



## Cisco Catalyst 8000V エッジソフトウェアインストールおよび コンフィギュレーションガイド

最終更新：2025年7月29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/>



## 目次

### Full Cisco Trademarks with Software License ?

---

#### 第 1 章

#### はじめに 1

対象読者および適用範囲 1

機能の互換性 1

表記法 2

通信、サービス、およびその他の情報 3

マニュアルに関するフィードバック 4

トラブルシューティング 4

---

#### 第 2 章

#### Cisco Catalyst 8000V の概要 5

Cisco Catalyst 8000V ルータを使用した仮想化のメリット 6

ルータ インターフェイス 6

Cisco IOS XE および Cisco Catalyst 8000V 7

Cisco Unified Computing System (UCS) 製品 8

---

#### 第 3 章

#### 設置の概要 9

インストール ファイル 9

サポートされるハイパーバイザ 11

インストールファイルのダウンロード 12

注意事項と制約事項 12

次の作業 13

第 4 章	<b>インストールコマンドを使用したソフトウェアのインストール</b>	<b>15</b>
	インストールコマンドを使用したソフトウェアのインストール	15
	インストールコマンドを使用したソフトウェアのインストールに関する制約事項	15
	インストールコマンドを使用したソフトウェアのインストールに関する情報	16
	インストールモードのプロセスフロー	17
	プラットフォームをインストールモードで起動	23
	1 ステップインストールまたはバンドルモードからインストールモードへの変換	24
	3 ステップインストール	25
	インストールモードでのアップグレード	27
	インストールモードでのダウングレード	27
	ソフトウェアインストールの中止	28
	インストールコマンドを使用したソフトウェアインストールの設定例	28
	インストールコマンドを使用したソフトウェアインストールのトラブルシューティング	41
第 5 章	<b>パブリックおよびサブリン IaaS クラウドにおける Cisco Catalyst 8000V の互換性マトリックス</b>	<b>43</b>
	AWS でサポートされるインスタンスタイプ	43
	Microsoft Azure でサポートされるインスタンスタイプ	46
	Google Cloud Platform でサポートされるインスタンスタイプ	50
	Sovereign Cloud でサポートされるインスタンスタイプ	52
第 6 章	<b>VMware ESXi 環境でのインストール</b>	<b>55</b>
	VMware 要件	56
	サポートされている VMware 機能と操作	59
	一般的な機能 (vCenter サーバー)	59
	操作 (vCenter サーバーおよび vSphere Web クライアントの場合)	60
	高可用性	61
	ストレージオプション (vCenter サーバーおよび vSphere Web クライアントの場合)	62
	vSphere を使用した VM への OVA の展開	63
	制限事項および要件	63
	VM への OVA の展開	63

COT を使用した VM への OVA の展開	66
COT のダウンロード	67
COT を使用した Cisco Catalyst 8000V の基本的なプロパティの編集	67
カスタムプロパティの編集	68
cot edit-properties	69
cot inject-config	70
COT を使用した Cisco Catalyst 8000V VM の展開	71
例	72
.iso ファイルを使用した VM の手動作成	73
VMware ESXi 構成でのパフォーマンスの向上	75

---

**第 7 章**

<b>KVM 環境でのインストール</b>	<b>77</b>
KVM のインストール要件	77
KVM インスタンスの作成	80
GUI ツールを使用した VM の作成	80
シリアルコンソールの追加	81
ホスト USB デバイスの追加	81
VM を作成する前の設定のカスタマイズ	82
CLI を使用した VM の作成	83
VM のクローン作成	85
KVM 構成のパフォーマンスの向上	85
halt_poll_ns パラメータの設定	89

---

**第 8 章**

<b>NFVIS 環境でのインストール</b>	<b>91</b>
NFVIS での VM のインストール	93
NFVIS での VM のインストール (リリース 4.5.1 以降)	94
NFVIS 環境での Cisco Catalyst 8000V のインストール	94
NFVIS でのイメージのアップロード	94
ネットワークの作成	95
VM パッケージの作成	95
VM の展開	96

NFVIS での VM のインストール (リリース 4.5.0 以前)	97
NFVIS での仮想マシンの展開	97
NFVIS 用 Cisco Catalyst 8000V イメージのダウンロード	98
NFVIS でのイメージのアップロード	99
Web インターフェイスを使用した VM パッケージの作成	99
ネットワークの作成	100
仮想マシンの監視	101
Cisco ISRV と Cisco Catalyst 8000V の間でのアップグレードとダウングレード	102

---

**第 9 章**

<b>OpenStack 環境へのインストール</b>	<b>105</b>
OpenStack のインストール要件	106
OpenStack へのインストールに関する制約事項	106
OpenStack への Cisco Catalyst 8000V のインストール	106
インスタンスの起動	107
Heat テンプレートを使用した VM のインストール	108

---

**第 10 章**

<b>デイゼロ設定</b>	<b>111</b>
デイゼロ設定の前提条件	113
デイゼロ設定の制約事項	113
ブートストラップメカニズムの選択	113
.txt または .xml ファイルを使用したデイゼロ設定	114
ブートストラップ ファイルの作成	114
ブートストラップのプロパティ	115
iosxe_config.txt ファイルの例	117
ovf-env.xml ファイルの例	117
OVF テンプレートのデイゼロ設定	119
config-drive を使用したデイゼロ設定	119
カスタムデータを使用したデイゼロ設定	120
デイゼロ ブートストラップ ファイルの編集	120
IOS 設定プロパティの設定	121
スクリプトプロパティの設定	121

スクリプトログイン情報プロパティの設定	122
Python パッケージプロパティの設定	123
ライセンスプロパティの設定	124
デイゼロ ブートストラップ ファイルの提供	125
カスタムデータ設定の確認 (Microsoft Azure)	125
カスタムデータ設定の確認 (Google Cloud Platform)	129
コントローラモードでのデイゼロ設定	129
ルータの動作モードとデイゼロ設定の確認	130
よく寄せられる質問	131

---

**第 11 章****Security-Enhanced Linux のサポート 133**

概要	133
SELinux の前提条件	133
SELinux の制限事項	133
SELinux に関する情報	134
SELinux の設定	134
SELinux の設定 (EXEC モード)	134
SELinux の設定 (CONFIG モード)	135
SELinux の例	135
Syslog メッセージリファレンス	135
SELinux の有効化の確認	136
SELinux のトラブルシューティング	137

---

**第 12 章****Cisco Catalyst 8000V ネットワーク インターフェイスの VM ネットワーク インターフェイスへのマッピング 139**

サポートされるネットワーク インターフェイスの速度	139
ルータ ネットワーク インターフェイスの vNIC へのマッピング	140
Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除	141
実行中の VM からの vNIC の削除	142
Cisco Catalyst 8000V ネットワーク インターフェイスと VM の複製	142

Cisco Catalyst 8000V ネットワーク インターフェイスと vSwitch インターフェイスのマッピング 143

第 13 章 VNF セキュアブートの有効化 145

第 14 章 コンソールアクセスの設定 149

Cisco Catalyst 8000V を VM として起動 149

Cisco Catalyst 8000V コンソールへのアクセス 151

仮想 VGA コンソールからの Cisco Catalyst 8000V へのアクセス 151

仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセス 151

仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセスの概要 151

VMware ESXi でのシリアルコンソールアクセスの作成 151

KVM でのシリアルコンソールアクセスの作成 152

仮想シリアルポートでの Cisco Catalyst 8000V コンソールへの Telnet セッションの開始  
153

インストール後のコンソールポートアクセスの変更 154

第 15 章 Cisco Catalyst 8000V ハードウェアと VM の要件の確認 157

第 16 章 Cisco IOS XE ソフトウェアのアップグレード 159

Cisco Catalyst 8000V のアップグレードのための前提条件 160

Cisco CSR1000V および Cisco ISRV アップグレードの HSECK9 ライセンス要件 161

Cisco Catalyst 8000V のアップグレードの制約事項 161

インストールモードのプロセスフロー 163

Cisco Catalyst 8000V をインストールモードで起動する場合 168

1 ステップインストールまたはバンドルモードからインストールモードへの変換 168

3 ステップインストール 170

リリース 17.06.02 からリリース 17.07.01 へのアップグレード出力の例 172

インストールモードでのアップグレード 174

インストールモードでのダウングレード 174

ソフトウェアインストールの中止 175

インストールコマンドを使用したソフトウェアインストールのトラブルシューティング	176
よく寄せられる質問	177

---

**第 17 章****vCPU 分散の設定 179**

vCPU 分散：コントロールプレーン超高	179
vCPU 分散：コントロールプレーン高	180
vCPU 分散：データプレーン高	180
vCPU 分散：データプレーン並	181
vCPU 分散：サービスプレーン高	181
vCPU 分散：サービスプレーン中	182
データプレーン、コントロールプレーン、サービスプレーン全般にわたる vCPU 分散の設定	182
アクティブ vCPU 分散テンプレートの決定	183

---

**第 18 章****Web ユーザ インターフェイス管理 185**

Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定	185
基本または詳細モードセットアップ ウィザードの使用	186
LAN 設定を行います。	187
プライマリ WAN 設定を行います。	188
セカンダリ WAN 設定を行います。	189
セキュリティ設定の構成	190

---

**第 19 章****GRUB モードへのアクセスと使用 191**

GRUB モードへのアクセス	192
GRUB メニューの使用	193
GRUB モードの開始とイメージの選択	193
コンフィギュレーションレジスタ (confreg) の変更	195
コンフィギュレーションレジスタ設定の変更	197
コンフィギュレーションレジスタの設定の表示	198

---

**第 20 章****工場出荷時の状態へのリセット 199**

初期設定へのリセットに関する情報	199
初期設定へのリセット実行の前提条件	200
初期設定へのリセット実行の制限事項	200
初期設定へのリセットの実行方法	201
初期設定へのリセット後におけるスマートライセンスの復元	201
初期設定へのリセット後の動作	203

---

**第 21 章**
**VRF ルート共有の設定 205**

VRF ルート共有に関する情報	205
VRF ルート共有の前提条件	206
VRF ルート共有に関する制約事項	206
VRF ルート共有の設定方法	206
サンプルトポロジと使用例	206
VRF ルート共有の設定	209
VRF ルート共有の確認	210

---

**第 22 章**
**ブリッジドメイン インターフェイスの設定 211**

ブリッジドメイン インターフェイスの制約事項	211
ブリッジドメイン インターフェイスに関する情報	212
イーサネット仮想回線の概要	213
ブリッジドメイン インターフェイスのカプセル化	213
MAC アドレスの割り当て	214
IP プロトコルのサポート	214
IP 転送のサポート	214
パケット転送	215
レイヤ 2 から 3	215
レイヤ 3 からレイヤ 2	215
ブリッジドメインとブリッジドメイン インターフェイスのステートをリンクする	215
BDI の初期状態	216
BDI のリンク状態	216
ブリッジドメイン インターフェイスの統計情報	216

ブリッジドメインインターフェイスの作成または削除	217
ブリッジドメインインターフェイスのスケラビリティ	217
ブリッジドメイン仮想 IP インターフェイス	217
ブリッジドメインインターフェイスの設定方法	218
例	220
ブリッジドメインインターフェイス設定の表示と確認	220
ブリッジドメイン仮想 IP インターフェイスの設定	222
VIF インターフェイスのブリッジドメインへの関連付け	222
ブリッジドメイン仮想 IP インターフェイスの確認	222
ブリッジドメイン仮想 IP インターフェイスの設定例	222
ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow の設定	223
例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow	224
その他の参考資料	228
ブリッジドメインインターフェイスの機能情報	229

---

**第 23 章**

<b>MTP ソフトウェアサポートの設定</b>	<b>231</b>
利点	231
ソフトウェア MTP のサポートを設定するための前提条件	231
SRTP-DTMF インターワーキング	232
SRTP-DTMF インターワーキングの制約事項	232
サポートされる SRTP-DTMF インターワーキングのプラットフォーム	232
ソフトウェア MTP のサポートの設定	232
ソフトウェア MTP サポートの設定例	236
ソフトウェア MTP サポートの確認	237

---

**第 24 章**

<b>無線対応ルーティング</b>	<b>241</b>
無線対応ルーティングの利点	241
制約事項と制限	242
パフォーマンス	242
システム コンポーネント	242
PPPoE 拡張セッションでの QoS プロビジョニング	243

例：バイパスモードでの RAR 機能の設定 244

RAR セッションの詳細の確認 245





## 目次

### Full Cisco Trademarks with Software License ?

---

#### 第 1 章

#### はじめに 1

対象読者および適用範囲 1

機能の互換性 1

表記法 2

通信、サービス、およびその他の情報 3

マニュアルに関するフィードバック 4

トラブルシューティング 4

---

#### 第 2 章

#### Cisco Catalyst 8000V の概要 5

Cisco Catalyst 8000V ルータを使用した仮想化のメリット 6

ルータ インターフェイス 6

Cisco IOS XE および Cisco Catalyst 8000V 7

Cisco Unified Computing System (UCS) 製品 8

---

#### 第 3 章

#### 設置の概要 9

インストールファイル 9

サポートされるハイパーバイザ 11

インストールファイルのダウンロード 12

注意事項と制約事項 12

次の作業 13

---

#### 第 4 章

#### インストールコマンドを使用したソフトウェアのインストール 15

インストールコマンドを使用したソフトウェアのインストール	15
インストールコマンドを使用したソフトウェアのインストールに関する制約事項	15
インストールコマンドを使用したソフトウェアのインストールに関する情報	16
インストールモードのプロセスフロー	17
プラットフォームをインストールモードで起動	23
1 ステップインストールまたはバンドルモードからインストールモードへの変換	24
3 ステップインストール	25
インストールモードでのアップグレード	27
インストールモードでのダウングレード	27
ソフトウェアインストールの中止	28
インストールコマンドを使用したソフトウェアインストールの設定例	28
インストールコマンドを使用したソフトウェアインストールのトラブルシューティング	41
<hr/>	
第 5 章	<b>パブリックおよびソブリン IaaS クラウドにおける Cisco Catalyst 8000V の互換性マトリックス</b> 43
	AWS でサポートされるインスタンスタイプ 43
	Microsoft Azure でサポートされるインスタンスタイプ 46
	Google Cloud Platform でサポートされるインスタンスタイプ 50
	Sovereign Cloud でサポートされるインスタンスタイプ 52
<hr/>	
第 6 章	<b>VMware ESXi 環境でのインストール</b> 55
	VMware 要件 56
	サポートされている VMware 機能と操作 59
	一般的な機能 (vCenter サーバー) 59
	操作 (vCenter サーバーおよび vSphere Web クライアントの場合) 60
	高可用性 61
	ストレージオプション (vCenter サーバーおよび vSphere Web クライアントの場合) 62
	vSphere を使用した VM への OVA の展開 63
	制限事項および要件 63
	VM への OVA の展開 63
	COT を使用した VM への OVA の展開 66
	COT のダウンロード 67

COT を使用した Cisco Catalyst 8000V の基本的なプロパティの編集	67
カスタムプロパティの編集	68
cot edit-properties	69
cot inject-config	70
COT を使用した Cisco Catalyst 8000V VM の展開	71
例	72
.iso ファイルを使用した VM の手動作成	73
VMware ESXi 構成でのパフォーマンスの向上	75

---

## 第 7 章

<b>KVM 環境でのインストール</b>	<b>77</b>
KVM のインストール要件	77
KVM インスタンスの作成	80
GUI ツールを使用した VM の作成	80
シリアルコンソールの追加	81
ホスト USB デバイスの追加	81
VM を作成する前の設定のカスタマイズ	82
CLI を使用した VM の作成	83
VM のクローン作成	85
KVM 構成のパフォーマンスの向上	85
halt_poll_ns パラメータの設定	89

---

## 第 8 章

<b>NFVIS 環境でのインストール</b>	<b>91</b>
NFVIS での VM のインストール	93
NFVIS での VM のインストール (リリース 4.5.1 以降)	94
NFVIS 環境での Cisco Catalyst 8000V のインストール	94
NFVIS でのイメージのアップロード	94
ネットワークの作成	95
VM パッケージの作成	95
VM の展開	96
NFVIS での VM のインストール (リリース 4.5.0 以前)	97
NFVIS での仮想マシンの展開	97

NFVIS 用 Cisco Catalyst 8000V イメージのダウンロード	98
NFVIS でのイメージのアップロード	99
Web インターフェイスを使用した VM パッケージの作成	99
ネットワークの作成	100
仮想マシンの監視	101
Cisco ISRV と Cisco Catalyst 8000V の間でのアップグレードとダウングレード	102

---

**第 9 章**

<b>OpenStack 環境へのインストール</b>	<b>105</b>
OpenStack のインストール要件	106
OpenStack へのインストールに関する制約事項	106
OpenStack への Cisco Catalyst 8000V のインストール	106
インスタンスの起動	107
Heat テンプレートを使用した VM のインストール	108

---

**第 10 章**

<b>デイゼロ設定</b>	<b>111</b>
デイゼロ設定の前提条件	113
デイゼロ設定の制約事項	113
ブートストラップメカニズムの選択	113
.txt または .xml ファイルを使用したデイゼロ設定	114
ブートストラップ ファイルの作成	114
ブートストラップのプロパティ	115
iosxe_config.txt ファイルの例	117
ovf-env.xml ファイルの例	117
OVF テンプレートのデイゼロ設定	119
config-drive を使用したデイゼロ設定	119
カスタムデータを使用したデイゼロ設定	120
デイゼロ ブートストラップ ファイルの編集	120
IOS 設定プロパティの設定	121
スクリプトプロパティの設定	121
スクリプトログイン情報プロパティの設定	122
Python パッケージプロパティの設定	123

ライセンスプロパティの設定	124
デイゼロ ブートストラップ ファイルの提供	125
カスタムデータ設定の確認 (Microsoft Azure)	125
カスタムデータ設定の確認 (Google Cloud Platform)	129
コントローラモードでのデイゼロ設定	129
ルータの動作モードとデイゼロ設定の確認	130
よく寄せられる質問	131

---

 第 11 章

**Security-Enhanced Linux のサポート 133**

概要	133
SELinux の前提条件	133
SELinux の制限事項	133
SELinux に関する情報	134
SELinux の設定	134
SELinux の設定 (EXEC モード)	134
SELinux の設定 (CONFIG モード)	135
SELinux の例	135
Syslog メッセージリファレンス	135
SELinux の有効化の確認	136
SELinux のトラブルシューティング	137

---

 第 12 章

**Cisco Catalyst 8000V ネットワーク インターフェイスの VM ネットワーク インターフェイスへのマッピング 139**

サポートされるネットワーク インターフェイスの速度	139
ルータ ネットワーク インターフェイスの vNIC へのマッピング	140
Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除	141
実行中の VM からの vNIC の削除	142
Cisco Catalyst 8000V ネットワーク インターフェイスと VM の複製	142
Cisco Catalyst 8000V ネットワーク インターフェイスと vSwitch インターフェイスのマッピング	143

---

第 13 章	<b>VNF セキュアブートの有効化</b>	<b>145</b>
--------	------------------------	------------

---

第 14 章	<b>コンソールアクセスの設定</b>	<b>149</b>
	Cisco Catalyst 8000V を VM として起動	149
	Cisco Catalyst 8000V コンソールへのアクセス	151
	仮想 VGA コンソールからの Cisco Catalyst 8000V へのアクセス	151
	仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセス	151
	仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセスの概要	151
	VMware ESXi でのシリアルコンソールアクセスの作成	151
	KVM でのシリアルコンソールアクセスの作成	152
	仮想シリアルポートでの Cisco Catalyst 8000V コンソールへの Telnet セッションの開始	153
	インストール後のコンソールポートアクセスの変更	154

---

第 15 章	<b>Cisco Catalyst 8000V ハードウェアと VM の要件の確認</b>	<b>157</b>
--------	---	------------

---

第 16 章	<b>Cisco IOS XE ソフトウェアのアップグレード</b>	<b>159</b>
	Cisco Catalyst 8000V のアップグレードのための前提条件	160
	Cisco CSR1000V および Cisco ISRV アップグレードの HSECK9 ライセンス要件	161
	Cisco Catalyst 8000V のアップグレードの制約事項	161
	インストールモードのプロセスフロー	163
	Cisco Catalyst 8000V をインストールモードで起動する場合	168
	1 ステップインストールまたはバンドルモードからインストールモードへの変換	168
	3 ステップインストール	170
	リリース 17.06.02 からリリース 17.07.01 へのアップグレード出力の例	172
	インストールモードでのアップグレード	174
	インストールモードでのダウングレード	174
	ソフトウェアインストールの中止	175
	インストールコマンドを使用したソフトウェアインストールのトラブルシューティング	176
	よく寄せられる質問	177

---

**第 17 章****vCPU 分散の設定 179**

vCPU 分散：コントロールプレーン超 高 179

vCPU 分散：コントロールプレーン高 180

vCPU 分散：データプレーン高 180

vCPU 分散：データプレーン並 181

vCPU 分散：サービスプレーン高 181

vCPU 分散：サービスプレーン中 182

データプレーン、コントロールプレーン、サービスプレーン全般にわたる vCPU 分散の設定  
182

アクティブ vCPU 分散テンプレートの決定 183

---

**第 18 章****Web ユーザーインターフェイス管理 185**

Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定 185

基本または詳細モードセットアップ ウィザードの使用 186

LAN 設定を行います。 187

プライマリ WAN 設定を行います。 188

セカンダリ WAN 設定を行います。 189

セキュリティ設定の構成 190

---

**第 19 章****GRUB モードへのアクセスと使用 191**

GRUB モードへのアクセス 192

GRUB メニューの使用 193

GRUB モードの開始とイメージの選択 193

コンフィギュレーションレジスタ (confreg) の変更 195

コンフィギュレーションレジスタ設定の変更 197

コンフィギュレーションレジスタの設定の表示 198

---

**第 20 章****工場出荷時の状態へのリセット 199**

初期設定へのリセットに関する情報 199

初期設定へのリセット実行の前提条件 200

初期設定へのリセット実行の制限事項	200
初期設定へのリセットの実行方法	201
初期設定へのリセット後におけるスマートライセンスの復元	201
初期設定へのリセット後の動作	203

---

**第 21 章**

<b>VRF ルート共有の設定</b>	<b>205</b>
VRF ルート共有に関する情報	205
VRF ルート共有の前提条件	206
VRF ルート共有に関する制約事項	206
VRF ルート共有の設定方法	206
サンプルトポロジと使用例	206
VRF ルート共有の設定	209
VRF ルート共有の確認	210

---

**第 22 章**

<b>ブリッジドメインインターフェイスの設定</b>	<b>211</b>
ブリッジドメインインターフェイスの制約事項	211
ブリッジドメインインターフェイスに関する情報	212
イーサネット仮想回線の概要	213
ブリッジドメインインターフェイスのカプセル化	213
MAC アドレスの割り当て	214
IP プロトコルのサポート	214
IP 転送のサポート	214
パケット転送	215
レイヤ 2 から 3	215
レイヤ 3 からレイヤ 2	215
ブリッジドメインとブリッジドメインインターフェイスのステートをリンクする	215
BDI の初期状態	216
BDI のリンク状態	216
ブリッジドメインインターフェイスの統計情報	216
ブリッジドメインインターフェイスの作成または削除	217
ブリッジドメインインターフェイスのスケラビリティ	217

ブリッジドメイン仮想 IP インターフェイス	217
ブリッジドメインインターフェイスの設定方法	218
例	220
ブリッジドメインインターフェイス設定の表示と確認	220
ブリッジドメイン仮想 IP インターフェイスの設定	222
VIF インターフェイスのブリッジドメインへの関連付け	222
ブリッジドメイン仮想 IP インターフェイスの確認	222
ブリッジドメイン仮想 IP インターフェイスの設定例	222
ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow の設定	223
例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow	224
その他の参考資料	228
ブリッジドメインインターフェイスの機能情報	229

---

 第 23 章

<b>MTP ソフトウェアサポートの設定</b>	<b>231</b>
利点	231
ソフトウェア MTP のサポートを設定するための前提条件	231
SRTP-DTMF インターワーキング	232
SRTP-DTMF インターワーキングの制約事項	232
サポートされる SRTP-DTMF インターワーキングのプラットフォーム	232
ソフトウェア MTP のサポートの設定	232
ソフトウェア MTP サポートの設定例	236
ソフトウェア MTP サポートの確認	237

---

 第 24 章

<b>無線対応ルーティング</b>	<b>241</b>
無線対応ルーティングの利点	241
制約事項と制限	242
パフォーマンス	242
システム コンポーネント	242
PPPoE 拡張セッションでの QoS プロビジョニング	243
例：バイパスモードでの RAR 機能の設定	244
RAR セッションの詳細の確認	245



【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/](http://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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2020–2024 Cisco Systems, Inc. All rights reserved.





# 第 1 章

## はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

- [対象読者および適用範囲 \(1 ページ\)](#)
- [機能の互換性 \(1 ページ\)](#)
- [表記法 \(2 ページ\)](#)
- [通信、サービス、およびその他の情報 \(3 ページ\)](#)
- [マニュアルに関するフィードバック \(4 ページ\)](#)
- [トラブルシューティング \(4 ページ\)](#)

## 対象読者および適用範囲

このドキュメントは、Cisco Enterprise ルータの設定担当者を対象としています。このドキュメントの対象者は、主に次のとおりです。

- ネットワーキングに関する技術的な背景知識と経験を持つお客様。
- ルータベースのインターネットワーキングに関する基本的な知識に精通しているが、Cisco IOS ソフトウェアについては経験の浅いシステム管理者。
- インターネットワーキング装置のインストールと設定を担当しているシステム管理者、および Cisco IOS ソフトウェアに精通しているシステム管理者。

## 機能の互換性

コンフィギュレーションガイドで説明されているデバイスで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、それぞれのルータのドキュメントセットを参照してください。

特定の機能のサポートを確認するには、[Cisco Feature Navigator](#) ツールを使用します。これは、特定のソフトウェアリリース、フィーチャセット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェアイメージを判別できるツールです。

## 表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または <b>Ctrl</b>	^ および <b>Ctrl</b> シンボルは、Ctrl キーを表します。たとえば、 <b>^D</b> または <b>Ctrl+D</b> というキーの組み合わせは、 <b>Ctrl</b> キーを押しながら <b>D</b> キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
<i>string</i>	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティストリングとして <b>public</b> を設定する場合、ストリング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ストリングとみなされます。

コマンドシンタックスの説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	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。
	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1つを選択します。
[x   y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x   y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。たとえば、次の表を参照してください。

表記法	説明
[x {y z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

表記法	説明
screen	画面に表示される情報の例は、Courier フォントで表します。
<b>bold screen</b>	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
<>	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符 (!) は、コメント行を表します。また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります。
[]	角カッコは、システム プロンプトに対するデフォルトの応答です。



**注意** 「要注意」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。



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

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、[Cisco Services](#) [英語] にアクセスしてください。

- サービスリクエストを送信するには、[Cisco Support \[英語\]](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet \[英語\]](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press \[英語\]](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探するには、[Cisco Warranty Finder](#) にアクセスしてください。

### シスコバグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

## マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

## トラブルシューティング

トラブルシューティングの最新の詳細情報については、[https://www.cisco.com/c/ja\\_jp/support/index.html](https://www.cisco.com/c/ja_jp/support/index.html) にある Cisco TAC Web サイトを参照してください。

**製品カテゴリ**に移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、**トラブルシュート**および**アラート**を参照してください。



## 第 2 章

# Cisco Catalyst 8000V の概要

Cisco Catalyst 8000V エッジソフトウェアは、x86 サーバーハードウェアで実行されている仮想マシン（VM）に導入された仮想のフォームファクタルータです。このガイドでは、Cisco Catalyst 8000V の概要、インストール、アップグレード、および設定について説明します。

Cisco Catalyst 8000V は、それぞれ自律モードとコントローラモードを介して Cisco IOS XE と Cisco IOS XE SD-WAN の両方の機能をサポートします。Cisco Catalyst 8000V は、自律モードでは Cisco IOS XE ソフトウェアの機能とテクノロジーのサブセットをサポートし、仮想化プラットフォームで Cisco IOS XE セキュリティとスイッチング機能を提供します。コントローラモードでは、仮想環境とクラウド環境で包括的な SD-WAN、WAN ゲートウェイ、およびネットワークサービス機能を提供します。

VM 上に Cisco Catalyst 8000V を展開した場合、Cisco IOS XE ソフトウェアは、あたかも従来のシスコのハードウェアプラットフォーム上に展開されているかのように機能します。このルータには、アーキテクチャの一部として仮想ルートプロセッサと仮想フォワーディングプロセッサ（FP）が含まれており、ブランチオフィスやデータセンターなどの企業ロケーションからパブリッククラウドまたはプライベートクラウドへのセキュアな接続を提供します。

Cisco Catalyst 8000V は SSL VPN をサポートしています。Cisco IOS XE リリース 17.x 以降では、Cisco IOS-XE ルータを SSL VPN ゲートウェイとして実行している場合、TLS カプセル化により、余分な SSL VPN オーバーヘッドが追加されます。SSL VPN クライアントとサーバー間のパケットの IP フラグメンテーションとリアセンブルを防ぐには、TCP-MSS 値を最適に調整する必要があります。そうしないと、SSL VPN ゲートウェイで IPFragErr エラーによるパケットドロップが発生する可能性があります。

Cisco Catalyst 8000V ルータは、Enterprise Network Compute System（ENCS）プラットフォームおよび Cisco Cloud Services Platform 5000 シリーズでのルーティングおよび転送用の仮想 IOS XE オペレーティングシステムも提供します。

この仮想ルータの機能を使用するには、Cisco Catalyst 8000V ルータをハイパーバイザ上の仮想マシンとして展開する方法を確認してください。

- [Cisco Catalyst 8000V ルータを使用した仮想化のメリット](#)（6 ページ）
- [ルータ インターフェイス](#)（6 ページ）
- [Cisco IOS XE および Cisco Catalyst 8000V](#)（7 ページ）
- [Cisco Unified Computing System（UCS）製品](#)（8 ページ）

## Cisco Catalyst 8000V ルータを使用した仮想化のメリット

- **ハードウェアの独立性**：Cisco Catalyst 8000V ルータは、クラウドの仮想化の利点を活用してハードウェアの独立性を提供します。Cisco Catalyst 8000V は仮想マシン上で動作するため、仮想化プラットフォームでサポートされている任意の x86 ハードウェアでこのルータを使用できます。
- **リソースの共有**：Cisco Catalyst 8000V 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、これらのリソースは VM 間で共有できます。VM サーバーが特定の VM に割り当てるハードウェアリソースの量を調整できます。サーバー上の別の VM にリソースを再割り当てできます。
- **展開の柔軟性**：サーバー間で容易に VM を移動できます。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 Catalyst 8000V インスタンスを移動できます。
- **強化されたソフトウェアセキュリティ - セキュアなオブジェクトストア**：Cisco Catalyst 8000V では、NVRAM、ライセンス、およびその他のデータのストレージパーティションがオブジェクトストアとして作成されます。個々のオブジェクトストアはデータのセキュリティを確保するために暗号化されており、この製品は Cisco Secure Development ライフサイクル (CSDL) に準拠しています。さらに、Cisco Catalyst 8000V は 16G ディスクプロファイルをサポートします。

## ルータ インターフェイス

Cisco Catalyst 8000V ルータインターフェイスはハードウェアベースのシスコルータと同じ機能を実行します。Cisco Catalyst 8000V インターフェイスは次のように機能します。

- インターフェイスは、論理的にギガビットイーサネット (GE) インターフェイスと呼ばれます。
- 使用可能なインターフェイスの番号付けは、Cisco Catalyst 8000V バージョンによって異なります。

デバイスを初めて起動すると、Cisco Catalyst 8000V ルータインターフェイスは、Cisco Catalyst 8000V への vNIC 列挙に基づいて VM 上の vNIC インターフェイスにマッピングされます。次回起動時に、Cisco Catalyst 8000V ルータインターフェイスが vNIC MAC アドレスにマッピングされます。

詳細については、「[Cisco Catalyst 8000V Network Interfaces to the VM Network Interfaces](#)」を参照してください。

### インターフェイスの番号付け

- インターフェイスポートの番号付けは、1 からサポートされるインターフェイスの数までです。サポートされる vNIC と、各 VM インスタンスでサポートされる vNIC の最小数および最大数については、[VMware 要件 \(56 ページ\)](#) を参照してください。
- ギガビットイーサネット インターフェイス 0 はサポートされていません。
- 任意のインターフェイスを管理インターフェイスとして指定できます。ターゲット環境で使用可能な適切な Day0 ブートストラップメカニズムを実行することで、管理インターフェイスを指定できます。詳細については、[デイゼロ設定 \(111 ページ\)](#) を参照してください。

## Cisco IOS XE および Cisco Catalyst 8000V

Cisco Catalyst 8000V は、Cisco IOS XE および Cisco IOS XE SD-WAN で動作する仮想ルータです。このガイドでは、Cisco IOS XE での Cisco Catalyst 8000V の概要、インストール、および設定情報について説明します。

次の方法で Cisco Catalyst 8000V を設定および管理できます。

- VM にシリアルポートをプロビジョニングして接続し、Cisco IOS XE CLI コマンドにアクセスします。



---

(注) 基盤となるハイパーバイザが VM とシリアルポートの関連付けをサポートしている場合のみ、シリアルポートを使用して Cisco Catalyst 8000V VM を管理できます。詳細については、ハイパーバイザのドキュメンテーションを参照してください。

---

- Cisco IOS XE CLI コマンドにアクセスするには、リモート SSH または Telnet を使用します。



---

(注) デフォルトでは、Telnet はセキュリティ上の理由から無効になっています。SSH は、オンプレミス展開では無効になっています。リモートユーザー管理には SSH が推奨されますが、オンプレミス展開では SSH を手動で有効にする必要があります。

クラウド展開では、SSH はデフォルトで有効になっています。SSH にアクセスするには、クラウドセキュリティ設定でインバウンドトラフィックとアウトバウンドトラフィックの両方に SSH 接続が許可されていることを確認します。

---

Cisco Catalyst 8000V のソフトウェアは、標準の Cisco IOS XE CLI コマンドと表記規則を使用します。コマンドは大文字と小文字を区別せず、コマンドおよびパラメータは、現在使用可能な

他のコマンドまたはパラメータと区別可能な文字数まで省略できます。Cisco IOS XE CLI のすべての機能とその使用方法にアクセスするには、『[Configuration Fundamentals Configuration Guide](#)』を参照してください。

## Cisco Unified Computing System (UCS) 製品

表 1: Cisco Catalyst 8000V の Cisco UCS サーバーとの互換性

<p>Cisco Unified Computing System (UCS) 製品</p>	<p>Cisco UCS サーバーの要件は次のとおりです。</p> <ul style="list-style-type: none"> <li>• VMware 認定済みである。</li> <li>• 4 つ以上のコアが設定されている。</li> <li>• 最低 16 GB の UCS メモリ。SDWAN/コントローラモードを使用する場合は、SDWAN vManage、vBond、および vSmart に対応するために少なくとも 128 GB のメモリが必要です。</li> <li>• 最低 1 TB の UCS ストレージ。</li> <li>• UCS C220 M5 以上を推奨します。</li> </ul> <p>サポートされているハイパーバイザと互換性のある UCS ハードウェアおよびソフトウェアを確認するには、<a href="http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html">http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html</a> を参照してください。</p>
--	---



## 第 3 章

### 設置の概要

この章では、Cisco Catalyst 8000V をインストールする方法の概要を説明します。Cisco ハードウェアルータは、通常、Cisco IOS XE ソフトウェアをプレインストールして出荷されます。しかしながら、Cisco Catalyst 8000V はハードウェアベースのルータではないため、Cisco.com から Cisco IOS XE ソフトウェアをダウンロードして、仮想ルータを仮想マシンに直接インストールする必要があります。インストールに進む前に、Cisco Catalyst 8000V ソフトウェアをインストールして起動できるように、まず VM の属性をプロビジョニングする必要があります。

選択したハイパーバイザに依存するさまざまなインストールファイルとインストールオプションについては、次のセクションを参照してください。

- [インストールファイル \(9 ページ\)](#)
- [サポートされるハイパーバイザ \(11 ページ\)](#)
- [インストールファイルのダウンロード \(12 ページ\)](#)
- [注意事項と制約事項 \(12 ページ\)](#)
- [次の作業 \(13 ページ\)](#)

### インストール ファイル

次の表に、サポートされているハイパーバイザへの Cisco Catalyst 8000V のインストールに使用できるソフトウェアイメージを示します。

イメージタイプ	ハイパーバイザ	モード	セキュアブート	ファイル名の例
bin	ESXi、KVM、AWS、Microsoft Azure、GCP	アップグレード (バンドルモード) アップグレード (インストールモード)	不可	c8000v-universalk9.17.04.01a.SPA.bin

イメージタイプ	ハイパーバイザ	モード	セキュアブート	ファイル名の例
iso : VM にソフトウェアイメージをインストールするために使用されます。	ESXi、KVM	新規インストール	不可	c8000v-universalk9.17.04.01a.iso
ova : VM での OVA テンプレート (TAR 形式) の展開に使用されます。	ESXi	新規インストール	対応	c8000v-universalk9.17.04.01a.ova
qcow2 : KVM 環境でソフトウェアイメージをインストールするために使用されます。	KVM	新規インストール	不可	c8000v-universalk9.17.04.01a.qcow2
serial.qcow2	KVM	新規インストール	不可	c8000v-universalk9.17.04.01a.efi.qcow2
efi.qcow2	KVM	新規インストール	対応	c8000v-universalk9.17.04.01a.efi.qcow2
serial.efi.qcow2	KVM	新規インストール	対応	c8000v-universalk9.17.04.01a-serial.efi.qcow2
tar.gz	NFVIS	新規インストール	対応	c8000v-universalk9.17.04.01a-tar.gz



(注) セキュアブートは特定のイメージタイプでサポートされますが、この機能はデフォルトでは有効になっていません。ハイパーバイザのセキュアブートを有効にする方法については、「[VNF Secure Boot](#)」を参照してください。

# サポートされるハイパーバイザ

ハイパーバイザは、単一のハードウェア ホスト マシンを複数のオペレーティング システムで共有できるようにします。各オペレーティングシステムがホストのプロセッサ、メモリ、およびその他のリソースを専有していたとしても、ハイパーバイザは、各オペレーティングシステムに必要なリソースのみを制御して割り当てます。そうすることにより、オペレーティングシステム (VM) が相互に干渉しないようにします。

Cisco Catalyst 8000V でサポートされるハイパーバイザは次のとおりです。

- **VMware ESXi** : Cisco Catalyst 8000V は VMware ESXi ハイパーバイザ上で動作します。VMware ESXi ハイパーバイザは、仮想化拡張機能を含む x86 ハードウェア上で動作します。VMware の要件を確認し、ESXi 環境に Cisco Catalyst 8000V をインストールする方法を調べるには、「[Installing in VMware ESXi Environment](#)」を参照してください。
- **Red Hat KVM** : Cisco Catalyst 8000V は Red Hat Enterprise Linux (RHEL) 上でも動作します。
- **パブリッククラウド** : 上記のハイパーバイザとは別に、Cisco Catalyst 8000V を Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Alibaba Cloud で展開して使用することもできます。詳細については、それぞれのパブリッククラウド展開ガイドを参照してください。

## 仮想マシン処理リソース

Cisco Catalyst 8000V は低遅延アプリケーションであり、ホスト側の処理リソースがオーバーサブスクライブされている場合、正しく機能しない可能性があります。デフォルトでは、ほとんどのハイパーバイザは処理リソースのオーバーコミットをサポートしています。とはいえ、Cisco Catalyst 8000V では、仮想 CPU (vCPU) をオーバーサブスクライブしている状態で、確実にスケジューリング設定しなかった場合、パケット処理のドロップ、エラーメッセージ、またはシステム停止が発生する可能性があります。

Cisco Catalyst 8000V vCPU は、実際の物理コアで動作するようにホストハイパーバイザによってスケジューリング設定される必要があります。各ハイパーバイザには、物理コアへの vCPU のスケジューリング設定に影響を及ぼすさまざまな制御機能があります。ベストプラクティスとして、vCPU と実際の物理コアの比率を 1:1 にすることを推奨します。

仮想マシン処理リソースの詳細については、ハイパーバイザが提示する各ハイパーバイザのチューニングガイドを参照してください。また、本ガイドの該当するハイパーバイザのセクションを参照できます。この資料は、パフォーマンスを向上させ、システム全体の確定性を改善させるために使用可能な設定について説明しています。

# インストールファイルのダウンロード

## 手順

- ステップ1 シスコの [Software Download](#) ページに移動します。
- ステップ2 ページの下部にある [Select a Product] フィールドで、Cisco Catalyst 8000V を検索します。
- ステップ3 Cisco Catalyst 8000V のリンクをクリックし、ダウンロードページに移動します。
- ステップ4 左側のペインから該当するリリースを選択します。たとえば、Bengaluru 17.4.1 を選択します。
- ステップ5 使用可能なイメージのリストで [Download] または [Add to Cart] をクリックします。手順に従ってソフトウェアをダウンロードしてください。

(注)

ダウンロードするインストールファイルを確認するには、[インストールファイル \(9 ページ\)](#) を参照してください。

## 注意事項と制約事項

ネットワークに Cisco Catalyst 8000V ルータをインストールする前に留意すべき一般的な注意事項と制限事項を以下に示します。

- ネストされた VM 内の Cisco Catalyst 8000V はテストされていないため、推奨されません。
- ハイパーバイザが vNIC ホット追加/削除をサポートしていない場合、VM の電源が入っているときに、VM のハードウェア（メモリ、CPU、ハードドライブのサイズなど）に変更を加えないでください。
- Gigabit Ethernet0 インターフェイスは使用できなくなりました。任意のインターフェイスを管理インターフェイスとして指定できます。
- 仮想 VGA コンソールまたは仮想シリアルポートのコンソールのいずれかを使用して、Cisco IOS XE CLI にアクセスできます。初回インストール中に GRUB モードからコンソールを選択するか、ルータの起動後に Cisco IOS XE **platform console** コマンドを使用してコンソールを変更します。詳細については、[Cisco Catalyst 8000V を VM として起動 \(149 ページ\)](#) を参照してください。
- I350 デバイスで仮想機能を実行している場合、HSRP/VRRP などの冗長プロトコルはサポートされません。
- qcow2 ファイルの場合、インストール時に選択したイメージによって、選択できるコンソールのタイプが決まります。

- vNIC は、インターフェイスでのデュプレックス設定をサポートしていません。
- vNIC は自動ネゴシエーションをサポートしていません。
- Cisco IOS XE 17.9.1 以降、**show license udi** コマンドは Cisco Catalyst 8000V でサポートされなくなりました。
- Cisco Catalyst 8000V は、L2TP クライアントや L2TP ネットワークサーバー (LNS) を含む L2TP 機能をサポートしていません。
- コントローラモードの Cisco Catalyst 8000V インスタンスは 4GB メモリ構成をサポートしますが、シスコでは、機能豊富な大規模環境には 8GB メモリを使用することを推奨しています。これは、高いメモリ使用率の問題を回避するためです。



(注) 一部のハイパーバイザは、シリアルコンソールアクセスをサポートしない場合があります。ハイパーバイザのマニュアルを使用して、サポートを確認してください。

## 次の作業

インストールファイルをダウンロードしたので、展開に進むことができます。選択したハイパーバイザに応じて、展開手順は異なります。

適切なハイパーバイザ環境での Cisco Catalyst 8000V の展開方法については、このガイドの次の章を参照してください。

- [VMware ESXi 環境でのインストール](#)
- [カーネル仮想マシンサポート \(KVM\) 環境でのインストール](#)

### パブリッククラウドでの展開

- Amazon Web Services 環境での Cisco Catalyst 8000V 展開の詳細については、『[Deploying Cisco Catalyst 8000V Edge Software on Amazon Web Services](#)』を参照してください。
- Microsoft Azure 環境での Cisco Catalyst 8000V 展開の詳細については、『[Deploying Cisco Catalyst 8000V on Microsoft Azure](#)』を参照してください。
- Google Cloud Platform での Cisco Catalyst 8000V 展開の詳細については、『[Deploying Cisco Catalyst 8000V on Google Cloud Platform](#)』を参照してください。
- Alibaba Cloud での Cisco Catalyst 8000V の展開の詳細については、『[Deploying Cisco Catalyst 8000V on Alibaba Cloud](#)』を参照してください。



---

(注) インストールを続行する前に、次の章を参照してください。

- [Day 0 Configuration](#)
  - [VNF Secure Boot](#)
  - [Configuring Console Access](#)
-



## 第 4 章

# インストールコマンドを使用したソフトウェアのインストール

---

- [インストールコマンドを使用したソフトウェアのインストール \(15 ページ\)](#)
- [インストールコマンドを使用したソフトウェアのインストールに関する情報 \(16 ページ\)](#)
- [インストールコマンドを使用したソフトウェアインストールの設定例 \(28 ページ\)](#)
- [インストールコマンドを使用したソフトウェアインストールのトラブルシューティング \(41 ページ\)](#)

## インストールコマンドを使用したソフトウェアのインストール

Cisco IOS XE 17.15.1a 以降、Cisco IOS XE プラットフォームはデフォルトでインストールモードで出荷されます。ユーザーは、一連の **install** コマンドを使用して、プラットフォームを起動し、Cisco IOS XE ソフトウェアバージョンにアップグレードまたはダウングレードできます。

## インストールコマンドを使用したソフトウェアのインストールに関する制約事項

- ISSU はこの機能ではカバーされません。
- インストールモードでは、システムの再起動が必要です。

# インストールコマンドを使用したソフトウェアのインストールに関する情報

インストールモードで出荷されるルータの場合、一連の **install** コマンドを使用して、インストールモードでプラットフォームを起動、アップグレード、およびダウングレードできます。この更新は、Cisco Catalyst 8000 エッジプラットフォームに適用されます。

Cisco IOS XE 17.15.1a リリース以降、この更新はすべての Cisco IOS XE プラットフォームに適用されます。

次の表に、バンドルモードとインストールモードの違いを示します。

表 2: バンドルモードとインストールモード

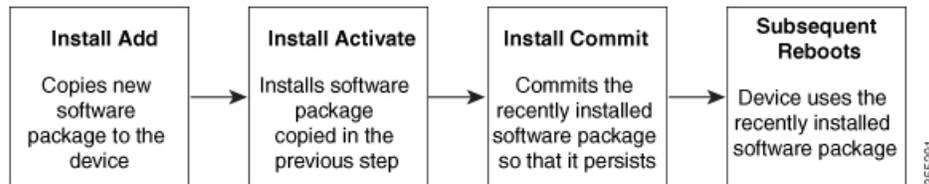
バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。  (注) USB および TFTP ブートからのバンドルブートはサポートされていません。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI :  #boot system file <filename>	CLI :  #install add file bootflash: [activate commit]
このモードでアップグレードするには、boot system が新しいソフトウェアイメージをポイントするようにします。	このモードでアップグレードするには、install コマンドを使用します。
イメージの自動アップグレード：新しい Field Replaceable Unit (FRU) がモジュラ型シャーシに挿入された場合、アクティブな FRU と同じバージョンで新しい FRU を実行するには、手動による作業が必要です。	イメージの自動アップグレード：新しい FRU がモジュラ型シャーシに挿入された場合、結合する FRU は、アクティブな FRU と同期してイメージバージョンに自動アップグレードされます。
ロールバック：複数のソフトウェアメンテナンスの更新 (SMU) を使用して以前のイメージにロールバックするには、複数回のリロードが必要になる場合があります。	ロールバック：1回のリロードで、複数のパッチを含む、Cisco IOS XE ソフトウェアの以前のバージョンへのロールバックを有効にします。

## インストールモードのプロセスフロー

インストールモードのプロセスフローは、プラットフォームでソフトウェアのインストールとアップグレードを実行するための次の3つのコマンドで構成されています。**install add**、**install activate**、**install commit**

次のフローチャートは、**install** コマンドを使用したインストールプロセスを説明しています。

Process with Install Commit



**install add** コマンドは、ソフトウェアパッケージをローカルまたはリモートの場所からプラットフォームにコピーします。FTP、HTTP、HTTPS、またはTFTPを使用できます。このコマンドは、パッケージファイルの個々のコンポーネントをサブパッケージと **packages.conf** ファイルに展開します。またファイルを検証して、イメージファイルがこれからインストールする先のプラットフォーム用のものであることを確認します。

**install activate** コマンドは、必要な検証を実行し、**install add** コマンドを使用して以前に追加されたパッケージをプロビジョニングします。また、システムのリロードをトリガーします。

**install commit** コマンドは、**install activate** コマンドを使用して以前にアクティブ化されたパッケージを確認し、リロード後も更新が持続されるようにします。



- (注) 更新をインストールすると、以前にインストールしたソフトウェアイメージが置換されます。どんな時でも、1つのデバイスにインストールできるのは1つのイメージのみです。

次の一連のインストールコマンドが使用できます。

表 3: インストールコマンド一覧

コマンド	構文	目的
<b>install add</b>	<b>install add file</b> <i>location:filename.bin</i>	<p>イメージ、パッケージ、およびSMUの内容をソフトウェアリポジトリにコピーします。ファイルの場所はローカルでもリモートでもかまいません。このコマンドは次のことを行います。</p> <ul style="list-style-type: none"> <li>• ファイルのチェックサム、プラットフォームの互換性チェックなどを検証します。</li> <li>• パッケージの個々のコンポーネントをサブパッケージと <code>packages.conf</code> に展開します。</li> <li>• イメージをローカルインベントリにコピーし、次の手順で使用できるようにします。</li> </ul>
<b>install activate</b>	<b>install activate</b>	<p><b>install add</b> コマンドを使用して追加されたパッケージをアクティブ化します。</p> <ul style="list-style-type: none"> <li>• <b>show install summary</b> コマンドを使用して、非アクティブなイメージを確認します。このイメージがアクティブ化されます。</li> <li>• このコマンドを実行すると、システムがリロードされます。アクティベーションを続行するかどうかを確認します。確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> </ul>

コマンド	構文	目的
<b>(install activate) auto abort-timer</b>	<b>install activate auto-abort timer</b> <30-1200>	<p><b>auto-abort timer</b> は自動的に開始され、デフォルト値は 120 分です。指定された時間内に <b>install commit</b> コマンドが実行されない場合、アクティベーションプロセスは中止され、システムは最後にコミットされた状態に戻ります。</p> <ul style="list-style-type: none"> <li>• <b>install activate</b> コマンドを実行しながらタイマーの値を変更できます。</li> <li>• <b>install commit</b> コマンドはタイマーを停止し、インストールプロセスを続行します。</li> <li>• <b>install activate auto-abort timer stop</b> コマンドは、パッケージをコミットせずにタイマーを停止します。</li> <li>• 確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> <li>• このコマンドは、3ステップインストールのバリエーションでのみ有効です。</li> </ul>
<b>install commit</b>	<b>install commit</b>	<p><b>install activate</b> コマンドを使用してアクティブ化されたパッケージをコミットし、リロード後も持続するようにします。</p> <ul style="list-style-type: none"> <li>• <b>show install summary</b> コマンドを使用して、コミットされていないイメージを確認します。このイメージがコミットされます。</li> </ul>

