Cisco Intersight 管理モード コンフィギュレーション ガイド

最終更新：2024 年 9 月 17 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

はじめに：

通信、サービス、偏向のない言語、およびその他の情報 ix

第 1 章

Intersight 管理モードの概要 1

Intersight 管理モードの概要 1

サポート対象ハードウェア 2

第 2 章

ファブリック インターコネクトの設定 17

ファブリック インターコネクトの初期構成 17

コンソールを使用したファブリック インターコネクト A の設定 19

コンソールを使用したファブリック インターコネクト B の設定 21

GUI を使用したファブリック インターコネクト A の構成 22

GUI を使用したファブリック インターコネクト B の構成 25

ファブリック インターコネクト パスワードのガイドライン 27

Cisco UCS 6500 シリーズ ファブリック インターコネクトへの移行 28

Cisco UCS 6500 シリーズ ファブリック インターコネクトと UCSX-9508 シャーシを使用した既存のドメインでの UCSX-I-9108-25G から UCSX-I-9108-100G IFM への移行 30

ファブリック インターコネクトのビュー 31

ファブリック インターコネクトの詳細ビュー 31

ファブリック インターコネクトのインベントリ ビュー 36

ファブリック インターコネクトの接続ビュー 36

ファブリック インターコネクトの UCS ドメイン プロファイル ビュー 38

第 3 章

シャーシと FEX のライフサイクル 39

シャーシおよびファブリック エクステンダの検出とアクション 39

シャーシの詳細ビュー 42
シャーシのインベントリ ビュー 43
シャーシの接続ビュー 44
ファブリック エクステンダの詳細ビュー 44
ファブリック エクステンダのインベントリ ビュー 45
ファブリック エクステンダの接続ビュー 46

第 4 章 サーバのライフサイクル 47
サーバの検出とアクション 47
サーバ インベントリの表示 51
ハードウェア互換性リスト（HCL）との準拠 57

第 5 章 UCS ドメイン プロファイルの設定 59
UCS ドメイン プロファイルの概要 59
UCS ドメイン プロファイルの作成 59
UCS ドメイン プロファイルの詳細 60

第 6 章 サーバ プロファイルの設定 63
サーバー プロファイル 63
UCS サーバ プロファイルの作成 73
UCS サーバ プロファイルの詳細 76

第 7 章 UCS シャーシ プロファイルの設定 79
UCS シャーシ プロファイルの概要 79
シャーシ プロファイル テンプレートの作成とプロファイルの取得 80
シャーシ プロファイルの作成 82
UCS シャーシ プロファイルの詳細 82

第 8 章 UCS ドメイン ポリシーの設定 85
ドメイン ポリシー 85
ポート ポリシーの作成 89

イーサネット ネットワーク グループ ポリシーの作成 101
イーサネット ネットワーク制御ポリシーの作成 103
VLAN ポリシーの作成 105
VSAN ポリシーの作成 108
NTP ポリシの作成 110
ネットワーク接続ポリシーの作成 112
SNMP ポリシーの作成 114
システム QoS ポリシーの作成 117
Syslog ポリシーの作成 119
スイッチ制御ポリシーの作成 121
フロー制御ポリシーの作成 131
リンク集約ポリシーの作成 134
リンク集約ポリシーの作成 135
マルチキャスト ポリシーの作成 136

第 9 章 サーバ ポリシーの設定 139
サーバ ポリシー 140
ポリシーの作成 149
サポートされている UCS サーバ ポリシー 149
証明書管理ポリシーの作成 155
アダプタ設定ポリシーの作成 157
LAN 接続ポリシーの作成 162
イーサネット アダプタ ポリシーの作成 173
イーサネット QoS ポリシーの作成 183
イーサネット ネットワーク ポリシーの作成 185
イーサネット ネットワーク グループ ポリシーの作成 190
イーサネット ネットワーク制御ポリシーの作成 193
SAN 接続ポリシーの作成 195
ファイバ チャネル アダプタ ポリシーの作成 204
ファイバ チャネル ネットワーク ポリシーの作成 208
ファイバチャネル QoS ポリシーの作成 209

FC ゾーンポリシーの作成 211
ファームウェア ポリシーの作成 212
BIOS ポリシーの作成 213
ブート順序ポリシーの作成 232
iSCSI ブート ポリシーの設定 247
iSCSI アダプタ ポリシーの作成 252
iSCSI スタティック ターゲット ポリシーの作成 253
デバイス コネクタ ポリシーの作成 254
ドライブ セキュリティ ポリシーの作成 255
ディスク グループ ポリシーの作成 256
IMC アクセス ポリシーの作成 260
IPMI Over LAN ポリシーの作成 263
LDAP ポリシーの作成 265
ローカル ユーザ ポリシーの作成 271
NTP ポリシの作成 275
SD カード ポリシーの作成 276
Serial over LAN ポリシーの作成 278
SSH ポリシーの作成 280
仮想 KVM ポリシーの作成 281
仮想メディア ポリシーの作成 283
ネットワーク接続ポリシーの作成 288
SMTP ポリシーの作成 290
SNMP ポリシーの作成 292
ストレージ ポリシーの作成 295
Syslog ポリシーの作成 311
サーバの電源ポリシーの作成 313

第 10 章 UCS シャーシ ポリシーの設定 317
シャーシ ポリシー 317
IMC アクセス ポリシーの作成 318
SNMP ポリシーの作成 319

シャーシの電源ポリシーの作成 322
温度ポリシーの作成 325

第 11 章 プールの設定 327
プール 327
ID プール 327
プールの割り当て 328
プールの削除 328
予約済みの識別子 329
IP プール 330
IP プールの作成 331
IP プールの詳細 333
MAC プール 334
MAC プールの作成 335
MAC プールの詳細 335
UUID プール 337
UUID プールの作成 337
UUID プールの詳細 338
WWN プール 339
WWNN プールの作成 340
WWNN プールの詳細 341
WWPN プールの作成 342
WWPN プールの詳細 343
IQN プール 343
IQN プールの作成 343
IQN プールの詳細 344
リソース プール 346
リソース プールの作成 347
リソース プールの詳細 347
仮想ルーティングおよび転送 350
VRF インスタンスの作成 351

第 12 章 デバイス コンソールの管理 353

デバイス コンソール 353

第 13 章 ファームウェアの管理 355

Intersight を使用した Cisco UCS ドメインでのファームウェアアップグレード 355

ファブリック インターコネクト ファームウェアのアップグレード 358

サーバ ファームウェアのアップグレード 360

RMA でのサーバおよびファブリック インターコネクトのアップグレードおよび交換 362

第 14 章 テクニカル サポートの管理 367

Cisco TAC との統合 367

テクニカル サポートの診断ファイル収集 368

通信、サービス、偏向のない言語、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。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービス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 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 Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press 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には、Cisco Warranty Finder にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメント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。

Cisco バグ検索ツール

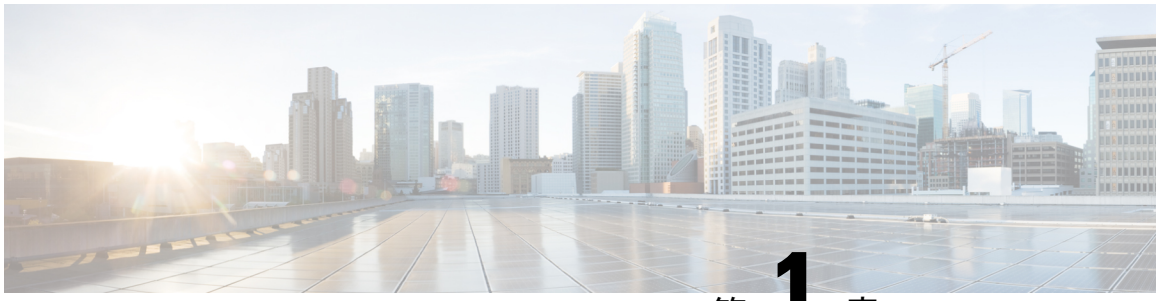
Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

偏向のない言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェ

通信、サービス、偏向のない言語、およびその他の情報

イスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



第 1 章

Intersight 管理モードの概要

- Intersight 管理モードの概要 （1 ページ）
- サポート対象ハードウェア （2 ページ）

Intersight 管理モードの概要

Cisco Intersight は、シスコとサードパーティの IT インフラストラクチャ向けの分析機能が組み込まれた SaaS 方式の管理プラットフォームです。Intersight Managed Mode（IMM）は、Redfish ベースの標準モデルを通じて UCS ファブリックインターコネクトシステムを管理する新しいアーキテクチャです。Intersight マネージドモードは、UCS システムの機能と Intersight のクラウドベースの柔軟性を統合し、スタンドアロンおよびファブリックインターコネクト接続システムの管理エクスペリエンスを統合します。Intersight Management Model は、UCS-FI-6454、UCS-FI-64108、UCS-FI-6536、UCSX-S9108-100G ファブリック インターコネクト、および Cisco UCS B シリーズ（M5、M6）、Cisco UCS C シリーズ（M5、M6、M7、M8）および Cisco UCS X シリーズ（M6、M7）サーバのポリシーと運用管理を標準化します。

ファブリックインターコネクトの初期設定時に、ファブリック接続 UCS システムのネイティブ UCS 管理モード（UMM）または Intersight 管理モード（IMM）を選択できます。UMM と IMM の間で切り替えることを選択した場合は、現在の構成を消去して、初期セットアップから開始する必要があります。

（注） 構成を消去する前に、Intersight からデバイスを要求解除し、すべてのラック サーバーをデコミッションする必要があります。

- Intersight 管理モードを設定する前に、システム要件、サポートされているハードウェアとソフトウェア、および UMM から IMM に移行するために必要な手順を確認してください。
- Intersight の機能の最新の更新については、「ヘルプ センター」を参照してください。
- IMM モードのサーバには、最低 Essentials ライセンスが必要です。

サポート対象ハードウェア

Supported Hardware for Intersight Managed Mode

This section includes the supported hardware for Intersight Managed Mode.

Table 1 lists the hardware components and the minimum required infrastructure firmware version.

Table 2 includes the supported hardware components along with the supported server and infrastructure firmware versions.

Table 3 shows the supported combination of components.

（注）

- The Intersight Managed Mode (IMM) now supports up to 20 chassis with 160 blade servers.
- Cisco UCS 6454 and 64108 Fabric Interconnects, require the port-based licensing in IMM but will not be enforced until further notice.

  Beginning with UCS software release version 4.2(3), the Cisco UCS 6536 Fabric Interconnect supports a perpetual software license. This license activates all ports and software features of the Fabric Interconnect.
- In IMM, after discovery of a rack server, online swapping of cables on rack network adapters between Fabric Interconnects is not supported.
- The minimum supported Infrastructure firmware version for Intersight Managed Mode is 4.1(3).

表 *1 : Supported Hardware Components with Required Minimum Infrastructure Versions*

Fabric Components				
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**
UCS-FI-6454	Fabric Interconnect			4.1(3b)
UCS-FI-64108	Fabric Interconnect			4.1(3b)
UCS-FI-6536	Fabric Interconnect			4.2(2b)

Fabric Components				
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**
N20-C6508 UCSB-5108-AC2	Chassis			4.1(3b)
		Input/Output Module (IOM)	UCS-IOM-2204XP UCS-IOM-2208XP UCS-IOM-2408	4.1(3b)
			UCS-IOM-2304 UCS-IOM-2304V2	4.2(3c)
UCSX-9508	Chassis			4.2(1e)
		X-Fabric Modules (XFM)	UCSX-F-9416	4.2(2a)
		Intelligent Fabric Module (IFM)	UCSX-I-9108-25G	4.2(1e)
			UCSX-I-9108-100G	4.2(2a)
Cisco Nexus 2232PP	Fabric Extender (FEX)			4.1(3b)
N9K-C93108YC-FX3	Fabric Extender (FEX)			4.2(2a)

表 *2 : Supported Hardware Components with Required Minimum Firmware Versions*

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSX-410C-M7	X-Series M7 Server			4.2(3e)	5.1(1.230052)
		Adapters	UCSX-ML-V5Q50G (Secure Boot) UCSX-ME-V5Q50G (Secure Boot) UCSX-ML-V5D200G	N/A	5.1(1.230052)
			UCSX-ML-V5D200GV2 (Secure Boot)	N/A	5.2(0.230061)
		Graphics processing unit (GPU)	UCSX-GPU-A16 UCSX-GPU-A40 UCSX-GPU-A100-80	N/A	5.1(1.230052)
			UCSX-GPU-H100-80 UCSX-GPU-L40 UCSX-GPU-L4 UCSX-GPU-FLEX140 UCSX-GPU-FLEX170	N/A	5.2(0.230127)
		Storage Controller	UCSX-M2-HWRAID UCSX-X10C-RAIDF	N/A	5.1(1.230052)
			UCSX-M2-PT-FPN	N/A	5.2(0.230127)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSX-210C-M7	X-Series M7 Server			4.2(3b)	5.1(0.230096)
		Adapters	UCSX-ML-V5Q50G (Secure Boot) UCSX-ME-V5Q50G (Secure Boot) UCSX-ML-V5D200G	N/A	5.1(0.230096)
			UCSX-ML-V5D200GV2 (Secure Boot)	N/A	5.2(0.230061)
		Graphics processing unit (GPU)	UCSX-GPU-T4-MEZZ UCSX-GPU-A16 UCSX-GPU-A40	N/A	5.1(0.230096)
			UCSX-GPU-A100-80	N/A	5.1(0.230096)
			UCSX-GPU-H100-80 UCSX-GPU-L40 UCSX-GPU-L4 UCSX-GPU-FLEX140 UCSX-GPU-FLEX170 UCSX-GPU-FLX140MZ	N/A	5.2(0.230127)
		Storage Controller	UCSX-X10C-PT4F UCSX-X10C-RAIDF UCSX-M2-HWRAID	N/A	5.1(0.230096)
			UCSX-M2-PT-FPN	N/A	5.2(0.230041)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSX-210C-M6	X-Series M6 Server			4.2(1a)	5.0(1b)
		Adapters	UCSX-V4-Q25GML UCSX-V4-Q25GME	N/A	5.0(1b)
			UCSX-ML-V5Q50G (Secure Boot) UCSX-ME-V5Q50G (Secure Boot)	N/A	5.1(0.230054)
			UCSX-ML-V5D200G	N/A	5.0(2b)
			UCSX-ML-V5D200GV2 (Secure Boot)	N/A	5.2(0.230061)
		Rear Mezzanine Adapters	UCSX-V4-PCIME	N/A	5.0(2d)
		Trusted Platform Module (TPM)	UCSX-TPM1-001 UCSX-TPM2-001 UCSX-TPM2-002 UCSX-TPM-002C	4.1(3b)	N/A
		Graphics processing unit (GPU)	UCSX-GPU-A100-80	N/A	5.0(2e)
			UCSX-GPU-T4-MEZZ UCSX-GPU-T4-16 UCSX-GPU-A16 UCSX-GPU-A40	N/A	5.0(2d)
		Storage Controller	UCSX-X10C-PT4F UCSX-X10C-RAIDF UCSX-M2-HWRAID	N/A	5.0(4b)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSB-B200-M6	B-Series M6 Server			4.1(3b)	4.2(3b)
		Adapters	UCSB-ML-V5Q10G	N/A	4.2(3b)
			UCSB-MLOM-40G-04 UCSB-VIC-M84-4P	4.1(3b)	4.2(3b)
		Trusted Platform Module (TPM)	UCSX-TPM-002C	4.1(3b)	N/A
		Storage Controller	UCS-M2-HWRAID UCSB-RAID12G-M6 UCSB-MSTOR-M6 UCSB-LSTOR-PT-M6	N/A	4.2(3b)
UCSB-B200-M5 UCSB-B480-M5	B-Series M5 Server			4.1(3b)	4.1(3b)
		Adapters	UCSB-MLOM-40G-03 UCSB-VIC-M83-8P	4.1(3b)	4.2(2e)
			UCSB-MLOM-40G-04 UCSB-VIC-M84-4P	4.1(3b)	4.1(3b)
			UCSB-MLOM-PT-01	4.1(3b)	N/A
		Trusted Platform Module (TPM)	UCSX-TPM2-001, UCSX-TPM2-002	4.1(3b)	N/A
		Storage Controller	UCS-M2-HWRAID UCSB-MRAID12G UCSB-MRAID12G-HE UCSB-LSTOR-PT	N/A	4.1(3c)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSC-C220-M7	C-Series M7 Server			4.2(3b)	4.3(1.230097)
		Adapters	UCSC-M-V5Q50G UCSC-M-V5D200G	N/A	4.3(1.230097)
			UCSC-P-V5D200G (Secure Boot) UCSC-P-V5Q50G (Secure Boot)	4.3(2.230117)	4.3(2.230184)
			UCSC-M-V5D200GV2 (Secure Boot) UCSC-M-V5Q50GV2 (Secure Boot)	N/A	4.3(2.230258)
		Graphics processing unit (GPU)	UCSC-GPU-A16 UCSC-GPU-A100-80	N/A	4.3(1.230097)
			UCSC-GPU-L4 UCSC-GPU-FLEX140	N/A	4.3(2.230207)
		Storage Controller	UCS-M2-NVRAID	4.3(2.230117)	4.3(2.230207)
		Virtual Drives	UCS-SD16TKA3X-EP UCS-SD32TKA3X-EP UCS-SD16TBKANK9 UCS-SD19TKA1X-EV UCS-SD38TKA1X-EV UCS-SD76TKA1X-EV UCS-SD15TKA1X-EV UCS-SD38TBKANK9 UCS-SD76TBKANK9	4.3(2.230117)	4.3(2.230207)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSC-C240-M7	C-Series M7 Server			4.2(3b)	4.3(1.230097)
		Adapters	UCSC-M-V5Q50G UCSC-M-V5D200G	N/A	4.3(1.230097)
			UCSC-P-V5D200G (Secure Boot) UCSC-P-V5Q50G (Secure Boot)	4.3(2.230117)	4.3(2.230184)
			UCSC-M-V5D200GV2 (Secure Boot) UCSC-M-V5Q50GV2 (Secure Boot)	N/A	4.3(2.230258)
		Graphics processing unit (GPU)	UCSC-GPU-A16 UCSC-GPU-A100-80	N/A	4.3(1.230097)
			UCSC-GPU-H100-80 UCSC-GPU-L40 UCSC-GPU-L4 UCSC-GPU-FLEX140 UCSC-GPU-FLEX170	N/A	4.3(2.230207)
		Storage Controller	UCS-M2-NVRAID	4.3(2.230117)	4.3(2.230207)
		Virtual Drives	UCS-SD16TKA3X-EP UCS-SD32TKA3X-EP UCS-SD16TBKANK9 UCS-SD19TKA1X-EV UCS-SD38TKA1X-EV UCS-SD76TKA1X-EV UCS-SD15TKA1X-EV UCS-SD38TBKANK9 UCS-SD76TBKANK9	4.3(2.230117)	4.3(2.230207)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSC-C220-M6 UCSC-C240-M6 UCSC-C245-M6 UCSC-C225-M6	C-Series M6 Server			4.1(3b)	4.1(3b)
		Adapters	UCSC-PCIE-C25Q-04 UCSC-PCIE-C100-04	4.1(3b)	4.1(3b)
			UCSC-M-V100-04 UCSC-M-V25-04	4.1(3b)	4.2(1d)
			UCSC-M-V5D200G	N/A	4.2(2f)
			UCSC-M-V5Q50G	N/A	4.2(2b)
			UCSC-P-V5D200G (Secure Boot) UCSC-P-V5Q50G (Secure Boot)	4.3(2.230117)	4.3(2.230184)
			UCSC-M-V5D200GV2 (Secure Boot) UCSC-M-V5Q50GV2 (Secure Boot)	N/A	4.3(2.230258)
		Graphics processing unit (GPU)	UCSC-GPU-A16 UCSC-GPU-A100-80	N/A	4.2(3b)
		Storage Controller	UCS-M2-HWRAID UCSC-RAID-M6T UCSC-RAID-M6SD UCSC-RAID-M6HD UCSC-SAS-M6HD UCSC-SAS-M6T	N/A	4.2(1a)

Fabric Components					
Model	**Component**	**Sub-Component**	**Sub-Component Model**	**Minimum Infrastructure Firmware Versions**	**Minimum Server Firmware Versions**
UCSC-C220-M5 UCSC-C240-M5 UCSC-C480-M5	C-Series M5 Server			4.1(3b)	4.1(3b)
		Adapters	UCSC-MLOM-C40Q-03 UCSC-PCIE-C40Q-03	4.1(3b)	4.2(2g)
			UCSC-PCIE-C25Q-04 UCSC-MLOM-C25Q-04 UCSC-PCIE-C100-04 UCSC-MLOM-C100-04	4.1(3b)	4.1(3b)
		Graphics processing unit (GPU)	UCSC-GPU-A100-80	N/A	4.2(3b)
		Storage Controller	UCS-M2-HWRAID UCSC-RAID-M5HD UCSC-RAID-M5 UCSC-SAS-M5, UCSC-SAS-M5HD UCSC-SAS12GHBA UCSC-9400-8E	N/A	4.1(3b)

（注） Post Infra Firmware release 4.2(3c), the Server Firmware bundle in Intersight Infrastructure Service (IIS) will bear the version number in a new format instead of the letter format.

With Infra Firmware release 4.3(2), the Infra Firmware bundle in IIS will bear the version number in a new format instead of the letter format.

For example: 4.3(2.230117) , where 23 represents year, 0117 shows the incremental build number.

For more information on Cisco Intersight Infrastructure Firmware release notes, Server Firmware release notes, and Release Bundle Content document see Release Notes.

表 *3 : Supported Combination of Hardware Components in IMM*

Component	Supported Combination
Topologies	Direct-Attached Racks through 10G/25G/100G connections Break-out port configuration through 10G/25G connections FEX-Attached Racks through 10GE connections Chassis through 10G/25G/100G connections N9K-C93108YC-FX3 FEX through 10G/25G connections
Fabric Interconnects	UCS-FI-6536 and direct-attached rack server are supported at 40G and 100G on Cisco UCS 1400 and 15000 series VIC adapters.
Input/Output Module (IOM)	• UCS-IOM-2204XP and UCS-IOM-2208XP are not supported on Cisco UCS 6500 Series Fabric Interconnects. • UCS-IOM-2304 and UCS-IOM-2304V2 are supported only with Cisco UCS 6500 series Fabric Interconnect. • When there is a mixed IOM configuration, Access Policy deployment can fail resulting in Server Profile deployment failure. It will recover once both the IOMs are replaced.
X-Fabric Modules (XFM)	UCS 9416 X-Fabric module is supported only on UCSX-9508 chassis and required for Peripheral Component Interconnect Express (PCIe) node and GPU discovery or inventory support in IMM.
Fabric Extender (FEX)	Cisco Nexus 2232PP is not supported on Cisco UCS 6500 Series Fabric Interconnects.
Rear Mezzanine Adapters	• UCS PCI mezz card for X-Fabric connectivity. • The UCSX-210C Compute Node must include a UCSX-V4-PCIME or a supported mezz card when paired with a X440p PCIe node.

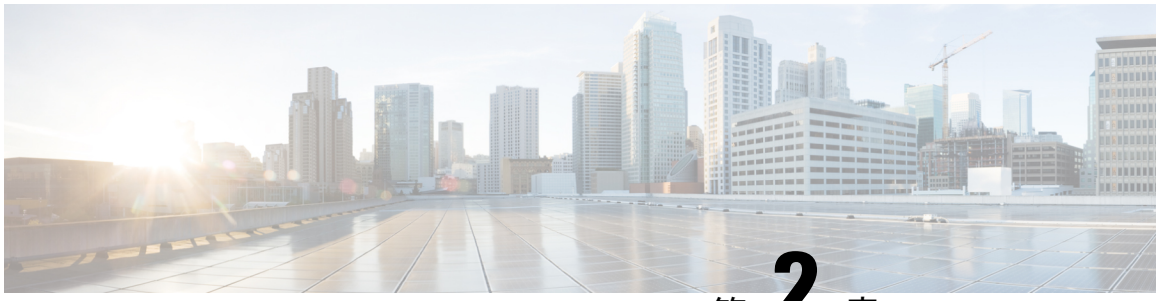
Component	Supported Combination
Adapters	

Component	Supported Combination

	• UCSX-X10C-GPUFM is an adapter that supports the GPU, UCSX-GPU-T4-MEZZ. For more information, see Cisco UCS X10c Front Mezzanine GPU Module Installation and Service Guide.
	• UCSX-V4-Q25GME is a mezz card requires UCS VIC 14000 bridge connector (UCSX-V4-BRIDGE) and UCSX-V4-Q25GML mLOM support in the X210c Compute Node. For more information, see Cisco UCS X210c M6 Compute Node.
	• The UCSX-210C Compute Node must include a UCSX-V4-PCIME or a supported mezz card when paired with a X440p PCIe node.
	• UCSX-ML-V5D200G adapter is supported on Cisco UCS 6500 series Fabric Interconnect at 40G and 100G speed, as well as on Cisco UCS 6400 series Fabric Interconnect at 25G speed.
	• Cisco UCS C-Series and X-Series M7 servers support only Cisco UCS 15000 series VIC adapters.
	• UCSX-ME-V5Q50G is a mezz card that requires UCS VIC 15000 bridge connector (UCSX-V5-BRIDGE) and UCSX-ML-V5Q50G mLOM support in the X210c Compute Node. However, this mezz adapter is not supported with UCSX-ML-V5D200G mLOM.
	  • On a B-series server, installing a combination of Cisco UCS 1400 and UCS 15000 series VIC adapters is not supported.
	  • Cisco UCS VIC 1300 Series adapters are supported on B-Series and C-Series M5 servers with the following combination.
	  • UCS-FI-6454 and UCS-IOM-2408
	  • UCS-FI-6536 and UCS-IOM-2408
	  • UCS-FI-6454 and UCS-IOM-2204XP
	  • UCS-FI-6454 and UCS-IOM-2208XP
	  • UCS-FI-6536 and direct-attached rack server at 40G
	  • UCS-FI-6454 and rack server connected through FEX
	  • UCS-FI-6454 and direct-attached rack server with 10G QSA

Component	Supported Combination
	• UCS-FI-6536 and UCS-IOM-2304 or UCS-IOM-2304V2 • UCS-FI-64108 and UCS-IOM-2408 • UCS-FI-64108 and UCS-IOM-2204XP • UCS-FI-64108 and UCS-IOM-2208XP • UCS-FI-64108 and direct-attached rack server • UCS-FI-64108 and rack server connected through FEX • UCSC-M-V100-04, UCSC-PCIE-C100-04, UCSC-MLOM-C100-04 are supported only on Cisco UCS 6500 Series Fabric Interconnects. • The following combinations are not supported on UCS C series M6 servers: • 1400 Series MLOM adapters with 15000 Series PCIE adapters • UCSC-M-V5Q50GV2 and UCSC-M-V5D200GV2 are not supported with 14xx PCIE adapters • Ensure that you have upgraded servers to the VIC supported release versions before installing the VIC adapters into the server. If you install VIC adapters on servers running an earlier release and later decide to upgrade the servers to the supported version, you need to perform A/C power cycle for the servers to enable the adapters.

Component	Supported Combination
Graphics processing unit (GPU)	• All supported X-Series GPU are supported on UCS X440P with UCSX-210C-M6 and UCSX-210C-M7 Compute Nodes. • Mixing of GPU models are not supported in the server. For more information, see Cisco UCS X440p PCIe Node Installation and Service Guide. • Specific GPUs are also supported on the X210c Compute Nodes. They require the UCSX-X10C-GPUFM adapter to support a GPU in the Front Mezz. • The GPU supported in the X210c M7 Front Mezz includes UCSX-GPU-T4-MEZZ. For more information, see Cisco UCS X10c Front Mezzanine GPU Module Installation and Service Guide.



