します。ただし、このボックスは、最小限の構成でシンプルなスタンドアロン VM を展開するために作成されたものです。この手順については、事前にパッケージ化されたボックスを使用した VirtualBox と Vagrant への Cisco Nexus 9000v の展開 （21 ページ）で説明します。

ここでは、他の種類の VM ゲストと同様の仮想マシンを作成するための基本的な手順と概念を示しています。これらの手順は主に Mac ユーザー向けですが、Windows ユーザー向けにはわずかな違いがあり、それらは強調表示されています。

事前にパッケージ化されたボックスを使用した VirtualBox と Vagrant への Cisco Nexus 9000v の展開

Vagrant/vbox の使用に関する次のカスタマイズ ガイドラインと注意事項を参照してください。

- Vagrant ファイルでのユーザーのカスタマイズはもう必要ありません。
- Windows ユーザーの名前付きパイプを変更する必要はありません。シリアル コンソールには、ポート 2023 を使用してアクセスできます。これで、すべてのユーザーが **telnet localhost 2023** コマンドを使用し、ポート 2023 を使用してシリアル コンソールにアクセスできます。
- これで、標準のボックス プロセスを、他の VM ディストリビューションと同様に使用できます。ベース ボックス名を使用して VM を簡単に起動できます。
- ボックス名は、**base** 以外にも、**config.vm.box**フィールドを使用して別の名前に変更できます。
- リリース イメージ ファイルから **.box** で事前に焼き付けられた設定以外の別の設定をスイッチに適用する必要があれば、引き続きブートストラップ設定も可能です。この場合、**vb.customize pre-boot** を使用します。たとえば次のようになります：

```
vb.customize "pre-boot", [
                                "storage attach", :id,
                                "--storagectl", "SATA",
                                "--port", "1",
                                "--device", "0",
                                "--type", "dvddrive",
                                "--medium", "./nxosv_config.iso", ]
```

- VM インターフェイスの MAC アドレスは、**config.vm.base_mac** フィールドを使用してカスタマイズできますが、この変更は、**vagrant up** CLI コマンドを入力する前、および **vagrant init** CLI コマンドを入力した後に行う必要があります。**vagrant up** CLI コマンドの入力後、または VM の作成後に MAC アドレスを変更する場合は、ボックス コマンドを使用して VM を変更する必要があります。

  たとえば、**vboxmanage list vms** CLI コマンドを入力して、**vagrant up** CLI コマンドによって作成された VM を見つけます。

  ```
  vboxmanage list vms
  ```

  以前のコマンドで表示された VM を参照します。たとえば、次の例は、**vboxmanage list vms** コマンドから test_default_1513628849309_59058 が見つかったところです。

  ```
  vboxmanage modifyvm test_default_1513628849309_59058 --macaddress1 080B206CEEAC
  ```

事前にパッケージ化されたボックスを使用し、Vagrant を用いて VirtualBox に Cisco Nexus 9000v を展開するには、次の手順を実行します。

手順

ステップ 1 Mac または PC（GitBash）でターミナルを開き、ディレクトリを作成します。

ステップ 2 リリースされたイメージをこのディレクトリにダウンロードします（たとえば、nexus9000v-final.9.2.1.box）。

ステップ 3 **vagrant init** を実行します。

ステップ 4 **vagrant box add base nxosv-final.9.2.1.box** を実行します。

ステップ 5 現在のディレクトリで **vagrant up** コマンドを使用して VM を起動します。

ステップ 6 起動が完了するまで数分待ちます。次の手順に進みます。

ステップ 7 **vagrant ssh** を実行して Nexus 9000v bash シェルにアクセスし、パスワードとして **vagrant** を入力します。

ステップ 8 **telnet localhost 2023** を使用して、シリアル コンソールから起動プロセスを監視できます。

VM の削除

手順

ステップ 1 VM をシャットダウンします。

```
nexus9000v-user@fe-ucs-dt13:~/n9kv/box-test$ vagrant halt --force box-test ==> box-test:
Forcing shutdown of VM...
nexus9000v-user@fe-ucs-dt13:~/n9kv/box-test$
```