コマンド	構文	目的
<b>install abort</b>	<b>install abort</b>	<p>インストールを中止し、システムを最後にコミットされた状態に戻します。</p> <ul style="list-style-type: none"> <li>このコマンドは、パッケージがアクティブ化された状態（コミットされていない状態）の場合にのみ適用されます。</li> <li><b>install commit</b> コマンドを使用してイメージをすでにコミットしている場合は、<b>install rollback to</b> コマンドを使用して望みのバージョンに戻ります。</li> </ul>
<b>install remove</b>	<b>install remove {file &lt;filename&gt;   inactive}</b>	<p>プラットフォームリポジトリから非アクティブなパッケージを削除します。このコマンドを使用して、スペースを解放します。</p> <ul style="list-style-type: none"> <li><b>file</b> : 指定されたファイルを削除します。</li> <li><b>inactive</b> : 非アクティブなファイルをすべて削除します。</li> </ul>

コマンド	構文	目的
<b>install rollback to</b>	<b>install rollback to {base   label   committed   id}</b>	<p>保存されているインストールポイントか、最後にコミットされたインストールポイントに、ソフトウェアセットをロールバックします。このコマンドには次のような特長があります。</p> <ul style="list-style-type: none"> <li>• リロードが必要です。</li> <li>• パッケージがコミットされた状態の場合にのみ適用されます。</li> <li>• 確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> </ul> <p>(注) 以前のイメージへのインストールのロールバックを実行する場合は、以前のイメージはインストールモードでインストールされている必要があります。バンドルモードではSMUロールバックのみが可能です。</p>
<b>install deactivate</b>	<b>install deactivate file &lt;filename&gt;</b>	<p>プラットフォームリポジトリからパッケージを削除します。このコマンドは、SMUでのみサポートされています。</p> <ul style="list-style-type: none"> <li>• 確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> </ul>

次の show コマンドも使用できます。

表 4: *show* コマンドの一覧

コマンド	構文	目的
<b>show install log</b>	<b>show install log</b>	プラットフォームがブートされた後に実行されたすべてのインストール操作の履歴と詳細を提供します。
<b>show install package</b>	<b>show install package &lt;filename&gt;</b>	指定された .pkg/.bin ファイルに関する詳細を提供します。
<b>show install summary</b>	<b>show install summary</b>	すべての FRU のイメージバージョンとそれに対応するインストール状態の概要を提供します。 <ul style="list-style-type: none"> <li>• 表示される表には、この情報が適用される FRU が示されます。</li> <li>• 存在するイメージとその状態に関してすべての FRU が同期している場合、1つの表のみが表示されます。</li> <li>• ただし、FRU 間でイメージまたは状態の情報が異なる場合は、スタックの残りの部分と異なる各 FRU が個別の表にリストされます。</li> </ul>
<b>show install active</b>	<b>show install active</b>	すべての FRU のアクティブなパッケージに関する情報を提供します。 <p>FRU 間で情報に異なる場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。</p>

コマンド	構文	目的
<b>show install inactive</b>	<b>show install inactive</b>	すべての FRU に非アクティブなパッケージがあれば、そのパッケージに関する情報を提供します。  FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
<b>show install committed</b>	<b>show install committed</b>	すべての FRU のコミットされたパッケージに関する情報を提供します。  FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
<b>show install uncommitted</b>	<b>show install uncommitted</b>	すべての FRU について、コミットされていないパッケージがある場合はそのパッケージに関する情報を提供します。  FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
<b>show install rollback</b>	<b>show install rollback {point-id   label}</b>	保存されているインストールポイントに関連付けられたパッケージを表示します。
<b>show version</b>	<b>show version [rp-slot] [installed   user-interface]   provisioned   running]</b>	ハードウェアとプラットフォームの情報とともに、現在のパッケージに関する情報を表示します。

## プラットフォームをインストールモードで起動

単一のコマンド（1 ステップインストール）または複数の個別のコマンド（3 ステップインストール）を使用してソフトウェアパッケージをインストールして、アクティブ化し、コミットできます。

プラットフォームがバンドルモードで動作している場合、1 ステップインストールの手順を使用して、最初にバンドルモードからインストールモードに変換する必要があります。その後のプラットフォームでのインストールとアップグレードは、1 ステップまたは3 ステップのバリエーションのいずれかで実行できます。

## 1 ステップインストールまたはバンドルモードからインストールモードへの変換



- (注)
- すべての CLI アクション（追加、アクティブ化など）は、使用可能なすべての FRU で実行されます。
  - 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
  - このワークフローの2番目のステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。
  - プロンプトレベルが [None] に設定されていて、保存されていない設定がある場合、インストールは失敗します。コマンドを再発行する前に、設定を保存する必要があります。

以下で説明する1ステップインストールの手順を使用して、バンドルブートモードで実行されているプラットフォームをインストールモードに変換します。コマンドの実行後、プラットフォームはインストールブートモードでリブートします。

後で、1 ステップインストールの手順を使用してプラットフォームをアップグレードすることもできます。

この手順では、特権 EXEC モードで **install add file activate commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

### 手順の概要

1. **enable**
2. **install add file location: filename [activate commit]**
3. **exit**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
	Device>enable	
ステップ 2	<b>install add file location: filename [activate commit]</b> 例 : <pre>Device#install add file rootflash:c8000e-universalk9_EFD_V177_THRPTIME_LATEST_20211021_031123_V17_7_0_117.SSA.bin activate commit</pre>	ソフトウェア インストール パッケージをローカルまたはリモートの場所 (FTP、HTTP、HTTPS、または TFTP 経由) からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。プラットフォームおよびイメージバージョンの検証および互換性チェックを実行し、パッケージをアクティブ化し、そのパッケージをコミットして複数回リロードしても維持されるようにします。  このコマンドを実行すると、プラットフォームがリロードされます。
ステップ 3	<b>exit</b> 例 : <pre>Device#exit</pre>	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

## 3 ステップインストール



- (注)
- すべての CLI アクション (追加、アクティブ化など) は、使用可能なすべての FRU で実行されます。
  - 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
  - このワークフローの install activate ステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。

3 ステップインストール手順は、プラットフォームがインストールモードになった後でのみ使用できます。このオプションにより、インストール時により多くの柔軟性と制御がもたらされます。

この手順では、個別の **install add**、**install activate**、および **install commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

### 手順の概要

1. **enable**
2. **install add file location: filename**
3. **show install summary**
4. **install activate [auto-abort-timer <time>]**
5. **install abort**

6. **install commit**
7. **install rollback to committed**
8. **install remove {file filesystem: filename | inactive}**
9. **show install summary**
10. **exit**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device>enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>install add file location: filename</b> 例： Device#install add file bootflash:c8000e-universal9_HD_V177_THROTTLE_LATEST_20211027_030841_V17 7 0 120.SPA.bin	ソフトウェア インストール パッケージをリモートの場所 (FTP、HTTP、HTTPS、または TFTP 経由) からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。
ステップ 3	<b>show install summary</b> 例： Device#show install summary	(オプション) すべての FRU のイメージバージョンとそれに対応するインストール状態の概要を提供します。
ステップ 4	<b>install activate [auto-abort-timer &lt;time&gt;]</b> 例： Device# install activate auto-abort-timer 120	以前に追加されたパッケージをアクティブ化し、プラットフォームをリロードします。 <ul style="list-style-type: none"> <li>• ソフトウェアの完全インストールを実行する場合は、パッケージファイル名を指定しないでください。</li> <li>• 3 ステップインストールのバリエーションでは、<b>install activate</b> コマンドで <b>auto-abort-timer</b> が自動的に開始されます。タイマーのデフォルトは 120 分です。タイマーの期限が切れる前に <b>install commit</b> コマンドが実行されない場合、インストールプロセスは自動的に終了します。プラットフォームがリロードされ、最後にコミットされたバージョンで起動します。</li> </ul>
ステップ 5	<b>install abort</b> 例： Device#install abort	(オプション) ソフトウェアインストールのアクティブ化を中止し、プラットフォームを最後にコミットされたバージョンに戻します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>このコマンドは、イメージがアクティブ化されている状態でのみ使用できます。イメージがコミットされた状態の場合は使用できません。</li> </ul>
ステップ 6	<b>install commit</b> 例： Device#install commit	新しいパッケージのインストールをコミットし、リロード後も変更が持続されるようにします。
ステップ 7	<b>install rollback to committed</b> 例： Device#install rollback to committed	(オプション) 最後にコミットした状態にプラットフォームをロールバックします。
ステップ 8	<b>install remove {file filesystem: filename   inactive}</b> 例： Device#install remove inactive	(オプション) ソフトウェア インストール ファイルを削除します。 <ul style="list-style-type: none"> <li><b>file</b> : 特定のファイルを削除します</li> <li><b>inactive</b> : 未使用および非アクティブ状態のインストールファイルを削除します。</li> </ul>
ステップ 9	<b>show install summary</b> 例： Device#show install summary	(オプション) 現在のシステムの状態に関する情報を表示します。このコマンドの出力は、このコマンドよりも先に実行された <b>install</b> コマンドに応じて変化します。
ステップ 10	<b>exit</b> 例： Device#exit	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

## インストール モードでのアップグレード

1 ステップインストールまたは 3 ステップインストールを使用して、インストールモードでプラットフォームをアップグレードします。

## インストールモードでのダウングレード

ダウングレード先のイメージがインストールモードでインストールされている場合、**install rollback** コマンドを使用して、プラットフォームを適切なイメージにポイントすることにより、プラットフォームを以前のバージョンにダウングレードします。

この **install rollback** コマンドはプラットフォームをリロードし、前のイメージで起動します。



- (注) **install remove inactive** コマンドを使用して前のファイルを削除していない場合にのみ、**install rollback** コマンドは成功します。

または、**install** コマンドを使用して古いイメージをインストールすることでダウングレードすることもできます。

## ソフトウェアインストールの中止

ソフトウェアパッケージのアクティブ化は次の方法で中止できます。

- 新しいイメージをアクティブ化した後にプラットフォームをリロードすると、3 ステップインストールのバリエーションでは **auto-abort-timer** がトリガーされます。**install commit** コマンドを発行する前にタイマーが期限切れになった場合、インストールプロセスが終了します。プラットフォームはリロードし、最後にコミットしたバージョンのソフトウェアイメージで起動します。

または、**install commit** コマンドを使用せずに、**install auto-abort-timer stop** コマンドを使用してこのタイマーを停止します。このプロセスでは、新しいイメージはコミットされていないままです。

- **install abort** コマンドを使用して、新しいソフトウェアのインストール前に実行していたバージョンにプラットフォームを戻します。このコマンドは、**install commit** コマンドを発行する前に使用します。

## インストールコマンドを使用したソフトウェアインストールの設定例

以下は、1 ステップインストールまたはバンドルモードからインストールモードへの変換の例です。

```
Router# install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
activate commit
install_add_activate_commit: START Thu Oct 28 21:57:21 UTC 2021
```

```
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]
Building configuration...
```

```
[OK]Modified configuration has been saved
```

```
*Oct 28 21:57:39.818: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
config file
*Oct 28 21:57:39.925: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot
```

```
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bininstall_add_activate_commit:
Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.07.01.0.1515
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_async_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
--- Starting Activate ---
Performing Activate on Active/Standby

*Oct 28 22:05:49.484: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Activate package(s) on R0
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
  [1] Commit package(s) on R0

Building configuration...
  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

[OK]
*Oct 28 22:06:55.375: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
config fileSend model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit Thu Oct 28 22:07:22 UTC 2021

Router#
```

```
*Oct 28 22:07:22.661: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.binOct
28 22:07:26.864: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload
action requested
```

□

Press RETURN to get started!

以下は、3 ステップインストールの例です。

```
Router# install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
install_add: START Thu Oct 28 22:36:43 UTC 2021
```

```
*Oct 28 22:36:44.526: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bininstall_add:
Adding PACKAGE
install_add: Checking whether new add is allowed ....
```

```
--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add
```

```
Image added. Version: 17.07.01.0.1601
SUCCESS: install_add Thu Oct 28 22:40:25 UTC 2021
```

```
Router#
*Oct 28 22:40:25.971: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
```

```
Router# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS Thu Oct 28 22:09:30 Universal 2021
[0|install_op_boot(INFO, )]: cleanup_trap remote_invocation 0 operation install_op_boot
.. 0 .. 0
[1|display_install_log]: START Thu Oct 28 22:12:11 UTC 2021
[2|install_add]: START Thu Oct 28 22:36:43 UTC 2021
[2|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
[2|install_add(CONSOLE, )]: Adding PACKAGE
[2|install_add(CONSOLE, )]: Checking whether new add is allowed ....
[2|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
[remote|install_add]: START Thu Oct 28 22:37:12 UTC 2021
[remote|install_add]: END SUCCESS Thu Oct 28 22:40:10 UTC 2021
[remote|install_add(INFO, )]: cleanup_trap remote_invocation 1 operation install_add
.. 0 .. 0
[2|install_add(INFO, )]: Remote output from R0
[2|install_add(INFO, )]: install_add: START Thu Oct 28 22:37:12 UTC 2021
Expanding image file:
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
Verifying parameters
Expanding superpackage
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
... parameters verified
```

```
Validating package type
... package type validated
Copying package files

c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    WARNING: A different version of provisioning file packages.conf already exists in
bootflash:
  WARNING: The provisioning file from the expanded bundle will be saved as
  WARNING: bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_0.conf
... package files copied
SUCCESS: Finished expanding all-in-one software package.
Image file expanded
SUCCESS: install_add Thu Oct 28 22:40:10 UTC 2021
[2|install_add]: END SUCCESS Thu Oct 28 22:40:25 UTC 2021
[2|install_add(INFO, )]: cleanup_trap remote_invocation 0 operation install_add .. 0
.. 0
[3|COMP_CHECK]: START Thu Oct 28 22:40:26 UTC 2021
[3|COMP_CHECK]: END FAILED exit(1) Thu Oct 28 22:40:27 UTC 2021
[3|COMP_CHECK(INFO, )]: cleanup_trap remote_invocation 0 operation COMP_CHECK .. 1 ..
```

## インストールコマンドを使用したソフトウェアインストールの設定例

```

1
[4|install_activate]: START Thu Oct 28 22:42:53 UTC 2021
[4|install_activate(INFO, require user prompt)]: install_cli
[4|install_activate(CONSOLE, )]: Activating PACKAGE
[4|install_activate(INFO, )]: Acquiring transaction lock...
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: tmp_global_trans_lock: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: tmp lock does not exist: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: tmp_global_trans_lock: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: local_trans_lock:
/bootflash/.installer/install_local_trans_lock
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: validate_lock: lock_duration is 7200
[4|install_activate(INFO, )]: install type stored in lock PACKAGE, install type PACKAGE,
install operation install_activate
[4|install_activate(INFO, )]: lock duration: 7200
[4|install_activate(INFO, )]: extend trans lock done.
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, require user prompt)]: install_cli
[4|install_activate( FATAL)]: Cannot proceed activate because of user input
[4|install_activate(INFO, )]: cleanup_trap remote_invocation 0 operation install_activate
.. 6 .. 0
[5|install_add]: START Thu Oct 28 22:45:48 UTC 2021
[5|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
[5|install_add(CONSOLE, )]: Adding PACKAGE
[5|install_add(CONSOLE, )]: Checking whether new add is allowed ....
[5|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
[5|install_add( FATAL)]: Super package already added. Add operation not allowed. install
remove inactive can be used to discard added packages

Router# install activate
install_activate: START Thu Oct 28 23:57:57 UTC 2021
install_activate: Activating PACKAGE

*Oct 28 23:57:57.823: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activateFollowing packages shall be activated:
/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_ngwic_tle1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby

```

```
*Oct 29 00:04:19.400: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Activate package(s) on R0
--- Starting list of software package changes ---
Old files list:
  Modified
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_ngwic_tle1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
  Modified c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

New files list:
  Added
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  Added
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  Added
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  Added
```

```

c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_ngwic_tlel.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Finished list of software package changes
    [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

Send model notification for install_activate before reload
Install will reload the system now!
SUCCESS: install_activate  Fri Oct 29 00:05:09 UTC 2021

Router#
*Oct 29 00:05:09.504: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
  install activate PACKAGEOct 29 00:05:14.494: %PMAN-5-EXITACTION: R0/0: pvp: Process
manager is exiting: reload action requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610

System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running   : Boot ROM1
Last reset cause        : LocalSoft
C8300-2N2S-6T platform with 8388608 Kbytes of main memory

```

□

```
Press RETURN to get started!
```

□

```
Router# install commit
install_commit: START Fri Oct 29 00:13:58 UTC 2021
install_commit: Committing PACKAGE

--- Starting Commit ---
Performing Commit on Active/Standby

*Oct 29 00:13:59.552: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit [1] Commit package(s) on R0
[1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

SUCCESS: install_commit Fri Oct 29 00:14:03 UTC 2021

Router#
*Oct 29 00:14:03.712: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install_commit PACKAGE
```

以下は、インストールモードでのダウングレードの例です。

```
ROUTER# install activate file bootflash:c8000be-universalk9.17.06.01a.SPA.bin activate
commit

install_add_activate_commit: START Fri Dec 10 18:07:17 GMT 2021

*Dec 10 18:07:18.405 GMT: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot
bootflash:c8000be-universalk9.17.06.01a.SPA.bininstall_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
[1] Add package(s) on R0
[1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.06.01a.0.298
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000be-rpboot.17.06.01a.SPA.pkg
/bootflash/c8000be-mono-universalk9.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_async.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_1t3e3.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_10g.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_prince.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_xdsl.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_ssd.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_shdsl.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_ge.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_cwan.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.17.06.01a.SPA.pkg
```

```

/bootflash/c8000be-firmware_nim_async.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_ngwic_tle1.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dreamliner.17.06.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby
  [1] Activate package(s) on R0
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
  [1] Commit package(s) on R0
Building configuration...

  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

[OK]
*Dec 10 18:14:57.782 GMT: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
config fileSend model notification for install_add_activate_commit before reload
/usr/binos/conf/install_util.sh: line 164: /bootflash/.prst_sync/reload_info: No such
file or directory
/usr/binos/conf/install_util.sh: line 168: /bootflash/.prst_sync/reload_info: No such
file or directory
cat: /bootflash/.prst_sync/reload_info: No such file or directory
Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Dec 10 18:15:23 GMT 2021

ROUTER#
*Dec 10 18:15:23.955 GMT: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install one-shot PACKAGE bootflash:c8000be-universalk9.17.06.01a.SPA.binDec
10 18:15:27.708: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action
requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 17.3(5r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
ROUTER platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□

ROUTER#

```

```

ROUTER# show version
Cisco IOS XE Software, Version 17.06.01a
Cisco IOS Software [Bengaluru], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.6.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sat 21-Aug-21 03:27 by mcpre

```

Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.  
 All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: 17.3(5r)

```

ROUTER uptime is 0 minutes
Uptime for this control processor is 2 minutes
System returned to ROM by LocalSoft
System image file is "bootflash:packages.conf"
Last reload reason: LocalSoft

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Technology Package License Information:

```

-----
Technology      Type          Technology-package Current  Technology-package Next Reboot
-----
Smart License   Perpetual     None          None
Smart License   Subscription  None          None

```

The current crypto throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

```

cisco ROUTER (1RU) processor with 3747220K/6147K bytes of memory.
Processor board ID FDO2521M27S
Router operating mode: Autonomous
5 Gigabit Ethernet interfaces
2 2.5 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
7573503K bytes of flash memory at bootflash:.
1875361792K bytes of NVMe SSD at harddisk:.

```

```
16789568K bytes of USB flash at usb0:.
Configuration register is 0x2102
```

以下は、ソフトウェアのインストールを終了する例です。

```
Router# install abort
install_abort: START Fri Oct 29 02:42:51 UTC 2021

This install abort would require a reload. Do you want to proceed? [y/n]
*Oct 29
02:42:52.789: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install aborty
--- Starting Abort ---
Performing Abort on Active/Standby

    [1] Abort package(s) on R0
    [1] Finished Abort on R0
Checking status of Abort on [R0]
Abort: Passed on [R0]
Finished Abort

Send model notification for install_abort before reload
Install will reload the system now!
SUCCESS: install_abort  Fri Oct 29 02:44:47 UTC 2021

Router#
*Oct 29 02:44:47.866: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install_abort PACKAGEOct 29 02:44:51.577: %PMAN-5-EXITACTION: R0/0: pvp: Process manager
is exiting: reload action requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610

System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running   : Boot ROM1
Last reset cause       : LocalSoft
C8300-2N2S-6T platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□
```

以下は、show コマンドの出力例です。

### show install log

```
Device# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS Thu Oct 28 22:09:30 Universal 2021
```

### show install summary

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
```

```

State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version
-----
IMG   C   17.07.01.0.1515
-----

Auto abort timer: inactive
-----

```

### show install package *filesystem: filename*

```

Device# show install package
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
Package: c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin

Size: 831447859
Timestamp: 2021-10-23 17:08:14 UTC
Canonical path:
/bootflash/c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin

```

```

Raw disk-file SHA1sum:
 5c4e7617a6c71ffbcc73dcd034ab58bf76605e3f
Header size:      1192 bytes
Package type:     30000
Package flags:    0
Header version:   3

```

```

Internal package information:
Name: rp_super
BuildTime: 2021-10-21_13.00
ReleaseDate: 2021-10-21_03.11
BootArchitecture: i686
RouteProcessor: radium
Platform: C8000BE
User: mcpre
PackageName: universalk9
Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
CardTypes:

```

```

Package is bootable from media and tftp.
Package contents:

```

```

Package:
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
Size: 2966620
Timestamp: 2021-10-21 20:10:44 UTC

```

```

Raw disk-file SHA1sum:
 501d59d5f152ca00084a0da8217bf6f6b95dddb1
Header size:      1116 bytes
Package type:     40000
Package flags:    0
Header version:   3

```

```

Internal package information:
Name: firmware_nim_ge
BuildTime: 2021-10-21_13.00
ReleaseDate: 2021-10-21_03.11
BootArchitecture: none
RouteProcessor: radium
Platform: C8000BE
User: mcpre

```

```

PackageName: firmware_nim_ge
Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
CardTypes:

```

Package is not bootable.

```

Package:
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
Size: 10204252
Timestamp: 2021-10-21 20:10:43 UTC

```

```

Raw disk-file SHA1sum:
  a57bed4ddecfd08af3b456f69d11aaeb962865ea
Header size:      1116 bytes
Package type:     40000
Package flags:    0
Header version:   3

```

```

Internal package information:
Name: firmware_prince
BuildTime: 2021-10-21 13:00
ReleaseDate: 2021-10-21_03.11
BootArchitecture: none
RouteProcessor: radium
Platform: C8000BE
User: mcpre
PackageName: firmware_prince
Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
CardTypes:

```

Package is not bootable.

### show install active

```

Device# show install active
[ R0 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
IMG   C    17.07.01.0.1515
-----
Auto abort timer: inactive
-----

```

### show install inactive

```

Device# show install inactive
[ R0 ] Inactive Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
No Inactive Packages

```

### show install committed

```

Device# show install committed
[ R0 ] Committed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----

```

```
IMG C 17.07.01.0.1515

-----
Auto abort timer: inactive
-----

show install uncommitted

Device# show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type St  Filename/Version
-----
No Uncommitted Packages
```

## インストールコマンドを使用したソフトウェアインストールのトラブルシューティング

**問題** ソフトウェアインストールのトラブルシューティング

**解決法** インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次の show コマンドを使用します。

- **show install summary**
- **show install log**
- **show version**
- **show version running**

**問題** インストールに関するその他の問題

**解決法** インストールに関する問題を解決するには、次のコマンドを使用します。

- **dir <install directory>**
- **more location:packages.conf**
- **show tech-support install** : このコマンドはインストール情報に固有の情報を表示する show コマンドを自動的に実行します。
- **request platform software trace archive target bootflash <location>** : このコマンドは、最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、この情報を指定された場所に保存します。





## 第 5 章

# パブリックおよびソブリン IaaS クラウド における Cisco Catalyst 8000V の互換性マト リックス

この章では、Cisco Catalyst 8000V ルータでサポートされているさまざまなパブリック クラウドコンピューティングインスタンスのサイズについて説明します。次のトピックでは、サポートされている各パブリッククラウドとソブリン IaaS クラウドのコンピューティング インスタンスの詳細について説明します。

- [AWS](#) でサポートされるインスタンスタイプ (43 ページ)
- [Microsoft Azure](#) でサポートされるインスタンスタイプ (46 ページ)
- [Google Cloud Platform](#) でサポートされるインスタンスタイプ (50 ページ)
- [Sovereign Cloud](#) でサポートされるインスタンスタイプ (52 ページ)

## AWS でサポートされるインスタンスタイプ

AMI は、さまざまなインスタンスタイプをサポートしています。インスタンスタイプによって、インスタンスのサイズと必要なメモリ容量が決まります。Cisco Catalyst 8000V では、次のインスタンスタイプがサポートされています。

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.16.1a	<ul style="list-style-type: none"><li>• t3.medium</li><li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li><li>• c5n.18xlarge、c5n.4xlarge</li><li>• c6in.8xlarge、c6in.2xlarge、c6in.xlarge、c6in.large</li></ul>

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.15.3a Cisco IOS XE 17.15.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.4xlarge</li> <li>• c6in.8xlarge、c6in.2xlarge、c6in.xlarge、c6in.large</li> </ul>
Cisco IOS XE 17.14.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.4xlarge</li> <li>• c6in.8xlarge、c6in.2xlarge、c6in.xlarge、c6in.large</li> </ul>
Cisco IOS XE 17.13.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.4xlarge</li> <li>• c6in.8xlarge、c6in.2xlarge、c6in.xlarge、c6in.large</li> </ul>
Cisco IOS XE 17.12.4b Cisco IOS XE 17.12.4a Cisco IOS XE 17.12.2、 Cisco IOS XE 17.12.1	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、 c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>
Cisco IOS XE 17.11.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、 c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>
Cisco IOS XE 17.10.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、 c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.9.6 Cisco IOS XE 17.9.5f Cisco IOS XE 17.9.5e Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.4 Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>
Cisco IOS XE 17.8.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>
Cisco IOS XE 17.6.8a Cisco IOS XE 17.6.7 Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.6 Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.5.1a	<ul style="list-style-type: none"> <li>• t3.medium、t2.medium</li> <li>• c4.8xlarge、c4.4xlarge、c4.2xlarge、c4.xlarge、c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	<ul style="list-style-type: none"> <li>• t3.medium、t2.medium</li> <li>• c4.8xlarge、c4.4xlarge、c4.2xlarge、c4.xlarge、c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> <li>• c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large</li> </ul>

インスタンスタイプの詳細については、[Amazon EC2 インスタンスタイプ](#)を参照してください。

## Microsoft Azure でサポートされるインスタンスタイプ

次の 2、4、および 8 つの NIC ソリューションテンプレートは、現在、パブリッククラウドの Microsoft Azure マーケットプレイスで提供されています。

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.16.1a	<ul style="list-style-type: none"> <li>• Dsv5 シリーズ : Standard_D16s_v5</li> <li>• Dsv2 シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• Dv2 シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• Fsv2 シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.15.3a	<ul style="list-style-type: none"> <li>• <b>Dsv5</b> シリーズ : Standard_D16s_v5、Standard_D8s_v5、Standard_D4s_v5</li> <li>• <b>Dv5</b> シリーズ : Standard_D16_v5、Standard_D8_v5、Standard_D4_v5</li> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.15.1a	<ul style="list-style-type: none"> <li>• <b>Dsv5</b> シリーズ : Standard_D16s_v5、Standard_D8s_v5、Standard_D4s_v5</li> <li>• <b>Dv5</b> シリーズ : Standard_D16_v5、Standard_D8_v5、Standard_D4_v5</li> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.14.1a	<ul style="list-style-type: none"> <li>• <b>Dv5</b> シリーズ : Standard_D16_v5</li> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.13.1a	<ul style="list-style-type: none"> <li>• <b>Dv5</b> シリーズ : Standard_D16_v5</li> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.12.4b Cisco IOS XE 17.12.4a	<ul style="list-style-type: none"> <li>• <b>Dsv5</b> シリーズ : Standard_D16s_v5、Standard_D8s_v5、Standard_D4s_v5</li> <li>• <b>Dv5</b> シリーズ : Standard_D16_v5、Standard_D8_v5、Standard_D4_v5</li> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.12.2 Cisco IOS XE 17.12.1	<ul style="list-style-type: none"> <li>• <b>Dv5</b> シリーズ : Standard_D16_v5</li> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.11.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.10.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.9.6 Cisco IOS XE 17.9.5f Cisco IOS XE 17.9.5e Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.8.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.6.8a Cisco IOS XE 17.6.7 Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.5a、 Cisco IOS XE 17.6.4a Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2a Cisco IOS XE 17.6.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.5.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	<ul style="list-style-type: none"> <li>• <b>Dsv2</b> シリーズ : Standard_DS4_v2、Standard_DS3_v2、Standard_DS2_v2</li> <li>• <b>Dv2</b> シリーズ : Standard_D4_v2、Standard_D3_v2、Standard_D2_v2</li> <li>• <b>Fsv2</b> シリーズ : Standard_F32s_v2、Standard_F16s_v2</li> </ul>

## Google Cloud Platform でサポートされるインスタンスタイプ

Cisco IOS XE リリース	サポートされるインスタンスタイプ (BYOLのみ)
Cisco IOS XE 17.16.1a	<b>N1</b> : n1-standard-8、n1-standard-4
Cisco IOS XE 17.15.3a	<b>N1</b> : n1-standard-8、n1-standard-4 <b>N2</b> : n2-standard-8、n2-standard-4
Cisco IOS XE 17.15.1a	<b>N1</b> : n1-standard-8、n1-standard-4 <b>N2</b> : n2-standard-8、n2-standard-4

<b>Cisco IOS XE</b> リリース	サポートされるインスタンスタイプ ( <b>BYOL</b> のみ)
Cisco IOS XE 17.14.1a	<b>N1</b> : n1-standard-8、 n1-standard-4
Cisco IOS XE 17.13.1a	<b>N1</b> : n1-standard-8、 n1-standard-4
Cisco IOS XE 17.12.4b Cisco IOS XE 17.12.4a	<b>N1</b> : n1-standard-8、 n1-standard-4 <b>N2</b> : n2-standard-8、 n2-standard-4
Cisco IOS XE 17.12.2 Cisco IOS XE 17.12.1a	<b>N1</b> : n1-standard-8、 n1-standard-4
Cisco IOS XE 17.11.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2
Cisco IOS XE 17.10.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2
Cisco IOS XE 17.9.6 Cisco IOS XE 17.9.5f Cisco IOS XE 17.9.5e Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2
Cisco IOS XE 17.8.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2
Cisco IOS XE 17.6.8a Cisco IOS XE 17.6.7 Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2
Cisco IOS XE 17.5.1a	<b>N1</b> : n1-standard-8、 n1-standard-4、 n1-standard-2

Cisco IOS XE リリース	サポートされるインスタンスタイプ (BYOLのみ)
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	<b>N1</b> : n1-standard-8、n1-standard-4、n1-standard-2、n1-standard-1

## Sovereign Cloud でサポートされるインスタンスタイプ

表 5: *Alibaba Cloud* (中国) でサポートされるインスタンス

Cisco IOS XE リリース	インスタンスタイプ (BYOLのみ)
Cisco IOS XE 17.16.1a Cisco IOS XE 17.15.1a Cisco IOS XE 17.14.1a Cisco IOS XE 17.13.1a Cisco IOS XE 17.12.1a Cisco IOS XE 17.11.1a Cisco IOS XE 17.10.1a Cisco IOS XE 17.9.1a Cisco IOS XE 17.8.1a Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.6 Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	<ul style="list-style-type: none"> <li>• ecs.g5.4xlarge</li> <li>• ecs.g5.large</li> </ul>

表 6: AWS (中国) でサポートされるインスタンス

Cisco IOS XE リリース	インスタンスタイプ (BYOL のみ)
Cisco IOS XE 17.16.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>
Cisco IOS XE 17.15.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>
Cisco IOS XE 17.14.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>
Cisco IOS XE 17.13.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>
Cisco IOS XE 17.12.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>
Cisco IOS XE 17.11.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>
Cisco IOS XE 17.10.1a	<ul style="list-style-type: none"> <li>• t3.medium</li> <li>• c4.large</li> <li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li> </ul>

Cisco IOS XE リリース	インスタンスタイプ (BYOL のみ)
Cisco IOS XE 17.9.1a	<ul style="list-style-type: none"><li>• t3.medium</li><li>• c4.large</li><li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li></ul>
Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.6 Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	<ul style="list-style-type: none"><li>• t3.medium</li><li>• c4.large</li><li>• c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large</li></ul>



## 第 6 章

# VMware ESXi 環境でのインストール

仮想マシンの基本的な作成と管理を可能にするハイパーバイザである VMware ESXi は、Cisco Catalyst 8000V によってサポートされるハイパーバイザの 1 つです。このハイパーバイザは、仮想化拡張機能を含む x86 ハードウェア上で動作します。同じハイパーバイザを使用して複数の VM を同時に実行できます。

Cisco IOS XE 17.12.1 リリース以降、Cisco Catalyst 8000V は、VMware ESXi 7.0.x 上の Intel x550 NIC を搭載した Intel Atom® C3000 プロセッサ (Denverton) CPU ベースのサーバーでサポートされます。異なるバージョンのハイパーバイザオペレーティングシステムを使用する他の x86 CPU で Cisco Catalyst 8000V を実行できますが、サポートは VMware ESXi 7.0.x でのみ使用できます。

この章では、ESXi での Cisco Catalyst 8000V の展開方法と、展開を成功させるための要件について説明します。要件と展開手順を読む前に、ESXi ハイパーバイザのさまざまな展開方法を示す次の情報を参照してください。



**注意** ホストリソースのオーバーサブスクリプションは、パフォーマンスの低下につながり、インスタンスが不安定になる可能性があります。ホストハイパーバイザに関するガイドラインとベストプラクティスに従うことを推奨します。

### VM に OVA テンプレートを展開します。

**OVA ファイルを使用した展開：**この方法では、ソフトウェアダウンロードページから .ova ファイルをダウンロードし、このファイルを展開に使用する必要があります。さらに、次の 2 つの方法を使用して OVA ファイルを展開できます。

- **vSphere クライアントを使用した展開：**この手順では、VMware vSphere クライアントまたは vSphere Web クライアントを使用して \*.ova インストールファイルを展開する必要があります。VMware vSphere Web クライアントは、仮想拡張を含む x86 ハードウェア上で実行され、VMware vCenter サーバーにアクセスする Web アプリケーションです。VMware vSphere Web クライアントソフトウェアを使用して、VMware vCenter サーバー上で VM を作成、設定、管理したり、Cisco Catalyst 8000V インスタンスを起動または停止したりすることができます。



(注) Cisco Catalyst 8000V の展開にはこの方法を推奨します。

- **共通 OVF ツール (COT) を使用した展開** : COT は、Cisco Catalyst 8000V などの仮想アプリケーションを編集できるツールです。このツールを使用して、.ova ファイルを ESXi サーバーに展開し、VM をプロビジョニングすることもできます。

VMware vSphere 製品の詳細については、[VMware 製品のマニュアル](#)を参照してください。

### .ISO ファイルの手動展開

ESXi ハイパーバイザの 3 番目の展開オプションは、.iso ファイルを使用した VM の手動作成と Cisco Catalyst 8000V のインストールです。シスコのソフトウェアダウンロードページから .iso ファイルをダウンロードし、このファイルをインストールに使用します。この方法では、VMware ESXi ホストに .iso ファイルをインストールし、vSphere GUI を使用して手動で VM を作成します。このオプションは、OVA を変更する場合にのみ使用することをお勧めします。ただし、手動展開ではサポートされている設定から逸脱する可能性があるため、このオプションは推奨されません。



**重要** ESXi 6.5 以降を使用して VM を作成します。VM バージョン 13 以降を使用していることを確認します。EFI ファームウェアモードを選択するには、[VM Options]>[Boot Options]>[Firmware]>[EFI]の順に移動します。セキュアブート機能を有効にするには、このファームウェアモードを選択する必要があります。詳細については、[VNFセキュアブートの有効化 \(145ページ\)](#)を参照してください。



**重要** VM の作成後にファームウェアモードを (BIOS から EFI、またはその逆に) 変更することはできません。

- [VMware 要件 \(56 ページ\)](#)
- [サポートされている VMware 機能と操作 \(59 ページ\)](#)
- [vSphere を使用した VM への OVA の展開 \(63 ページ\)](#)
- [COT を使用した VM への OVA の展開 \(66 ページ\)](#)
- [.iso ファイルを使用した VM の手動作成 \(73 ページ\)](#)
- [VMware ESXi 構成でのパフォーマンスの向上 \(75 ページ\)](#)

## VMware 要件

次のセクションでは、ESXi 環境に Cisco Catalyst 8000V 17.4.1 以降のリリースをインストールするための要件を指定します。これらの要件は完全にテスト済みで、パフォーマンスベンチマークに適合しています。

## ESXi ハイパーバイザの要件

Cisco IOS XE リリース	vSphere Web Client	vCenter Server
Cisco IOS XE 17.16.x リリース Cisco IOS XE 17.15.x リリース Cisco IOS XE 17.14.x リリース Cisco IOS XE 17.13.x リリース Cisco IOS XE 17.12.x リリース	VMware vSphere Web クライアントのバージョン 8.0 および 7.0 がサポートされています。	VMware ESXi 8.0 および ESXi 7.0
Cisco IOS XE 17.11.x リリース Cisco IOS XE 17.10.x リリース Cisco IOS XE 17.9.x リリース Cisco IOS XE 17.8.x リリース Cisco IOS XE 17.7.x リリース Cisco IOS XE 17.6.x リリース	VMware vSphere Web クライアントのバージョン 7.0 および 6.7 がサポートされています。	VMware ESXi 7.0 および ESXi 6.7
Cisco IOS XE 17.5.x リリース	VMware vSphere Web クライアントのバージョン 6.7 および 6.5 がサポートされています。	VMware ESXi 6.7 および ESXi 6.5
Cisco IOS XE 17.4.x リリース	VMware vSphere Web クライアントのバージョン 6.7 および 6.5 がサポートされています。	VMware ESXi 6.7 および ESXi 6.5



- (注) ESXi サーバーの管理にスタンドアロンの vSphere クライアントを使用しないでください。ESXi 6.0 以降では、OVA を展開する場合、Cisco Catalyst 8000V を ESXi に直接展開することはできなくなりました。 .ova ファイルを展開するには、vSphere クライアントが必要です。

## vCPU の要件

次の vCPU 設定がサポートされています。

- 1 vCPU : 最低 4 GB の RAM 割り当てが必要
- 2 vCPU : 最低 4 GB の RAM 割り当てが必要
- 4 vCPU : 最低 4 GB の RAM 割り当てが必要
- 8 vCPU : 最低 4 GB の RAM 割り当てが必要
- 16 vCPU : 最低 8 GB の RAM 割り当てが必要 (Cisco IOS XE 17.11.1a 以降でサポート)



- (注) 必要な vCPU 設定は、インストールされているスループットライセンスとテクノロジーパッケージによって異なります。詳細については、使用中のリリースのデータシートを参照してください。

### vNIC の要件

このセクションに記載されている仮想ネットワーク インターフェイス カード (vNIC) は、ESXi インストールでサポートされています。最大 8 つの vNIC がサポートされます。

- ixgbe : Cisco IOS XE 17.10.1 以降でサポート
- ConnectX-5VF : Cisco IOS XE 17.9.1 以降でサポート
- iavf : Cisco IOS XE 17.9.1 以降でサポート
- i40eVF : Cisco IOS XE 17.4.1 から Cisco IOS XE 17.8.x でサポート
- VMXNET3 : Cisco IOS XE 17.4.1 以降でサポート
- iXGBEVF : Cisco IOS XE 17.4.1 以降でサポート



- (注) サポートされている NIC ドライバのバージョンとファームウェアのバージョンは、ハイパーバイザパッケージに含まれているデフォルトのバージョンです。

### その他の要件

- VMware vCenter : インストールツール
- VMware vSwitch : 標準または分散型の vSwitch がサポートされています
- ハードドライブ : 単一のハードディスクドライブのみがサポートされています。1 台の VM 上で複数のハードディスクドライブはサポートされません
- 仮想ディスク : 16 GB と 8 GB 両方の仮想ディスクがサポートされています
- 仮想 CPU コア : 1 つの仮想 CPU コアが必要です。これには、ホストマシンの BIOS セットアップで仮想化テクノロジー (VT) が有効にされた 64 ビットプロセッサが必要です。
- 仮想ハードディスク領域 : 最小 8 GB のサイズが必要です
- このインストールには、デフォルトのビデオ、SCSI コントローラセット、およびインストール済みの仮想 CD/DVD ドライブも必要です。

### 次のステップ

インストールを進める前に、セキュアブート設定についてよく理解しておいてください。セキュアブートの詳細については、[VNFセキュアブートの有効化 \(145ページ\)](#) を参照してください。

## サポートされている VMware 機能と操作

VMware では、仮想アプリケーションを管理したり、複製、移行、シャットダウン、復帰などの操作を実行したりするためのさまざまな機能と操作がサポートされています。

これらの操作の一部では、VM の実行時状態が保存され、再起動時に復元されます。ランタイム状態にトラフィック関連の状態が含まれている場合、ランタイム状態を再開または再生すると、追加のエラー、統計情報、またはメッセージがユーザーのコンソールに表示されます。設定のみに基づいて回復される保存状態の場合は、これらの機能と動作を問題なく使用できます。

「サポートされている VMware 機能と操作：ストレージオプション (vCenter Server と vSphere Client の両方)」の表に、Cisco Catalyst 8000V でサポートされる VMware の機能と操作を示します。VMware の機能と操作の詳細については、[VMware のマニュアル](#) を参照してください。

Cisco Catalyst 8000V のすべてのバージョンで次の VMware 機能および動作はサポートされていませんが、パケットのドロップ、接続の切断、およびその他のエラー統計が発生するリスクを承知の上であれば、サポート対象外のバージョンでも使用および実行できます。

- 分散リソース スケジューリング (DRS)
- 耐障害性
- 再開
- スナップショット
- 一時停止

## 一般的な機能 (vCenter サーバー)

表 7: サポートされている VMware 機能および操作：一般機能 (vCenter Server のみ)

サポートされているエンティティ	説明
複製	仮想マシンまたはテンプレートを複製したり、仮想マシンをテンプレートに複製したりできます。
移行	データストレージがまだ共有ストレージの同じ場所にある間でも、仮想マシンの状態全体および必要に応じた設定ファイルが新しいホストに移動されます。
VMotion	VM の実行中に、ある物理サーバから別の物理サーバに VM を移動できます。

## 操作 (vCenter サーバーおよび vSphere Web クライアントの場合)

サポートされているエンティティ	説明
テンプレート	テンプレートを仮想マシンとして複製することにより、テンプレートを使用して新しい仮想マシンを作成します。

## 操作 (vCenter サーバーおよび vSphere Web クライアントの場合)

表 8: サポートされている VMware 機能と操作 : 操作 (vCenter Server および vSphere Client の場合)

サポートされているエンティティ	説明
電源オン	仮想マシンの電源を投入し、ゲストオペレーティングシステムがインストールされている場合はゲストオペレーティングシステムをブートします。
電源オフ	電源が再度オンになるまで仮想マシンを停止します。電源オフオプションは、「強制」電源オフを行います。これは、物理マシンの電源コードを引き抜くことに相当し、常に機能します。
シャットダウン	シャットダウン（「安全な」電源オフ）は、VMware ツールを使用してゲストオペレーティングシステムのグレースフルシャットダウンを実行します。特定の状況（VMware ツールがインストールされていない場合や、ゲストオペレーティングシステムが停止している場合など）では、正常にシャットダウンできないことがあり、電源オフオプションを使用する必要があります。
一時停止	仮想マシンを一時停止します。
リセット/再起動	仮想マシンを停止し、再起動（リブート）します。
OVF の作成	ディレクトリ内の複数のファイルで構成される OVF パッケージは、圧縮形式で保存されたディスクファイルを含む仮想マシンの状態をキャプチャします。OVF パッケージをローカルコンピュータにエクスポートできます。
OVA の作成	OVF パッケージ/テンプレートから 1 つの OVA パッケージファイルを作成できます。そうすると、OVA の配布が容易になります。たとえば、Web サイトからダウンロードしたり、USB キーを介して移動したりすることができます。

表 9: サポートされている VMware 機能と操作 : ネットワーク機能

サポートされているエンティティ	説明
カスタム MAC アドレス	vCenter Server と vSphere Client の両方から。仮想ネットワークアダプタの MAC アドレスを手動で設定できます。

サポートされているエンティティ	説明
分散 vSwitch	vCenter Server からのみ。vCenter Server データセンター上の 1 台の vSphere 分散型スイッチで、データセンターのすべての関連ホストに対するネットワークトラフィックを処理できます。
分散リソース スケジューラ	ホスト間の自動ロード バランシングを提供します。
NIC ロード バランシング	vCenter Server と vSphere Client の両方から。ロード バランシング ポリシーとフェールオーバー ポリシーにより、アダプタが故障した場合に、アダプタ間でネットワークトラフィックを分散する方法と、トラフィックを再ルーティングする方法を指定できます。
NIC チーミング	vCenter Server と vSphere Client の両方から。各仮想スイッチが NIC チームを形成する 2 個のアップリンク アダプタに接続する環境をセットアップできます。これにより、NIC チームでは、メンバーの一部または全体をまたがって、物理ネットワークと仮想ネットワーク間のトラフィックの負荷を共有するか、ハードウェア障害やネットワーク障害の発生時にパッシブ フェールオーバーを提供します。  (注) NIC チーミングにより、多数の ARP パケットが Cisco Catalyst 8000V にフラッディングし、CPU が過負荷になるおそれがあります。この状況を回避するには、ARP パケットの数を減らし、アクティブ-アクティブではなく、アクティブ-スタンバイとして NIC チーミングを実装します。
vSwitch	vCenter Server と vSphere Client の両方から。vSwitch はレイヤ 2 物理スイッチの仮想化バージョンです。vSwitch では、仮想マシン間でトラフィックを内部的にルーティングでき、外部ネットワークにリンクできます。vSwitch を使用すると、複数ネットワーク アダプタの帯域幅を組み合わせ、このアダプタ間で通信トラフィックを分散できます。物理 NIC フェールオーバーを処理するように vSwitch を設定することもできます。

## 高可用性



- (注) Cisco IOS ベースの高可用性は、Cisco Catalyst 8000V インスタンスではサポートされていません。高可用性は、VM ホストでのみサポートされます。

## ストレージオプション (vCenter サーバーおよび vSphere Web クライアントの場合)

表 10: サポートされている VMware 機能および操作 : ハイ アベイラビリティ

サポートされているエンティティ	説明
VM レベルのハイ アベイラビリティ	オペレーティング システムの障害をモニタするために、VM レベルのハイアベイラビリティでは、VMware ハイアベイラビリティ クラスタのハートビート情報をモニタします。ユーザ指定の間隔までに、指定した仮想マシンからハートビートが受信されていないと、障害が検出されます。VM レベルのハイアベイラビリティは、VMware vCenter Server を使用して VM のリソース プールを作成することによって有効化されます。
ホストレベルのハイアベイラビリティ	物理サーバをモニタするために各サーバ上のエージェントでは、ハートビートが失われたときに、リソース プール内の他のサーバにある影響を受けるすべての仮想マシンの再起動を自動的に開始できるように、リソース プール内の他のサーバとのハートビートを維持します。ホストレベルのハイアベイラビリティは、サーバまたはホストのリソース プールを作成し、vSphere でハイアベイラビリティを有効にすることによって有効になります。
耐障害性	ハイアベイラビリティを使用することで、ESXi ホストの耐障害性が有効になります。Cisco Catalyst 8000V ルータを実行する VM の耐障害性を有効にすると、クラスタ内の別のホストにセカンダリ VM が作成されます。プライマリホストが停止すると、セカンダリホストの VM が Cisco Catalyst 8000V のプライマリ VM を引き継ぎます。

## ストレージオプション (vCenter サーバーおよび vSphere Web クライアントの場合)

表 11: サポートされている VMware 機能と操作 : ストレージオプション (vCenter Server と vSphere Client の両方)

サポートされているエンティティ	説明
ストレージオプション (vCenter Server および vSphere Client の両方)	
ローカルストレージ	ローカルストレージは ESXi ホスト内にある内部ハードディスクにあります。ローカルストレージデバイスは複数ホストにまたがる共有をサポートしません。ローカルストレージデバイス上のデータストアは 1 台のホストによってのみアクセスできます。

サポートされているエンティティ	説明
外部ストレージ ターゲット	外部ストレージに Cisco Catalyst 8000V インスタンスを展開できます。この外部ストレージとは、ストレージエリア ネットワーク (SAN) のことです。
USB ストレージのマウントまたはパススルー	<p>Cisco Catalyst 8000V に USB スティックを接続し、ストレージデバイスとして使用できます。ESXi では、USB コントローラを追加し、Cisco Catalyst 8000V にディスクデバイスを割り当てる必要があります。</p> <ul style="list-style-type: none"> <li>• Cisco Catalyst 8000V はホットプラグをサポートしています。</li> <li>• 一度に使用できる USB ディスクのホットプラグ対応デバイスは、2 台のみです。</li> <li>• USB ハブはサポートされていません。</li> </ul>

## vSphere を使用した VM への OVA の展開

Cisco Catalyst 8000V OVA ファイルパッケージを使用して、Cisco Catalyst 8000V を VM に展開できます。OVA パッケージには、Cisco IOS XE リリースとサポート対象のハイパーバイザに基づいたデフォルトの VM 設定が入っている OVF ファイルが含まれています。

### 制限事項および要件

OVA パッケージを VM に展開する場合は、次の制限事項が適用されます。

仮想 CPU 設定を変更した場合は、Cisco Catalyst 8000V インスタンスをリブートする必要があります。RAM 割り当ての変更では、Cisco Catalyst 8000V インスタンスをリブートする必要はありません。

OVA パッケージには、仮想 CPU 設定を選択するオプションがあります。

OVA を展開する場合、VM には、OVF 環境ファイル用に 1 台と .iso ファイル用に 1 台の合計 2 台の仮想 CD/DVD ドライブが必要です。

### VM への OVA の展開

VMware vSphere クライアントで次の手順を実行します。

## 手順

- ステップ 1** VMware vSphere Client にログインします。
- ステップ 2** [vSphere Client] メニューバーから、[File] > [Deploy OVF Template] を選択します。
- ステップ 3** OVA ウィザードで、展開する Cisco Catalyst 8000V OVA の送信元を指定します。[Next] をクリックします。
- OVA に関する情報を示す [OVF Template Details] が表示されます。[Next] をクリックします。
- ステップ 4** [Name and Inventory Location] で、VM の名前を指定し、[Next] をクリックします。
- ステップ 5** [Deployment Configuration] で、ドロップダウンメニューから必要なハードウェア設定プロファイルを選択し、[Next] をクリックします。
- ステップ 6** [Storage] で、VM に使用するデータストアを選択します。[Next] をクリックします。
- ステップ 7** [Disk Format] で、ディスクフォーマットのオプションを選択します。

- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed

(注)

[Thin Provision] オプションはサポートされていません。[Thick Provision Eager Zeroed] オプションを指定すると、インストールに時間がかかりますが、優れたパフォーマンスを得られます。