第 2 章

ファブリック インターコネクトの設定

- ファブリック インターコネクトの初期構成 （17 ページ）
- コンソールを使用したファブリック インターコネクト A の設定 （19 ページ）
- コンソールを使用したファブリック インターコネクト B の設定 （21 ページ）
- GUI を使用したファブリック インターコネクト A の構成 （22 ページ）
- GUI を使用したファブリック インターコネクト B の構成 （25 ページ）
- ファブリック インターコネクト パスワードのガイドライン （27 ページ）
- Cisco UCS 6500 シリーズ ファブリック インターコネクトへの移行 （28 ページ）
- Cisco UCS 6500 シリーズ ファブリック インターコネクトと UCSX-9508 シャーシを使用した既存のドメインでの UCSX-I-9108-25G から UCSX-I-9108-100G IFM への移行 （30 ページ）
- ファブリック インターコネクトのビュー （31 ページ）
- ファブリック インターコネクトの詳細ビュー （31 ページ）
- ファブリック インターコネクトのインベントリ ビュー （36 ページ）
- ファブリック インターコネクトの接続ビュー （36 ページ）
- ファブリック インターコネクトの UCS ドメイン プロファイル ビュー （38 ページ）

ファブリック インターコネクトの初期構成

ファブリック インターコネクトの初期設定は、ファブリック インターコネクトの初回起動時にシリアルコンソールを使用して実行できます。これは、工場出荷時のインストール中、または既存の設定がクリアされた後に発生します。設定ウィザードでは、管理モード、および各ファブリック インターコネクトの管理サブネット、ゲートウェイ、DNS IP アドレスなどの他のパラメータを選択できます。管理モードでは、ファブリック インターコネクトを Cisco UCS Manager または Cisco Intersight のどちらで管理するかを選択できます。

Cisco Intersight と Cisco UCS Manager 間のファブリック インターコネクトの管理モードを変更できます。ただし、これはすべてのエンドポイント設定がリセットされ、現在の設定が失われるため、中断を伴うプロセスです。

（注） 管理モードを変更する前に、検出されたすべてのサーバ、シャーシ、およびファブリック エクステンダ（FEX）を停止する必要があります。

両方の管理モードで使用できる消去設定オプションを使用すると、既存の設定をクリアして、ファブリック インターコネクトをリブートできます。ファブリック インターコネクトがリブートすると、初期設定画面が表示され、適切な管理モードでファブリック インターコネクトを設定できます。

この構成プロセスは、クラスタ設定の Cisco UCS 6400 シリーズ ファブリック インターコネクト、Cisco UCS 6500 シリーズ ファブリック インターコネクト、および Cisco UCS ファブリック インターコネクト 9108 100G で有効です。

（注） Cisco UCS 6500 シリーズ ファブリック インターコネクトは、ファームウェア バージョン 4.2(3b) 以降の UCSM 管理モード（UMM）をサポートします。

クラスタ内のファブリック インターコネクトを設定するには、次の手順を実行します。

1. コンソールを使用したファブリック インターコネクト A の設定
2. コンソールを使用したファブリック インターコネクト B の設定

ファブリック インターコネクトの初期設定が完了したら、Cisco Intersight プラットフォームで使用するためにそれらを要求する必要があります。Cisco Intersight でのデバイスの要求の詳細については、「Intersight 管理モードでのターゲット要求」を参照してください。

ファブリック インターコネクトを要求すると、使用可能なデバイスのリストに表示されます。Cisco Intersight によって管理されるファブリック インターコネクトのデバイスタイプは、**[Intersight 管理対象ドメイン（Intersight Managed Domain）]** です。**[デバイス IP（Device IP）]** フィールドには両方のファブリック インターコネクトの IP アドレスが表示され、**[デバイス ID（Device ID）]** フィールドには両方のファブリック インターコネクトのシリアル番号が表示されます。ファブリック インターコネクトが **[ファブリック インターコネクト（Fabric Interconnects）]** テーブルビューに表示されます。

ファブリック インターコネクトを要求した後、接続されたシャーシとサーバを検出するようにファブリック インターコネクトのポートを設定する必要があります。ファブリック インターコネクトごとに、ポート、ファンモジュール、電源ユニット（PSU）などのコンポーネントのプロパティとインベントリを表示できます。

コンソールを使用したファブリック インターコネクト A の設定

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトが起動すると、電源投入時のセルフテスト メッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

ステップ 4 入力ファブリック インターコネクトの管理モードに入ります。

- **intersight** では、Cisco Intersight を使用してファブリック インターコネクトを管理します。
- **ucsm** では、Cisco UCS Manager を使用してファブリック インターコネクトを管理します

注：

- スタンドアロン オプションは、Intersight 管理対象モードではサポートされていません。
- ファブリック インターコネクトがデフォルト モードである Intersight 管理モードのみのファブリック インターコネクトである場合は、[いいえ（No）] を選択して、必要なモードを選択できます。

ステップ 5 **y** と入力して、初期設定を続行することを確認します。

ステップ 6 強力なパスワードを使用するには、**y** と入力します。

ステップ 7 管理アカウントのパスワードを入力します。詳細については、ファブリック インターコネクト パスワードのガイドラインを参照してください。

ステップ 8 確認のために、管理アカウントのパスワードを再入力します。

ステップ 9 **yes** と入力して、クラスタ構成の初期設定を続行します。

ステップ 10 ファブリック インターコネクトのファブリックに入ります（**A** または **B**）。

ステップ 11 システム名を入力します。

ステップ 12 ファブリック インターコネクトの管理ポートの IPv4 または IPv6 アドレスを入力します。

IPv4 アドレスを入力する場合は、IPv4 サブネット マスクを入力するように求められます。IPv6 アドレスを入力する場合は、IPv6 ネットワーク プレフィックスを入力するように求められます。

ステップ 13 各 IPv4 サブネット マスク、または IPv6 ネットワーク プレフィックスを入力し、**Enter** キーを押します。

ファブリック インターコネクトの管理ポート用に入力したアドレス タイプに応じて、デフォルト ゲートウェイの IPv4 または IPv6 アドレスが求められます。

ステップ 14 次のいずれかを入力します。

- デフォルト ゲートウェイの IPv4 アドレス
- デフォルト ゲートウェイの IPv6 アドレス

ステップ 15 DNS サーバーの IPv4 または IPv6 アドレスを入力します。

アドレス タイプはファブリック インターコネクトの管理ポートのアドレス タイプと同じである必要があります。

ステップ 16 デフォルトのドメイン名を指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 17 （任意） デフォルト ドメイン名を入力します。

ステップ 18 設定の要約を確認し、 **yes** と入力して設定を保存および適用します。設定を一部変更するために再びやり直すには、 **no** と入力します。

設定を再実行することを選択した場合、以前に入力した値がカッコに入れられて表示されます。以前に入力した値をそのまま使用する場合は、**Enter** を押します。

例

これは、コンソールアドレスと管理アドレスを使用してクラスタ構成の Cisco Intersight 管理モードでファブリック インターコネクト A を設定する例です。

```
Enter the configuration method (console/gui)?  console
Enter the management mode [ucsm/intersight]? intersight
You have chosen to setup a new Fabric Interconnect in “intersight” managed mode. Continue?
 (y/n): y
Enforce strong password? (y/n) [y]:n

Enter the password for "admin":
Confirm the password for "admin":

Enter the switch fabric (A/B) []: A

Enter the system name: UCS

Physical Switch Mgmt0 IP address : 15.XX.XX.XX

Physical Switch Mgmt0 IPv4 netmask : 255.255.255.X

IPv4 address of the default gateway : 15.XX.XX.XX

DNS IP address : 15.XX.XX.XX

Configure the default domain name? (yes/no) [n]:

Following configurations will be applied:

Management Mode=intersight
Switch Fabric=A
System Name=UCS-A
Enforced Strong Password=no
Physical Switch Mgmt0 IP Address=15.XX.XX.XX
Physical Switch Mgmt0 IP Netmask=255.255.255.X
Default Gateway=15.XX.XX.XX
Ipv6 value=0
DNS Server=15.XX.XX.XX

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

次のタスク

コンソールを使用してファブリック インターコネクト B を設定します。

コンソールを使用したファブリック インターコネクト B の設定

ここでは、管理ポートに対し IPv4 または IPv6 アドレスを使用してファブリック インターコネクト B をセットアップする手順について説明します。

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトが起動すると、電源投入時のセルフテスト メッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

（注） ファブリック インターコネクト A は、クラスタ内のファブリック インターコネクト B を検出するはずです。検出されない場合、L1 ポートと L2 ポートの間の物理接続を確認し、ピア ファブリック インターコネクト B がクラスタ設定用にイネーブルになっていることを確認します。

ステップ 4 **y** と入力して、ファブリック インターコネクト B をクラスタに追加します。

ステップ 5 ピア ファブリック インターコネクトの admin パスワードを入力します。

ステップ 6 ファブリック インターコネクト B の管理ポートの IP アドレスを入力します。

ステップ 7 設定の要約を確認し、 **yes** と入力して設定を保存および適用します。設定を一部変更するために再びやり直すには、 **no** と入力します。

設定を再実行することを選択した場合、以前に入力した値が示され、それらの値はカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

例

次に、コンソールアドレスと管理アドレスを使用してクラスタ構成の Cisco Intersight 管理モードでファブリックインターコネクト B を設定する例を示します。

```
Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
 will be added to the cluster. Continue (y/n) ? y


Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect management mode : intersight
Peer Fabric interconnect Mgmt0 IPv4 Address: 15.XX.XX.XX
```

```
Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4
Address

Physical Switch Mgmt0 IP address : 15.XX.XX.XX

Local fabric interconnect model(UCS-FI-6454)
Peer fabric interconnect is compatible with the local fabric interconnect. Continuing
with the installer...

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

次のタスク

Cisco Intersight を介して Intersight 管理対象ドメインを要求します。詳細については、ターゲット クレイム Intersight 管理モードを参照してください。

GUI を使用したファブリック インターコネクト A の構成

GUI を使用したファブリック インターコネクト *A* の構成

この手順では、GUI を使用したファブリック インターコネクト A の構成について説明します。

GUI を使用してファブリック インターコネクト A を構成する方法の詳細については、「クラスタ構成の初期システム セットアップ」を参照してください。

1. ファブリック インターコネクトの電源を入れます。

   ファブリックインターコネクトが起動すると、電源投入時のセルフテストメッセージが表示されます。

2. システムがリースを取得する場合は手順 6 に移動します。それ以外の場合は次のステップに進みます。

3. コンソール ポートに接続します。

4. インストール方式プロンプトに **gui** と入力します。

   .

5. システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

   - ファブリック インターコネクトの管理ポートの IPv4 または IPv6 アドレス。
   - ファブリック インターコネクトの管理ポートの IPv4 サブネット マスクまたは IPv6 プレフィクス。
   - ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IPv4 または IPv6 アドレス

（注） クラスタ設定では、設定時に両方のファブリック インターコネクトに同じ管理インターフェイスのアドレス タイプを割り当てる必要があります。

6. プロンプトから Web ブラウザに Web リンクをコピーし、Cisco UCS ファブリック インターコネクト セットアップ GUI 起動ページに移動します。

（注） 希望に応じて、次の 2 つのモードの間で選択できます。UCSM 管理対象と Intersight 管理対象ファブリック インターコネクト。

7. 「**Cisco UCS ファブリック インターコネクト セットアップ GUI**」起動ページで、**[簡易設定（Express Setup）]** を選択します。

8. **[簡易設定（Express Setup）]** ページで、ファブリック インターコネクト構成の詳細を入力します。

（注） Cisco UCS Manager 4.2(2) 以降から、GUI セットアップ方法を選択して、ファブリック インタコネクトを構成します。ファブリック インターコネクトのデフォルトが Intersight 管理対象モードに設定されている場合、確認中に変更を選択し、コンソールセットアップ方法のみで必要なモードを再び選択できます。

9. **[基本設定（Basic Settings）]** エリア：

   - **[ファブリック設定（Fabric Setup）]** オプションで **[ファブリック A（Fabric A）]** を選択します。
   - Cisco Intersight マネージド モードで使用する IPv4 または IPv6 アドレスを選択します。

   [Submit (送信)] をクリックします。

10. [System Setup] 領域で、次のフィールドに値を入力します。

フィールド	説明
[強力なパスワードの適用（Enforce Strong Password）]	[はい] または [いいえ] を選択して、強力なパスワードを適用します。

フィールド	説明
システム名	Cisco UCS ドメインに割り当てられる名前。 スタンドアロン設定では、システム名に「-A」が追加されます。クラスタ設定では、ファブリック A に割り当てられたファブリック インターコネクトに「-A」が、ファブリック B に割り当てられたファブリックインターコネクトに「-B」が追加されます。
[管理パスワード（Admin Password）]	ファブリックインターコネクト上の管理者アカウントに使用されるパスワード。 Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。このパスワードは空にできません。
[Confirm Admin Password]	ファブリックインターコネクト上の管理者アカウントに使用されるパスワード。
[Mgmt IP Address]	ファブリックインターコネクトの管理ポートのスタティック IPv4 または IPv6 アドレス。
[Mgmt IP Netmask] または [Mgmt IP Prefix]	ファブリックインターコネクトの管理ポートの IPv4 サブネット マスクまたは IPv6 プレフィクス。 （注） [Mgmt IP Address] に入力したアドレス タイプに基づいて、[Mgmt IP Netmask] または [Mgmt IP Prefix] の入力が求められます。
[Default Gateway]	ファブリック インターコネクト上の管理ポートに割り当てられるデフォルト ゲートウェイの IPv4 アドレス。 （注） [Mgmt IP Address] フィールドに入力したアドレス タイプに基づいて、システムから [Default Gateway] アドレス タイプへの入力が求められます。

フィールド	説明
DNS サーバーの IP（DNS Server IP）	ファブリック インターコネクトに割り当てられる DNS サーバの IPv4 または IPv6 アドレス。
ドメイン名	ファブリック インターコネクトが存在するドメインの名前。

（注）
- Intersight 管理対象モード ファブリック インターコネクトの場合、DNS は必須です
- スタンドアロン オプションは、Intersight 管理対象モードではサポートされていません。

11. [送信（Submit）] をクリックします。

セットアップ操作の結果がページに表示されます。

次の作業

GUI を使用したファブリック インターコネクト B の構成

GUI を使用したファブリック インターコネクト B の構成

GUI を使用したファブリック インターコネクト *B* の構成

ここでは、GUI を使用したファブリック インターコネクト B のセットアップ手順を説明します。

以下に示す従属ファブリックインターコネクトの設定手順に従うか、または「Cisco UCS Manager Initial Setup part 2」を視聴します。

（注）新しいファブリックインターコネクトを既存の高可用性クラスタに追加する場合、たとえば、新規インストール時またはファブリックインターコネクトの交換時に、認証方式がリモートに設定されている限り、新しいデバイスはクラスタにログインできません。新しいファブリックインターコネクトをクラスタに正常に追加するには、認証方式を一時的にローカルに設定し、プライマリ ファブリック インターコネクトのローカル管理者資格情報を使用する必要があります。

1. ファブリック インターコネクトの電源を入れます。

ファブリックインターコネクトが起動すると、電源投入時セルフテストメッセージが表示されます。

2. システムがリースを取得する場合はステップ 6 に移動します。それ以外の場合は次のステップに進みます。
3. コンソール ポートに接続します。
4. インストール方式プロンプトに **gui** と入力します。

.

5. システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。
   - ファブリック インターコネクトの管理ポートの IPv4 または IPv6 アドレス。
   - ファブリック インターコネクトの管理ポートの IPv4 サブネット マスクまたは IPv6 プレフィクス。
   - ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IPv4 または IPv6 アドレス

（注） クラスタ設定では、設定時に両方のファブリック インターコネクトに同じ管理インターフェイスのアドレス タイプを割り当てる必要があります。

6. プロンプトから Web ブラウザに Web リンクをコピーし、Cisco UCS ファブリック インターコネクト セットアップ GUI 起動ページに移動します。

（注） 希望に応じて、次の 2 つのモードの間で選択できます。UCSM 管理対象と Intersight 管理対象ファブリック インターコネクト。

7. 「**Cisco UCS ファブリック インターコネクト セットアップ GUI**」起動ページで、**[簡易設定（Express Setup）]** を選択します。
8. **[簡易設定（Express Setup）]** ページで、ファブリック インターコネクト構成の詳細を入力します。

（注） Cisco UCS Manager 4.2(2) 以降から、GUI セットアップ方法を選択して、ファブリック インターコネクトを構成します。ファブリック インターコネクトのデフォルトが Intersight 管理対象モードに設定されている場合、確認中に変更を選択し、コンソールセットアップ方法のみで必要なモードを再び選択できます。

9. **[基本設定（Basic Settings）]** エリア：
   - **[ファブリックの設定（Fabric Setup）]** オプションに対して **[ファブリック B（Fabric B）]** が選択されていることを確認します。

10. **[System Setup (システム セットアップ)]** 領域の **[Admin Password of Master (マスターの管理者パスワード)]** フィールドに管理者アカウントのパスワードを入力します。

    [Manager の初期設定（Manager Initial Setup）] エリアが表示されます。

11. **[Manager の初期設定（Manager Initial Setup）]** エリアで表示されるフィールドは、最初のファブリック インターコネクトを IPv4 または IPv6 のどちらの管理アドレスに設定したかによって異なります。次のように、設定に適したフィールドに入力します。

フィールド	説明
[Peer FI is IPv4 Cluster enabled. ローカル ファブリック インターコネクト Mgmt0 IPv4 アドレスを指定してください	ローカル ファブリック インターコネクトの Mgmt0 インターフェイスの IPv4 アドレスを入力します。
[Peer FI is IPv6 Cluster enabled. ローカル ファブリック インターコネクトの Mgmt0 IPv6 アドレスを指定してください	ローカルのファブリック インターコネクトの Mgmt0 インターフェイスの IPv6 を入力します。

12. [送信（Submit）] をクリックします。

    セットアップ操作の結果がページに表示されます。

次の作業

Cisco Intersight を介して Intersight 管理対象ドメインを要求します。詳細については、「Intersight 管理対象モードのターゲット クレーム」を参照してください。

ファブリック インターコネクト パスワードのガイドライン

シスコでは強力なパスワードを使用することを推奨しています。そうしなかった場合、ファブリック インターコネクトの管理ユーザーに対するパスワードの強度チェックで、Cisco Intersight は次の要件を満たさないパスワードを拒否します。

- 8 文字以上、80 文字以下。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回以上繰り返す文字を含まない。

- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワードのディクショナリ チェックに合格する。たとえば、辞書に記載されている標準的な単語に基づいたパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- 空白にすることはできません。

Cisco UCS 6500 シリーズ ファブリック インターコネクトへの移行

Cisco UCS 6400 シリーズ ファブリック インターコネクト-B の Cisco UC5 6500 シリーズ ファブリック インターコネクト-B への置き換え

ここでは、Cisco UCS 6400 シリーズ ファブリック インターコネクトから Cisco UCS 6500 シリーズ ファブリック インターコネクトに移行するプロセスをつ名します。

手順

1. 移行中のトラフィック損失を最小に抑えるために、シャーシからファブリック A および B に冗長パスがあることを確認し、vNIC が冗長であるか、ファブリック フェイルオーバーが有効になっているかを確認してください。IFM の移行中は、処理中のパケット損失が予想されるため、次の一連の操作はメンテナンス時間帯にのみ実行することが最良です。
2. Cisco UCS 6400 シリーズ ファブリック インターコネクトのプラグを電源から抜いて電源を切ります。

   KVM セッションを使用して移行をモニタしている場合は、ファブリック インターコネクトを電源オフにしたときに KVM セッションの再接続が必要になることがあります。
3. ネットワーク管理ポート、L1/L2 ポート、ラック サーバー、シャーシ IOM/IFM ポート、ファブリック エクステンダ、アップリンク ポート、およびファイバー接続などのすべての接続を Cisco UCS 6400 ファブリック インターコネクト B から切断します。
4. Cisco UCS 6400 シリーズ ファブリック インターコネクト-B を Cisco UC5 6500 シリーズ ファブリック インターコネクト-B に置き換えます。
5. ネットワーク管理ポート、L1/L2 ポート、ラック サーバー、シャーシ IOM/IFM ポート、ファブリック エクステンダ、アップリンク ポート、ファイバー接続などのすべての接続を、新しい Cisco UCS 6500 シリーズ ファブリック インターコネクトに接続します。

   UCS 6500 シリーズ ファブリック インターコネクトへの接続には、適切なケーブルを使用する必要があります。詳細については、『Cisco UCS 6500 Series Fabric Interconnect Hardware Installation Guide』および『Cisco UCS 6500 Series Fabric Interconnect Data Sheet』を参照してください。

（注） UCSX-9508 シャーシの UCSX-I-9108-100G に IFM を移行することを選択できます。

UCS-IOM-2204/2208XP は、Cisco UCS 6500 シリーズ ファブリック インターコネクトではサポートされていません。Cisco UCS 5100 シリーズ シャーシの UCS-IOM-2408 に移行できます。

6. 新しい Cisco UCS 6500 シリーズ ファブリック インターコネクトに電源を接続すると、自動的にブートし、POST テストが実行されます。

   重要 コンソール ポートを端末に直接接続し、ブート シーケンスを確認します。ある時点で基本システム設定ダイアログが表示されます。ここでは、スイッチをピアインターコネクトとして構成します。Cisco UCS 6500 シリーズ ファブリック インターコネクトが以前に設定されているか、クラスタの一部であった場合、クラスタに追加する前にすべての設定情報を消去する必要があります。L1 および L2 接続をすぐに切断し、ファブリック インターコネクトにログインして、構成の消去を実行して、既存の設定を消去します。

7. Cisco UCS 6500 シリーズ ファブリック インターコネクト B の新しいポート ポリシーを作成して、ファブリック インターコネクトとの接続を反映します。
   - 必要に応じてイーサネット/FC ブレークアウト ポートを構成します。
   - 必要に応じて、ポート ロール/ポート チャネルを構成します。

8. クラスタのドメインプロファイルを編集し、新しい Cisco UCS 6500 シリーズ ファブリック インターコネクト B ポート ポリシーを参照するようにファブリック インターコネクト B ポート ポリシーを変更します。

（注） **ドメイン プロファイルの展開**は、置換ワークフローの一部になります。したがって、ポートポリシーの変更後にプロファイルを展開する必要はありません。ファブリック インターコネクト モデルが更新されていないため、ドメイン プロファイルの展開は失敗します。

9. **[操作（Operate）]** > **[ファブリック インターコネクト（Fabric Interconnects）]** に移動して、新しい Cisco UCS 6500 シリーズ ファブリック インターコネクトと古い Cisco UCS 6400 シリーズ ファブリック インターコネクトを表示します。

10. Cisco UCS 6400 シリーズ ファブリック インターコネクトの **[ファブリック インターコネクトを置換する（Replace Fabric Interconnect）]** オプションをクリックして、置換ワークフローを開始します。

11. 以下を確認します。
    - 接続解除されたファブリック インターコネクト クラスタがインベントリから削除されます。
    - ドメイン プロファイルが新しいファブリック インターコネクト クラスタに再割り当てされ、展開されます。

- サーバー、シャーシ、およびFEXがインベントリに登録され、新しいファブリック インターコネクト クラスタで検出されます。
- サーバおよびシャーシプロファイルは、ファブリック インターコネクト関連のポリシーを使用して再展開されます。

（注）

- 異なる IFM モデルが混在している場合、両方の IFM が同じになるまで、シャーシ プロファイルはプッシュされません。

  たとえば、IFM を UCSX-I-9108-25G から UCSX-I-9108-100G に移行し、移行前にシャーシ プロファイルを展開した場合、シャーシに異なるIFMモデルが混在している場合、シャーシ プロファイルは展開されません。シャーシ プロファイルは、シャーシ内の両方の IFM が UCSX-I-9108-100G に移行された後に自動的に展開されます。

Cisco UCS 6400 シリーズ ファブリック インターコネクト-A の Cisco UC5 6500 シリーズ ファブリック インターコネクト-A への置き換え

ファブリック インターコネクト A について上記の手順を繰り返し、UCS 6400 シリーズ ファブリック インターコネクトから UCS 6500 シリーズ ファブリック インターコネクトへの移行を完了します。

Cisco UCS 6500 シリーズ ファブリック インターコネクトと UCSX-9508 シャーシを使用した既存のドメインでの UCSX-I-9108-25G から UCSX-I-9108-100G IFM への移行

次の手順に従って、Cisco UCS 6500 シリーズ ファブリック インターコネクトおよびUCSX-9508 シャーシを使用して UCSX-I-9108-25G IFM から 100G IFM に移行します。

手順

1. 移行中のトラフィック損失を最小に抑えるために、シャーシからファブリック A および B に冗長パスがあることを確認し、vNIC が冗長であるか、ファブリック フェイルオーバーが有効になっているかを確認してください。IFM の移行中は、処理中のパケット損失が予想されるため、次の一連の操作はメンテナンス時間帯にのみ実行することが最良です。
2. 一度に 1 つの IFM を交換します。

   ファブリック インターコネクト B ポート ポリシーから開始し、移行する UCSX-I-9108-25G IFM に向けてサーバ ポートを構成解除します。サーバー ポートの構成が解除されると、ピア ファブリック インターコネクトがこれらの移行中の UCS シャーシのトラフィック転送を引き継ぎます。
3. ドメイン プロファイルを展開します。

4. 移行する各シャーシから、ピア Cisco UCS 6500 シリーズ ファブリック インターコネクト B と対応する UCSX-I-9108-25G IFM を接続しているケーブルを外します。
5. 移行中の UCSX-I-9108-25G IFM を外して、UCSX-I-9108-100G IFM に置き換えます。適切なケーブルを使用して、UCSX-I-9108-100G IFM をピア Cisco UCS 6500 シリーズ ファブリック インターコネクト B に接続します。詳細については、「Cisco UCS 6500 シリーズ ファブリック インターコネクト データ シート」を参照してください。

   この時点で、移行する UCS シャーシには UCSX-I-9108-25G と UCSX-I-9108-100G IFM が混在しています。
6. ファブリック インターコネクト B ポート ポリシーを設定してから、ドメイン プロファイルを展開します。IFM とファブリック インターコネクトの間で 100GbE リンクが確立されていることを確認します。
   - UCSX-I-9108-100G IFM は、ファームウェアがファブリック インターコネクトと同じでない場合、自動アップグレードされます。
   - IFM がオンラインになると、自動的に検出され、インベントリされます。シャーシ内のブレードが検出され、サーバープロファイルが自動的に展開されます。サーバーがリブートされたり、中断されたりすることはありません。
   - シャーシ プロファイルは、シャーシ内の両方の IFM が UCSX-I-9108-100G に移行された後に自動的に展開されます。
7. Cisco UCS 6500 シリーズ ファブリック インターコネクト B への IFM 移行が完了したら、手順 3 ～ 7 を繰り返して、Cisco UCS 6500 シリーズ ファブリック インターコネクト-A に接続されている他の UCSX-I-9108-25G を交換し、UCSX-I-9108- UCS ドメインの 100G IFM 移行を完了します。

ファブリック インターコネクトのビュー

ファブリック インターコネクトの詳細ビュー

[ファブリック インターコネクト（Fabric Interconnects）] テーブル ビューでファブリック インターコネクトを選択すると、そのファブリック インターコネクトに固有の情報を含む [詳細（Details）] ページが表示されます。ファブリック インターコネクトが **[未接続（Not Connected）]** ステータスの場合、デバイスの詳細を表示して問題を解決できます。トラブルシューティングのその他の推奨事項を表示するには、「トラブルシューティング」を参照してください。

ファブリック インターコネクトの **[健全性（Health）]** ステータスの他に、[ファブリック インターコネクトの詳細（Fabric Interconnects Details）] ページには次の情報を表示できます。

- **名前（Name）**：ファブリック インターコネクトの名前が表示されます。

- **ピア スイッチ（Peer Switch）**：表示するデバイスに応じて、ファブリック インターコネクト A または B の名前。[ピア FI（Peer FI）] をクリックし、もう一方のファブリック インターコネクトの詳細を表示します。
- ユーザー ラベル（**User Label**）：ファブリック インターコネクトに割り当てられたユーザー ラベル。
- **モデル（Model）**：ファブリック インターコネクトのモデル番号。
- **組織（Organizations）**：ファブリック インターコネクトが割り当てられている組織が表示されます。
- **拡張モジュール（Expansion Modules）**：ファブリック インターコネクトの拡張モジュールの数。
- **シリアル（Serial）**：ファブリック インターコネクトのシリアル番号。
- **管理 IP（Management IP）**：ファブリック インターコネクトの管理インターフェイスの IP アドレス。
- **スイッチ プロファイル（Switch Profile）** ファブリック インターコネクトが属する UCS ドメイン用に作成されたスイッチ プロファイルの名前。
- **スイッチ プロファイルのステータス（Switch Profile Status）**：ファブリック インターコネクトに関連付けられているスイッチ プロファイルの現在のステータス。
- **バンドル バージョン（Bundle Version）**：ファブリック インターコネクトがアップグレードされたファームウェア バンドルのバージョン。
- **NX-OS バージョン（NX-OS Version）**：ファブリック インターコネクトで実行中のファームウェア バージョン。
- **ポート（Ports）**：ポートの総数
- **使用中（Used）**：使用ポートの数
- **使用可能（Available）**：使用可能なポートの数。
- [タグ（Tags）]：ファブリック インターコネクトの既存のタグ。[管理（Manage）] タグから新しいタグの追加や既存のタグの変更を行えます。

Properties 領域に、ファブリック インターコネクトのグラフィカルビューが表示されます。

（注） Cisco UCS ファブリック インターコネクト 9108 100G の場合、すべてのポートのレイアウトを含む前面図のみが表示されます。

Health Overlay 機能を使用すると、ファブリック インターコネクトのポートのヘルスをモニタできます。また、この領域には次の情報が表示されます。

- **モード（Mode）**：UCS ファブリック インターコネクトは、イーサネットまたはファイバ チャネルという、2 種類のメイン スイッチング モードで動作します。これらのモードは相

互に独立しています。サーバとネットワーク間またはサーバとストレージデバイス間で、ファブリック インターコネクトがデバイスとして動作する方法を決定します。

- **イーサネット モード**：イーサネット スイッチング モードにより、サーバとネットワーク間のスイッチング デバイスとしてファブリック インターコネクトがどのように動作するのかが決まります。ファブリック インターコネクトは、次のイーサネット スイッチング モードのいずれかで動作します。
  - **エンドホスト モード**では、ファブリック インターコネクトが、仮想ネットワークインターフェイスカード（vNIC）を介して接続されているすべてのサーバ（ホスト）に代わって、ネットワークに対するエンド ホストとして動作できます)。
  - **スイッチモード**：ファブリック インターコネクトで STP を実行して、ループを回避できるようにします。ブロードキャストおよびマルチキャストパケットは、従来の方法で処理されます。
- **FC モード**：ファイバ チャネル スイッチング モードは、サーバとストレージ デバイス間のスイッチング装置としてファブリック インターコネクトがどのように動作するかを決定します。ファブリック インターコネクトは、次のファイバ チャネル スイッチング モードのいずれかで動作します。
  - **エンドホスト モード**：エンドホストを使用すると、ファブリック インターコネクトは、仮想ホスト バス アダプタ（vHBA）を介して接続されているすべてのサーバ（ホスト）に代わって、接続されているファイバ チャネル ネットワークに対するエンド ホストとして動作することができます。
  - **スイッチ モード**：スイッチ モードを使用して、ファブリック インターコネクトをストレージ デバイスに直接接続することが—できます。
- **Admin Evac State**：ファブリック インターコネクトトラフィックの退避状態を指定します。次のいずれかのオプションになります。
  - **無効**：ファブリック インターコネクトでトラフィックを再開します。
  - **有効**：ファブリック インターコネクトでトラフィックを停止します。
- **Oper Evac State**：ファブリック インターコネクト トラフィックの運用上の退避状態を指定します。

- **FC ゾーンカウント**
  - **FC Zone Limit**：このファブリック インターコネクトで許可されているファイバ チャネル ゾーンの最大数。
  - **FC User Zone Limit**：このファブリック インターコネクトで許可されているユーザ作成のファイバ チャネル ゾーンの最大数。
  - **FC Zone Count**：このファブリック インターコネクトで定義されているファイバ チャネル ゾーンの数。

- **FC User Zone Count**：このファブリック インターコネクトで定義されているユーザ作成のファイバ チャネル ゾーンの数。

- **アクセス**
  - **IP Address**：ファブリック インターコネクトと通信するときに使用するIPアドレス。
  - **Subnet Mask**：IP アドレスに関連付けられたサブネット マスク。
  - **Default Gateway**：IP アドレスに関連付けられたゲートウェイ。
  - **MAC**：MAC アドレス

- **VLANの詳細**
  - **VLAN Port Limit**：このファブリック インターコネクトで許可されているファイバ チャネル ゾーンの最大数。
  - **Access VLAN Port Count**：利用可能な VLAN アクセス ポートの数。
  - **Border VLAN Port Count**：利用可能な VLAN ボーダー ポートの数。
  - **Compressed Optimization Sets**：VP 最適化グループの数。
  - **Compressed VLAN Port Count**：圧縮 VLAN ポートの数。
  - **Uncompressed VLAN Port Count**：非圧縮 VLAN ポートの数。
  - **予約済み VLAN 範囲（Reserved VLAN Range（Reserved VLAN Range）**：システムで使用するために予約されている VLAN ID の範囲。

- **ファブリック インターコネクト ライセンス**

  このセクションは、Cisco UCS 6536 ファブリック インターコネクトおよびCisco UCS ファブリック インターコネクト9108 100Gにのみ関連します。これらのファブリック インターコネクト（FI）は、すべてのポートとソフトウェア機能をアクティブにする永久ソフトウェアライセンスをサポートします。

（注） このセクションは、ポートベースのラインセンスが必要な Cisco UCS 6454 および 64108 ファブリック インターコネクトには適用されません。これらのファブリック インターコネクトの未使用ポートをアクティブにするには、ポートごとに製品アクティベーション キーをインストールする必要があります。

サポート対象のファブリック インターコネクト モデル

Intersight 管理モードでサポートされるファブリック インターコネクト モデルは次のとおりです。

UCS FI-6454

UCS-FI-64108

UCS-FI-6536

UCSX-S9108-100G

UCSM管理モードでサポートされるファブリック インターコネクト モデルは次のとおりです。

UCS-FI-6248UP、UCS-FI-6296UP

UCS-FI-6332、UCS-FI-6332-16UP

UCS-FI-M-6324

UCS FI-6454

UCS-FI-64108

UCS-FI-6536

アラーム

Intersight は、管理対象のすべての UCS と HyperFlex システムに関するアラームの追跡とセットアップを行うための障害監視機能を提供しています。発生したセットアップの失敗（フォールト）またはしきい値に関するアラームを通知します。Intersight でのアラームには、障害が発生した時点で影響を受けたオブジェクトの動作状態に関する情報が含まれています。特定のアラームをクリックして障害コード、ソース タイプおよび名前、障害が発生したコンポーネント、障害の説明を表示します。