ステップ 2 システムから VM を削除します。

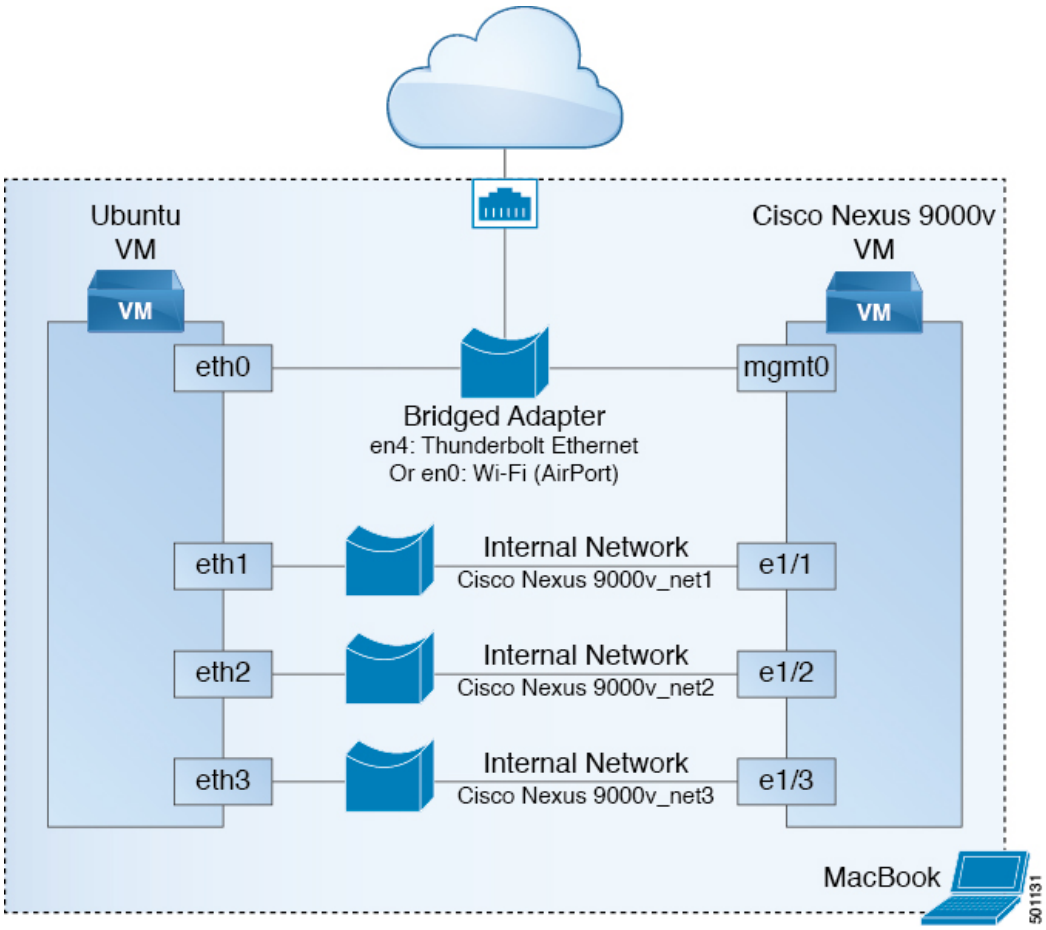
```
nexus9000v-user@fe-ucs-dt13:~/n9kv/box-test$ vagrant destroy box-test
    box-test: Are you sure you want to destroy the 'box-test' VM? [y/N] y
==> box-test: Destroying VM and associated drives...
nexus9000v-user@fe-ucs-dt13:~/n9kv/box-test$
```

ネットワーク トポロジの例

Cisco Nexus 9000v の主な利点は、ハードウェアや複雑なケーブル接続作業を行うことなく、迅速にネットワーク トポロジをセットアップして、Cisco Nexus 9000 スイッチ プラットフォームのルック アンド フィールを獲得できることです。

たとえば、ラップトップ上の Cisco Nexus 9000 仮想マシンに接続するサーバーを備えた 2 ノード システムをすばやくセットアップできます。大規模なリソース サーバーを使用して、より複雑なシステムをセットアップして、複数ノードのシミュレーションを実行することもできます。トポロジを使用すると、実際の顧客ネットワーク環境に適用できるシミュレートされたネットワークで、ツール提供と自動化を実行できます。次の例は、ラップトップまたは UCS サーバーで VM を相互接続する方法を示しています。