[Next] をクリックします。

- ステップ 8** [Network Mapping] で、ドロップダウンリストを使用して、宛先ネットワーク上に 1 つ以上の仮想ネットワーク インターフェイス カード (vNIC) を割り当てます。

OVA の展開時に作成された 3 つのデフォルト vNIC のネットワークマッピングを選択します。ブートストラッププロパティを設定するときに、ルータの管理インターフェイスにマッピングする vNIC を選択できます。

(注)

ブートストラッププロパティを変更すると、システムはユーザーが新規の VM を開始しようとしていると判断します。そのため、VM を再起動すると、既存のネットワーク設定がすべて削除されます。

- ステップ 9** [Power On] 時に接続する vNIC を選択します。[Next] をクリックします。

OVA テンプレートを使用した Cisco Catalyst 8000V のインストールが完了すると、追加の 2 つの vNIC が割り当てられます。Cisco Catalyst 8000V は最大 10 の vNIC をサポートします。VM で追加の vNIC を手動で作成する必要があります。

- ステップ 10** VM のプロパティを設定します。

(注)

ブートストラッププロパティを変更すると、システムはユーザーが新規の VM を開始しようとしていると判断します。そのため、VM を再起動すると、既存のネットワーク設定がすべて削除されます。

(注)

VM 作成時のブートストラッププロパティはオプションです。これらのプロパティを設定して、起動する前の VM を簡単にプロビジョニングできます。

表 12: OVA ブートストラップのプロパティ

プロパティ	説明
ブートストラップのプロパティ	
コンソール	コンソールモードを設定します。 設定可能な値 : virtual、serial
Login Username	ルータのログインユーザー名を設定します。
ログインパスワード (Login Password)	ルータのログインパスワードを設定します。
管理インターフェイス	Cisco Catalyst 8000V インスタンスの管理インターフェイスを指定します。形式は GigabitEthernetx または GigabitEthernetx.xxx である必要があります。 (注) GigabitEthernet0 インターフェイスはサポートされなくなりました。
管理 vVLAN	dot1Q VLAN インターフェイスを設定します。GigabitEthernetx.xxx 形式を使用して管理インターフェイスを設定する必要があります。
管理インターフェイス IPv4 アドレス/マスク	管理インターフェイスの IPv4 アドレスとサブネットマスクを設定します。
Management IPv4 Default Gateway	IPv4 管理デフォルトゲートウェイアドレスを設定します。DHCP を使用する場合は、フィールドに「dhcp」と入力します。
管理 IPv4 ゲートウェイ	IPv4 管理デフォルトゲートウェイアドレスを設定します。DHCP を使用する場合は、フィールドに「dhcp」と入力します。
管理 IPv4 ネットワーク	管理ゲートウェイがルーティングする IPv4 ネットワーク（「192.168.2.0/24」や「192.168.2.0 255.255.255.0」など）を設定します。デフォルトルート（0.0.0.0/0）が必要な場合は、空白のままにすることができます。
PNSC IPv4 アドレス	Cisco Prime Network Services Controller の IP アドレスを設定します。 この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V インスタンスをリモートで管理する場合に使用されます。
ルータ名	ルータのホスト名を設定します。
リソーステンプレート	リソーステンプレートを設定します。 設定可能な値 : default、service_plane_medium、service_plane_heavy
機能	

プロパティ	説明
SCP サーバーの有効化	IOS SCP 機能を有効にします。
SSH ログインの有効化と Telnet ログインの無効化	SSH を使用したリモートログインを有効にし、Telnet を介したリモートログインを無効にします。ログインユーザー名とパスワードを設定する必要があります。
追加の設定プロパティ	
Enable Password	特権（有効化）アクセス用のパスワードを設定します。
Domain Name	ネットワークドメイン名を設定します。
License Boot Level	<p>Cisco Catalyst 8000V インスタンスの起動時に使用可能なライセンス テクノロジー レベルを設定します。使用可能なライセンスレベルは次のとおりです。</p> <ul style="list-style-type: none"> <li>• network-essentials</li> <li>• network-advantage</li> <li>• network-premier</li> </ul> <p>(注) Cisco DNA ライセンスの詳細については、『<a href="#">Cisco DNA Software for SD-WAN and Routing</a>』を参照してください。</p>

ルータプロパティの設定を完了したら、[Next] をクリックします。テンプレートを展開するときに表示される設定を示す [Ready to Complete] 画面が表示されます。

ルータのブート後に、詳細プロパティも設定できます。

**ステップ 11** VM の電源を自動的にオンにするには、[Power On After Deployment] を選択します。

**ステップ 12** [Finish] をクリックして OVA を展開します。

OVA により .iso ファイルが展開され、[Power On After Deployment] 設定が選択されている場合は VM の電源が自動的にオンになります。VM の電源がオンになると、Cisco Catalyst 8000V デバイスによりインストールおよび起動プロセスが開始されます。ブートストラップ設定ファイルが OVA に含まれている場合は、ルータ設定が自動的に有効化されます。

詳細については、『[Booting the Cisco Catalyst 8000V and Accessing the Console](#)』を参照してください。

## COT を使用した VM への OVA の展開

Cisco Catalyst 8000V OVA ファイルパッケージを使用して、Cisco Catalyst 8000V を VM に展開できます。OVA パッケージには、Cisco IOS XE リリースとサポート対象のハイパーバイザに基づいたデフォルトの VM 設定が入っている OVF ファイルが含まれています。VMware vSphere

または COT または共通 OVF ツールを使用して OVA を展開できます。このセクションでは、COT を使用した展開方法について説明します。

共通 OVF ツールは、1 つ以上の VM の属性を作成し、Cisco Catalyst 8000V ソフトウェアをブレインストールして VM を迅速に展開できる、Cisco Catalyst 8000V ソフトウェアパッケージに含まれる Linux ベースのアプリケーションです。このツールを使用すると、複数の VM に Cisco Catalyst 8000V を展開するプロセスを高速化できます。

COT は、.ova ファイルに VM の属性を入力するためのシンプルなコマンドラインインターフェイスを提供します。COT は Linux シェルと Mac OS X のどちらでも実行できます。ただし、VMware OVF ツールがインストールされていることを確認してください。



---

**危険** 共通 OVF ツール (COT) は、シスコの正式なサポートなしで提供されます。自己責任で使用してください。

---

## COT のダウンロード

<http://cot.readthedocs.io/en/latest/installation.html> GitHub サイトに示されている手順に従って、COT ライブラリとスクリプトをダウンロードしてインストールします。

## COT を使用した Cisco Catalyst 8000V の基本的なプロパティの編集

COT を使用して Cisco Catalyst 8000V を展開する前に、COT を使用して OVA パッケージの Cisco Catalyst 8000V VM の基本プロパティまたはカスタムプロパティを編集できます。

OVA の基本プロパティを編集するには、**cot edit-properties** コマンドを使用します。

### **cot edit-properties**

**-p key1=value1, --properties key1=value1**

このコマンドは、キーと値のペアを使用してプロパティを設定します。たとえば、**-p "login-username=cisco"** は、キーと値のペアを使用してログインユーザー名を設定します。

**-o output**

既存の OVA を更新する代わりに新しい OVA を作成する場合は、新しい OVA パッケージの名前またはパスを指定します。

**cot edit-properties** コマンドの詳細については、[http://cot.readthedocs.io/en/latest/usage\\_edit\\_properties.html](http://cot.readthedocs.io/en/latest/usage_edit_properties.html) を参照してください。

### COT を使用した Cisco Catalyst 8000V の基本プロパティの編集 (サンプル)

```
cot edit-properties c8000v-universalk9.ova
-p "login-username=cisco"

-p "login-password=cisco"
-o c8000v-universalk9-customized.ova
```

```

\# save modifications to a new OVA
cot info c8000v-universalk9-customized.ova
# verify the new values of properties in the OVA
(...)
Properties:
  <config-version>                "1.0"
  Router Name                      ""
  Login Username                   "cisco"
  Login Password                   "cisco"
  Management Interface             "GigabitEthernet1"
  Management VLAN                  ""
  Management Interface IPv4 Address/Mask ""

```

次の表に、上記の例で使用される `cot edit-properties` コマンドと引数を示します。

スクリプトステップ	説明
<code>cot edit properties c8000v-universalk9.ova</code>	OVA ファイルの基本的な環境プロパティを編集します。
<code>-p "login-username=cisco"</code>	ブートストラップログインユーザー名を設定します。
<code>-p "login-password=cisco"</code>	ブートストラップログインパスワードを設定します。
<code>-o "c8000v-universalk9-customized.ova"</code>	テキストファイルからの設定コマンドを含む、変更された OVA を保存します。

## カスタムプロパティの編集

vSphere GUI を使用して、Cisco IOS XE CLI コマンドに基づくカスタム属性を Cisco Catalyst 8000V インスタンスに追加できます。Cisco Catalyst 8000V インスタンスの起動前または後に、これらのプロパティを追加できます。Cisco Catalyst 8000V インスタンスの起動後にこれらのカスタム属性を設定した場合、プロパティ設定を有効にするには、ルータをリロードするか、VM の電源を再投入する必要があります。

vApp オプションを編集してカスタム Cisco Catalyst 8000V プロパティを追加するには、以下の手順を実行します。

### 手順

- ステップ 1 vSphere GUI で [Options] タブを選択します。
- ステップ 2 [vApp Options] > [Advanced] を選択します。
- ステップ 3 [Advanced Property Configuration] 画面で、[Properties] ボタンをクリックします。
- ステップ 4 プロパティを追加するには、[New] をクリックします。
- ステップ 5 [Edit Property Settings] 画面で、Cisco IOS XE CLI コマンドに基づく新しいカスタムプロパティを作成するための情報を入力します。

(注)

カスタムプロパティを追加する前に、カスタムプロパティの基になる Cisco IOS XE コマンドが、使用中の Cisco Catalyst 8000V バージョンでサポートされていることを確認します。

- a) (任意) ラベルを入力します。これはプロパティを説明する文字列です。
- b) クラス ID として「com.cisco.c8000v」と入力します。
- c) ID「ios-config-xxxx」をプロパティに割り当てます。「xxxx」は、カスタムプロパティを適用する順序を決定する 0001 ~ 9999 のシーケンス番号です。
- d) (任意) プロファイルの説明を入力します。
- e) プロパティタイプとして「string」と入力します。これは、サポートされる唯一のタイプです。
- f) デフォルト値として、カスタムプロパティが基にする Cisco IOS XE CLI コマンドを入力します。

**ステップ 6** [OK] をクリックします。

**ステップ 7** [Advanced Property Configuration] 画面で、[OK] をクリックします。

**ステップ 8** Cisco Catalyst 8000V インスタンスを再起動します。

新規または編集されたプロパティを有効にするには、ルータを再起動する必要があります。

## cot edit-properties

少数の設定コマンドを OVA に事前適用するには、**cot edit-properties** コマンドを使用します。

もっと多くのコマンドを使用するには、**cot inject-config** コマンドを使用します。

**cot edit-properties** コマンドの詳細については、  
[http://cot.readthedocs.io/en/latest/usage\\_edit\\_properties.html](http://cot.readthedocs.io/en/latest/usage_edit_properties.html) を参照してください。

### 概要と説明

**cot edit-properties** *ova-filename*

**-o** *output*

既存の OVA を更新する代わりに新しい OVA を作成する場合は、新しい OVA パッケージの名前またはパスを指定します。

**-c** *config-file*

OVA に追加する IOS XE コマンドを含むテキストファイルの名前を指定します。

### 例

この例では、以前に作成されたテキストファイル `iosxe_config.txt` (IOS XE config コマンドを含む) が、**cot edit-properties** コマンドを使用して OVA に追加されます。最後に、**cot info** コマンドを使用して、変更された OVA を表示します。

```
$ cat iosxe_config.txt

interface GigabitEthernet1
no shutdown
ip address 192.168.100.10 255.255.255.0
```

```

!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.100.1
$ cot edit-properties c8000v-universalk9.ova \
  -o c8000v-universalk9-customized.ova \
  -c iosxe_config.txt
$ cot info c8000v-universalk9-customized.ova

...

Properties:
  <config-version>          "1.0"
  Router Name               ""

...

Intercloud Tunnel Interface Gateway IPv4 Address  ""
<ios-config-0001>          "interface GigabitEthernet1"
<ios-config-0002>          "no shutdown"
<ios-config-0003>          "ip address 192.168.100.10 255.255.255.0"
<ios-config-0004>          "ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.100.1"

```

次の表に、この例で使用する **cot edit properties** コマンドと引数を示します。

スクリプトステップ	説明
<pre> cot edit properties c8000v-universalk9.ova </pre>	OVA ファイルのカスタム環境プロパティを編集します。
<pre> -o "c8000v-universalk9-customized.ova" </pre>	テキストファイルからの設定コマンドを含む新しい OVA。
<pre> -c iosxe_config.txt </pre>	IOS XE 設定コマンドを含むテキストファイル。このファイルに含まれる各行の設定により、OVF の XML で <code>com.cisco.productname.ios-config-xxxx</code> などのエントリが生成されます。

## cot inject-config

OVA に事前適用する設定コマンドが多数ある場合は、**cot inject-config** コマンドを使用します。たとえば、完全な実行コンフィギュレーションを追加する場合に使用します。このコマンドは、設定コマンドに（XML の代わりに）プレーンテキストを使用するため、ファイルサイズとロード時間の点で効率的です。**cot inject-config** コマンドの詳細については、[http://cot.readthedocs.io/en/latest/usage\\_inject\\_config.html](http://cot.readthedocs.io/en/latest/usage_inject_config.html) を参照してください。

### 概要と説明

**cot inject-config ova-filename**

**-o output**

既存の OVA を更新する代わりに新しい OVA を作成する場合は、新しい OVA パッケージの名前またはパスを指定します。

**-c config-file**

OVA に埋め込むテキストファイルの名前 (iosxe\_config.txt など) を指定します。

### 例

この例では、**cot inject-config** コマンドがテキストファイル iosxe\_config.txt の Cisco IOS XE コマンドを OVA に追加します。

```
$ cat iosxe_config.txt
interface GigabitEthernet1
no shutdown
ip address 192.168.100.10 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.100.1
$ cot inject-config c8000v-universalk9.ova \

-o c8000v-universalk9-customized.ova \
  -c iosxe_config.txt
$ cot info c8000v-universalk9-customized.ova
```

<..簡潔にするために、その他の出力が省略されています..>

Files and Disks:	File Size	Capacity	Device
c8000v_harddisk.vmdk	71.50 kB	8.00 GB	harddisk @ SCSI 0:0
bdeo.sh	52.42 kB		
README-OVF.txt	8.53 kB		
README-BDEO.txt	6.75 kB		
cot.tgz	116.78 kB		
c8000v-universalk9.iso	484.80 MB		cdrom @ IDE 1:0
config.iso	350.00 kB		cdrom @ IDE 1:1

次の表に、この例で使用する **cot inject-config** コマンドと引数を示します。

スクリプトステップ	説明
<code>cot inject-config c8000v-universalk9.ova</code>	OVA ファイルのカスタム環境プロパティを編集します。
<code>-o "c8000v-universalk9-customized.ova"</code>	テキストファイルからの <code>config</code> コマンドを含む、新規または変更された OVA の名前。
<code>-c iosxe_config.txt</code>	IOS XE 設定コマンドを含むテキストファイルの名前。

## COT を使用した Cisco Catalyst 8000V VM の展開

Cisco Catalyst 8000V VM を展開するには、次の手順に示すように **cot deploy ... esxi** コマンドを使用します。以下の説明は一般的なガイダンスを示していることに注意してください。実行する必要のある正確な手順は、VMware 環境と設定の特性に応じて異なる場合があります。

## 手順

**cot deploy ... esxi** コマンドを実行して Cisco Catalyst 8000V を展開します。スクリプトオプションについては、[http://cot.readthedocs.io/en/latest/usage\\_deploy\\_esxi.html](http://cot.readthedocs.io/en/latest/usage_deploy_esxi.html) を参照してください。

(注)

デフォルト値は、Cisco Catalyst 8000V のバージョンによって異なります。

## 例

次の表に、vCenter 環境での Cisco Catalyst 8000V VM の展開に使用する **cot deploy** コマンドとその引数の例を示します。

スクリプトステップ	説明
<code>cot deploy</code>	
<code>-s '10.122.197.5/UCS/host/10.122.197.38'</code>	vCenter サーバー 10.122.197.5、ターゲットホスト UCS/ホスト/10.122.197.38
<code>-u administrator -p password</code>	ESXi サーバーのログイン情報。指定しない場合、COT はユーザー ID を使用し、パスワードの入力を求めます。
<code>-n XE3.13</code>	新しく作成された Cisco Catalyst 8000V VM の名前。
<code>-c 1CPU-4GB</code>	OVF ハードウェア設定プロファイル。これが指定されていない場合、COT は使用可能なプロファイルのリストを表示し、プロファイルを選択するように求めます。
<code>-N "GigabitEthernet1=VM Network"</code> <code>-N "GigabitEthernet2=VM Network"</code> <code>-N "GigabitEthernet3=VM Network"</code>	Cisco Catalyst 8000V OVA の各 NIC をサーバーの vSwitch にマッピングします。
<code>esxi</code>	ターゲットハイパーバイザ（現在は常に ESXi）
<code>~/Downloads/c8000v-universalk9.ova</code>	展開する OVA
<code>-ds=datastore38a</code>	ESXi 固有のパラメータ（ここでは、ディスクストレージ用に使用するデータストア）。

## .iso ファイルを使用した VM の手動作成

以下の手順に従って、VMware ESXi ホストに .iso ファイルをインストールし、vSphere GUI を使用して手動で VM を作成します。この手順には、Cisco Catalyst 8000V の展開に関する一般的なガイドラインが記載されていますが、実行する必要がある正確な手順は、使用中の VMware 環境と設定の特性によって異なる可能性があります。この手順に含まれる指示は、VMware ESXi 5.0 に基づいています。

### 手順

- ステップ 1 Cisco Catalyst 8000V ソフトウェア インストール イメージ パッケージから C8000V\_esxi.iso ファイルをダウンロードし、VM データストアにコピーします。
- ステップ 2 vSphere クライアントで、[Create a New Virtual Machine] オプションを選択します。
- ステップ 3 [Configuration] で、カスタム設定を作成するオプションを選択して [Next] をクリックします。
- ステップ 4 [Name and Location] で、VM の名前を指定して [Next] をクリックします。
- ステップ 5 [Storage] で、VM に使用するデータストアを選択します。[Next] をクリックします。
- ステップ 6 [Virtual Machine Version] フィールドで、[Virtual Machine Version 15] またはそれ以降の使用可能なバージョンを選択します。[Next] をクリックします。

(注)

Cisco Catalyst 8000V には、6.5 Update 2 より前のバージョンの ESXi サーバーとの互換性がありません。

- ステップ 7 [Guest Operating System] で、[Linux] を選択し、ドロップダウンメニューから [Other 3.x Linux (64-bit)] 設定を選択します。[Next] をクリックします。
- ステップ 8 [CPU] の下で、次の設定を選択します。
  - 仮想ソケット (仮想 CPU) の数
  - ソケットあたりのコア数

ソケットごとのコアの数は、選択されている仮想ソケットの数に関係なく、常に [1] に設定する必要があります。たとえば、4 vCPU 構成の Cisco Catalyst 8000V では 4 ソケット、ソケットあたり 1 コアとして設定する必要があります。

[Next] をクリックします。

- ステップ 9 [Memory] で、**Cisco Catalyst 8000V** リリースでサポートされるメモリサイズを設定します。[Next] をクリックします。
- ステップ 10 [Network] で、少なくとも 3 つの仮想ネットワーク インターフェイス カード (vNIC) を割り当てます。
  - a) 接続する vNIC の数をドロップダウンメニューから選択します。

(注)

VMware ESXi インターフェイスでは、最初の VM の作成中は、vNIC を 4 個だけ作成できます。VM が作成され、Cisco Catalyst 8000V を最初に起動した後に、vNIC をさらに追加できます。

- b) vNIC を追加します。

各 vNIC に異なるネットワークを選択します。

ドロップダウンメニューからアダプタタイプを選択します。使用中のリリースでサポートされているアダプタタイプについては、本ガイドの要件のセクションを参照してください。

- c) すべての vNIC を選択して電源投入時に接続します。  
d) [Next] をクリックします。

(注)

Cisco Catalyst 8000V の実行中に、vSphere を使用して vNIC を VM に追加することができます。既存の VM に vNICs を追加する方法の詳細は、vSphere のマニュアルを参照してください。

**ステップ 11** [SCSI Controller] で、[VMware Paravirtual] を選択します。[Next] をクリックします。

**ステップ 12** [Select a Disk] で、[Create a New Virtual Disk] をクリックします。

**ステップ 13** [Create a Disk] フィールドで、以下の項目を設定します。

- a) [Capacity: Disk Size] : 使用中のリリースに必要な仮想ハードディスクサイズについては、本ガイドの要件のセクションを参照してください。  
b) [Disk Provisioning] : [Thick Provision Lazy Zeroed] または [Thick Provision Eager Zeroed] のいずれかを選択します。

(注)

[Thin Provision] オプションはサポートされていません。[Thick Provision Eager Zeroed] オプションを指定すると、インストールにかかる時間が長くなりますが、優れたパフォーマンスが得られます。

- c) [Location] : 仮想マシンと同じ場所に保存します。

[Next] をクリックします。

**ステップ 14** [Advanced Options] フィールドで、仮想デバイスノード用に [SCSI (0:0)] を選択します。

**ステップ 15** [Ready to Complete] 画面で、完了前の [Edit the Virtual Machine] 設定をクリックします。[Continue] チェックボックスをオンにします。

**ステップ 16** [Hardware] タブで、[New CD/DVD Drive] をクリックします。

- a) VM の起動元の [Device Type] を選択します。

.iso ファイルから起動する [Datastore ISO file] オプションを選択します。ステップ 1 で設定したデータストア上の .iso ファイルの場所を参照します。

- b) [Device Status] フィールドで、[Connect at Power On] チェックボックスをオンにします。  
c) VM を起動するホスト上の [Virtual Device Node CD/DVD] ドライブを選択します。

**ステップ 17** [Resources] タブで、[CPU] 設定をクリックします。

[Resource Allocation] 設定を [Unlimited] に設定します。

**ステップ 18** [OK] をクリックします。

**ステップ 19** [Finish] をクリックします。

Cisco Catalyst 8000V 用の VM が設定され、起動する準備が整いました。VM の電源がオンになると Cisco Catalyst 8000V が起動されます。「[Booting the Cisco Catalyst 8000V VM and Accessing the Console](#)」のセクションを参照してください。

(注)

手動でインストールした Cisco Catalyst 8000V にデイゼロを設定するには、上記のブートストラップ設定を含む ISO をポイントする 2 番目の CD/DVD ドライブを接続します。サポートされているブートストラップ ISO の内容の詳細については、[デイゼロ設定 \(111 ページ\)](#) を参照してください。

(注)

仮想 VGA コンソールの代わりに ESXi ホストのシリアルポートから Cisco Catalyst 8000V にアクセスして設定する場合は、VM の電源をオンにしてルータを起動する前に、この設定を使用するよう VM をプロビジョニングします。

## VMware ESXi 構成でのパフォーマンスの向上

ホストと仮想マシンの設定を変更することで、ESXi 環境で実行される Cisco Catalyst 8000V のパフォーマンスを向上させることができます。

- ハイパーバイザのパフォーマンス設定を有効にします。
- サポートされている物理 NIC で SR-IOV を有効にして、vSwitch のオーバーヘッドを制限します。
- 物理 NIC と同じ NUMA ノードで動作するように VM の vCPU を設定します。
- [VM Latency Sensitivity] を [High] に設定します。

VMware バージョン 6.7 および 6.5 でのベストプラクティスの詳細については、[https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/Perf\\_Best\\_Practices\\_vSphere65.pdf](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/Perf_Best_Practices_vSphere65.pdf) と <https://www.vmware.com/techpapers/2019/vsphere-esxi-vcenter-server-67U2-performance-best-practices.html> を参照してください。

### ホスト設定の変更

VMware ESXi 設定のパフォーマンスを向上させるには、ホスト設定で次の変更を行います。

- [Power Management] で [High Performance] オプションを選択します。
- [Hyperthreading] を無効にします。
- サポートされている物理アダプタの SR-IOV を有効にします。

### 仮想マシン設定の変更

VMware ESXi 設定のパフォーマンスを向上させるには、ホスト設定で次の変更を行います。

- ESXi バージョンが使用中の Cisco Catalyst 8000V バージョンと互換性があることを確認します。
- [Virtual Hardware: CPU] の予約を [Maximum] に設定します。
- [Virtual Hardware: Memory] ですべてのゲストメモリを予約します。
- [Virtual Hardware: SCSI Controller] から [VMware Paravirtual] を選択します。
- [Virtual Hardware: Network Adapter: Adapter Type] オプションから、サポートされている NIC の SR-IOV を選択します。
- [General Guest OS Version] > [VM Options] オプションを [Other 3.x or later Linux (64-bit)] に設定します。
- [Advanced Latency Sensitivity] の [VM Options] オプションを [High] に設定します。
- [VM Options] > [Advanced Edit Configuration] で、「numa.nodeAffinity」を SRIOV NIC と同じ NUMA ノードに追加します。



## 第 7 章

# KVM 環境でのインストール

Red Hat Enterprise Linux (RHEL) は、Red Hat が製造するエンタープライズ仮想化製品です。カーネルベース仮想マシン (KVM) をベースとする RHEL 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。

Cisco Catalyst 8000V 仮想ルータを Red Hat KVM 仮想化の仮想マシンとしてインストールできます。インストール手順では、最初に VM を手動で作成します。その後、.iso ファイルまたは qcow2 ファイルを使用したインストールが続きます。次を使用して、KVM 環境に Cisco Catalyst 8000V をインストールできます。

- **GUI ツール** : KVM サーバーに virt-manager RPM パッケージをダウンロードしてインストールします。virt-manager は、仮想マシンを管理するためのデスクトップユーザー インターフェイスです。GUI を使用したインストールは、推奨されるインストール方法です。
- **コマンドライン インターフェイス** : このインストール方法では、コマンドライン インターフェイスを使用して Cisco Catalyst 8000V VM をインストールします。



(注) KVM 環境での OVA テンプレートの展開はサポートされていません。

Cisco Catalyst 8000V は、KVM 実装で Virtio vNIC タイプをサポートします。KVM は最大 26 の vNIC をサポートします。

- [KVM のインストール要件 \(77 ページ\)](#)
- [KVM インスタンスの作成 \(80 ページ\)](#)
- [VM のクローン作成 \(85 ページ\)](#)
- [KVM 構成のパフォーマンスの向上 \(85 ページ\)](#)
- [halt\\_poll\\_ns パラメータの設定 \(89 ページ\)](#)

## KVM のインストール要件

ここでは、Cisco Catalyst 8000V Cisco IOS XE 17.4.x リリース以降を KVM 環境にインストールする場合の要件を指定します。

## RHEL バージョン (Red Hat Enterprise Linux をベースとした Linux KVM)

Cisco IOS XE リリース	Red Hat Enterprise Linux のバージョン
Cisco IOS XE 17.16.x リリース	Red Hat Enterprise Linux 9.2 および 8.10 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.15.x リリース	Red Hat Enterprise Linux 9.2, 8.10 および 8.4 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.14.x リリース	Red Hat Enterprise Linux 9.2, 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.13.x リリース	Red Hat Enterprise Linux 9.2, 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.12.x リリース	Red Hat Enterprise Linux 9.2, 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.11.x リリース	Red Hat Enterprise Linux 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.10.x リリース	Red Hat Enterprise Linux 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.9.x リリース	Red Hat Enterprise Linux 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.8.x リリース	Red Hat Enterprise Linux 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.7.x リリース	Red Hat Enterprise Linux 8.4 および 7.7 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.6.x リリース	Red Hat Enterprise Linux 7.7 および 7.5 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.5.x リリース	Red Hat Enterprise Linux 7.7 および 7.5 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.4.x リリース	Red Hat Enterprise Linux 7.7 および 7.5 をベースとした Linux KVM を推奨。

Cisco IOS XE 17.12.1 リリース以降、Cisco Catalyst 8000V は、RHEL 8.4 KVM ハイパーバイザ上の Intel x550 NIC を搭載した Intel Atom® C3000 プロセッサ (Denverton) CPU ベースのサーバーでもサポートされます。異なるバージョンのハイパーバイザ オペレーティングシステムを使用する他の x86 CPU で Cisco Catalyst 8000V を実行できますが、サポートは KVM のバージョン表のバージョンでのみ使用できます。

**SUSE Linux® Enterprise Server (SLES) バージョン**

Cisco IOS XE リリース	SUSE Linux® Enterprise Server バージョン
Cisco IOS XE 17.16.x リリース	SUSE Linux Enterprise Server バージョン 15 SP5 をサポート
Cisco IOS XE 17.15.x リリース	SUSE Linux Enterprise Server バージョン 15 SP5 をサポート
Cisco IOS XE 17.14.x リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.13.x リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.12.x リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.11.x リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.10.x リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.9.x リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.6.3 リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート

**サポートされている vNIC**

vNIC	サポートされているリリース
Ixgbe	Cisco IOS XE リリース 17.10.1 以降
iavf	Cisco IOS XE リリース 17.9.1 以降
ConnectX-5VF	Cisco IOS XE リリース 17.9.1 以降
i40evf	Cisco IOS XE リリース 17.4.1 から Cisco IOS XE 17.8.x リリース
Virtio	Cisco IOS XE リリース 17.4.1 以降
ixgbevf	Cisco IOS XE リリース 17.4.1 以降



(注) VM インスタンスごとにサポートされる vNIC の最大数は 26 で、最大 16 の SRIOV インターフェイスを含みます。



(注) i40evf ドライバで vNIC を使用する場合、物理 VLAN の最大数は 512 に制限され、すべての VF (仮想機能) で共有されます。VF の VLAN 数は、信頼できない VF のホスト (PF) ドライバによってさらに制限される場合があります。Intel i40e PF ドライバは、信頼されていない VF を最大 8 つの VLAN/サブインターフェイスに制限します。

### サポートされている vCPU 構成

このセクションに記載されている vCPU 構成がサポートされています。

- 1 vCPU : 最低 4 GB の RAM 割り当てが必要
- 2 vCPU : 最低 4 GB の RAM 割り当てが必要
- 4 vCPU : 最低 4 GB の RAM 割り当てが必要
- 8 vCPU : 最低 8 GB の RAM 割り当てが必要
- 16 vCPU : 最低 8 GB の RAM 割り当てが必要 (Cisco IOS XE 17.11.1a 以降でサポート)

## KVM インスタンスの作成

### GUI ツールを使用した VM の作成

#### 始める前に

KVM サーバーに virt-manager RPM パッケージをダウンロードしてインストールします。

シスコのソフトウェアダウンロードページから .qcow2 イメージまたは .iso イメージをダウンロードし、ファイルをローカルデバイスまたはネットワークデバイスにコピーします。

#### 手順

- ステップ 1 virt-manager GUI を起動します。
- ステップ 2 [Create a New Virtual Machine] をクリックします。
- ステップ 3 次のいずれかを実行します。
  - a) .qcow2 ファイルをダウンロードした場合は、[Import Existing Disk Image] を選択します。

- b) .iso ファイルをダウンロードした場合は、[Local Install Media (ISO Image or CDROM)] を選択します。
- ステップ 4** Cisco Catalyst 8000V qcow2 または iso ファイルの場所を選択します。
- ステップ 5** メモリと CPU のパラメータを設定します。
- ステップ 6** 仮想マシンのストレージを設定します。
- ステップ 7** (オプション) VM を作成する前にハードウェアを追加するには、[Customize configuration before install] を選択します。[Add Hardware] ボタンが表示されます。追加ディスクやシリアルポートインターフェイスなど、さまざまなハードウェアオプションを追加するには、このボタンをクリックします。
- ステップ 8** (オプション) シリアルコンソールを追加するには、[シリアルコンソールの追加 \(81 ページ\)](#) に記載されている手順に従います。
- ステップ 9** (オプション) VM を作成する前に設定をカスタマイズする場合は、[VM を作成する前の設定のカスタマイズ \(82 ページ\)](#) を参照してください。
- ステップ 10** [Finish] をクリックします。
- ステップ 11** Cisco Catalyst 8000V コンソールにアクセスするには、次のいずれかのアクションを実行します。
- 仮想コンソールを使用している場合は、VM インスタンスをダブルクリックして VM コンソールにアクセスします。
  - シリアルコンソールを使用している場合は、「[Booting the Cisco Catalyst 8000V and Accessing the Console](#)」を参照してください。

---

## シリアルコンソールの追加

このタスクを実行し、シリアルコンソールを追加して Cisco Catalyst 8000V インスタンスへのアクセスを有効にします。次の手順を実行して、ハードウェアにシリアルコンソールを追加し、カーネル コンソールオプションを設定します。

### 手順

- 
- ステップ 1** writ-manager GUI で、[Add Hardware] をクリックします。
- ステップ 2** メニューから [Serial] オプションを選択します。
- ステップ 3** [Device Type] ドロップダウンリストから、[TCP net console (tcp)] を選択します。
- ステップ 4** ポート番号を指定し、[Use Telnet] チェックボックスをオンにします。
- ステップ 5** [Finish] をクリックします。
- ステップ 6** 必要なハードウェアをすべて追加したら、[Begin Installation] をクリックします。
- 

## ホスト USB デバイスの追加

Cisco IOS XE 17.9.x バージョン、17.12.x バージョン、またはそれ以降のバージョンを使用する場合、KVM 上の Cisco Catalyst 8000V は USB デバイスパススルーをサポートします。これにより、ホストマシンに接続された USB デバイスを VM に直接渡すことができます。USB ホス

## VM を作成する前の設定のカスタマイズ

トデバイスを追加するには、`virt-manager`、`virsh` などのツールを使用して、または VM の XML 設定を直接編集して、VM の設定を変更する必要があります。`virt-manager` を使用して USB ホストデバイスを追加するには、次の手順を実行します。

### 手順

**ステップ 1** `virt-manager` GUI で、[Add Hardware] をクリックします。

**ステップ 2** USB ホストデバイスを選択します。

**ステップ 3** [USB Device] ドロップダウンリストから、Cisco Catalyst 8000V に接続する USB デバイスを選択します。

**ステップ 4** [Finish] をクリックします。

(注)

Cisco Catalyst 8000V は、USB ディスクのホットプラグ、および最大 2 台の USB ディスクのホットプラグ対応デバイスをサポートします。デバイスを追加する場合は、`virt-manager` を使用して一度に 1 つのデバイスを追加してください。

## VM を作成する前の設定のカスタマイズ

### 始める前に

`.qcow2` または `.iso` イメージを使用して [GUI ツールを使用した VM の作成 \(80 ページ\)](#) タスクを実行します。[Customize configuration before install] オプションをオンにしてから、[Finish] をクリックします。[Add Hardware] ボタンが表示されます。次に、この手順を実行します。この手順では、デイズロ設定に進む前に設定をカスタマイズする方法について説明します。

### 手順

**ステップ 1** [Add Hardware] をクリックします。

**ステップ 2** [Storage] オプションをクリックします。

**ステップ 3** [Select Managed Or Other Existing Storage] チェックボックスをクリックします。

**ステップ 4** [Browse] をクリックし、`c8000v_config.iso` ファイルの場所に移動します。

この手順は、デイズロまたはブートストラップ設定を追加する場合にのみ適用されます。

**ステップ 5** [Device-type] ドロップダウンリストから、[IDE CDROM] を選択します。

**ステップ 6** [Finish] をクリックします。

**ステップ 7** 仮想マネージャでブートデバイス順序を含む VM ブートオプションを調整するには、[IDE CDROM] または `[c8000v_config.iso]` を選択し、上向き矢印を使用してこのデバイスをブート順序の最初のオプションとして移動します。

**ステップ 8** [Apply] をクリックして、ブート順序に加えた変更を適用します。

イメージディスク デバイス オプションは、ブートデバイス順序の 2 番目のオプションとして下にプッシュされます。

**ステップ 9** 必要なハードウェアをすべて追加したら、[Begin Installation] をクリックして、新しい VM の展開を開始します。

### 次のタスク

デイゼロ設定を実行します。これを行う方法については、[デイゼロ設定 \(111 ページ\)](#) を参照してください。

## CLI を使用した VM の作成

- KVM サーバーに `virt-install` RPM パッケージをダウンロードしてインストールします。
- Cisco Catalyst 8000V ソフトウェア インストール イメージ パッケージから **qcow2** イメージをダウンロードし、ローカルデバイスまたはネットワークデバイスにコピーします。

### 手順

**ステップ 1** `.qcow2` イメージの VM を作成するには、`virt-install` コマンドを使用してインスタンスを作成し、起動します。次の構文を使用します。

例 :

```
virt-install \
  --connect=qemu:///system \
  --name=my_c8kv_vm \
  --os-type=linux \
  --os-variant=rhel4 \
  --arch=x86_64 \
  --cpu host \
  --vcpus=1,sockets=1,cores=1,threads=1 \
  --hvm \
  --ram=4096 \
  --import \
  --disk path=<path_to_c8000v_qcow2>,bus=ide,format=qcow2 \
  --network bridge=virbr0,model=virtio \
  --noreboot
```

**ステップ 2** `.iso` イメージの VM を作成するには、次の手順を実行します。

- a) **qemu-img** コマンドを使用し、**.qcow2** 形式で 8 G のディスクイメージを作成します。

例 :

```
qemu-img create -f qcow2 c8000v_disk.qcow2 8G
```

- b) **virt-install** コマンドを使用して、Cisco Catalyst 8000V インスタンスをインストールします。これには、新しい VM を作成するための適切な権限が必要です。次の例では、4G の RAM、1 つのネットワーク

インターフェイス、および 1 つのシリアルポートを備えた 1 つの vCPU Cisco Catalyst 8000V を作成します。

例：

```
virt-install \
  --connect=qemu:///system \
  --name=my_c8000v_vm \
  --description "Test VM" \
  --os-type=linux \
  --os-variant=rhel4 \
  --arch=x86_64 \
  --cpu host \
  --vcpus=1,sockets=1,cores=1,threads=1 \
  --hvm \
  --ram=4096 \
  --cdrom=<path_to_c8000v_iso> \
  --disk path=c8000v_disk.qcow2,bus=virtio,size=8,sparse=false,cache=none,format=qcow2 \
  --network bridge=virbr0,model=virtio \
  --noreboot
```

**virt-install** コマンドで新しい VM インスタンスを作成し、Cisco Catalyst 8000V は指定したディスクファイルにイメージをインストールします。

インストールが完了すると、Cisco Catalyst 8000V VM はシャットダウンされます。**virsh start** コマンドを実行することで VM を起動できます。

(注)

c8000v\_config.iso ディスクイメージを使用してデイズロ設定を指定する場合は、**virt-install** コマンドにパラメータを追加します。たとえば、**--disk path=/my/path/c8000v\_config.iso,device=cdrom,bus=ide** です。詳細については、[デイズロ設定 \(111 ページ\)](#) を参照してください。

### Red Hat Enterprise Linux - ホストモードの設定

Red Hat Enterprise Linux に固有の[問題](#)により、**virt-install** を使用して Red Hat Enterprise Linux 環境で Cisco Catalyst 8000V を起動する場合は、次のようにホストモードを設定します。

- Red Hat Enterprise Linux 6 の場合は次を使用します。

```
--cpu host
```

- Red Hat Enterprise Linux 7 の場合は次を使用します。

```
--cpu host-model
```

# VM のクローン作成

## 問題

KVM 環境では、**virt-manager** 仮想マシンマネージャを使用して Cisco Catalyst 8000V 仮想マシンの複製を作成すると、Cisco Catalyst 8000V 仮想マシンが起動できない場合があります。この問題は、**virt-manager** によって作成され複製されたイメージのサイズが、元の Cisco Catalyst 8000V VM イメージと比較して増加したことが原因で発生します。余分なバイト (KB 範囲) が原因で起動が失敗します。

## 回避策

次の 3 つの回避策があります。

- **virt-clone** コマンドを使用して、Cisco Catalyst 8000V VM イメージを複製します。
- ブートアップ中に **virt-manager** によって作成された複製の Cisco Catalyst 8000V VM イメージの場合は、**packages.conf** の代わりに起動する GOLDEN イメージを選択します。
- [Create a new virtual machine] ウィンドウで、新しい Cisco Catalyst 8000V VM を作成する前に、[Allocate Entire Disk Now] の選択を解除します。これにより、複製された Cisco Catalyst 8000V VM イメージが起動できるようになります。ただし、この回避策はネストされた複製をサポートしていません。この方法は、最初に複製された Cisco Catalyst 8000V VM イメージでのみ使用します。

# KVM 構成のパフォーマンスの向上

KVM ホストの一部の設定を変更することによって、KVM 環境内で実行されている Cisco Catalyst 8000V のパフォーマンスを向上させることができます。これらの設定は、Cisco Catalyst 8000V インスタンスの IOS XE の構成時の設定とは無関係です。

KVM 設定のパフォーマンスを向上させるために、次のことを推奨します。

- vCPU のピン止めの有効化
- エミュレータのピン止めの有効化
- NUMA チューニングの有効化。すべての vCPU が同じソケットの物理コアにピン止めされていることを確認します。
- hugepage メモリバッキングの設定
- IDE ではなく virtio を使用
- SPICE ではなくグラフィック VNC を使用
- 未使用のデバイスの USB、タブレットなどの取り外し

- memballoon の無効化



(注) これらの設定は、サーバーでインスタンス化できる VM の数に影響を与える可能性があります。

調整手順は、ホストでインスタンス化する少数の VM に対して最も影響があります。

上記に加えて、次の手順を実行します。

### CPU ピンニングの有効化

KVM CPU アフィニティオプションを使用して特定のプロセッサに仮想マシンを割り当てることで、KVM 環境のパフォーマンスを向上させます。このオプションを使用する場合は、KVM ホストで CPU ピンニングを構成します。

KVM ホスト環境で、次のコマンドを使用します。

- **virsh nodeinfo** : 次のコマンドを使用して、ホストトポロジを確認し、ピン止めに使用できる vCPU の数を確認します。
- **virsh capabilities** : 使用可能な vCPU の数を確認します。
- **virsh vcpupin <vmname> <vcpu#> <host core#>** : 仮想 CPU をプロセッサコアのセットにピン止めします。

この KVM コマンドは、Cisco Catalyst 8000V インスタンス上の vCPU ごとに実行する必要があります。次に、仮想 CPU 1 をホストコア 3 にピン止めする例を示します。

**virsh vcpupin c8000v 1 3**

次の例は、vCPU が 4 個の Cisco Catalyst 8000V 構成を使用し、ホストに 8 個のコアが搭載されている場合に必要になる KVM コマンドを示しています。

**virsh vcpupin c8000v 0 2**

**virsh vcpupin c8000v 1 3**

**virsh vcpupin c8000v 2 4**

**virsh vcpupin c8000v 3 5**

ホストのコア番号は、0 ~ 7 のどの番号でもかまいません。詳細については、KVM のドキュメンテーションを参照してください。



(注) CPU ピン止めを構成する場合は、ホストサーバーの CPU トポロジを検討してください。複数のコアがある Cisco Catalyst 8000V インスタンスを使用している場合は、複数のソケットにまたがる CPU ピン止めを設定しないでください。

## BIOS 設定

次の表に示す推奨 BIOS 設定を適用して、KVM 設定のパフォーマンスを最適化します。

設定	推奨される設定
Intel Hyper-Threading Technology	無効
Number of Enable Cores	すべて
Execute Disable	有効
Intel VT	有効
Intel VT-D	有効
Intel VT-D coherency サポート	有効
Intel VT-D ATS サポート	有効
CPU パフォーマンス	高スループット
Hardware Prefetcher	無効
Adjacent Cache Line Prefetcher	無効
DCU Streamer Prefetch	無効
Power Technology	カスタム
[Enhanced Intel Speedstep Technology]	無効
[Intel Turbo Boost Technology]	有効
[Processor Power State C6]	無効
Processor Power State C1 Enhanced	無効
Frequency Poor Override	有効
P-State Coordination	HW_ALL
Energy Performance	パフォーマンス

Red Hat Enterprise Linux の要件については、後続のセクションを参照してください。

## ホスト OS 設定

ホスト側では、hugepage を使用し、エミュレータのピン止めを有効にすることをお勧めします。次に、ホスト側の推奨設定の一部を示します。

- IOMMU=pt の有効化
- intel\_iommu=on の有効化

- hugepage の有効化
- ネットワーキング パフォーマンスを向上させるためにシステムがサポートしている場合は、SR-IOV を使用。システムに存在する可能性のある SR-IOV の制限を確認してください。

hugepage とエミュレータのピン止めを有効にすることに加えて、次の設定も推奨されます。  
nmi\_watchdog=0 elevator=cfq transparent\_hugepage=never



(注) VPP または OVS-DPDK で Virtio VHOST USER を使用する場合、QEMU のバージョンでサポートされていれば、バッファサイズを 1024 に増やすことができます (rx\_queue\_size='1024')。

## IO 設定

SR-IOV を使用してパフォーマンスを向上させることができます。ただし、これにより、仮想機能 (VF) の数、QoS サポートなどの SR-IOV の OpenStack の制限、ライブ移行、セキュリティグループのサポートなど、いくつかの制限が発生する可能性があることに注意してください。

fd.io VPP や OVS-DPDK などの最新の vSwitch を使用する場合は、VPP ワーカーレッドまたは OVS-DPDK PMD スレッド用に少なくとも 2 つのコアを予約します。

コマンドラインから VPP を実行するには、次のパラメータを設定します。

- -cpu host : このパラメータにより、VM はホスト OS フラグを継承します。これを xml 設定に含めるには、libvirt 0.9.11 以降が必要です。
- -m 8192 : 最適なゼロパケットドロップ率を実現するには、8GB RAM が必要です。
- rombar=0 : PXE 起動遅延を無効にするには、各デバイスオプションリストの最後に rombar=0 を設定するか、"<rom bar=off />" をデバイスの xml 設定に追加します。

## KVM パフォーマンス向上のためのサンプル XML

### NUMA チューニングのサンプル XML

```
<numatune>
  <memory mode='strict' nodeset='0' />
</numatune>
```

### vCPU およびエミュレータのピン止めのサンプル XML

```
<cputune>
  <vcpupin vcpu='0' cpuset='3' />
  <emulatorpin cpuset='3' />
</cputune>
```

### Hugepage のサンプル XML

```
<currentMemory unit='KiB'>4194304</currentMemory>
<memoryBacking>
  <hugepages>
    <page size='1048576' unit='KiB' nodeset='0'/>
  </hugepages>
  <nosharepages/>
</memoryBacking>
```

### IDE の代わりに virtio のサンプル XML

```
<devices>
  <emulator>/usr/libexec/qemu-kvm</emulator>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2'/>
    <source file='/var/lib/libvirt/images/rhel7.0.qcow2'/>
    <backingStore/>
    <target dev='vda' bus='virtio'/>
    <boot order='1'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
  </disk>
```

### VNC グラフィックのサンプル XML

```
<graphics type='vnc' port='5900' autoport='yes' listen='127.0.0.1' keymap='en-us'>
  <listen type='address' address='127.0.0.1'/>
</graphics>
```

### memballoon を無効にするための XML

```
<memballoon model='none'>
```

## halt\_poll\_ns パラメータの設定

halt\_poll\_ns は、アイドル状態の KVM ゲスト仮想 CPU (vcpus) の処理方法の動作を変更できる KVM パラメータです。

KVM ゲストの仮想 CPU に実行するスレッドがない場合、QEMU は従来、アイドル状態の CPU を停止します。この設定は、デフォルトで 400 ナノ秒の期間を指定します。この場合、仮想 CPU は CPU アイドル状態になる前に待機してポーリングします。

仮想 CPU が停止する前のポーリング期間中に新しい作業が到着すると、仮想 CPU はすぐに作業を実行できるようになります。新しい作業が到着したときに仮想 CPU がアイドル状態であった場合は、新しい作業を開始する前に仮想 CPU をアイドル状態から戻す必要があります。アイドル状態から実行状態になるまでにかかる時間は、遅延の影響を受けやすいワークロードに悪影響を与える追加の遅延を引き起こします。

デフォルトのカーネルパラメータでは、ゲスト Cisco Catalyst 8000V ルータの CPU がホスト CPU の 100% を消費します。

halt\_poll\_ns は、次の 2 つの方法で設定できます。

- **Large halt\_poll\_ns** : この場合、仮想 CPU をスリープ解除するイベントのビジースピンの多くの CPU が費やされ、acpi ディープスリープの発生が少なくなります。これは、より多くの電力が消費されることを意味します。ただし、ディープスリープ状態からのウェイクアップは少なく、設定されている状態によっては、キャッシュミスなどの問題が発生する可能性があります。
- **Small halt\_poll\_ns** : この場合、CPU をスリープ解除するイベントのビジースピンの費やされる CPU 時間が少なくなり、より多くの acpi ディープスリープが発生します。この場合、消費電力は少なくなりますが、ディープスリープ状態からのウェイクアップが多くなります。ウェイクアップが多いと、ディープスリープ インスタンスが大量に発生する可能性があります。設定によっては大量のキャッシュミスが発生し、ウェイクアップ時間が長くなる可能性があります。

### halt\_poll\_ns パラメータの設定

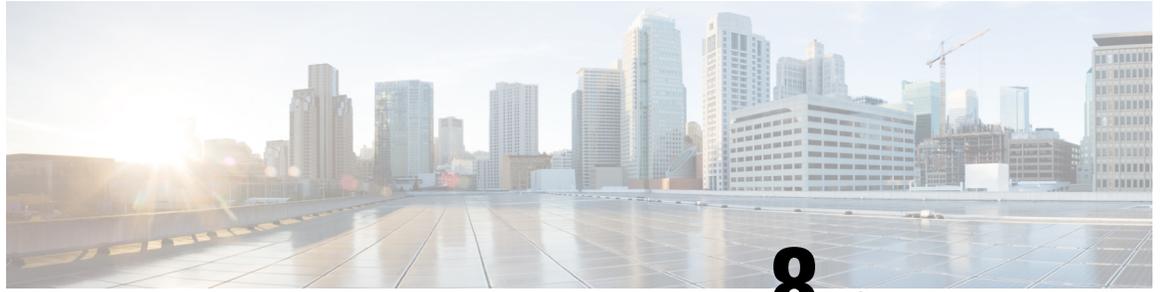
halt\_poll\_ns パラメータは次のように設定できます。

1. 実行時に、echo 0 > /sys/module/kvm/parameters/halt\_poll\_ns を実行します。

2. モジュールをロードする場合は、次の設定を実行します。

```
# rmmod kvm_intel
# rmmod kvm
# modprobe kvm halt_poll_ns=0
# modprobe kvm_intel
```

3. デバイスを起動するときに、grub2 のパラメータセクションに kvm.halt\_poll\_ns=<specify value> を追加します。



## 第 8 章

# NFVIS 環境でのインストール

Cisco Enterprise Network Function Virtualization Infrastructure Software (Cisco Enterprise NFVIS) は、サービスプロバイダーや企業が仮想ルータ、ファイアウォール、WAN 加速化などの仮想化ネットワーク機能をサポート対象のシスコのデバイス上へ容易に動的に展開できるようにする Linux ベースのインフラストラクチャ ソフトウェアです。