（注） アラームを生成するには、Intersight管理対象デバイスがファームウェアバージョン4.1（3）以降で実行されている必要があります。

アラームの詳細を表示するには、いずれかのカテゴリをクリックします。

- **All(Info)**：重大と警告の両方の障害の合計数を表示します。
- **Critical**：重大な障害の総数が表示されます。サービスに影響を与える状態で、早急な是正措置を必要とする場合に発生します。たとえば、このシビラティ（重大度）は管理対象オブジェクトがサービス停止状態になっており、その機能を早急に回復させる必要があることを示している場合があります。
- **Warning**：警告障害の総数が表示されます。潜在的または差し迫ったサービスに影響する障害が発生した場合に発生します。

  この障害は、システムに重大な影響を与えるものであることも、すぐに影響を与えたりするものではないこともあります。警告ステータスは、障害を診断し、問題を修正して適切に処理し、サービスに影響を与えるさらに重大な障害の発生を防ぐ必要があることを示しています。

ファブリック インターコネクトのインベントリ ビュー

[Fabric Interconnects] テーブルビューでファブリックインターコネクトを選択すると、**Inventory** タブでコンポーネントのインベントリを表示できます。

選択したファブリックインターコネクトについて、次の各コンポーネントの詳細を表示できます。

- **[Ports & Port Channels]**：ファブリックインターコネクトのイーサネットポート、FC ポート、イーサネットポートチャネル、および FC ポートチャネルの概要を表示できます。特定のポートをクリックすると、そのポートのプロパティとグラフィカルビューを表示できます。

  このビューからポートまたはポートチャネルを **Enable** または **Disable** は無効にできます。ポートを無効にすると、トラフィックが中断する可能性があります。無効なポートに接続されているデバイスもオフラインになります。ポートチャネルを無効にすると、メンバーポートも無効になります。

  ファブリック インターコネクト インベントリ ビューの **[リセット（Reset）]** オプションを使用すると、サーバー ロールが設定されているポートまたはイーサネット ポートをリセットできます。**リセット（Reset）** アクションは、FEX インベントリ ビューの FEX のバックプレーンポートでも使用できます。

（注） このアクションは、設定が正しくないためにポートが収束していない場合にのみ試行する必要があります。ポートをリセットにすると、トラフィックが中断する可能性があります。

- **ファンモジュール**：ファブリックインターコネクトのファンモジュールの概要を確認できます。特定のファンモジュールをクリックすると、ファンモジュールのファンのリスト、およびそのファンモジュールのプロパティとグラフィカルビューを表示できます。
- **PSU**：ファブリックインターコネクトの電源装置（PSU）の概要を確認できます。特定の PSU をクリックすると、その PSU のプロパティとグラフィカルビューを表示できます。
- **[ローカルストレージ（Local Storage）]**：サイズや現在の使用状況などの詳細を含む、ファブリックインターコネクトのパーティションの概要を表示できます。

ファブリック インターコネクトの接続ビュー

[接続（Connections）] ビューには、ファブリック インターコネクトに直接または間接的に接続されているすべてのコンポーネント（サーバ、シャーシ、ファブリック エクステンダ（FEX）など）のリストが表示されます。

（注） Cisco UCS Fabric Interconnects 9108 100G は現在、ファブリック エクステンダ、ラック サーバ、または Intersight マネージド モードでのシャーシの追加はサポートされていません。

選択したファブリック インターコネクトで使用可能な情報に応じて、次の情報が表示されます。

- **[コンピューティング（Compute）]**
  - **[サーバ（Servers）]**：ファブリック インターコネクトに接続されているすべてのサーバの詳細。これらの詳細は、名前、Name、Health、User Label、Slot Id、Management IP、Model、および Serial です。
  - **[シャーシ（Chassis）]**：ファブリック インターコネクトに接続されているすべてのシャーシの詳細。これらの詳細は、Name、Health、Model、および Serial です。

（注） Cisco UCS ファブリック インターコネクト 9108 100G の場合、再稼働、デコミッション、削除などのシャーシアクションは許可されません。

- **[ネットワーク（Network）]**
  - **[ファブリック エクステンダ（Fabric Extenders）]**：ファブリック インターコネクトに接続されているファブリックエクステンダの詳細。これらの詳細は、Name、Health、Model、Vendor、および Serial です。

（注） Cisco UCS ファブリック インターコネクト 9108 100G の場合、Fabric Extender（FEX; ファブリック エクステンダ）は現在サポートされていません。

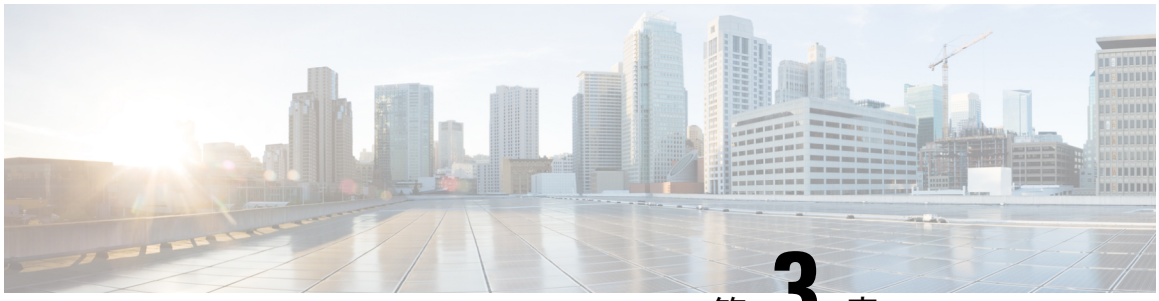
- **[廃止（Decommissioned）]**
  - **[デバイス（Devices）]**：デコミッションされたデバイスの詳細。これらの詳細は、Type、Model、Serial、Decommissioned Date です。

ファブリックインターコネクトのUCSドメインプロファイル ビュー

[UCS ドメインプロファイル（UCS Domain Profile）] ビューには、ポート設定、VLAN および VSAN 設定、および UCS ドメイン設定がグラフィック表示されます。さらに、次の情報が表示されます。

- **[詳細（Details）]**
  - **[ステータス（Status）]**：ファブリックインターコネクトペアから UCS ドメインプロファイルの割り当てを解除します
  - **[名前（Name）]**
  - **[ファブリック インターコネクト A（Fabric Interconnect A）]**：ファブリック インターコネクト A の名前。
  - **[ファブリック インターコネクト B（Fabric Interconnect B）]**：ファブリック インターコネクト B の名前。
  - **[最終更新日（Last Update）]**：Last Update：UCS ドメインプロファイルが最後に更新された日時。
  - **[説明（Description）]**：UCS ドメインプロファイルのオプションの説明
- **[タグ（Tags）]**：ドメイン（Domain）の既存のタグ。**[管理（Manage）] タ**グから新しいタグの追加や既存のタグの変更を行えます。
- **[ポリシー（Policies）]**

  UCS ドメイン プロファイルにアタッチされているポリシーを表示します。**[ポリシー（Policies）] ペ**インには、ポート、VLAN、VSAN、および UCS ドメイン設定の詳細が表示されます。ポートロール、ポートチャネル、および関連付けられたポリシーのリストを含む、ファブリックインターコネクトのポート設定がグラフィカルに表示されます。
  VLAN、VSAN、および UCS ドメイン設定には、選択したドメインプロファイルに関連付けられたドメイン ポリシーがリストされます。



第 3 章

シャーシと FEX のライフサイクル

- シャーシおよびファブリック エクステンダの検出とアクション （39 ページ）
- シャーシの詳細ビュー （42 ページ）
- シャーシのインベントリ ビュー （43 ページ）
- シャーシの接続ビュー （44 ページ）
- ファブリック エクステンダの詳細ビュー （44 ページ）
- ファブリック エクステンダのインベントリ ビュー （45 ページ）
- ファブリック エクステンダの接続ビュー （46 ページ）

シャーシおよびファブリック エクステンダの検出とアクション

シャーシおよびファブリック エクステンダの検出

ファブリック インターコネクトに接続されているシャーシおよびファブリック エクステンダ（FEX）は、Cisco Intersight で自動的に検出されます。ファブリック インターコネクトに接続されたシャーシと FEX を検出するには、ファブリック インターコネクトが Cisco Intersight で要求されていることを確認します。

ファブリック インターコネクトが要求されたら、次の手順を実行します。

1. サーバ ポートを両方のファブリック インターコネクトに接続します。たとえば、ポート 1 と 2 を FI-A に、ポート 3 と 4 を FI-B に接続します。
2. UCS ドメイン プロファイルを使用して、両方のファブリック インターコネクトのサーバ ポートを設定します。*[UCS* ドメイン プロファイルの作成（*Creating a UCS Domain Profile*）*]* では、UCS ドメイン プロファイルの作成と UCS ファブリック インターコネクト ドメインへの割り当てに関する詳細情報を提供します。

サーバポートを設定して適用すると、ファブリック インターコネクトに接続されているすべてのシャーシと FEX が自動的に検出されます。ファームウェア バージョンがファブリック インターコネクトのファームウェア バージョンと一致しない場合、検出時にシャーシと FEX はファブリック インターコネクトとファームウェアを自動同期します。このため、シャーシと FEX

が GUI に表示されるまでに 25ー30 分かかる場合があります。nxos CLI で show fex コマンドを使用すると、シャーシと FEX のステータスを確認できます。

シャーシアクション

左側のナビゲーションパネルで、**[シャーシ（Chassis）]** をクリックして **[シャーシ（Chassis）]** テーブルビューを表示します。次の操作を実行して、1 つ以上のシャーシを管理できます。

シャーシ アクション

- **再検出**：シャーシの検出プロセスを開始して、シャーシ インベントリ プロセスが開始します。
- **デコミッション**：シャーシと IOM のインベントリを削除します。デコミッションされたシャーシは、最終的にリコミッションすることが予測されるので、シャーシ ID を含むシャーシ情報部分は Cisco Intersight によって保持されています。[デコミッション（Decommission）] は、シャーシは物理的に存在し接続されているものの、一時的に設定から削除する場合に実行します。
- **[削除（Remove）]**：物理的に削除されたシャーシの設定を Cisco Intersight から削除します。

  システムから物理的にシャーシを取り外す前に、シャーシが接続されているサーバー ポートの構成を解除してください。

  シャーシを追加する必要がある場合、前に取り外したシャーシを再び Cisco Intersight 構成に追加する場合は、再接続して再度検出する必要があります。検出時に、Cisco Intersight は、以前に割り当てた ID とは異なる新しい ID をシャーシに割り当てます。
- **[リコミッション（Recommission）]**：シャーシと IOM がオンラインに戻り、シャーシ検出プロセスが開始されてから、シャーシ インベントリ プロセスが開始されます。このアクションが完了を実行すると、シャーシおよびシャーシ内のすべてのサーバにアクセスできるようになります。

  廃止されたシャーシのリストは、**[デバイス（Devices）]** 領域で確認できます。**[ファブリック インターコネクト（Fabric Interconnects）]** > ***[ファブリック インターコネクト名（Fabric Interconnect Name）]*** > **[接続（Connections）]** > **[解放済み（Decommissioned）]** の下にあります。

  シャーシをリコミッションさせるときに、シャーシIDを構成するオプションがあります。
- **[ロケータをオン/オフにする（Turn On/Off Locator）]**：LED ロケータをオン/オフに切り替えます。

（注） このオプションは、Intersight管理モードのサーバでのみ使用できます。

- **シャーシ スロット**の電源の再投入：シャーシ スロットの電源の再投入は、応答のないデバイスの回復を試みます。この操作は、省略記号（...）アイコンをクリックして、シャーシ テーブル ビューとシャーシ接続ビューから開始できます。

（注） サーバー スロットの電源を再投入すると、サーバーがダウンし、アプリケーション サービスに影響を与える可能性があります。したがって、このオプションは、そのシャーシ スロット内のサーバーに関する問題をデバッグする際に注意して使用する必要があります。

- **[ファームウェアのアップグレード（Upgrade Firmware）]**：このアクションは、Cisco UCS S3260 シャーシでのみサポートされます。
- **[テクニカル サポート バンドルの収集（Collect Tech Support Bundle）]**：テクニカル サポートバンドルを収集します。アカウント管理者は、デバイスを選択し、選択したデバイスのテクニカル サポート バンドル ファイルを収集できます。ダウンロードしたファイルには、**[管理（Admin）]** > **[テクニカル サポート バンドル（Tech Support Bundles）]** セクションに移動してアクセスできます。このファイルは、問題をトラブルシューティングするために TAC チームと共有できます。

FEX アクション

左側のナビゲーションパネルで、**[ファブリック インターコネクト（Fabric Interconnects）]** > ***[ファブリック インターコネクト名（Fabric Interconnect Name）]*** > **[接続（Connections）]** > **[ファブリック エクステンダ（Fabric Extenders）]** をクリックして、**[FEX]** テーブル ビューを確認します。次の操作を実行して、1 つ以上の FEX を管理できます。

FEX アクション

- **[解放（Decommission）]**解放は、FEX は物理的に存在し接続されているものの、一時的に Cisco Intersight 設定から削除する場合に実行します。このアクションにより、FEX がオフラインになり、FEX インベントリが削除されます。解放された FEX は最終的に再稼働することが予測されるので FEX を含むシャーシ情報部分は Cisco Intersight によって、将来使用するために保持されています。
- **[削除（Remove）]**：FEX を削除するには、システムから FEX を物理的に削除します。FEX の物理的な削除が完了すると、その FEX の設定が Cisco Intersight から削除されます。

  削除した FEX を Cisco Intersight 設定に戻すには、ファブリック インターコネクトで設定されているサーバポートに再接続する必要があります。FEX は自動的に検出されます。ディスカバリ中に、Cisco Intersight は、以前に割り当てられた ID とは異なる新しい ID を FEX に割り当てます。
- **[再稼働（Recommission）]**：FEX を再稼働すると、FEX がオンラインに戻り、FEX ディスカバリプロセスが開始され、次に FEX インベントリプロセスが開始されます。このアクションが完了すると、FEX にアクセスできます。

解放された FEX のリストは、**[デバイス（Devices）]** 領域で確認できます。**[ファブリック インターコネクト（Fabric Interconnects）]** > ***[ファブリック インターコネクト名（Fabric Interconnect Name）]*** > **[接続（Connections）]** > **[解放済み（Decommissioned）]** の下にあります。

- **[ロケータをオンにする（Turn On Locator）]**：選択した FEX の LED ロケータをオンにします。ロケータは、大規模データセンター環境で管理者が特定のノードを見つけるのに役立つインジケータです。
- **[ロケータをオフにする（Turn Off Locator）]**：選択した FEX の LED ロケータをオフにします。ロケータは、大規模データセンター環境で管理者が特定のノードを見つけるのに役立つインジケータです。

シャーシの詳細ビュー

シャーシテーブルビューでシャーシを選択すると、そのシャーシに固有の情報を含む [詳細（Details）]ページが表示されます。シャーシの **[健全性（Health）]** ステータスの他に、[シャーシの詳細（Chassis Details）] ページには次の情報を表示されます。

- **[名前（Name）]**
- **[シリアル（Serial）]**：シャーシのシリアル番号
- **[モデル（Model）]**：シャーシのモデル番号（例：UCSB-5108-AC2）
- **[リビジョン（Revision）]**：シャーシのリビジョン番号
- **[部品番号（Part Number）]**：シャーシの部品番号
- **[管理モード（Management Mode）]**：シャーシの管理モード。
- **[契約ステータス（Contract Status）]**：関連する契約の現在の有効性に基づく、管理対象シャーシの契約ステータス。
- **[UCS ドメイン（UCS Domain）]**：UCS Domain：選択したシャーシが属する UCS ドメインの名前
- **[シャーシ プロファイル（Chassis Profiles）]**：関連するシャーシ プロファイル構成ステータスを表示します。
- **[タグ（Tags）]**：デフォルトでは、選択したオブジェクトの既存のタグが表示されます。**[管理（Manage）]** をクリックして、新しいタグを追加するか、既存のタグを変更します。

[プロパティ] 領域には、シャーシの前面図と背面図、シャーシのヘルス オーバーレイ、およびシャーシとそのコンポーネントのハードウェア プロパティの概要がグラフィカルに表示されます。

（注）：

- シャーシの詳細ビューは、Cisco UCS S3260 シャーシおよび Intersight 管理モード シャーシでサポートされています。
- Cisco UCS X シリーズ ダイレクトの場合、シャーシ（UCSX-9508）の背面図が表示されます。これは、Cisco UCS ファブリック インターコネクト 9108 100G の背面図と同じです。

[Alarms（アラーム）]：は、管理対象のすべての UCS システムに関するアラームの追跡とセットアップを行うための障害監視機能を提供します。発生したエンドポイントの障害またはしきい値に関するアラームを通知します。

シャーシのインベントリ ビュー

シャーシが検出されと、そのすべてのコンポーネントのインベントリが使用可能になります。**[シャーシ（Chassis）]**：テーブル ビューでシャーシを選択すると、**[インベントリ（Inventory）]** タブでコンポーネントのインベントリを表示できます。

選択したシャーシについて、次の各コンポーネントの詳細を表示できます。

- **[IO モジュール（IO Modules）]**：シャーシ内の IO モジュールの名前、ベンダー、モデル番号、管理 IP アドレス、動作状態、およびファームウェア バージョンを表示できます。特定の IO モジュールをクリックすると、全般プロパティ、バックプレーン ポートとファブリック ポートの詳細、グラフィック ビュー、および IO モジュールの正常性オーバーレイを表示できます。

  アクション：IO モジュールまたはそのピア IO モジュールを [シャーシインベントリ ビュー（Chassis Inventory View）] からリセットできます。対応する IO モジュールを介してピア IO モジュールをリセットすると、ピア IO モジュールのリブートが開始されます。これは、Intersight から直接到達できないピア IO モジュールを回復するのに役立ちます。

  - Cisco UCS X シリーズ シャーシでは、各インテリジェント ファブリック モジュール（IFM）にファンモジュールが含まれています。ファン モジュールをクリックすると、ファンのプロパティと動作状態を表示できます。
  - Cisco UCS X シリーズ ダイレクト シャーシ（UCSX-9508）の場合、IFM セクションには「ファブリック インターコネクト モジュール（インテリジェント ファブリック モジュール）」というラベルが付いています。IFM セクション内に、[ファブリック ポート（Fabric Ports）] サブセクションは存在しません。

- **[XFM モジュール（XFM Modules）]**：シャーシ内の X-Fabric モジュール（XFM）の概要を確認できます。特定の XFM をクリックして、ファン モジュールの詳細を表示します。ファン モジュールをクリックすると、ファンの ID、モデルと動作状態を表示できます。

（注） XFM（UCSX-F-9416）スロットは、UCX 9508 シャーシのそれぞれの 2 つのスロットに存在する必要があります。

- [サーマル（Thermal）]：**[サーマル（Thermal）]** セクションの **[一般（General）]** タブには、サーマル構成と統計が表示されます。**[ファンモジュール（Fan Modules）]** タブには、ファンモジュールの名前、ファンの数、モデル番号、および動作状態が表示されます。特定のファン モジュールをクリックすると、ファン モジュールの一般的な詳細、ファンの詳細、グラフィック ビュー、および正常性オーバーレイを表示できます。
- **[電力（Power）]**：[電力（Power）]セクションの**[一般]**タブには、電力構成と統計が表示されます。**[PSU]** タブには、PSU（電源装置）の名前、モデル番号、ベンダー名、シリアル番号、および動作状態が表示されます。特定の PSU をクリックすると、PSU の一般的な詳細、グラフィック ビュー、および正常性オーバーレイを表示できます。
- **[サーバー（Servers）]**—選択したシャーシのサーバーの名前、スロットID、モデル番号、およびシリアル番号を表示できます。

シャーシの接続ビュー

[接続（Connections）]ビューには、シャーシに直接または間接的に接続されているすべてのコンポーネント（ファブリックインターコネクトやサーバなど）のリストが表示されます。

選択したシャーシで使用可能な情報に応じて、次の情報が表示されます。

- **[ネットワーク（Network）]**
  - **[スイッチ（Switches）]**：シャーシに接続されているファブリック インターコネクトの詳細を表示します。これらの詳細は、名前（Name）、健全性（Health）、モデル（Model）、ベンダー（Vendor）、およびシリアル（Serial）です。

ファブリック エクステンダの詳細ビュー

FEX テーブルビューでファブリック エクステンダ（FEX）を選択すると、シャーシに固有の情報を含む[詳細（Details）]ページが表示されます。FEX の **[健全性（Health）]** ステータスの他に、[FEX の詳細（FEX Details）] ページには次の情報を表示されます。

- **[名前（Name）]**
- **[シリアル（Serial）]**：ファブリック エクステンダのシリアル番号
- **[モデル（Model）]**：ファブリック エクステンダのモデル番号
- **[ベンダー（Vendor）]**：製造元の名前
- **[リビジョン（Revision）]**：ファブリック エクステンダのリビジョン番号
- **[部品番号（Part Number）]**：ファブリック エクステンダの部品番号
- **[ポート（Ports）]**：ファブリックエクステンダのポートの総数と動作ステータス。ステータスは以下のいずれかになります。

- **[使用済み（Used）]**：ファブリック インターコネクトおよびサーバに現在接続されているポートの数
- **[使用可能（Available）]**：ファブリック エクステンダで使用可能なポートの数

- **[タグ（Tags）]**：ファブリック インターコネクトの既存のタグ。**[管理（Manage）]** タグでは、新しいタグの追加や既存のタグの変更を行えます。

ファブリック エクステンダのインベントリ ビュー

ファブリック エクステンダ（FEX）が検出されると、そのすべてのコンポーネントのインベントリが使用可能になります。**[FEX]F** テーブル ビューで FEX を選択すると、**[インベントリ（Inventory）]** タブでそのコンポーネントのインベントリを表示できます。

選択した FEX について、次の各コンポーネントの詳細を表示できます。

- **[ポート（Ports）]**：選択した FEX のすべての **[バックプレーン ポート（Backplane Ports）]** と **[ファブリック ポート（Fabric Ports）]** の詳細。

  [バックプレーン ポート（Backplane Ports）] テーブルには、ホスト ポートであるサーバ ポートが表示されます。これには、ポートの **[名前（Name）]**、**[ステータス（Status）]**、ポートが属する **[ポート チャネル ID（Port Channel ID）]**、ポートの **[速度（Speed）]**、および **[ピア（Peer）]** サーバ ポートなどの情報が含まれます。

  [ファブリック ポート（Fabric Ports）] テーブルには、ファブリック インターコネクトに接続されているネットワーク ポートが表示されます。これには、ポートの **[名前（Name）]**、**[ステータス（Status）]**、所属する **[ポート チャネル ID（Port Channel ID）]**、接続先のファブリック インターコネクトの **[スイッチ スロット ID（Switch Slot ID）]**、**[ピア（Peer）]** ファブリックインターコネクト、およびファブリック インターコネクトの **[スイッチ ポート ID（Switch Port ID）]** などの情報が含まれます。

  また、各ポートの詳細なハードウェア情報とグラフィック表示も含まれます。

- **[ファン モジュール（Fan Modules）]**：**[名前（Name）]**、**[ファン (Fans)]**、**[モデル（Model）]**、**[ステータス（Status）]** など、FEX 上のすべてのファン モジュールの詳細。

  また、各ファンモジュールとその中のファンの詳細なハードウェア情報とグラフィック表示も含まれます。

- **[PSU]**：**[名前（Name）]**、**[ID]**、**[モデル（Model）]**、**[ベンダー（Vendor）]**、**[シリアル（Serial）]**、**[ステータス（Status）]** など、FEX の電源ユニット（PSU）の詳細。

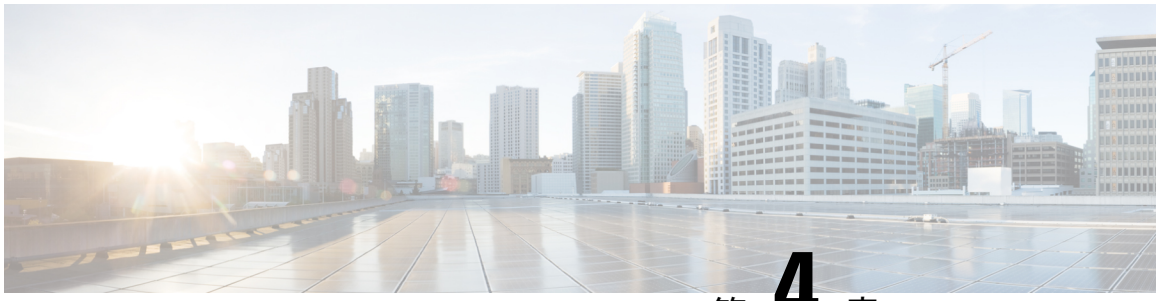
  また、各 PSU の詳細なハードウェア情報とグラフィック表示も含まれています。

ファブリック エクステンダの接続ビュー

[接続（Connections）] ビューには、ファブリック エクステンダ（FEX）に直接または間接的に接続されているすべてのコンポーネント（サーバやファブリック インターコネクトなど）のリストが表示されます。

選択した FEX で使用可能な情報に応じて、次の情報が表示されます。

- **[コンピューティング（Compute）]**
  - **[サーバ（Servers）]**：FEX に接続されているすべてのサーバの詳細。これらの詳細は、名前（Name）、健全性（Health）、ユーザ ラベル（User Label）、モデル（Model）、およびシリアル（Serial）です。
- **[ネットワーク（Network）]**
  - **[スイッチ（Switches）]**：FEX に接続されているファブリックインターコネクトの詳細を表示します。これらの詳細は、名前（Name）、健全性（Health）、モデル（Model）、ベンダー（Vendor）、およびシリアル（Serial）です。



第 4 章

サーバのライフサイクル

- サーバの検出とアクション （47 ページ）
- サーバ インベントリの表示 （51 ページ）
- ハードウェア互換性リスト（HCL）との準拠 （57 ページ）

サーバの検出とアクション

シャーシまたは FEX が検出されると、シャーシに接続されたブレードサーバまたは FEX に接続されたラックサーバが自動的に要求され、検出されます。*[*シャーシおよび *FEX* のディスカバリと操作（*Chassis and FEX Discovery and Operations*）*]* では、このプロセスに関する情報を提供します。サーバを要求して検出するには、工場出荷時の状態になっている必要があります。

ファブリック インターコネクトに直接接続されているラックサーバの場合は、ファブリック インターコネクトの要求後に次の手順を実行します。

1. サーバ ポートを両方のファブリック インターコネクトに接続します。たとえば、ポート 1 と 2 を FI-A に、ポート 3 と 4 を FI-B に接続します。
2. 両方のファブリック インターコネクトのサーバ ポートを構成します。

検出されたサーバは **[サーバ（Servers）]** ページに表示されます。

サーバの操作

サーバアクションを使用すると、サーバを管理できます。Cisco Intersight で [サーバ（Servers）] をクリックすると、[サーバ テーブル（Servers Table）] ビューが表示されます。[サーバ テーブル（Servers Table）] ビューページで、省略記号（…）アイコンをクリックしてサーバ アクションを実行します。

[サーバ アクション（Server Actions）]：サーバを管理するために次の操作を実行できます。

- **[電源（Power）]**
  - **[電源オン/オフ（Power On/Off）]** — サーバーの電源をオン/オフにします。
  - **[電源サイクル（Power Cycle）]**：サーバの電源をオフにしてからオンに戻します。

- **[ハード リセット（Hard Reset）]**：サーバを再起動します。
- **[OS のシャットダウン（Shut Down OS）]**：オペレーティング システムでサポートされている場合、サーバをシャットダウンします。

- **[システム（System）]**
  - **[ロケータをオン/オフにする（Turn On/Off Locator）]**：LED ロケータをオン/オフに切り替えます。
  - **[CMOS のリセット（Reset CMOS）]**：BIOS 構成設定を元の状態にリセットします。これにより、サーバが正常な状態でない場合の回復に役立ちます。CMOS をリセットするオプションは、サーバの電源がオフの場合にのみ表示されます。リセットを完了するには、サーバの電源をオンにする必要があります。[CMOS のリセット（Reset CMOS）] 確認ウィンドウにあるトグル ボタンを使用して、サーバの電源をオンにする追加オプションがあります。

（注） このオプションは、Intersight 管理モードのサーバでのみ使用できます。

  - **[フロント パネルのロック（Lock Front Panel）]**：サーバの物理的な電源ボタンをロックします。フロント パネルがすでにロックされているサーバの場合、このオプションは **[フロント パネルのロック解除（Unlock Front Panel）]** と表示されます

（注） このオプションは、Intersight 管理モードのサーバでのみ使用できます。

  - **[再検出（Rediscover）]**：サーバとそのサーバのすべてのエンドポイントを再検出します。
  - **[解放（Decommission）]**：サーバを解放し、Cisco UCS 設定からサーバを削除します。ただし、サーバのハードウェアは Cisco UCS インスタンスに物理的に残っています。
  - **[シスコ IMC の再起動（Reboot IMC）]**：Cisco IMC を再起動します。
  - **証明書**：
    - **[KMIP クライアント証明書の設定（Set KMIP Client Certificate）]**：KMIP サーバと Cisco IMC 間の安全な通信を確保するために KMIP クライアント証明書を設定します。
    - **[IMC 証明書（IMC certificates）]**：サードパーティ管理の認証局（CA）からサーバの証明書と秘密キーを設定します。このオプションは、Intersight 管理モードのサーバでのみ使用できます。
  - **[アセット タグの設定（Set Asset Tags）]**：カスタム アセット タグを設定できます。

- **ユーザーラベルの設定（Set User Label）**：選択したサーバのユーザーラベルを設定、更新、または削除できます。それは1～64文字の英数字で指定する必要があります。使用できる特殊文字は - _ .です。# $ % & * + , ( ) [ ] { } | / . ? @ _ : ; ~
- **[システム イベント ログのダウンロード（Download System Event Log）]**：選択したサーバのシステム イベント ログをダウンロードします。これらのログは、過不足の電圧、温度、ファン イベントなどサーバ関連イベントをレコードします。
- **[システム イベント ログのクリア（Clear System Event Log）]**：選択したサーバのシステム イベント ログをクリアします。

- **[オペレーティング システムのインストール（Install Operating System）]**—シンプルなプロセスで、一元化されたデータセンターから 1 台以上の Cisco UCS C シリーズ スタンドアロン サーバに対して、無人 OS インストールが行えます。
- **[ファームウェアのアップグレード（Upgrade Firmware）]**：ファームウェアのアップグレードを実行します。詳細については、「ファームウェアのアップグレード」を参照してください。
- **IMC の起動（Launch IMC）**：Cisco Integrated Management Controller (CIMC) を起動します。このアクションは、C シリーズ スタンドアロン サーバーのみで使用できます。

（注） *[ローカル ダウンロードのテクニカル サポート データの生成（Generate Technical Support Data for Local Download）]* および *[ローカルダウンロードへのハードウェアインベントリデータのダウンロード（Download Hardware Inventory Data to Local Download）]* オプションは、相互起動 CIMC インターフェイスではサポートされていません。

- **[仮想 KVM の起動（Launch Virtual KVM）]**：ファブリック インターコネクト接続およびスタンドアロン サーバの仮想キーボード、ビデオ、およびマウス（KVM）コンソールを直接起動します。エンドポイントおよびサーバへのローカル ネットワーク接続が必要です。
- **[トンネル vKVM の起動（Launch Tunneled vKVM）]**：トンネル vKVM は、Intersight を介して KVM トラフィックをトンネリングすることによって機能します。Intersight 管理モードのすべてのサーバ、Cisco UCS C シリーズ スタンドアロン M4、M5、M6、M7 および M8 サーバ、UCS S シリーズ、および Hyperflex HX シリーズ エッジ スタンドアロン M4 および M5 サーバのトンネル vKVM セッションを起動できます。
- **[TAC ケースを開く（Open TAC Case）]**：ケースを開いて、サーバの問題を報告します。
- **[ライセンス階層の設定（Set License Tier）]**：サーバを新しいライセンス階層に更新します。ライセンス階層の更新は、関連付けられたサーバプロファイルを持つサーバでは行えません。ライセンス階層を移動するには、選択したサーバからプロファイルの割り当て解除し、割り当てをやり直します。