ラップトップ上の VirtualBox トポロジ

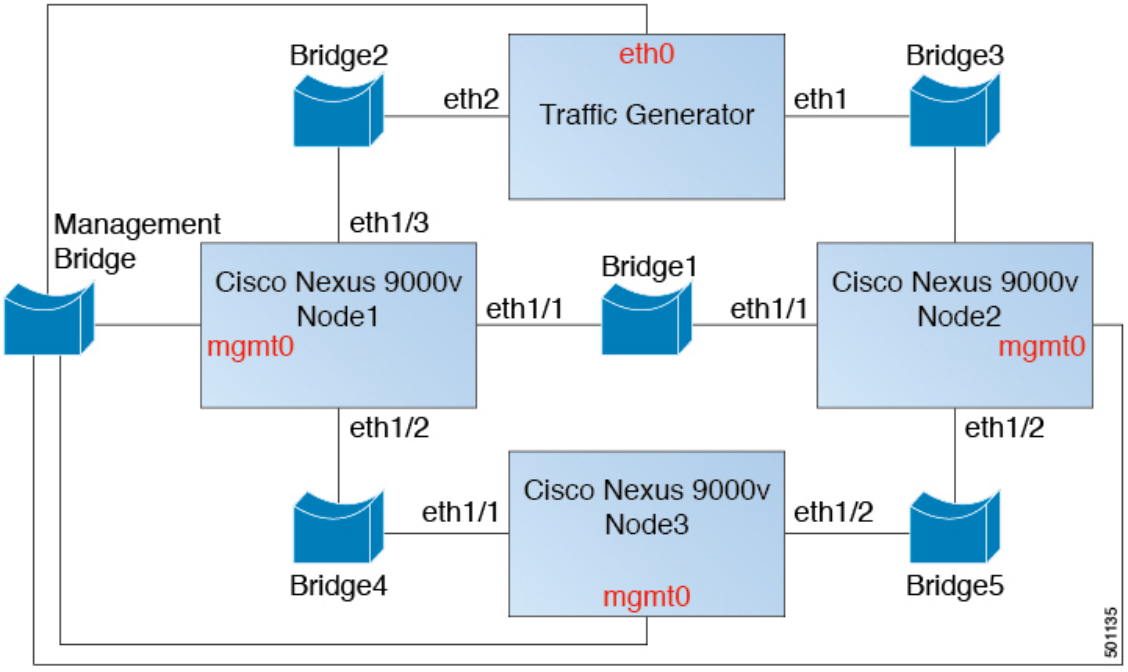


上の図の例は、Cisco Nexus 9000v と Ubuntu VM の 2 ノード システムの一般的な構成です。この場合、Ubuntu VM と Cisco Nexus 9000v の両方にクラウドから到達可能な IP を静的に設定します。または DHCP プロトコルを通して ダイナミックに取得するようにします。同様に、Ubuntu と Cisco Nexus 9000v の両方を管理ネットワーク経由で管理できます。Ubuntu VM は、Cisco Nexus 9000v のデータ ポート、eth1/1、eth1/2、および eth1/3、または ... e1/9 を介し、Cisco Nexus 9000v との間でパケットを送受信できます。

セットアップのための鍵：

- 管理接続のため、ラップトップの物理イーサネット ポートへブリッジまたは NAT 接続
- VM 間のデータ ポートの内部ネットワークで、「無差別モード（Promiscuous Mode）」を「すべて許可（Allow All）」に変更

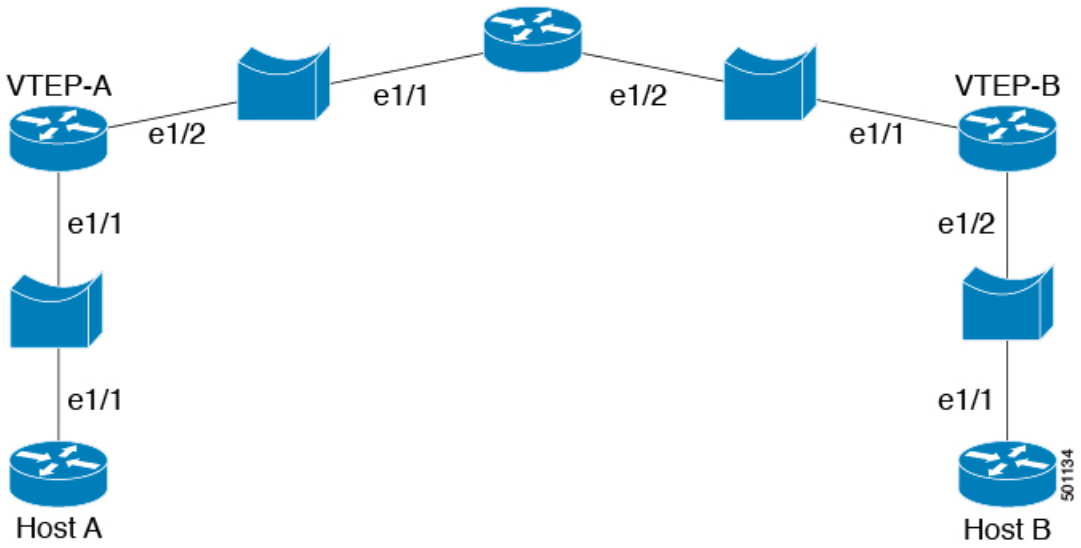
トラフィック ジェネレーターを使用した 3 ノード トポロジ



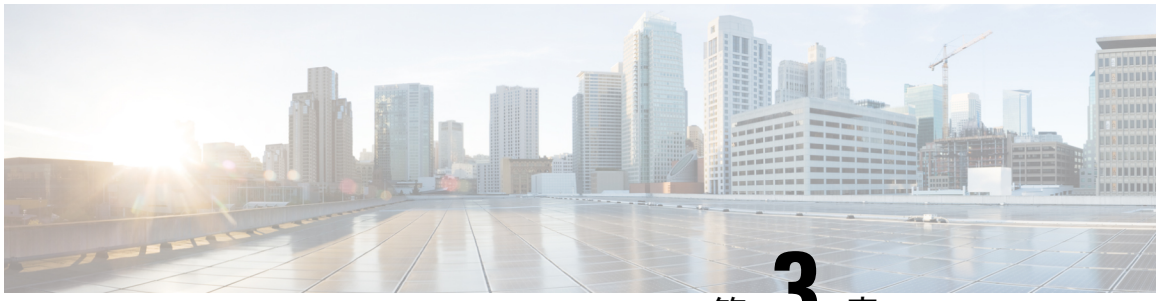
上の図のノードは、ハイパーバイザ固有のマシン定義を使用してインスタンス化されています。ネットワーキングのため、各データ ポート インターフェイスのペアは、一意のブリッジ/vSwitch に接続する必要があります。Cisco Nexus 9000v（mgmt0）のすべての管理ポートは、管理ブリッジに接続し、一意の IP アドレスを提供される必要があります。これにより、外部ネットワークからこれらのデバイスにアクセスできるようになります。