Cisco Enterprise NFVIS ソリューションは、重要なネットワーク機能をソフトウェアに容易に変換できるようにし、ネットワークサービスを分散された場所に数分で展開できるようにします。このソリューションは、仮想デバイスと物理デバイスの両方から構成される多様なネットワーク上で実行できる、完全に統合されたプラットフォームを実現します。

この章では、シスコ サービス統合型仮想ルータ (ISRv) から Cisco Catalyst 8000V にアップグレードする方法について説明します。使用中のハードウェアが Cisco NFVIS で実行されているときに、この設定を Cisco Catalyst 8000V に展開する場合は、「*NFVIS* での VM のインストール」のセクションに記載されている手順を実行します。



(注) Cisco IOS XE 17.4.x 以降のリリースでは、ISRv は Cisco Catalyst 8000V に置き換えられます。Cisco Catalyst 8000V の展開には NFVIS バージョン 4.4 以降が必要です。

### NFVIS を実行しているサポート対象ハードウェア プラットフォーム

- Cisco 5400 シリーズ エンタープライズ ネットワーク コンピューティング システム (ENCS)
- クラウド サービス プラットフォーム 5000 シリーズ (CSP)
- Cisco 8200 UCPE シリーズ

### サポートされる NIM

- NIM-4G-LTE-VZ
- NIM-4G-LTE-ST
- NIM-4G-LTE-NA
- NIM-4G-LTE-GA

- NIM-4G-LTE-LA
- NIM-LTEA-EA
- NIM-LTEA-LA
- NIM-1MFT-T1/E1
- NIM-2MFT-T1/E1
- NIM-4MFT-T1/E1
- NIM-8MFT-T1/E1
- NIM-1CE1T1-PRI
- NIM-2CE1T1-PRI
- NIM-8CE1T1-PRI
- NIM-16A
- NIM-24A
- NIM-VA-B
- NIM-VAB-A
- NIM-VAB-M
- NIM-4SHDSL-EA
- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- NIM-ES2-8-P
- NIM-ES2-8 NIM-ES2-4

#### サポートされる NIC

ハードウェア	vNIC
ENCS	virtio、igbvf、i40evf
UCPE	virtio、igbvf、ixgbevf

ハードウェア	vNIC
CSP	<ul style="list-style-type: none"> <li>• virtio、igbvf : Cisco IOS XE 17.4.1 以降でサポート</li> <li>• i40evf : Cisco IOS XE 17.4.1 ~ 17.8.x でサポート</li> <li>• ConnectX-5VF および iavf : Cisco IOS XE 17.9.1 以降でサポート</li> <li>• Ixgbe : Cisco IOS XE 17.10.1 以降でサポート</li> </ul>

#### サポートされるプロファイル

- Mini : 1vCPU
- Small : 2vCPU
- Medium : 4vCPU
- Large : 4vCPU



(注) Cisco Catalyst 8000V は低遅延 VM として機能し、専用の vCPU コアで想定どおりに動作しません。

- [NFVIS での VM のインストール \(93 ページ\)](#)
- [NFVIS での VM のインストール \(リリース 4.5.1 以降\) \(94 ページ\)](#)
- [NFVIS での VM のインストール \(リリース 4.5.0 以前\) \(97 ページ\)](#)
- [仮想マシンの監視 \(101 ページ\)](#)
- [Cisco ISRV と Cisco Catalyst 8000V の間でのアップグレードとダウングレード \(102 ページ\)](#)

## NFVIS での VM のインストール

Cisco IOS XE 17.4.1 リリース以降は、NFVIS に Cisco Catalyst 8000V VM を新規インストールするか、Cisco ISRv から Cisco Catalyst 8000V にアップグレードできます。インストールまたはアップグレードのために実行する必要がある主なタスクは次のとおりです。

- **VM イメージの登録** : VM イメージを登録するには、VM イメージを最初に NFVIS サーバーにコピーまたはダウンロードするか、あるいは HTTP または HTTPS サーバー上でイメージをホストする必要があります。ファイルをダウンロードしたら、登録 API を使用してイメージを登録します。この API を使用すると、tar.gz ファイルをホストする場所 (HTTP または HTTPS サーバ上) へのファイルパスを指定することができます。イメージの登録

は1回限りのアクティビティです。イメージをHTTPまたはHTTPSサーバー上に登録し、登録がアクティブ状態になると、登録されたイメージを使用して複数のVM展開を実行できるようになります。

- **カスタムプロファイルの作成**：VMイメージを登録した後、必要に応じてVMイメージのカスタムプロファイルを作成できます。このプロファイルは、イメージファイルで定義されたプロファイルが要件に一致しない場合に特に役立ちます。カスタムプロファイルでは、VMが実行する仮想CPUなど、VMイメージの特定のプロファイリングの詳細や、VMが使用する仮想メモリの量を指定することができます。必要なトポロジに応じて、展開時にVMに接続する追加のネットワークやブリッジを作成できます。
- **VMの展開**：展開APIを使用してVMを展開します。このAPIでは、導入時にシステムに渡すパラメータに値を指定できます。展開するVMに応じて、必須のパラメータとオプションのパラメータがあります。APIの詳細については、「[VM Lifecycle Management APIs](#)」を参照してください。
- **VMの管理と監視**：VMステータスを取得したり、ログをデバッグしたりできるようにするAPIとコマンドを使用してVMを監視できます。VM管理APIを使用すると、VMを起動、停止、またはリブートでき、CPU使用率などのVMの統計情報を表示できます。VMプロファイルを変更または更新することもできます。VMプロファイルをイメージファイル内の既存のプロファイルのいずれかに変更できます。または、VMの新しいカスタムプロファイルを作成できます。VM上のvNICは追加または更新することもできます。

## NFVIS での VM のインストール (リリース 4.5.1 以降)

### NFVIS 環境での Cisco Catalyst 8000V のインストール

Cisco Catalyst 8000V を NFVIS バージョン 4.5.1 以降にインストールする場合は、このセクションの手順に従います。

NFVIS の以前のリリースに Cisco Catalyst 8000V をインストールするには、[NFVIS 環境でのインストール \(91 ページ\)](#) を参照してください。

### NFVIS でのイメージのアップロード

#### 手順

**ステップ 1** NFVIS ポータルにログインします。

**ステップ 2** [Configuration] > [Virtual Machine] > [Images] > [Image Repository] の順に選択します。

**ステップ 3** 次のいずれかを実行して、インストールファイルをアップロードします。

- [Local] > [Select File] の順に選択し、デバイスからインストールファイルを見つけて選択します。

- [Remote] を選択します。

**ステップ 4** [Remote] を選択した場合は、次の詳細を入力します。

- [Image Name] : このフィールドでイメージファイルの名前を指定します。
- [Protocol] : ドロップダウンリストからプロトコルを選択します。
- [IP Address] : このフィールドでリモートロケーションの IP アドレスを指定します。
- [Port] : このフィールドでリモートロケーションのポートを指定します。
- [Image File Path] : このフィールドでイメージファイルへのファイルパスを指定します。

## ネットワークの作成

### 手順

**ステップ 1** NFVIS ポータルで、[Configuration] > [Virtual Machine] > [Networking] > [Networks] の順に選択します。

**ステップ 2** 新しいネットワークを作成するには、[+] アイコンをクリックします。

**ステップ 3** [Add Network] 領域で、次の詳細を入力します。

- [Network] : このドロップダウンリストから、適切なネットワークを選択します。
- [Mode] : VNF がブートするモードを入力します。
- [VLAN] : VM の VLAN を選択します。
- [VLAN-Range] : VM の VLAN の範囲を入力します。
- [Native VLAN] : このフィールドから VM のネイティブ VLAN を選択します。
- [Bridge] : VM の仮想ネットワーク インターフェイス コントローラ (vNIC) 間のレイヤ 2 ドメインです。[Existing] または [Create New] オプションボタンを選択します。
- [Interface] : このフィールドから VM のインターフェイスを選択します。

(注)

このインストールでは Single Root Input/Output Virtualization (SR-IOV) はサポートされていません。

**ステップ 4** [Submit] をクリックします。

## VM パッケージの作成

### 手順

**ステップ 1** NFVIS ポータルで、[Configuration] > [Virtual Machine] > [Images] > [Image Package] の順に選択します。

**ステップ 2** VM パッケージを作成するには、[+] アイコンをクリックします。

**ステップ 3** [Image Packaging] 領域で、次の詳細を入力します。

- a) [Name] : VM パッケージングに関連付けられている名前。
- b) [Version] : パッケージのバージョン。
- c) [VM Type] : パッケージを作成する VM のタイプ。
- d) [Dedicate Cores (Optimize)] : コンテナに必要な専用コア。デフォルトでは、値は [False] です。
- e) [Serial Console] : シリアルコンソールを介したアクセスを有効または無効にするフィールド。デフォルトでは、値は [Disable] です。
- f) [SRIOV Driver] : VM インターフェイスでサポートされる SRIOV。
- g) [Local] : バンドルするイメージが intdatastore で使用可能な場合に使用する必要があるオプション。
- h) [Upload Raw Images] : ローカルマシンからパッケージ化するイメージをアップロードするオプション。
- i) [Raw Disk File Bus] : このドロップダウンリストからルートディスクイメージバスを選択します。
- j) [Thick Disk Provisioning] : ドロップダウンリストから [true] を選択して、シックプロビジョニングを有効にします。デフォルトでは、値は [false] です。

**ステップ 4** ブートストラップファイルをアップロードするには、次のいずれかを実行します。

- [Local] を選択し、[Add Local File] オプションを選択して、ローカルで使用可能なブートストラップファイルを追加します。
- [Upload Bootstrap Files] オプションを選択して、コンピュータからブートストラップ設定ファイルを参照します。
- [Monitored] ドロップダウンフィールドから VM の追跡状態を選択します。デフォルトでは、値は [False] です。

**ステップ 5** VM パッケージを生成するには、[Submit] をクリックします。

## VM の展開

### 手順

**ステップ 1** NFVIS ポータルで、[Configuration] > [Deploy] の順に選択します。

**ステップ 2** [VM Deployment] ウィンドウで、[Router] アイコンを選択します。

**ステップ 3** VM をクリックします。VM の周囲に 4 つのドラッグハンドラが表示されます。これらのハンドラのいずれかから、いずれかのネットワークにドラッグし、詳細を入力します。

**ステップ 4** [VM Details] エリアで、以下の詳細を入力します。

- a) [VM Name] : VM の名前を指定します。
- b) [Image] : ドロップダウンリストから適切な値を選択します。
- c) [Profile] : ドロップダウンリストからプロファイルを選択します。デフォルトのプロファイルは、展開時にプロファイルが指定されていない場合に使用されます。

- d) [Group Name] : この VM を特定のグループに関連付ける場合は、グループを選択します。
- e) [VNC Password] : このフィールドに VNC パスワードを入力します。
- f) [Controller] : 自律モードで展開するには [non-vManage] を選択し、コントローラモードで VM を展開するには [vManage] を選択します。
- g) [Tech Package] : ドロップダウンフィールドから、適切な技術パッケージを選択します。使用可能なオプションは、ネットワークエッセンシャル、ネットワークアドバンテージ、ネットワークプレミアです。
- h) [NGIO] : VM で使用可能な NIM 有効化機能を決定する次世代入出力 (NGIO) オプション。NGIO ドロップダウンリストから [ENABLE] を選択して NGIO を有効にします。
- i) [SSH Username] : Cisco Catalyst 8000V VM にリモートでログインするためのユーザー名。
- j) [SSH Password] : VM にアクセスするための SSH パスワード。
- k) [Port Number] : VM への SSH 接続に必要なポート番号。
- l) [External Port Number] : VM への SSH 接続に必要な外部ポート番号。

ステップ 5 [Deploy] をクリックします。

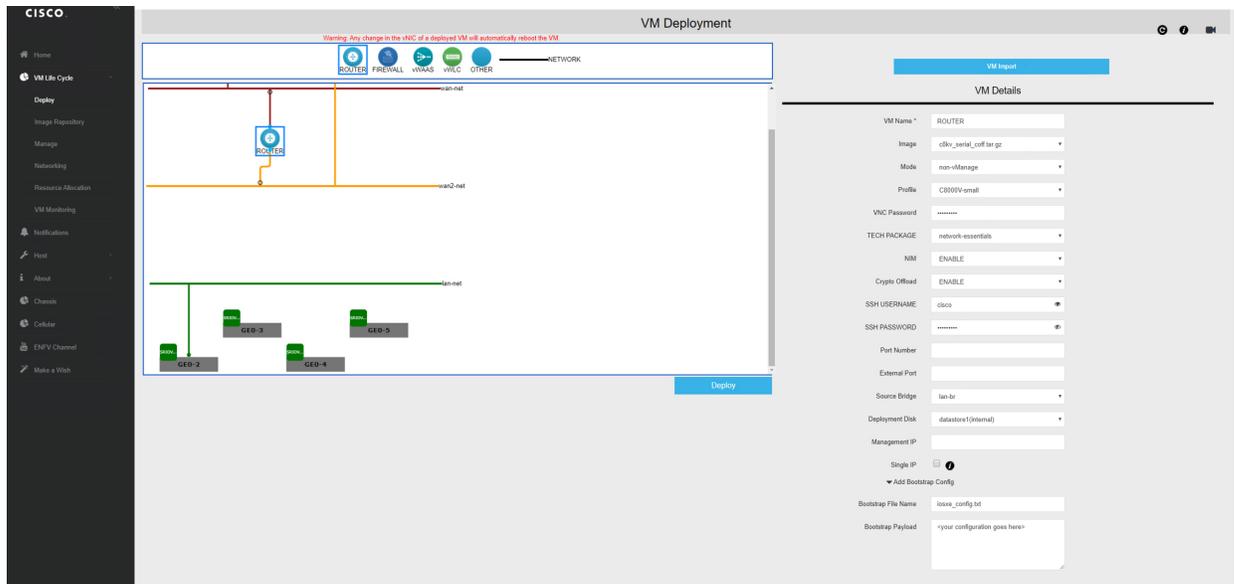
## NFVIS での VM のインストール（リリース 4.5.0 以前）

### NFVIS での仮想マシンの展開

#### 手順

- ステップ 1 NFVIS ポータルから [VM Lifecycle] > [Deploy] を選択します。
- ステップ 2 [VM Deployment] ウィンドウで、[Router] アイコンを下のパインにドラッグアンドドロップし、必要に応じて適切なネットワークにマッピングします。
- ステップ 3 [VM Details] セクションで、[VM Name] を入力します。
- ステップ 4 [Image] ドロップダウンフィールドから、適切な値を選択します。
- ステップ 5 [Mode] ドロップダウンフィールドから、[non-vManage] オプションを選択します。
- ステップ 6 [Profile] ドロップダウンリストから、プロファイル名を選択します。
- ステップ 7 [Tech Package] ドロップダウンフィールドから、適切な技術パッケージを選択します。
- ステップ 8 特定のネットワーク機能を持つ物理ハードウェアがインストールされている場合は、[NIM] ドロップダウンフィールドから [ENABLE] を選択して VM に渡すことができます。
- ステップ 9 [Crypto Offload] ドロップダウンフィールドから [ENABLE] オプションを選択して、暗号化処理をハードウェアチップにオフロードします。
- ステップ 10 Cisco Catalyst 8000V への SSH ログイン用のユーザー名とパスワードを入力します。
- ステップ 11 必要に応じて、[VNC Password]、[Port Number]、[External Port]、[Source Bridge]、[Deployment Disk]、[Management IP] などの他の VM 詳細情報を追加します。

- ステップ 12** VM を展開する前にブートストラップ設定ファイルを提供するため、[Add Bootstrap Config] オプションを選択します。ブートストラップ設定ファイルに「iosxe\_config.txt」というファイル名が使用されていることを確認します。



(注)  
ギガビットイーサネット 1 インターフェイスは、NFVIS ホストとの管理通信用に予約されています。

- ステップ 13** [Deploy] をクリックします。

### 次のタスク

VM インスタンスを展開したら、[Manage] タブでインスタンスの詳細を確認します。このタブには、VM インスタンスの概要が表示されます。

コンソールにアクセスするには、VM の横にある [Console] 記号をクリックします。次の NFVIS コマンドを使用して、VM のシリアルコンソールに接続することもできます。

```
vmConsole <ROUTER-NAME>
```

## NFVIS 用 Cisco Catalyst 8000V イメージのダウンロード

### 手順

- ステップ 1** <https://software.cisco.com/download/home> に移動します。
- ステップ 2** ページ下部の検索バーで Cisco Catalyst 8000V を検索します。
- ステップ 3** リストから [Software Type] を選択します。たとえば、IOS XE ソフトウェアを選択します。

**ステップ 4** ファイルのリストから、tar.gz 拡張子を持つ最新の Cisco Catalyst 8000V イメージファイルをダウンロードします。

(注)

NFVIS で Cisco Catalyst 8000V イメージを展開するには、イメージをイメージプロパティファイルにパッケージ化する必要があります。

## NFVIS でのイメージのアップロード

### 手順

**ステップ 1** NFVIS ポータルにログインします。

**ステップ 2** [VM Lifecycle] > [Image Repository] を選択します。

**ステップ 3** [Image Registration] タブをクリックし、[Images] オプションの横にあるアップロード矢印をクリックします。

**ステップ 4** [Drop Files or Click] オプションから適切なファイルを選択します。

The screenshot shows the NFVIS web portal interface. On the left is a navigation sidebar with options like Home, VM Life Cycle, Image Repository, and VM Monitoring. The main content area is titled 'Image Registration' and has a 'Drop Files or Click' button. Below this is a table for 'Images' with columns for Image Name, State, Type, Version, Storage Location, Secure Boot, and Action. The table contains three entries:

Image Name	State	Type	Version	Storage Location	Secure Boot	Action
q8000v-vmkernel@BLD_POLARIS_DEV_LATEST_20201003_1 E2629_V17_5_3_42-serial.tar.gz	ACTIVE	ROUTER	BLD_POLARIS_DEV_LATEST_20201003_102 E29_V17_5_3_42	datstore1(internal)		⬇️ ⬇️
cdlx_serial_cofl.tar.gz	ACTIVE	ROUTER	version	datstore1(internal)		⬇️ ⬇️
cdlx_serial_cofl_new_branch.tar.gz	ACTIVE	ROUTER	version	datstore1(internal)		⬇️ ⬇️

At the bottom of the table, it says 'Showing 1 to 3 of 3 entries' and has 'Previous' and 'Next' navigation buttons.

**ステップ 5** [Start] をクリックしてイメージをアップロードします。

イメージをアップロードすると、NFVIS はそれぞれのプロファイルを作成し、イメージを登録します。選択したファイルは同じページの [Images] セクションに表示されています。

## Web インターフェイスを使用した VM パッケージの作成

### 手順

**ステップ 1** NFVIS Web ポータルから、[Image Repository] > [Image Packaging] を選択します。[Create] アイコンをクリックします。

## ネットワークの作成

ステップ2 [VM Packages] をクリックします。

ステップ3 [Image Packaging] タブに詳細を入力します。[Dedicated Code] ドロップダウンリストから [Yes] を選択します。

ステップ4 [Submit] をクリックします。ブートストラップファイルがアップロードされます。

イメージを作成したら、そのイメージを登録し、プロファイルが VFVIS に適切に入力されるようにする必要があります。

ステップ5 作成したイメージを選択し、[Register] をクリックします。

## ネットワークの作成

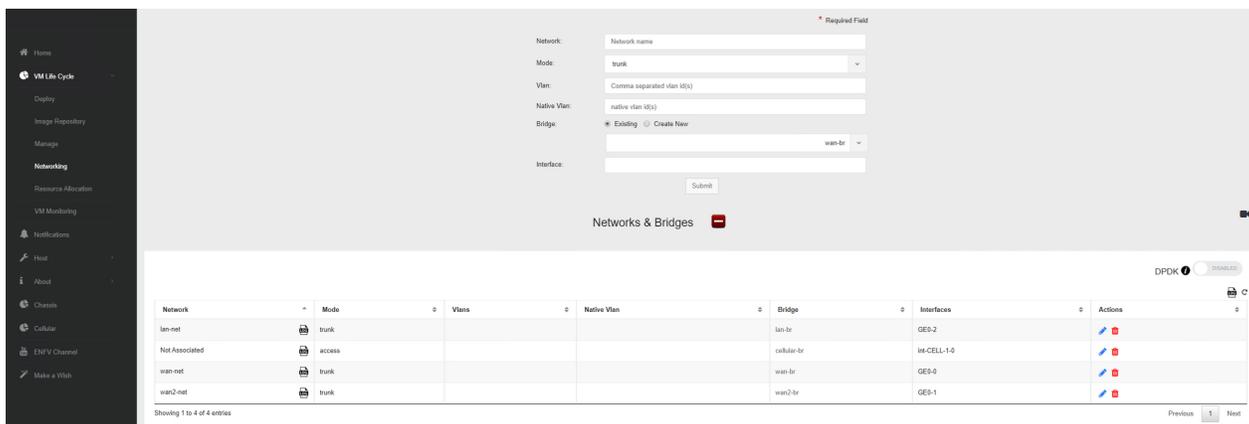
### 手順

ステップ1 NFVIS ポータルから、[VM Lifecycle] > [Networking] を選択します。[Networks & Bridges] ページが表示されます。

ステップ2 [Networks & Bridges] の横にある [Create] アイコンをクリックします。

ステップ3 [Network]、[Mode]、[VLAN]、[Bridge]、および [Interface] の各フィールドに適切な値を入力します。

Single Root Input/Output Virtualization (SRIOV) はサポートされていません。



**ステップ 4** [Submit] をクリックします。ネットワークが作成されました。

## 仮想マシンの監視

この手順では、VM を監視する手順を指定し、リソース割り当て、VM 統計情報などの動作情報を表示します。

### 手順

**ステップ 1** VM のリソース割り当てを表示するには、次のステップに従います。

- NFVIS ポータルから、[VM Life Cycle] > [Resource Allocation] を選択します。全体的な CPU 割り当てが表示された [VM CPU Allocation] タブが表示されます。
- [VM Memory Allocation] をクリックして、全体的なメモリ割り当てを表示します。
- [VM Disk Allocation] をクリックして、全体的なディスク割り当てを表示します。

**ステップ 2** VM 統計情報を表示するには、次のステップを実行します。

- NFVIS ポータルから、[VM Life Cycle] > [Resource Allocation] を選択します。  
VM ごとの全体的な CPU 使用率が示された [VM CPU Utilization] タブが表示されます。
- [Memory Allocation] をクリックして、VM ごとのメモリ使用率を表示します。
- [VNC Utilization] タブをクリックして、VM ごとの VNIC 使用率を表示します。
- [Disk Utilization] タブをクリックして、VM ごとのディスク使用率を表示します。

Cisco Catalyst 8000V の最初のインターフェイスは、Cisco NFVIS 管理ネットワーク（通常はギガビットイーサネット 1）用に常に予約されています。Cisco NFVIS は、このインターフェイスに IP アドレスを割り当て、インターフェイス経由で ICMP ping を使用して VM を周期的に監視します。

### 警告

インターフェイスをシャットダウンしたり、IP アドレスを変更したりすると、NFVIS VM のリカバリとリロードが発生する可能性があります。

## Cisco ISRV と Cisco Catalyst 8000V の間でのアップグレードとダウングレード

Cisco IOS XE 17.4.x 以降のリリースでは、シスコのサービス統合型仮想ルータ (ISRV) が Cisco Catalyst 8000V に置き換えられます。ユーザーは、既存の ISRV ルータを Cisco Catalyst 8000V にアップグレードできます。Cisco Catalyst 8000V の最新リリースにアップグレードする方法については、[Cisco IOS XE ソフトウェアのアップグレード \(159 ページ\)](#) を参照してください。

### (注)

- Cisco Catalyst 8000V から Cisco ISRV にダウングレードすることはできません。
- Cisco ISRV から Cisco Catalyst 8000V にアップグレードする場合、サポートされる Cisco ISRV の最小バージョンは 16.12.4、17.2.3、17.3.2 です。上記以外のバージョンが実行されている Cisco ISRV デバイスを使用している場合は、Cisco Catalyst 8000V にアップグレードできません。
- Cisco IOS XE 17.1.x 以前のリリースから Cisco IOS XE 17.4.x にアップグレードする場合、**install add file bootflash:c8000v-universalk9.XXX.bin activate commit** コマンドはサポートされません。Cisco ISRV を Cisco Catalyst 8000V にアップグレードするには、c8000v-universalk9.XXX.bin ファイルを Configuration フォルダの bootflash: にコピーします。次に、**write memory** コマンドを使用して設定をコピーし、アップグレードプロセスを開始します。
- Cisco IOS XE 16.12.3 以前のリリースを実行している既存の Cisco CSR1000V ユーザーが Cisco Catalyst 8000V にアップグレードする場合、Web UI を使用してアップグレードすることはできません。Cisco Catalyst 8000V にアップグレードする前に、まず Cisco CSR1000V リリース 16.12.4、17.2.3、または 17.3.2 にアップグレードする必要があります。
- すべてのライセンス情報は、Cisco Catalyst 8000V へのアップグレード後も保持されます。

### サポートされているアップグレードパス

#### 自律モード

- 16.12.x > 17.4 C8000V
- 17.2.x > 17.4 C8000V
- 17.3.x > 17.4 C8000V

#### コントローラモード

- 16.12.2 ISRV > 16.12.4 ISRV > 17.4 C8000V
- 16.12.3 ISRV > 16.12.4 ISRV > 17.4 C8000V
- 16.12.4 ISRV > 17.4 C8000V
- 17.1.1 ISRV > 17.3.x ISRV > 17.4 C8000V
- 17.2.1 ISRV > 17.2.2 ISRV > 17.4 C8000V
- 17.2.2 ISRV > 17.4 C8000V
- 17.3.x ISRV > 17.4 C8000V



---

(注) コントローラモードで Cisco ISRV を Cisco Catalyst 8000V にアップグレードする場合は、最初に Cisco IOS XE を 17.3.1 以降のリリースまたは 16.12.4 以降のリリースにアップグレードします。

---





## 第 9 章

# OpenStack 環境へのインストール

Cisco IOS XE リリース 17.7.1 以降では、ハイパーバイザマネージャとして機能する OpenStack Train に Cisco Catalyst 8000V をインストールして起動できます。OpenStack Train リリースは、仮想マシン (VM) またはインスタンスを起動できるオープンソースクラウドインフラストラクチャソフトウェアの 20 番目のバージョンです。

このインストールでは、8 GB と 16 GB の両方のディスクがサポートされます。次のいずれかの方法を使用して、OpenStack に Cisco Catalyst 8000V VM をインストールできます。

- OpenStack ダッシュボードを使用して VM を手動で作成し、qcow2 イメージを使用してインストールする。
- Heat テンプレートを使用したインストールを実行する。OpenStack では、Heat は、OpenStack コア REST API を介してテンプレート形式を使用して複合クラウドアプリケーションをオーケストレーションするサービスです。Heat テンプレートは、クラウドアプリケーションのインフラストラクチャをテキストファイルで記述します。これらのテンプレートは、Heat が OpenStack API を呼び出すことを可能にするリソース間の関係を指定します。このアクションにより、アプリケーションを起動するための正しい順序ですべてのインフラストラクチャが作成されます。

Cisco Catalyst 8000V インスタンスをインストールして起動すると、指定したブートストラップまたはデゼロ設定データに基づいて、ルータは自律モードまたはコントローラモードで起動します。

### サポートされている機能

OpenStack の Cisco Catalyst 8000V インストールでサポートされる機能は次のとおりです。

- IPv6
- CDNA ライセンスモデル
- 自律モードでの vNIC のホット追加および削除
- [OpenStack のインストール要件 \(106 ページ\)](#)
- [OpenStack へのインストールに関する制約事項 \(106 ページ\)](#)
- [OpenStack への Cisco Catalyst 8000V のインストール \(106 ページ\)](#)

## OpenStack のインストール要件

OpenStack に Cisco Catalyst 8000V をインストールするための要件は次のとおりです。

- OpenStack リリース：トレインリリース
- Red Hat Enterprise Linux (RHEL) 8.2 (Ootpa)
- RHEL OSP バージョン 16.1 (トレイン)
- CVIM バージョン 4.2
- 仮想ディスク：8 GB と 16 GB 両方の仮想ディスクがサポートされています
- サポートされる最小プロファイル：4 GB のメモリと 8 GB または 16 GB の仮想ディスクを搭載した 1 vCPU

## OpenStack へのインストールに関する制約事項

OpenStack heat デプロイメントによって生成されたコンソール URL には、トークンの存続可能時間 (TTL) が適用され、デフォルト設定は 10 分です。使用する NoVNC URL は、特に低プロファイルのインスタンスの起動時や異なるセットアップの使用時など、特定の条件下では、このデフォルトの時間が経過すると期限切れになります。

この制限を克服するには、ポータルの組み込みインスタンス VNC コンソールを使用するか、コンピューティングノードの **virsh console** コマンドを使用してインスタンスのコンソールにアクセスします。

## OpenStack への Cisco Catalyst 8000V のインストール

次のいずれかの方法で Cisco Catalyst 8000V をインストールすることができます。

- OpenStack GUI を使用します。これを行う方法については、[インスタンスの起動 \(107 ページ\)](#) を参照してください。
- Heat テンプレートを使用します。このインストールの実行方法については、[Heat テンプレートを使用した VM のインストール \(108 ページ\)](#) を参照してください。
- CLI を使用します。OpenStack CLI で **openstack server create** コマンドを実行することで VM を作成できます。詳細については、<https://docs.openstack.org/python-openstackclient/train/cli/command-objects/server.html#server-create> を参照してください。

## インスタンスの起動

### 手順

- ステップ 1** OpenStack ポータルで、[Images] をクリックし、起動するイメージを選択します。  
または、[Instances]、[Launch Instance] の順にクリックすることもできます。
- ステップ 2** 左側のペインで、[Details] をクリックし、次の詳細を指定します。
- [Instance Name] : インスタンスの名前を入力します。
  - [Description] : インスタンスの説明を入力します。このフィールドは任意です。
  - [Availability Zone] : このフィールドは、クラウドの論理パーティションを指定します。このフィールドに **Nova** と入力します。
  - [Count] : 作成するインスタンスの数を入力します。同じ設定で複数のインスタンスを作成するには、数を増やします。
- ステップ 3** [Next] をクリックします。
- ステップ 4** 左ペインで、[Source] をクリックします。
- ステップ 5** [Select Boot Source] ドロップダウンフィールドから、[Image]、[Instance Snapshot]、[Volume]、または [Volume Snapshot] を選択します。
- [Source] オプションでは、インスタンスの作成に使用するテンプレートを指定します。イメージ、インスタンスのスナップショット（イメージスナップショット）、ボリューム、またはボリュームスナップショット（有効な場合）を使用できます。新しいボリュームを作成して、永続ストレージを使用することもできます。
- ステップ 6** インスタンスの削除時にボリュームを削除するには、[Delete Volume on Instance Delete] フィールドで [Yes] を選択します。
- ステップ 7** 左側のペインで [Flavor] をクリックします。
- ステップ 8** メモリとストレージの要件に基づいてオプションを選択します。
- ステップ 9** [Next] をクリックします。
- ステップ 10** [Networks] オプションから、Cisco Catalyst 8000V VM とそのネットワーク内のサーバーを接続するネットワークを選択します。このオプションは、トポロジを設定する場合にも必要です。
- （注）  
VM に接続する SRIOV ポートを選択する場合は、[Network Ports] ドロップダウンリストを使用して NIC を選択できます。
- ステップ 11** [Next] をクリックします。
- ステップ 12** [Security Groups] ドロップダウンリストから、インスタンスを起動するセキュリティグループを選択します。デフォルトのセキュリティグループも使用できます。

**ステップ 13** [Next] をクリックします。

**ステップ 14** [Configuration] セクションで、ユーザーデータをコピーして [Customization Script] フィールドに貼り付けます。次に、ユーザーデータ設定スクリプトの例を示します。

```
hostname c8kv-ios_cfg
license smart enable
username lab privilege 15 secret lab
ip domain-name cisco.com
interface GigabitEthernet1
ip address 10.0.0.5 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
login local
exit
```

**ステップ 15** XML ファイルまたは iosxe\_config.txt ファイルをアップロードして、ユーザーデータまたは設定データを提供することもできます。[Choose File] をクリックし、XML または .txt ファイルを参照します。

(注)

デイズロ設定の詳細については、[デイズロ設定 \(111 ページ\)](#) を参照してください。

**ステップ 16** [Configuration Drive] チェックボックスをオンにして、[Next] をクリックします。

**ステップ 17** [Launch Instance] をクリックしてインスタンスを起動します。

(注)

自律モードからコントローラモードに切り替える場合は、ciscosdwan\_cloud\_init.cfg ファイルをブートフラッシュにコピーする必要があります。

## Heat テンプレートをを使用した VM のインストール

OpenStack の Heat テンプレートを使用すると、インスタンス、ボリューム、セキュリティグループなどの OpenStack リソースを作成できます。このテンプレートは、クラウドアプリケーションのインフラストラクチャをテキストファイルの形式で指定し、インフラストラクチャ、サービス、およびアプリケーションの展開を自動化できるようにします。

Heat テンプレートを使用して OpenStack VM をインストールするには、次の手順を実行します。

### 手順

**ステップ 1** OpenStack のポータルにログインします。

**ステップ 2** 上部のメニューオプションから、[Project] をクリックします。

**ステップ 3** [Orchestration] をクリックし、[Stack] を選択します。

**ステップ 4** [Stacks] ウィンドウで、[Launch Stack] をクリックします。

- ステップ 5** [Template Source] ドロップダウンリストから、テンプレートの提供方法に基づいて、[File]、[URL]、または [Direct Input] を選択します。
- ステップ 6** [File] オプションを選択した場合は、[Choose File] オプションをクリックし、テンプレートファイルを保存した場所を参照してこのファイルをアップロードし、[Next] をクリックします。
- ステップ 7** [Stack Name] フィールドにスタックの名前を入力します。
- ステップ 8** ロールバックを有効にするには、[Rollback on Failure] チェックボックスをオンにします。
- ステップ 9** [Password for user “admin”] フィールドに、管理者のパスワードを入力します。
- ステップ 10** [Launch] をクリックします。
- 起動が完了すると、[Stacks] ウィンドウの [Status] 列に「Create Complete」というメッセージが表示されます。
-





## 第 10 章

# デイレゼロ設定

Cisco Catalyst 8000V は、Cisco IOS XE と Cisco IOS XE SD-WAN の両方の機能をサポートします。自律モードでインスタンスを起動することで、Cisco IOS XE の機能にアクセスできます。同様に、Cisco SD-WAN 機能にアクセスして使用するには、インスタンスをコントローラモードで起動します。

自律モードは、Cisco Catalyst 8000V インスタンスが起動するデフォルトのモードです。自律モードでデイレゼロの設定を続行する場合は、この章を参照してください。



(注) Cisco Catalyst 8000V インスタンスをコントローラモードで展開する場合は、「[Install and Upgrade for Cisco Catalyst 8000V Controller Mode](#)」を参照してください。



注目 システムが4つのパラメータ (OTP、UUID、VBOND、ORG) をいずれも検出できない場合、デバイスは自律モードで起動します。

### ハイパーバイザとクラウド全体でのブートストラップのサポート

次の表に、自律モードでの Cisco Catalyst 8000V のハイパーバイザとクラウド全体のブートストラップサポートの概要を示します。

ハイパーバイザ	CD-ROMの <code>iosxe_config.txt</code>	CD-ROMの <code>ovf-env.xml</code>	OVA のイン ストール	Config-drive 形式	カスタム データ	ユーザー データ
VMware	対応	はい	はい	対応	非対応	非対応
KVM	対応	対応	非対応	対応	非対応	非対応
AWS	非対応	非対応	非対応	非対応	対応	はい
Azure	非対応	非対応	非対応	非対応	対応	はい
GCP	非対応	非対応	非対応	対応	はい	はい

デイゼロ設定の機能サポート

ハイパーバイザ	CD-ROMの iosxe_config.txt	CD-ROMの ovf-env.xml	OVA のインストール	Config-drive 形式	カスタムデータ	ユーザーデータ
raw 設定のコピーと貼り付け	対応	対応	非対応	対応	はい	はい
特定の設定フィールドの対応可否	非対応	対応	はい	はい	はい	はい
GUI の対応可否	非対応	非対応	対応	非対応	非対応	非対応
ゲストシェルブートストラップ	対応 (IOS の手動設定による)	対応 (IOS の手動設定による)	非対応	対応 (IOS の手動設定による)	対応	対応 (IOS の手動設定による)

- パブリッククラウドには、VM にブートストラップ情報を提供できる入力メカニズムが1つあります。ただし、デバイス側では、カスタムデータ、ユーザーデータ、およびSDWAN (vManage からダウンロードした ciscosdwan\_cloud\_init.cfg ファイルを使用) の3つのブートストラップ入力形式が各クラウドでサポートされます。たとえば、AWS では、EC2 ユーザーデータ テキスト ボックスまたは [File Upload] オプションを使用して、起動時にインスタンスに上記のいずれかの形式でブートストラップ情報を提供できます。その後 Cisco Catalyst 8000V は、提供された設定情報を決定して処理します。
- 上記の表のカスタムデータとユーザーデータの列は、ブートストラップ入力形式を参照しており、元の名前の由来であるクラウドネイティブのブートストラップ入力メカニズムではありません。すべてのパブリッククラウドは両方の形式をサポートしていますが、カスタムデータ形式はより成熟しており、ほとんどのアプリケーションに推奨されるオプションです。
- プライベートクラウドの場合、iosxe\_config.txt 形式または ovf-env.xml 形式の構成ファイルを指定することで、ブートストラップ構成を実行できます。Cisco Catalyst 8000V のインストール中に、付属の CD-ROM を使用して構成ファイルを VM にアップロードする必要があります。
- [デイゼロ設定の前提条件 \(113 ページ\)](#)
- [デイゼロ設定の制約事項 \(113 ページ\)](#)
- [ブートストラップメカニズムの選択 \(113 ページ\)](#)
- [.txt または .xml ファイルを使用したデイゼロ設定 \(114 ページ\)](#)
- [OVF テンプレートのデイゼロ設定 \(119 ページ\)](#)
- [config-drive を使用したデイゼロ設定 \(119 ページ\)](#)
- [カスタムデータを使用したデイゼロ設定 \(120 ページ\)](#)
- [コントローラモードでのデイゼロ設定 \(129 ページ\)](#)

- ルータの動作モードとデイゼロ設定の確認 (130 ページ)
- よく寄せられる質問 (131 ページ)

## デイゼロ設定の前提条件

- Cisco Catalyst 8000V インスタンスをコントローラモードで展開する場合は、vManage からブートストラップ設定ファイルを生成し、生成された設定ファイルの名前を `ciscosdwan_cloud_init.cfg` に変更します。デバイスがコントローラモードで自動的に起動し、vManage に登録されるようにするには、同じファイルを使用します。

vManage から自動生成された設定ファイルを手動で編集しないでください。これを行うと、コントローラが同期しなくなり、デバイスの最初の電源投入と起動が成功しない可能性があります。

## デイゼロ設定の制約事項

- PayG ライセンスモデルを使用する場合、コントローラモードは PayG ライセンスモデルをサポートしていないため、モード切り替えを実行できません。
- 自律モードのみが Dual-IOSd をサポートします。
- ペイロード暗号化のないイメージと NO-LI イメージは、コントローラモードではサポートされていません。
- オンボーディングして動作モードを決定後、コントローラモードから自律モードに、またはその逆に切り替えると構成が失われます。
- 自律モードからコントローラモードに、またはその逆に切り替えると、Cisco Federal Licensing と Smart Licensing の登録が機能しなくなります。ライセンスを機能させるには、再登録する必要があります。
- GUI を使用して Cisco Catalyst 8000V VM を展開する場合、VM に追加されたネットワークインターフェイスの順序は、インターフェイスが作成された順序と一致しない場合があります。これは、インターフェイスの番号付け順序がドライバの名前と PCI アドレスに基づいているためです。この動作により、デイゼロ設定が一部のネットワークインターフェイスに誤って適用される可能性があります。このシナリオが発生した場合は、VM の展開後に、影響を受けるネットワーク インターフェイスを手動で設定する必要があります。

## ブートストラップメカニズムの選択

ハイパーバイザとクラウド全体でサポートされているブートストラップ方式がわかったので、次のステップは、デイゼロ設定を実行するために選択するメカニズムを決定することです。次を使用して、デバイスのデイゼロ設定を構成できます。

- **GUI ツール** : VMware に Cisco Catalyst 8000V をインストールし、OVA 展開を選択した場合は、OVA 展開ウィザードを使用して設定を実行できます。このウィザードはブートストラップ固有のフィールドをサポートしているため、ブートストラップ構成ファイルを手動で作成する必要はありません。
- **.txt ファイル/.xml ファイル** : プライベートクラウド内で、IOS 設定コマンドを使用してデイゼロ設定を行う場合は、`iosxe_config.txt` ファイルを選択することをお勧めします。この方法では、適用する CLI をファイルに貼り付け、CD-ROM として VM に提供できます。
- **カスタムデータ** : AWS、Microsoft Azure、または GCP に Cisco Catalyst 8000V を展開する場合は、推奨される方法はカスタムデータ形式のブートストラップ設定です。この設定方法は、ユーザーデータを使用した設定よりも機能的で柔軟性があります。ユーザーデータを使用して行うデイゼロ設定は、主に、すでに確立されたユーザーデータ展開を持つユーザーを対象としています。

これらの各メカニズムの詳細については、以下をお読みください。

## .txt または .xml ファイルを使用したデイゼロ設定

新しいすぐに使用できるデバイスで、インストール中に自律モードでデバイスを起動する場合は、ブートストラップ関連の設定を指定できます。

KVM 環境などのプライベートクラウドでは、`iosxe_config.txt` ファイルまたは `ovf-env.xml` ファイルを指定してブートストラップ設定を実行できます。この方法では、CLI を介して適用する設定を収集し、ファイルに貼り付けて、このコンテンツを CD-ROM として VM に提供できます。ハイパーバイザ環境に応じて、データはブートストラップ設定に使用されます。

次の項では、このブートストラップ設定方法について詳しく説明します。

### ブートストラップ ファイルの作成

この手順では、ブートストラップ構成ファイルを作成するために実行する必要がある手順について説明します。`.txt` または `.xml` 形式のこのファイルを使用すると、シンプルで柔軟な方法でデバイスのデイゼロ設定を指定できます。

この手順は、KVM などのハイパーバイザで仮想マシンを作成するときに実行できます。

#### 手順

**ステップ 1** `iosxe_config.txt` または `ovf-env.xml` ファイルを作成します。

- `iosxe_config.txt` ファイルを作成するには、IOS `conf t` コマンドを 1 行ずつ含むファイルをこの名前で作成します。
- `ovf-env.xml` ファイルを作成するには、[Bootstrap Properties] から設定するプロパティを選択し、指定した名前のファイルに配置します。

(注)

.xml ファイルの個々のプロパティの詳細については、[ブートストラップのプロパティ \(115 ページ\)](#) を参照してください。

**ステップ 2** .xml または .txt ファイルを仮想マシンで使用可能な形式に変換するには、次のコマンドを使用してファイルからディスクイメージを作成します。

例 :

```
mkisofs -l -o /my/path/c8000v_config.iso <configuration_filename>
```

**ステップ 3** Cisco Catalyst 8000V 仮想マシンの作成中に **c8000v\_config.iso** を追加ディスクとしてマウントします。

## ブートストラップのプロパティ

**ovf-env.xml** ファイルを作成できる個々のブートストラッププロパティについては、次の表を参照してください。

表 13: ブートストラップのプロパティ

プロパティ	説明
console	コンソールモードを設定します。設定可能な値には、auto、virtual、serial などがあります。
domain-name	ルータのドメイン名。
enable-scp-server	IOS SCP 機能を有効にします。
enable-ssh-server	SSH を使用したリモートログインを有効にし、Telnet を介したリモートログインを無効にします。ログインユーザー名とパスワードを設定する必要があります。
hostname	ルータのホスト名。
ios-config	<p>Cisco IOS コマンドの実行を有効にします。</p> <p>複数のコマンドを実行するには、複数の ios-config のインスタンスと各インスタンスに付加されている番号を使用します。たとえば、ios-config-1、ios-config-2 などです。コマンドは、付加された番号に従って番号順に実行されます。</p> <p><b>例</b></p> <pre>ios-config-1="username cisco priv 15 pass ciscoxyz" ios-config-2="ip scp server enable" ios-config-3="ip domain lookup" ios-config-4="ip domain name cisco.com"</pre>

プロパティ	説明
ライセンス	Cisco Catalyst 8000V インスタンスの起動時に使用可能なライセンステクノロジー レベルを設定します。
login-password	ルータのログインパスワード。
login-username	ルータのユーザー名。
mgmt-interface	Cisco Catalyst 8000V インスタンスの管理インターフェイスを指定します。形式は GigabitEthernetx または GigabitEthernetx.xxx である必要があります。
mgmt-ipv4-addr	GigabitEthernet0 管理インターフェイスの IPv4 形式の管理ゲートウェイアドレス/マスク。
mgmt-ipv4-gateway	IPv4 管理デフォルト ゲートウェイ アドレス。DHCP を使用している場合は、フィールドに <b>dhcp</b> と入力します。
mgmt-ipv4-network	管理ゲートウェイがルーティングする IPv4 ネットワーク（「192.168.2.0/24」や「192.168.2.0 255.255.255.0」など）を設定します。この値が指定されていない場合は、デフォルトルート（0.0.0.0/0）が使用されます。
mgmt-vlan	dot1Q VLAN インターフェイスを設定します。GigabitEthernetx.xxx 形式を使用して管理インターフェイスを設定する必要があります。
pnc-agent-local-port	（任意）サービスマネージャからポリシーを受信するように、ローカル Cisco Catalyst 8000V の Cisco Prime Network Services Controller サービスエージェント SSL ポートを設定します。  この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V をリモートで管理する場合に使用されます。
pnc-ipv4-addr	Cisco Prime Network Services Controller の IP アドレスを設定します。  この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V インスタンスをリモートで管理する場合に使用されます。
pnc-shared-secret-key	コントローラから SSL 証明書を設定するために、Cisco Prime Network Services Controller エージェントの Cisco Prime Network Services Controller 共有秘密キーを設定します。  この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V インスタンスをリモートで管理する場合に使用されます。
privilege-password	特権（有効化）アクセス用のパスワードを設定します。
resource-template	リソーステンプレートを設定します。設定可能な値には、default、service_plane_medium、service_plane_heavy などがあります。



(注) **ovf-env.xml** ファイルのサンプルについては、[ovf-env.xml ファイルの例 \(117ページ\)](#) を参照してください。

## iosxe\_config.txt ファイルの例

```
hostname ultra-ios_cfg
license smart enable
username lab privilege 15 password lab
ip domain-name cisco.com
crypto key generate rsa modulus 1024
interface GigabitEthernet1
ip address 10.0.0.5 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
login local
exit
```

### OpenStack 環境の iosxe\_config.txt ファイルの例

```
hostname c8kv-ios_cfg
license smart enable
username lab priv 15 secret lab
ip domain-name cisco.com
interface GigabitEthernet1
ip address 10.0.0.5 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
login local
exit
```

## ovf-env.xml ファイルの例

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="com.cisco.c8000v.license.1" oe:value="security"/>
    <Property oe:key="com.cisco.c8000v.console.1" oe:value="serial"/>

  <Property oe:key="com.cisco.c8000v.config-version.1" oe:value="1.0"/>
    <Property oe:key="com.cisco.c8000v.domain-name.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.enable-scp-server.1" oe:value="False"/>
    <Property oe:key="com.cisco.c8000v.enable-ssh-server.1" oe:value="False"/>
    <Property oe:key="com.cisco.c8000v.hostname.1" oe:value="lab"/>
    <Property oe:key="com.cisco.c8000v.license.1" oe:value="ax"/>
    <Property oe:key="com.cisco.c8000v.login-password.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.login-username.1" oe:value="lab"/>
    <Property oe:key="com.cisco.c8000v.mgmt-interface.1" oe:value="GigabitEthernet1"/>

    <Property oe:key="com.cisco.c8000v.mgmt-ipv4-addr.1" oe:value="172.25.223.251/25"/>
```

```

<Property oe:key="com.cisco.c8000v.mgmt-ipv4-gateway.1" oe:value="172.25.223.129"/>
    <Property oe:key="com.cisco.c8000v.mgmt-ipv4-network.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.mgmt-vlan.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.pnsc-agent-local-port.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.pnsc-ipv4-addr.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.pnsc-shared-secret-key.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.privilege-password.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.remote-mgmt-ipv4-addr.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.resource-template.1"
oe:value="service_plane_medium"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0001" oe:value="logging buffered
10000"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0002" oe:value="hostname uut-ovf"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0003" oe:value="ip domain-name
cisco.com"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0004" oe:value="crypto key generate
rsa modulus 1024"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0005" oe:value="interface
GigabitEthernet2"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0006" oe:value="ip address 10.0.0.5
255.255.255.0"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0007" oe:value="no shut"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0008" oe:value="exit"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0009" oe:value="ip route 0.0.0.0
0.0.0.0 10.0.0.1"/>
  </PropertySection>
</Environment>

```

### OpenStack の ovf-env.xml ファイルの例

```

<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="com.cisco.c8000v.license.1" oe:value="network-premier addon
dna-premier"/>
    <Property oe:key="com.cisco.c8000v.console.1" oe:value="virtual"/>
    <Property oe:key="com.cisco.c8000v.config-version.1" oe:value="1.0"/>
    <Property oe:key="com.cisco.c8000v.domain-name.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.enable-scp-server.1" oe:value="False"/>
    <Property oe:key="com.cisco.c8000v.enable-ssh-server.1" oe:value="False"/>
    <Property oe:key="com.cisco.c8000v.hostname.1" oe:value="lab"/>
    <Property oe:key="com.cisco.c8000v.login-password.1" oe:value="lab#123"/>
    <Property oe:key="com.cisco.c8000v.login-username.1" oe:value="lab"/>
    <Property oe:key="com.cisco.c8000v.mgmt-interface.1" oe:value="GigabitEthernet1"/>
    <Property oe:key="com.cisco.c8000v.mgmt-ipv4-addr.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.mgmt-ipv4-gateway.1" oe:value="192.168.8.1"/>
    <Property oe:key="com.cisco.c8000v.mgmt-ipv4-network.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.mgmt-vlan.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.pnsc-agent-local-port.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.pnsc-ipv4-addr.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.pnsc-shared-secret-key.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.privilege-password.1" oe:value="lab#123"/>
    <Property oe:key="com.cisco.c8000v.remote-mgmt-ipv4-addr.1" oe:value=""/>
    <Property oe:key="com.cisco.c8000v.resource-template.1" oe:value="service-plane-medium"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0001" oe:value="logging buffered 10000"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0002" oe:value="hostname uut-ovf"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0003" oe:value="ip domain name cisco.com"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0005" oe:value="interface GigabitEthernet2"/>
    <Property oe:key="com.cisco.c8000v.ios-config-0006" oe:value="ip address dhcp"/>

```