- **[テクニカル サポート バンドルの収集（Collect Tech Support Bundle）]**：テクニカル サポート バンドルを収集します。アカウント管理者は、デバイスを選択し、選択したデバイスのテクニカル サポート バンドル ファイルを収集できます。ダウンロードしたファイルには、[管理]>[テクニカル サポート バンドル]セクションに移動してアクセスできます。このファイルは、問題をトラブルシューティングするためにTACチームと共有できます。

[サーバの一括操作（Bulk Server Actions）]

[サーバ（Servers）]テーブル ページでは、1 台以上のサーバを管理するために、以下の操作を実行できます。

- **[電源（Power）]**
  - **[電源オン（Power On）]**：1 台以上のサーバの電源をオンにします。
  - **[電源オフ（Power Off）]**：1 台以上のサーバの電源をオフにします。
  - **[電源サイクル（Power Cycle）]**：1 台以上のサーバの電源をオフにしてからオンに戻します。
  - **[ハード リセット（Hard Reset）]**：サーバを再起動します。
  - **[OS のシャットダウン（Shut Down OS）]**：オペレーティング システムでサポートされている場合、サーバをシャットダウンします。
- **[システム（System）]**
  - **[ロケータをオンにする（Turn On Locator）]**：LED ロケータをオンにします。
  - **[ロケータをオフにする（Turn Off Locator）]**：LED ロケータをオフにします。
  - **[CMOS のリセット（Reset CMOS）]**：BIOS 構成設定を元の状態にリセットします。これにより、サーバが正常な状態でない場合の回復に役立ちます。CMOS をリセットするオプションは、サーバの電源がオフの場合にのみ表示されます。リセットを完了するには、サーバの電源をオンにする必要があります。[CMOS のリセット（Reset CMOS）] 確認ウィンドウにあるトグル ボタンを使用して、サーバの電源をオンにする追加オプションがあります。

（注） このオプションは、Intersight管理モードのサーバでのみ使用できます。

- **[フロント パネルのロック（Lock Front Panel）]**：サーバの物理的な電源ボタンをロックします。フロント パネルがすでにロックされているサーバの場合、このオプションは **[フロント パネルのロック解除（Unlock Front Panel）] と**表示されます

（注） このオプションは、Intersight管理モードのサーバでのみ使用できます。

- **[シスコ IMC の再起動（Reboot IMC）]**：Cisco IMC を再起動します。

- **[オペレーティング システムのインストール（Install Operating System）]**—シンプルなプロセスで、一元化されたデータセンターから 1 台以上の Cisco UCS C シリーズ スタンドアロン サーバに対して、無人 OS インストールが行えます。
- **[ファームウェアのアップグレード（Upgrade Firmware）]**：ファームウェアのアップグレードを実行します。
- **[ライセンス階層の設定（Set License Tier）]**：1 台以上のサーバを新しいライセンス階層に更新します。ライセンス階層の更新は、関連付けられたサーバプロファイルを持つサーバでは行えません。ライセンス階層を移動するには、選択したサーバからプロファイルの割り当て解除し、割り当てをやり直します。

サーバ インベントリの表示

サーバが検出されると、そのすべてのコンポーネントのインベントリが使用可能になります。**[サーバ（Server）]** テーブルビューでサーバを選択すると、**[インベントリ（Inventory）]** タブでそのコンポーネントのインベントリを表示できます。

選択したサーバについて、次の各コンポーネントの詳細を表示できます。

- **ブート**：サーバに設定されているデバイスの実際のブート順序を確認できます。ブート順序には、デバイス名、デバイスタイプ、ブートモード（レガシーまたは UEFI）、セキュアブートモード（有効または無効）などの設定の詳細が含まれます。ブート順序ポリシーのサーバプロファイルで設定されたデバイスは、サーバのブート時にサーバ BIOS がデバイスを検出しない場合、実際のブート順序に表示されないことがあります。
- **[管理コントローラ（Management Controller）]**：ファームウェア バージョン、アウトバンド管理アクセスの概要、ハードウェアの詳細、およびサーバー証明書の詳細を表示できます。また、証明書セクションから最新のサーバー証明書を表示またはコピーすることもできます。

（注） Intersight 管理モード (IMM) での UCS B シリーズ（M5、M6）および X シリーズ（M6、M7）サーバのサーバ証明書操作は、サーバ ファームウェア 4.2 以降のバージョンでのみサポートされます。ただし、UCS C シリーズ（M5、M6、M7、M8）サーバのサーバ ファームウェア バージョンに制限はありません。

- **[CPU]**：アーキテクチャ、モデル、ソケットの指定、ベンダーなど、プロセッサに関する詳細を表示できます。**[CPU]** を展開すると、各プロセッサのハードウェアとリソースの詳細の状態と概要が表示されます。

- **[Memory]**：メモリカードの場所、ID、容量、クロック速度などのメモリカードの概要を表示できます。**[Memory]** を展開すると、各メモリカードの状態とハードウェアの詳細が表示されます。
- **[Network Adapters]**：ネットワーク アダプタ カードの詳細（接続先のスロット、モデル、シリアル、ベンダー、接続先のインターフェイスなど）を確認できます。

  アダプタを選択すると、次の詳細を表示できます。

  - **全般（General）**：ファームウェアバージョン、インターフェイスの詳細（DCE/NIC/HBA）、ハードウェアの詳細、および各アダプタに関連するアラームのリストが表示されます。
  - **インターフェイス**：名前、MACアドレス、VIF ID、動作状態、パッシブ VIF ID、パッシブ動作状態、およびレート制限を表示できます。省略記号（[...]）をクリックして、vNIC および vHBA に対して次の **アクション** を実行します。
    - **vNIC**：有効、有効（アクティブ）、有効（パッシブ）、無効、無効（アクティブ）、無効（パッシブ）、接続のリセット、接続のリセット（アクティブ）、接続のリセット（パッシブ）。
    - **vHBA**：接続の有効化、無効化、リセット。

（注） vNICおよびvHBAの有効化または無効化は、スタンドアロンモードには適用されません。

- **GPU**：GPU のリストを表示できます。GPU を展開すると、各 GPU の一般情報と GPU コントローラ情報を含む GPU インベントリの詳細が表示されます。
  - **全般**
    - **[メイン（Main）]**：スロットID、モデル、シリアル番号、ベンダー、GPUの数、およびファームウェア バージョンを表示できます。
    - **[PCIe エンクロージャ（PCIe Enclosure）]**：スロット ID、モデル、シリアル番号、およびベンダー情報を表示できます。
  - **[GPU コントローラ（GPU Controllers）]**：GPU コントローラ名と PCI アドレス情報を表示できます。

  GPUへの挿入、削除、または置換操作を含む変更操作では、再検出をトリガーする必要があります。したがって、再検出により、変更を検出し、サーバーインベントリを更新できます。
- **[PCIe デバイス（PCIe Devices）]**：PCIe デバイスとそのスロット ID のリストを表示できます。PCIe デバイスを展開すると、各デバイスの構成とハードウェア情報が表示されます。

- **[構成（Configuration）]**：デバイスのファームウェア バージョンを表示できます。
- **[ハードウェア（Hardware）]**：デバイスのスロット ID、製品名、シリアル番号、およびベンダー情報を表示できます。

- **[ストレージ コントローラ（Storage Controllers）]**：サーバに関連付けられているストレージコントローラのリストを表示できます。[ストレージコントローラ（Storage Controllers）] テーブル ビューには、ストレージ コントローラの名前、 識別子、タイプ、ファームウェア バージョン、シリアル番号、サポートされているハイブリッド スロットが表示されます。

  [ストレージ コントローラ（Storage Controllers）] を展開すると、コントローラ設定の詳細が表示され、次の操作を実行できます。

  次の操作を実行して、1 つ以上のストレージコントローラを管理できます。

  - **全般**
    - **[構成（Configuration）]**：ストレージコントローラのファームウェア バージョンを表示できます。

（注） Intersight 管理モードおよびスタンドアロン モードの Cisco UCS C シリーズ（M7、M8）は、M.2 RAID0 および RAID1 コントローラの UCS-M2-NVRAID ストレージコントローラをサポートします。

UCSM 管理モードの Cisco UCS C シリーズ（M7）は、Cisco UCS C220 M7 ストレージ コントローラ（最大 10 台のSAS/SATA）および Cisco UCS C240 M7（最大 28 台のSAS/SATA）または NVMe ディスク ドライブをサポートします。

RAIDまたは直接接続モードで U.3 ドライブを処理する Cisco Tri-Mode 24G SAS RAIDコントローラ w/4GB キャッシュ（UCSC- RAID -HP）。

- **ハードウェア**：ストレージコントローラのコントローラ識別子、識別子タイプ、RAID サポート、ディスク数、シリアル番号、モデル、およびベンダー情報を表示できます。

- **[Physical Drives]**：1 台の物理ドライブまたは複数の物理ドライブで、**未設定の良好な**ドライブ状態と **JBOD** ドライブ状態を切り替えることができます。

  [物理ドライブ（Physical Drives）] テーブル ビューには、PID、ベンダー、プロトコル、Security フラグ、タイプ、ドライブの状態が表示されます。

  次の 2 つのモデルがサポートされています。UCS-NVM2-400GB、UCS-NVM2-960GB

- **[Virtual Drives]**：未使用の仮想ドライブを選択して削除し、RAID コントローラの使用済み領域を再利用できます。仮想ドライブを削除すると、ファイルシステム上のすべての情報が破棄され、RAID コントローラから仮想ドライブが削除されます。

（注） これは、Cisco Boot Optimized M.2 RAID コントローラでサポートされている唯一のストレージ操作です。

- **ストレージ コントローラと物理ドライブ操作**

次の表に、サポートされている SED ドライブ操作を示します。

ストレージ コントローラと物理ドライブ操作	説明
安全消去	キー暗号キーを削除し、SED に保存されているデータを消去するには、このオプションを使用します。 物理ドライブの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。
外部設定のインポート	物理ドライブのユーザー設定をクリアし、仮想ドライブを削除するには、このオプションを使用します。 コントローラの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。
外部設定のクリア	このオプションは、物理ドライブまたは仮想ドライブに保存されているすべてのデータをクリアまたは消去します。 コントローラの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。
設定をクリア	このオプションは、サーバがサーバプロファイルに関連付けられていない場合に、仮想ドライブを削除したり、ストレージ コントローラのユーザー設定をクリアしてコントローラを再利用したりする場合に使用します。 コントローラの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。

ストレージ コントローラと物理ドライブ操作	説明
セキュリティの無効化	このアクションを使用して、コントローラのセキュリティを無効にします。 コントローラの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。
セキュリティの変更	コントローラでセキュリティをすでに有効にした後にキー暗号キーを変更するには、このオプションを使用します。 コントローラの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。
ディスクのロック解除	暗号化されたドライブが別のサーバーから挿入されたときに、ドライブのロックを解除してデータにアクセスするには、このオプションを使用します。 コントローラの横にある **[アクション（Actions）]** メニューには、このオプションが表示されます。

- **ハイブリッド ストレージ スロット**：ハイブリッド スロットは、RAID コントローラが SAS/SATA モードで U.3 ドライブを処理できるかどうかを示します。スロット ID、要求されたモード、および現在のモードを表示できます。適用可能な値は [RAID] と [Direct] です。

- **[TPM]** により、要求されたサーバのデータおよびハードウェアコンポーネントを保護できます。TPM では、キー識別子の状態とハードウェアの詳細の概要を表示することもできます。

  サーバー インベントリ ビューの右隅にある **[アクション（Actions）]** ボタンから **[TPM のクリア（Clear TPM）]** オプションを使用して、TPM 構成をクリアまたはリセットすることもできます。

  [注意：（Caution:）]

  [TPM のクリア（Clear TPM）] は、災害復旧とデータ損失の操作を目的としています。必要な場合以外は使用しないでください。

  [TPM のクリア（Clear TPM）] アクションを使用する前に、次のことを確認する必要があります。

  - サーバー プロファイルが構成されています。
  - オペレーティング システムがインストールされています。

- サーバーが電源オフ状態です。

（注） TPM のクリア アクションは、Cisco UCS B シリーズおよび C シリーズ M5 以降のサーバーとファームウェア バージョン 4.2（2a）以降でのみサポートされます。

TPM の次のコンポーネントを表示できます。

- キー識別子
  - **[アクティブ化ステータス（Activation Status）]**：TPM がアクティブ化/非アクティブ化状態にあることを示します。TPM 構成がクリア/リセットされると、アクティベーション ステータスは非アクティブと表示されます。
  - **[有効状態（Enabled State）]** - TPM が有効/無効状態であることを示します。TPM 構成がクリア/リセットされると、有効状態は無効と表示されます。

- ハードウェア
  - **[所有権（Ownership）]**—所有権のステータスを所有/未所有として表示します。TPM 構成がクリア/リセットされると、所有権の状態は未所有と表示されます。いつでも所有権を取り戻すには、電源サイクル サーバーのスイッチを入れる必要があります。

（注） このプロパティは、TPM 1.2 バージョンでのみ表示できます。2.0 の場合、アクティベーション ステータス、有効状態、および所有権ステータスをオペレーティング システムで表示できます。

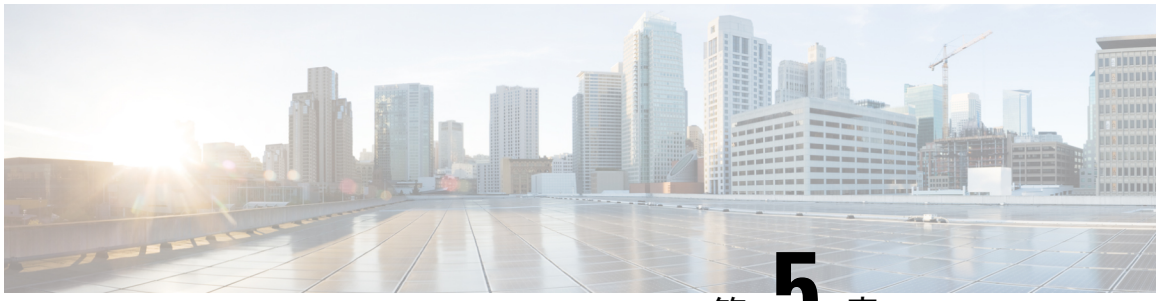
  - バージョン
  - モデル
  - ベンダー
  - シリアル
  - ファームウェアバージョン

（注） このプロパティは、TPM 2.0 バージョンでのみ表示できます。

ハードウェア互換性リスト（HCL）との準拠

Cisco Intersight は、ファームウェア、サーバーモデル、プロセッサ、アダプタ、オペレーティングシステム、およびドライババージョンの検証されていない組み合わせを実行することでサービスに生じる問題の影響を評価し、軽減します。Intersight では、ハードウェアとソフトウェアがシスコまたはシスコ パートナーによって検証済みであるかどうか確認するため、Cisco UCS システム、HyperFlex システム、Intersight Managed Mode（IMM）サーバ、および Cisco UCS S シリーズ サーバの互換性を評価します。Cisco Intersight は、サーバ モデル、プロセッサ、ファームウェア、アダプタ、OS、およびドライバの互換性を確認後、検証の問題を報告し、 ハードウェア互換性リスト（HCL）へのコンプライアンス ステータスを表示します。**この機能には、Cisco Intersight Essentials 以上の来世巣が必要です**。

Cisco UCS ツール、ホストユーティリティの vSphere インストールバンドル（VIB）、または OS 検出ツール、オープン ソース スクリプトを使用して、OS およびドライバ情報を収集し、HCL へのコンプライアンスを評価します。ハードウェア互換性ステータスの詳細、Cisco UCS ツールをダウンロードする方法の詳細な説明と手順、および OS ディスカバリツールの使用方法については、リソースの Compliance with Hardware Compatibility List（HCL）を参照してください。



第 5 章

UCS ドメイン プロファイルの設定

- UCS ドメイン プロファイルの概要 （59 ページ）
- UCS ドメイン プロファイルの作成 （59 ページ）
- UCS ドメイン プロファイルの詳細 （60 ページ）

UCS ドメイン プロファイルの概要

UCS ドメイン プロファイルの概要

UCS ドメインプロファイルは、再利用可能なポリシーを使用してファブリック インターコネクト ペアを設定し、ポートとポートチャネルの設定を可能にし、ネットワーク内の VLAN と VSAN を設定します。また、ファブリック インターコネクトのポートの特性を定義し、設定します。UCS ドメインプロファイルを作成し、ファブリック インターコネクト ドメインに関連付けることができます。ドメイン関連ポリシーは、作成時または作成後にプロファイルに接続できます。1 つの UCS ドメインプロファイルを 1 つのファブリック インターコネクト ドメインに割り当てることができます。

重要

- Cisco Intersight は、UCS ドメインプロファイルごとに 1 つのポートポリシーのアタッチをサポートします。
- UCS ドメインプロファイルにアタッチされているポリシーは、プロファイルの作成前に作成することも、プロファイルの作成中に作成することもできます。
- UCS ドメインにアタッチされているポリシーと、特定の UCS ドメインに関連付けられているすべての UCS ドメインプロファイルのグローバルポリシーが共有されます。

UCS ドメイン プロファイルの作成

UCS ドメイン プロファイルは、再利用可能なポリシーを使用してファブリック インターコネクト ペアの展開を合理化し、ポートとポートチャネルの設定を可能にし、ネットワーク内の VLAN と VSAN を設定します。

ステップ 1 Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

ステップ 2 **[サービス プロファイル（Service Profiles）]** > **[UCS ドメイン プロファイル（UCS Domain Profiles）]** タブに移動し、**[UCS ドメイン プロファイルの作成（Create UCS Domain Profile）]** をクリックします。

ステップ 3 **[全般（General）]** ページで、プロファイルの名前を入力します。必要に応じて、プロファイルの識別に役立つ短い説明とタグ情報を含めます。タグは key：value 形式である必要があります。たとえば、Org: IT または Site: APJ などです。

ステップ 4 **[ドメイン割り当て（Domain Assignment）]** ページで、スイッチ ペアをドメイン プロファイルに割り当てます。**[後で割り当てる（Assign Later）]** をクリックして、後でスイッチ プロファイルをドメイン プロファイルに割り当てることもできます。

ステップ 5 **[次へ（Next）]** をクリックします。

ステップ 6 **[VLAN と VSAN の設定（VLAN & VSAN Configuration）]** ページで、各スイッチの VLAN および VSAN ポリシーを **[UCS ドメイン プロファイル（UCS Domain Profile）]** UCS ドメイン プロファイルにアタッチし、**[次へ（Next）]** をクリックします。

（注） システム予約済み VLAN を構成するには、VLAN および VSAN ポリシーが予約済み VLAN 範囲と競合しないようにする必要があります。競合がある場合、展開は失敗します。

ステップ 7 **[ポートの設定（Ports Configuration）]** ページで、各スイッチのポートポリシーを **[UCS ドメイン プロファイル（UCS Domain Profile）]** にアタッチし、**[次へ（Next）]** をクリックします。

ステップ 8 **[UCS ドメインの設定（UCS Domain Configuration）]** ページで、必要なコンピューティングおよび管理ポリシーを **[UCS ドメイン プロファイル（UCS Domain Profile）]** にアタッチし、**[次へ（Next）]** をクリックします。

注：この手順では、VLAN ポート数の最適化を有効にするために、スイッチ制御ポリシーを作成してアタッチする必要があります。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 **[サマリー（Summary）]** ページで、UCS ドメイン プロファイルとそれに関連付けられているポリシーの詳細を確認します。

ステップ 11 **[展開（Deploy）]** をクリックして、割り当てられたファブリックインターコネクトドメインに UCS ドメイン プロファイルを展開します。

UCS ドメイン プロファイルの詳細

[UCS Domain Profile Details] ページには、ステータスと **[Actions]** メニューに加えて、[Port Configuration]、[VLAN and VSAN Configuration]、および [UCS Domain Configuration] がグラフィック表示されます。[UCS Domain Profiles Table] ビューから [UCS Domain Details] に移動します。このページでは、次の作業を行うことができます。

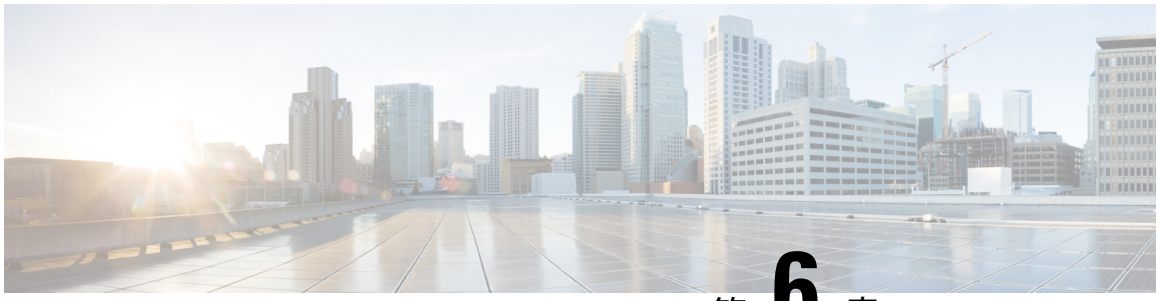
- UCS ドメイン プロファイル **アクション**を実行します。

- **Deploy**：ファブリックインターコネクトペアに UCS ドメインプロファイルを展開します。
- **Unassign**：ファブリックインターコネクトペアから UCS ドメインプロファイルの割り当てを解除します。
- **Edit**：UCS ドメインプロファイルのプロパティを編集します。
- **Clone**：既存の UCS ドメインプロファイルと同様のプロパティを使用して UCS ドメインプロファイルを複製します。クローンは、元の UCS ドメインプロファイルと同じポリシーに関連付けられます。
- **タグの設定**

- UCS ドメインプロファイルの**詳細**の表示

[プロパティ（Property）]	**[基本情報（Essential Information）]**
ステータス（Status）	ファブリックインターコネクトペアでの UCS ドメインプロファイルの展開のステータス。次のようになります。 • **OK** • **失敗（Failed）** • **未展開（Not Deployed）**
名前（Name）	UCS ドメインプロファイル名。
[Fabric Interconnect A]	UCS ドメインの関連するファブリックインターコネクト A の名前。
Fabric Interconnect B	UCS ドメインの関連するファブリックインターコネクト B の名前。
[最終更新（Last Update）]	UCS ドメインプロファイルが最後に更新された日時。
タグ（Tags）	選択したオブジェクトの既存のタグがデフォルトで表示されます。**[管理（Manage）]**をクリックして、新しいタグを追加するか、既存のタグを変更します。

- UCS ドメイン**プロファイル**にアタッチされているポリシーを表示します。**Policies** ペインには、ポート、VLAN および VSAN、および UCS ドメイン設定の詳細が表示されます。ポートロール、ポートチャネル、および関連付けられたポリシーのリストを含む、ファブリックインターコネクトのポート設定がグラフィカルに表示されます。VLAN、VSAN、および UCS ドメイン設定には、選択したドメインプロファイルに関連付けられたドメイン ポリシーがリストされます。



第 6 章

サーバ プロファイルの設定

- サーバー プロファイル （63 ページ）
- UCS サーバ プロファイルの作成 （73 ページ）
- UCS サーバ プロファイルの詳細 （76 ページ）

サーバー プロファイル

Cisco Intersight では、サーバ プロファイルによるリソース管理により、ポリシー適合とサーバ構成を合理化できます。サーバー プロファイル テーブル ビューを表示するには、**Service Selector** ドロップダウン リストから **[サービスとしてのインフラストラクチャ（Infrastructure Service）]** を選択します。**[構成（CONFIGURE）]>[プロファイル（Profiles）]** に移動します。サーバ プロファイル ウィザードを使用してサーバ プロファイルを作成するか、C シリーズ サーバの設定の詳細を Cisco IMC から直接インポートできます。サーバプロファイル ウィザードを使用して、サーバをプロビジョニングするためのサーバプロファイルを作成できます。また、サーバをスムーズに展開するためのポリシーを作成し、構成の不一致が原因で生じる障害を排除できます。[サーバ プロファイル（Server Profiles）] ウィザードは、サーバ ポリシーを次の4つのカテゴリにグループ化し、プロファイルに関連付けられているポリシーの概要ビューを迅速に提供します。

- **[コンピューティング ポリシー（Compute Policies）]**：BIOS、ブート順序、および仮想メディア。
- **[ネットワーク ポリシー（Network Policies）]**：アダプタ構成、iSCSI のブート、LAN 接続、SAN 接続のポリシー。
  - LAN 接続ポリシーでは、イーサネット ネットワーク ポリシー、イーサネット ネットワーク制御ポリシー、イーサネット ネットワーク グループ ポリシー、イーサネット アダプタ ポリシー、またはイーサネット QoS ポリシーを作成することができます。LAN 接続ポリシーをサーバ プロファイルに接続すると、MAC アドレスプールのアドレスまたは静的 MAC アドレスが自動的に割り当てられます。

（注） 静的 MAC アドレスを持つ LAN 接続ポリシーは、1 つのサーバ プロファイルにのみ接続できます。

- SAN 接続ポリシーではファイバチャネル ネットワーク ポリシー、ファイバチャネル アダプタ ポリシー、またはファイバ チャネル QoS ポリシーを作成する必要があります。SAN 接続ポリシーをサーバ プロファイルに接続すると、WWPN および WWNN プールのアドレス、または静的 WWPN および WWNN アドレスが自動的に割り当てられます。

（注） 静的 WWPN または静的 WWNN を持つ SAN 接続ポリシーは、1 つのサーバ プロファイルにのみ接続できます。

- **[ストレージポリシー（Storage Policies）]**：SD カードおよびストレージのポリシー
- **[管理ポリシー（Management Policies）]**：デバイス コネクタ、IPMI Over LAN、LDAP、ローカルユーザ、ネットワーク接続、SMTP、SNMP、SSH、Serial Over LAN、Syslog、NTP 証明書管理、および仮想 KVM ポリシー

ポリシーの詳細と説明については、「**サーバー ポリシー**」の項を参照してください。ポリシー作成ワークフローの例については、「ネットワーク ポリシーの作成」を参照してください。

サーバー プロファイル リスト ビュー

Intersight UI で **[プロファイル（Profiles）] > [UCS サーバー プロファイル（UCS Server Profiles）]** を選択すると、UCS サーバー プロファイル リスト ビューが表示されます。

リスト ビューには、次の詳細が表形式で表示されます。

- 名前（Name）：サーバー プロファイルの名前
- ステータス（Status）：サーバープロファイルの展開ステータス。

  プロファイルの **[ステータス（Status）]** には、以下の値のいずれかが表示されます。

  - **未割り当て（Not Assigned）**：ポリシーはサーバー プロファイルに割り当てられていません。

（注）
- サーバープロファイルにポリシーを展開すると、結果に応じてステータスが *[未割り当て（Not Assigned）]* から新しいステータスに自動的に変更されます。場合によっては、更新されたステータスを確認するには、画面を更新する必要があります。
- 各プロファイルの展開後に、電源の再投入/電源投入を行う必要があります。

  - **OK**：ポリシーはサーバ プロファイルに正常に展開されています
  - **進行中（In Progress）**：サーバー プロファイルへのポリシーの展開が進行中です

- **失敗（Failed）**：サーバ プロファイルの検証、設定、または展開に失敗しました
- **不整合（Inconsistent）**：ポリシー設定にまだ展開またはアクティブ化されていない変更があることを示しますエンドポイントのポリシー設定が、サーバープロファイルで最後に展開されたポリシー設定と同期していないことを示している場合もあります。サーバープロファイルの展開後にエンドポイントの設定を手動で変更すると、Intersight が設定の変更を自動的に検出し、サーバ プロファイルに **[非整合（Inconsistent）]** と表示されます。詳細については、「サーバープロファイルのばらつき」および「サーバー プロファイルの展開とアクティブ化 」の項を参照してください。

- 不整合の理由（Inconsistency Reason）：ステータスが [不整合（*Inconsistent*）] として表示される理由。例：展開されていない、アクティブ化されていない、同期していない
- ターゲット プラットフォーム（Target Platform）：プロファイルを適用できるプラットフォームがスタンドアロン UCS サーバーか、FI 接続 UCS サーバーかを示します。
- UCS サーバーテンプレート（UCS Server Template）：サーバープロファイルに添付されているテンプレート、またはプロファイルの派生元のテンプレート。
- サーバー（Server）：プロファイルが接続されているサーバーの名前。
- リソース プール（Resource Pool）：プロファイルが属するプール。
- ユーザー ラベル（User Label）：ユーザー ラベルは、サーバープロファイルのフィルタリングに役立つ識別子です。それは1～64文字の英数字で指定する必要があります。使用できる特殊文字は - _ .です。# $ % & * + , ( ) [ ] { } | / . ? @ _ : ; ~
- 最終更新日（Last Update）：プロファイルが最後に更新された日付。
- 組織（Organization）：組織の名前。

（注） **ユーザー ラベル（User Label）** など、一部の列はデフォルトで無効になっています。このようなカラムをサーバー プロファイル テーブル ビューに表示するには、テーブル ビューのカスタマイズ時にカラムを有効にする必要があります。

サーバー プロファイルのアクション

サーバー プロファイルを作成した後、サーバー プロファイルで実行できるアクションは次のとおりです。

- 展開（Deploy）：接続されているサーバーにプロファイルを展開します。
- アクティブ化（Activate）：接続されているサーバーでプロファイルをアクティブ化します。アクティブ化時にサーバーの電源が再投入されます。
- 編集（Edit）：プロファイルの編集
- クローン（Clone）：プロファイルのクローン作成

- テンプレートにアタッチ（Attach to Template）：使用可能なテンプレートのいずれかにサーバープロファイルをアタッチします。

（注）
- テンプレートの作成中に、**[USC サーバ プロファイルをプロファイル テンプレートにアタッチする（Attach UCS Server Profile to Profile Template）]** ボタンをオンにすると、選択したプロファイルが作成中のテンプレートにアタッチされます。
- トグルボタンをオフのままにすると、選択したプロファイルのプロパティはテンプレートに適用されますが、プロファイルはテンプレートにアタッチされません。

- テンプレートの作成（Create a Template）：サーバー プロファイルは、既存のテンプレートを作成するために使用できます。このテンプレートを使用して、同じ設定の複数のプロファイルを作成し、複数のサーバに展開できます。
- テンプレートから切り離す（Detach from Template）：テンプレートからプロファイルを切り離します。

（注）
- **[テンプレートの作成（Create a Template）]** および **[テンプレートへの添付（Attach to Template）]** アクションは、サーバ プロファイルがどのテンプレートにも添付されていない場合にのみ実行できます。
- サーバ プロファイルは、既存のテンプレートに添付できます。この添付ファイルは、プロファイルの設定プロパティを上書きし、テンプレートプロパティに置き換えます。
- テンプレートにアタッチしているサーバプロファイル変更できません変更は、関連するテンプレートで行うことができます。
- サーバ プロファイルは、要件に応じてテンプレートからデタッチし、変更できます。
- 切り離されたサーバプロファイルは、いつでもテンプレートに再アタッチできます。

- サーバーの割り当て解除（Unassign Server）：プロファイルからサーバーの割り当てを解除します。

- ユーザー ラベルの設定（Set User Label）：[ユーザー ラベルの設定（**Set User Label**）] アクションを使用して、各サーバー プロファイルのユーザー ラベルを設定、更新、または削除することもできます。