相互接続する必要のある各データ ポート インターフェイス ペアは、同じブリッジ/vSwitch にマッピングする必要があります。VirtualBox トポロジと同様に、vSwitch/Bridge では、ネットワークが Cisco Nexus 9000v ノード間で機能するために、「無差別モード（Promiscuous Mode）」を「受け入れ（Accept）」に設定し、「Vlan ID」を「すべて（All）」に設定する必要があります。データ ポート通信のハイパーバイザ固有の処理については、「トラブルシューティング」のセクションをお読みください。

5 ノード VXLAN トポロジ



このトポロジは、Cisco Nexus 9000v プラットフォームの基本的な vxlan 機能をシミュレートできます。他のトポロジの例に示すように、同様のブリッジ/vSwitch をセットアップする必要があります。



第 3 章

Cisco Nexus 9000v のトラブルシューティング

この章は、次の項で構成されています。

- すべてのハイパーバイザに共通の問題 （27 ページ）
- ESXi ハイパーバイザー （28 ページ）
- KVM または QEMU ハイパーバイザ （31 ページ）
- VirtualBox （31 ページ）
- L2FWDER のトラブルシューティング （32 ページ）
- VM ログの収集 （41 ページ）

すべてのハイパーバイザに共通の問題

VM が「loader >」プロンプトに落ちたときに起動する方法

通常、初回の起動は成功します。ただし、VM のプロビジョニング方法によっては、システムブートが失敗し、VGA コンソールまたはシリアル コンソールに「loader>」プロンプトが表示される場合があります。

例：

```
loader > dir
Setting listing for bootflash:
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Going to print files for device bootflash:
 .rpmstore
 nxos.7.9.3.15.9.66. bin
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Clearing listing for bootflash:
```

```
loader >
```

ブートを続行するには、「loader >」プロンプトで **boot nxos.7.0.3.I5.0.66.bin** コマンドを入力します。

VM が「loader >」プロンプトにドロップしないようにする方法

リロード/シャットダウン後に「loader>」プロンプトにドロップしないようにするには、（POAP インターフェイスのセットアップの後に）Cisco Nexus 9000v をセットアップしたらすぐ、システムでブート イメージを設定する必要があります。

例：

```
config t
  boot nxos n9000-dk9.7.0.3.I2.0.454.bin
copy running starting
```

ESXi ハイパーバイザー

SATA コントローラを使用して Cisco Nexus 9000v の起動プロセスを高速化する方法

Cisco Nexus 9000v は、ハイパーバイザでハードウェア プラットフォームと同じイメージ ブートを使用します。ESXi 5.5 以降のバージョンは、Cisco Nexus 9000v の起動時間を高速化するために使用できる ESXi サーバ上の SATA コントローラをサポートしています。SATA コントローラを備えた VM を作成するには、通常の ESXi VM 作成手順が適用されます。ただし、VM の正常な起動には以下が必要です。

- このサポートにアクセスするには、VMware vSphere Web Client が必要です。
- vmdk イメージを ESXi サーバーにダウンロードします。

  vmkfstools（ESXi サーバーで使用可能なコマンド ライン ツール）を使用して、このモノリス型の vmdk を VMware ネイティブ ディスク タイプに変換します。

  例：

  ```
  vmkfstools -i nexus9000v-final.7.0.3.I5.0.66.vmdk
  nexus9000v-final.7.0.3.I5.0.66-esx.vmdk)
  ```

- ESXi 5.5 (またはそれ以降) および VM バージョン 10 と互換性のある VM を作成します。
- SATA コントローラを追加します。
- SATA コントローラを選択した状態で既存のディスクを追加します。
- ESXi VM の作成手順に従い、VM 起動プロセスを続行します。

シリアル コンソールから「loader >」プロンプトにアクセスする方法

EFI BIOS は、デフォルトで VM コンソールへのすべての入出力を設定します。VM が「loader >」プロンプトにドロップしたら、vSphere クライアントに移動して「loader >」にアクセスして、別のイメージを起動する必要があります。この動作を変更するには、ESXi VM 編集モードで追加の構成を追加します。

次のいずれかの方法を使用できます。

- vSphere クライアントの [構成パラメーター（Configuration Parameters）] ウィンドウで、構成に 1 行追加します（[設定の編集（Edit Settings）] > [VM オプション（VM Options）] > [詳細（Advanced）] > [構成の編集（Edit Configuration）]）。
- VM が作成されたら、.vmx ファイルに **efi.serialconsole.enabled = "TRUE"** を追加します。

EFI シリアル コンソールが有効になっていない場合に ESXi 上のスイッチに接続する方法

ESXi で、VM コンソールを監視しているときに、「Leaving grub land」と表示される場合があります。この後は、何も起きていないように見えますが、通信は設定したシリアル ポートに転送されています。

```
Read length 646737920
Hd5 for size 646737920
    [Initrd, addr-Ox59236000, size=0x268c70000]

segment header
length: 4, vendor: 16 flags: 4, loadaddr: 2500000, image len: 600 memory length
: 600
Reading data for vendor seg . Length 1536

Image length: 651842048 bytes

image hash: d411d638 b48101f6 2e5e7fOb f0130b67
Leaving grub land
```