```
<Property oe:key="com.cisco.c8000v.ios-config-0007" oe:value="no shut"/>
<Property oe:key="com.cisco.c8000v.ios-config-0008" oe:value="exit"/>
<Property oe:key="com.cisco.c8000v.ios-config-0009" oe:value="ip route 0.0.0.0 0.0.0.0
192.168.8.1"/>
<Property oe:key="com.cisco.c8000v.ios-config-0010" oe:value="interface GigabitEthernet1"/>
<Property oe:key="com.cisco.c8000v.ios-config-0011" oe:value="ip address dhcp"/>
<Property oe:key="com.cisco.c8000v.ios-config-0012" oe:value="no shut"/>
</PropertySection>
</Environment>
```

## OVF テンプレートのデイレゼロ設定

デイレゼロのブートストラップを完全にサポートする OVF 展開は、vCenter UI または COT ツールを介して VMware でのみサポートされます。ESXi ハイパーバイザで実行されている Cisco Catalyst 8000V のデイレゼロ設定は、[VM への OVA の展開 \(63 ページ\)](#) で入手できます。

COT ツールを使用して展開のデイレゼロ設定を実行する方法については、[COT を使用した Cisco Catalyst 8000V の基本的なプロパティの編集 \(67 ページ\)](#) を参照してください。

## config-drive を使用したデイレゼロ設定

Cisco Catalyst 8000V の起動時に設定がロードされるように指定するには、**--config-drive** オプションを使用します。CD-ROM および 2 番目のハードドライブには、**config-drive** 形式の設定情報を含めることもできます。いずれの場合も、この情報は、`iosxe_config.txt` ファイルまたは `ovf-env.xml` ファイルのいずれかの形式と一致する内容を持つファイルです。

デイレゼロ設定に **config drive** オプションを使用するには、**--config-drive** オプションを **true** に設定し、起動するルータ設定を入力する構成ファイルの名前を指定します。次の方法で構成情報を指定できます。

### XML/TXT ファイルとして

このオプションでは、次の 2 つの形式のいずれかで構成ファイルを指定する必要があります。

- `ovf-env.xml` ファイル形式の `xml` ファイルとして (OVF 展開の場合)
- `iosxe_config.txt` ファイル形式のテキストファイルとして

`.txt` ファイルまたは `.xml` ファイルのいずれか 1 つの構成ファイルタイプのみを使用し、両方は使用しないことを強く推奨します。

次の設定例を参照してください。次のいずれかの設定を使用して、ファイルシステムで構成ファイルを指定します。

```
nova boot c8000v-vm-174 --image c8000v-174 --flavor c8000v.2vcpu.4gb --nic
port-id=6773bell-7b95-48cd-b372-fb8a3cae2b50 --config-drive=true --file
ovf-env.xml=/home/stack/conf_files/ut/ovf-env.xml
```

または

```
nova boot c8000v-vm-174 --image c8000v-174 --flavor c8000v.2vcpu.4gb --nic
port-id=6773be11-7b95-48cd-b372-fb8a3cae2b50 --config-drive=true --file
iosxe_config.txt=/home/stack/conf_files/ut/iosxe_config.txt
```



(注) これらのファイル名はハードコードされており、`config-drive` 設定を起動するのに必要です。

### ユーザーデータの使用

OpenStack などの特定の環境では、`user_data` オプションを使用して、`config-drive` 形式でファイルシステムにファイルを提供します。OpenStack 環境については、次のユーザーデータの例を参照してください。

```
openstack server create "admin-VK-C8KISOSerial-20210917"
--config-drive true
--image c8kv-image-176
--flavor m1.large
--network mgmt-nt
--network prod-nt
--block-device-mapping id=admin-VK-EmptyVolume-SerialTest:type=volume
--user-data userdata.txt
```

## カスタムデータを使用したデイズロ設定

Cisco Catalyst 8000V インストールファイルをダウンロードし、環境にイメージを展開した後、デバイスが完全に機能するようにするには、Cisco Catalyst 8000V インスタンスを手動で設定する必要があります。設定手順を自動化するため、またはオンプレミスサイトに接続するために、サポートされているすべてのパブリッククラウドとプライベートクラウドで Cisco Catalyst 8000V カスタムデータまたはユーザーデータをアップロードできます。

クラウド サービス プロバイダーまたはプライベートクラウドのカスタムデータをアップロードすることで、デイズロ設定やブートストラップ設定を自動化できます。ブートストラップ構成ファイル (`iosxe_config.txt` ファイル) をアップロードまたはアタッチするか、ユーザーデータを提供してこれらのプロセスを自動化し、最小限の操作またはまったく操作せずにデバイスを機能状態にします。

デイズロブートストラップファイルを使用すると、Cisco IOS XE 設定コマンドを実行したり、デイズロのゲストシェルに Python パッケージをインストールしたり、デイズロのゲストシェルでスクリプトを実行したり、必要なテクノロジーパッケージを使用して Cisco Catalyst 8000V インスタンスを起動するためのライセンス情報を提供したりできます。

カスタムデータを使用して Cisco Catalyst 8000V インスタンスを起動するには、次の手順を実行します。

## デイズロ ブートストラップ ファイルの編集

ブートストラップファイルを編集するには、IOS Configuration、Scripts、Script credentials、Python package、および Licensing の各プロパティを設定します。プロパティは、任意の順序でブートストラップファイルに配置できます。プロパティ間の依存関係は、次の各プロパティの説明に

記載されています。<https://github.com/csr1000v/customdata-examples>にあるブートストラップファイルの例を参照してください。

ブートストラップファイルのプロパティを定義したら、ファイルをアップロードします。

## IOS 設定プロパティの設定

デイゼロで特定の IOS 設定をブートストラップする場合は、IOS 設定プロパティを設定します。次の例を参照してください。

```
Section: IOS configuration
hostname C8000V1
interface GigabitEthernet1
description "static IP address config"
ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2
description "DHCP based IP address config"
ip address dhcp
```

Section: IOS configuration という最初の行の後に、Cisco Catalyst 8000V ルータで実行する Cisco IOS XE 設定コマンドのリストを入力します。

このコマンドを実行すると、上記の IOS 設定がデイゼロの Cisco Catalyst 8000V ルータに適用されます。

## スクリプトプロパティの設定

スクリプトプロパティは、展開を自動化し、他の自動化の目標を達成するのに役立ちます。ゲストシェルのコンテキストで Day0 に Python または bash スクリプトを実行する場合は、Scripts プロパティで Python または bash スクリプトのパブリック URL と引数を指定することで同じことを実現できます。

スクリプトには、スクリプトの最初の行にシバン (!) 文字を含むコードを含める必要があります。この行は、スクリプトコードの解析に使用する必要があるスクリプトインタープリタ (Python または Bash) を Cisco IOS-XE に通知します。たとえば、Python スクリプトの最初の行には `#!/usr/bin/env python` を含めることができますが、bash スクリプトの最初の行には `#!/bin/bash` を含めることができます。この行により、Python または Bash スクリプトを Linux 環境で実行可能コードとして実行できます。

スクリプトを実行すると、Cisco Catalyst 8000V インスタンスのゲストシェルコンテナでスクリプトが実行されます。ゲストシェルコンテナにアクセスするには、`guestshell EXEC` モードコマンドを使用します。ゲストシェルコマンドの詳細については、『[Programmability Configuration Guide](#)』を参照してください。

Scripts プロパティを設定するには、次の形式に従います。

```
Section: scripts
public_url <arg1> <arg2>
```

このスクリプトでは、プロパティの最初の行に `Section: Scripts` と記載する必要があります。プロパティの2行目に、スクリプトの URL とスクリプトの引数を入力します。スクリプトは、python または bash スクリプトのいずれかです。Cisco Catalyst 8000V インスタンスの作成時に

ブートストラップファイルがアップロードされると、最初の起動時にゲストシェルでスクリプトが実行されます。

スクリプトのその他の例については、<https://github.com/csr1000v/customdata-examples> の「Scripts」セクションを参照してください。また、次の2つの例も参照してください。

### 例 1

```
Section: Script
https://raw.githubusercontent.com/csr1000v/customdata-examples/master/scripts/smartLicensingConfigurator.py --idtoken "<token_string>"
--throughput <throughput_value>
```

Scripts プロパティの2行は、指定された URL の customdata-examples リポジトリから smartLicensingConfigurator.py スクリプトを取得します。スクリプトは、引数 idtoken と throughput を使用して、Cisco Catalyst 8000V のゲストシェルコンテナで実行されます。

### 例 2

```
Section: Scripts
ftp://10.11.0.4/dir1/dir2/script.py -a arg1 -s arg2
```

Scripts プロパティのこれらの2行は、IP アドレス 10.11.0.4 の FTP サーバーから script.py スクリプトを取得し、引数 arg1 と arg2 を使用して Cisco Catalyst 8000V のゲストシェルコンテナで ./script.py -a arg1 -s arg2 bash コマンドでスクリプトを実行します。



- (注) Scripts プロパティのスクリプトで、標準の CentOS Linux リリース（ゲストシェルで使用される CentOS Linux リリース。現在は CentOS Linux リリース 7.1.1503）に含まれていない Python パッケージが必要な場合は、Python パッケージプロパティの Python パッケージに関する情報を含める必要があります。詳細については、[Python パッケージプロパティの設定（123 ページ）](#)を参照してください。

ブートストラップファイルをアップロードして bash または Python スクリプトを実行する前に、Scripts プロパティで使用する予定の URL をテストすることをお勧めします。

ftp://10.11.0.4/dir1/dir2/script.py -a arg1 -s arg2 URL をテストするには、最初に curl ソフトウェアツールを実行してスクリプトファイルをダウンロードします。ゲストシェルで、次の例に示すように、curl コマンドを入力します。

```
curl -m 30 --retry 5 --user username:password
ftp://10.11.0.4/dir1/dir2/script_needs_credentials.py.
```

curl コマンドが成功すると、URL が正しいかどうかを確認する Python スクリプトのコピーがダウンロードされます。

## スクリプトログイン情報プロパティの設定

Script プロパティで FTP サーバーを指定していて、そのサーバーにユーザー名とパスワードのログイン情報が必要な場合は、Script credentials プロパティを使用してログイン情報を指定します。FTP サーバーに匿名でアクセスできる場合は、Script credentials プロパティを使用する必要はありません。

Script credentials プロパティの URL とパラメータと一致する URL とパラメータを使用して、Scripts プロパティを設定します。Script credentials プロパティを設定するには、次の形式に従います。

```
Section: Script credentials
public_url <username> <password>
```

### 例 1

```
Section: Script credentials
ftp://10.11.0.4/dir1/dir2/script1.py userfoo foospass
```

Script credentials プロパティの 2 行目は、Python スクリプト script1.py のユーザー名 (userfoo) とパスワード (foospass) のログイン情報の値を指定します。

Scripts プロパティにも含まれている FTP サーバーの名前を含めます。Scripts プロパティの例は、ftp://10.11.0.4/dir1/dir2/script1.py -a arg1 -s arg2 です。[スクリプトプロパティの設定 \(121 ページ\)](#) の例 2 を参照してください。

## Python パッケージプロパティの設定

Python パッケージが Scripts プロパティのスクリプトに必要であり、標準の CentOS Linux リリース 7.1.1503 の一部ではない場合は、Python パッケージプロパティにパッケージに関する情報を含める必要があります。ブートストラップファイルに Python パッケージプロパティを含めることで、Scripts プロパティで指定したスクリプトを実行する前に、Cisco Catalyst 8000V が必要な Python パッケージをダウンロードしてインストールするようにします。



(注) Cisco Catalyst 8000V はゲストシェルで Python 3 のみサポートします。

Python パッケージプロパティを設定するには、次で指定される形式に従います。

```
Section: Python package
package_name [ version ] [ sudo ] { [ pip_arg1 [ ..[ pip_arg9 ] ] ] }
```

引数: *version*、**sudo**、および *pip\_arg1* ~ *pip\_arg9* はオプションです。pip コマンドの引数は、「{」と「}」のかっこの中に配置する必要があります。

*version* 引数を指定すると、特定のバージョン番号がダウンロードされます。

*sudo* 引数を指定すると、パッケージは sudo ユーザーとしてダウンロードされます。

### 設定例 (Microsoft Azure)

#### 例 1

この例では、Python パッケージプロパティの 2 行目は、*package\_name* が *ncclient* で、*version* が「0.5.2」であることを指定しています。ブートストラップファイルがアップロードされると、*ncclient* パッケージのバージョン 0.5.2 が Cisco Catalyst 8000V のゲストシェルコンテナにインストールされます。

```
Section: Python package
```

```
ncclient 0.5.2
```

### 例 2

```
Section: Python package
```

```
c8000v_azure_guestshell 1.1.2 sudo {--user}
```

この例では、Python パッケージプロパティの 2 行目で、*package\_name* が「c8000v\_azure\_guestshell」、*version* が「1.1.2」と指定されています。ブートストラップファイルがアップロードされると、c8000v\_azure\_guestshell パッケージのバージョン 1.1.2 が Cisco Catalyst 8000V のゲストシェルコンテナにインストールされます。次のコマンドが `sudo` ユーザーとして実行されます。 `sudo pip install c8000v_azure_guestshell==1.1.2 --user。`



(注) 引数を指定しない場合、`--user` がデフォルトの引数として使用されます。

## 設定例 (Google Cloud Platform)

### 例 1

```
Section: Python package
```

```
ncclient 0.5.2
```

この例では、Python パッケージプロパティの 2 行目は、*package\_name* が「ncclient」で、*version* が「0.5.2」であることを指定しています。ブートストラップファイルがアップロードされると、ncclient パッケージのバージョン 0.5.2 が Cisco Catalyst 8000V インスタンスのゲストシェルコンテナにインストールされます。

### 例 2

```
Section: Python package
```

```
c8000v_gcp_ha 3.0.0 sudo {--user}
```

この例では、Python パッケージプロパティの 2 行目は、*package\_name* が「c8000v\_gcp\_ha」で、*version* が「3.0.0」であることを指定しています。ブートストラップファイルがアップロードされると、c8000v\_gcp\_ha package パッケージのバージョン 3.0.0 が Cisco Catalyst 8000V インスタンスのゲストシェルコンテナにインストールされます。次のコマンドが `sudo` ユーザーとして実行されます。 `pip3 install c8000v_gcp_ha=3.0.0 --user。`



(注) 引数を指定しない場合、`--user` がデフォルトの引数として使用されます。

## ライセンスプロパティの設定

Cisco Catalyst 8000V のライセンス テクノロジー レベルを指定するライセンスプロパティを設定します。

次のようにプロパティの最初の行を入力します。Section: License。次の形式を使用して、ライセンスの技術レベルを指定するプロパティの2行目を入力します。TechPackage:tech\_level。



- (注) TechPackage: と tech\_level の間にはスペースを入れないでください。設定可能な tech\_level 値には、ax、security、appx、ibase などがあります。

tech\_level は小文字にする必要があります。

#### 例 1

```
Section: License
TechPackage:security
```

## デイズロ ブートストラップ ファイルの提供

次の Azure CLI コマンドを実行して、Cisco Catalyst 8000V VM を作成するデイズロ ブートストラップ ファイルを指定します。

```
az vm create --name C8000V-name --resource-group resource-group { [ arg1 [ ..[ arg9 ] ] } --custom-data bootstrap-file
```

**az vm create** コマンドの詳細については、<https://docs.microsoft.com/en-us/cli/azure/vm?view=azure-cli-latest#az-vm-create> を参照してください。

次の例を参照してください。

```
az vm create -n c8000V-VM-Name -g MyResourceGroup --image
cisco:cisco-c8000V-1000v:16_6:16.6.120170804 --data-disk-sizes-gb 8 --availability-set
myAv1Set --nics nic1 nic2 nic3 nic4 --admin-username azureuser --admin-password
"+Cisco123456" --authentication-type password -l westus --size Standard_DS4_v2
--custom-data bootstrap.txt..
```

このコマンドを実行すると、Cisco Catalyst 8000V VM が作成されます。ルータは、ブートストラップファイル「bootstrap.txt」のコマンドを使用して設定されます。

カスタム データ ブートストラップ設定ファイルを指定するには、**Cisco C8000V Settings** オプションを使用します。

Linux VM の管理の詳細については、「[Tutorial: Create and Manage Linux VMs with the Azure CLI 2.0](#)」を参照してください。

## カスタムデータ設定の確認 (Microsoft Azure)

デイズロ ブートストラップ ファイルをアップロードすると、VM が作成され、設定コマンドが実行されます。次のコマンドを実行して、各プロパティの設定コマンドを確認します。

ライセンスプロパティが機能しているかどうかを確認するには、Cisco Catalyst 8000V の Cisco IOS XE CLI で **show version** コマンドを入力します。たとえば、セキュリティライセンスへの参照が表示されます。

スクリプトプロパティでコマンドを実行した後にエラーが発生したかどうかを確認するには、`/home/guestshell/customdata` ディレクトリの `customdata.log` ファイルを調べます。`scriptname.log` ファイルには、スクリプトによって `STDOUT` に送信される出力が保存されます。

Python プロパティが機能したかどうかを確認するには、`pip freeze | grep package-name` コマンドを入力して、現在インストールされている Python パッケージを表示します。目的のパッケージ `package-name` を検索します。

IOS の設定プロパティで Cisco IOS XE コマンドが成功したかどうかを確認するには、`show running-configuration` コマンドを入力します。次に、このコマンドの出力例を示します。

```
Router#show version
Cisco IOS XE Software, Version
Copyright (c) 1986-2020 by Cisco Systems, Inc.

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON

Router uptime is 1 minute
Uptime for this control processor is 7 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
Last reload reason: Unknown reason

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: ipbase
License Type: N/A(Smart License Enabled)
Next reload license Level: ipbase

The current throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C8000V (VXE) processor (revision VXE) with 2271486K/3075K bytes of memory.
Processor board ID 9MUG8CATY8R
```

```

Router operating mode: Controller-Managed
1 Gigabit Ethernet interface
32768K bytes of non-volatile configuration memory.
8106756K bytes of physical memory.
11530240K bytes of virtual hard disk at bootflash:.

Configuration register is 0x2102

[guestshell@guestshell ~]$ pip3 freeze | grep gpg==1.10.0
gpg==1.10.0
[guestshell@guestshell ~]$

Router#show running-config
Building configuration...

Current configuration : 6982 bytes
!
! Last configuration change at 14:34:36 UTC Fri Nov 6 2020 by NETCONF
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform console serial
!
hostname Router
!
boot-start-marker
boot-end-marker
!
vrf definition 65528
!
  address-family ipv4
  exit-address-family
!
no logging buffered
no logging rate-limit
!
aaa new-model
!
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization exec default local
!
aaa session-id common
fhrp version vrrp v3
!
no ip dhcp use class
!
no ip igmp ssm-map query dns
login on-success log
ipv6 unicast-routing
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-2465303444
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2465303444

```

```

revocation-check none
rsaкеypair TP-self-signed-2465303444
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-2465303444
certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32343635 33303334 3434301E 170D3230 31313036 31343333
  35345A17 0D333031 31303631 34333335 345A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34363533
  30333434 34308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100B02F AD33A0FF 0C50D3F2 D06CFDC6 F3CB73BB 4070D649 E07D16CE
  E6271C90 34E86882 822C8D71 E4BAC29D 85285258 51E748E1 8C9FB2C5 12242A22
  7FB71551 02CB4DBC 64089D2F 8DDB6C4A D3E2F112 8E16E71F FE70D102 F59862A3
  E920E77E 52E62E02 1979F800 3D13601F 27C42F81 483BFB34 697F1C20 3952626A
  CA1F5805 26D50A39 33F264D6 1AD485A0 8EB45882 FC97DCA2 106C8FAD 8CD8C0E6
  FF609188 B4677AB0 FBBE77F2 359EA002 E1A5D37D EA895FF3 92732A2B 63465DFD
  4A2A277C 17E7F720 2007A6B6 A7C7296F D0CD2707 8C7C9690 F86B0642 1BA9F28C
  F729157B 8C472E40 78A4E6BE 70471018 4B62EE36 48193FCA 062DB09F 38BC420B
  687E5866 DFA10203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 14ABBD00 3D02C6E1 7706FA96 29B037A8 583E7B2E
  69301D06 03551D0E 04160414 ABBD003D 02C6E177 06FA9629 B037A858 3E7B2E69
  300D0609 2A864886 F70D0101 05050003 82010100 40C60BF0 2184CF86 08CACB66
  73E74D63 E87A6661 DC839037 D0DB08D0 33C4993C EC326432 E3573D1B EC3B42AF
  F410BF72 2AAB6D8F 1406B352 FE6B5365 CCA7E094 96980FC7 A4B77A02 49CB8C01
  3EC87F01 58BFEE33 0DA222DB 0A1BA130 0AC01F1F FDBF2085 D41EFA45 7A4C7F5E
  2D004D04 D11433BF 69337D90 117A86ED 2CF57A49 AD7DA227 129E53DF 55E12E03
  4D8E0097 A29DC365 11E8B386 891C310E F19EDF6D D9B3EA1E E26ABDD8 EF82D8E9
  B0484E26 C0FC1D71 91B19B70 221E1A1A 090F8EA1 3A5FC4FD A4EF36CD EFD2F1F4
  6056C87D 8A76ED1A 68FB76F5 956C6B50 7EFA9D8C 90EA910F 187EBD13 0BF76E5A
  0B9CE20E AA5927C4 7AD13C28 58C6E920 76E36475
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBAE3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEB7CF9F 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0

```

```

D697DF7F 28
quit
!
license udi pid C8000V sn 9MUG8CATY8R
diagnostic bootup level minimal
memory free low-watermark processor 69848
!
!
username admin privilege 15 secret 9
$14$vKLj$yfnFjRidlKJg9.$4obKgKyy4TsoUs0sJ2t3HXpNA3XjYWRBnnYKBwVeJrw
!
redundancy
!
interface Loopback65528
vrf forwarding 65528
ip address 192.168.1.1 255.255.255.255
!

```

## カスタムデータ設定の確認 (Google Cloud Platform)

カスタムデータスクリプトを実行すると、VMが作成され、設定コマンドが実行されます。同じことを確認するには、次のコマンドとスクリプトを使用します。

- **show version** : Cisco Catalyst 8000V インスタンスの Cisco IOS XE CLI でライセンスプロパティが機能したかどうかを確認するには、**show version** コマンドを入力します。たとえば、セキュリティライセンスへの参照が出力に表示されます。
- スクリプトプロパティでコマンドを実行した後にエラーが発生したかどうかを確認するには、`/bootflash/<cloud>/` ディレクトリの `customdata.log` ファイルを調べます。`scriptname.log` ファイルには、スクリプトによって `STDOUT` に送信される出力が保存されます。
- Python プロパティが機能したかどうかを確認するには、ゲストシェルから `pip freeze | grep <package-name>` コマンドを入力して、現在インストールされている Python パッケージを表示します。ここで、`package-name` は、特に検索するパッケージを指します。
- IOS 設定プロパティで Cisco IOS XE コマンドを確認するには、**show running-configuration** コマンドを実行します。

## コントローラモードでのデイゼロ設定

コントローラ (SD-WAN) モードで Cisco Catalyst 8000V のデイゼロ設定を実行する場合は、vManage からダウンロードした `ciscosdwan_cloud_init.cfg` ファイルの内容を指定する必要があります。

コントローラモードに切り替える場合、または Cisco SD-WAN 機能で Cisco Catalyst 8000V をブートストラップする場合は、「[Install and Upgrade for Cisco Catalyst 8000V Controller Mode](#)」を参照してください。



- (注) Cisco CSP-5000 ハイパーバイザで実行されている Cisco Catalyst 8000V インスタンスの場合、[Day Zero Config] 画面で設定を入力する場合は、次の形式を維持してください。
- [Source File Name] : このフィールドの値を `day0_ciscosdwan_cloud_init.cfg` の形式で入力します。
  - [Destination File Name] : このフィールドの値を `day0-dest-filename/openstack/content/ciscosdwan_cloud_init.cfg` の形式で入力します。



- (注) SD-WAN 形式の設定では、最初の起動時に `confd` が設定を正常に適用できない場合、ボックスではデイゼロで設定が機能していない可能性があります。これは、ログインに SSH が必要なパブリッククラウド環境では特に重要です。プロビジョニング時に問題が発生した場合は、設定を慎重に確認してください。

## ルータの動作モードとデイゼロ設定の確認

IOS XE 17.4 以降のリリースに正常に展開またはアップグレードされたかどうかを確認するには、**show version** コマンドを実行します。このコマンドはインスタンスのバージョンを表示し、**operating device-mode** パラメータは Cisco Catalyst 8000V インスタンスが実行されているモードを表示します。

### 自律モードでの Cisco Catalyst 8000V インスタンスの設定出力例

```
Device# show version | inc operating
Router operating mode: Autonomous
Device# show platform software device-mode
Operating device-mode: Autonomous
Device-mode bootup status:
-----
Device# show platform software chasfs r0 brief | inc device_managed_mode
/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [autonomous]
/tmp/fp/chasfs/etc/device_managed_mode : [autonomous]
Device# show version | inc Last reload
Last reload reason: Enabling autonomous-mode
```

## よく寄せられる質問

- Q.** これまで Cisco IOS XE イメージを使用していました。これからどのモードを選択すればよいでしょうか。
- A.** これまで Cisco IOS XE universalk9 イメージを使用していた場合は、IOS XE 17.4 イメージを展開し、自律モードを開始します。

- Q.** Cisco Catalyst 8000V 17.4 リリースにアップグレードする場合、ブートストラップ設定を指定する必要がありますか。
- A.** 既存の非 SD WAN ユーザーであり、IOS XE 17.4 リリース（自律モード）にアップグレードする場合は、アップグレードを直接実行できます。デイズロまたはカスタムデータの設定を再度実行する必要はありません。

Microsoft Azure または Google Cloud Platform で実行されている Cisco Catalyst 8000V インスタンスの場合、デバイスは、Cisco Catalyst 8000V インスタンスを初めて設定したときに指定したカスタムデータを使用します。

AWS で実行されている Cisco Catalyst 8000V インスタンスの場合、デバイスはクラウドサービスプロバイダーからカスタムデータを取得します。

- Q.** モードを切り替えた後、カスタムデータ設定はどうなりますか。
- A.** 既存の設定データが削除されます。新規インストールの場合と同様に、ブートストラップまたはカスタムデータ設定を実行する必要があります。
- Q.** 初期設定へのリセット後、カスタムデータはどうなりますか。
- A.** 初期設定へのリセットを実行すると、ディスク上の設定とファイルが消去されます。ルータは新規インストールのように起動し、適切な場所で構成ファイルを探します。このアクションによって、モードおよび関連する設定が決定されます。
- Q.** PayG ライセンスを使用して Cisco Catalyst 8000V インスタンスを任意のモードで展開できますか。
- A.** PayG ライセンスモデルを使用する場合、Cisco Catalyst 8000V インスタンスをコントローラモードで展開したり、コントローラモードに切り替えたりすることはできません。このモードは、PayG ライセンスモデルをサポートしていません。





## 第 11 章

# Security-Enhanced Linux のサポート

この章では SELinux の機能について説明します。具体的な内容は次のとおりです。

- [概要 \(133 ページ\)](#)
- [SELinux の前提条件 \(133 ページ\)](#)
- [SELinux の制限事項 \(133 ページ\)](#)
- [SELinux に関する情報 \(134 ページ\)](#)
- [SELinux の設定 \(134 ページ\)](#)
- [SELinux の有効化の確認 \(136 ページ\)](#)
- [SELinux のトラブルシューティング \(137 ページ\)](#)

## 概要

Security-Enhanced Linux (SELinux) は、Linux カーネルセキュリティ モジュールとシステムユーティリティで構成されるソリューションで、強力な柔軟な Mandatory Access Control (MAC) アーキテクチャを Cisco IOS-XE プラットフォームに組み込みます。

SELinux には機密性と整合性の要件に基づいて情報を分離するための拡張メカニズムが備わっています。これにより、アプリケーションのセキュリティメカニズムの改ざんやバイパスの脅威に対処し、悪意のあるアプリケーションや欠陥のあるアプリケーションによって引き起こされる可能性のある障害を封じ込めることができます。

## SELinux の前提条件

この機能に関する固有の要件はありません。

## SELinux の制限事項

この機能に関する特定の制限はありません。

## SELinux に関する情報

SELinux はユーザープログラムやシステムサービスを、割り当てられた機能を実行するために必要になる最小限の権限に制限する強制アクセス制御ポリシーを適用します。これにより、（バッファのオーバーフローや設定ミスなどによって）侵害された場合、害を生じさせるこれらのプログラムやデーモンの能力が削減または排除されます。これは、Cisco IOS-XE プラットフォームで MAC を適用することによる最小権限の原則の実用的な実装です。この制限メカニズムは、従来の Linux アクセス制御メカニズムとは独立して機能します。SELinux は、アプリケーションプロセスからリソースオブジェクトへのアクセスを制御するポリシーを定義する機能を提供します。これにより、プロセス動作の明確な定義と制限を明確にできます。

SELinux は、システムで有効になっている場合、**Permissive モード**または**Enforcing モード**のいずれかで動作します。

- **Permissive モード**では、SELinux はポリシーを適用せず、リソースアクセスポリシーの違反によって発生した拒否のシステムログのみを生成します。操作は拒否されず、リソースアクセスポリシー違反についてのみログに記録されます。
- **Enforcing モード**では、SELinux ポリシーが有効になり、適用されます。アクセスポリシールールに基づいてリソースアクセスを拒否し、システムログを生成します。

サポートされている Cisco IOS XE プラットフォームでは、SELinux はデフォルトで **Enforcing モード**で有効になっています。Enforcing モードでは、必要な許可ポリシーを持たないシステムリソースアクセスは違反として扱われ、操作は拒否されます。拒否が発生すると、違反操作は失敗し、システムログが生成されます。Enforcing モードでは、ソリューションはアクセス違反防止モードで機能します。

## SELinux の設定

Enforcing モードで SELinux 機能を有効化または操作するために必要な追加の要件や設定手順はありません。

SELinux の機能の一部として、次のコマンドが導入されています。

```
set platform software selinux {default | enforcing | permissive}
platform security selinux {enforcing | permissive}
show platform software selinux
```



(注) これらの新しいコマンドは、サービス内部コマンドとして実装されます。

## SELinux の設定 (EXEC モード)

`set platform software selinux` コマンドを使用して、EXEC モードで SELinux を設定します。

次に、EXEC モードでの SELinux 設定の例を示します。

```
Device# set platform software selinux ?

default Set SELinux mode to default
enforcing Set SELinux mode to enforcing
permissive Set SELinux mode to permissive
```

## SELinux の設定 (CONFIG モード)

**platform security selinux** コマンドを使用して、コンフィギュレーションモードで SELinux を設定します。

次の例は、CONFIG モードでの SELinux 設定を示しています。

```
Device(config)# platform security selinux

enforcing Set SELinux policy to Enforcing mode
permissive Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

## SELinux の例

次に、モードを Enforcing から Permissive に変更した場合の出力例を示します。

```
**Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!"
```

次に、モードを Permissive から Enforcing に変更した場合の出力例を示します。

```
**Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode upgraded to enforcing!"
```



(注) SELinux モードが変更されると、この変更はシステムセキュリティイベントと見なされ、システムログメッセージが生成されます。

## Syslog メッセージリファレンス

機能重大度ニーモニック	<b>%SELINUX-1-VIOLATION</b>
重大度の意味	アラートレベルログ
メッセージ	該当なし

機能重大度	%SELINUX-1-VIOLATION
メッセージの説明	リソースのアクセスポリシーが存在しないプロセスによって、リソースアクセスが実行されました。操作にフラグが設定され、リソースアクセスが拒否されました。プロセスリソースアクセスが拒否されたという情報を含むシステムログが生成されました。
コンポーネント	SELINUX
推奨処置	次の関連情報を添付ファイルとして Cisco TAC にご連絡ください。 <ul style="list-style-type: none"> <li>• コンソールまたはシステムに出力されるとおりのメッセージ</li> <li>• <b>show tech-support</b> コマンドの出力（テキストファイル）</li> <li>• ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）： <b>request platform software trace archive target &lt;URL&gt;</b></li> <li>• <b>show platform software selinux</b> コマンドの出力</li> </ul>

次に、syslog メッセージの例を示します。

例 1 :

```
*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

例 2 :

```
*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

## SELinux の有効化の確認

**show platform software selinux** コマンドを使用して、SELinux 設定モードを表示します。

```
Device# show platform software selinux
=====
IOS-XE SELINUX STATUS
```

```
=====
SELinux Status :    Enabled
Current Mode :      Enforcing
Config file Mode :  Enforcing
```

## SELinux のトラブルシューティング

デバイスまたはネットワークで SELinux 違反のインスタンスがある場合は、次の詳細を Cisco TAC に連絡してください。

- コンソールまたはシステムログに出力されるとおりのメッセージ。次に例を示します。

```
device#request platform software trace archive target
flash:selinux_btrace_logs
```

- **show tech-support** コマンドの出力 (テキストファイル)
- ボックスからの Btrace ファイルのアーカイブ (次のコマンドを使用) :  
**request platform software trace archive target <URL>**
- **show platform software selinux** コマンドの出力





## 第 12 章

# Cisco Catalyst 8000V ネットワーク インターフェイスの VM ネットワーク インターフェイスへのマッピング

この章では、Cisco Catalyst 8000V 上の論理インターフェイスを vNIC および vNIC MAC アドレスにマッピングする方法について説明します。この章のセクションでは、ネットワーク インターフェイスを追加および削除する方法、および Cisco Catalyst 8000V でサポートされているインターフェイス速度についても説明します。

- [サポートされるネットワーク インターフェイスの速度 \(139 ページ\)](#)
- [ルータ ネットワーク インターフェイスの vNIC へのマッピング \(140 ページ\)](#)
- [Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除 \(141 ページ\)](#)
- [実行中の VM からの vNIC の削除 \(142 ページ\)](#)
- [Cisco Catalyst 8000V ネットワーク インターフェイスと VM の複製 \(142 ページ\)](#)
- [Cisco Catalyst 8000V ネットワーク インターフェイスと vSwitch インターフェイスのマッピング \(143 ページ\)](#)

## サポートされるネットワーク インターフェイスの速度

次の表に、Cisco Catalyst 8000V でサポートされるすべてのネットワーク インターフェイスの速度を示します。

Cisco IOS XE リリース	インターフェイス速度 (Mbps)
Cisco IOS XE 17.15.1a 以降	最大 40000
Cisco IOS XE 17.9.1 から Cisco IOS XE 17.14.x リリース	最大 25000
Cisco IOS XE 17.4.1 から Cisco IOS XE 17.8.x リリース	最大 10000 台

## ルータ ネットワーク インターフェイスの vNIC へのマッピング

Cisco Catalyst 8000V では、GigabitEthernet ネットワーク インターフェイスを、VM によって割り当てられた論理的な仮想ネットワーク インターフェイス カード (vNIC) 名にマッピングします。次に、VM は物理 MAC アドレスに対して論理 vNIC 名をマッピングします。

Cisco Catalyst 8000V インスタンスを初めて起動したときに、VM の作成時に追加された論理 vNIC インターフェイスに、ルータインターフェイスがマッピングされます。

Cisco Catalyst 8000V インスタンスを起動した後、**show platform software vnic-if interface-mapping** コマンドを使用して、vNIC を持つルータ上の論理インターフェイスと vNIC MAC アドレスの間のマッピングを表示する必要があります。このコマンドの出力は、Cisco IOS XE のリリースバージョンによって異なります。



(注) GigabitEthernet0 インターフェイスはサポートされなくなりました。

```
Router# show platform software vnic-if interface-mapping
```

Interface Name	Short Name	vNIC Name	Mac Addr
GigabitEthernet2	Gi2	eth2 (vmxnet3)	0050.5689.0034
GigabitEthernet1	Gi1	eth1 (vmxnet3)	0050.5689.000b

ディスプレイに表示される vNIC 名は、Cisco Catalyst 8000V インスタンスがハイパーバイザ上のインターフェイスにマッピングするために使用する論理インターフェイスです。VM のインストール中に追加された対応する NIC 名に常にマッピングされるわけではありません。たとえば、表示されている論理「eth1」vNIC 名は、VM インストールプロセスで追加された「NIC1」に必ずしもマッピングされない場合があります。



**注意** Cisco Catalyst 8000V でギガビットイーサネット ネットワーク インターフェイスの設定を開始する前に、インターフェイスのマッピングを確認することが重要です。これにより、ネットワーク インターフェイス構成が VM ホスト上の正しい物理 MAC アドレスインターフェイスに適用されます。

ルータを再起動し、vNIC を追加または削除しない場合、インターフェイスマッピングは以前と同じままになります。ルータを再起動して vNIC を削除する場合は、残りのインターフェイスの設定がそのまま残っていることを確認します。詳細については、「Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除」を参照してください。[Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除 \(141 ページ\)](#)

# Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除

Cisco Catalyst 8000V は、ルータの GigabitEthernet インターフェイスを、VM によって割り当てられた論理 vNIC 名にマッピングします。この論理 vNIC 名は、VM ホストの MAC アドレスにマッピングされます。Cisco Catalyst 8000V で GigabitEthernet インターフェイスを追加または削除するには、VM の vNIC を追加または削除します。ルータがアクティブな間に vNIC を追加できません。

VM から vNIC を削除するには、最初に VM の電源をオフにする必要があります。vNIC を削除した場合は、ルータを再起動する必要があります。vNIC を追加および削除する方法の詳細は、[VMware のマニュアル](#)を参照してください。



(注) インターフェイスのホット追加/削除は、コントローラモードで動作する Cisco Catalyst 8000V ではサポートされていません。インターフェイスのホット追加/削除を実行する必要がある場合は、CLI を使用して、コントローラモードでリセット操作を設定 (**request platform software sdwan config reset**) します。



注意 Cisco Catalyst 8000V ネットワーク インターフェイス設定を更新せずに vNIC を削除すると、ルータの再起動時に設定の不一致が発生するリスクがあります。ルータを再起動して vNIC を削除すると、残りの論理 vNIC 名が別の MAC アドレスに再割り当てされる可能性があります。その結果、Cisco Catalyst 8000V インスタンスの GigabitEthernet ネットワーク インターフェイスは、ハイパーバイザ上の異なる物理インターフェイスに再割り当てされる可能性があります。

ネットワーク インターフェイスを追加または削除する前に、まず **show platform software vnic-if interface-mapping** コマンドを使用して、インターフェイスと vNIC のマッピングを確認します。

```
Router# show platform software vnic-if interface-mapping
```

Interface Name	Driver Name	Mac Addr
GigabitEthernet3	vmxnet3	000c.2946.3f4d
GigabitEthernet2	vmxnet3	0050.5689.0034
GigabitEthernet1	vmxnet3	0050.5689.000b

VM のネットワーク インターフェイスを追加または削除した後、ネットワーク インターフェイスの設定を変更する前に、新しいインターフェイスと vNIC のマッピングを確認します。次の例は、新しい vNIC が追加された後のインターフェイスマッピングを示しています。新しい vNIC は、Cisco Catalyst 8000V インスタンスの GigabitEthernet4 ネットワーク インターフェイスにマッピングされます。

```
Router# show platform software vnic-if interface-mapping
```

Interface Name	Driver Name	Mac Addr
GigabitEthernet4	vmxnet3	0010.0d40.37ff
GigabitEthernet3	vmxnet3	000c.2946.3f4d
GigabitEthernet2	vmxnet3	0050.5689.0034
GigabitEthernet1	vmxnet3	0050.5689.000b

## 実行中の VM からの vNIC の削除

実行中の VM から vNIC を削除するには、`clear platform software` コマンドを使用します（後述）。ハイパーバイザ設定から vNIC を削除する前に、このコマンドを実行します。これは、「2段階ホットリムーブ」の一部です。

2段階ホットリムーブをサポートするハイパーバイザを確認するには、「vNIC Two-Step Hot Remove Support = Yes」のハイパーバイザを探します

**clear platform software vnic-if interface GigabitEthernetinterface-number**

*interface-number* : 0 ~ 32 の値。

例 :

```
Router# clear platform software vnic-if interface GigabitEthernet4
```

次に、ハイパーバイザ設定から vNIC を削除します。



(注) ハイパーバイザから vNIC 設定を削除する前に、`clear platform software vnic-int interface` コマンドを実行する必要がなくなりました。このコマンドは、将来のリリースでは廃止される予定です。

## Cisco Catalyst 8000V ネットワーク インターフェイスと VM の複製

Cisco Catalyst 8000V インスタンスを初めてインストールすると、vNIC 名を MAC アドレスにマッピングするデータベースが作成されます。このデータベースは、vNIC を追加または削除する場合に、ルータインターフェイス間の永続的なマッピングと vNIC から MAC アドレスへのマッピングを維持するために使用されます。インターフェイスは、VMware が保持する保存済みの汎用一意識別子 (UUID) にマッピングされます。

ルータ ネットワーク インターフェイスと vNIC 間のマッピングは、Cisco Catalyst 8000V がインストールされている現在の VM にのみ適用されます。VM が複製された場合、保存されている UUID は現在の UUID と一致せず、インターフェイスマッピングはルータ設定と一致しません。

インターフェイスマッピングの不一致を防ぐには、複製前に元の VM で次の手順を実行します。



- (注) 複製プロセスを開始する前に、複製された VM で必要な数の設定済み vNIC が元の VM に含まれていることを確認します。

## 手順

**ステップ 1** 元の VM で **clear platform software vnic-if nhtable** コマンドを入力します。

このコマンドは、元の VM の永続的なインターフェイス データベースをクリアし、ハイパーバイザへのインターフェイスマッピングを更新します。

**ステップ 2** Cisco Catalyst 8000V をリブートします。

**ステップ 3** 複製された VM で、**show platform software vnic-if interface-mapping** コマンドを使用してインターフェイスのマッピングを確認します。

**ステップ 4** 複製された VM のルータインターフェイスを適宜設定します。

複製された VM のルータ設定は、元の VM の設定と一致する必要があります。

# Cisco Catalyst 8000V ネットワーク インターフェイスと vSwitch インターフェイスのマッピング

Cisco Catalyst 8000V インターフェイスに対応するために、さまざまな方法で ESXi のネットワーク インターフェイスを設定できます。各 Cisco Catalyst 8000V ルータインターフェイスが 1 つのホストイーサネット インターフェイスにマッピングされるように、ネットワーク インターフェイスを設定できます。

または、複数の Cisco Catalyst 8000V インターフェイスが 1 つのホスト ESXi イーサネット インターフェイスを共有するようにネットワーク インターフェイスを設定することもできます。

3 番目の方法は、Cisco Catalyst 8000V インターフェイスを vSwitch のトランクインターフェイスに直接マッピングすることです。





## 第 13 章

# VNF セキュアブートの有効化

セキュアブートは、Unified Extensible Firmware Interface (UEFI) 標準の一部であり、OEM (Original Equipment Manufacturer) によって信頼されているソフトウェアのみを使用してデバイスを起動します。UEFI (Unified Extensible Firmware Interface) 仕様は、受け入れ可能なデジタル署名を持たないソフトウェアのロードを防ぐセキュアブート方法を定義しています。デバイスが起動すると、ファームウェアはブートソフトウェアとオペレーティングシステムの署名をチェックします。署名が有効な場合、デバイスが起動し、ファームウェアがオペレーティングシステムに制御を渡します。

セキュアブート機能は、システムの起動プロセス中に悪意のあるソフトウェアアプリケーションと不正なオペレーティングシステムがシステムにロードされないようにします。セキュアブート機能を有効にすると、許可されたソフトウェアアプリケーションのみがデバイスから起動します。この機能により、デバイス上で起動するソフトウェアアプリケーションがシスコによって認定されていることを確認できます。セキュアなコンピューティングシステムによって、システム上の意図したソフトウェアがマルウェアや改ざんされたソフトウェアを使用せずに実行されるようにします。

システムブートモードとブートローダーのバージョンを表示するには、**show platform software system boot** コマンドを実行します。

```
Router#show platform software system boot
Boot mode: EFI
Bootloader version: 2.0
```

### 機能制限

- 次のセキュアブート環境がサポートされています。
  - ESXi バージョン 6.5 以上
  - オープンスタックライセンスを使用した KVM RHEL 7.5
  - NFVIS リリース 3.11 以降
- EFI ファームウェアモードのみがセキュアブートをサポートします
- GRUB2 および新しいディスクパーティションレイアウトが使用可能です



- (注) 各ハイパーバイザには、ゲスト VM のセキュアブートを可能にする固有のプロセスがあります。セキュアブートを有効にするには、ハイパーバイザ固有のマニュアルを参照してください。
- セキュアブートを有効にするためのハイパーバイザ固有の一連の手順を以下におおまかに示します。

### ESXi セキュアブートの設定

- VM バージョン 13 以上を使用する ESXi 6.5 以降のバージョンを使用して VM を作成します。EFI ファームウェアモードを選択するには、[VM Options]>[Boot Options]>[Firmware]>[EFI] の順に移動します。
- 初回起動後、IOS プロンプトが完了したら、VM の電源をオフにします。
- [Edit Settings]>[VM Options]>[Boot Options]>[Secure Boot] で EFI セキュアブートを有効にします。
- VM の電源をオンにすると、VNF が安全に起動します。



- 重要** VM の作成後にファームウェアモードを（BIOS から EFI、またはその逆に）変更することはできません。

### KVM セキュアブートの設定

- VM を作成します。
  - VM が作成され、VNF IOS プロンプトが完了したら、VM の電源をオフにします。
  - [EFI Firmware] メニューから PK、KEK、および db 証明書をインストールし、リセットします。
- カスタムキーを作成するには、[セキュアブートのカスタムキーに関する説明](#)を参照してください。db 証明書については、[MicCorUEFCA2011\\_2011-06-27.crt](#) および [MicWinProPCA2011\\_2011-10-19.crt](#) を参照してください。
- VM をセキュアブートします。

### NFVIS セキュアブートの設定

- NFVIS 3.11 リリース以降にアップグレードします。
- Cisco Catalyst 8000V EFI tarball を NFVIS リポジトリに登録します。
- 登録された EFI イメージを使用して VM を作成します。

- VM をセキュアブートします。





## 第 14 章

# コンソールアクセスの設定

- [Cisco Catalyst 8000V を VM として起動 \(149 ページ\)](#)
- [Cisco Catalyst 8000V コンソールへのアクセス \(151 ページ\)](#)

## Cisco Catalyst 8000V を VM として起動

VM の電源がオンになると Cisco Catalyst 8000V が起動します。設定に応じて、仮想 VGA コンソールまたは仮想シリアルポート上のコンソールでインストールプロセスをモニターできます。



- (注) 仮想 VGA コンソールの代わりにハイパーバイザのシリアルポートから Cisco Catalyst 8000V にアクセスして設定する場合は、VM の電源をオンにしてルータを起動する前に、この設定を使用するよう VM をプロビジョニングする必要があります。

### 手順

**ステップ 1** VM の電源を入れます。VM の電源投入後 5 秒以内に、次の 2 つのステップ（ステップ 2 または 3）のいずれかで説明したコンソールを選択し、ルータのブートアップを表示して Cisco Catalyst 8000V CLI にアクセスします。

**ステップ 2** (オプション) **Virtual Console** を選択します

仮想コンソールの使用を選択した場合、この手順の残りのステップは適用されません。Cisco Catalyst 8000V は、5 秒以内に他のオプションを選択しない場合、仮想コンソールを使用して起動します。Cisco Catalyst 8000V インスタンスがブートプロセスを開始します。

**ステップ 3** (オプション) **Serial Console** を選択します

VM で仮想シリアルポートコンソールを使用するには、このオプションを選択します。

このオプションを機能させるには、仮想シリアルポートが VM にすでに存在している必要があります。

(注)

ブートプロセス中にコンソールポートを選択するオプションは、Cisco Catalyst 8000V の初回起動時にのみ使用できます。Cisco Catalyst 8000V の初回起動後にコンソールポートアクセスを変更するには、[インストール後のコンソールポートアクセスの変更 \(154 ページ\)](#) を参照してください。

Cisco Catalyst 8000V がブートプロセスを開始します。

**ステップ 4** `telnet://host-ipaddress:portnumber` または `telnet host-ipaddress portnumber` (UNIX xTerm 端末から) 2つのコマンドのいずれかを使用して、VM に Telnet 接続します。次の例は、VM での Cisco Catalyst 8000V 初期ブート出力を示しています。

システムは最初に SHA-1 を計算します。これには数分かかる場合があります。SHA-1 が計算されると、カーネルが起動します。初期インストールプロセスが完了すると、.iso パッケージファイルが仮想 CD-ROM から削除され、VM がリブートされます。これにより、Cisco Catalyst 8000V が仮想ハードドライブから正常に起動できるようになります。

(注)

システムは、初回インストール時にのみ再起動します。

Cisco Catalyst 8000V の起動に必要な時間は、使用するリリースとハイパーバイザによって異なる場合があります。

**ステップ 5** 起動後、メインのソフトウェアイメージおよびゴールデンイメージと、強調表示されたエントリを 3 秒以内に自動的に起動する手順を示す画面が表示されます。ゴールデンイメージのオプションを選択せず、メインのソフトウェアイメージを起動させます。

(注)

Cisco Catalyst 8000V には、シスコの多くのハードウェアベースのルータに含まれている ROMMON イメージは含まれていません。インストール中、インストールされたバージョンのバックアップコピーがバックアップパーティションに保存されます。このコピーは、ブートイメージをアップグレードした場合、元のブートイメージを削除した場合、または何らかの理由でディスクが破損した場合に、起動元として選択できます。バックアップコピーからの起動は、ROMMON から別のイメージを起動することと同じです。GRUB モードにアクセスするための構成レジスタの設定変更の詳細については、[GRUB モードへのアクセス \(192 ページ\)](#) を参照してください。

これで、標準コマンド `enable`、`configure terminal` の順に入力して、ルータ設定環境を開始できます。

Cisco Catalyst 8000V インスタンスを初めて起動するとき、ルータが起動するモードはリリースバージョンによって異なります。

サポートされているスループットと機能を取得するには、ソフトウェアライセンスをインストールするか、評価ライセンスを有効にする必要があります。リリースバージョンに応じて、ブートレベルを有効にするか、最大スループットレベルを変更して、Cisco Catalyst 8000V を再起動する必要があります。

インストールされているライセンス テクノロジー パッケージは、`license boot level` コマンドで設定されたパッケージレベルと一致する必要があります。ライセンスパッケージが設定と一致しない場合、スループットは 100 Kbps に制限されます。

(VMware ESXi のみ) .iso ファイルを使用して VM を手動で作成した場合は、基本的なルータプロパティを設定する必要があります。Cisco IOS XE CLI コマンドを使用するか、vSphere GUI でプロパティを手動で設定できます。

# Cisco Catalyst 8000V コンソールへのアクセス

## 仮想 VGA コンソールからの Cisco Catalyst 8000V へのアクセス

Cisco Catalyst 8000V ソフトウェアイメージをインストールする場合、使用する設定は仮想 VGA コンソールです。次の場合、仮想 VGA コンソールから Cisco Catalyst 8000V CLI にアクセスするために他の設定を変更する必要はありません。

- 起動プロセス中にコンソール設定を変更しないでください
- VM 設定に 2 つの仮想シリアルポートを追加しないでください。これは、自動コンソール検出を使用している場合に適用されます。

## 仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセス

### 仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセスの概要

デフォルトでは、仮想 VGA コンソールを使用して Cisco Catalyst 8000V インスタンスにアクセスできます。自動コンソール検出を使用して、2 つの仮想シリアルポートが検出された場合、Cisco Catalyst 8000V CLI は最初の仮想シリアルポートで使用できます。