サーバー プロファイル詳細ビュー

プロファイルをクリックすると、**[一般（General）]**、**[サーバー（Server）]**、および **[在庫（Inventory）]** タブの下で、**[サーバー プロファイルの詳細ビュー（Server Profile Details View）]** にリダイレクトされ、プロファイルにアタッチされたポリシーの設定の詳細が表示されます。

サーバ プロファイルの変動

サーバ プロファイルの変動は、エンドポイントでの構成が、サーバ プロファイルで最後に展開済みとされているポリシーと同期していない場合に生じます。

Cisco Intersight は、スタンドアロン サーバーおよび Intersight 管理モード サーバーのサーバー プロファイル変動の検出をサポートしています。Intersightマネージドモードサーバーの場合、変動の検出に必要なファームウェア バージョンは次のとおりです。

- 4.2 リリースの場合、Cisco IMC バージョンは 4.2(1b) 以降である必要があります。
- 4.1 リリースの場合、Cisco IMC バージョンは次のとおりである必要があります。
  - ラック サーバーの場合 - 4.1(3d) 以降
  - ブレード サーバーの場合 - 4.1(33e) 以降

エンドポイントで設定変更を検索するチェックは、30 分ごとに実行されます。

Intersightで現在展開されているポリシー設定に関連してエンドポイントで変更されたポリシー設定を確認するには、[サーバ プロファイルの詳細（Server Profile details）] ビューに移動し、**[変更の表示（View Changes）]** をクリックします。**[変更のみ（Changes Only）]** または **[すべて（All）]** のポリシー設定の詳細を表示するように選択できます。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[保存された設定（Saved Settings）]	Intersight のポリシー設定を表示します。
[最後に展開された設定（Last Deployed Settings）]	サーバ プロファイルに展開された最新のポリシー設定を表示します。
[エンドポイント設定（Endpoint Settings）]	エンドポイントでの設定を表示します。

サーバプロファイルのステータスを **[OK]** に戻すには、プロファイルを再展開するか、エンドポイントで値を変更します。Intersight のデバイス コネクタ ポリシーを使用して、 Cisco IMC で許可される設定変更を制御できます。デバイス コネクタ ポリシーで、**[Intersight からのみ設定（Configuration from Intersight only）]** を選択すれば、Cisco IMC からの直接許可による設定変更を停止できます。

サーバー プロファイル変動の制限 - スタンドアロン サーバー

スタンドアロン サーバーの場合、エンドポイントでの設定変更は、特定の条件下の次のポリシーでは検出されません。

[Policy（ポリシー）]	エンドポイントの設定
SD カード ポリシー	SD カードが取り外された場合。
ストレージ ポリシー	• ポリシー内のいずれかの仮想ドライブに [展開可能（Expand to Available）] が設定されている場合。 • すべての導入後に電源の再投入が行われない場合。 • Intersight から設定されていない追加のドライブグループがある場合
ブート順序ポリシー	すべての導入後に電源の再投入が行われない場合。 SAN ブート デバイスでは、Intersight は**インターフェイス名**と**ターゲット WWPN** の変動を検出しません。 （注） シスコでは、システム内でサーバプロファイル モビリティを提供する SAN ブートの使用を推奨しています。SAN からブートした場合、あるサーバから別のサーバにサーバプロファイルを移動すると、新しいサーバは、同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、新しいサーバーは同じサーバーと認識されます。 SANブートを使用するには、次の項目が設定されていることを確認してください。 • Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。 • オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN（論理ユニット番号）。

[Policy（ポリシー）]	エンドポイントの設定
ローカルユーザ、SNMP、LDAP、およびIPMI over LAN ポリシー	エンドポイントでパスワードが変更された場合。
仮想メディア ポリシー	エンドポイントでパスワード、マウントオプション、または認証プロトコルに変更がある場合。
BIOS ポリシー	• 「platform-default」として設定されたBIOSトークン値は、そのプラットフォームのデフォルト値に変更されます。このようなBIOSトークンでは、変動検出は行われません。詳細については、「サポートされる UCS サーバー ポリシー」での BIOS ポリシーの項の表 16 を参照してください。 • 値が他の BIOS トークン値に依存する BIOS トークンは、ばらつきの検出に対して考慮されません。ポリシーが展開されているサーバーでサポートされていない値を持つBIOSトークンについて、ばらつきが報告される場合があります。詳細については、「Cisco UCS サーバの BIOS トークン」を参照してください。
IPMI over LAN ポリシー	「権限レベル」フィールドは考慮されません。
ネットワーク接続ポリシー	ポリシーの [優先 IPv6 DNS サーバ（Preferred IPv6 DNS Server）] および [代替 IPv6 DNS サーバ（Alternate IPv6 DNS Server）] フィールドは考慮されません。サーバ プロファイルが一時的に非同期状態に移行することがあります。
アダプタ設定ポリシー	このポリシーは、変動計算では考慮されません。

[Policy（ポリシー）]	エンドポイントの設定
イーサネット アダプタ ポリシー	usNIC またはVMMQに異なるイーサネットアダプタポリシーがある場合、usNIC または VMMQに接続されたイーサネットアダプタポリシーの設定変更は計算されません。 VMQ 設定の制限により、VMQ の割り込み数はイーサネットアダプタポリシーの割り込みの値をオーバーライドし、VMQの仮想マシンキューの数は受信キューカウント、送信キューカウント、および完了キューカウント（受信+送信）の値をオーバーライドします。イーサネットアダプタポリシー割り込み数、仮想マシンキュー数、受信キューカウント、送信キューカウント、および完了キューカウントについては、検出されません。 Intersight は、「割り込み数」、「仮想マシンキュー数」、「受信キューカウント」、「送信キューカウント」、および「完了キューカウント」の変動を検出しません。
LAN 接続ポリシー	「CDN」フィールドは考慮されません。
IMC アクセスポリシー	インバンドIPv6とIPv4の両方の設定が使用可能な場合、IPv6 DNS 設定が優先されます。

サーバー プロファイル変動の制限 - Intersight 管理モード サーバー

Intersight 管理モード サーバーの場合、エンドポイントでのサーバー構成変更は、特定の条件下の次のポリシーでは検出されません。

（注） 名前はエンドポイント設定ではないため、[名前（Name）] フィールドはどのポリシーでもサポートされていません。

（注） プールと ID の変動の検出はサポートされていません

[Policy（ポリシー）]	エンドポイントの設定
SD カード ポリシー	SDカードが取り外されている場合、変動の検出はサポートされません。

[Policy（ポリシー）]	エンドポイントの設定
ストレージ ポリシー、ブート順序ポリシー、BIOS ポリシー、仮想メディア ポリシー	変動の検出は、Intersight 管理対象モード サーバーのブート順序ポリシーではサポートされていません
ローカル ユーザー ポリシー、SNMP ポリシー、証明書管理ポリシー	エンドポイントでパスワード、コミュニティ文字列、秘密キーなどのセキュリティ保護されたフィールドに変更がある場合、変動の検出はサポートされません。
LAN 接続ポリシー	次に対して変動の検出はサポートされていません。 • VMQ 接続 • 割り込みの数 • 仮想マシン キューの数 • Consistent Device Naming (CDN) • vNICの自動配置 ID • イーサネット アダプタ ポリシー • 割り込み設定 - 割り込み • 完了 - 完了キュー数、完了リング サイズ • VMMQ アダプタ ポリシー • usNICアダプタポリシー （注） 変動の検出は、サーバーの電源が入っている場合にのみサポートされます
IMC アクセスポリシー	アウトオブバンド構成では、変動検出はサポートされていません。
SAN 接続ポリシー	自動 vNIC 配置 ID に対して変動検出はサポートされていません。 （注） 変動の検出は、サーバーの電源が入っている場合にのみサポートされます
電源ポリシー	電源のプライオリティ（Power Priority）プロパティでは、ドリフト検出はサポートされていません。

サーバ プロファイルのインポート

Intersight では、スタンドアロン モードの C シリーズ サーバおよび Intersight 管理モード（IMM）の FI アタッチ サーバの構成の詳細を、Cisco IMC から直接インポートすることができます。サーバー プロファイルのインポートでは、プロファイルやポリシーを手動で作成する必要なく、サーバーの既存の構成を Intersight に移行できます。サーバ プロファイルのインポート操作では、サーバ構成に基づき、プロファイルと関連付けられたポリシーが作成されます。ゴールデン構成プロファイルを作成してそのプロファイルを複製し、Intersight ですでに要求されている別のサーバに適用することができます。

サーバ プロファイル構成は、Intersight の次の場所からインポートできます。

- **[サーバ（Servers）]** テーブル ビュー：テーブル ビューでスタンドアロン モードの Cisco UCS C シリーズ サーバまたは Intersight 管理モード（IMM）の FI アタッチ サーバを選択し、省略符号（**[…]**）をクリックして、**[サーバ プロファイルのインポート（Import Server Profile）]** を選択します。
- [サーバの詳細（Server details）] ページにアクセスするには、[サーバ（Servers）] テーブル ビューで、スタンドアロン モードの C シリーズサーバまたは Intersight 管理モード（IMM）の FI アタッチ サーバをクリックします。右上隅の **[アクション（Actions）]** をクリックし、**[サーバ プロファイルのインポート（Import Server Profile）]** を選択します。このオプションは、サーバに関連付けられたサーバプロファイルがない場合にのみ有効です。

（注） サーバプロファイルのインポートが部分的だと、テンプレートにアタッチすることも、テンプレートの作成に使用することもできません。

サーバ プロファイル インポートのインポート方法、およびエンドポイントでの手動設定変更の検出の詳細については、「サーバプロファイルのインポート」（「リソース」）を参照してください。

影響の予測

スタンドアロンおよび Intersight Managed Mode サーバの Estimate Impact ワークフローは、サーバ プロファイルが展開されたときに、サーバ プロファイルにアタッチされたさまざまなポリシーによって引き起こされる中断を分析します。ポリシーがアタッチ、デタッチ、または更新されると、インパクト分析ワークフローがトリガされます。混乱は、各ポリシーに対して示されています。ポリシーによって引き起こされる可能性のある混乱は次のとおりです。

- 永続メモリ ポリシーやアダプタ ポリシーなどのスタンドアロン サーバ ポリシーでは、即時の再起動が必要です。このような場合、ポリシーに対して示される中断は**即時リブート**です。
- サーバプロファイルでのアクティブ化アクションでは、サーバを再起動して、サーバ上のポリシー構成をアクティブ化する必要があります。このような場合、ポリシーに対して示される中断は、**Activate Requires Reboot** です。

- IMC アクセス ポリシーなどの一部のポリシーでは、サーバ管理ネットワークが短時間停止します。このような場合、ポリシーに対して示される中断は、**ネットワーク管理の停止**です。

サーバ プロファイルの展開とアクティブ化

展開と**アクティブ化**は、サーバプロファイルで実行できる2つの明示的なアクションです。ポリシー構成のステージングは、サーバプロファイルの展開の一部として行われます。ポリシーのステージングにより、ポリシー構成をステージングし、ポリシーをアクティブ化するための保留中のアクションを把握できます。ポリシーをアクティブ化するには、サーバを手動で再起動するか、メンテナンス ウィンドウ中にサーバ プロファイルの**アクティブ化**アクションを使用します。ポリシーのアクティブ化の失敗は、**アクティブ化**アクションがトリガされたときに識別されます。

サーバプロファイル テーブル ビューの**ステータス** ウィジェットには、**不整合**状態のプロファイルの数が表示されます。サーバプロファイルにまだ展開またはアクティブ化されていないポリシー変更がある場合、サーバプロファイルは**不整合**状態になります。**不整合の理由**ウィジェットは、プロファイルが**不整合**状態にある理由を示します。サーバープロファイルは、次の理由で**不整合**状態になる可能性があります。

- サーバーに割り当てられたサーバプロファイルに添付されたポリシーに変更があります。
- ポリシー構成が、エンドポイントに展開された構成と同期していません。
- ポリシーは**アクティブ化されていない**状態です。

展開アクションを使用して、構成の変更をステージングできます。展開中に、トグルボタンを有効にして**すぐに再起動**するように選択できます。有効にすると、サーバが再起動し、サーバプロファイルがすぐにアクティブになります。無効にした場合、ポリシー構成の変更は次の再起動時に有効になります。

サーバプロファイルの詳細の**アクティブ化**アクションは、サーバを再起動し、サーバの構成をアクティブ化します。**展開**をトリガーして構成の変更をステージングし、後でメンテナンス ウィンドウ中に**アクティブ化**をトリガして、展開された構成をアクティブにすることができます。

ポリシー編集ページの **[更新および展開（Update and Deploy）]** オプションを使用すると、ポリシー構成を変更し、ポリシーが添付されている複数のサーバプロファイルに変更を展開できます。

UCS サーバ プロファイルの作成

サーバプロファイルでは、1台のサーバとそのサーバのストレージ、管理、およびネットワークの特性を定義します。サーバ プロファイルがサーバに展開されると、Cisco Intersight が、そのサーバプロファイルで指定された設定に一致するように、サーバとその接続を自動的に設定します。

（注） サーバ プロファイルは、サーバ プロファイルテンプレートから取得することもできます。詳細は、サーバ プロファイル テンプレートを参照してください。

ステップ 1 Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

ステップ 2 **[サービス プロファイル（Service Profiles）]** > **[CS サーバ プロファイル CS Server Profiles）]** タブに移動し、**[UCS サーバ プロファイルの作成（Create UCS Server Profile）]** をクリックします。

ステップ 3 **[全般（General）]** ページで、以下の情報を設定します。

a) **[名前（Name）]**：サーバ プロファイルの名前です。

b) **[ターゲット プラットフォーム（Target Platform）]**：ポリシーが適用されるターゲット プラットフォームです。これは、**[スタンドアロン（Standalone）]** サーバまたは **[FI 接続サーバ（FI Attached）]** サーバのいずれかです。

スタンドアロン サーバ用に作成された UCS サーバ プロファイルは、FI 接続サーバに展開できません。同様に、FI 接続サーバ用に作成された UCS サーバ プロファイルをスタンドアロン サーバに展開することはできません。

c) （任意）**[タグ（Tag）]**：プロファイルのタグです。タグは key：value 形式である必要があります。たとえば、Org: IT または Site: APJ などです。

d) （任意）**[説明（Description）]**：プロファイルの識別に役立つ説明です。

ステップ 4 **[サーバー割り当て（Server Assignment）]** ページで、サーバー プロファイルにサーバーを割り当てます。サーバーの割り当てには、次のオプションのいずれかを選択できます。

- **[特定のサーバからの割り当て（Assign from a Specific Server）]**：このオプションを使用して、直ちにサーバをサーバ プロファイルに割り当てます
- **[リソース プールからのサーバーの割り当て（Assign Server from a Resource Pool）]**：このオプションを使用して、リソース プールからサーバーをサーバー プロファイルに割り当てます。
- **[シャーシ スロットの場所による割り当て（Assign by Chassis Slot Location）**：このオプションを使用して、ドメイン名、シャーシ ID、およびスロット ID を使用してサーバをサーバ プロファイルに事前に割り当てます。
- **[シリアル番号による割り当て（Assign by Serial Number）]**：このオプションを使用して、サーバのシリアル番号を使用してサーバをサーバ プロファイルに事前に割り当てます。

  （注）
  - Cisco UCS B シリーズ サーバは、**シャーシ スロットの場所**または**シリアル番号**を使用して事前に割り当てることができます。
  - Cisco Intersight 管理モード C シリーズ サーバおよび Cisco UCS C シリーズ スタンドアロン サーバは、**シリアル番号**を使用してのみ事前に割り当てることができます。

- **[後で割り当て（Assign Later）]**：このオプションを使用して、後でサーバーをサーバー プロファイルに割り当てます。

サーバー割り当てテーブルには、サーバーまたはリソース プールのリストとその詳細が表示されます。次のいずれかのオプションを使用して、詳細を表示できます。

- **[すべてを表示（Show All）]**：現在存在するすべてのサーバーまたはリソース プールを表示します。
- **[選択を表示（Show Selected）]**：選択されている現在のサーバーまたはリソース プールを表示します。
- **[選択を解除（Unselect）]**：選択を解除します。

ステップ 5 [次へ（Next)] をクリックします。

ステップ 6 **[コンピューティング構成（Compute Configuration）]** ページで、以下を実行します。

a) 適切な**[UUID 割り当て（UUID Assignment）]** を選択します。

- **[プール（Pool）]**：サーバーへの UUID プールの関連付けを許可します。
- **[静的（Static）]**：静的UUIDアドレスを使用したサーバーへのUUIDの関連付けを許可します。

b) 既存のポリシーを選択するか、新しいポリシーを作成します。

c) [次へ（Next)] をクリックします。

ステップ 7 **[管理（Management）]** ページで、**[UCS サーバ プロファイル（UCS Server Profile）]** に必要なポリシーをアタッチし、**[次へ（Next）]** をクリックします。

ステップ 8 **[ストレージ（Storage）]** ページで、必要なポリシーを **[UCS サーバ プロファイル（UCS Server Profile）]** にアタッチし、**[次へ（Next）]** をクリックします。

ステップ 9 **[ネットワーク設定（Network Configuration）]** ページで、必要なポリシーを **[UCS サーバ プロファイル（UCS Server Profile）]** にアタッチし、**[次へ（Next）]** をクリックします。

ステップ 10 **[概要（Summary）]** ページで、UCS サーバプロファイルとそれに関連付けられているポリシーの詳細を確認します。

ステップ 11 **[展開（Deploy）]** をクリックしてUCS サーバプロファイルを作成し、割り当てられたサーバに展開します。

（注）
- **[リソース プールからサーバーを割り当て（Assign Server from a Resource Pool）]** 割り当てタイプの場合に、リソースがリソース プールで使用できないと、サーバー プロファイルのステータスは **[リソース プールからサーバーを割り当て（Waiting for Resources）]** に変わります。同様の動作は、サーバ プロファイルの事前割り当てにも見られます。後でサーバーがリソース プールに追加されると、サーバーは **[リソースを待機中（Waiting for Resources）]** ステータスのものからサーバー プロファイルに自動的に追加されます。

  サーバプロファイルが待機状態になると、**アラーム**が発生します。サーバがサーバプロファイルに割り当てられると、自動的にクリアされます。
- リソースプールは、サーバーの動的選択をサポートしていません。サーバーをリソースプールに手動で割り当て、自動化されたサーバー プロファイルの割り当てを続行できます。
- サーバプロファイルの事前割り当ては、サーバが割り当てられるまでの1回限りの操作です。サーバが割り当てられると、事前に割り当てられたプロパティは失われ、他の既存のサーバプロファイルとして機能し続けます。
- リソース プールの作成とリソース プールの詳細の表示の詳細については、「リソース プール」を参照してください。
- UUID プールの作成と UUID プールの詳細の表示の詳細については、「UUID プール」を参照してください。

UCS サーバ プロファイルの詳細

[UCS サーバ プロファイルの詳細（UCS Server Profile Details）] ページには、UCS サーバ プロファイルとその割り当て先のサーバの詳細が表示されます。[UCS Server Profiles Table] ビューから [UCS Server Details] に移動します。このページでは、次の作業を行うことができます。

- UCS サーバ プロファイル **アクション**を実行します。
  - **[展開（Deploy）]**：ファブリック インターコネクト ペアに UCS サーバ プロファイルを展開します。

（注） このアクションは、サーバが割り当てられているサーバプロファイルで実行できます。

  - **[割当解除（Unassign）]**：ファブリック インターコネクト ペアから UCS サーバ プロファイルの割り当てを解除します。

（注） このアクションは、サーバが割り当てられているサーバプロファイルで実行できます。

- **[編集（Edit）]** : UCS サーバ プロファイルのプロパティを編集します。
- **[複製（Clone）]** : 既存の UCS サーバ プロファイルと同様のプロパティを使用して UCS サーバ プロファイルを複製します。クローンは、元の UCS サーバ プロファイルと同じポリシーに関連付けられます。
- **[Delete（削除）]**—Delete the server profile.
- **[Attach to template（テンプレートに接続）]** : 既存のサーバ プロファイルテンプレートにサーバ プロファイルを接続します。

（注） このアクションは、どのテンプレートにもアタッチされていないサーバ プロファイルで実行できます。

- **[テンプレートの作成（Create a template）]** : サーバ プロファイルのプロパティを使用して新しいテンプレートを作成します。

（注） このアクションは、どのテンプレートにもアタッチされていないサーバプロファイルで実行できます。

- **[テンプレートから分離（Detach from template）]** : サーバプロファイルをテンプレートから分離し、そのプロパティを変更します。

（注） このアクションは、サーバプロファイルテンプレートにアタッチされているサーバ プロファイルで実行できます。

- **[タグの管理（Manage Tags）]** : key：value形式でプロファイルのタグを設定します。

- UCS サーバ プロファイルの [**Details（詳細）]** は、**[全般（General）]** タブでを表示します。

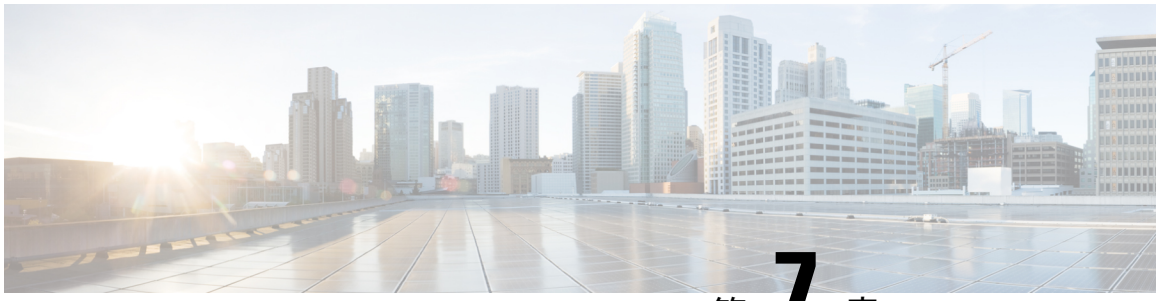
[プロパティ（Property）]	**[基本情報（Essential Information）]**
ステータス（Status）	ファブリック インターコネクト ペアでのUCSサーバプロファイルの展開のステータス。次のようになります。 • **OK** • **失敗（Failed）** • **[未割り当て（Not Assigned）]** • **未展開（Not Deployed）**
名前（Name）	UCS サーバ プロファイル名。

[プロパティ（Property）]	[基本情報（Essential Information）]
サーバ（Server）	関連付けられているサーバの名前。
[最終更新（Last Update）]	UCS サーバ プロファイルが最後に更新された日時。
タグ（Tags）	選択したオブジェクトの既存のタグがデフォルトで表示されます。[管理（Manage）]をクリックして、新しいタグを追加するか、既存のタグを変更します。

サーバ プロファイルに関連付けられているポリシーを表示します。関連付けられたポリシーの詳細を表示するには、ポリシー名をクリックします。

サーバプロファイルに関連付けられているポリシーを展開した後にそのポリシーを変更したり、または新しいポリシーをプロファイルに追加した場合は、[サーバ プロファイル（Server Profile）] テーブル ビューにプロファイルへの編集内容または参照先のポリシーを反映した未展開の変更が表示されます。[サーバ プロファイルの詳細（Server Profile Detail）] ビューには参照先のポリシーが強調表示され、[変更の表示（View Changes）] ウィンドウには実際の変更を表示することができます。[サービスプロファイル（Service Profiles）] テーブルビューから設定の詳細を表示することもできます。

- [サーバ（Server）] タブで、割り当てられたサーバとそのプロパティを表示します。
- [インベントリ（Inventory）] タブで、割り当てられたサーバのインベントリを表示します。



第 7 章

UCS シャーシ プロファイルの設定

- UCS シャーシ プロファイルの概要 （79 ページ）
- シャーシ プロファイル テンプレートの作成とプロファイルの取得 （80 ページ）
- シャーシ プロファイルの作成 （82 ページ）
- UCS シャーシ プロファイルの詳細 （82 ページ）

UCS シャーシ プロファイルの概要

UCS シャーシ プロファイルの概要

UCS シャーシ プロファイルは、シャーシ ポリシーを作成し、Intersight 管理モード（IMM）が要求するシャーシに関連付けることを可能にします。シャーシプロファイルがシャーシに関連付けられると、Cisco Intersight は自動的にシャーシ プロファイルのポリシーで指定された設定に一致するようにシャーシを設定します。シャーシ関連ポリシーは、作成時または作成後にプロファイルに関連付けることが接続できます。

重要

- シャーシ プロファイル機能は、次の場合にのみ Cisco Intersight で使用できます。
  - Cisco Intersight の Essentials ライセンスがインストールされている。
  - アカウント管理者またはサーバ管理者のいずれかである。
- シャーシプロファイルにアタッチされたポリシーは、プロファイルの作成前に作成することも、プロファイルの作成中に作成することもできます。
- 展開後にシャーシポリシーが変更されると、シャーシプロファイルは**[変更保留（Pending Changes）]**状態に設定されるので、変更されたポリシーを手動でシャーシに再度関連付ける必要があります。
- シャーシポリシーは、シャーシ内の両方の入出力モジュール（IOM）に適用されます。いずれかのIOMにだけポリシーを適用できない場合でも、シャーシポリシーの関連付けワークフローは失敗します。
- IMC アクセス ポリシーと SNMP ポリシーは、現在、Cisco UCS X シリーズ ダイレクト シャーシ（UCSX-9508）ではサポートされていません。

シャーシプロファイルテンプレートの作成とプロファイルの取得

シャーシ プロファイル テンプレートを使用すると、シャーシ プロファイルを簡単に取得して大規模に展開できるテンプレートを定義できます。この方法は、同じポリシーセットを使用する多数のシャーシ プロファイルが必要な場合に特に便利です。テンプレートで加えたプロパティの変更は、すべての派生プロファイルと継承されます。それらの変更されたプロファイルは個別に展開できます。詳細については、「シャーシ プロファイル テンプレート」を参照してください。

シャーシ プロファイル テンプレートを作成し、プロファイルを取得するには、次の手順を実行します。

1. Cisco Intersight にログインします。
2. **[サービス セレクタ（Service Selector）]**ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[構成（Configure）]** > **[テンプレート（Templates）]** の順に選択し、**[シャーシ プロファイル テンプレート テーブル ビュー（Chassis Profile Template Table View）]** を起動します。
4. シャーシテンプレートを作成するには、**[UCS シャーシ プロファイル テンプレートの作成（Create UCS Chassis Profile Template）]** をクリックします。
5. [全般（General）] ページで、次の手順を実行します。

1. リストからテンプレートの組織を選択します。このフィールドは、組織間で共有している構成の機能をサポートします。
2. テンプレートの名前を入力します。
3. テンプレートのタグを入力します。タグは key：value 形式である必要があります。たとえば、Org: IT または Site: APJ などです。
4. テンプレートの識別を可能にする説明を入力します。
5. **[次へ（Next）]** をクリックします。

6. **[シャーシの設定（Chassis Configuration）]** ページで、IMC アクセス ポリシー、電源ポリシー、SNMPポリシー、および温度ポリシーを作成または選択し、**[次へ（Next）]**をクリックします。
7. **[概要（Summary）]** ページで、次の手順を実行します。
   1. テンプレートとそれにアタッチされているポリシーの詳細を確認します。
   2. 後でプロファイルを取得する場合は、**[閉じる（Close）]** をクリックします。このテンプレートからプロファイルを取得するには、**[プロファイルの取得（Derive Profiles）]** をクリックします。
8. テンプレートを取得するには、次の手順を実行します。
   1. **[全般（General）]** ページで、次の手順を実行します。
      1. **[シャーシの割り当て（Chassis Assignment）]** で、テンプレートを複数のシャーシに割り当てます。

         サーバーの割り当てには、次のオプションのいずれかを選択できます。

         - **[今すぐ割り当て（Assign now）]**：このオプションを使用して、シャーシをすぐにシャーシ プロファイルに割り当てます。
         - **[後で割り当て（Assign later）]**：後でシャーシをシャーシ プロファイルに割り当てるには、このオプションを使用します。

      2. **[取得するプロファイルの数（Number of Profiles to lease ）]** フィールドに、取得するプロファイルの数を入力します。
   2. **[詳細（Details）]** ページで、プロファイルの説明、タグ、および自動生成された名前を表示および編集し、**[次へ（Next）]** をクリックします。
   3. **[概要（Summary）]**ページで、シャーシプロファイルテンプレートの設定を確認し、**[プロファイルの取得（Derive Profiles）]** をクリックします。

テーブル ビューには、シャーシ テンプレートとその詳細のリストが表示されます。

シャーシ プロファイルの作成

シャーシ プロファイルは、再利用可能なポリシーを使用してシャーシを設定します。

ステップ 1 Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

ステップ 2 **[プロファイル（Profiles）]> [シャーシ プロファイル（Chassis Profiles）]** タブに移動し、**[USC シャーシ プロファイルの作成（Create UCS Chassis Profile）]** をクリックします。

ステップ 3 **[全般（General）]** ページで、組織を選択し、プロファイルの名前を入力します。必要に応じて、プロファイルの識別に役立つ短い説明とタグ情報を含めます。タグは key：value 形式である必要があります。たとえば、Org: IT または Site: APJ などです。

ステップ 4 **[シャーシ割り当て（Chassis Assignment）]** ページで、**[シャーシ プロファイル（Chassis Profile）]** にシャーシを割り当てます。**[後で割り当てる（Assign Later）]** をクリックして、後でシャーシプロファイルにシャーシを割り当てることもできます。

ステップ 5 **[次へ（Next）]** をクリックします。

ステップ 6 **[シャーシ設定（Chassis Configuration）]** ページで、必要なポリシーをアタッチし、**[次へ（Next）]** をクリックします。

ステップ 7 **[サマリー（Summary）]** ページで、**[UCS シャーシ プロファイル]** とそれに関連付けられているポリシーの詳細を確認します。

ステップ 8 **[展開（Deploy）]** をクリックして、割り当てられたファブリックインターコネクトに **[UCS シャーシ プロファイル]** を展開します。

UCS シャーシ プロファイルの詳細

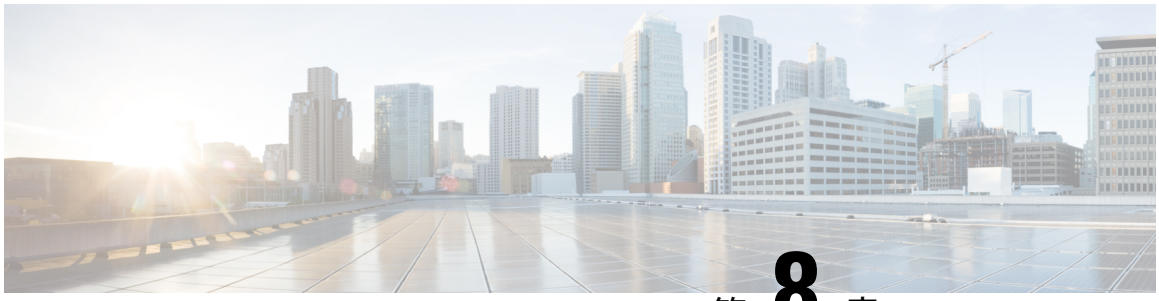
[UCS シャーシ プロファイルの詳細（UCS Chassis Profile Details）] ページでは、次の操作を実行できます。