スイッチに接続するには、ターミナルを開いて、**telnet** <*esxi host*> <*port number*> コマンドを入力する必要があります。

```
rahushen@rtp-ads-15Ø->
rahushen@rtp-ads-15Ø->telnet fe-ucs-dt7 7ØØØ
Trying 1Ø.122.84.213...
Connected to fe-ucs-dt7.
Escape character is '^]'.

User Access Verification
switch login: admin
Password :
Cisco NX-OS Software
Copyright (c) 2ØØ2-2Ø15, Cisco Systems, Inc. All rights reserved.
Cisco Nexus 9000v software ("Cisco Nexus 9000v") and related documentation,
files or other reference materials ("Documentation") are
the proprietary property and confidential information of Cisco
```

```
Systems, Inc. ("Cisco") and are protected, without limitation,
pursuant to United States and International copyright and trademark
laws in the applicable jurisdiction which provide civil and criminal
penalties for copying or distribution without Cisco's authorization.

Any use or disclosure, in whole or in part, of the Cisco Nexus 9000v Software
or Documentation to any third party for any purposes is expressly
prohibited except as otherwise authorized by Cisco in writing.
The copyrights to certain works contained herein are owned by other
third parties and are used and distributed under license. Some parts
of this software may be covered under the GNU Public License or the
GNU Lesser General Public License. A copy of each such license is
available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/Iicenses/lgpl.html
*****************************************************************************
* Cisco Nexus 9000v is strictly limited to use for evaluation, demonstration      *
* and NX-OS education. Cisco Nexus 9000v is provided as-is and is not supported   *
* by Cisco's Technical Advisory Center. Any use or disclosure, in whole  *
* or in part of the Cisco Nexus 9000v Software or Documentation to any third      *
* party for any purposes is expressly prohibited except as otherwise     *
* authorized by Cisco in writing.                                                 *
*****************************************************************************

switch#
```

Cisco Nexus 9000v が起動するとすぐに vCenter または UCS サーバーの接続が失われる

⚠

注意 vNIC を vSwitch またはブリッジに接続する場合、ネットワーク接続が正しくないと、ハイパーバイザー サーバーまたは ESXi 上の vCenter への接続が失われることがあります。

Cisco Nexus 9000v は、ネットワーキングのために KVM/QMEU コマンド ラインまたは ESXi のグラフィカル表現から入力された vNIC ユーザーを、ハイパーバイザ サーバ内の外部または内部でネットワーキングに使用します。最初の NIC は、常に Cisco Nexus 9000v 管理インターフェイスとして使用されます。後続の NIC は、e1/1、e1/2、および e1/9 までのように、データ ポートとして使用されます。

Cisco Nexus 9000v VM の最初の NIC のみを、ラボの LAN 物理スイッチまたはラボの物理スイッチに直接接続する vSwitch (VM ネットワーク) に管理インターフェイスとして接続します (つまり、データ ポート vNIC を物理スイッチに接続して、サーバー管理接続と競合させてはなりません）。

Cisco Nexus 9000v のデータ ポートが ESXi サーバーでトラフィックを渡していない

スムーズな操作を確保するには、vSwitch の特定の構成設定を有効にする必要があります。

1. Cisco Nexus 9000v に接続する vSwitch のすべてのインスタンスが「無差別モード（Promiscuous Mode）」=「受け入れ（Accept）」になっていて、UCS サーバを指している

ことを確認します。このオプションには、vSphere Client から [構成（Configuration）] > [プロパティ（Properties）] > [編集（Edit）] でアクセスできます。

2. vSwitch のすべてのインスタンスがすべての VLAN を通過することを確認します。このオプションには、vSphere Client から [構成（Configuration）] > [プロパティ（Properties）] > [編集（Edit）] でアクセスできます。

KVM または QEMU ハイパーバイザ

KVM または QEMU ハイパーバイザでのマルチキャスト

Cisco Nexus 9000v マルチキャスト機能はブロードキャストとしてサポートされています。この機能を正しく動作させるには、この環境のすべてのブリッジインターフェイスで IGMP マルチキャスト スヌーピングを無効にする必要があります。

次の例は、Linux プロンプトから vxlan_br1、vxlan_br2、vxlan_br3、および vxlan_br4 を無効にする方法を示しています。

```
echo 0 > /sys/devices/virtual/net/vxlan_br1/bridge/multicast_snooping

echo 0 > /sys/devices/virtual/net/vxlan_br2/bridge/multicast_snooping

echo 0 > /sys/devices/virtual/net/vxlan_br3/bridge/multicast_snooping

echo 0 > /sys/devices/virtual/net/vxlan_br4/bridge/multicast_snooping
```