シリアルコンソールを使用するように VM を設定することもできます。シリアルコンソールは常に Cisco Catalyst 8000V CLI の最初の仮想シリアルポートの使用を試みます。ハイパーバイザ上に仮想シリアルポートを設定するには、次の項を参照してください。



(注) Citrix XenServer は、シリアルコンソールを介したアクセスをサポートしていません。

## VMware ESXi でのシリアルコンソールアクセスの作成

VMware vSphere を使用して次の手順を実行します。詳細については、VMware vSphere のマニュアルを参照してください。

### 手順

**ステップ 1** VM の電源をオフにします。

**ステップ 2** VM を選択し、仮想シリアルポートを設定します。

- [Edit Settings] > [Add] の順に選択します。
- [Device Type] > [Serial port] の順に選択します。[Next] をクリックします。
- [Select Port Type] を選択します。

[Connect via Network] を選択し、[Next] をクリックします。

ステップ 3 [Select Network Backing] > [Server (VM listens for connection)] を選択します。

次の構文を使用して [Port URI] を入力します。

```
telnet://:portnumber
```

ここで、*portnumber* は仮想シリアルポートのポート番号です。

[I/O mode] で、[Yield CPU on poll] オプションを選択し、[Next] をクリックします。

ステップ 4 VM の電源を投入します。

ステップ 5 VM の電源がオンになったら、仮想シリアルポート コンソールにアクセスします。

ステップ 6 仮想シリアルポートのセキュリティ設定を行います。

- a) 仮想シリアルポートの [ESXi host] を選択します。
- b) [Configuration] タブをクリックし、[Security Profile] をクリックします。
- c) [Firewall] セクションで、[Properties] をクリックし、次に [VM serial port connected over Network] の値を選択します。

これで、Telnet ポート URI を使用して Cisco IOS XE コンソールにアクセスできるようになります。仮想シリアルポートを設定すると、VM の仮想コンソールから Cisco Catalyst 8000V にアクセスすることはできなくなります。

(注)

これらの設定を使用するには、Cisco Catalyst 8000V のブートアップ中に GRUB メニューの **Auto Console** オプションまたは **Serial Console** オプションを選択する必要があります。仮想 VGA コンソールを使用して Cisco Catalyst 8000V ソフトウェアをすでにインストールしている場合は、Cisco IOS XE **platform console auto** コマンドまたは Cisco IOS XE **platform console serial command** のいずれかを設定し、仮想シリアルポートを介したコンソールアクセスが機能するように VM をリロードする必要があります。

## KVM でのシリアルコンソールアクセスの作成

サーバーの KVM コンソールを使用して、次の手順を実行します。詳細については、KVM のマニュアルを参照してください。

### 手順

ステップ 1 VM の電源をオフにします。

ステップ 2 デフォルトの [Serial 1] デバイス（存在する場合）をクリックし、[Remove] をクリックします。これにより、最初の仮想シリアルポートとしてカウントされるデフォルトの `pty` ベースの仮想シリアルポートが削除されます。

ステップ 3 [Add Hardware] をクリックします。

ステップ 4 [Serial] を選択して、シリアルデバイスを追加します。

ステップ 5 [Character Device] で、ドロップダウンメニューから [TCP Net Console (tcp)] デバイスタイプを選択します。

- ステップ 6 [Device Parameters] で、ドロップダウンメニューからモードを選択します。
- ステップ 7 [Host] で、**0.0.0.0** と入力します。サーバーは、任意のインターフェイスで Telnet 接続を受け入れます。
- ステップ 8 ドロップダウンメニューからポートを選択します。
- ステップ 9 [Use Telnet] オプションを選択します。
- ステップ 10 [Finish] をクリックします。

これで、Telnet ポート URI を使用して Cisco IOS XE コンソールにアクセスできるようになります。詳細については、[仮想シリアルポートでの Cisco Catalyst 8000V コンソールへの Telnet セッションの開始 \(153 ページ\)](#) を参照してください。

(注)

これらの設定を使用するには、Cisco Catalyst 8000V の起動中に GRUB メニューの **Auto Console** オプションまたは **Serial Console** オプションを選択する必要があります。仮想 VGA コンソールを使用して Cisco Catalyst 8000V ソフトウェアをすでにインストールしている場合は、仮想シリアルポートを介したコンソールアクセスを機能させるために、Cisco IOS XE **platform console auto** コマンドまたは **platform console serial** コマンドを設定し、VM をリロードする必要があります。

## 仮想シリアルポートでの Cisco Catalyst 8000V コンソールへの Telnet セッションの開始

Cisco IOS XE CLI コマンドを使用して、次の手順を実行します。

### 手順

ステップ 1 VM に Telnet 接続します。

- 次のコマンドを使用します。 **telnet://host-ipaddress:portnumber**
- または、UNIX 端末から次のコマンドを使用します。

**telnet host-ipaddress portnumber**

ステップ 2 Cisco Catalyst 8000V IOS XE パスワードプロンプトで、ログイン情報を入力します。次に、*mypass* というパスワードを入力する例を示します。

例：

```
User Access Verification
Password: mypass
```

(注)

パスワードが設定されていない場合は、**Return** を押します。

ステップ 3 ユーザー EXEC モードで、次のように **enable** コマンドを入力します。

例：

```
Router> enable
```

**ステップ 4** パスワードプロンプトに、システムパスワードを入力します。次に、*enablepass* というパスワードを入力する例を示します。

例：

```
Password: enablepass
```

**ステップ 5** イネーブルパスワードが許可されると、特権 EXEC モードプロンプトが次のように表示されます。

例：

```
Router#
```

**ステップ 6** これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

**ステップ 7** Telnet セッションを終了するには、次の例のように **exit** または **logout** コマンドを使用します。

例：

```
Router# logout
```

## インストール後のコンソールポートアクセスの変更

Cisco Catalyst 8000V インスタンスが正常に起動したら、Cisco IOS XE コマンドを使用して、ルータへのコンソールポートアクセスを変更できます。コンソールポートアクセスを変更した後は、ルータをリロードするか、電源を再投入する必要があります。

### 手順

#### ステップ 1 enable

例：

```
Router> enable
```

特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

#### ステップ 2 configure terminal

例：

```
Router# 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** 次のいずれかを実行します。

- **platform console virtual**
- **platform console serial**

例：

```
Router(config)# platform console virtual
```

例：

```
Router(config)# platform console serial
```

**platform console x** のオプション：

- **virtual**：ハイパーバイザの仮想 VGA コンソールを介して Cisco Catalyst 8000V にアクセスすることを指定します。
- **serial**：VM のシリアルポートを介して Cisco Catalyst 8000V にアクセスすることを指定します。

**Note**：このオプションは、ハイパーバイザがシリアルポート コンソール アクセスをサポートしている場合にのみ使用してください。

#### ステップ 4 end

例：

```
Router(config)# end
```

コンフィギュレーション モードを終了します。

#### ステップ 5 copy system:running-config nvram:startup-config

例：

```
Router# copy system:running-config nvram:startup-config
```

実行設定を、NVRAM スタートアップ設定にコピーします。

#### ステップ 6 reload

例：

```
Router# reload
```

オペレーティング システムをリロードします。

---

#### 次のタスク

コンソールアクセスを設定したら、Cisco Catalyst 8000V ライセンスをインストールします。ライセンスをインストールして使用する方法については、このガイドの「ライセンス」の章を参照してください。





## 第 15 章

# Cisco Catalyst 8000V ハードウェアと VM の要件の確認

Cisco Catalyst 8000V の問題をトラブルシューティングしやすくするために、サポートされているハードウェアにルータがインストールされ、次の VM の要件が満たされていることを確認します。

- サーバハードウェアがハイパーバイザベンダーでサポートされていることを確認します。  
VMware を使用している場合、サーバーが VMware ハードウェア互換性リストに含まれていることを確認します。詳細については、VMware のマニュアルを参照してください。
- 使用されている I/O デバイス (FC、iSCSI、SAS など) が VM ベンダーによってサポートされていることを確認します。
- 十分な RAM が VM とハイパーバイザ ホスト用のサーバに割り当てられていることを確認します。  
VMware を使用している場合、サーバーに VM と VMware ESXi の両方をサポートするのに十分な RAM があることを確認します。
- Cisco Catalyst 8000V でハイパーバイザのバージョンがサポートされていることを確認します。
- メモリの量、CPU の数、およびディスクサイズについて適切に VM が設定されていることを確認します。
- サポートされているネットワーク ドライバを使用して vNIC が設定されていることを確認します。
- Cisco IOS XE 17.6.1 以降、ホストと VM が RDRAND または RDSEED、あるいはその両方の命令をサポートしている場合は、FIPS モードを有効にできます。それ以外の場合は、エラーメッセージが表示されます。



- 
- (注) 一部のハイパーバイザには、VM での RDSEED または RDRAND、あるいはその両方の使用をブロックする設定オプションまたはランタイムオプションがあります。これらのオプションは有効にしないでください。つまり、FIPS モードを有効にする場合は、RDSEED または RDRAND、あるいはその両方がハイパーバイザによってブロックされないようにする必要があります。
-



## 第 16 章

# Cisco IOS XE ソフトウェアのアップグレード

Cisco Catalyst 8000V 仮想ルータは、Cisco CSR1000V または Cisco ISRv と同じプラットフォームである Cisco IOS XE プラットフォームで動作します。Cisco Catalyst 8000V ルータを使用するには、まず [Cisco Software Download](#) ページからソフトウェアイメージを取得します。インストールファイルを取得し、インストールまたはアップグレードを開始します。インストールファイルの詳細については、[インストールファイル \(9 ページ\)](#) を参照してください。

既存の Cisco CSR1000V または Cisco ISRv を使用している場合は、[Cisco Software Download] ページから最新のインストールファイルをダウンロードし、この章で説明する手順に従ってアップグレードプロセスを開始する必要があります。

### Cisco Catalyst 8000V のソフトウェアパッケージ

Cisco Catalyst 8000V のソフトウェアイメージは、統合パッケージおよびオプションのサブパッケージとして使用できます。各統合パッケージには、ソフトウェアサブパッケージのコレクションが含まれています。各ソフトウェアサブパッケージは、仮想ルータのさまざまな要素を制御する個別のソフトウェアファイルです。統合パッケージを使用すると、個々のサブパッケージすべてを1度のソフトウェアイメージのダウンロードでアップグレードすることができます。

個々のソフトウェアサブパッケージは別々にアップグレードすることができます。あるいは、特定の統合パッケージのソフトウェアサブパッケージすべてを、統合パッケージ全体のアップグレードの一環としてアップグレードすることも可能です。統合パッケージに含まれる個々のサブパッケージを使用してルータを実行する場合は、Cisco.com からイメージをダウンロードし、そのイメージから個々のサブパッケージを抽出します。

サブパッケージを使用したアップグレードは、統合パッケージを使用したアップグレードよりもメモリ消費が少なくなります。このため、特にフットプリントが小さい展開状況では、サブパッケージを使用したアップグレード方法を推奨します。



- (注) Cisco ISRV または Cisco CSR1000V を Cisco Catalyst 8000V にアップグレードしても、ファイルシステムのレイアウトは変更されず、ファイルシステムに依存するセキュアオブジェクトストアなどの新機能も一切提供されません。これらの機能を利用するには、新規インストールを実行する必要があります。



**重要** 既存の Cisco CSR1000V または Cisco ISRV を使用するユーザーが Cisco Catalyst 8000V にアップグレードする場合、ライセンスは現状のまま機能します。ただし、250 Mbps を超えるスループットレベルを実行するには、HSECK9 ライセンスが必須です。アップグレード前に 250 Mbps を超えるスループットレベルを実行していた場合は、アップグレード後にサービスを継続するために HSECK9 ライセンスを購入する必要があります。アップグレード後に HSECK9 ライセンスが使用できない場合、スループットは 250 Mbps に制限されます。Cisco DNA サブスクリプションベースのライセンスモデルに切り替える場合は、新しい Catalyst 8000V 展開を実行する必要があります。

- [Cisco Catalyst 8000V のアップグレードのための前提条件 \(160 ページ\)](#)
- [Cisco CSR1000V および Cisco ISRV アップグレードの HSECK9 ライセンス要件 \(161 ページ\)](#)
- [Cisco Catalyst 8000V のアップグレードの制約事項 \(161 ページ\)](#)
- [インストールモードのプロセスフロー \(163 ページ\)](#)
- [Cisco Catalyst 8000V をインストールモードで起動する場合 \(168 ページ\)](#)
- [インストールモードでのアップグレード \(174 ページ\)](#)
- [インストールモードでのダウングレード \(174 ページ\)](#)
- [ソフトウェアインストールの中止 \(175 ページ\)](#)
- [インストールコマンドを使用したソフトウェアインストールのトラブルシューティング \(176 ページ\)](#)
- [よく寄せられる質問 \(177 ページ\)](#)

## Cisco Catalyst 8000V のアップグレードのための前提条件

- シスコのソフトウェアダウンロードページから Cisco Catalyst 8000V ソフトウェアイメージを取得します。インストールファイルの入手方法については、「[インストールファイルのダウンロード](#)」を参照してください。
- アップグレードを実行する前に、ハイパーバイザのバージョンを確認します。Cisco Catalyst 8000V で現在使用中の Cisco IOS XE バージョンでハイパーバイザのバージョンがサポートされていない場合、アップグレードは成功しません。
- Cisco Catalyst 8000V ソフトウェアイメージに関する VM のメモリ要件が満たされていることを確認します。アップグレード後のバージョンに以前のバージョンよりも大きなメモリ

が必要になる場合は、アップグレードプロセスを開始する前に、VM に対するメモリの割り当てを引き上げます。

## Cisco CSR1000V および Cisco ISRV アップグレードの HSECK9 ライセンス要件

スループットが 250 Mbps を超える Cisco CSR1000V または Cisco ISRV ルータを Cisco Catalyst 8000V (Cisco IOS XE Bengaluru 17.4.1 以降) にアップグレードする場合は、高セキュリティ (HSECK9) ライセンスが必要です。

アップグレード前の構成に応じて、アップグレードする前に、対応する HSECK9 ライセンス要件を満たしていることを確認します。

- Cisco CSR1000V または Cisco ISRV が CSSM に接続されている場合は、次のことを確認する必要があります。

- 250 Mbps を超えるスループットは、スタートアップ構成の一部です。

スタートアップ構成を確認するには、特権 EXEC モードで **show running-config** コマンドを入力します。次に例を示します。

```
Device# show running-config | include throughput
platform hardware throughput level MB 500
```

- CSSM 内の対応するスマートアカウントとバーチャルアカウントで、必要な数の HSECK9 ライセンス (DNA\_HSECK9) の残高がプラスになっています。

アップグレード前のアクションは必要ありません。デバイスが CSSM に接続されている限り、アップグレード時にデバイスは HSECK9 要求を自動的にトリガーし、必要なスマートライセンス認証コード (SLAC) をインストールします。

- Cisco CSR1000V または Cisco ISRV が特定のライセンス予約 (SLR) を使用している場合は、SLR 承認コードを更新して HSECK9 ライセンス (DNA\_HSECK9) を含めてから、デバイスをアップグレードする必要があります。これにより、アップグレード後もスループットが中断されなくなります。

この例では、SLR 承認コードを更新する方法を示します。 [Example: Smart Licensing \(SLR With Throughput >250 Mbps, Without Export-Controlled License\) to Smart Licensing Using Policy.](#)

スループットが 250 Mbps 以下の場合、HSECK9 ライセンスのインストールは必要ありません。

## Cisco Catalyst 8000V のアップグレードの制約事項

- 新しいソフトウェアバージョンへのアップグレードは、同じ VM 上でのみ実行できます。この手順では、別の VM で同じまたはアップグレードされたソフトウェアバージョンを実

行している既存のルータをインストールまたは再ホストする方法については説明していません。

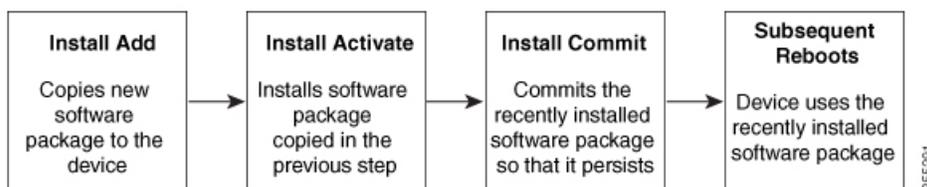
- .bin ファイルは、ソフトウェアのアップグレードまたはダウングレードに適用されます。 .iso ファイル、 qcow2 ファイル、 および .ova ファイルは、初回インストールのみに使用します。
- Cisco Catalyst 8000V にアップグレードする場合、ライセンスは現状のまま機能します。ただし、CDNA ライセンスモデルに切り替える場合は、新規インストールを実行する必要があります。
- Cisco Catalyst 8000V ルータは、In-Service Software Upgrade (ISSU) をサポートしていません。
- x86 ハードウェアのシステム要件は、ルータで現在実行されているハードウェアの要件と異なる場合があります。
- Cisco CSR1000V または Cisco ISRv からのアップグレードの場合、ディスクパーティション構造は以前のバージョンと同じままであり、セキュア オブジェクト ストレージ機能は使用できません。
- 16.12.x より前の Cisco CSR1000V または Cisco ISRv から Cisco Catalyst 8000V にアップグレードする場合は、まず現在のバージョンから 16.12.x にアップグレードします。その後、Cisco Catalyst 8000V の最新バージョンにアップグレードしてください。
- Cisco Catalyst 8000V は PCI パススルーをサポートしていないため、PCI パススルーを実行している Cisco CSR1000V を Cisco Catalyst 8000V にアップグレードすることはできません。
- Cisco Catalyst 8000V を新しくインストールした場合、Cisco ISRv または Cisco CSR1000V にダウングレードすることはできません。以前に保有していた Cisco CSR1000V を Cisco Catalyst 8000V にアップグレードした場合、Cisco CSR1000V にダウングレードできますが、Cisco ISRv にダウングレードすることはできません。
- Cisco CSR1000V から Cisco Catalyst 8000V にアップグレードする場合、または Cisco Catalyst 8000V の下位バージョンから上位バージョンにアップグレードする場合は、N-2 または N-1 から N へのリリースアップグレードパスのみがサポートされます。ここで、N-1 および N-2 は拡張メンテナンスリリースを指します。たとえば、CSR1000V 17.3.x インスタンスを Cisco Catalyst 8000V 17.11.1a リリースにアップグレードする場合、17.6.x は更新する必要がある最も低い N-x バージョンです。
- Cisco Catalyst 8000V は、L2TP クライアントや L2TP ネットワークサーバー (LNS) を含む L2TP 機能をサポートしていません。

## インストールモードのプロセスフロー

インストールモードのプロセスフローは、Cisco Catalyst 8000V のインストールとアップグレードを実行するための 3 つのコマンド (**install add**、**install activate**、**install commit**) で構成されています。

次のフローチャートは、インストールコマンドを使用したインストールプロセスを説明しています。

Process with Install Commit



**install add** コマンドは、ソフトウェアパッケージをローカルまたはリモートの場所からプラットフォームにコピーします。FTP、HTTP、HTTPS、または TFTP を使用できます。このコマンドは、.package ファイルの個々のコンポーネントをサブパッケージと packages.conf ファイルに展開します。またファイルを検証して、イメージファイルが Cisco Catalyst 8000V に固有であることを確認します。

**install activate** コマンドは、必要な検証を実行し、**install add** コマンドを使用して以前に追加されたパッケージをプロビジョニングします。また、システムのリロードをトリガーします。

**install commit** コマンドは、**install activate** コマンドを使用して以前にアクティブ化されたパッケージを確認し、リロード後も更新が持続されるようにします。



- (注) 更新をインストールすると、以前にインストールしたソフトウェアイメージが置換されます。インスタンスには、常に 1 つのイメージのみをインストールできます。

次の表に、Cisco IOS XE プラットフォームをインストールまたはアップグレードするときに使用するコマンドのリストを示します。

表 14: インストールコマンド一覧

コマンド	構文	目的
<b>install add</b>	<b>install add file</b> <i>location:filename.bin</i>	<p>イメージおよびパッケージの内容をソフトウェアリポジトリにコピーします。ファイルの場所はローカルでもリモートでもかまいません。このコマンドは次のことを行います。</p> <ul style="list-style-type: none"> <li>• ファイルのチェックサム、プラットフォームの互換性チェックなどを検証します。</li> <li>• パッケージの個々のコンポーネントをサブパッケージと <code>packages.conf</code> に展開します。</li> <li>• イメージをローカルインベントリにコピーし、次の手順で使用できるようにします。</li> </ul>
<b>install activate</b>	<b>install activate</b>	<p><b>install add</b> コマンドを使用して追加されたパッケージをアクティブ化します。</p> <ul style="list-style-type: none"> <li>• <b>show install summary</b> コマンドを使用して、非アクティブなイメージを確認します。</li> <li>• このコマンドを実行すると、システムがリロードされます。アクティベーションを続行するかどうかを確認します。確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> </ul>

コマンド	構文	目的
(install activate) auto abort-timer	install activate auto-abort timer <30-1200>	<p><b>auto-abort timer</b> は自動的に開始され、デフォルト値は 120 分です。指定された時間内に <b>install commit</b> コマンドが実行されない場合、アクティベーションプロセスは中止され、システムは最後にコミットされた状態に戻ります。</p> <ul style="list-style-type: none"> <li>• <b>install activate</b> コマンドを実行しながらタイマーの値を変更できます。</li> <li>• <b>install commit</b> コマンドはタイマーを停止し、インストールプロセスを続行します。</li> <li>• <b>install activate auto-abort timer stop</b> コマンドは、パッケージをコミットせずにタイマーを停止します。</li> <li>• 確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> <li>• このコマンドは、3 ステップインストールのバリエーションでのみ有効です。</li> </ul>
install commit	install commit	<p><b>install activate</b> コマンドを使用してアクティブ化されたパッケージをコミットし、リロード後も持続するようにします。</p> <ul style="list-style-type: none"> <li>• <b>show install summary</b> コマンドを使用して、コミットされていないイメージを確認します。</li> </ul>

コマンド	構文	目的
<b>install abort</b>	<b>install abort</b>	<p>インストールを中止し、システムを最後にコミットされた状態に戻します。</p> <ul style="list-style-type: none"> <li>このコマンドは、パッケージがアクティブ化された状態（コミットされていない状態）の場合にのみ適用されます。</li> <li><b>install commit</b> コマンドを使用してイメージをすでにコミットしている場合は、<b>install rollback to</b> コマンドを使用して望みのバージョンに戻ります。</li> </ul>
<b>install remove</b>	<b>install remove {file &lt;filename&gt;   inactive}</b>	<p>プラットフォームリポジトリから非アクティブなパッケージを削除します。このコマンドを使用して、スペースを解放します。</p> <ul style="list-style-type: none"> <li><b>file</b> : 指定されたファイルを削除します。</li> <li><b>inactive</b> : 非アクティブなファイルをすべて削除します。</li> </ul>

コマンド	構文	目的
<b>install rollback to</b>	<b>install rollback to {base   label   committed   id}</b>	<p>保存されているインストールポイントか、最後にコミットされたインストールポイントに、ソフトウェアセットをロールバックします。このコマンドには次のような特長があります。</p> <ul style="list-style-type: none"> <li>• リロードが必要です。</li> <li>• パッケージがコミットされた状態の場合にのみ適用されます。</li> <li>• 確認プロンプトを自動的に無視するには、このコマンドと <b>prompt-level none</b> キーワードを使用します。</li> </ul> <p>(注) 以前のイメージへのインストールのロールバックを実行する場合は、以前のイメージはインストールモードでインストールされている必要があります。</p>

上記のコマンドとは別に、次の show コマンドを使用してインストールまたはアップグレードを確認することもできます。

表 15: show コマンドの一覧

コマンド	構文	目的
<b>show install log</b>	<b>show install log</b>	プラットフォームがブートされた後に実行されたすべてのインストール操作の履歴と詳細を提供します。
<b>show install package</b>	<b>show install package &lt;filename&gt;</b>	指定された .pkg/.bin ファイルに関する詳細を提供します。
<b>show install summary</b>	<b>show install summary</b>	イメージバージョンとそれに対応するインストール状態の概要を提供します。

コマンド	構文	目的
<b>show install active</b>	<b>show install active</b>	アクティブなパッケージに関する情報を提供します。
<b>show install inactive</b>	<b>show install inactive</b>	非アクティブなパッケージがある場合は、そのパッケージに関する情報を提供します。
<b>show install committed</b>	<b>show install committed</b>	コミットされたパッケージに関する情報を提供します。
<b>show install uncommitted</b>	<b>show install uncommitted</b>	コミットされていないパッケージがある場合は、そのパッケージに関する情報を提供します。
<b>show install rollback</b>	<b>show install rollback {point-id   label}</b>	保存されているインストールポイントに関連付けられたパッケージを表示します。
<b>show version</b>	<b>show version [rp-slot] [installed   user-interface]   provisioned   running]</b>	プラットフォームの情報とともに、現在のパッケージに関する情報を表示します。

## Cisco Catalyst 8000V をインストールモードで起動する場合

単一のコマンド（1 ステップインストール手順）または複数の個別のコマンド（3 ステップインストール手順）を使用してソフトウェアパッケージをインストールして、アクティブ化し、コミットできます。

Cisco Catalyst 8000V デバイスがバンドルモードで動作している場合、1 ステップインストールの手順を使用して、最初にバンドルモードからインストールモードに変換する必要があります。その後、1 ステップまたは3 ステップのインストール方法を使用して、後続のインストールとアップグレードを実行できます。

### 1 ステップインストールまたはバンドルモードからインストールモードへの変換

この手順では、特権 EXEC モードで **install add file activate commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

1 ステップインストールの手順は、バンドルブートモードで実行されているプラットフォームをインストールモードに変換します。コマンドの実行後、プラットフォームはインストールブートモードでリブートします。



- (注)
- すべての CLI アクション（追加、アクティブ化など）が実行されます。
  - 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
  - このワークフローの 2 番目のステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。
  - プロンプトレベルが [None] に設定されていて、保存されていない設定がある場合、インストールは失敗します。コマンドを再発行する前に、設定を保存する必要があります。

## 手順の概要

1. **enable**
2. **install add file location: filename [activate commit]**
3. **exit**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>install add file location: filename [activate commit]</b> 例： Device# install add file bootflash:c8000v-universalk9.BLD_POLARIS_DEV_LATEST_20220227_153436.SSA.bin activate commit	ソフトウェア インストール パッケージをローカルまたはリモートの場所（FTP、HTTP、HTTPS、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。プラットフォームおよびイメージバージョンの検証および互換性チェックを実行し、パッケージをアクティブ化し、そのパッケージをコミットして複数回リロードしても維持されるようにします。  このコマンドを実行すると、プラットフォームがリロードされます。
ステップ 3	<b>exit</b> 例：	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device# exit	

## 3 ステップインストール

3 ステップインストールの手順では、個別の **install add**、**install activate**、および **install commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。



- (注)
- この手順は、プラットフォームがインストールモードになった後のみ実行できます。
  - すべての CLI アクション（追加、アクティブ化など）が実行されます。
  - 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
  - このワークフローの **install activate** ステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。

### 手順の概要

1. **enable**
2. **install add file location: filename**
3. **show install summary**
4. **install activate [auto-abort-timer <time>]**
5. **install abort**
6. **install commit**
7. **install rollback to committed**
8. **install remove {file filesystem: filename | inactive}**
9. **show install summary**
10. **exit**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>install add file location: filename</b> 例：	ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイ

	コマンドまたはアクション	目的
	<pre>Device# install add file bootflash:c8000v-universalk9_HLD_POLARIS_DEV_LATEST_20220227_153436.SSA.bin</pre>	ルの個々のコンポーネントをサブパッケージおよび <code>packages.conf</code> ファイルに展開します。
ステップ 3	<p><b>show install summary</b></p> <p>例 :</p> <pre>Device# show install summary</pre>	(オプション) イメージバージョンとそれに対応するインストール状態の概要を提供します。
ステップ 4	<p><b>install activate [auto-abort-timer &lt;time&gt;]</b></p> <p>例 :</p> <pre>Device# install activate auto-abort-timer 120</pre>	<p>以前に追加されたパッケージをアクティブ化し、プラットフォームをリロードします。</p> <ul style="list-style-type: none"> <li>ソフトウェアの完全インストールを実行する場合は、パッケージファイル名を指定しないでください。</li> <li><b>install activate</b> コマンドで <b>auto-abort-timer</b> が自動的に開始されます。タイマーのデフォルトは 120 分です。タイマーの期限が切れる前に <b>install commit</b> コマンドが実行されない場合、インストールプロセスは自動的に終了します。プラットフォームがリロードされ、最後にコミットされたバージョンで起動します。</li> </ul>
ステップ 5	<p><b>install abort</b></p> <p>例 :</p> <pre>Device# install abort</pre>	<p>(オプション) ソフトウェアインストールのアクティブ化を中止し、プラットフォームを最後にコミットされたバージョンに戻します。</p> <p>このコマンドは、イメージがアクティブ化されている状態でのみ使用できます。イメージがコミットされた状態の場合は使用できません。</p>
ステップ 6	<p><b>install commit</b></p> <p>例 :</p> <pre>Device# install commit</pre>	新しいパッケージのインストールをコミットし、リロード後も変更が持続されるようにします。
ステップ 7	<p><b>install rollback to committed</b></p> <p>例 :</p> <pre>Device# install rollback to committed</pre>	(オプション) 最後にコミットした状態にプラットフォームをロールバックします。
ステップ 8	<p><b>install remove {file filesystem: filename   inactive}</b></p> <p>例 :</p> <pre>Device# install remove inactive</pre>	<p>(オプション) ソフトウェア インストール ファイルを削除します。</p> <ul style="list-style-type: none"> <li><b>file</b> : 特定のファイルを削除します。</li> <li><b>inactive</b> : 未使用および非アクティブ状態のインストールファイルを削除します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 9	<b>show install summary</b>  例： Device# show install summary	(オプション) 現在のシステムの状態に関する情報を表示します。このコマンドの出力は、このコマンドよりも先に実行された <b>install</b> コマンドに応じて変化します。
ステップ 10	<b>exit</b>  例： Device# exit	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

## リリース 17.06.02 からリリース 17.07.01 へのアップグレード出力の例

```

=====
Upgrade steps
install add file bootflash:/ c8000v-universalk9.17.07.01a.SPA.bin
install activate
install commit
=====

Router#show version | inc IOS XE
Cisco IOS XE Software, Version 17.06.02
Router#show version | inc mode
Router operating mode: Autonomous

Router# dir bootflash:*bin*
Directory of bootflash:/*bin*

Directory of bootflash:/

   31  -rw-   832807301   Mar 7 2022 02:07:28 +00:00  c8000v-universalk9.17.07.01a.SPA.bin
5183766528 bytes total (2348220416 bytes free)

Router#install add file bootflash:/c8000v-universalk9.17.07.01a.SPA.bin
install_add: START Mon Mar 7 02:16:30 UTC 2022
install_add: Adding PACKAGE
install_add: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.07.01a.0.1883
SUCCESS: install_add Mon Mar 7 02:20:07 UTC 2022
VK5-C8K-8G-1762-1#

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version
-----
IMG   C   17.06.02.0.2786

```

```
IMG I 17.07.01a.0.1883
```

```
-----
Auto abort timer: inactive
-----
```

```
=====
install activate
=====
```

```
Router# show install summary
```

```
[ R0 ] Installed Package(s) Information:
```

```
State (St): I - Inactive, U - Activated & Uncommitted,
```

```
          C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type St Filename/Version
-----
```

```
IMG C 17.06.02.0.2786
```

```
IMG I 17.07.01a.0.1883
```

```
Router# install activate
```

```
install_activate: START Mon Mar 7 02:50:00 UTC 2022
```

```
install_activate: Activating PACKAGE
```

```
Following packages shall be activated:
```

```
/bootflash/c8000v-rpboot.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-mono-universalk9.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_nim_xdsl.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_nim_shdsl.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_nim_ge.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_nim_cwan.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_nim_async.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_ngwic_t1e1.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_dsp_sp2700.17.07.01a.SPA.pkg
```

```
/bootflash/c8000v-firmware_dreamliner.17.07.01a.SPA.pkg
```

```
This operation may require a reload of the system. Do you want to proceed? [y/n]y
```

```
--- Starting Activate ---
```

```
Performing Activate on Active/Standby
```

```
[1] Activate package(s) on R0
```

```
--- Starting list of software package changes ---
```

```
Old files list:
```

```
Modified c8000v-firmware_dreamliner.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_dsp_sp2700.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_ngwic_t1e1.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_nim_async.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_nim_cwan.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_nim_ge.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_nim_shdsl.17.06.02.SPA.pkg
```

```
Modified c8000v-firmware_nim_xdsl.17.06.02.SPA.pkg
```

```
Modified c8000v-mono-universalk9.17.06.02.SPA.pkg
```

```
Modified c8000v-rpboot.17.06.02.SPA.pkg
```

```
New files list:
```

```
Added c8000v-firmware_dreamliner.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_dsp_sp2700.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_ngwic_t1e1.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_nim_async.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_nim_cwan.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_nim_ge.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_nim_shdsl.17.07.01a.SPA.pkg
```

```
Added c8000v-firmware_nim_xdsl.17.07.01a.SPA.pkg
```

```
Added c8000v-mono-universalk9.17.07.01a.SPA.pkg
```

```
Added c8000v-rpboot.17.07.01a.SPA.pkg
```

```
Finished list of software package changes
```

```
[1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

Send model notification for install_activate before reload
Install will reload the system now!
SUCCESS: install_activate Mon Mar 7 02:57:34 UTC 2022
```

```
=====
install commit
=====
```

```
Router# show version | inc IOS XE
Cisco IOS XE Software, Version 17.07.01a
Router# show version | inc mode
Router operating mode: Autonomous
Router# show license udi
UDI: PID:C8000V,SN:9JM01Z7G2JH
```

## インストールモードでのアップグレード

この章に記載されている 1 ステップインストールまたは 3 ステップインストールの手順を使用して、インストールモードで Cisco Catalyst 8000V をアップグレードします。

## インストールモードでのダウングレード

ダウングレード先のイメージがインストールモードでインストールされている場合、**install rollback** コマンドを使用して、プラットフォームを適切なイメージにポイントすることにより、プラットフォームを以前のバージョンにダウングレードします。

この **install rollback** コマンドはプラットフォームをリロードし、前のイメージで起動します。



(注) **install remove inactive** コマンドを使用して前のファイルを削除していない場合にのみ、**install rollback** コマンドは成功します。



(注) このコマンドを使用できない場合は、**install** コマンドを使用して古いイメージをインストールすることでダウングレードすることもできます。

### ダウングレードの設定例

```
=====
install rollback
=====

Router# install rollback to base
install_rollback: START Tue Mar 01 03:25:46 UTC 2022
```

```

install_rollback: Rolling back to base
This operation may require a reload of the system. Do you want to proceed? [y/n]
*Mar 29 21:17:36.496: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
rollback
--- Starting Rollback ---
Performing Rollback on all members
  [1] Rollback package(s) on R0
  [1] Finished Rollback package(s) on R0
Checking status of Rollback on [R0]
Rollback: Passed on [R0]
Finished Rollback operation
SUCCESS: install_rollback Tue Mar 01 03:30:16 UTC UTC 2022

```

## ソフトウェアインストールの中止

ソフトウェアパッケージのアクティブ化は次の方法で中止できます。

- install commit** コマンドを発行する前に **auto-abort-timer** が期限切れになるようにします。新しいイメージをアクティブ化した後にプラットフォームをリロードすると、(3ステップインストールの方法で) **auto-abort-timer** がトリガーされます。タイマーが期限切れになるとインストールプロセスが終了します。プラットフォームはリロードし、最後にコミットしたバージョンのソフトウェアイメージで起動します。
- install commit** コマンドを使用せずに、**install auto-abort-timer stop** コマンドを使用してこのタイマーを停止します。このプロセスでは、新しいイメージはコミットされていないままです。
- install abort** コマンドを使用して、新しいソフトウェアのインストール前に実行していたバージョンにプラットフォームを戻します。このコマンドは、**install commit** コマンドを発行する前に使用します。

### 中止の設定例

```

=====
install abort
=====
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
Type  St   Filename/Version
-----
IMG   U    17.09.01.0.154628

-----
Auto abort timer: active , time before rollback - 01:56:56
-----

Router# show version | inc IOS XE
Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20220227_153436
Router# show version | inc mode
Router operating mode: Autonomous

```

```
Router# install abort
install_abort: START Tue Mar 01 04:03:52 UTC 2022

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Abort ---
Performing Abort on all members
 [1] Abort packages(s) on R0
 [1] Finished Abort packages(s) on R0
Checking status of Abort on [R0]
Abort: Passed on [R0]
Finished Abort operation

SUCCESS: install_abort Tue Mar 01 04:04:45 UTC 2022

Router# Mar 1 04:04:50.161: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
reload action requested
```

## インストールコマンドを使用したソフトウェアインストールのトラブルシューティング

**問題** ソフトウェアインストールのトラブルシューティング

**解決法** インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次の `show` コマンドを使用します。

- `show install summary`
- `show install log`
- `show version`
- `show version running`

**問題** インストールに関するその他の問題

**解決法** インストールに関する問題を解決するには、次のコマンドを使用します。

- `dir <install directory>`
- `more location:packages.conf`
- `show tech-support install` : このコマンドはインストール情報に固有の情報を表示する `show` コマンドを自動的に実行します。
- `request platform software trace archive target bootflash <location>` : このコマンドは、最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、この情報を指定された場所に保存します。

## よく寄せられる質問

- Q. Cisco Catalyst 8000V を Cisco CSR1000V や Cisco ISRv にダウングレードできますか。
- A. Cisco CSR1000V または Cisco ISRv 17.3.x 以降のバージョンから Cisco Catalyst 8000V にアップグレードした場合にのみ、Cisco Catalyst 8000V からダウングレードできます。



- 
- (注) Cisco Catalyst 8000V を新しくインストールした場合、Cisco CSR1000V や Cisco ISRv にダウングレードすることはできません。
- 

- Q. Cisco CSR1000V 16.12.x 以前のバージョンからアップグレードする場合、Secure Object Storage はサポートされますか。
- A. いいえ。Secure Object Storage はアップグレードでは引き継がれません。Secure Object Storage のサポートを有効にするには、新規インストールを実行するか、VM を再インストールする必要があります。
- Q. Cisco CSR1000V または Cisco ISRv から Cisco Catalyst 8000V にアップグレードする場合、ライセンスを変更する必要がありますか。
- A. Cisco Catalyst 8000V にアップグレードしても、ライセンスは同じままです。ただし、ライセンスはアップグレード後に SL から SLE に移行します。アップグレード前のスループットが 250M 以下の場合、アップグレード後もそのまま保持されます。

スループットが 250M を超え、デバイスが CSSM に登録されていた場合、接続はそのまま維持され、スループットによってデバイスへの SLAC のインストールが自動的にトリガーされます。対応するスループットは、SLAC がインストールされると設定されます。

デバイスが CSSM に接続されておらず、スループットが 250M を超えていた場合は、オフラインモードで SLAC を手動でインストールするか、CSSM との信頼を確立するために SLE コマンドを設定する必要があります。次に、SLAC のインストールをトリガーするようにスループットを設定します。



- 
- (注) SLAC がインストールされていない場合、スループットは 250M のままです。
- 

- Q. アップグレードプロセスの自動化は可能ですか。
- A. いいえ。移行の自動化は現在サポートされていません。
- Q. ダウングレードの実行時、障害モードではどんな処理が実行されますか。
- A. ダウングレードの結果として Cisco CSR1000V イメージが起動すると、システムはパーティションの形式をチェックします。パーティションの形式が要件に一致しない場合、起動は停

止されます。アップグレードまたはダウングレードの結果として Cisco Catalyst 8000V イメージが起動する場合、既存のパーティション形式を使用して起動を続行します。

- Q. アップグレード後のメモリとパフォーマンスにはどのような影響がありますか。
- A. Cisco Catalyst 8000V イメージのサイズが若干大きくなる場合があります、全体的なメモリフットプリントに影響が及ぶ可能性があります。とはいえ、その結果として全体的なメモリ要件が変更されることはありません。このイメージに必要な最小 RAM は 4 GB で、この機能によるパフォーマンスへの影響はありません。



## 第 17 章

# vCPU 分散の設定

この章では、テンプレートを使用したコントロールプレーン (CP)、データプレーン (DP)、およびサービスプレーン (SP) の vCPU の割り当てと分散を指定します。サービスプレーンには、SNORT を実行しているコンテナが含まれていることに注意してください。

vCPU 分散には、次のいずれかのテンプレートを使用します。

- [vCPU 分散：コントロールプレーン超高 \(179 ページ\)](#)
- [vCPU 分散：コントロールプレーン高 \(180 ページ\)](#)
- [vCPU 分散：データプレーン高 \(180 ページ\)](#)
- [vCPU 分散：データプレーン並 \(181 ページ\)](#)
- [vCPU 分散：サービスプレーン高 \(181 ページ\)](#)
- [vCPU 分散：サービスプレーン中 \(182 ページ\)](#)
- [データプレーン、コントロールプレーン、サービスプレーン全般にわたる vCPU 分散の設定 \(182 ページ\)](#)
- [アクティブ vCPU 分散テンプレートの決定 \(183 ページ\)](#)

## vCPU 分散：コントロールプレーン超高

次の表に、コントロールプレーン超高テンプレートの vCPU 分散を示します。

表 16: コントロールプレーン超高：vCPU 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1 1/2	1 1/2	0 ~ 5
サービスプレーン	1/3	1/2	1 1/2	1 1/2	0 ~ 5
データプレーン	1/3	1	1	5	6 ~ 15



- (注) コントロールプレーン超高テンプレートを 사용하면、サービスプレーンアプリケーションは、その動作のために 1.5 のフルコアを取得できます。たとえば、Wide Area Application Services (WAAS) の場合です。

## vCPU 分散 : コントロールプレーン高

次の表に、コントロールプレーン高テンプレートの vCPU 分散を示します。

表 17: コントロールプレーン高 : vCPU 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1	1	0 ~ 3
サービスプレーン	1/3	1/2	1	1	0 ~ 3
データプレーン	1/3	1	2	6	4 ~ 15



- (注) コントロールプレーン高テンプレートは、データプレーン高テンプレートと比較して、コントロールプレーン/サービスプレーンのサービスに追加のコアを割り当てます (コントロールプレーン用に 1 つのコア、サービスプレーン用に別のコアがあります)。サービスプレーンアプリケーションがない場合、コントロールプレーンはすべてのリソース (両方のコア) を使用します。

## vCPU 分散 : データプレーン高



- (注) データプレーン高テンプレートは、デフォルトの vCPU 分散テンプレートです。[Template] オプションの設定出力に [None] と表示されている場合でも、データプレーン高テンプレートがデフォルトで適用されます。

上記のステートメントは、コントローラモードで実行されている Cisco Catalyst 8000V インスタンスには適用されません。

次の表に、データプレーン高テンプレートの vCPU 分散を示します。

表 18: データプレーン高：vCPU 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1/2	1/2	0 ~ 1
サービスプレーン	1/3	1/2	1/2	1/2	0 ~ 1
データプレーン	1/3	1	3	7	2 ~ 15



(注) デフォルトでは、Cisco Catalyst 8000V コアの割り当ては、パフォーマンスのためにより大きなデータプレーンを優先します。サービスプレーンアプリケーションがない場合、コントロールプレーンはサービスプレーンのリソースも使用します。

## vCPU 分散：データプレーン並

データプレーン並テンプレートの vCPU 分散を使用して、vCPU 分散のテンプレートを使用する前と同じように Cisco Catalyst 8000V を強制的に動作させることができます。

つまり、ovf-env.xml ファイルで指定されているように、vCPU 分散用のデータプレーン高テンプレートを使用して Cisco Catalyst 8000V VM を作成するとします。後でデータプレーン並テンプレートで CLI コマンドを使用して、データプレーン高テンプレートによって以前に適用された XML ファイル設定を上書きできます。

## vCPU 分散：サービスプレーン高

次の表に、サービスプレーン高テンプレートの vCPU 分散を示します。

表 19: サービスプレーン高：vCPU 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1	2	0 ~ 7
サービスプレーン	1/3	1/2	1	2	0 ~ 7
データプレーン	1/3	1	2	4	8 ~ 15



(注) サービスプレーン高テンプレートを使用すると、サービスプレーンアプリケーション (Snort IPS など) は、その動作に最大 2 つのフルコアを使用できます。

## vCPU 分散：サービスプレーン中

次の表に、サービスプレーン中テンプレートの vCPU 分散を示します。

表 20: サービスプレーン中：vCPU 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1	1	0 ~ 3
サービスプレーン	1/3	1/2	1	1	0 ~ 3
データプレーン	1/3	1	2	6	4 ~ 15

## データプレーン、コントロールプレーン、サービスプレーン全般にわたる vCPU 分散の設定

Cisco Catalyst 8000V CLI で `platform resource` コマンドを入力して、vCPU 分散用のテンプレートを選択します。

**configure template**

**platform resource** *template*

例：

```
Router# configure template
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# platform resource ?
  control-plane-extra-heavy Use Control Plane Extra Heavy template
  control-plane-heavy      Use Control Plane Heavy template
  data-plane-heavy         Use Data Plane Heavy template
  data-plane-normal        Use Data Plane Normal template
  service-plane-heavy      Use Service Plane Heavy template
  service-plane-medium    Use Service Plane Medium template
Router(config)# platform resource service-plane-heavy
```



---

(注) `platform resource` コマンドを入力した後、Cisco Catalyst 8000V インスタンスを再起動してテンプレートをアクティブにする必要があります。

---

## アクティブ vCPU 分散テンプレートの決定

vCPU 分散に使用されているテンプレートを確認するには、次のコマンドを使用します。

**show platform software cpu alloc**

例 :

```
Router# show platform software cpu alloc
CPU alloc information:
Control plane cpu alloc: 0-1
Data plane cpu alloc: 2-3
Service plane cpu alloc: 0-1
Template used: CLI-service_plane_heavy
```



---

(注) コントロールプレーンとサービスプレーンは、コア 0 と 1 を共有します。

---





## 第 18 章

# Web ユーザ インターフェイス管理

Web ユーザーインターフェイスを使用すると、わかりやすいグラフィカルインターフェイスを使用してルータのパフォーマンスを監視できます。



- (注) 暗号マップトンネルを管理および設定するには、CLIを使用します。また、仮想トンネルインターフェイス (VTI) を使用してトンネルを設定し、CLIまたはGUIを使用してトンネルを作成することもできます。

次のいずれかのタスクの手順を実行して、ルータを設定できます。

- [Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定 \(185 ページ\)](#)
- [基本または詳細モードセットアップウィザードの使用 \(186 ページ\)](#)

## Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定

クイック セットアップ ウィザードを使用して、基本的なルータ設定を実行できます。ルータを設定するには、以下の手順を実行します。

### 始める前に

- Web UI にアクセスする前に、デバイスで基本設定を行う必要があります。

### 手順

**ステップ 1** シリアルケーブルの RJ-45 側をルータの RJ-45 コンソールポートに接続します。

**ステップ 2** デバイスの初期設定ウィザードが表示された後、次のシステムメッセージがルータに表示されたら、「No」と入力してデバイスプロンプトを表示します。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

**ステップ3** コンフィギュレーション モードで、次の設定パラメータを入力します。