- シャーシ プロファイル **[アクション（Action）]** の実行：
  - **[展開（Deploy）]**：ファブリック インターコネクト ペアにシャーシ プロファイルを展開します。
  - **[編集（Edit）]**：シャーシ プロファイルのプロパティを編集します。
  - **[シャーシの割り当て解除（Unassign Chassis）]**：ファブリックインターコネクトペアからシャーシプロファイルの割り当てを解除します。
- UCS シャーシ プロファイルの **[詳細（Details）]** の表示：
  - **[ステータス（Status）]**：ファブリック インターコネクト ペアでのシャーシプロファイルの展開のステータス。
    - **OK**

- **[未割り当て（Not Assigned）]**
- **未展開（Not Deployed）**
- **[失敗（Failed）]**
- **[変更を未展開（Not Deployed Changes）]**

- **[名前（Name）**：シャーシ プロファイルの名前。
- **[シャーシ（Chassis）]**：シャーシの詳細。
- **[最終更新日（Last Update）]**：シャーシ プロファイルが最後に更新された日時。
- **[説明（Description）]**：シャーシプロファイルの説明。
- **[組織（Organization）]**：選択した組織が表示されます。デフォルトの組織を設定するには、**[デフォルト（default）]** をクリックします。
- **[タグ（Tags）]**：デフォルトでは、選択したオブジェクトの既存のタグが表示されます。新しいタグを追加するか、既存のタグを変更するには、**[設定（Set）]**をクリックします。

- シャーシ プロファイルにアタッチされている **[ポリシー（Policies）]** を表示します。



第 8 章

UCS ドメイン ポリシーの設定

- ドメイン ポリシー （85 ページ）
- ポート ポリシーの作成 （89 ページ）
- イーサネット ネットワーク グループ ポリシーの作成 （101 ページ）
- イーサネット ネットワーク制御ポリシーの作成 （103 ページ）
- VLAN ポリシーの作成 （105 ページ）
- VSAN ポリシーの作成 （108 ページ）
- NTP ポリシの作成 （110 ページ）
- ネットワーク接続ポリシーの作成 （112 ページ）
- SNMP ポリシーの作成 （114 ページ）
- システム QoS ポリシーの作成 （117 ページ）
- Syslog ポリシーの作成 （119 ページ）
- スイッチ制御ポリシーの作成 （121 ページ）
- フロー制御ポリシーの作成 （131 ページ）
- リンク集約ポリシーの作成 （134 ページ）
- リンク集約ポリシーの作成 （135 ページ）
- マルチキャスト ポリシーの作成 （136 ページ）

ドメイン ポリシー

Cisco Intersight のドメイン ポリシーを使用すると、ポート設定、ネットワーク制御設定、VLAN と VSAN の設定など、UCS ファブリック インターコネクトのさまざまなパラメータを設定できます。ドメイン ポリシーは、任意の数のドメイン プロファイルに割り当てることで、構成基準を提供できます。Cisco Intersight のドメイン ポリシーは、アプリケーションに固有の新機能です。ドメイン プロファイルを使用したポリシーベースの構成は Cisco Intersight Essentials の機能であり、Cisco UCS B シリーズ M5 および M6 サーバ、Cisco UCS C シリーズ M5、M6、および M7 サーバ、および UCS ドメイン内の Cisco UCS X シリーズ M6 および M7 サーバでサポートされます。

Cisco Intersight のドメイン ポリシー作成ウィザードには 2 つのページがあります。

- **[全般（General）]**：組織を選択し、ポリシーの名前を入力できます。オプションで、ポリシーの識別に役立つ短い説明とタグ情報を含められます。タグはkey：value形式である必要があります。たとえば、Org:IT または Site:APJ などです。
- **[ポリシーの詳細（Policy Details）]**：ポリシーの詳細ページには、UCS ドメイン ポリシーに適用可能なプロパティがあります。

Cisco Intersight で設定できるドメイン ポリシーは次のとおりです。

- **[ポート ポリシー（Port Policy）]**：ファブリック インターコネクトのポートとポート ロールを設定します。各ファブリック インターコネクトには、ポートの集合が固定ポート モジュール内に存在します。ポートまたはポート チャネルをイネーブルまたはディセーブルにできます。

  ポート ポリシーはスイッチ モデルに関連付けられます。ネットワーク設定の制限は、スイッチ モデルによっても異なります。

  サポートされるポートとポート チャネルの最大数は次のとおりです。

  - イーサネット アップリンク、Fibre Channel over Ethernet（FCoE）アップリンク ポート チャネル、およびアプライアンス ポート チャネル（組み合わせ）：12
  - ポート チャネルあたりのイーサネット アップリンク ポート：16
  - ポート チャネルごとの FCoE アップリンク ポート：16
  - イーサネット アップリンクおよび FCoE アップリンク ポート（複合）：31
  - サーバ ポート：Cisco UCS 6454 では 54 ポート、Cisco UCS 64108 ファブリック インターコネクトでは 108 ポート

- **[イーサネット ネットワーク制御ポリシー（Ethernet Network Control Policy）]**：アプライアンス ポート、アプライアンス ポート チャネル、または vNICS のネットワーク制御構成を行います。
- **イーサネットネットワークグループポリシー（Ethernet Network Group Policy）**：アプライアンス ポート、アプライアンス ポート チャネル、または vNIC の許可 VLAN およびネイティブ VLAN を構成します。
- **[VLAN 設定ポリシー（VLAN Configuration Policy）]**：特定の外部 LAN への接続を生成します。
- **[VSAN 設定ポリシー（VSAN Configuration Policy）]**：ファイバ チャネル ファブリックを 1 つ以上のゾーンに分割します。各ゾーンでは、VSAN で相互通信できるファイバ チャネル イニシエータとファイバ チャネル ターゲットのセットが定義されます。
- **[NTP ポリシー（NTP Policy）]**：NTP サービスを有効にして、Cisco Intersight によって管理される UCS システムが NTP サーバの時刻と同期するように設定します。NTP サービスを有効化するには、NTP サーバとして動作する 1 ～ 4 台のサーバの IP/DNS アドレスを指定する必要があります。NTP サービスを有効にすると、Cisco Intersight によりエンドポイ

ント側で NTP の詳細が設定されます。詳細については、「NTP ポリシーの作成」を参照してください。

- **[ネットワーク接続ポリシー（Network Connectivity Policy）]**：エンドポイントから DNS サーバ上のリソース レコードを追加または更新するために使用される DNS ドメイン設定と、エンドポイント上の IPv4 および IPv6 用の DNS サーバ設定を指定します。

- **[システム QoS ポリシー（System QoS Policy）]**（プレビュー）：個々の vNIC にシステム クラスを割り当てることで、接続されたネットワークの重要性に基づいてネットワーク トラフィックの優先順位付けを行います。Intersight は、DCE（Data Center Ethernet）を使用して、Cisco UCS ドメイン内のすべてのトラフィックを処理します。イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。それ以外の 6 つの仮想レーンの Quality of Service（QoS）を設定できます。Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

  各システム クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。たとえば、[ファイバ チャネル優先度（Fibre Channel Priority）] システム クラスを設定して、FCoE トラフィックに割り当てる DCE 帯域幅の割合を決定することができます。構成のセットアップでは、システム クラスの各入力を検証して、重複または無効なエントリを防止します。

  この機能はプレビューであり、実稼働環境で使用するためのものではありません。Cisco では、テスト ネットワークまたはテスト システムでこの機能を使用することを推奨しています。

  次のリストは、設定可能なシステム クラスをまとめたものです。

  - Platinum、Gold、Silver、および Bronze：これらは、サービスプロファイルの QoS ポリシーに含めることができる設定可能なシステム クラスのセットです。各システム クラスはトラフィック レーンを 1 つ管理します。これらのシステム クラスのプロパティはすべて、カスタム 設定やポリシーを割り当てるために使用できます。

  - ベスト エフォート（Best Effort）：基本的なイーサネット トラフィックのために予約されたレーンに対する QoS を設定するシステム クラスです。このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。このシステム クラスをディセーブルにはできません。

  - ファイバ チャネル（Fibre Channel）：これは、Fibre Channel over Ethernet トラフィックのために予約されたレーンでの Quality of Service を設定するシステム クラスです。このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。このシステム クラスをディセーブルにはできません。

- **マルチキャストポリシー（Multicast Policy）**（プレビュー）：インターネット グループ管理プロトコル（IGMP）のスヌーピングおよびIGMPクエリアの設定に使用されます。IGMPスヌーピングは、特定のマルチキャスト伝送に含まれるべき VLAN のホストを動的に決定します。

  1 つ以上の VLAN に関連付けることができるマルチキャスト ポリシーを作成、変更、削除できます。マルチキャスト ポリシーが変更されると、そのマルチキャスト ポリシーに関連付けられたすべてのVLANが再処理され変更が適用されます。デフォルトでは、IGMPスヌーピングが有効になり、IGMP クエリアが無効になります。IGMP クエリアをイネーブルにすると、ローカルおよびピア IGMP スヌーピングクエリアインターフェイスの IPv4 アドレスを設定できます。

- **[Simple Network Management Protocol（SNMP）ポリシー（Simple Network Management Protocol (SNMP) Policy）]**：管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するためのSNMPを設定します。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。

- **[Syslog ポリシー（Syslog Policy）]**：エンドポイントのローカル ロギングとリモート ロギング（最小シビラティ（重大度））を設定できます。このポリシーは、ローカルファイルおよびリモート syslog サーバに syslog メッセージを保存するための設定サポートも提供します。

- **[スイッチ制御ポリシー（Switch Control Policy）]**（プレビュー）：次を含むファブリック インターコネクト（FI）の複数のネットワーク操作を設定および管理できます。

  - **[ポート数の最適化（Port Count Optimization）]**：VLAN ポート数の最適化が有効になっている場合は、仮想ポート（VP）グループがファブリック インターコネクト（FI）で設定され、VLANポート数の最適化が無効になっている場合は、設定された VP グループが FI から削除されます。

  - **[MAC エージングタイム（MAC Aging Time）]**：MAC アドレステーブルエントリの MAC エージングタイムを設定できます。MAC エージングタイムは、MAC エントリが期限切れになり、MAC アドレステーブルからエントリを廃棄するまでの時間を指定します。

  - **[リンク制御グローバル設定（Link Control Global Settings）]**：メッセージ間隔時間の設定を秒単位で有効にし、err-disabled状態のポートの回復アクションをリセットできます。

- **[フロー制御ポリシー（Flow Control Policy）]**：ポートおよびポート チャネルのプライオリティフロー制御の設定を有効にします。

- **[リンク制御ポリシー（Link Control Policy）]**：ポートのリンク制御管理状態と設定（通常またはアグレッシブ）モードを有効にします。

- **[リンク集役ポリシー（Link Aggregation Policy）]**リンク集約プロパティを設定できます。リンク集約は、複数のネットワーク接続を並列に組み合わせて、スループットを向上させ、冗長性を実現します。

ポート ポリシーの作成

ポートポリシーは、イーサネットまたはファイバチャネルトラフィックを伝送するユニファイドポート、ポートの役割、速度などのポートパラメータの設定に使用されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ポート（Port）]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
スイッチ モデル	次の スイッチ モデルのいずれか 1 つを選択します。 • Cisco UCS 64108 ファブリック インターコネクト • Cisco UCS 6454 ファブリック インターコネクト • Cisco UCS 6536 ファブリック インターコネクト • Cisco UCS ファブリック インターコネクト 9108 100G （注） スイッチモデルは、さまざまなネットワーク設定機能をポリシーに提供します。ポリシーが作成されると、スイッチモデルは変更できません。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
ユニファイド ポート デフォルトでは、未設定のすべてのポートはイーサネット ポートです。青いスライダーを使用して、ファイバーチャネルポートの範囲を選択します。選択したファイバーチャネル ポートが青色で強調表示されます。	
ファイバ チャネル（FC）	ファイバチャネル用に選択されたポート範囲を表示します。 （注） • Cisco UCS 6454 ファブリック インターコネクトの有効なFCポート範囲：**[ポート 1 ～ 16（Port 1-16）]** • Cisco UCS 64108 ファブリック インターコネクトの有効な FC ポート範囲：**ポート 1 ～ 16** • Cisco UCS 6536 ファブリック インターコネクトの有効なFCポート範囲：**ポート 33 ～ 36** • Cisco UCS ファブリック インターコネクト 9108 100G の有効な FC ポート範囲：**ポート 1 ～ 2**
イーサネット	イーサネット用に選択されたポート範囲を表示します。

7. **[ブレイクアウトオプション]**ページで、ファイバーチャネルまたはイーサネットのブレイクアウト ポートを構成します。

（注） ブレイクアウト ポートを構成するには、ファブリック インターコネクト ファームウェアをファームウェア バージョン 4.2(2a) 以降にアップグレードする必要があります。

Cisco UCS 6536 ファブリック インターコネクトでは、FC ブレークアウトのみがサポートされています。

- グラフィック画像内の有効なポートをクリックするか、画像の下にある表でポート番号を選択して、ブレイクアウトするポートを選択します。

  以下は、さまざまなCisco UCSファブリック インターコネクトのブレイクアウト ポート範囲です。

- Cisco UCS 64108 ファブリック インターコネクト、有効なブレイクアウト ポート範囲は 97 ～ 108
- Cisco UCS 6454 ファブリック インターコネクト、有効なブレークアウトポート範囲は 49 ～ 54
- Cisco UCS 6536 ファブリック インターコネクト。有効なブレイクアウト ポートの範囲は 1 ～ 36
- Cisco UCS ファブリック インターコネクト 9108 100G、有効なブレイクアウト ポート範囲は 1 ～ 8

• [構成（Configure）] をクリックします。

ポップアップ ウィンドウが表示されます。ブレークアウト ポートに設定できる管理速度が表示されます。

イーサネット ブレークアウト ポートは、ブレークアウトなし、4x10G の管理速度、4x25G の管理速度の 3 つのオプションで構成できます。

FC ブレークアウト ポートは、4x8G、4x16G、および 4x32G の 3 つの異なる**管理速度**で構成できます。

• 目的の速度を選択します

（注） イーサネットブレークアウトを構成し、FI のリブートを必要とせずにブレークアウト速度を切り替えることができます。

FC ブレークアウト速度を変更しても、FI をリブートする必要はありません。

イーサネット ブレイクアウトから FC ブレイクアウトへの切り替え、またはその逆の切り替え、またはイーサネット ポートから FC ブレイクアウト ポートへの切り替え、またはその逆の切り替えには、毎回 FI のリブートが必要です。

• [設定（Set）] をクリックします。

• [次へ（Next）] をクリックします。

8. **[ポート ロール（Port Roles）]** ページで、グラフィック イメージで、またはグラフィック画像の下にある表で選択して、ポート ロール用に構成する必要があるポートを選択します。

選択したポート	選択したポート番号を示します。
名前	ユーザが決定したポート名。
タイプ（Type）	タイプは**イーサネット**または **FC**. です。

[ロール（Role）]	

	ポートロールタイプを選択します。 イーサネット ポートのロールは次のとおりです。 • **Unconfigured**：デフォルト • **サーバ（Server）** トラフィックはすべて、I/O モジュールを経由して、ファブリック インターコネクトのサーバ ポートへ進みます。 （注） • Cisco UCS 6454 ファブリックインターコネクトの場合、許可されるサーバポートの最大数は、54 です。Cisco UCS 64108 ファブリックインターコネクトの場合、許可されるサーバポートの最大数は、108 です。 • Cisco UCS 6536 ファブリック インターコネクトの場合、サーバー ロールは 10G ブレークアウト ポートではサポートされていません。 • サーバー ポート構成は、Cisco UCS 6454 ファブリック インターコネクトのポート 49 ～ 54 および Cisco UCS 64108 ファブリック インターコネクトのポート 97 ～ 108 でブレークアウト ポートを構成した後にのみ、直接接続 Cisco UCS C シリーズ サーバーを検出するためにサポートされます。 • Cisco UCS 6454 ファブリック インターコネクトの場合はポート 49 ～ 54、Cisco UCS 64108 ファブリック インターコネクトの場合はポート 97 ～ 108 にブレークアウト ポートを設定した後、シャーシ、シャーシに接続されたブレードサーバ、またはFEX に接続されたラック サーバの検出はサポートされません。 • Cisco UCS ファブリック インターコネクト 9108 100G、サーバーロールはポートロール構成には使用できません。 • **イーサネットアップリンク**：イーサネットトラフィックはユニファイドアップリンクポートを通過します。 （注） 許可されるイーサネットアップリンクポートと FCoE アップリンクポートの最大数は 31 です。 • **アプライアンス**：トラフィックがアップリンクポートを通過することなく、ネットワークファイルシステムがファブリックインターコネクトに直接接続できるようにします。

	FC ポートのロールは次のとおりです。 • **FC アップリンク**：FC トラフィックは FC アップリンク ポートを通過します。FC ポートのロールを FC アップリンク ポートとして指定するには、ポートの VSAN スコープが、VSAN 設定ポリシーでストレージおよびアップリンクとして、またはアップリンクとして作成されている必要があります。 • **[FC ストレージ（FC Storage）]**—FC ポートはストレージ ポートとして機能します。FC ポートのロールを FC ストレージ ポートとして指定するには、ポートの VSAN スコープが、VSAN 設定ポリシーでストレージおよびアップリンクとして、またはストレージとして作成されている必要があります。さらに、FC がスイッチング モードになっている必要があります。 • **[未構成（Unconfigured）]**—未構成は、ポートのデフォルトのロールです。

管理速度	管理ポートの速度です。次のオプションがあります。 • 1GBPS • 10GBPS • 25GBPS • 40GBPS • 100GBPS （注） • ブレークアウト ポートのどのロールに対しても、管理速度を選択することはできません。 • Cisco UCS 6536 ファブリック インターコネクトの場合、サーバ ポートでは 25G/40G/100G 接続のみがサポートされます。 • Cisco UCS ファブリック インターコネクト 9108 100G の場合、1 Gbps の速度はポート 7 および 8 でのみ使用できます。 （注） 25GBPS の管理速度が選択されている場合、**[25GBPS 銅線ケーブル ネゴシエーションを有効にする（Enable 25GBPS Copper Cable Negotiation）]** は、3 メートルを超える銅ケーブルに対して自動的に有効になります。 25GBPS 銅線ケーブル ネゴシエーションを有効にします。 • アプライアンス、イーサネット アップリンク、FCoE アップリンク ポート ロールでのみサポートされます。 • ブレークアウト ポートをサポートしていません。 • ファームウェア バージョン 4.2(1a) 以降をサポートします。 • [自動（Auto）] に設定された FEC 構成のみをサポートします。
[VSAN ID]	VSAN 構成ポリシーで指定されている FC ポートの VSAN ID です。
FEC	ポートの前方誤り訂正設定: • 自動（Auto） • Cl91：25 GBPS および 100 GBPS の管理速度でサポート （注） サーバー ポート ロールに Cl91 が存在しません。 • Cl74：25GBPS の管理速度でサポート

優先度（Priority）	トラフィックをルーティングし、QoS を保証するポートのプライオリティを選択します。
モード（Mode）	ポート モードを選択します。ポート モードは、Trunk または Access です。
[接続されているデバイスの種類とデバイス番号（Connected Device Type and Device Number）]	各ポートまたは一連のポートのデバイス タイプとデバイス番号を選択します。 （注） このオプションは、サーバーの役割にのみ適用されます。 デフォルトでは、このオプションは無効になっています。 イネーブルにするには： • ポートを選択し、**[構成（Configure）]** をクリックします。 • **[手動シャーシ/サーバー番号付（Manual Chassis/Server Numbering）]**けボタンをオンにします。 各ポートの**[接続デバイス タイプ（Connected Device Type）]**と**[デバイス番号（Device Number）]**を指定できるテーブルが表示されます。 （注） **[自動入力番号付け（Auto-Fill Numbering）]**を有効にして、好みに応じて各ポートの**[接続デバイス タイプ（Connected Device Type）]**、**[開始デバイス番号（Starting Device Number）]**、および**[デバイスごとのポート（Ports per Device）]**を編集できます。 • [保存] をクリックして、[ポート ロール] リスト ビューに [接続されたデバイス タイプ] 列と [デバイス番号] 列を表示します。 （注） 選択した **[デバイス番号（Device Number）]** が他のポートの他のサーバー/シャーシにすでに割り当てられている場合、次に使用可能な番号が検出されたサーバーに割り当てられます。このアクションにより、ポート ポリシーの展開が失敗することはありません。 （注） ポート ポリシーの変更は FEX には適用されません。

イーサネット ネットワーク グループ	イーサネット アップリンクまたはアプライアンス ポートに接続するイーサネット ネットワーク グループ ポリシーを選択します。イーサネットネットワークグループポリシーは、許可されたVLANとネイティブ VLAN を指定します。 （注） イーサネット ネットワーク グループ ポリシーは、イーサネットアップリンクおよびアプライアンス ロールを持つポートにのみ適用されます。 （注） 分離 VLAN を構成するためのイーサネット ネットワーク グループを作成するには、グループが完全に分離していることを確認します。VLANの部分的なオーバーラップは許可されません。
イーサネットネットワーク制御	アプライアンスポートにアタッチするイーサネットネットワーク制御ポリシーを選択します。イーサネットネットワーク制御ポリシーでは、CDP の有効化または無効化、MAC 登録モードの指定、アップリンク障害時のアクション、MAC セキュリティの詳細および LLDP の詳細を指定できます。 （注） イーサネットネットワーク制御ポリシーは、アプライアンス ロールを持つポートにのみ適用されます。
[ポート（Port）]	有効なポート範囲を選択します。 • **ポート 1 ～96**：自動、10 GBPS、および 25 GBPS • **ポート 89～96**：自動、1 GBPS、10 GBPS、および 25 GBPS • **ポート 97～108**：自動、40 GBPS、および 100 GBPS
ポートチャネル **[ポートチャネルの作成（Create Port Channel）]** をクリックして、選択したポートのロールを選択します。 グラフィックイメージ内のポートをクリックするか、テーブル内の目的のポートの横にあるボックスをクリックして、設定するポートを選択します。	

[ロール（Role）]	ポートチャネルのロールタイプ。ロールタイプは次のいずれかになります。 • イーサネットアップリンクポートチャネル • FC アップリンクポートチャネル • FCoE アップリンクポートチャネル • アプライアンス ポートチャネル （注） • 許可されているポートの最大数： • イーサネットアップリンク ポートチャネル、FCoE アップリンク ポート チャネル、およびアプライアンス ポート チャネル（組み合わせ）は 12 • FC アップリンク ポート チャネルは 4 • ポートチャネルあたりのイーサネットポートは 16 • ポートチャネルごとのFCoEアップリンクポート：16 • どのポート チャネルに対しても、通常のポートとブレイクアウト ポートを組み合わせることはできません。たとえば、メンバーが 1/96 および 1/97/1 のアップリンク ポート チャネル ID 100 は許可されません。 • Cisco UCS 6536 ファブリック インターコネクトの速度が 100G のポートが N9K-C93180YC-FX3 に接続されている場合、ポート ロールを割り当てるときに**自動ネゴシエーション**を無効にする必要があります。 • FCアップリンク ポートチャネルの場合、ポート速度が異なるポート チャネルは許可されません。たとえば、FC アップリンク ポート チャネル ID 101、メンバー 1/33、ポート速度 8Gbps、および 1/34、ポート速度 16Gbps は許可されません。
PC ID	このスイッチに対してローカルなポートチャネルの固有識別子。

管理速度	アップリンク、アップリンクポートチャネル、および FCoE アップリンクポートチャネルの管理ポートチャネル速度オプションは次のとおりです。 • 1GBPS • 10GBPS • 25GBPS • 40GBPS • 100GBPS FC アップリンクおよび FC アップリンクポートチャネルの管理ポートチャネル速度オプションは次のとおりです。 • 8GBPS • 16GBPS • 32GBPS （注） ブレークアウト ポートの任意のロールには、管理速度を選択できません。
優先度（Priority）	トラフィックをルーティングし、QoS を保証するためのポートチャネルのプライオリティを選択します。
モード（Mode）	ポートチャネルモードを選択します。ポートチャネルモードは、Trunk または Access です。
イーサネット ネットワーク グループ	イーサネット アップリンクまたはアプライアンス ポート チャネルに接続するイーサネット ネットワーク グループ ポリシーを選択します。イーサネットネットワークグループポリシーは、許可された VLAN とネイティブ VLAN を指定します。 （注） イーサネット ネットワーク グループ ポリシーは、イーサネットアップリンクおよびアプライアンス ロールを持つポート チャネルに適用されます。 （注） 分離 VLAN を構成するためのイーサネット ネットワーク グループを作成するには、グループが完全に分離していることを確認します。VLAN の部分的なオーバーラップは許可されません。

イーサネットネットワーク制御	アプライアンスポートチャネルにアタッチするイーサネットネットワーク制御ポリシーを選択します。イーサネットネットワーク制御ポリシーでは、CDP の有効化または無効化、MAC 登録モードの指定、アップリンク障害時のアクション、MAC セキュリティの詳細および LLDP の詳細を指定できます。 （注） イーサネットネットワーク制御ポリシーは、アプライアンスロールを持つポートチャネルにのみ適用されます。
[ポート チャネル（Port Channel）]	選択有効ポート チャネルの範囲は 1 ～ 256 です。
ピン グループ ピン グループを使用して、サーバー上の vNIC/vHBA から、イーサネット/FC トラフィックをファブリック インターコネクトのアップリンク イーサネット/FC ポートにピン接続します。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。FI がスイッチング モード (イーサネットおよび FC) の場合、静的ピン接続はサポートされません。 サーバーにピン接続を構成するには、LAN/SAN 接続ポリシーに LAN/SAN ピン グループを含める必要があります。 **[ピン グループの作成（Create Pin Group）]** をクリックして、LAN および SAN データトラフィックを流すことができる FI のポート/ポート チャネルを指定します。	
ピングループタイプ	ピンされたポート/ポート チャネルにフローする必要があるデータトラフィックのタイプ。タイプは次のとおりです。 • LAN • SAN
ピングループ名	ピン グループの名前。この名前は、ピン グループが作成されると、LAN/SAN 接続ポリシーの作成ページに表示されます。
インターフェイスタイプ	ファブリック インターコネクトのインターフェイスのタイプ。 • Port • ポート チャネル
Port Selection	使用可能な表から、データ トラフィック フローにピンする必要があるポートとブレークアウト ポートを選択できます。 デフォルトでは有効。

9. [保存（Save）] をクリックします。

イーサネット ネットワーク グループ ポリシーの作成

イーサネット ネットワーク グループ ポリシーを使用すると、UCS サーバ上の VLAN の設定を管理できます。これらの設定には、許可される VLAN の定義、ネイティブ VLAN の指定、QinQ VLAN の指定が含まれます。

（注） イーサネット ネットワーク グループがポート ポリシーに割り当てられている場合、指定された VLAN セットは、他のアップリンク インターフェイスで指定された VLAN セットと同一であるか、または分離されている必要があります。VLAN が VLAN ポリシーで定義されていること、および **[アップリンクでの自動許可（Auto Allow on Uplinks）]** が無効になっていることを確認します。

このポリシーは、VIC QinQ トンネリングもサポートします。QinQ（802.1Qin802.1Q）トンネルにより、ネットワーク内の異なる VLAN を分離および分離できます。QinQ VLAN を設定するには、特定のポート、ポート チャネル、または vNIC の VLAN 設定の一部として、目的の VLAN ID を指定できます。これにより、単一の VLAN トランクを介した複数の VLAN の伝送が可能になります。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク グループ（Ethernet Network Group）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
VLAN 設定	

プロパティ（Property）	基本情報（Essential Information）
ネイティブ VLAN	このプロパティを使用すると、仮想インターフェイスのネイティブ VLAN ID または対応する vEthernet を 1 ～ 4093 の範囲で指定できます。 • ネイティブ VLAN が許可された VLAN にすでに含まれていない場合は、許可されたVLANのリストに自動的に追加されます。 • QinQ トンネリングが有効になっている場合、ネイティブ VLAN と許可 VLAN のプロパティが組み合わされます。
Q-in-Q トンネリングを有効にする	スライドして、VIC QinQ（802.1Qin802.1Q）トンネリングを有効にします。
[許可された VLAN（Allowed VLAN）]	仮想インターフェイスに許可される VLAN を参照します。カンマ区切りの VLAN ID と VLAN ID 範囲のリストを指定することで、許可された VLAN を指定できます。 たとえば、VLAN ID 10、20、30 ～ 40 を入力して VLAN 10、20、30 ～ 40 の範囲を許可できます。 （注） このプロパティは、*[QinQ トンネリングの有効化（Enable QinQ Tunneling）]* スライダが無効になっている場合にのみ表示されます。
QinQ VLAN	このプロパティにより、QinQ トンネリングの構成が有効になり、単一の VLAN 内の複数の VLAN のカプセル化が容易になります。サポートされる VLAN ID の範囲は 2 ～ 4093 で、ネットワークトラフィックを効果的に管理および分離できます。 （注） このプロパティは、*[QinQ トンネリングの有効化（Enable QinQ Tunneling）]* スライダが有効になっている場合にのみ使用できます。

（注） サーバーを隔離ホストまたはコミュニティ ホストにするには、許可VLANとネイティブVLANの両方で隔離 VLAN またはコミュニティ VLAN の ID を指定します。

7. **[作成（Create）]** をクリックします。

イーサネット ネットワーク制御ポリシーの作成

UCS ドメインのネットワーク制御設定を設定するイーサネットネットワーク制御ポリシー。このポリシーは、ポート ポリシーで定義されたアプライアンス ポート、および FI 接続された UCS サーバ上の LAN 接続ポリシーで定義された vNIC にのみ適用されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク コントロール（Ethernet Network Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[CDP の有効化（Enable DNS）]	インターフェイスの Cisco Discovery Protocol（CDP）を有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MAC 登録モード（MAC Register Mode）]	スイッチに登録する必要があるMACアドレスを決定します。次のように指定します。 • [ネイティブ VLAN のみ（Only Native VLAN）]：MACアドレスはネイティブVLAN のみに追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。 • [すべてのホスト VLAN（All Host VLANS）]：MAC アドレスは関連付けられたすべての VLAN に追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
[アップリンク障害時の動作（Action on Uplink Fail）]	スイッチがエンドホスト モードのとき、使用可能なアップリンク ポートがないと、インターフェイスがどのように動作するか決定します。 • [リンク ダウン（Link Down）]：スイッチ上でアップリンク接続が失われたときにvNICの動作状態をダウンに変更します。vNIC のファブリック フェールオーバーが有効になります。これがデフォルトのオプションです。 • [警告（Warning）]：使用可能なアップリンク ポートがない場合であっても、サーバ間の接続を維持します。スイッチ上でアップリンク接続が失われたときのファブリック フェールオーバーは無効になります。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MAC セキュリティ（MAC Security）] **[構築（Forge）]**	パケットがサーバからスイッチに送信される場合に、構築されたMACアドレスが許可されるか、または拒否されるかを決定します。次のように指定します。 • **[許可（Allow）]**：すべてのサーバ パケットは、そのパケットと関連付けられているMACアドレスとは無関係に、スイッチで受け入れられます。これがデフォルトのオプションです。 • **[拒否（Deny）]**：最初のパケットがファブリック インターコネクトに送信された後、それ以降のすべてのパケットは、それと同じMACアドレスを使用する必要があります。そうでなかった場合、スイッチによりメッセージなしで拒否されます。実質的に、このオプションによって、関連する vNIC のポート セキュリティが有効になります。
[LLDP]	インターフェイスが LLDP パケットを送受信できるかどうかを決定します。 • インターフェイス上での LLDP パケットの伝送を有効にするには、**[伝送を有効化（Enable Transmit）]** をクリックします。 • インターフェイス上での LLDP パケットの受信を有効にするには、**[受信を有効化（Enable Receive）]** をクリックします。