VirtualBox

VirtualBox または Vagrant でのネットワーキング

VirtualBox または Vagrant でデータプレーン インターフェイスを使用するには、次のことを確認してください。

- インターフェイスが「無差別（promiscuous）」モードである必要があります。

  VirtualBox ネットワーク設定で、無差別モードで「すべて許可」を選択します。

- **show interface mac** コマンドを使用して、トポロジ内の Cisco Nexus 9000v のすべてのインスタンスに一意の MAC アドレスがあることを確認します。

VM が VirtualBox/Vagrant で起動できない

次の点を確認します。

- メモリやvCPUなどの十分なリソースが使用可能であることを確認します。PCまたはサーバーで大量のメモリを消費するすべてのアプリケーションを閉じます。使用可能な空きメモリを確認してください。
- VirtualBox GUI に移動し、Vagrant ソフトウェアから作成された対応する VM （Vagrant 構成ファイルで指定されたタグ付きの長い名前）または vmdk から手動で作成された VM をオフにします。
- 「シリアル コンソール」が正しくプロビジョニングされていることを確認します。
- ブロック ディスク タイプをチェックし、SATA コントローラを使用していることを確認します。
- VM をもう一度オンにします。「loader >」プロンプトとともに VGA コンソールが表示されます。「VMが『loader>』プロンプトに落ちたときに起動する方法」のトラブルシューティング トピックに従い、シリアル コンソールから起動プロセスを監視します。

L2FWDER のトラブルシューティング

概要

L2fwder は、Cisco Nexus 9000v の集中型転送コンポーネントであり、次のことを実行します。

- vmnic との間での Rx および Tx パケットの送受信
- L2 スイッチングまたはブリッジング
  - MAC ラーニング
    - パケット パスで学習したダイナミック MAC
    - MTS 通知を介して L2FM から学習した静的 MAC
      - VMAC
      - GW-MAC
  - スイッチング
    - 一連の潜在的なブリッジ ドメインの維持
      - 各ブリッジ ドメインのインターフェイスの追跡
        - 転送状態で
        - STP 状態としてのブロック状態で
    - ブリッジ ドメイン ベースの MAC テーブルの宛先 MAC に基づくパケットのスイッチング

- ユニキャスト トラフィック
- BUM トラフィック

- VXLAN カプセル化解除

- レイヤ 3 処理用のパケットを kstack および netstack にパンティングする
- VXLAN のデキャップ
  - NVE 処理のために最初のパケットを kstack/netstack にパンティングすることによる NVE ピア学習。
  - リモート VTEP インターフェイスに対するリモート MAC の学習。
  - ARP がリモート ホスト ルートを学習する際の、レイヤ 3 ゲートウェイの場合の、ARP パケットの kstack/netstack へのパンティング。
- VXLAN カプセル化
  - netstack およびパケット マネージャによって実行されます。（sup-generated パケットの場合、ハードウェア、つまり Nexus 9000 プラットフォームでの処理に似ています）。
- VXLAN BGP EVPN
  - Cisco Nexus 9000v では、MAC ルートは L2FWDER によって L2FM を置き換えることによって L2RIB に直接生成されますが、HMM は Cisco Nexus 9000v の場合と同様に MAC IP ルートを L2RIB に生成し続けます。

L2FWDER のコマンド

一般的なコマンド	**debug l2fwder** ?	
	err	コントロールおよびデータパス エラー。
	fdb	fdb を介したイベント。
	ha	システムマネージャからのイベント。
	ipc	ipc を介したイベント。
	packet	パケット転送の情報。
	pkttrace	パケット トレース。
	vxlan	VXLAN プラグイン。

clear コマンド	**clear mac address-table datapath dynamic**
	clear mac address-table datapath static

RX/TX パスのトラブルシューティング

- Rx パス

  vmnic からの正常なピックアップを監視して、kstack/netstack へ送信するログ。

```
l2fwder_get_data_with_wrr(515):Packet received over Driver type 0

l2fwder_input(67):In   0x0800 78   0 5254.005b.cf97 -> 5254.004c.4e42 Eth1/4

l2fwder_ethernet_output(196):Driver TUN

l2fwder_action_send_to_stack(865):l2fwder_action_send_to_stack: tx to ifindex 0 iod
 8

l2fwder_ethernet_output(304):l2fwder_ethernet_output: driver_type[2] pktQ count[1]
```

- Tx パス

  tuntap からの正常なピックアップを監視して、kstack/netstack へ送信するログ。

```
l2fwder_get_data_with_wrr(515):Packet received over Driver type 2

l2fwder_ethernet_output(199):Driver ETH

l2fwder_ethernet_output(251):Out  0x0800 78   0 5254.004c.4e42 -> 5254.005b.cf97
Eth1/4

l2fwder_ethernet_output(304):l2fwder_ethernet_output: driver_type[0] pktQ count[1]
```

- 既知のユニキャスト MAC 転送

```
l2fwder_action_process(934):l2fwder_action_process: process action 1

l2fwder_action_tx_unicast(796):l2fwder_action_tx_unicast: tx to ifindex 1a000600 iod
 8  h_type 0

l2fwder_ethernet_output(199):Driver ETH
```