```
!  
ip dhcp pool WEBUIPool  
network 192.168.1.0 255.255.255.0  
default-router 192.168.1.1  
username webui privilege 15 password cisco  
!  
interface gig 0/0/1  
ip address 192.168.1.1 255.255.255.0  
!
```

**ステップ4** イーサネットケーブルでデバイスとルータを接続し、gig 0/0/1 インターフェイスに接続します。

**ステップ5** システムを DHCP クライアントとして設定し、ルータの IP アドレスを自動的に取得します。

**ステップ6** ブラウザを起動し、ブラウザのアドレス行にデバイスの IP アドレスを入力します。セキュアな接続の場合は、「https://192.168.1.1/#/dayZeroRouting」と入力します。あまりセキュアではない接続の場合は、「http://192.168.1.1/#/dayZeroRouting」と入力します。

**ステップ7** デフォルトのユーザー名 (webui) とデフォルトのパスワード (cisco) を入力します。

---

## 基本または詳細モード セットアップ ウィザードの使用

基本モードまたは詳細モードのセットアップを使用してルータを設定するには、次の手順を実行します。

### 手順

---

**ステップ1** [Basic Mode] または [Advanced Mode] を選択し、[Go To Account Creation Page] をクリックします。

**ステップ2** ユーザー名とパスワードを入力します。確認のためにパスワードを再入力します。

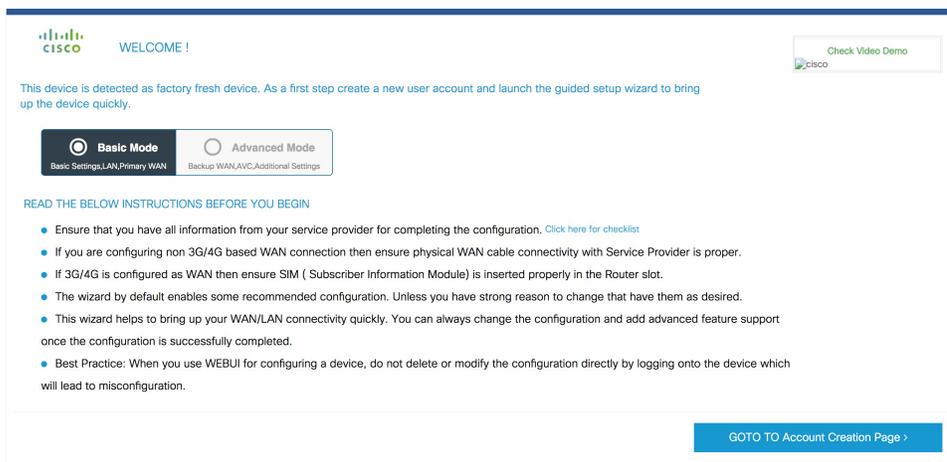
**ステップ3** [Create and Launch Wizard] をクリックします。

**ステップ4** デバイス名とドメイン名を入力します。

**ステップ5** [Time Zone] ドロップダウンリストから、適切なタイムゾーンを選択します。

**ステップ6** [Date and Time] ドロップダウンリストから、適切な日時モードを選択します。

**ステップ7** [LAN Settings] をクリックします。



## LAN 設定を行います。

### 手順

ステップ 1 [Web DHCP Pool/DHCP Pool] 名または [Create and Associate Access VLAN] オプションを選択します。

a) [Web DHCP Pool] を選択した場合は、次を指定します。

[Pool Name] : DGCP プール名を入力します。

[Network] : ネットワークアドレスおよびサブネットマスクを入力します。

b) [Create and Associate Access VLAN] オプションを選択した場合は、次を指定します。

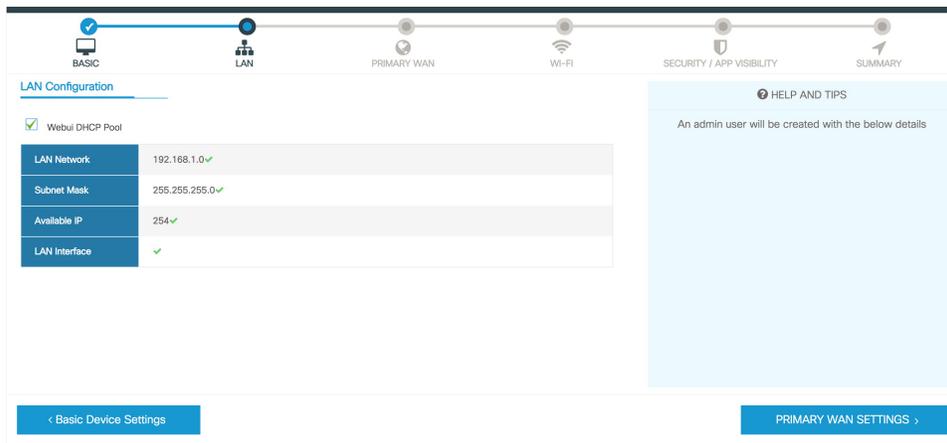
[Access VLAN] : アクセス VLAN の識別番号を入力します。指定できる範囲は 1 ~ 4094 です。

[Network] : VLAN の IP アドレスを入力します。

[Management Interfaces] : インターフェイスを選択し、右矢印と左矢印を使用して選択したリストボックスに移動します。ダブルクリックするかドラッグアンドドロップして、選択したリストボックスにインターフェイスを移動することもできます。

ステップ 2 [Primary WAN Settings] をクリックします。

プライマリ WAN 設定を行います。



## プライマリ WAN 設定を行います。

### 手順

- ステップ 1 プライマリ WAN タイプを選択します。プライマリ WAN は、ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド (xDSL) を設定できます。
- ステップ 2 ドロップダウンリストからインターフェイスを選択します。
- ステップ 3 サービスプロバイダーから DNS サーバ情報を直接取得するには、[Get DNS Server info directly from ISP] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。
- ステップ 4 [Get IP automatically from ISP] チェックボックスをオンにして、サービスプロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネットマスクを入力します。
- ステップ 5 [Enable NAT] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。
- ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは PAP と CHAP です。
- ステップ 7 サービスプロバイダーから提供されたユーザー名とパスワードを入力します。
- ステップ 8 [Security/APP Visibility WAN Settings] をクリックします。

The screenshot shows the 'WAN Configuration' page in the Cisco Catalyst 8000V Web User Interface. The page is divided into several sections: 'WAN Configuration', 'DNS / IP Address', and 'Profile'. In the 'DNS / IP Address' section, three checkboxes are checked: 'Get DNS Server info directly from ISP', 'Get IP automatically from ISP', and 'Enable NAT'. In the 'Profile' section, there is an 'Access Point Name (APN)' field and an unchecked checkbox for 'Configure username and password if provided by service'. A 'HELP AND TIPS' box on the right contains the text 'An admin user will be created with the below details'. Navigation buttons for '< LAN SETTINGS' and 'Wi-Fi >' are located at the bottom of the page.

## セカンダリ WAN 設定を行います。

詳細設定では、セカンダリ WAN 接続を設定する必要があります。

### 手順

- ステップ 1** セカンダリ WAN タイプを選択します。ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド (xDSL) をセカンダリ WAN として設定できます。
- ステップ 2** ドロップダウンリストからインターフェイスを選択します。
- ステップ 3** サービス プロバイダーから DNS サーバ情報を直接取得するには、[**Get DNS Server info directly from ISP**] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。
- ステップ 4** [**Get IP automatically from ISP**] チェックボックスをオンにして、サービス プロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。
- ステップ 5** [**Enable NAT**] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。
- ステップ 6** [**Enable PPPoE**] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。
- ステップ 7** サービスプロバイダーから提供されたユーザー名とパスワードを入力します。
- ステップ 8** [**Security/APP Visibility WAN Settings**] をクリックします。

## セキュリティ設定の構成

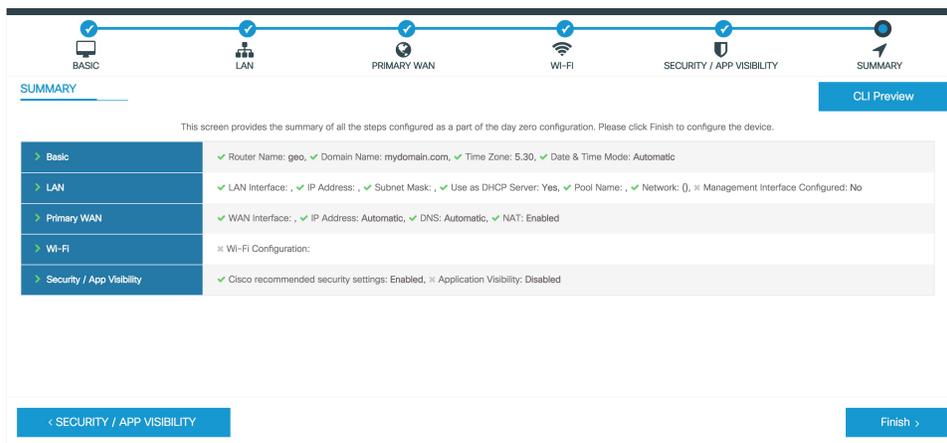
### 手順

**ステップ 1** すべてのパスワードがプレーンテキストで表示されないようにするには、**[Enable Recommended Settings]** チェックボックスをオンにします。パスワードは暗号化されます。

**ステップ 2** **[Day 0 Config Summary]** をクリックします。

**ステップ 3** 設定をプレビューするには、**[CLI preview]** をクリックします。

**ステップ 4** **[Finish]** をクリックして、デイゼロセットアップを完了します。





## 第 19 章

# GRUB モードへのアクセスと使用

Cisco Catalyst 8000V は、NVRAM 内に 16 ビットのコンフィギュレーションレジスタを搭載しています。各ビットの値は1（オン、つまり設定）または0（オフ、つまり解除）です。各ビットの設定は、次回のリロードまたはオフ/オン時のルータ動作に影響を与えます。GRUB モードでは、他のシスコルータの ROMMON オプションに相当するコンフィギュレーションレジスタ オプションのサブセットがサポートされます。

コンフィギュレーションレジスタを使用すると、次の作業を行うことができます。

- ルータで GRUB モード（ブートストラッププログラム）を強制的に起動させる
- 起動元およびデフォルトのブートファイル名を選択する
- 忘れたパスワードを回復する

次の表でコンフィギュレーションレジスタビットについて説明します。

表 21: コンフィギュレーションレジスタビットの説明

ビット番号	16進数	意味
00 ~ 03	0x0000 ~ 0x000F	ブートフィールド。ブートフィールドの設定によって、ルータがオペレーティングシステムをロードするかどうか、どこからシステムイメージを取得するかが決まります。  詳細については、表「コンフィギュレーションレジスタのブートフィールドビットの説明」を参照してください。

ビット番号	16進数	意味
06	0x0040	システム ソフトウェアに NVRAM の内容を無視させます。これは、パスワード回復に使用できます。



(注) クラウドソリューションで実行されている Cisco Catalyst 8000V の GRUB モードの開始は、クラウドプロバイダーのコンソールアクセス機能によって異なります。クラウドプロバイダーがコンソールへの制限付きアクセスを提供している場合、パスワード回復のために GRUB モードにアクセスすることはできません。



(注) ルータの再起動時に自動的に GRUB モードになるようにルータを設定するには、0x000 設定を使用します。

- [GRUB モードへのアクセス \(192 ページ\)](#)
- [GRUB メニューの使用 \(193 ページ\)](#)
- [コンフィギュレーションレジスタ \(confreg\) の変更 \(195 ページ\)](#)
- [コンフィギュレーションレジスタ設定の変更 \(197 ページ\)](#)
- [コンフィギュレーションレジスタの設定の表示 \(198 ページ\)](#)

## GRUB モードへのアクセス

GRUB モードにアクセスするには、次の手順を実行します。

### 手順

#### ステップ 1 enable

例 :

```
Router> enable
```

特権 EXEC モードを有効にします。

- プロンプトが表示されたらパスワードを入力します。

#### ステップ 2 config-register 0x0000

例 :

```
Router# config-register 0x0000
```

値「0000」（0x0）を入力して GRUB モードを開始します。

次に、GRUB モードを開始する例を示します。

```
Router(config)# config-register 0x0000
```

```
GNU GRUB version 2.02
```

```
Minimal BASH-like line editing is supported. For the first word, TAB  
lists possible command completions. Anywhere else TAB lists possible  
device or file completions. ESC at any time exits.
```

```
grub> confreg 0x2102
```

grub> プロンプトで疑問符を入力すると、システムヘルプの表示と **config register** コマンドの入力の2つのオプションが表示されます。

---

## GRUB メニューの使用

GRUB メニューを使用して、ルータにロードされているソフトウェアイメージを表示し、どのイメージから起動するかを選択します。GRUB メニューにアクセスするには、GRUB プロンプトで「ESC」と入力します。次に、GRUB メニューの表示を示します。

上下の矢印キーを使用して、どのイメージからルータを起動するかを選択します。GRUB プロンプトに戻るには、文字「c」を入力します。

## GRUB モードの開始とイメージの選択

GR およびユニファイドブートローダー（GRUB）モードから新しいシステムイメージをロードするには、EXEC モードで次の手順を実行します。

### 手順

---

#### ステップ 1 **dir bootflash:**

このコマンドを使用して、ブートフラッシュメモリ内のすべてのファイルおよびディレクトリを表示します。

例：

```
Router# dir bootflash:
```

```
Directory of bootflash:/  
 3  -rw-      6458388   Dec 18 2020 00:00:58 c8000v.tmp  
1580 -rw-      6462268   Dec 18 2020 06:14:02 c8000v-ata  
63930368 bytes total (51007488 bytes free)
```

#### ステップ 2 **configure terminal**

このコマンドを使用して、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。

例：

```
Router# configure terminal  
Router(config)#
```

### ステップ 3 **boot system bootflash:system-image-filename.bin**

次回システム リロード後またはオフ/オン後に新しいシステム イメージをロードします。次に例を示します。

例：

```
Router(config)# boot system bootflash:  
c8000v-universalk9.17.04.01a.SPA.bin
```

(注)

新しいシステムイメージが、**dir bootflash:** コマンド出力に表示される最初のファイルまたは唯一のファイルの場合は、このステップを実行する必要はありません。

### ステップ 4 **do write**

または

**do write memory**

例：

```
Router(config)# do write memory
```

(注)

**do write** コマンドまたは **do write memory** コマンドを入力すると、ブートフラッシュディスクで使用可能なイメージの GRUB メニューリストが更新されます。

### ステップ 5 **config-register 0x0000**

このコマンドを使用して、GRUB モードを開始します。

次に、GRUB モードを開始する設定出力の例を示します。

例：

```
GNU GRUB version 2.02
```

```
Minimal BASH-like line editing is supported. For the first word, TAB  
lists possible command completions. Anywhere else TAB lists possible  
device or file completions. ESC at any time exits.
```

```
grub> confreg 0x2102
```

例：

(注)

**config-register** を 0x0000 に設定した場合は、システムを自動起動するために、デフォルトの 0x2102 にリセットする必要があります。値が 0x0 の場合、システムは GRUB モードで停止します。

**ステップ 6** `grub>` プロンプトで「ESC」と入力して、GRUB メニューにアクセスします。

起動に使用できるイメージを含む GRUB メニューが表示されます。

例：

```
Cisco IOS XE Software, Version 2020-09-17_09.24_kamitch
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
Version 17.5.20200916:194029 [HEAD-/scratch/kamitch/git/polaris-work/boottime1 106]
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Wed 16-Sep-20 15:45 by kamitch
```

```
Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: IOS-XE ROMMON
```

```
Router uptime is 18 minutes
Uptime for this control processor is 21 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
```

上下の矢印キーを使用して、ルータを起動するイメージを選択します。GRUB プロンプトに戻るには、文字「c」を入力します。

**ステップ 7** ルータのソフトウェアイメージを新しいバージョンにアップグレードするには、`.bin` ファイルを選択します。

**ステップ 8** **Enter** を押して選択したイメージを起動し、アップグレードプロセスを開始します。

## コンフィギュレーションレジスタ (confreg) の変更

このセクションでは、**confreg** GRUB コマンドを使用して、コンフィギュレーションレジスタを変更する方法について説明します。このコマンドは、他のシスコ製ハードウェアルータの **confreg** ROMOM コマンドに似ています。このルータには ROMOM モードが含まれていないため、同様の機能は GRUB コマンドモードで処理されます。

グローバルコンフィギュレーションモードで **config-register** コマンドを使用して、Cisco IOS CLI からコンフィギュレーションレジスタの設定を変更することもできます。



(注) 変更したコンフィギュレーションレジスタ値は、NVRAMに自動的に書き込まれますが、新しい値が有効になるのは、ルータをリセットまたはオフ/オンしてからです。

## 手順

**confreg** [*value*]

例 :

```
grub> confreg 0x2102
```

GRUB コマンドモードでコンフィギュレーションレジスタの設定値を変更します。

- 任意で、コンフィギュレーションレジスタに対応する新しい16進値を入力します。値の範囲は0x0～0xFFFF です。
- 値を入力しなかった場合、16ビットのコンフィギュレーションレジスタの各ビットについて、入力が求められます。

## 次のタスク

次のコードは、GRUB モードを開始して、コンフィギュレーションレジスタを使用する例です。GRUB モードにアクセスするには、Cisco IOS XE **config-register** コマンドを入力し、値として「0000」を指定します。

```
Router(config)# config-register 0x0000

GNU GRUB version 0.97 (638K lower / 3143616K upper memory)
 [ Minimal BASH-like line editing is supported. For the first word, TAB
   lists possible command completions. Anywhere else TAB lists the possible
   completions of a device/filename. ESC at any time exits to menu. ]
grub> help
 [ Minimal BASH-like line editing is supported. For the first word, TAB
   lists possible command completions. Anywhere else TAB lists the possible
   completions of a device/filename. ESC at any time exits to menu. ]
confreg [VALUE] help [--all] [PATTERN ...]
grub> confreg
      Configuration Summary
      (Virtual Configuration Register: 0x0)
enabled are:
boot: the boot loader
do you wish to change the configuration? y/n [n
]:
ignore system config info? y/n [n
]:
automatically boot default system image? y/n [n
]:
Configuration Register: 0x0
grub> confreg
      Configuration Summary
      (Virtual Configuration Register: 0x0)
enabled are:
boot: the boot loader
do you wish to change the configuration? y/n [n
]:
ignore system config info? y/n [n]:
```

```

automatically boot default system image? y/n [n]:
Configuration Register: 0x42
grub> confreg 0x2102
Configuration Register: 0x2102
grub> confreg
      Configuration Summary
      (Virtual Configuration Register: 0x2102)
enabled are:
boot: default image
do you wish to change the configuration? y/n [n
]:
grub>
grub>
      GNU GRUB  version 2.02  (638K lower / 3143616K upper memory)
-----
0: C8000v - packages.conf
1: C8000v - c800v-packages-universalk9
2: C8000v - GOLDEN IMAGE
-----
      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, or 'c' for a command-line.
Highlighted entry is 0:
Booting 'C8000v - packages.conf'
root (hd0,0)
  Filesystem type is ext2fs, partition type 0x83
kernel /packages.conf rw root=/dev/ram console=ttyS1,9600 max_loop=64 HARDWARE=
virtual SR_BOOT=harddisk:packages.conf
Calculating SHA-1 hash...done
SHA-1 hash:
      calculated  817e1716:e8e62778:7dd0b806:32db2bdd:13e51407
      expected    817e1716:e8e62778:7dd0b806:32db2bdd:13e51407
package header rev 1 structure detected
Calculating SHA-1 hash...done
SHA-1 hash:
      calculated  d4eaba99:34cbda63:26151233:9d0e9aa4:9c625302
      expected    d4eaba99:34cbda63:26151233:9d0e9aa4:9c625302
Package type:0x7531, flags:0x0
  [Linux-bzImage, setup=0x2e00, size=0x2c18c00]
  [isord @ 0x7e6d0000, 0x191f000 bytes]

```

## コンフィギュレーションレジスタ設定の変更

コンフィギュレーションレジスタの設定値は、GRUB からでも Cisco IOS XE CLI からでも変更できます。ここでは、Cisco IOS XE CLI からコンフィギュレーションレジスタの設定値を変更する方法について説明します。

Cisco IOS XE CLI からコンフィギュレーションレジスタの設定値を変更する手順は、次のとおりです。

### 手順

**ステップ 1** ルータの電源を投入します。

**ステップ 2** 初期ダイアログを開始するかどうか尋ねられるので、no と応答します。

例：

```
Would you like to enter the initial dialog? [yes]: no
```

数秒後にユーザー EXEC プロンプト (Router>) が表示されます。

**ステップ 3** 「enable」と入力して特権 EXEC モードを開始し、プロンプトが表示されたらパスワードを入力します。

例：

```
Router> enable
Password: password
Router#
```

**ステップ 4** 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。

例：

```
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
```

**ステップ 5** コンフィギュレーションレジスタの設定値を変更するには、**config-register value** コマンドを入力します。  
*value* は **0x** を前に加えた 16 進数です。

例：

```
Router(config)# config-register 0x
value
```

**ステップ 6** グローバル コンフィギュレーション モードを終了します。

例：

```
Router(config)# end
Router#
```

**ステップ 7** 変更した設定を NVRAM に保存します。

```
Router# copy running-config startup-config
```

新しいコンフィギュレーションレジスタの設定値が NVRAM に保存されても、有効になるのは次回のルータリロード時またはオフ/オン時です。

---

## コンフィギュレーションレジスタの設定の表示

現在有効なコンフィギュレーションレジスタの設定値および次回のルータリロード時に使用される設定値を表示するには、特権 EXEC モードで **show version** コマンドを入力します。

コンフィギュレーションレジスタの設定値は、**show version** コマンド出力の最終行に示されます。

```
Configuration register is 0x142 (will be 0x142 at next reload)
```



## 第 20 章

# 工場出荷時の状態へのリセット

この章では、Cisco Catalyst 8000V の初期設定へのリセットの実行について説明します。初期設定へのリセット機能は、ルータから機密情報を削除したり、ルータを完全に機能する状態にリセットしたりするのに役立ちます。

- [初期設定へのリセットに関する情報 \(199 ページ\)](#)
- [初期設定へのリセット実行の前提条件 \(200 ページ\)](#)
- [初期設定へのリセット実行の制限事項 \(200 ページ\)](#)
- [初期設定へのリセットの実行方法 \(201 ページ\)](#)

## 初期設定へのリセットに関する情報

初期設定へのリセットは、ルータの現在の実行コンフィギュレーション情報およびスタートアップコンフィギュレーション情報をクリアし、ルータを以前の完全に機能する状態にリセットするプロセスです。初期設定へのリセットプロセスでは、**factory-reset all** コマンドを使用します。



(注) Cisco Catalyst 8000V インスタンスの初期設定へのリセットにかかる時間は、ストレージのタイプやルータに存在するデバイスなどの要因によって異なります。

### 削除される情報 :

初期設定へのリセットを実行すると、次の情報が削除されます。

- ライセンス : ユーザーがインストール、製造元が提供
- 不揮発性ランダム アクセス メモリ データ
- ユーザーのログイン情報
- 起動設定
- すべての書き込み可能ファイルシステムおよび個人データ

- ROMMON 変数
- 永続ストレージデバイス
- ブートフラッシュで実行されているコンテナ

#### 保持される情報：

ただし、次の情報は初期設定へのリセット後も保持されます。

- リセット完了後にルータへのアクセスを提供するファイルを含む重要な情報
- 初期設定へのリセットを実行する前にインストールされていたソフトウェアパッケージ
- UDI およびスマートライセンスファイル

#### サポートされているシナリオ：

初期設定へのリセット機能は、次のシナリオで使用できます。

- Cisco Catalyst 8000V インスタンスを安全な方法で削除する場合。
- 悪意のある攻撃によってルータのデータが侵害された場合、ルータを初期設定にリセットしてから、今後の使用のためにもう一度設定しなおす必要があります。

#### サポート対象プラットフォーム：

初期設定へのリセットは、Amazon Web Services、Microsoft Azure、GCP クラウド、VMware ESXi、Hyper-V を含むすべてのプラットフォームで実行されている Cisco Catalyst 8000V インスタンスでサポートされています。

## 初期設定へのリセット実行の前提条件

- 初期設定へのリセット操作を実行する前に、すべてのソフトウェアイメージ、設定、および個人データがバックアップされていることを確認してください。
- 初期設定へのリセットプロセスが進行中の場合は、電源の中断がないことを確認します。
- インスタンスのブートフラッシュに少なくとも 8 GB のメモリがあることを確認します。

## 初期設定へのリセット実行の制限事項

- ルータにインストールされているソフトウェアパッチは、初期設定へのリセット操作後に復元されません。
- 初期設定へのリセットプロセス中は、Cisco Catalyst 8000V インスタンスを再起動しないでください。

- 仮想テラタイプ (VTY) セッションを介して `factory reset` コマンドが発行された場合、初期設定へのリセットプロセスの完了後にセッションは復元されません。

## 初期設定へのリセットの実行方法

### 手順

**ステップ 1** Cisco Catalyst 8000V インスタンスにログインします。

**ステップ 2** コマンドプロンプトで、**factory-reset all** コマンドを実行します。

次の情報が表示されます。

```
factoryreset#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: All writable file systems and personal data
2: Licenses
3: Configuration
4: User Credentials
The system will reload to perform a factory reset.
Note that any day0 configuration will be applied after reload
DO NOT STOP OR INTERRUPT THE POWER DURING RESET
Are you sure you want to continue? [confirm]Connection to 172.18.25.29 closed by remote host.
Connection to 172.18.25.29 closed.
```

**ステップ 3** `confirm` と入力して初期設定へのリセットを続行します。

(注)

初期設定へのリセットプロセスにかかる時間は、ストレージのタイプと、Cisco Catalyst 8000V インスタンスを展開するクラウドサービスによって異なります。

(注)

初期設定へのリセットプロセスを終了する場合は、**Escape** キーを押します。

### 次のタスク

初期設定へのリセットプロセスが完了すると、プロセスが成功したかどうかを示すログファイルがブートフラッシュに保存されます。

## 初期設定へのリセット後におけるスマートライセンスの復元

リセット後、スマートライセンスの設定も削除されます。トークン ID を使用して、ルータでスマートライセンスを再設定する必要があります。接続モードでは、スマートライセンス用にインスタンスを登録するときに、強制オプションを使用する必要があります。つまり、**license**

**smart register idtoken \*\*\*\*\*token\*\*\*\*\* force** コマンドを使用する必要があります。登録プロセスが開始されます。

強制オプションを使用せず、スマートライセンスを直接設定すると、ライセンスの登録が失敗します。次に、失敗した登録の出力例を示します。

```
router#show license status
router#show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 15 22:03:29 2019 UTC
  Failure reason: The product
  regid.2013-08.com.cisco.C8KV,1.0_1562da96-9176-4f99-a6cb-14b4dd0fal35 and sudi containing
  udiSerialNumber:9XIVK9PIVVK,udiPid:C8000V has already been registered.

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
```

**license smart register idtoken \*\*\*\*\*token\*\*\*\*\* force** コマンドを実行すると、ライセンスは登録済み (Registered) 状態になります。次に、Registered 状態の設定出力の例を示します。

```
router#show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: InternalTestDemoAccount8.cisco.com
  Virtual Account: RTP-CSR-DT-Prod
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Feb 15 22:04:07 2019 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Dec 14 22:04:06 2020 UTC
  Registration Expires: Dec 15 21:59:05 2021 UTC
```

```
License Authorization:
Status: AUTHORIZED on Dec 15 22:04:11 2020 UTC
Last Communication Attempt: SUCCEEDED on Feb 15 22:04:11 2019 UTC
Next Communication Attempt: Dec 17 22:04:11 2020 UTC
Communication Deadline: Dec 16 21:58:10 2020 UTC

Export Authorization Key:
Features Authorized:
<none>
```

## 初期設定へのリセット後の動作

初期設定へのリセットが正常に完了すると、ルータが起動します。ただし、初期設定へのリセットプロセスが開始される前に、コンフィギュレーションレジスタが ROMMON から手動で起動するように設定されていた場合、ルータは ROMMON で停止します。



**重要** 現在のブートイメージがリモートイメージであるか USB または NIM-SSD に保存されている場合は、初期設定へのリセットプロセスを開始する前に、必ずイメージのバックアップを作成してください。

初期設定にリセットしても、Cisco Catalyst 8000V インスタンスの UDI は変更されません。初期設定へのリセット後に UDI が同じであるかどうかを確認するには、初期設定へのリセットプロセスの前後に **factoryreset#show license udi** コマンドを実行します。

スマートライセンスを設定したら、**#show license status** コマンドを実行して、インスタンスでスマートライセンスが有効になっているかどうかをチェックします。



(注) 初期設定へのリセットを実行する前に SLR を有効にしていた場合は、同じライセンスを使用し、スマートエージェントから受け取ったライセンスキーを入力します。





## 第 21 章

# VRF ルート共有の設定

次の章では、Cisco Catalyst 8000V インスタンスで VRF ルート共有を設定する方法について説明します。VRF ルート共有は、オンプレミスサイトとパブリッククラウドサイト間でトラフィックを転送する必要がある場合に必要です。クラウド全体に共有サービスを展開するには、VxLAN ピア間で VRF ルート共有を設定します。

- [VRF ルート共有に関する情報 \(205 ページ\)](#)
- [VRF ルート共有の前提条件 \(206 ページ\)](#)
- [VRF ルート共有に関する制約事項 \(206 ページ\)](#)
- [VRF ルート共有の設定方法 \(206 ページ\)](#)
- [VRF ルート共有の確認 \(210 ページ\)](#)

## VRF ルート共有に関する情報

APIC レイヤ (オンプレミス) とパブリッククラウドサイトがあるハイブリッドクラウドソリューションでは、Cisco Catalyst 8000V インスタンスはレイヤ 3 境界を介してデータセンターを接続します。Cisco Catalyst 8000V インスタンスには、2 セットのインポートおよびエクスポートルートターゲットで設定された VRF インスタンスがあります。インポート/エクスポートルートターゲットの 1 つのセットは、オンプレミスルータの VxLAN カプセル化および L3 ルーティング情報を使用して BGP EVPN セッションに関連付けられます。インポート/エクスポートルートターゲットの他のセットは、サービスプロバイダーネットワークの L3VPN BGP ネイバーに関連付けられます。Cisco Catalyst 8000V インスタンスは、オンプレミスサイトとサービスプロバイダーネットワーク間のルートをステッチすることで、EVPN 全体で L3 トラフィックの移動を可能にします。

Cisco Catalyst 8000V インスタンスは、VRF に同じ VTEP IP (VxLAN トンネルエンドポイント) と RMAC (ルータ MAC アドレス) がある場合でも、EVPN を介してトラフィックを転送します。この機能により、Cisco Catalyst 8000V インスタンスはバインディングラベルを使用してルーティングと転送チェーンを設定します。

VRF ルート共有機能を使用すると、ハイブリッドクラウド全体に共有サービスを展開できます。パブリッククラウドで実行される共有サービスは、オンプレミスサイトのエンドポイントで使用できます。Cisco Catalyst 8000V インスタンスは、オンプレミスサイト上の複数の VRF

と L3 プレフィックスを共有し、その逆も同様です。APIC レイヤはアドレスをインポートし、サービスは APIC 側で使用されます。

## VRF ルート共有の前提条件

VRF ルート共有機能を設定して ACI とパブリッククラウド間のトラフィックを有効にする前に、次のことを確認します。

- ACI の vPC ペアで VRF1 と VRF2 を設定します。
- VRF3 は、VGW とピアリングする Cisco Catalyst 8000V インスタンス上の VRF4 であり、VRF ごとに 2 つの RT があります。
- Cisco Catalyst 8000V インスタンスは、VRF1&2 の EVPN ルートを ACI から VRF3&4 にインポートします。
- Cisco Catalyst 8000V 側の IP BGP は、パブリッククラウドのゲートウェイにルートを再配布します。
- ACI からのルートのネクストホップは、ACI の境界リーフのスパインです。
- ルート共有 VRF 全体でプレフィックスの重複はありません。
- L3 VPN ルーティングをアドバタイズし、VRF プレフィックスを EVPN ネイバーに転送します。advertise l2vpn evpn コマンドを実行し、スティーチング RT をエクスポートして、ネイティブルートを EVPN にプッシュします。

## VRF ルート共有に関する制約事項

- VRF 共有機能は、最大 32 の共通 VRF と 1000 のカスタマー VRF の組み合わせをサポートします。
- この機能は RT フィルタをサポートしていません。
- VRF ルート共有は、IPv4 アドレスでのみサポートされ、IPv6 アドレスではサポートされません。

## VRF ルート共有の設定方法

### サンプルトポロジと使用例

ハイブリッドクラウドでの VRF ルート共有を説明するために、サンプルトポロジについて考えてみましょう。サンプルトポロジでは、Cisco Catalyst 8000V インスタンスがパブリッククラウドの VM に展開されていると見なします。サイト A は ACI 展開サイトで、サイト B はパブ

リッククラウドです。リーフ 1 とリーフ 2 は、ACI の仮想ポートチャネル (vPC) ペアです。これらの 2 つの vPC は、異なるルート識別子 (RD) で設定されます。ここでは、VRF 1 と VRF 2 が ACI の vPC ペアで設定されています。次の例を参考にしてください。

VRF1 - RT : RT-EVPN-1、プレフィックス : 192.168.1.1

VRF2 - RT : RT-EVPN-2、プレフィックス : 192.168.2.2

Cisco Catalyst 8000V インスタンスで VRF3 と VRF4 が設定されています。これら 2 つの VRF は音声ゲートウェイ (VGW) とペアになっており、これら 2 つの VRF には 2 つの異なるルートターゲット (RT) があります。次の例を参考にしてください。

VRF3 - EVPN 用 RT : RT-EVPN-3、IP BGP 用 RT : RT-3、プレフィックス : 192.168.3.3

VRF4 - EVPN 用 RT : RT-EVPN-4、IP BGP 用 RT : RT-4、プレフィックス : 192.168.4.4

このトポロジでは、BGP-EVPN ファブリックが ACI とパブリッククラウドの Cisco Catalyst 8000V インスタンスの間に存在し、Cisco Catalyst 8000V インスタンスと Azure などのクラウドサービスプロバイダーの間で IP BGP プロトコルが使用されます。BGP-EVPN ファブリックは、EVPN と IP BGP 間のステッチングルートを再配布します。

ACI サイトとパブリッククラウド間のトラフィックフローを有効にするには、ACI と Cisco Catalyst 8000V インスタンスの両方が VRF ルート共有をサポートする必要があります。

Cisco Catalyst 8000V インスタンスは、VRF1 および VRF2 の EVPN ルートを ACI から VRF3 および VRF4 にインポートできる必要があります。Cisco Catalyst 8000V 側の IP BGP は、パブリッククラウド内の VGW へのルートを再配布します。



- (注) VTEP (VxLAN トンネルエンドポイント) IP と RMAC (ルート MAC アドレス) が 2 つのリーフで同じで、VNIC だけが異なる場合、Cisco Catalyst 8000V インスタンスはトンネルを介してトラフィックを転送できます。

## ユースケース

同じトポロジ例を使用して、Cisco Catalyst 8000V インスタンスで VRF ルート共有を設定する使用例を次に示します。

- VRF1 と VRF2 は VRF3 と通信できるが、VRF3 と VRF4 は相互に通信できない場合は、次の設定を実行します。

```
vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
vrf definition VRF4
rd 400:1
address-family ipv4
```

- VRF1 と VRF2 が VRF3 および 4 と通信できるが、VRF3 と VRF4 が相互に通信できない場合は、次の設定を実行します。

```

vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
vrf definition VRF4
rd 400:1
address-family ipv4
route-target export RT-EVPN-4 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching

```

- VRF1 と VRF2 は VRF3 と通信できるが、VRF3 と VRF4 は相互に通信できる場合は、次の設定を実行します。

```

vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
route-target export RT-3
route-target import RT-4
vrf definition VRF4
rd 400:1
address-family ipv4
route-target import RT-3
route-target export RT-4

```

- VRF1 と VRF2 は VRF3 および 4 と通信できるが、VRF3 と VRF4 は相互に通信できる場合は、次の設定を実行します。

```

vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
route-target export RT-3
route-target import RT-4
vrf definition VRF4
rd 400:1
address-family ipv4
route-target export RT-EVPN-4 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
route-target import RT-3
route-target export RT-4

```



(注) 上記の使用例では、Cisco Catalyst 8000V インスタンスは VRF3 と VRF4 の両方で EVPN を設定する必要があります。

IP BGP はすでに VRF3 と VRF4 からすべてのルートをインポートしていますが、BGP はインポートされた VRF のルートを EVPN ピアにアドバタイズしません。

EVPN全体で共有が行われる場合にのみ、設定で**Stitching** キーワードを使用する必要があります。

## VRF ルート共有の設定

### 手順

VRF 1 および VRF 2（オンプレミス）が VRF 3 および VRF 4（パブリッククラウド内）と通信できるハイブリッドクラウドで VRF ルート共有を設定するには、次の設定を実行します。このソリューション例では、VRF 3 と VRF 4 は相互に通信できません。

例：

```
vrf definition vrf3
rd 3:3
address-family ipv4
Route-target export 100:3
Route-target import 100:4
route-target export 3:3 stitching
route-target import 1:1 stitching
route-target import 2:2 stitching
exit-address-family
!
!
vrf definition vrf4
rd 4:4
address-family ipv4
Route-target import 100:3
Route-target export 100:4
route-target export 4:4 stitching
route-target import 1:1 stitching
route-target import 2:2 stitching
exit-address-family
!
!
interface BDI100
no shutdown
vrf forwarding vrf3
ip address 10.1.1.1 255.255.255.224
!
interface GigabitEthernet4.2
encapsulation dot1Q 2
vrf forwarding vrf3
ip address 10.4.4.1 255.255.255.224
bridge-domain 100
member vni 10100
!
interface nve1
source-interface loopback0
host-reachability protocol bgp
member vni 10100 vrf vrf3
!
router bgp 100
bgp router-id 10.11.11.11
no bgp default ipv4-unicast
neighbor 192.168.22.22 remote-as 200
neighbor 198.162.22.22 update-source loopback0
neighbor 198.162.22.22 ebgp-multihop 255
```

```

address-family ipv4 vrf vrf3
redistribute connected
neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
advertise l2vpn evpn
exit-address-family
!
address-family l2vpn evpn
neighbor 198.162.22.22 activate
neighbor 198.162.22.22 send-community both
exit-address-family
end

```

## VRF ルート共有の確認

### 手順

#### ステップ1 show ip bgp l2vpn evpn summary.

VRF デフォルトアドレスファミリ (L2VPN EVPN) の BGP サマリー情報を指定します。

例 :

```

show ip bgp l2vpn evpn summary
BGP router identifier 10.11.11.11, local AS number 100
BGP table version is 8, main routing table version 8
7 network entries using 2408 bytes of memory
.....
BGP activity 14/0 prefixes, 16/0 paths, scan interval 60 secs
7 networks peaked at 17:34:38 Aug 14 2019 CST (00:00:26.895 ago)
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
198.162.22.22  4      200     6      5       4    0    0 00:01:23      4
Device#

```

#### ステップ2 show ip route vrf vrf3 bgp | in binding.

VRFに関連付けられたIPルーティングテーブル情報を表示します。出力にバインディングラベルが付いている場合は、設定が成功し、BGPがバインディングラベルをネクストホップとして使用していることを示しています。

例 :

```

+++ 17:35:05 Minuet(default) exec +++
show ip route vrf vrf3 bgp | in binding
B      10.2.1.0/24 [20/0] via binding label: 0x3000001, 00:00:26
B      10.2.2.0/24 [20/0] via binding label: 0x3000002, 00:00:26
B      192.168.1.0/24 [20/0] via binding label: 0x3000001, 00:00:26
B      192.168.2.0/24 [20/0] via binding label: 0x3000002, 00:00:26
Device#

```



## 第 22 章

# ブリッジ ドメイン インターフェイスの設定

Cisco C8000V ルータは、レイヤ 3 IP アドレスにレイヤ 2 イーサネットセグメントをパッケージングするためのブリッジ ドメイン インターフェイス (BDI) 機能をサポートします。

- [ブリッジ ドメイン インターフェイスの制約事項 \(211 ページ\)](#)
- [ブリッジ ドメイン インターフェイスに関する情報 \(212 ページ\)](#)
- [ブリッジドメイン仮想 IP インターフェイスの設定 \(222 ページ\)](#)
- [その他の参考資料 \(228 ページ\)](#)
- [ブリッジ ドメイン インターフェイスの機能情報 \(229 ページ\)](#)

## ブリッジ ドメイン インターフェイスの制約事項

ブリッジ ドメイン インターフェイスに関連する制約事項は次のとおりです。

- システムごとにサポートされるブリッジ ドメイン インターフェイスは 4096 のみです。
- ブリッジ ドメイン インターフェイスの場合、最大伝送単位 (MTU) サイズは 1500 および 9216 バイトの間で設定できます。
- ブリッジ ドメイン インターフェイスは次の機能のみをサポートします。
  - IPv4 マルチキャスト
  - QoS マーキングとポリシング。シェーピングとキューイングはサポートされません。
  - IPv4 VRF
  - IPv6 ユニキャスト転送
  - BGP、OSPF、EIGRP、RIP、IS-IS、STATIC などのダイナミックルーティング
  - IOS XE 3.8.0 以降の Hot Standby Router Protocol (HSRP)
  - IOS XE 3.8.0 以降の Virtual Router Redundancy Protocol (VRRP)
  - Flexible NetFlow



(注) Flexible NetFlow は、Cisco IOS XE 17.7.1a 以降のリリースでサポートされています。

- ブリッジドメインインターフェイスは次の機能をサポートしません。
  - PPP over Ethernet (PPPoE)
  - 双方向フォワーディング検出 (BFD) プロトコル
  - QoS
  - Network-Based Application Recognition (NBAR) または Advanced Video Coding (AVC)

## ブリッジドメインインターフェイスに関する情報

ブリッジドメインインターフェイスは、レイヤ2ブリッジ型ネットワークとレイヤ3のルーテッドネットワークトラフィック間のトラフィックの双方向フローを許可する論理インターフェイスです。ブリッジドメインインターフェイスは、ブリッジドメインと同じインデックスによって識別されます。各ブリッジドメインは、レイヤ2ブロードキャストドメインを表します。ブリッジドメインに関連付けることができるブリッジドメインインターフェイスは、1つだけです。

ブリッジドメインインターフェイスは次の機能をサポートします。

- IP 終了
- レイヤ3 VPN の終了
- アドレス解決プロトコル (ARP) 、G-ARP および P-ARP の処理
- MAC アドレスの割り当て

ブリッジドメインインターフェイスを設定する前に、次の概念を理解しておく必要があります：

- イーサネット仮想回線の概要
- ブリッジドメインインターフェイスのカプセル化
- MAC アドレスの割り当て
- IP プロトコルのサポート
- IP 転送のサポート
- パケット転送
- ブリッジドメインインターフェイスの統計情報

## イーサネット仮想回線の概要

イーサネット仮想回線（EVC）は、プロバイダーが提供しているレイヤ2サービスの単一インスタンスのエンドツーエンド表現です。さまざまなパラメータが統合されて、サービスが提供されます。シスコ EVC フレームワークでは、ブリッジドメインは、サービスインスタンスと呼ばれているレイヤ2インターフェイス（1つまたは複数）で構成されます。サービスインスタンスは、あるルータ上のあるポート上で EVC をインスタンス化したものです。サービスインスタンスは、設定に基づいてブリッジドメインに関連付けられます。

着信フレームは、次の基準に基づいてサービスインスタンスとして分類できます。

- シングル 802.1Q VLAN タグ、優先度タグ付き、または 802.1ad VLAN タグ
- 両 QinQ（内部および外部）VLAN タグ、または 802.1ad S-VLAN と C-VLAN タグの両方
- 外部 802.1p CoS ビット、内部 802.1p CoS ビット、またはその両方
- ペイロードイーサネットタイプ（5つの選択肢をサポート：IPv4、IPv6、PPPoE-all、PPPoE-discovery、PPPoE-session）

サービスインスタンスは、他のマッピング基準もサポートします。

- [Untagged]：802.1Q または 802.1ad ヘッダがないすべてのフレームにマッピングします。
- [Default]：すべてのフレームにマッピングします。

EVC アーキテクチャの詳細については、『[Carrier Ethernet Configuration Guide](#)』の「Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router」のセクションを参照してください。

## ブリッジドメインインターフェイスのカプセル化

セキュリティグループの分類には、送信先グループや宛先グループが含まれます。これは送信元の SGT と DGT で指定します。SGT ベースの PBR 機能では、SGT/DGT ベースの packets 分類のために PBR ルートマップの `match` 句を使用できます。SGT ベースの PBR 機能では設定できるタグの数に制限はありませんが、プラットフォームで使用できるメモリに基づいてタグを設定することをお勧めします。

EVC はブリッジドメインに存在する各イーサネットフローポイント（EFP）で様々なカプセル化を使用する機能を提供します。パケットは異なるカプセル化を設定した1つまたは複数の EFP から出力されている可能性があるため、BDI 出力ポイントは出力パケットのカプセル化を認識しないことがあります。

ブリッジドメインでは、すべての EFP で異なるカプセル化がある場合、BDI のタグ付けを解除する必要があります（802.1Q タグなしを使用）。EFP でブリッジドメインのすべてのトラフィック（ポップまたはプッシュ）をカプセル化します。ブリッジドメインのトラフィックのカプセル化を可能にするためには、各 EFP で `rewrite` を設定します。

ブリッジドメインでは、すべての EFP で同じカプセル化がある場合は、`encapsulation` コマンドを使用して BDI 上にカプセル化を設定します。BDI でのカプセル化をイネーブルにすると、タグのプッシングまたはポップングが有効になり、それにより EFP で `rewrite` コマンドを設定す

る必要がなくなります。BDI でのカプセル化の設定の詳細については、「ブリッジドメインインターフェイスの設定方法」を参照してください。

## MAC アドレスの割り当て

Cisco C8000V ルータ上のすべてのブリッジドメインインターフェイスは、同じ MAC アドレスを共有します。最初のブリッジドメインインターフェイスに MAC アドレスが割り当てられます。その後、同じ MAC アドレスが、そのブリッジドメインで作成されたすべてのブリッジドメインインターフェイスに割り当てられます。



(注) **mac-address** コマンドを使用して、ブリッジドメインインターフェイスにスタティック MAC アドレスを設定できます。

## IP プロトコルのサポート

ブリッジドメインインターフェイスは、Cisco C8000V ルータを有効にし、次の IP 関連プロトコルのレイヤ 2 ブリッジドメインのレイヤ 3 のエンドポイントとして機能します。

- ARP
- DHCP
- HTTP
- ICMP
- NTP
- RARP
- SNMP
- TCP
- Telnet
- TFTP
- UDP

## IP 転送のサポート

ブリッジドメインインターフェイスは次の IP 転送機能をサポートします。

- IPv4 の入力および出力アクセス コントロール リスト (ACL)
- IPv4 の入力および出力 QoS ポリシー。ブリッジドメインインターフェイスの入力および出力サービス ポリシーでサポートされる動作は次のとおりです。
  - 分類

- マーキング
- ポリシング
- IPv4 L3 VRF

## パケット転送

ブリッジドメインインターフェイスはレイヤ2およびレイヤ3ネットワークインフラ間のブリッジングおよび転送サービスを提供します。

### レイヤ2から3

レイヤ2ネットワークからレイヤ3ネットワークへのパケットフローの間に、着信パケットの宛先MACアドレスがブリッジドメインインターフェイスのMACアドレスと一致するか、宛先MACアドレスがマルチキャストアドレスの場合、パケットまたはパケットのコピーがブリッジドメインインターフェイスに転送されます。



(注) MACアドレスラーニングは、ブリッジドメイン上のインターフェイスで実行できません。

### レイヤ3からレイヤ2

パケットがルータの物理インターフェイスのレイヤ3に到達すると、ルート検索アクションが実行されます。ルート検索がブリッジドメインインターフェイスに向かうと、ブリッジドメインインターフェイスはレイヤ2カプセル化を追加し、対応するブリッジドメインにフレームを転送します。バイトカウンタが更新されます。

ブリッジドメインインターフェイスが属するブリッジドメインでのレイヤ2検索中に、ブリッジドメインは、宛先MACアドレスに基づいて適切なサービスインスタンスにパケットを転送します。

## ブリッジドメインとブリッジドメインインターフェイスのステートをリンクする

ブリッジドメインインターフェイスはレイヤ3のルーティング可能なIOSインターフェイスおよびブリッジドメインのポートとして機能します。ブリッジドメインインターフェイスとブリッジドメインのいずれも、個々の管理状態で動作します。

ブリッジドメインインターフェイスをシャットダウンすると、レイヤ3データサービスは停止しますが、関連するブリッジドメインの状態は書き換えられず、影響を受けません。

ブリッジドメインをシャットダウンすると、サービスインスタンスやブリッジドメインインターフェイスを含むすべての関連メンバへのレイヤ2転送が停止します。関連するサービスインスタンスはブリッジドメインの動作状態に影響を与えます。ブリッジドメインインターフェイスは、関連するサービスインスタンスの1つが起動しない限り、動作することはできません。



(注) ブリッジドメインインターフェイスは内部インターフェイスであるため、ブリッジドメインインターフェイスの動作状態はブリッジドメインの動作状態には影響しません。

## BDIの初期状態

BDI最初の管理ステートは、BDIの作成方法によって異なります。スタートアップコンフィギュレーションで起動時にBDIを作成すると、BDIのデフォルトの管理状態がアップになります。スタートアップコンフィギュレーションに `shutdown` コマンドが含まれていない限り、この状態のままになります。この動作は、他のすべてのインターフェイスと一致します。コマンドプロンプトでBDIを動的に作成すると、デフォルトの管理状態はダウンになります。

## BDIのリンク状態

BDIは、管理上のダウン状態、動作上のダウン状態、アップ状態の3種類のステートからなるリンク状態を維持します。BDIのリンク状態は、対応するユーザーによって設定されたBDI管理状態セットおよびインターフェイスステートの下位レベルの障害表示の状態の2つの独立する入力から得られます。BDIのリンク状態は、2つの入力の状態に基づいて定義されます。

障害表示の状態	BDI 管理	
{start emdash} {end emdash}	<b>Shutdown</b>	<b>No Shutdown</b>
<b>No faults asserted</b>	Admin-down	Up
<b>At least one fault asserted</b>	Admin-down	Operationally-Down

## ブリッジドメインインターフェイスの統計情報

ブリッジドメインインターフェイスなどの仮想インターフェイスの場合は、プロトコルカウンタはQFPから定期的に検索されます。

パケットがレイヤ2ブリッジドメインネットワークからドメインのインターフェイスを介してレイヤ3のルーティングネットワークに流れると、パケットはブリッジドメインインターフェイスの入力パケットおよびバイトとして処理されます。パケットがレイヤ3インターフェイスに到達し、ブリッジドメインインターフェイスを介してレイヤ2ブリッジドメインに転送されると、パケットは出力パケットおよびバイトとして処理され、カウンタが適宜更新されます。

BDIはすべてのCisco IOSインターフェイスで、ケースとしてレイヤ3パケットカウンタの標準セットを維持します。レイヤ3のパケットカウンタを表示するには、`show interface` コマンドを使用します。

カウンタの表記法は、レイヤ3クラウドに関連しています。たとえば、`input` はレイヤ2 BD からレイヤ3クラウドに入るトラフィックを示し、`output` はレイヤ3クラウドからレイヤ2 BD に向かうトラフィックを示します。

BDI ステータスの統計情報を表示するには、**show interfaces accounting** コマンドを使用します。送受信されるパケットおよびバイト全体のカウンタを表示するには、**show interface <if-name>** コマンドを使用します。

## ブリッジドメインインターフェイスの作成または削除

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義する場合は、名前を付け、どのように IP アドレスに割り当てられるかを指定します。システムにブリッジドメインを追加する前にブリッジドメインインターフェイスを作成できます。この新しいブリッジドメインインターフェイスは、関連するブリッジドメインの設定後にアクティブになります。



- (注) ブリッジドメインインターフェイスが作成されると、ブリッジドメインが自動的に作成されます。

ブリッジドメインインターフェイスとブリッジドメインを作成すると、システムは、ブリッジドメインとブリッジドメインインターフェイスのペアをマッピングするために必要なアソシエーションを保持します。

ブリッジドメインとブリッジドメインインターフェイスのマッピングはシステムに保持されます。ブリッジドメインインターフェイスは、アソシエーションを示すために関連するブリッジドメインのインデックスを使用されます。

## ブリッジドメインインターフェイスのスケラビリティ

次の表に、Cisco C8000V ルータのフォワーディングプロセッサ (FP) のタイプに基づいた、ブリッジドメインインターフェイスのスケラビリティの数値を示します。

表 22: Cisco C8000V ルータのフォワーディングプロセッサのタイプに基づいた、ブリッジドメインインターフェイスのスケラビリティの数値

説明	0
ルータごとのブリッジドメインインターフェイスの最大数	

## ブリッジドメイン仮想 IP インターフェイス

仮想 IP インターフェイス (VIF) 機能は、複数の BDI インターフェイスを BD インスタンスに関連付けるのに役立ちます。BD-VIF インターフェイスは、IOS 論理 IP インターフェイスの既存のすべての L3 機能を継承します。



- (注) すべての BD-VIF インターフェイスに一意的な MAC アドレスを設定する必要があり、異なる VRF に属している必要があります。

仮想 IP インターフェイス (VIF) 機能には、次の制限事項があります。

- BD-VIF インターフェイスは IP マルチキャストをサポートしていません。
- 自動生成された MAC アドレスを持つ BD-VIF インターフェイスの数は、プラットフォームによって異なります。
- BD-VIF インターフェイスは MPLS をサポートしていません。
- ブリッジドメインごとの BD-VIF インターフェイスの最大数と、システムごとの BD-VIF インターフェイスの総数は、プラットフォームのタイプによって異なります。

サポートされる BD-VIF の最大数は、プラットフォームによって異なります。

- ASR 1000 は、ブリッジドメインに対して最大 100 の BD-VIF をサポートします。
- CSR 1000v は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。
- ISR 4000 は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。

Cisco IOS XE 17.7.1a リリースから、BD-VIF は [Flexible Netflow \(FnF\)](#) をサポートします。

## ブリッジドメインインターフェイスの設定方法

ブリッジドメインインターフェイスを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface BDI** {*interface number*}
4. **encapsulation encapsulation dot1q** <*first-tag*> [*second-dot1q* <*second-tag*>]
5. 次のいずれかを実行します。
6. **match security-group destination tag** *sgt-number*
7. **mac address** {*mac-address*}
8. **no shut**
9. **shut**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Router> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 : <pre>Router# configure terminal</pre>	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	<b>interface BDI {interface number}</b> 例 : <pre>Router(config-if)# interface BDI3</pre>	ブリッジドメインインターフェイスを指定します。
ステップ 4	<b>encapsulation encapsulation dot1q &lt;first-tag&gt; [second-dot1q &lt;second-tag&gt;]</b> 例 : <pre>Router(config-if)# encapsulation dot1q 1 second-dot1q 2</pre>	カプセル化タイプを定義します。 例では、カプセル化タイプとして dot1q を定義しています。
ステップ 5	次のいずれかを実行します。 例 : <b>ip address ip-address mask</b> 例 : 例 : <b>ipv6 address {X:X:X:X::X link-local   X:X:X:X::X/prefix [anycast   eui-64]   autoconfig [default]}</b> 例 : <pre>Router(config-if)# ip address 10.2.2.1 255.255.255.0</pre> 例 : 例 : <pre>Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64</pre>	ブリッジドメインインターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 6	<b>match security-group destination tag sgt-number</b> 例 : <pre>Router(config-route-map)# match security-group destination tag 150</pre>	security-group destination security tag の値を設定します。

## 例

	コマンドまたはアクション	目的
ステップ 7	<b>mac address {mac-address}</b> 例： Router(config-if)# mac-address 1.1.3	ブリッジドメインインターフェイスのMACアドレスを指定します。
ステップ 8	<b>no shut</b> 例： Router(config-if)# no shut	ブリッジドメインインターフェイスを有効にします。
ステップ 9	<b>shut</b> 例： Router(config-if)# shut	ブリッジドメインインターフェイスを無効にします。

## 例

次に、IP アドレス 10.2.2.1 255.255.255.0 でブリッジドメインインターフェイスを設定する例を示します。