7. **[作成（Create）]** をクリックします。

VLAN ポリシーの作成

VLAN ポリシーによって特定の外部 LAN への接続が生成されます。VLAN は、ブロードキャスト トラフィックを含む、その外部 LAN へのトラフィックを切り離します。VLAN ポリシーを使用して、VLAN およびプライベート VLAN を作成できます。

（注） それぞれのVLANがマルチキャストポリシーに関連付けられていることを確かめてください。既存の VLAN を編集し、マルチキャスト ポリシーに関連付けることができます。マルチキャスト ポリシーをプライベート VLAN に関連付けることはできません。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[VLAN]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、**[VLAN の追加（Add VLAN）]** をクリックし、次のポリシーの詳細を設定します。

（注） イーサネット ネットワーク ポリシーごとに許可される VLAN の最大数は 3000 です。

[プロパティ（Property）]	[基本情報（Essential Information）]
VLANの追加	VLAN の追加をクリックして、VLAN とプライベート VLAN を追加します。
[名前/プレフィックス（Name/Prefix）]	単一の VLAN の場合、VLAN 名を指定します。VLAN の範囲の場合、各 VLAN 名に使用されるプレフィックスを指定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[VLAN ID]	VLAN ID 番号または 2 ～ 4093 の番号の範囲を入力します。ハイフンを使用してIDの範囲を入力することができ、複数のIDまたはID範囲をカンマで区切って入力できます。有効なVLAN IDまたはID範囲として、たとえば50、200、2000～2100を指定できます。3915～4042、4043～4047、4094、および4095のVLANは使用できません。該当するIDはシステム使用のために予約されているためです。 VLAN ID に割り当てる名前によって抽象化層が追加されることで、ネームド VLAN を使用するサービス プロファイルに関連付けされたすべてのサーバを一括してアップデートできるようになります。
[アップリンクでの自動許可（Auto Allow on Uplinks）]	このファブリックインターコネクトの全アップリンク ポートおよびポート チャネルでこの VLAN を許可するかどうかを決定するために使用されます。 **有効**：アップリンク ポートおよびポート チャネルでこの VLAN を許可します。 **無効**：非接続VLANの設定を無効にします。
マルチキャストポリシー	**[ポリシーの選択（Select Policy）]** をクリックし、VLAN に関連付ける必要があるマルチキャストポリシーを選択します。 すべての VLAN で使用可能な新しいマルチキャスト ポリシーを作成するには、**[新規作成（Create New）] を**クリックします。 （注） プライベート VLAN のマルチキャスト ポリシーは追加できません。
[VLAN 共有を有効にする（Enable VLAN Sharing）]	プライベート VLAN の作成を**[有効（Enable）]**にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[共有タイプ（Sharing Type）]	共有タイプは次のとおりです。 • [プライマリ（Primary）]：プライベート VLAN のプライマリ VLAN。セカンダリ VLAN はプライマリ VLAN にマッピングされます。 （注） 隔離 VLAN またはコミュニティ VLAN を作成する前に、プライマリ VLAN を作成する必要があります。 • [隔離（Primary）]：セカンダリ VLAN の 2 つの共有タイプの 1 つ。特定のプライマリ VLAN の下でマップできる隔離 VLAN は 1 つだけです。 • [コミュニティ（Community）]：セカンダリ VLAN の共有タイプの 1 つ。プライマリ VLAN には複数のコミュニティ VLAN をマップできます。
プライマリ VLAN ID	コミュニティまたは隔離 VLAN がマッピングされるプライマリ VLAN。 （注） セカンダリ VLAN がプライマリ VLAN にマッピングされている場合、プライマリ VLAN を変更または削除することはできません。

（注） ドメイン プロファイルの VLAN 構成が変更された場合、サーバー プロファイルの対応する変更は、サーバー プロファイルが再展開された後にのみ有効になります。

7. [追加（Add）] をクリックします。

VSAN ポリシーの作成

VSAN ポリシーを使用すると、同じ SAN ファブリックに物理的に接続されているデバイスを分離する Virtual SAN（VSAN）を作成できます。VSAN により、ファイバチャネル ファブリックのセキュリティと安定性が向上し、共通の物理インフラストラクチャ上に複数の論理 SAN を作成できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[VSAN]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次の手順を実行します。
   - **[トランキングモード（Trunking Mode）]** をクリックして、ファイバチャネルアップリンクトランキングを有効または無効にします。

     ファブリック インターコネクト上の名前付き VSAN でトランキングを有効ににした場合、そのファブリック インターコネクトのすべてのファイバ チャネル アップリンク ポートで、Cisco UCS ドメインのすべての名前付き VSAN が許可されます。ファブリック インターコネクトがファイバ チャネル エンドホスト モード用に設定されている場合、ファイバ チャネル アップリンクのトランキングを有効にすると、ID が 3840～4079 の範囲にあるすべての VSAN が動作不能になります。
   - **[VSAN の追加（Add VSAN）]** をクリックし、次のポリシーの詳細を設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[名前（Name）]	ユーザが VSAN コンフィギュレーションに付けた名前。

[プロパティ（Property）]	[基本情報（Essential Information）]
VSAN の範囲	VSAN の範囲です。VSAN がストレージおよびアップリンク VSAN、ストレージ VSAN、またはアップリンク VSAN のいずれであるかを示します。 VSAN の範囲は次のとおりです。 • ストレージとアップリンク • ストレージ • アップリンク （注） VSAN の FC ゾーン ポリシーを作成する場合、VSAN スコープはストレージである必要があります。
[VSAN ID]	スイッチ上の VSAN の一意の識別子。VSAN ID は 1 ～ 4093 の範囲で指定できます
[FCoE VLAN ID]	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。 VSAN 設定に関連付けられている FCOE VLAN の ID は、2 ～ 4093 である必要があります。3915ー4042、4043～4047、4094、4095のVLAN IDは、システム使用のために予約されています。 デフォルトでは、VLAN 4048 はスイッチの VSAN-1 にマッピングされます。VSAN ポリシーで FCoE に VLAN 4048 を使用しようとすると、エラーが発生します。この場合、VSAN ポリシーで別の FCOE VLAN ID を使用するように VSAN-1 を明示的に設定する必要があります。

7. **[作成（Create）]** をクリックします。

NTP ポリシの作成

NTP ポリシーは、Cisco Intersight によって管理される UCS システムが NTP サーバの時刻と同期するように設定するために、NTP サービスを有効にします。NTP サービスを有効化するには、NTP サーバとして動作する 1 ～ 4 台のサーバの IP/DNS アドレスを指定する必要がありま

す。NTP サービスを有効にすると、Cisco Intersight によりエンドポイント側で NTP の詳細が設定されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[NTP]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[Enable NTP]	NTP ポリシー設定をイネーブルにします。
NTP サーバ （NTP Servers）	NTP サーバの IP アドレスまたはホスト名のコレクション。
[タイム ゾーン（Time Zone）]	エンドポイントのタイムゾーンを選択できるタイムゾーンのコレクション。 このプロパティは、スイッチおよび Cisco IMC（スタンドアロン）サーバに適用されます。

NTP の設定にホスト名を使用する場合は、ネットワーク接続ポリシーで DNS サーバ情報を設定する必要があります。

7. **[作成（Create）]** をクリックします。

ネットワーク接続ポリシーの作成

ネットワーク接続ポリシーを使用すると、IPv4 アドレスと IPv6 アドレスを設定して割り当てることができます。

[ダイナミック DNS（Dynamic DNS）]

ダイナミック DNS（DDNS）は、 DNS サーバのリソース レコードを追加または更新するために使用されます。DDNS オプションを有効にすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、DNS サーバのリソース レコードを更新します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ネットワーク 接続（Network Connectivity）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のプロパティを設定します。

[共通プロパティ（Common Properties）]

[プロパティ（Property）]	[基本情報（Essential Information）]
[ダイナミック DNS の有効化]（Enable Dynamic DNS）	ダイナミック DNS を有効化します。 このプロパティは、ファブリック インターコネクトには適用されません。
[ダイナミック DNS 更新ドメイン（Dynamic DNS Update Domain）]	ダイナミック DNS ドメインを指定します。このドメインは、メイン ドメインまたはサブ ドメインのどちらにもできます。 このプロパティは、ファブリックインターコネクトには適用されません。

IPv4 のプロパティ

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP から IPv4 DNS サーバアドレスを取得	IPv4 アドレスが Dynamic Host Configuration Protocol（DHCP）から取得されるか、または特定の DNS サーバのセットから取得されるか。 • [有効（Enabled）]：Intersight は DHCP を使用します • [無効（Disabled）]：Intersight は IPv4 DNS サーバの設定済みセットを使用します。 このプロパティは、ファブリック インターコネクトには適用されません。
[優先 IPv4 DNS サーバ（Preferred IPv4 DNS Server）]	プライマリ DNS サーバの IP アドレス。このプロパティは、**[IPv4 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。
[代替 IPv4 DNS サーバ（Alternate IPv4 DNS Server）]	セカンダリ DNS サーバの IP アドレス。このプロパティは、**[IPv4 DNS サーバ アドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[IPv6 の有効化（Enable IPv6）]	IPv6 を有効にするかどうかを指定します。IPv6 プロパティは、このプロパティが有効になっている場合にのみ設定できます。

[IPv6 のプロパティ（IPv6 Properties）]

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP から IPv6 DNS サーバアドレスを取得	IPv6 アドレスが Dynamic Host Configuration Protocol（DHCP）から取得されるか、または特定の DNS サーバのセットから取得されるか。 • [有効（Enabled）]：Intersight は DHCP を使用します • [無効（Disabled）]：Intersight は IPv6 DNS サーバの設定済みセットを使用します。 このプロパティは、ファブリック インターコネクトには適用されません。
[優先 IPv6 DNS サーバ（Preferred IPv4 DNS Server）]	プライマリ DNS サーバの IP アドレス。このプロパティは、**[IPv6 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。
[代替 IPv6 DNS サーバ（Alternate IPv4 DNS Server）]	セカンダリ DNS サーバの IP アドレス。このプロパティは、**[IPv6 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。

7. **[作成（Create）]** をクリックします。

SNMP ポリシーの作成

SNMP ポリシーでは、管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。このポリシーは、SNMPv1、SNMPv2（v2c を含む）、SNMPv3 などの SNMP バージョンをサポートします。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。

SNMP ポリシーを使用すると、SNMP を有効または無効にしたり、アクセスおよびコミュニティ ストリングを指定したり、データの取得に使用する SNMP ユーザの詳細を指定したりできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。

3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SNTP]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP の有効化（Enable DNS）]	エンドポイントでの SNMP ポリシーの状態を表示します。エンドポイントから指定ホストに SNMP トラップを送信するには、このオプションを有効にします。
[アクセス コミュニティ ストリング（Access Community String）]	SNMPv1、SNMPv2 コミュニティストリング、またはSNMPv3ユーザ名を入力します。フィールドには 18 文字まで入力できます。
[トラップ コミュニティ ストリング（Trap Community String）]	他のデバイスに SNMP トラップを送信する際に使用する SNMP コミュニティ グループの名前を入力します。 （注） このフィールドは、SNMPv2c トラップホストまたは宛先にのみ適用されます。
[システム連絡先（System Contact）]	SNMP の実装担当者の連絡先。電子メールアドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。
[システムの場所（System Location）]	SNMP エージェント（サーバ）が動作するホストの場所。
[SNMP ユーザ（SNMP Users）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[名前（Name）]	SNMPv3ユーザ名を入力します。このフィールドは 1〜31 文字で指定する必要があります。
[セキュリティ レベル（Security Level）]	エージェントとマネージャーの間での通信で使用するセキュリティ メカニズムを選択します。 • AuthPriv • AuthNoPriv
[認証タイプ（Auth Type）]	ユーザの許可プロトコルとして **[SHA]** を選択します。 （注） MD5 認証プロトコルはサポートされていません。
[認証パスワード（Auth Password）]	ユーザの認証パスワードを入力します。
[認証パスワードの確認（Auth Password Confirmation）]	ユーザの認証パスワードを確認のため入力します。
[プライバシータイプ（Privacy Type）]	ユーザのプライバシープロトコルとして **[AES]** を選択します。 （注） **[DES]**プライバシータイプは、セキュリティ標準を満たすために廃止されました。
[プライバシー パスワード（Privacy Password）]	ユーザのプライバシー パスワードを入力します。
[プライバシーパスワードの確認（Privacy Password Confirmation）]	ユーザのプライバシー パスワードを確認のため入力します。
[SNMP トラップの宛先（SNMP Trap Destinations）]	
[有効化（Enable）]	SNMP ポリシーを使用するには、このオプションを有効にします。
[SNMP バージョン（SNMP Version）]	トラップの SNMP バージョンとして **[V2]** または **[V3]** を選択します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ユーザ（User）]	トラップの SNMP ユーザを選択します。最大 15 のトラップ ユーザを定義できます。 （注） このフィールドは SNMPv3 にのみ適用されます。
[トラップ タイプ（Trap Type）]	宛先にトラップが送信されたとき、どのタイプであれば通知を受信するかを選択します: • [トラップ（Trap）] • [情報（Inform）]
[宛先アドレス（Destination Address）]	SNMP トラップ情報の送信先アドレスを指定します。最大 10 のトラップ宛先を定義できます。
[ポート（Port）]	入力のサーバーがトラップの宛先と通信するために使用するポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 162 です。

7. [作成（Create）] をクリックします。

システム QoS ポリシーの作成

システム Quality of Service (QoS) ポリシーは、発信トラフィックにシステム クラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS が決定されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [システム QoS（System QoS）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
Platinum **Gold** **Silver** **Bronze**	このオプションを使用すると、ファブリックインターコネクトに関連付けられた QoS クラスを設定し、そのクラスをQoSポリシーに割り当てることができます。 （注） デフォルトでは、**Best Effort** または **Fibre Channel** システム クラスがイネーブルになっています。
CoS	0 ～ 6 の整数を入力して、サービス クラス（CoS）を設定します。0は最低プライオリティを表し、6は最高プライオリティを表します。QoS ポリシーを削除する際や、割り当てられたシステム クラスが無効な際に、システム クラスをトラフィックのデフォルト システム クラスにする必要がある場合を除き、この値を 0 に設定することは避けるよう推奨します。
重み付け	1 ～ 10 の整数。整数を入力すると、[重み付け（Weight）] フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が決定されます。
パケット ドロップを許可する	送信中にこのシステムクラスのパケットドロップを許可するように選択できます。 このフィールドは、[Best Effort] クラスの場合はつねににオンで、パケットのドロップが許可されます。[Fibre Channel] の場合はつねにオフで、パケットのドロップは許可されません。
[MTU]	チャネルの最大伝送単位（MTU）です。1500 ～ 9216 の範囲の整数を入力します。この値は最大パケット サイズに対応します。

7. **[作成（Create）]** をクリックします。

Syslog ポリシーの作成

Syslogポリシーでは、エンドポイントからのロギング レベルとして、記録する最小シビラティ（重大度）を定義します。ポリシーはまた、sisylog メッセージを保存するターゲットの場所と、リモート ロギング サーバのホスト名または IP アドレス、ポート情報、および通信プロトコルを定義します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[Syslog]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
ローカルロギング（Local Logging）	

[プロパティ（Property）]	[基本情報（Essential Information）]
[報告する最小シビラティ（重大度）（Minimum Severity to Report）]	リモート ログで報告する最低のシビラティ（重大度）レベルを選択します。シビラティ（重大度）は次のとおりです。 • 0 緊急 • 1 アラート • 2 重大 • 3 エラー • 4 警告 • 5 通知 • 6 情報 • 7 デバッグ
[リモートロギング：Syslog サーバ 1 および Syslog サーバ 2（Remote Logging - Syslog Server 1 and Syslog Server 2）]	
[有効化（Enable）]	Syslog ポリシーを有効または無効にするには、このオプションを選択します。
[ホスト名/IP アドレス（Hostname/IP Address）]	Cisco IMC ログを保存する Syslog サーバのホスト名または IP アドレスを入力します。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。 （注） リモート ロギング アドレスとして IPv4 と IPv6 の両方がある場合は、コマンドライン インターフェイス（CLI）を使用して、ファブリック インター コネクトでの IPv4 と IPv6 を設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[報告する最小シビラティ（重大度）（Minimum Severity to Report）]	リモート ログで報告する最低のシビラティ（重大度）レベルを選択します。シビラティ（重大度）は次のとおりです。 • 0 緊急 • 1 アラート • 2 重大 • 3 エラー • 4 警告 • 5 通知 • 6 情報 • 7 デバッグ

7. [作成（Create）] をクリックします。

スイッチ制御ポリシーの作成

スイッチ制御ポリシーは、VLAN 数の最適化、、MAC アドレスのエージング時間の設定、およびリンク制御のグローバル設定をサポートします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [スイッチ制御（Switch Control）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
スイッチング モード	
イーサネット	イーサネット切り替えモードを指定します。切り替えモードは、エンド ホストまたはスイッチのいずれかです。 エンドホスト モードでは、ファブリック インターコネクトは、複数のリンクを持つエンド ホストとしてアップストリーム デバイスに表示されます。このモードでは、スイッチはスパニング ツリー プロトコルを実行せず、一連のトラフィック転送ルールに従ってループを回避します。 スイッチ モードでは、スイッチはループを回避するためにスパニング ツリー プロトコルを実行し、ブロードキャストおよびマルチキャスト パケットは従来の方法で処理されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
FC	FC 切り替えモードを指定します。切り替えモードは、エンド ホストまたはスイッチのいずれかです。 エンドホストモードを使用すると、ファブリック インターコネクトは、vHBA を介して接続されているすべてのサーバー（ホスト）に代わって、接続されているファイバ チャネル ネットワークに対するエンドホストとして動作することができます。これは、vHBA をファイバ チャネル アップリンク ポートにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ファイバチャネルポートはファブリックの残りの部分に対してサーバー ポート（N ポート）となります。エンドホスト モードの場合、ファブリック インターコネクトは、アップリンク ポートがトラフィックを相互に転送するのを拒否することでループを回避します。 スイッチ モードは従来のファイバ チャネル スイッチング モードです。スイッチ モードを使用して、ファブリック インターコネクトをストレージ デバイスに直接接続することができます。ファイバ チャネル スイッチ モードの有効化は、SAN が存在しない（たとえば、ストレージに直接接続された 1 つの Cisco UCS システム）POD モデル、または SAN が存在する（アップストリーム MDS を使用）ポッド モデルで役に立ちます。
VLAN ポート数	

[プロパティ（Property）]	[基本情報（Essential Information）]
VLAN ポート数最適化の有効化	VLN ポート数の最適化を有効にします。このオプションは、デフォルトで無効です。 （注） • IMM の Cisco UCS 6400 シリーズおよび 6500 シリーズ FI で VLAN ポート数の最適化が有効になっている PV 数は 108000 です。 • VLAN ポート数の最適化は、Cisco UCS ファブリック インターコネクト 9108 100G では常に有効です。
システム予約済み VLAN	

[プロパティ（Property）]	[基本情報（Essential Information）]
予約済み VLAN 開始 ID	

[プロパティ（Property）]	[基本情報（Essential Information）]
	予約済みVLAN範囲の開始IDを指定するには、このオプションを選択します。デフォルトでは、開始 ID は 3915 です。開始 ID + 127 の VLAN ID は、VLAN または VSAN ポリシーの構成に使用できません。たとえば、VLAN 開始 ID が 3912 に変更される場合、予約済み VLAN 範囲は 3912-4039 です。予約済みVLAN範囲は、ユーザー定義のVLANまたはVSANポリシーには使用できません。 （注） 始める前に： • 新しい予約済みVLAN範囲内の既存のVLANをすべて削除します。 • VLAN または VSAN ポリシーで使用されている予約済み VLAN ブロックに、VLAN またはFCoE VLAN がないことを確認します。つまり、ファブリックインターコネクト A と B の両方の VLAN および VSAN ポリシーが、予約済みのVLAN範囲と競合しないようにします。 • 予約済み VLAN 開始 ID が変更された場合、新しい範囲に含まれていない古い範囲の VLAN は、新しいスイッチ制御ポリシーが展開された後にVLANおよびVSANポリシーに使用できます。 • デフォルトの予約済みVLAN範囲は 3916 ～ 4095 です。このシステム予約済みVLAN範囲は変更できますが、VLAN 1002 ～ 1005 は内部使用のためにブロックされており、システム予約済み範囲の一部として使用できないことに注意してください。 （注） • 変更を有効にするために、ファブリックインターコネクトが再起動します。複数の変更が加え

[プロパティ（Property）]	[基本情報（Essential Information）]
	られた場合でも、再起動は 1 回だけ発生します。 • デバイスの要求解除では、以前に構成された予約済み VLAN は削除されません。その後の要求では、ユーザーが新しい範囲を使用する場合は、スイッチコントロールポリシーを介して予約済み VLAN を構成する必要があります。
予約済み VLAN 終了 ID	予約済み VLAN 範囲の終了 ID。システムは、指定された VLAN 開始 ID から 128 の予約済み VLAN をブロックします。デフォルトでは、終了 ID は 4042 です。この ID は、VLANポリシーの構成には使用できません。
MAC アドレステーブルのエージングタイム	
Default	このオプションでは、エンド-ホストモードのデフォルトのMACアドレスエージング時間を 14,500 秒 に設定します。
Custom	ユーザがスイッチのMACアドレスエージングタイムを設定できるようにするには、このオプションを選択します。 スイッチモデルUCS-FI-6454以降のバージョンの場合、有効な時間範囲は 120ー918000 秒です。ユーザが時間範囲を定義すると、スイッチは定義された時間を 5 の倍数にリセットします。
なし	MACアドレスエージングプロセスを無効にするには、このオプションを選択します。このオプションは、MACエントリが期限切れにならず、MACアドレステーブルから破棄されないようにします。
エージングタイム (秒)	MACアドレスのエージングタイムを秒単位で定義します。このフィールドは、**[カスタム（Custom）]** オプションを選択した場合にのみ有効になります。
単一方向リンク検出（UDLD）グローバル設定	

[プロパティ（Property）]	[基本情報（Essential Information）]
メッセージの間隔	アドバタイズメント モードで、双方向に設定されているポートで、UDLDプローブ メッセージ間隔（秒）を定義します。 （注） 有効なメッセージ間隔の時間の範囲は 7ー90 秒です。
リカバリアクション	errdisable のポートを回復するには、**[Reset]** を選択します。 （注） デフォルトでは **[なし（None）]** オプションが選択されています。
ファブリック ポート チャネル **vHBA**	

[プロパティ（Property）]	[基本情報（Essential Information）]
ファブリック ポート チャネルの vHBA リセットの有効化	

[プロパティ（Property）]	[基本情報（Essential Information）]
	仮想ホスト バス アダプタ（vHBA）は、仮想マシンを論理的にファブリック インターコネクト上の仮想インターフェイスに接続し、仮想マシンがそのインターフェイスによってトラフィックを送受信できるようにします。これは現在、ファイバ チャネル モード (エンドホスト モード/スイッチ モード) を使用して実現されています。 ファブリック インターコネクトと I/O モジュール（IOM）間のメンバー リンクの追加または削除を伴うポート チャネル操作です。このような操作を行うと、I/O の一時停止が長くなったり、仮想マシンからそのターゲットへの接続が切断されたりする可能性があり、vHBA リセットのサポートが必要になります。 **ファブリック ポートチャネル vHBA リセット**が有効に設定されている場合、Cisco UCS IOM ポート チャネル メンバーシップが変更されると、ファブリック インターコネクトは、その Cisco UCS IOM を介して構成された各 vHBA に登録済み状態変更通知（Registered State Change Notification、RSCN）パケットを送信します。RSCN は、仮想インターフェイス カード (VIC) または VIC ドライバがファブリック ポートチャネル vHBA をリセットし、接続を復元できるようにします。 デフォルトでは、ファブリック ポートチャネルの vHBA リセットは無効に設定されています。 無効（デフォルト）の場合、vHBA のリセットは、ファブリック ポート チャネルのすべてのメンバーがダウンしている場合にのみ実行されます。 （注） • この機能は、Cisco Intersight インフラストラクチャ ファームウェア バージョン 4.1(3e) 以降でサポートされています。 • ESX NFNIC ドライバ バージョン 5.0.0.37 以降または 4.0.0.87 以

[プロパティ（Property）]	[基本情報（Essential Information）]
	降は、この RSCN を処理します。 • Linux FNIC ドライバ バージョン 2.0.0.85 以降は、この RSCN を処理します。

7. **[作成（Create）]** をクリックします。

.

（注）
- [ポリシーの詳細（Policy Details）] ページで、既存のすべてのスイッチ制御ポリシーのリンク制御グローバル設定フィールドの値が空白として表示されます。これらのポリシーは、ポリシーの編集/更新時に正しい値を表示します。
- ファブリック インターコネクトの切り替えモードを変更すると、ファブリック インターコネクトはリブートします。

フロー制御ポリシーの作成

ポートごとにプライオリティ フロー制御を構成して、システム QoS ポリシーおよびイーサネット QoS ポリシーによって定義された CoS の no-drop 動作を有効にします。自動およびオンの優先順位では、受信および送信リンク レベルのフロー制御はオフになります。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[フロー制御（Flow Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

プロパティ（**Property**）	基本情報（**Essential Information**）
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（**Property**）	基本情報（**Essential Information**）
プライオリティフロー制御モード	
Auto	Auto はプライオリティフローを送受信します。このフィールドは、デフォルトでイネーブルにされています。
オン（On）	ローカルポートでプライオリティ制御フローをイネーブルにします。 （注） **送信方向**と**受信方向**を同時に有効にすることはできません。

プロパティ（Property）	基本情報（Essential Information）
[オフ（Off）]	ローカル ポートでプライオリティ制御フローを有効にします。 （注） **[送信方向（Send）]** と **[受信方向（Receive）]** を同時に有効にすることができます。
	送信 有効にすると、リンク レベル フロー制御は送信方向に構成されます。
	[受信（Receive）] 有効にすると、リンク レベル フロー制御は受信方向に構成されます。

（注） 優先順位フロー制御が**自動、オン**モードの場合、フロー制御を有効にすることはできず、オプションはリストされません。フロー制御を有効にするには、優先フロー制御を**オフ**モードに設定する必要があります。

（注） フロー制御は、フロー制御対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされています。

- イーサネット アップリンク ポートおよびポート チャネル

7. **[作成（Create）]** をクリックします。

リンク集約ポリシーの作成

このポリシーは、リンク集約プロパティの設定に使用できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[リンク アグリゲーション（Link Aggregation）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[個別に一時停止）Suspend Individual）]	
[いいえ（False）]	**[いいえ（False）]** を選択して、ピアポートからの PDU の受信を続行します。
[はい（True）]	ピアポートから PDU を受信していないポートを一時停止するには、**[はい（True）]** を選択します。
[ACP レート（LACP Rate）]	
[標準（Normal）]	ポートは 30 秒ごとに 1 PDU を受信します。このタイムアウトは 90 秒です。
[高速（Fast）]	ポートはピア ポートから 1 秒ごとに 1 PDU を受信します。このタイムアウトは 3 秒です。

（注） リンク集約は、リンク集約対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされています。

- イーサネット アップリンク ポート チャネル
- FCoE アップリンク ポート チャネル

7. **[作成（Create）]** をクリックします。

リンク集約ポリシーの作成

このポリシーは、ポートのリンク制御管理状態と構成（通常またはアグレッシブ）モードの構成を有効にします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[リンク制御（Link Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[リンク制御の管理状態（Link Control Administrative State）] 管理者が設定および管理を行うポートのリンク制御状態。	
[リンク制御モード（Link Control Mode）]	

プロパティ（Property）	基本情報（Essential Information）
[標準（Normal）]	光ファイバ接続上のインターフェイスの誤った接続による単方向リンクを検出します。
[アグレッシブ（Aggressive）]	光ファイバ リンク上のインターフェイスの誤った接続による単方向リンクに加え、光ファイバ リンクおよびツイストペア リンク上の一方向トラフィックによる単方向リンクも検出します。 • **[UDLD 管理状態（Administrative State）]** が無効の場合、ポリシーを **[アグレッシブ（Aggressive）]** モードに設定できません。 • **[UDLD モード（UDLD Mode）]**（（[通常（normal）] または [アグレッシブ（aggressive）]）を構成する場合、必ず単方向リンクの両側に同じモードを構成してください。

（注） リンク制御ポリシーは、リンク制御対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされています。

- イーサネット アップリンク ポート
- FCoE アップリンク ポート
- イーサネット アップリンク ポート チャネル
- FCoE アップリンク ポート チャネル

7. **[作成（Create）]** をクリックします。

マルチキャスト ポリシーの作成

マルチキャストポリシーは、Internet Group Management Protocol（IGMP）のスヌーピングおよび IGMP クエリアの設定に使用されます。

（注） それぞれの VLAN がマルチキャスト ポリシーに関連付けられていることを確かめてください。既存の VLAN を編集し、マルチキャスト ポリシーに関連付けることができます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[マルチキャスト（Multicast）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

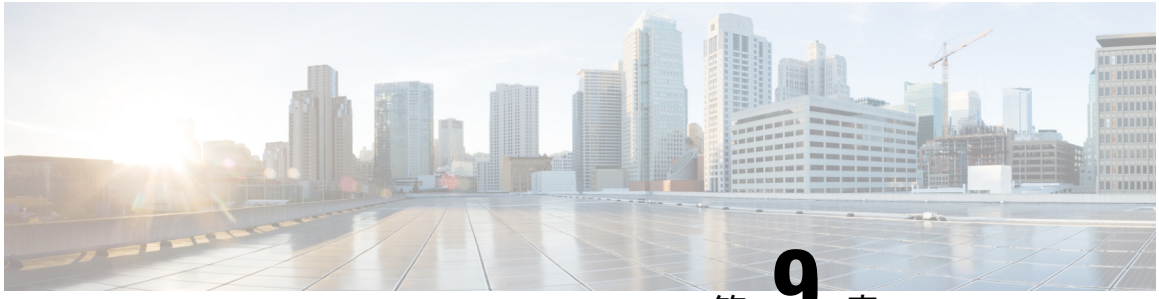
[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[スヌーピングの状態（Snooping State）]	IGMP スヌーピングが、どのインターフェイスがホスト、またはマルチキャスト トラフィックの受信で重要な他のデバイスに接続されているかを検出するため、VLAN 内の IGMP プロトコル メッセージを調べるかどうかを決定します。次のいずれかになります。 • **[有効（Enabled）]**：IGMP スヌーピングは、このポリシーに関連付けられた VLAN に使用されます。 • **[無効（Disabled）]**：IGMP スヌーピングは、関連付けられた VLAN に使用されません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[クエリアの状態（Querier State）]	IGMP スヌーピング クエリアが、IP マルチキャスト トラフィックを受信する必要のあるホストからの IGMP レポート メッセージをトリガーするために、IGMP クエリーを定期的に送信するかどうかを決定します。次のいずれかになります。 • [有効（Enabled）]：IGMP クエリーは定期的に送信されます。 • [無効（Disabled）]：IGMP クエリーは送信されません。これがデフォルトのオプションです。
クエリアの IP アドレス	IGMP スヌーピング クエリア インターフェイスの IPv4 アドレス。 このフィールドは、[クエリアの状態（Querier State）] が有効な場合にのみ表示されます。
[クエリアの IP アドレスのピア（Querier IP Address Peer）]	（オプション）ピア IGMP スヌーピング クエリア インターフェイスの IPv4 アドレス。このピア IP アドレスは FI-B に割り当てられます。 このフィールドは、[クエリアの状態（Querier State）] が有効な場合にのみ表示されます。