- MAC データベース（FDB）ルックアップに関連していて、正常なルックアップ（BUM トラフィック以外）を記録するログ。

```
l2fwder_get_mac_lookup_fwd_info(857):Lookup Result is * 0xPo200(1) ret is 1
l2fwder_get_mac_lookup_fwd_info(897):action ucast
```

- BUM トラフィックの MAC データベース（FDB）ルックアップ

MAC 学習のトラブルシューティング

- L2FWDER の MAC データベースをチェックするコマンド:

```
switch# show system internal l2fwder mac
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
G   100    5254.004c.4e42    static   -          F     F   sup-eth1(R)
G   200    5254.004c.4e42    static   -          F     F   sup-eth1(R)
*   200    5254.00c5.9daf   dynamic   00:07:45   F     F      Po200
```

- 静的 MAC 学習をチェックするイベント履歴コマンド:

```
Event:E_DEBUG, length:73, at 930108 usecs after Wed Sep 14 04:13:14 2016
    [117] [23935]: Learning SUCCESS for static 1 mac 52:54:00:c5:9d:af bd 200
```

- 動的 MAC 学習のデバッグ ログ チェック：

```
l2fwder_fdb_insert_entry(231):FDB insert for MAC 52:54:00:c5:9d:af bd 200 total
entries 1
```

レイヤ 2/レイヤ 3 トラフィックの l2fwder/pktmgr/netstack でのパケット ドロップのトラブルシューティング

- L2FWDER グローバル カウンタ：

```
switch(config)# show l2fwder statistics
 Decap stats:
                              RX    DROP
                DCE_CORE       0       0
           2 dot1q decap       0       0
           Sub-interface       0       0
              Switchport  140940       0
              Undefined   210758       0
                   Stack  635671       0
           1 dot1q decap       0       0
```

```
                    VXLAN       0       0
              PORT_CHANNEL  105986       0


Encap stats:
                                  TX    DROP
                 DCE_CORE       0       0
           2 dot1q decap        0       0
           Sub-interface        0       0
              Switchport   482493       0
               Undefined   211186       0
                    Stack       0       0
           1 dot1q decap        0       0
                    VXLAN       0       0
             PORT_CHANNEL       0       0


Switching stats:
          Unicast     860
            Flood   29372
        Multicast       0
             Punt   29615
             Drop       0
 LTL Packet Count       0


Punt stats:
      Packets punted 351004


SMM stats:
MAC                 Eth-type   Hit-count
=======================================
    0180.c200.0014    0x0000           0
    0180.c200.0015    0x0000           0
    0100.0cdf.dfdf    0x0000           0
```

```
    ffff.ffff.ffff    0x0806       29078
    0180.c200.0041    0x22f4           0
    0100.0ccc.cccc    0x0000       13963
    0180.c200.0002    0x0000           0
    0180.c200.0003    0x0000           0
    0180.c200.000e    0x0000           0
    0180.c200.0000    0x0000        1652
    0100.0ccc.cccd    0x0000       97087
    0001.0203.0405    0x0000        1604
    0000.0000.0000    0x0000           0


  Dropped          31
  Consumed     115690
  No Action     29070
  lookup fail  206781


RMM stats:
  Dropped         0
  Consumed   205699
  Rate Limit Dropped      0


VACL stats:
sw-bd        VACL           Hit-count
=======================================


  Dropped         0
  Consumed        0
  Copy+Fwd        0
  No Action       0


Port-Channel stats:
 VSL Drop Packets       0
```

```
MAC Learning Disabled stats:

 Packets recieved on Peer-Link:MAC Learning Disabled     313


Action Flood Stats:

 Port-Channel Split-Horizon Packets      48

 VSL Drop Packets                         0


    Forwarding state of ports in bridge domains


switch# show system internal l2fwder bd

Following is the BD State:-

BD_ID  State  Enh_Fwd  Mode

-----  -----  -------  -----

    1      1        0     0

List of all IODs: 9

List of BLK IODs: 8

----------------------------

BD_ID  State  Enh_Fwd  Mode

-----  -----  -------  -----

  100      0        0     0

List of all IODs: 5 7 16

List of BLK IODs: 16
```

VXLAN BGP EVPN のトラブルシューティング

Cisco Nexus 9000v では、L2FWDER はエミュレートされたデータ プレーンであり、送信元の MAC 学習を通じて接続されたホストの MAC 学習を担当します。

（注） BGP EVPN の詳細については、*Cisco 9000 Series NX-OS VXLAN Configuration Guide* を参照してください。

このセクションの例では、次の 2 つの VTEP エンド ポイントを考慮しています。

- VLAN 1001 および 1002 にそれぞれ MAC アドレス 2222.3333.4444、000c.2980.d40a を有するホストを持つ Leaf0（VTEP 1）。
- VLAN 1001 および 1002 にそれぞれ MAC アドレス 000c.29b9.1375、000c.29b9.1375 を有するホストを持つ Leaf1（VTEP 2）。

次の例は、2 つの VTEP エンドポイント間の MAC および MAC IP ルート交換を示しています。

- **Leaf0 のローカル MAC および MAC IP ルート**
  - 送信元 MAC 学習を表示するコマンド：

```
leaf0# show sys int l2fwder mac | inc dynamic
*  1002    000c.2980.d40a   dynamic   01:13:40   F     F     Eth1/2
*  1001    2222.3333.4444   dynamic   00:58:38   F     F     Eth1/2
```