```
Router# configure terminal
Router(config)# interface BDI3
Router(config-if)# encapsulation dot1Q 1 second-dot1q 2
Router(config-if)# ip address 10.2.2.1 255.255.255.0
Router(config-if)# mac-address 1.1.3
Router(config-if)# no shut
Router(config-if)# exit
```

## ブリッジドメインインターフェイス設定の表示と確認

## 手順の概要

1. **enable**
2. **show interfaces bdi**
3. **show platform software interface fp active name**
4. **show platform hardware qfp active interface if-name**
5. **debug platform hardware qfp feature**
6. **platform trace runtime process forwarding-manager module**
7. **platform trace boottime process forwarding-manager module interfaces**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Router> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>show interfaces bdi</b> 例：  Router# <b>show interfaces BDI3</b>	対応する BDI の設定の概要を表示します。
ステップ 3	<b>show platform software interface fp active name</b> 例：  Router# <b>show platform software interface fp active name BDI4</b>	フォーワーディングプロセッサのブリッジドメインインターフェイス設定を表示します。
ステップ 4	<b>show platform hardware qfp active interface if-name</b> 例：  Router# <b>show platform hardware qfp active interface if-name BDI4</b>	データパスのブリッジドメインインターフェイス設定を表示します。
ステップ 5	<b>debug platform hardware qfp feature</b> 例：  Router# <b>debug platform hardware qfp active feature l2bd client all</b>	選択した CPP L2BD Client のデバッグがオンになります。
ステップ 6	<b>platform trace runtime process forwarding-manager module</b> 例：  Router(config)# <b>platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info</b>	Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。
ステップ 7	<b>platform trace boottime process forwarding-manager module interfaces</b> 例：  Router(config)# <b>platform trace boottime slot</b>	ブートアップ中の、Route Processor Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。

コマンドまたはアクション	目的
<b>R0 bay 1 process forwarding-manager forwarding-manager level max</b>	

### 次のタスク

各コマンドに使用できるコマンドおよびオプションの詳細については、『[Cisco IOS Configuration Fundamentals Command Reference Guide](#)』を参照してください。

## ブリッジドメイン仮想 IP インターフェイスの設定

```
enable
configure terminal
[no] interface BD-VIF interface-number
  [ [no] vrf forwarding vrf-name]
  [ [no] mac address mac-address]
  [ [no] ip address ip-address mask]
  [ [no] ipv6 address {X:X:X:X::X link-local | X:X:X:X::X/prefix [anycast | eui-64] |
  autoconfig [default]}]
```

```
exit
```

BD-VIF インターフェイスを削除するには、このコマンドの 'no' 形式を使用します。

## VIF インターフェイスのブリッジドメインへの関連付け

```
enable
configure terminal
bridge-domain bridge-domain number
[no] member BD-VIF interface-number
exit
```

VIF インターフェイスの関連付けを解除するには、このコマンドの「no」形式を使用します。

## ブリッジドメイン仮想 IP インターフェイスの確認

インターフェイスおよび IP インターフェイスの既存のすべての show コマンドは、BD-VIF インターフェイスに使用できます。

```
show interface bd-vif bd-vif-id
show ip interface bd-vif bd-vif-id
show bd-vif interfaces in fman-fp
show pla sof inter fp ac brief | i BD_VIF
```

## ブリッジドメイン仮想 IP インターフェイスの設定例

Detail sample:

```

interface Port-channell
mtu 9000
no ip address
!Ethernet service endpoint one per neutron network
service instance 1756 ethernet
  description 4e8e5957-649f-477b-9e5b-f1f75b21c03c
  encapsulation dot1q 1756
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1756
!
interface BD-VIF5001
no shutdown
vrf forwarding vrf5001
ip address 10.0.0.1 255.255.255.0
interface BD-VIF5002
no shutdown
vrf forwarding vrf5002
ip address 10.0.0.2 255.255.255.0

bridge-domain 1756
member Port-channell service-instance 1756
member bd-vif5001
member bd-vif5002

```

## ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **{ip | ipv6}flow monitor *monitor-name* [sampler *sampler-name*] {input | output}**
5. **exit**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : Device# 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。

例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow

	コマンドまたはアクション	目的
ステップ 3	<b>interface</b> <i>type number</i> 例： Device (config)# interface BD-VIF 100	インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。BD-VIF 番号を入力します。
ステップ 4	<b>{ip   ipv6} flow monitor</b> <i>monitor-name</i> [ <b>sampler</b> <i>sampler-name</i> ] <b>{input   output}</b> 例： Device(config-if)# ip flow monitor FLOW-MONITOR-1 input	ルータがインターフェイスで送受信する IP トラフィックの Flexible NetFlow フローモニターを有効にします。
ステップ 5	<b>exit</b> 例： Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## 例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow

次に、フローモニターの QFP 情報およびフロー方向を表示する **show platform hardware qfp active interface if-name** コマンドの出力例を示します。次の表に、CLI 出力のキーを示します。

設定	出力
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration: 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001:DB8::1/32
end
```

```
Device# show platform hardware qfp active interface if-name BD-VIF 2
General interface information
```

```

Interface Name: BD-VIF2
Interface state: VALID
Platform interface handle: 20
QFP interface handle: 17
Rx uidb: 262138
Tx uidb: 262127
Channel: 0
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
  Egress: BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
ipv6_input enabled.
ipv6_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
66 PUNT INJECT DB
70 cpp_l2bd_svr
43 icmp_svr
45 ipfrag_svr
46 ipreass_svr
47 ipv6reass_svr
44 icmp6_svr
58 stile
Protocol 0 - ipv4_input
FIA handle - CP:0x55a7f59df038 DP:0x3fff1000
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_SRC_LOOKUP_ISSUE
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_SRC_LOOKUP_CONSUME
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_LOOKUP_PROCESS (M)
  IPV4_INPUT_FNF_FINAL
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x55a7f59df0d8 DP:0x3ffeff00
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_SRC_LOOKUP_ISSUE
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_SRC_LOOKUP_CONSUME
  IPV4_OUTPUT_STILE_LEGACY
  IPV4_OUTPUT_FRAG (M)
  IPV4_BDI_OUTPUT_FNF_FINAL.
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
Protocol 6 - ipv6_input
FIA handle - CP:0x55a7f59dee58 DP:0x3fff4300
  IPV6_INPUT_SANITY_CHECK (M)
  IPV6_INPUT_DST_LOOKUP_ISSUE (M)
  IPV6_INPUT_SRC_LOOKUP_ISSUE

```

## 例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow

```

IPV6_INPUT_ARL (M)
IPV6_INPUT_DST_LOOKUP_CONT (M)
IPV6_INPUT_SRC_LOOKUP_CONT
IPV6_INPUT_DST_LOOKUP_CONSUME (M)
IPV6_INPUT_SRC_LOOKUP_CONSUME
IPV6_INPUT_STILE_LEGACY
IPV6_INPUT_FNF_FIRST
IPV6_INPUT_FOR_US (M)
IPV6_INPUT_LOOKUP_PROCESS (M)
IPV6_INPUT_FNF_FINAL
IPV6_INPUT_LINK_LOCAL_CHECK (M)
IPV6_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 7 - ipv6_output
FIA handle - CP:0x55a7f59dee08 DP:0x3fff4b80
IPV6_VFR_REFRAG (M)
IPV6_OUTPUT_SRC_LOOKUP_ISSUE
IPV6_OUTPUT_SRC_LOOKUP_CONT
IPV6_OUTPUT_SRC_LOOKUP_CONSUME
IPV6_OUTPUT_L2_REWRITE (M)
IPV6_OUTPUT_STILE_LEGACY
IPV6_OUTPUT_FRAG (M)
IPV6_BDI_OUTPUT_FNF_FINAL
BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
LAYER2_BRIDGE
BDI_OUTPUT_GOTO_OUTPUT_FEATURE
IPV6_OUTPUT_DROP_POLICY (M)
DEF_IF_DROP_FIA (M)

```

□

次に、キャッシュ出力をレコード形式で表示する **show flow monitor** **[[name]** **[cache [format {csv | record | table}]]** **[statistics]** コマンドの出力例を示します。

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record
```

```

Cache type: Normal
Cache size: 1000
Current entries: 4
High Watermark: 4
Flows added: 101
Flows aged: 97
- Active timeout (1800 secs) 3
- Inactive timeout (15 secs) 94
- Event aged 0
- Watermark aged 0
- Emergency aged
IPV4 DESTINATION ADDRESS:
198.51.100.1 0
ipv4 source address: 10.10.11.1
trns source port: 25
trns destination port: 25
counter bytes: 72840
counter packets: 1821
IPV4 DESTINATION ADDRESS: 198.51.100.2
ipv4 source address: 10.10.10.2
trns source port: 20
trns destination port: 20
counter bytes: 3913860
counter packets: 7326
IPV4 DESTINATION ADDRESS: 198.51.100.200
ipv4 source address: 192.168.67.6
trns source port: 0
trns destination port: 3073
counter bytes: 51072
counter packets: 1824

```

```
Device# show flow monitor name FLOW-MONITOR-2 cache format record
```

```
Cache type: Normal
Cache size: 1000
Current entries: 2
High Watermark: 3
Flows added: 95
Flows aged: 93
- Active timeout (1800 secs) 0
- Inactive timeout (15 secs) 93
- Event aged 0
- Watermark aged 0
- Emergency aged 0
IPV6 DESTINATION ADDRESS: 2001:DB8:0:ABCD::1
ipv6 source address: 2001:DB8:0:ABCD::2
trns source port: 33572
trns destination port: 23
counter bytes: 19140
counter packets: 349
IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address: 2001:DB8::A8AA:BBFF:FEBB

trns source port: 521
trns destination port: 521
counter bytes: 92
counter packets: 1
```

次に、インターフェイスのフローステータスを表示する **show flow interface** コマンドの出力例を示します。

```
Device# show flow interface BD-VIF2001
```

```
Interface GigabitEthernet0/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Input
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction: Input traffic(ipv6): on
```

```
Device# show flow interface BD-VIF2002
```

```
Interface GigabitEthernet1/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Output
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction: Input traffic(ipv6): on
```

次に、Flexible NetFlow 設定のフロー 모니터の QFP 情報およびフロー方向を表示する **show platform hardware qfp active interface if-name | in FNF** コマンドの出力例を示します。次の表に、CLI 出力のキーを示します。

設定	出力
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL

設定	出力
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...
```

```
Current configuration : 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001::8/64
end
```

```
Device# show platform hardware qfp active interface if-name BD-VIF 2 | in FNF
IPV4_INPUT_FNF_FIRST
IPV4_INPUT_FNF_FINAL
IPV4_BDI_OUTPUT_FNF_FINAL.
IPV6_INPUT_FNF_FIRST
IPV6_INPUT_FNF_FINAL
IPV6_BDI_OUTPUT_FNF_FINAL
```

**clear flow monitor name** *monitor-name* [**cache** [**force-export**] | **force-export** | **statistics**] コマンドを使用すると、Flexible NetFlow フローモニター、フローモニターキャッシュ、またはフローモニター統計情報がクリアされ、フローモニターキャッシュ内のデータを強制的にエクスポートできます。

Flexible NetFlow の設定の詳細については、『[Flexible NetFlow Configuration Guide, Cisco IOS XE 17](#)』を参照してください。

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでのイーサネット仮想接続の設定	<a href="#">『Carrier Ethernet Configuration Guide』</a>
EVN Quality of Service	<a href="http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_evn_xe.html">http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_evn_xe.html</a>

## MIB

MIB	MIB のリンク
なし	<p>選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	<p><a href="https://www.cisco.com/c/en_in/support/index.html">https://www.cisco.com/c/en_in/support/index.html</a></p>

## ブリッジドメインインターフェイスの機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェアイメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。



- (注) 次の表は、特定のソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 23: ブリッジドメインインターフェイスの機能情報

機能名	リリース	機能情報
ブリッジドメインインターフェイスの設定	Cisco IOS XE Cupertino 17.7.1a	この機能は、Cisco C8000V ルータで導入されました。

機能名	リリース	機能情報
ブリッジドメイン仮想 IP インターフェイス	Cisco IOS XE Cupertino 17.7.1a	この機能は、Cisco C8000V ルータで導入されました。  ブリッジドメイン仮想 IP インターフェイス (VIF) は、複数のブリッジドメイン インターフェイス (BDI) を単一の BD インスタンスに接続し、L2 ネットワーク内の各 IP サブネットを単一の VRF に関連付けることができるようになりました。
ブリッジドメイン仮想 IP インターフェイス (BD-VIF) 上の Flexible NetFlow (FNF)	Cisco IOS XE Cupertino 17.7.1a	この機能は、Cisco C8000V ルータで導入されました。次のコマンドが導入されました。  <b>{ip   ipv6} flow monitor <i>monitor-name</i> [sampler <i>sampler-name</i>] {input   output}</b>



## 第 23 章

# MTP ソフトウェアサポートの設定

メディアターミネーションポイント (MTP) ソフトウェアデバイスは、Cisco Unified Communications Manager (CUCM) の大規模な導入に不可欠なコンポーネントです。これらの展開では、ソフトウェア MTP は、CUCM が Session Initiation Protocol (SIP) または H.323 エンドポイントを介してルーティングされたコールを Skinny Client Control Protocol (SCCP) コマンドでリレーできるようにすることで、2つの接続間のメディアストリームをブリッジするようにします。SCCP コマンドにより、CUCM はコールシグナリング用の MTP を確立できます。

Cisco IOS XE 17.8.1 以降では、Cisco Catalyst 8000V デバイスでソフトウェア MTP のサポートを設定できます。Cisco Catalyst 8000V デバイスで音声機能を使用する場合は、ソフトウェア MTP を活用して、H.323 エンドポイントまたは H.323 ゲートウェイを介してルーティングされるコールパークやコール転送などの補足サービスを有効にして使用できます。

- [利点 \(231 ページ\)](#)
- [ソフトウェア MTP のサポートを設定するための前提条件 \(231 ページ\)](#)
- [SRTP-DTMF インターワーキング \(232 ページ\)](#)
- [ソフトウェア MTP のサポートの設定 \(232 ページ\)](#)
- [ソフトウェア MTP サポートの確認 \(237 ページ\)](#)

## 利点

Cisco Catalyst 8000V でソフトウェア MTP を設定すると、次のことが可能になります。

- Cisco Catalyst 8000V インスタンスを信頼できるリレーポイントとして Unified CM に登録します。
- エンドポイントの 1 つが DTMF シグナリングをサポートしていない場合は、SWMTP サポートを活用します。

## ソフトウェア MTP のサポートを設定するための前提条件

- 着信コールレグと発信コールレグでコーデックとパケット化を設定します。

## SRTP-DTMF インターワーキング

Cisco IOS XE 17.10.1a 以降、Secure Real-time Transport Protocol (SRTP) デュアルトーン多重周波数 (DTMF) インターワーキングは、パススルーモードのソフトウェア MTP でサポートされています。SMTP は非セキュアコールの DTMF インターワーキングをサポートします。また、この機能はさらにセキュアコールの SRTP DTMF インターワーキングをサポートします。

この機能の CUCM サポートは、今後のリリースで実装される予定です。

### SRTP-DTMF インターワーキングの制約事項

- SRTP-DTMF インターワーキング機能は、コーデックパススルー形式のみをサポートします。
- SRTP-DTMF インターワーキング機能は、同じ宛先 IP とポートを持つ複数の同時同期ソース (SSRC) をサポートしていません。
- SRTP-DTMF インターワーキングをサポートするコールは、非セキュア DTMF インターワーキングでサポートされるコールと比較すると、パフォーマンスにわずかな影響を与える可能性があります。

### サポートされる SRTP-DTMF インターワーキングのプラットフォーム

Cisco IOS XE 17.10.1a 以降、次のプラットフォームは SMTP との SRTP DTMF インターワーキングをサポートしています。

- Cisco 4461 サービス統合型ルータ (ISR)
- Cisco Catalyst 8200 Edge シリーズ プラットフォーム
- Cisco Catalyst 8300 Edge シリーズ プラットフォーム
- Cisco 8300 シリーズ セキュアルータ
- Cisco Catalyst 8000V Edge ソフトウェア

## ソフトウェア MTP のサポートの設定

ソフトウェア MTP のサポートを有効にして設定するには、次の手順を実行します。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **sccp local interface-type interface-number [port port-number]**

4. **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number*
5. **sccp**
6. **sccp ccm group** *group-number*
7. **associate ccm** *identifier-number* **priority** *number*
8. **associate profile** *profile-identifier* **register** *device-name*
9. **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]
10. **trustpoint** *trustpoint-label*
11. **codec** *codec*
12. **maximum sessions** {**hardware** | **software**} *number*
13. **associate application** **sccp**
14. **no shutdown**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Router> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 :  Router# 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	<b>sccp local</b> <i>interface-type interface-number</i> [ <b>port</b> <i>port-number</i> ] 例 :  Router(config)# sccp local gigabitethernet0/0/0	Cisco UCM に登録するために SCCP アプリケーション (トランスコーディングと会議) が使用する、ローカルインターフェイスを選択します。  <ul style="list-style-type: none"> <li>• <b>interface type</b> : インターフェイスアドレスまたは仮想インターフェイスアドレス (イーサネットなど)。</li> <li>• <b>interface number</b> : Unified CM に登録するために SCCP アプリケーションが使用するインターフェイス番号。</li> <li>• (任意) <b>port port-number</b> : 選択したインターフェイスで使用するポート番号。適用可能な範囲は 1025 ~ 65535 で、デフォルトは 2000 です。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<p><b>sccp ccm</b> {<i>ipv4-address</i>   <i>ipv6-address</i>   <i>dns</i>} <b>identifier</b> <i>identifier-number</i> [<b>port</b> <i>port-number</i>] <b>version</b> <i>version-number</i></p> <p>例 :</p> <pre>Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+</pre>	<p>使用可能なサーバーのリストに Unified CM サーバーを追加し、次のパラメータを設定します。</p> <ul style="list-style-type: none"> <li>• <i>ipv4-address</i> : Cisco UCM サーバーの IP バージョン 4 アドレス。</li> <li>• <i>ipv6-address</i> : Cisco UCM サーバーの IP バージョン 6 アドレス。</li> <li>• <i>dns</i> : DNS 名。</li> <li>• <b>identifier</b> : Unified CM サーバーを識別する番号。適用可能な範囲は 1 ~ 65535 です。</li> <li>• <b>port</b> <i>port-number</i> (任意) : TCP ポート番号。適用可能な範囲は 1025 ~ 65535 で、デフォルトは 2000 です。</li> <li>• <b>version</b> <i>version-number</i> : Unified CM のバージョン。有効なバージョンは、3.0、3.1、3.2、3.3、4.0、4.1、5.0.1、6.0、および 7.0 以上です。</li> </ul>
ステップ 5	<p><b>sccp</b></p> <p>例 :</p> <pre>Router(config)# sccp</pre>	<p>SCCP および関連アプリケーション (トランスコーディングと会議) を有効にします。</p>
ステップ 6	<p><b>sccp ccm group</b> <i>group-number</i></p> <p>例 :</p> <pre>Router(config)# sccp ccm group 10</pre>	<p>Unified CM グループを作成し、SCCP Unified CM コンフィギュレーションモードを開始します。</p> <ul style="list-style-type: none"> <li>• <i>group-number</i> : Cisco Unified CM グループを識別します。適用可能な範囲は 1 ~ 50 です。</li> </ul>
ステップ 7	<p><b>associate ccm</b> <i>identifier-number</i> <b>priority</b> <i>number</i></p> <p>例 :</p> <pre>Router(config-sccp-ccm)# associate ccm 10 priority 3</pre>	<p>Unified CM をグループに関連付けて、グループ内の優先順位を設定します。</p> <ul style="list-style-type: none"> <li>• <i>identifier-number</i> : Unified CM 識別子。適用可能な範囲は 1 ~ 65535 です。</li> <li>• <b>priority</b> <i>number</i> : Unified CM グループ内の Unified CM の優先順位。適用可能な範囲は 1 ~ 4 です。最も高い優先順位は 1 です。</li> </ul>
ステップ 8	<p><b>associate profile</b> <i>profile-identifier</i> <b>register</b> <i>device-name</i></p> <p>例 :</p>	<p>デジタルシグナルプロセッサ (DSP) ファームプロファイルを Unified CM グループに関連付けます。</p> <ul style="list-style-type: none"> <li>• <i>profile-identifier</i> : DSP ファームプロファイル。適用可能な範囲は 1 ~ 65535 です。</li> </ul>

	コマンドまたはアクション	目的
	<pre>Router(config-sccp-ccm)# associate profile 1 register MTP0011</pre>	<ul style="list-style-type: none"> <li>• <b>register</b> <i>device-name</i> : Unified CM のデバイス名。デバイス名は最大 15 文字まで入力できます。</li> </ul>
ステップ 9	<p><b>dspfarm profile</b> <i>profile-identifier</i> {<b>conference</b>   <b>mtp</b>   <b>transcode</b>} [<b>security</b>]</p> <p>例 :</p> <pre>Router(config-sccp-ccm)# dspfarm profile 1 mtp</pre>	<p>DSP ファーム プロファイル コンフィギュレーション モードを開始し、DSP ファームサービスのプロファイルを定義します。</p> <ul style="list-style-type: none"> <li>• <b>profile-identifier</b> : プロファイルを一意に識別する番号。適用可能な範囲は 1 ~ 65535 で、デフォルトはありません。</li> <li>• <b>conference</b> : 会議用のプロファイルを有効にします。</li> <li>• <b>mtp</b> : MTP用のプロファイルを有効にします。</li> <li>• <b>transcode</b> : トランスコーディング用のプロファイルを有効にします。</li> <li>• <b>security</b> (任意) : セキュア DSP ファームサービス用のプロファイルを有効にします。設定例の詳細については、<a href="#">ソフトウェア MTP サポートの設定例 (236 ページ)</a> の項を参照してください。</li> </ul>
ステップ 10	<p><b>trustpoint</b> <i>trustpoint-label</i></p> <p>例 :</p> <pre>Router(config-dspfarm-profile)# trustpoint dspfarm</pre>	<p>(任意) トラストポイントを DSP ファーム プロファイルに関連付けます。</p>
ステップ 11	<p><b>codec</b> <i>codec</i></p> <p>例 :</p> <pre>Router(config-dspfarm-profile)# codec g711ulaw</pre>	<p>DSP ファーム プロファイルでサポートされるコーデックを指定します。</p> <ul style="list-style-type: none"> <li>• <b>codec-type</b> : 優先されるコーデックを指定します。サポートされるコーデックのリストを表示するには、?を入力します。</li> </ul> <p>サポートされるコーデックごとに、この手順を繰り返します。</p>
ステップ 12	<p><b>maximum sessions</b> {<b>hardware</b>   <b>software</b>} <i>number</i></p> <p>例 :</p> <pre>Router(config-dspfarm-profile)# maximum sessions software 10</pre>	<p>このプロファイルでサポートされる最大セッション数を指定します。</p> <ul style="list-style-type: none"> <li>• <b>hardware</b> : MTP ハードウェアリソースがサポートするセッションの数。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>software</b> : MTP ソフトウェアリソースがサポートするセッションの数。</li> <li>• <b>number</b> : プロファイルでサポートされるセッションの数。適用可能な範囲は 0 ~ x で、デフォルトは 0 です。x の値は、リソースプロバイダーで使用可能なリソースの数に応じて、実行時に決定されます。</li> </ul>
ステップ 13	<b>associate application sccp</b> 例 : <pre>Router(config-dspfarm-profile)# associate application sccp</pre>	SCCP を DSP ファーム プロファイルに関連付けます。
ステップ 14	<b>no shutdown</b> 例 : <pre>Router(config-dspfarm-profile)# no shutdown</pre>	インターフェイスのステータスを UP 状態に変更します。

## ソフトウェア MTP サポートの設定例

次の出力は、Cisco Catalyst 8000V デバイスでのソフトウェア MTP サポート設定の例です。

```
sccp local GigabitEthernet1
sccp ccm 9.35.46.100 identifier 1 priority 1 version 7.0
!
sccp ccm group 1
  bind interface GigabitEthernet1
  associate ccm 1 priority 1
  associate profile 10 register SWMTP1
  associate profile 1 register c8kvsmall-mtp1
  associate profile 2 register c8kv-sec-swmtpl
!
!
!
dspfarm profile 1 mtp
  codec g711ulaw
  maximum sessions software 20000
  associate application SCCP
```

次に、セキュアな dspfarm プロファイルを使用した SRTP-DTMF インターワーキング機能の設定例を示します。

```
sccp local GigabitEthernet0/0/0
sccp ccm 172.18.151.125 identifier 1 version 7.0
sccp
!
sccp ccm group 1
  bind interface GigabitEthernet0/0/0
  associate ccm 1 priority 1
  associate profile 1 register Router
!
```

```

dspfarm profile 1 mtp security
  trustpoint IOSCA
  codec g711ulaw
  codec pass-through
  tls-version v1.2
  maximum sessions software 5000
  associate application SCCP

```



- (注) dspfarm プロファイルがコーデックパススルーでプロビジョニングされていて、TLS およびセキュリティ関連の設定がない場合、SR-TP トラフィックは SMTP リソースを通過できます。SRTP-DTMF インターワーキングのサポートを必要とするトラフィックフローの場合は、SMTP dspfarm プロファイルには **security** キーワードと TLS およびコーデックパススルー設定を含める必要があります。この dspfarm リソースプロファイルは、SRTP-DTMF インターワーキングサポートに関係なく、SRTP トラフィックを通過させることもできます。

## ソフトウェア MTP サポートの確認

Cisco Catalyst 8000V デバイスで SWMTP のサポートが正常に設定されているかどうかを確認するには、**show sccp** コマンドを実行します。

```

Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.13.40.148, Port Number: 2000
                Priority: N/A, Version: 6.0, Identifier: 1
                Trustpoint: N/A

```

dspfarm プロファイルを確認するには、**show dspfarm profile** コマンドを実行します。

```

Router# show dspfarm profile 1
Dspfarm Profile Configuration

Profile ID = 1, Service = MTP, Resource ID = 1
Profile Service Mode : Non Secure
Profile Admin State : UP
Profile Operation State : RESOURCE ALLOCATED
Application : SCCP   Status : NOT ASSOCIATED
Resource Provider : NONE   Status : NONE
Total Number of Resources Configured : 20000
Total Number of Resources Available : 20000
Total Number of Resources Out of Service : 0
Total Number of Resources Active : 0
Hardware Configured Resources : 0
Hardware Resources Out of Service: 0
Software Configured Resources : 20000

Number of Hardware Resources Active : 0
Number of Software Resources Active : 0
Codec Configuration: num_of_codecs:1
Codec : g711ulaw, Maximum Packetization Period : 30

```

セキュア dspfarm プロファイルのステータスに関する情報を確認するには、**show dspfarm profile** コマンドを使用して、セキュアサービスモードが設定されていることを確認します。

```
Router# show dspfarm profile 2
Dspfarm Profile Configuration
  Profile ID = 2, Service = MTP, Resource ID = 2
  Profile Service Mode : secure
  Trustpoint : IOSCA
  TLS Version : v1.2
  TLS Cipher : AES128-SHA
  Profile Admin State : UP
  Profile Operation State : ACTIVE
  Application : SCCP Status : ASSOCIATED
  Resource Provider : NONE Status : NONE
  Total Number of Resources Configured : 8000
  Total Number of Resources Available : 8000
  Total Number of Resources Out of Service : 0
  Total Number of Resources Active : 0
  Hardware Configured Resources : 0
  Hardware Resources Out of Service: 0
  Software Configured Resources : 8000
  Number of Hardware Resources Active : 0
  Number of Software Resources Active : 0
  Codec Configuration: num_of_codecs:2
  Codec : pass-through, Maximum Packetization Period : 0
  Codec : g711ulaw, Maximum Packetization Period : 30
```

エンドポイント間のコール接続を確認するには、**show sccp connection details** コマンドを実行します。このコマンドは、接続が正常に確立されたことを示します。これは、設定出力の最後にあるアクティブな接続とコールレグによって示されます。

```
Router# show sccp connection details

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)

mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id   conn_id   call-id   codec   pkt-period   dtmf_method   type   bridge-info
mmbridge-info srtp_cryptosuite dscp
call_ref  spid      conn_id_tx
      (bid, cid)
16782237  16777254  110      g711u   20           rfc2833_pt thru   rtpspi (40,0)
      N/A      N/A
29751839  16777216  -        -        -           -           -
16782237  16777253  109      g711u   20           rfc2833_report rtpspi (40,0)
      N/A      N/A
29751839  16777216  -        -        -           -           -
Total number of active session(s) 1, connection(s) 2, and callegs 2
```

SMTP セキュア DTMF の場合、**show sccp connections** コマンドはコーデックタイプ (pass-th)、S タイプ (s-mtp)、および DTMF メソッド (rfc2833\_pt thru) に関する情報を表示します。

```
Router#sh sccp connections

sess_id   conn_id   stype   mode     codec   sport  rport  ripaddr conn_id_tx
dtmf_method
16791234  16777308  s-mtp   sendrecv pass_th  8006   24610  172.18.153.37
rfc2833_pt thru
16791234  16777306  s-mtp   sendrecv pass_th  8004   17576  172.18.154.2
rfc2833_report

Total number of active session(s) 1, and connection(s) 2
```

RTP 接続に関する情報を表示するには、**show rtpspi call** コマンドを使用します。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode LocalRTP RmtRTP LocalIP RemoteIP SRTP
1 22 19 Snd-Rcv 7242 17510 0x90D080F 0x90D0814 0
2 19 22 Snd-Rcv 18050 6900 0x90D080F 0x90D080F 0
```

SRTP DTMF インターワーキングがアクティブになっている場合、SRTP フィールドにはゼロ以外の値が表示されます。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode LocalRTP RmtRTP LocalIP RemoteIP SRTP
1 13 14 Snd-Rcv 8024 18270 0xA7A5355 0xAC129A02 1
2 14 13 Snd-Rcv 8026 24768 0xA7A5355 0xAC129925 1
```





## 第 24 章

# 無線対応ルーティング

無線対応ルーティング (RAR) は、無線がルーティングプロトコル OSPFv3 と情報を交換し、1 ホップルーティングネイバーのアップアランス、ディスアップアランス、およびリンク状態について信号で伝えるメカニズムです。

大規模なモバイルネットワークでは、ルーティングネイバーへの接続が距離と無線障害により中断されることがよくあります。該当する信号がルーティングプロトコルに到達しない場合、プロトコルタイマーを使用してネイバーのステータスが更新されます。ルーティングプロトコルには期間の長いタイマーがありますが、モバイルネットワークでは推奨されません。

RAR 機能は、Cisco ISR G2 および G3 シリーズ ルータ、Cisco ISR 4000 シリーズ ルータでサポートされています。

PPPoE 拡張は、Cisco 4000 シリーズ ISR でサポートされる RAR プロトコルです。集約による PPPoE 拡張のサポートは、Cisco IOS XE Fuji 16.7 リリースから導入されています。OSPFv3 および EIGRP は、サポートされているルーティングプロトコルです。

- [無線対応ルーティングの利点 \(241 ページ\)](#)
- [制約事項と制限 \(242 ページ\)](#)
- [パフォーマンス \(242 ページ\)](#)
- [システム コンポーネント \(242 ページ\)](#)
- [PPPoE 拡張セッションでの QoS プロビジョニング \(243 ページ\)](#)
- [例：バイパスモードでの RAR 機能の設定 \(244 ページ\)](#)
- [RAR セッションの詳細の確認 \(245 ページ\)](#)

## 無線対応ルーティングの利点

無線対応ルーティング機能には次のようなメリットがあります。

- 変更を即座に認識することで、ネットワーク コンバージェンスを高速化します。
- 障害の発生している、または減衰している無線リンクのルーティングを有効にします。
- ラインオブサイトパスと非ラインオブサイトパス間のルーティングを容易にします。

- 高速コンバージェンスと最適なルート選択が可能になるため、音声やビデオなど遅延の影響を受けやすいトラフィックが中断されません。
- 無線リソースと帯域幅の効率的な使用が可能になります。
- ルータで輻輳制御を実行することにより、無線リンクへの影響を軽減します。
- 無線電力の節減に基づくルート選択が可能になります。
- ルーティング機能と無線機能の分離を有効にします。
- RFC 5578、R2CP、および DLEP に準拠した無線へのシンプルなイーサネット接続を実現します。

## 制約事項と制限

無線対応ルーティング機能には次の制約事項と制限があります。

- DLEP および R2CP プロトコルは、Cisco 4000 シリーズ ISR ではサポートされていません。
- マルチキャストトラフィックは、集約モードではサポートされていません。
- 高可用性（HA）はサポートされていません。

## パフォーマンス

無線対応ルーティング機能は、無線または VMI インターフェイスごとに最大 10 のネイバーをサポートできます。合計 30 ～ 40 のネイバーに対応可能です。

## システム コンポーネント

無線対応ルーティング（RAR）機能は、PPPoE、仮想マルチポイント インターフェイス（VMI）、QoS、ルーティング プロトコル インターフェイス、RAR プロトコルなどのさまざまなコンポーネントで構成される MANET（モバイルアドホック ネットワーク）インフラストラクチャを使用して導入されます。

### Point-to-Point Protocol over Ethernet（PPPoE）

PPPoE は、クライアントとサーバーの間の明確に定義された通信メカニズムです。RAR の導入では、無線が PPPoE クライアントの役割を果たし、ルータが PPPoE サーバーの役割を果たします。その結果、明確に定義された予測可能な通信メカニズムを提供しながら、無線とルータを疎結合することが可能になります。

PPPoE はセッションまたは接続指向プロトコルであるため、外部無線から IOS ルータへのポイントツーポイント無線周波数（RF）リンクを拡張します。

## PPPoE 拡張

PPPoE 拡張は、ルータが無線と通信するときに使用されます。PPPoE の Cisco IOS 導入では、個々のセッションは仮想アクセスインターフェイス（無線ネイバーへの接続）で表され、これらの PPPoE 拡張を使用して QoS を適用できます。

RFC5578 は、信頼ベースのフロー制御とセッションベースのリアルタイムリンク メトリックをサポートするための PPPoE の拡張を実現します。この拡張は、可変帯域幅および制限付きバッファリング機能（無線リンクなど）を使用した接続に非常に役立ちます。

## 仮想マルチポイント インターフェイス (VMI)

PPPoE 拡張によってルータと無線間で通信するためのセットアップの大部分が実現しますが、VMI は、上位レイヤ（ルーティングプロトコルなど）が消費するイベントを管理および変換する必要に対処します。また、VMI はバイパスモードで動作します。

バイパスモードでは、無線ネイバーを表すすべての仮想アクセスインターフェイス (VAI) がルーティングプロトコル OSPFv3 および EIGRP に明示されるため、ルーティングプロトコルは、ユニキャストとマルチキャスト両方のルーティングプロトコルトラフィックに関してそれぞれの VAI と直接通信します。

集約モードでは、VMI がルーティングプロトコル (OSPF) に明示されるため、ルーティングプロトコルは VMI を活用して効率を最適化できます。ネットワークネイバーが、VMI でのブロードキャストおよびマルチキャスト機能を備えたポイントツーマルチポイントリンク上のネットワークの集合と見なされる場合、VMI は、PPPoE から作成された複数の仮想アクセスインターフェイスの集約に役立ちます。VMI は、単一のマルチアクセスレイヤ2ブロードキャスト対応インターフェイスを提供します。VMI レイヤは、ユニキャストルーティングプロトコルトラフィックを適切な P2P リンク（仮想アクセスインターフェイス）にリダイレクトし、フローする必要があるすべてのマルチキャスト/ブロードキャストトラフィックを複製します。ルーティングプロトコルは単一のインターフェイスと通信するため、ネットワークの完全性に影響を与えることなく、トポロジデータベースのサイズが縮小されます。

# PPPoE 拡張セッションでの QoS プロビジョニング

次の例では、PPPoE 拡張セッションでの QoS プロビジョニングについて説明します。

```
policy-map rar_policer
  class class-default
    police 10000 2000 1000 conform-action transmit exceed-action drop violate-action
    drop
policy-map rar_shaper
  class class-default
    shape average percent 1

interface Virtual-Template2
  ip address 10.92.2.1 255.255.255.0
  no peer default ip address
  no keepalive
  service-policy input rar_policer
end
```

## 例：バイパスモードでの RAR 機能の設定

次に、バイパスモードにおける RAR のエンドツーエンド設定の例を示します。



- (注) RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。認証され有効になっていないと、ポイントツーポイントプロトコルはこれを RAR セッションとして認識せず、PPPoE Active Discovery Initiate (PADI) の提示の際に *manet\_radio* をタグ付けしない場合があります。デフォルトでは、設定にバイパスモードが表示されません。モードがバイパスとして設定されている場合にのみ表示されます。

### RAR のサービスの設定

```
policy-map type service rar-lab
  pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

### ブロードバンドの設定

```
bba-group pppoe VMI2
  virtual-template 2
  service profile rar-lab
!
interface GigabitEthernet0/0/1
  description Connected to Client1
  negotiation auto
  pppoe enable group VMI2
!
```

### RAR のサービスの設定

```
policy-map type service rar-lab
  pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

### バイパスモードの設定

- 仮想テンプレートで明示的に設定された IP アドレス

```
interface Virtual-Template2
  ip address 192.168.90.3 255.255.255.0
  no ip redirects
  peer default ip address pool PPPoEpool2
  ipv6 enable
  ospfv3 1 network manet
  ospfv3 1 ipv4 area 0
  ospfv3 1 ipv6 area 0
  no keepalive
```

```
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

- 仮想テンプレートで設定された番号なしの VMI

```
interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

### バイパスモードでの仮想マルチポイント インターフェイスの設定

```
interface vmi2 //configure the virtual multi interface
ip address 192.168.2.1 255.255.0.0
physical-interface GigabitEthernet0/0/1
mode bypass

interface vmi3//configure the virtual multi interface
ip address 192.168.3.1 255.255.0.0
physical-interface GigabitEthernet0/0/1
mode bypass
```

### OSPF ルーティングの設定

```
router ospfv3 1
router-id 192.168.1.1
!
address-family ipv4 unicast
redistribute connected metric 1 metric-type 1
log-adjacency-changes
exit-address-family
!
address-family ipv6 unicast
redistribute connected metric-type 1
log-adjacency-changes
exit-address-family
!
ip local pool PPPoEpool2 192.168.12.3 192.168.12.254
```

## RAR セッションの詳細の確認

RAR セッションの詳細を取得するには、次の show コマンドを使用します。

```
Router#show pppoe session packets all
Total PPPoE sessions 2

session id: 9
local MAC address: 006b.f10e.a5e0, remote MAC address: 0050.56bc.424a
virtual access interface: Vi2.1, outgoing interface: Gi0/0/0
```

```
1646 packets sent, 2439363 received
176216 bytes sent, 117250290 received
```

```
PPPoE Flow Control Stats
Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes
Credit Grant Threshold: 28000 Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 32928 PADG Timer index: 0
PADG last rcvd Seq Num: 17313
PADG last nonzero Seq Num: 17306
PADG last nonzero rcvd amount: 2
PADG Timers: (ms) [0]-1000 [1]-2000 [2]-3000 [3]-4000 [4]-5000
PADG xmit: 33308 rcvd: 17313
PADC xmit: 17313 rcvd: 19709
In-band credit pkt xmit: 7 rcvd: 2434422
Last credit packet snapshot
PADG xmit: seq_num = 32928, fcn = 0, bcn = 65535
PADC rcvd: seq_num = 32928, fcn = 65535, bcn = 65535
PADG rcvd: seq_num = 17313, fcn = 0, bcn = 65535
PADC xmit: seq_num = 17313, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 61, bcn = 65533
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
PADQ xmit: 0 rcvd: 0
```

```
session id: 10
local MAC address: 006b.f10e.a5e1, remote MAC address: 0050.56bc.7dcb
virtual access interface: Vi2.2, outgoing interface: Gi0/0/1
1389302 packets sent, 1852 received
77869522 bytes sent, 142156 received
```

```
PPPoE Flow Control Stats
Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes
Credit Grant Threshold: 28000 Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 18787 PADG Timer index: 0
PADG last rcvd Seq Num: 18784
PADG last nonzero Seq Num: 18768
PADG last nonzero rcvd amount: 2
PADG Timers: (ms) [0]-1000 [1]-2000 [2]-3000 [3]-4000 [4]-5000
PADG xmit: 18787 rcvd: 18784
PADC xmit: 18784 rcvd: 18787
In-band credit pkt xmit: 1387764 rcvd: 956
Last credit packet snapshot
PADG xmit: seq_num = 18787, fcn = 0, bcn = 65535
PADC rcvd: seq_num = 18787, fcn = 65535, bcn = 65535
PADG rcvd: seq_num = 18784, fcn = 0, bcn = 65535
PADC xmit: seq_num = 18784, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 0, bcn = 64222
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
PADQ xmit: 0 rcvd: 1
```

```
Router#show pppoe session packets
Total PPPoE sessions 2
```

SID	Pkts-In	Pkts-Out	Bytes-In	Bytes-Out
9	2439391	1651	117252098	176714
10	1858	1389306	142580	77869914

```
Router#show vmi counters
Interface vmi2: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
    Queue Full         =          0

Output Counts:
  Transmit:
    VMI Process DQ     =        4280
    Fastswitch VA      =          0
    Fastswitch VMI     =          0
  Drops:
    Total               =          0
    QOS Error           =          0
    VMI State Error    =          0
    Mcast NBR Error    =          0
    Ucast NBR Error    =          0
Interface vmi3: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
    Queue Full         =          0

Output Counts:
  Transmit:
    VMI Process DQ     =        2956
    Fastswitch VA      =          0
    Fastswitch VMI     =          0
  Drops:
    Total               =          0
    QOS Error           =          0
    VMI State Error    =          0
    Mcast NBR Error    =          0
    Ucast NBR Error    =          0
Interface vmi4: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
    Queue Full         =          0

Output Counts:
  Transmit:
    VMI Process DQ     =          0
    Fastswitch VA      =          0
    Fastswitch VMI     =          0
  Drops:
    Total               =          0
    QOS Error           =          0
    VMI State Error    =          0
    Mcast NBR Error    =          0
    Ucast NBR Error    =          0
Router#

Router#show vmi neighbor details
1 vmi2 Neighbors
  1 vmi3 Neighbors
```

```

0 vmi4 Neighbors
2 Total Neighbors

vmi2  IPV6 Address=FE80::21E:E6FF:FE43:F500
      IPV6 Global Addr=:
      IPV4 Address=192.168.2.2, Uptime=05:15:01
      Output pkts=89, Input pkts=0
      No Session Metrics have been received for this neighbor.
      Transport PPPoE, Session ID=9
      INTERFACE STATS:
        VMI Interface=vmi2,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        V-Access intf=Virtual-Access2.1,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        Physical intf=GigabitEthernet0/0/0,
          Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
Local Credits: 65535  Peer Credits: 65535  Local Scaling Value 64 bytes
Credit Grant Threshold: 28000  Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 33038  PADG Timer index: 0
PADG last rcvd Seq Num: 17423
PADG last nonzero Seq Num: 17420
PADG last nonzero rcvd amount: 2
PADG Timers: (ms)  [0]-1000  [1]-2000  [2]-3000  [3]-4000  [4]-5000
PADG xmit: 33418  rcvd: 17423
PADC xmit: 17423  rcvd: 19819
In-band credit pkt xmit: 7  rcvd: 2434446
Last credit packet snapshot
  PADG xmit: seq_num = 33038, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33038, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17423, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17423, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
  ==== PADQ Statistics ====
  PADQ xmit: 0  rcvd: 0

vmi3  IPV6 Address=FE80::21E:7AFF:FE68:6100
      IPV6 Global Addr=:
      IPV4 Address=91.91.91.4, Uptime=05:14:55
      Output pkts=6, Input pkts=0
      METRIC DATA: Total rcvd=1, Avg arrival rate (ms)=0
        CURRENT: MDR=128000 bps, CDR=128000 bps
          Lat=0 ms, Res=100, RLQ=100, load=0
        MDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
        CDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
        Latency  Max=0, Min=0, Avg=0 (ms)
        Resource Max=100%, Min=100%, Avg=100%
        RLQ      Max=100, Min=100, Avg=100
        Load     Max=0%, Min=0%, Avg=0%
      Transport PPPoE, Session ID=10
      INTERFACE STATS:
        VMI Interface=vmi3,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        V-Access intf=Virtual-Access2.2,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        Physical intf=GigabitEthernet0/0/1,
          Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
Local Credits: 65535  Peer Credits: 65535  Local Scaling Value 64 bytes

```

```

Credit Grant Threshold: 28000    Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 18896        PADG Timer index: 0
PADG last rcvd Seq Num: 18894
PADG last nonzero Seq Num: 18884
PADG last nonzero rcvd amount: 2
PADG Timers: (ms)    [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
PADG xmit: 18896    rcvd: 18894
PADG rcvd: 18894    rcvd: 18896
In-band credit pkt xmit: 1387764 rcvd: 961
Last credit packet snapshot
  PADG xmit: seq_num = 18896, fcn = 0, bcn = 65535
  PADG rcvd: seq_num = 18896, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18894, fcn = 0, bcn = 65535
  PADG xmit: seq_num = 18894, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
  ==== PADQ Statistics ====
  PADQ xmit: 0    rcvd: 1

```

Router#**show vmi neighbor details vmi 2**

```

      1 vmi2 Neighbors

vmi2  IPV6 Address=FE80::21E:E6FF:FE43:F500
      IPV6 Global Addr=:
      IPV4 Address=192.168.2.2, Uptime=05:16:03
      Output pkts=89, Input pkts=0
      No Session Metrics have been received for this neighbor.
      Transport PPPoE, Session ID=9
      INTERFACE STATS:
        VMI Interface=vmi2,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        V-Access intf=Virtual-Access2.1,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        Physical intf=GigabitEthernet0/0/0,
          Input qcount=0, drops=0, Output qcount=0, drops=0

```

PPPoE Flow Control Stats

```

Local Credits: 65535    Peer Credits: 65535    Local Scaling Value 64 bytes
Credit Grant Threshold: 28000    Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 33100        PADG Timer index: 0
PADG last rcvd Seq Num: 17485
PADG last nonzero Seq Num: 17449
PADG last nonzero rcvd amount: 2
PADG Timers: (ms)    [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
PADG xmit: 33480    rcvd: 17485
PADG rcvd: 17485    rcvd: 19881
In-band credit pkt xmit: 7 rcvd: 2434460
Last credit packet snapshot
  PADG xmit: seq_num = 33100, fcn = 0, bcn = 65535
  PADG rcvd: seq_num = 33100, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17485, fcn = 0, bcn = 65535
  PADG xmit: seq_num = 17485, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
  ==== PADQ Statistics ====
  PADQ xmit: 0    rcvd: 0

```

Router#**show platform hardware qfp active feature ess session**

```

Current number sessions: 2
Current number TC flow: 0

```

Feature Type: A=Accounting D=Policing(DRL) F=FFR M=DSCP Marking L=L4redirect P=Portbundle  
T=TC

Session	Type	Segment1	SegType1	Segment2	SegType2	Feature	Other
21	PPP	0x0000001500001022	PPPOE	0x0000001500002023	LTERM	-----	
24	PPP	0x0000001800003026	PPPOE	0x0000001800004027	LTERM	-----	

Router#show platform software subscriber pppoe\_fctl evsi 21

PPPoE Flow Control Stats

Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes

Credit Grant Threshold: 28000 Max Credits per grant: 65535

Credit Starved Packets: 0

PADG xmit Seq Num: 33215 PADG Timer index: 0

PADG last rcvd Seq Num: 17600

PADG last nonzero Seq Num: 17554

PADG last nonzero rcvd amount: 2

PADG Timers: (ms) [0]-1000 [1]-2000 [2]-3000 [3]-4000 [4]-5000

PADG xmit: 33595 rcvd: 17600

PADC xmit: 17600 rcvd: 19996

In-band credit pkt xmit: 7 rcvd: 2434485

Last credit packet snapshot

PADG xmit: seq\_num = 33215, fcn = 0, bcn = 65535

PADC rcvd: seq\_num = 33215, fcn = 65535, bcn = 65535

PADG rcvd: seq\_num = 17600, fcn = 0, bcn = 65535

PADC xmit: seq\_num = 17600, fcn = 65535, bcn = 65535

In-band credit pkt xmit: fcn = 61, bcn = 65533

In-band credit pkt rcvd: fcn = 0, bcn = 65534

BQS buffer statistics

Current packets in BQS buffer: 0

Total en-queue packets: 0 de-queue packets: 0

Total dropped packets: 0

Internal flags: 0x0

Router#show platform hardware qfp active feature ess session id 21

Session ID: 21

EVSI type: PPP

SIP Segment ID: 0x1500001022

SIP Segment type: PPPOE

FSP Segment ID: 0x1500002023

FSP Segment type: LTERM

QFP if handle: 16

QFP interface name: EVSI21

SIP TX Seq num: 0

SIP RX Seq num: 0

FSP TX Seq num: 0

FSP RX Seq num: 0

Condition Debug: 0x00000000

session

Router#show ospfv3 neighbor

OSPFv3 1 address-family ipv4 (router-id 192.168.3.3)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
-------------	-----	-------	-----------	--------------	-----------

```
192.168.1.1          0    FULL/ -          00:01:32    19          Virtual-Access2.1
```

```
OSPFv3 1 address-family ipv6 (router-id 192.168.3.3)
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
192.168.1.1	0	FULL/ -	00:01:52	19	Virtual-Access2.1

```
Router#
```

```
Router#sh ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
```

```
Gateway of last resort is not set
```

```
          192.168.0.3/8 is variably subnetted, 3 subnets, 2 masks
C          192.168.3.0/24 is directly connected, Virtual-Access2.1
O          192.168.4.0/32 [110/1] via 192.168.4.0, 00:00:03, Virtual-Access2.1
L          192.168.5.0/32 is directly connected, Virtual-Access2.1
          192.168.0.5/32 is subnetted, 1 subnets
C          192.168.2.21 is directly connected, Virtual-Access2.1
```



## 翻訳について

このドキュメントは、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。