  - L2FWDER は、学習したエンド ホスト MAC を L2RIB テーブルの MAC ルートとして生成します。L2RIB で学習された MAC ルートを表示するコマンド：

```
leaf0# show l2route mac all | inc Local

Flags -(Rmac):Router MAC (Stt):Static (L):Local (R):Remote (V):vPC link
1001        2222.3333.4444 Local  L,            0          Eth1/2
1002        000c.2980.d40a Local  L,            0          Eth1/2
```

  - L2FWDER は mac ルートの生成を担当しますが、MAC IP ルート情報は L2RIB のホスト モビリティ マネージャー（HMM）によって生成されます。L2RIB の MAC IP ルート情報を表示するコマンドは次のとおりです。

```
switch# sh l2route mac-ip all | inc Local
Flags -(Rmac):Router MAC (Stt):Static (L):Local (R):Remote (V):vPC link
1001        2222.3333.4444 HMM    --            0          5.1.1.1        Local

1002        000c.2980.d40a HMM    --            0          5.2.1.1        Local
```

  - MAC IP ルート情報は、L2RIB の Host Mobility Manager（HMM）によって生成されます。MAC IP ルート情報を表示するコマンドは次のとおりです。

```
leaf0# show l2route mac-ip all | inc Local

Flags -(Rmac):Router MAC (Stt):Static (L):Local (R):Remote (V):vPC link
1001        2222.3333.4444 HMM    --            0          5.1.1.1        Local

1002        000c.2980.d40a HMM    --            0          5.2.1.1        Local
```

  - VNI ごとに BGP が学習したローカル MAC および MAC IP ルートを表示するコマンドは次のとおりです。

```
leaft1# show bgp l2vpn evpn vni-id 5001
BGP routing table information for VRF default, address family L2VPN EVPN

BGP table version is 79, local router ID is 6.1.1.1

Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best

Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist,
I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup
*>l[2]:[0]:[0]:[48]:[2222.3333.4444]:[0]:[0.0.0.0]/216
                     6.1.1.1
```

```
                    100      32768 i
*>l[2]:[0]:[0]:[48]:[2222.3333.4444]:[32]:[5.1.1.1]/272
                      6.1.1.1
          100      32768 i
```

- **Leaf1 のリモート MAC および MAC IP ルート**
  - リモート VTEP では、MAC および MAC IP ルート情報が BGP を介して L2RIB に流れ込み、最後に L2FWDER がエンド ホストの MAC 到達可能性情報を受信します。

```
leaft1# show bgp l2vpn evpn vni-id 5001
BGP routing table information for VRF default, address family L2VPN EVPN
BGP table version is 53, local router ID is 6.2.2.2
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-i
njected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup

   Network            Next Hop            Metric     LocPrf        Weight
Path
*>i[2]:[0]:[0]:[48]:[2222.3333.4444]:[0]:[0.0.0.0]/216
                      6.1.1.1
                    100             0 i
*>i[2]:[0]:[0]:[48]:[2222.3333.4444]:[32]:[5.1.1.1]/272
                      6.1.1.1
                    100             0 i

leaf1# show l2route mac all | inc BGP
1001        2222.3333.4444 BGP    SplRcv        0          6.1.1.1
1002        000c.2980.d40a BGP    SplRcv        0          6.1.1.1

eaf1# show l2route mac-ip all | inc BGP
1001        2222.3333.4444 BGP    --            0          5.1.1.1        6.1.1.1
1002        000c.2980.d40a BGP    --            0          5.2.1.1        6.1.1.1

leaf1# show system internal l2fwder mac  | inc nve-peer
*  1002    000c.2980.d40a    static   -          F     F  (0x47000001) nve-peer1
 6.1.1.1
*  1001    2222.3333.4444    static   -          F     F  (0x47000001) nve-peer1
 6.1.1.1
```

VXLAN Encap/Decap のトラブルシューティング

他のセクションで説明されている通常のデータパスデバッグに加えて、以下が追加されます。

NVE ピアのプロビジョニングと学習をチェックする NVE マネージャ コマンド。	**show nve vni**
	show nve peers all
	show ip overlay-traffic

コマンド

カウンター ゲージ コマンド。	**show l2fwder statistics**
	show system internal pktmgr stats
	show ip traffic
データパスのパケットをキャプチャするデバッグ コマンド。	**debug l2fwder** [**packet** | **pktrace** | **error**]
	debug pktmgr [**frame** | **pkt-errors** | **data** | **tunnel**]
	debug ip packet
	tcpdump （注）　（vmnic でデバッグします）。

VM ログの収集

Cisco Nexus 9000v は、物理ハードウェア プラットフォームのすべてのコードを使用します。したがって、ハードウェア プラットフォームから収集されたすべてのロギング ファイルとコア ファイルが Cisco Nexus 9000v システムに適用されます。問題が発生した場合は、VM のスナップショットを作成するか、.vmdk または .qcow2 ファイルのコピーを作成して、さらに分析することをお勧めします。