7. [作成（Create）] をクリックします。



第 9 章

サーバ ポリシーの設定

- サーバ ポリシー （140 ページ）
- ポリシーの作成 （149 ページ）
- サポートされている UCS サーバ ポリシー （149 ページ）
- 証明書管理ポリシーの作成 （155 ページ）
- アダプタ設定ポリシーの作成 （157 ページ）
- LAN 接続ポリシーの作成 （162 ページ）
- イーサネット アダプタ ポリシーの作成 （173 ページ）
- イーサネット QoS ポリシーの作成 （183 ページ）
- イーサネット ネットワーク ポリシーの作成 （185 ページ）
- イーサネット ネットワーク グループ ポリシーの作成 （190 ページ）
- イーサネット ネットワーク制御ポリシーの作成 （193 ページ）
- SAN 接続ポリシーの作成 （195 ページ）
- ファイバ チャネル アダプタ ポリシーの作成 （204 ページ）
- ファイバ チャネル ネットワーク ポリシーの作成 （208 ページ）
- ファイバチャネル QoS ポリシーの作成 （209 ページ）
- FC ゾーンポリシーの作成 （211 ページ）
- ファームウェア ポリシーの作成 （212 ページ）
- BIOS ポリシーの作成 （213 ページ）
- ブート順序ポリシーの作成 （232 ページ）
- iSCSI ブート ポリシーの設定 （247 ページ）
- iSCSI アダプタ ポリシーの作成 （252 ページ）
- iSCSI スタティック ターゲット ポリシーの作成 （253 ページ）
- デバイス コネクタ ポリシーの作成 （254 ページ）
- ドライブ セキュリティ ポリシーの作成 （255 ページ）
- ディスク グループ ポリシーの作成 （256 ページ）
- IMC アクセス ポリシーの作成 （260 ページ）
- IPMI Over LAN ポリシーの作成 （263 ページ）
- LDAP ポリシーの作成 （265 ページ）
- ローカル ユーザ ポリシーの作成 （271 ページ）

• NTP ポリシの作成 （275 ページ）
• SD カード ポリシーの作成 （276 ページ）
• Serial over LAN ポリシーの作成 （278 ページ）
• SSH ポリシーの作成 （280 ページ）
• 仮想 KVM ポリシーの作成 （281 ページ）
• 仮想メディア ポリシーの作成 （283 ページ）
• ネットワーク接続ポリシーの作成 （288 ページ）
• SMTP ポリシーの作成 （290 ページ）
• SNMP ポリシーの作成 （292 ページ）
• ストレージ ポリシーの作成 （295 ページ）
• Syslog ポリシーの作成 （311 ページ）
• サーバの電源ポリシーの作成 （313 ページ）

サーバ ポリシー

Cisco Intersight のポリシーでは、BIOS の設定、ファームウェア バージョン、ディスクグループの作成、Simple Mail Transfer Protocol（SMTP）、インテリジェント プラットフォーム管理インターフェイス（IPMI）の設定などを含む、UCS サーバの異なる構成が提供されます。一度設定したポリシーは、任意の数のサーバに割り当てることで、構成基準を提供できます。Cisco Intersight のポリシーはアプリケーションにネイティブなので、UCS システムからは直接インポートされません。サーバ プロファイルを使用したポリシーベースの構成は、Cisco Intersight Essentials の機能です。

Cisco Intersight のサーバポリシー作成ウィザードには、次の 2 つのページがあります。

- **[全般（General）]**：組織を選択し、ポリシーの名前を入力できます。オプションで、ポリシーの識別に役立つ短い説明とタグ情報を含められます。タグは key：value 形式である必要があります。たとえば、Org: IT または Site: APJ などです。
- **[ポリシーの詳細（Policy Details）]**：ポリシーの詳細ページには、スタンドアロン UCS サーバ、FI に接続された UCS サーバ、またはその両方に適用されるプロパティがあります。**[すべてのプラットフォーム（All Platforms）]** オプション、**[UCS サーバ（スタンドアロン）（UCS Servers (Standalone)）]** オプション、**UCS Servers (FI-Attached)[UCS サーバ（FI 接続）（UCS Servers (FI-Attached)）]** オプションをクリックすると、各プロパティを個別に表示できます。

サーバポリシーは、Cisco IMC から Cisco C シリーズスタンドアロンサーバの設定の詳細（サーバプロファイルとポリシー）をインポートする一環としてインポートできます。詳細については、「サーバー プロファイルのインポート」を参照してください。

Cisco Intersight で構成できるサーバ ポリシーの説明を次のリストに示します。

- **[アダプタ構成ポリシー（Adapter Configuration Policy）]**：VIC アダプタのイーサネット設定とファイバ チャネル設定を構成します。

- **[BIOS ポリシー（BIOS Policy）]**：管理対象デバイスの BIOS 設定の構成を自動化します。BIOS 設定の分類方法を含む BIOS ポリシーを 1 つ以上作成できます。サーバの BIOS ポリシーを指定しない場合、BIOS の設定は変更されません。BIOS ポリシーを指定すると、サーバの以前設定されていた値（ベア メタル サーバの構成設定を含む）がポリシーで指定された値で置き換えられます。BIOS ポリシー設定を適用するには、サーバをリブートする必要があります。
- **[ブート順序ポリシー（Boot Order Policy）]**：デバイスの線形順序を設定し、ブート順序とブート モードの変更を可能にします。さまざまなデバイス タイプに複数のデバイスを追加し、ブート順序を変更し、各ブート デバイス タイプのパラメータを設定することもできます。

  インベントリビューでは、サーバに設定されている実際のブート順序を表示できます。ブート順序には、デバイス名、デバイスタイプ、ブートモード（レガシーまたはUEFI）、セキュアブートモード（有効または無効）などの設定の詳細が含まれます。

（注） ブート順序ポリシーのサーバプロファイルで設定されたデバイスは、サーバのブート時にサーバ BIOS がデバイスを検出しない場合、実際のブート順序に表示されないことがあります。

Intersight は、ワンタイムブート (OTB) オプションを実行して、ブート順序ポリシーと既存のブート順序を一時的にオーバーライドするブートデバイスの設定機能を提供します。。ワンタイムブートデバイスを設定するには、[Servers Table] ビューまたは [Server Details] ページから [Power Cycle] または [Power On] を選択し、[Set One Time Boot Device] オプションをオンにします。この操作は、電源の再投入または電源投入アクションの一部として、ワンタイムブートデバイスからの起動を試みます。電源の再投入または電源投入後、OTB 設定はクリアされ、デフォルトのブート順序に従うように次のリブートが有効になります。

（注）
- OTB オプションは、サーバプロファイルに関連付けられたブート順序ポリシーで設定されたサーバで使用できます。OTB を正常に設定するには、Intersight で事前にブート順序ポリシーを使用してサーバプロファイルを展開する必要があります。
- アウトオブバンドブート順序の変更は、OTB デバイス設定の Intersight UI には反映されません。

PXE ブート設定の場合、サーバのブートポリシーで特定の PXE デバイスの MAC アドレスまたはスロットとポートの両方が存在しない場合、サーバポリシーをインポートしても PXE デバイスは作成されません。ただし、スロットとポートの両方が存在する場合、サーバ上の特定のスロットのブート可能インターフェイスブート順序は**ANY** に設定されます。

非 VIC アダプタの場合は、MAC アドレス、スロットとポートの両方、またはスロットのみを使用して PXE ブートを設定できます。

レガシーモードの SAN ブートデバイス設定の場合は、ブートターゲット論理ユニット番号（LUN）、デバイススロット ID、インターフェイス名、およびターゲット WWPN を指定します。Unified Extensible Firmware Interface（UEFI）モードの SAN ブートデバイス設定の場合は、レガシーモードでリストされているフィールドに加えて、ブートローダ名、説明、およびパスを入力します。

iSCSI ブートの場合は、ターゲットインターフェイスの詳細、認証メカニズム、およびイニシエータ IP ソースを提供します。

- **Non-Volatile Memory Express（NVMe）** ブートの場合は、NVMe ドライブを UEFI モードでブート可能として構成します。サーバー プロファイルの展開中には、この NVMe 構成設定により、定義された順序で BIOS を選択できます。

- **証明書管理ポリシー（Certificate Management Policy）**：外部証明書の証明書の詳細を指定し、ポリシーをサーバーにアタッチできます。Cisco Intersight は現在、次の証明書をサポートしています。
  - ルート CA 証明書
  - IMC 証明書

- **ディスク グループ ポリシー（Disk Group Policy）**：ディスク グループ ポリシーがストレージ ポリシーの一部になりました。

- **[デバイス コネクタ ポリシー（Device Connector Policy）]**：**[Intersight のみから構成（Configuration from Intersight only）]** オプションを選択することができ、Cisco IMC に許可される構成変更を制御できます。[Intersight のみから設定（Configuration from Intersight only）] オプションは、デフォルトで有効になっています。Intersight でデバイス コネクタ ポリシーを展開すると、次の変更を確認できるようになります。
  - 次の場合は検証タスクが失敗します。
    - Intersight の [読み取り専用（Read-only）] モードが要求済みデバイスで有効になっている場合。
    - Cisco UCS のスタンドアロン C シリーズ サーバーのファームウェアが 4.0(1) よりも前のバージョンの場合。
  - Intersight の読み取り専用モードが有効になっている場合は、Intersight から実行された場合にのみファームウェアのアップグレードが成功します。Cisco IMC からローカルで実行されたファームウェア アップグレードは失敗します。
  - IPMI over LAN の権限は、[読み取り専用（read-only）] レベルにリセットされることがあります。[Intersight のみから構成（Configuration from Intersight only）] がデバイス接続ポリシーを介して有効にされたか、または Cisco IMC のデバイス コネクタで同じ構成が有効になっている場合です。

注目 デバイス コネクタ ポリシーはサーバ プロファイルのインポートの一部としてインポートされません。

- **[イーサネット アダプタ ポリシー（Ethernet Adapter Policy）]**：アダプタのトラフィック処理方法など、アダプタのホスト側の動作を制御します。VIC仮想イーサネットインターフェイスごとに、VXLAN、NVGRE、ARFS、Interrupt 設定、および TCP Offload 設定などのさまざまな機能を設定できます。

  このポリシーには、サポートされるサーバオペレーティングシステムの推奨されるデフォルト設定が含まれます。ポリシーは 16 のデフォルト設定をサポートします。ポリシーの作成時に、デフォルト設定を選択してインポートできます。

（注） デフォルト設定を変更することはできません。ただし、デフォルト設定をインポートしたポリシーは変更できます。

- **[イーサネット ネットワーク ポリシー（Ethernet Network Policy）]**：ポートが単一の VLAN（アクセス）または複数の VLAN（トランク）トラフィックを伝送できるようにすることの決定を許可します。vNIC のデフォルト VLAN および QinQ VLAN を構成できます。タグが見つからない場合には、イーサネットパケットに関連付けられた VLAN を指定できます。
- **[イーサネット ネットワーク制御ポリシー（Ethernet Network Control Policy）]**：アプライアンス ポート、アプライアンス ポート チャネル、または vNIC のネットワーク制御設定を行います。
- **[イーサネットネットワークグループポリシー（Ethernet Network Group Policy）**：アプライアンス ポート、アプライアンス ポート チャネル、または vNIC の許可 VLAN およびネイティブ VLAN を構成します。
- **[イーサネット QoS ポリシー（Ethernet QoS Policy）]**：vNIC の発信トラフィックにシステム クラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS が決定されます。一部のアダプタでは、発信トラフィックでバーストやレートなどの付加的な制御を指定することもできます。
- **[ファイバ チャネル アダプタ ポリシー（Fibre Channel Adapter Policy）]**：アダプタのトラフィック処理方法など、ホスト側のアダプタの動作を制御します。FCPエラーの修復の有効化、キューのデフォルト設定の変更、パフォーマンス強化のための割り込み処理を実行できます。

  このポリシーには、サポートされるサーバオペレーティングシステムの推奨されるデフォルト設定が含まれます。ポリシーは9つのデフォルト設定をサポートします。ポリシーの作成時に、デフォルト設定を選択してインポートできます。

（注） デフォルト設定を変更することはできません。ただし、デフォルト設定をインポートしたポリシーは変更できます。

- **[ファイバ チャネル ネットワーク ポリシー（Fibre Channel Network Policy）]**：仮想インターフェイスの VSAN 構成を制御します。
- **[ファイバ チャネル QoS ポリシー（Fibre Channel QoS Policy）]**：vHBA の発信トラフィックにシステム クラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS が決定されます。一部のアダプタでは、発信トラフィックでバーストやレートなどの付加的な制御を指定することもできます。
- **[IPMI over LAN ポリシー（IPMI over LAN Policy）]**：サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイス用のプロトコルを定義します。Intelligent Platform Management Interface（IPMI）を使用すると、オペレーティング システムはシステムの正常性と制御システムのハードウェアに関する情報を取得し、適切なアクションを実行するよう Cisco IMC に指示します。IPMI メッセージを管理するための IPMI Over LAN ポリシーは、Cisco Intersight で作成できます。セッションごとに、次のユーザ ロールを IPMI ユーザに割り当てることができます。
  - [管理者（admin）]：IPMI ユーザは使用可能なすべてのアクションを実行できます。このオプションを選択した場合、管理者（Administrator）ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
  - [読み取り専用（read-only）]：情報は確認できますが、変更を加えることはできません。「管理者（Administrator）」、「運用者（Operator）」、または「ユーザ（User）」ロールの IPMI ユーザは、それ以外に所有している IPMI 権限とは関係なく、読み取り専用の IPMI セッションのみ作成できます。
  - [ユーザ（user）]：IPMI ユーザは一部の機能を実行できますが、管理タスクは実行できません。このオプションを選択した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。

重要 IPMI通信に使用する暗号キー。偶数桁の 16 進数を含めます。40 文字を超えないようにする必要があります。「00」を使用して、暗号化キーの使用を無効にすることができます。指定された暗号化キーが 40 文字未満の場合、IPMI コマンドは暗号化キーにゼロを追加して、40 文字の長さにする必要があります。

- **[LAN 接続ポリシー（LAN Connectivity Policy）]**：ネットワーク上のサーバと LAN 間の接続とネットワーク通信を決定します。LAN 接続ポリシーの一部として、イーサネット アダプタ、イーサネット QoS、およびイーサネット ネットワーク ポリシーを作成する必要があります。IMM サーバの場合、MAC ポリシーまたは静的 MAC アドレスを使用して MAC アドレスをサーバに割り当て、サーバがネットワークとの通信に使用する vNIC を識

別します。ネットワーク ポリシーの作成に関する詳細については、「ネットワーク ポリシーの作成」を参照してください。

- **[LDAP ポリシー（LDAP Policy）]**：LDAP 構成の設定とエンドポイントの設定を指定します。エンドポイントでは、ネットワーク内のディレクトリ情報の保存と維持のためにLDAPがサポートされています。LDAP ポリシーは、LDAP サーバの構成設定、DNS パラメータ（DNS SRV 要求に使用されるドメイン名を取得するオプションを含む）、バインド方式、検索パラメータ、およびグループ認証設定を決定します。LDAP ポリシーにより、複数の LDAP グループを作成して LDAP サーバ データベースに追加することもできます。

- **[ローカル ユーザ ポリシー（Local User Policy）]**：ローカル ユーザ設定の構成を自動化します。設定する必要があるローカル ユーザのリストを含む、1 つ以上のローカル ユーザ ポリシーを作成できます。

- **[永続メモリ モジュール（Persistent Memory Policy）]** は、メモリの低遅延とストレージの永続化を実現する不揮発性メモリ モジュールです。PMem モジュールは、モードに基づいて、データへのアクセスを高速化し、電源の再投入後もデータを保持します。Intersight では、USC M5 サーバでの Intel® Optane™ データセンター永続メモリモジュールのサポートが導入されました。このサーバは、第 2 世代 Intel® Xeon® スケーラブル プロセッサに基づいています。Intel® Optane™ PMem モジュールは、第二世代の Intel® Xeon® スケーラブル プロセッサとのみ、組み合わせて使用できます。永続メモリポリシーでは、永続メモリモジュールのセキュリティ、目標、、および名前空間を設定することができます。

  - [セキュリティ（Security）]：すべての永続メモリモジュールのセキュアパスフレーズを設定するために使用されます。

  - 目標：サーバのすべてのソケットに接続されているすべての PMem モジュールの揮発性メモリとリージョンを設定するために使用されます。Intersight は、永続メモリポリシーの一部としての目標の作成と変更のみをサポートします。永続メモリポリシーの作成または変更中に目標が変更されると、一部のデータが失われます。データ損失の詳細については、参考資料の「永続メモリポリシーの設定と展開中のデータ損失」の表を参照してください。

  - 名前空間：ソケット上の特定のソケットまたは PMem モジュールにマッピングされた領域を分割するために使用されます。Intersight は、永続メモリポリシーの一部として名前空間の作成と削除のみをサポートします。名前空間の変更はサポートされていません。永続メモリポリシーの作成中にネームスペースが作成または削除されると、一部のデータが失われます。データ損失の詳細については、参考資料の「永続メモリポリシーの設定と展開中のデータ損失」の表を参照してください。

    永続メモリモジュールの取り付けまたは交換、およびポリシーの展開を行う前に、永続メモリモジュールのメモリパフォーマンスのガイドラインと装着ルールを考慮することが重要です。PMem モジュールの装着に関するガイドラインは、CPU ソケットの数に基づいて次のように分類できます。

    - デュアル CPU：UCS C220 M6、C240 M6、および B200 M6 サーバ
    - デュアル CPU：UCS C220 M5、C240 M5、および B200 M5 サーバ
    - クアッド CPU：UCS C480 M5 および B480 M5 サーバ

- デュアル CPU： UCS S3260 M5 サーバ

永続メモリポリシーの作成、ポリシーの例外、およびポリシーに関するその他の注意事項の詳細については、参考資料の「リソースの永続メモリポリシー」を参照してください。

- **[SAN 接続ポリシー（SAN Connectivity Policy）]**：ネットワーク ストレージ リソースと、ネットワーク上のサーバと SAN 間の接続を決定します。このポリシーを使用して、サーバがストレージエリアネットワークとの通信に使用するvHBAを設定できます。WWNNおよび WWPN アドレスプール、または静的 WWNN および WWPN アドレスを使用して、vHBA を追加して設定できます。ファイバ チャネル アダプタ、ファイバ チャネル QoS、およびファイバ チャネル ネットワークのポリシーは、SAN 接続ポリシーの一部として作成する必要があります。ネットワーク ポリシーの作成に関する詳細については、「ネットワーク ポリシーの作成」を参照してください。

- **[SD カード ポリシー（SD Card Policy）]**：Cisco UCS C シリーズのスタンドアロン M4 サーバと M5 サーバに Cisco FlexFlash カードと FlexUtil Secure Digital（SD）カードを構成します。 このポリシーは、SD カードの仮想ドライブの詳細を指定します。SD カードは、オペレーティングシステムのみ、ユーティリティのみ、またはオペレーティングシステム+ユーティリティのモードで設定できます。

  Cisco FlexFlash コントローラに 2 つのカードがあり、SD カードポリシーでオペレーティングシステムが選択されている場合、設定された OS パーティションがミラーリングされます。Cisco FlexFlash コントローラで使用できるカードが 1 つだけの場合、設定されている OS パーティションは非 RAID です。ユーティリティパーティションは常に非 RAID として設定されます。

  .

（注）

1. このポリシーは、現在 Cisco UCS M6 サーバではサポートされていません。
2. Cisco UCS M5 サーバでは最大 2 つのユーティリティ仮想ドライブを有効化でき、Cisco UCS M4 サーバでは任意の数のサポートされているユーティリティ仮想ドライブを有効化できます。
3. 診断は Cisco UCS M5 サーバでのみサポートされています。
4. Cisco UCS M4 サーバでのみ User Partition ドライブの名前を変更できます。
5. FlexFlash 構成は、C460 M4 サーバではサポートされていません。
6. オペレーティング システムとユーティリティ モードでは、Cisco UCS M4 サーバには FlexFlash カード 2 枚、Cisco UCS M5 サーバには少なくとも FlexFlash カード 1 枚と FlexUtil カード 1 枚が必要です。

- **[SMTP ポリシー（SMTP Policy）]**：管理対象デバイスで SMTP クライアントの状態を設定します。発信通信の優先設定を指定し、報告する障害のシビラティ（重大度）とその報告を受け取る受信者を選択できます。
- **[SOL ポリシー（SOL Policy）]**：管理対象システムのシリアル ポートの入出力を IP 経由でリダイレクトできるようにします。サーバ/サーバ群のニーズを条件に特定の Serial over LAN 属性を分類する Serial over LAN ポリシーを 1 つ以上作成できます。
- **[SSH ポリシー（SSH Policy）]**：SSH クライアントを有効にし、暗号化されたセキュアな接続を確立します。サーバ/サーバ群の SSH プロパティの分類方法を含む SSH ポリシーを 1 つ以上作成できます。
- **[Simple Network Management Protocol（SNMP）ポリシー（Simple Network Management Protocol (SNMP) Policy）]**：管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP を設定します。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、サーバ上の既存のユーザやトラップは削除されますが、置き換えられません。
- **[ストレージポリシー（Storage Policy）]**：ストレージポリシーでは、ドライブグループ、仮想ドライブの作成、仮想ドライブのストレージ容量の設定、および M.2 RAID コントローラの設定を行うことができます。
- **[Syslog ポリシー（Syslog Policy）]**：エンドポイントから収集したログ ファイルをレポートするログ レベル（最低限のシビラティ（重大度））、Syslog メッセージを保存する宛

先、ホスト名/IP アドレス、ポート情報、リモート ロギングサーバ用の通信プロトコルを定義します。

- **[仮想メディアポリシー（Virtual Media Policy）]**：KVM コンソールと仮想メディアを使用してサーバにオペレーティングシステムをインストールし、リモートファイル共有からホストにファイルをマウントして、仮想メディア暗号化を有効化できます。別の OS イメージの仮想メディアマッピング、を含む 1 つ以上の仮想メディアポリシーを作成し、最大 2 つの仮想メディアマッピングを設定できます。1 つは ISO ファイル (CDD 経由)、もう 1 つは IMG ファイル (HDD 経由) です。

  仮想メディアのボリュームのさまざまなマウント オプションに関する詳細については、「仮想メディアのマウント オプション」を参照してください。
- **[仮想 KVM ポリシー（Virtual KVM Policy）]**：特定の仮想 KVM プロパティをグループ—化することができます。このポリシーにより、許可される同時 KVM セッション、ポート情報、およびビデオ暗号化オプションを指定できます。
- **[IMC アクセス ポリシー（IMC Access Policy）]**：IP プールとシャーシプロファイルのマッピングを介して、ネットワーク設定および管理できます。このポリシーを使用すると、VLAN を設定し、IP プールアドレスを介して IP アドレスと関連付けることができます。

  インバンド IP アドレス、アウトオブバンド IP アドレス、またはインバンド IP アドレスとアウトオブバンド IP アドレスの両方は、IMC アクセス ポリシーを使用して設定でき、次でサポートされます。

  - ドライブ セキュリティ、SNMP、Syslog、および vMedia ポリシー
  - vKVM クライアントを使用した vKVM、IPMI、SOL、および vMedia ポリシー

- **[電源ポリシー（Power Policy）]**：FI 接続サーバおよびシャーシの電源管理を有効にします。このポリシーを使用すると、サーバーの電力優先度であるシステムの電力プロファイリングと、電力復元状態を設定できます。詳細については、サーバーの電源ポリシーの作成を参照してください。
- **[NTP ポリシー（NTP Policy）]**：Intersight 管理型 Cisco IMC（スタンドアロン）サーバで NTP サービスを有効にできます。NTP サービスで NTP サーバを使用して時刻を同期します。NTP サービスを有効にし、4 つの NTP サーバのうち最低 1 つの IP アドレスまたは DNS を指定することにより、NTP サービスを設定する必要があります。

  NTP ポリシーでは、Cisco IMC（スタンドアロン）サーバでタイムゾーンを設定することもできます。NTP サービスを有効にし、タイムゾーンを選択すると、Cisco Intersight は NTP の詳細と、エンドポイントのタイムゾーンを設定します。
- **FC ゾーン ポリシー**：ホストとストレージデバイスの間のアクセス制御をセットアップできるようにします。FC ストレージ範囲が設定された VSAN 上に、単一のイニシエータの単一のターゲット、または単一のイニシエータの複数のターゲットゾーンを作成し、ゾーン ポリシーを vHBA を使用して SAN 接続ポリシーにアタッチできます。

（注） ゾーンは、ファブリック インターコネクトが FC スイッチング モードの場合にのみ構成できます。

構成のばらつきの検出は、FC ゾーン ポリシーではサポートされていません。

ポリシーの作成

Cisco Intersight では、ポリシー ウィザードを使用して UCS サーバまたは UCS ドメイン ポリシーを作成できます。新しいポリシーを作成して設定するには、次の手順を実行します。

ステップ 1 Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。

ステップ 3 **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。

ステップ 4 **[UCS サーバ（UCS Server）]** > *<A UCS server policy>* を選択します。

ステップ 5 **[スタート（Start）]** をクリックして、ポリシーの設定を開始します。

ステップ 6 **[全般（General）]** ページで、ポリシーの **[名前（Name）]** を入力します。オプションとして、**[説明（Description）]** と **[タグ（Tags）]** を入力します

ステップ 7 **[ポリシーの詳細（Policy Details）]** ページで、ポリシーのプロパティを設定します。

一部のポリシー プロパティは、特定のターゲット プラットフォーム（スタンドアロン UCS サーバ、FI 接続UCS サーバ、またはその両方）に適用できます。**[すべてのプラットフォーム（All Platforms）]** オプション、**[UCS サーバ（スタンドアロン）（UCS Servers (Standalone)）]** オプション、**UCS Servers (FI-Attached)[UCS サーバ（FI 接続）（UCS Servers (FI-Attached)）]** オプションをクリックすると、各プロパティを個別に表示できます。スタンドアロン サーバまたはFI接続サーバにのみ適用されるプロパティは、プロパティの横にアイコンで示されます。

ステップ 8 **[作成（Create）]** をクリックします。

サポートされている UCS サーバ ポリシー

次の表に、UCS サーバ ポリシーと、それらがサポートされる管理対象デバイスのリストを示します。この表に記載されているすべてのサーバポリシーは、Cisco Intersight Essentials ライセンスで使用できます。

UCS サーバ ポリシー	サポート対象のサーバ												
	Cisco UCS C シリーズ									Cisco UCS B シリーズ		Cisco UCS X シリーズ	
	スタンドアロン					IMM				IMM		IMM	
	M4	M5	M6	M7	M8	M5	M6	M7	M8	M5	M6	M6	M7
証明書管理ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい
デバイス コネクタ ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
IPMI Over LAN ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
LDAP ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
ローカル ユーザ ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
NTP ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
ネットワーク接続ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
永続メモリ ポリシー	—	はい	はい	いいえ	いいえ	—	—	—	—	—	—	—	—

UCS サーバ ポリシー	サポート対象のサーバ												
	Cisco UCS C シリーズ									Cisco UCS B シリーズ		Cisco UCS X シリーズ	
	スタンドアロン					IMM				IMM		IMM	
	M4	M5	M6	M7	M8	M5	M6	M7	M8	M5	M6	M6	M7
電源ポリシー	—	—	—	—	—	—	—	—	—	はい	はい	はい	はい
SD カードポリシー	はい	はい	—	—	—	はい	—	—	—	はい	—	—	—
SMTP ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
SNMP ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
SSH ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
Serial Over LAN（SoL）ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
Syslog ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
仮想 KVM ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
BIOS トークン ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

UCS サーバ ポリシー	サポート対象のサーバ												
	Cisco UCS C シリーズ									Cisco UCS B シリーズ		Cisco UCS X シリーズ	
	スタンドアロン					IMM				IMM		IMM	
	M4	M5	M6	M7	M8	M5	M6	M7	M8	M5	M6	M6	M7
仮想メディア ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
LAN 接続ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
SAN 接続ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
ブート順序ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
アダプタ設定ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
ドライブ セキュリティ ポリシー	いいえ	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
ストレージ ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
IMC アクセス ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい

UCS サーバ ポリシー	サポート対象のサーバ												
	Cisco UCS C シリーズ									Cisco UCS B シリーズ		Cisco UCS X シリーズ	
	スタンドアロン					IMM				IMM		IMM	
	M4	M5	M6	M7	M8	M5	M6	M7	M8	M5	M6	M6	M7
イーサネット アダプタ ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
イーサネット ネットワーク ポリシー	はい	はい	はい	はい	はい	—	—	—	—	—	—	—	—
イーサネット QoS ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
イーサネット ネットワーク制御ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい
イーサネット ネットワーク グループ ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい
FC ゾーン ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい

UCS サーバ ポリシー	サポート対象のサーバ												
	Cisco UCS C シリーズ									Cisco UCS B シリーズ		Cisco UCS X シリーズ	
	スタンドアロン					IMM				IMM		IMM	
	M4	M5	M6	M7	M8	M5	M6	M7	M8	M5	M6	M6	M7
ファイバ チャネル アダプタ ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
ファイバ チャネル ネットワーク ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
ファイバチャネル QoS ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
iSCSI ブート ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい
iSCSI アダプタ ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい

UCS サーバ ポリシー	サポート対象のサーバ												
	Cisco UCS C シリーズ									Cisco UCS B シリーズ		Cisco UCS X シリーズ	
	スタンドアロン					IMM				IMM		IMM	
	M4	M5	M6	M7	M8	M5	M6	M7	M8	M5	M6	M6	M7
iSCSI スタティック ターゲット ポリシー	—	—	—	—	—	はい	はい	はい	はい	はい	はい	はい	はい
ファームウェア ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
温度ポリシー	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

証明書管理ポリシーの作成

Intersight管理モードでは、証明書管理ポリシーを使用して、外部証明書の証明書の詳細を指定し、ポリシーをサーバーにアタッチできます。Cisco Intersight は現在、次の証明書をサポートしています。

- **ルート CA 証明書**： HTTPS ブート認証にはルート CA 証明書が必要です。証明書管理ポリシーを使用して、最大10個のルートCA証明書を展開できます。正常に起動するには、有効で期限切れになっていないルート CA 証明書が少なくとも 1 つ必要です。詳細については、「ブート順序ポリシーの作成」を参照してください

（注） Intersight 管理モード サーバーでは、サーバー プロファイルを削除すると、CIMC からルート CA 証明書が削除されます。

ただし、スタンドアロン モードの C シリーズ サーバーの場合、ルート CA 証明書は自動的に削除されません。CIMC から手動で削除するか、サーバーで初期設定へのリセットを実行する必要があります。さらに、スタンドアロンモードでCシリーズサーバーのプロファイルをエクスポートする場合、証明書管理ポリシーは含まれません。

- **IMC 証明書（IMC certificates）**： このオプションは、Intersight 管理モードのサーバーでのみ使用できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[証明書の管理（Certificate Management）]** の順に選択し、**[開始（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、指定する証明書を追加し、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
ルート CA	• **[証明書名（Certificate Name）]**：証明書の名前を入力します。 • **[証明書（Certificate）]**：証明書の詳細を入力します。

プロパティ（Property）	基本情報（Essential Information）
IMC	• [証明書（Certificate）]：証明書の詳細を入力します。 • [秘密キー（Private Key）]：証明書の秘密キーの詳細を入力します。

7. [作成（Create）] をクリックします。

アダプタ設定ポリシーの作成

アダプタ設定ポリシーは、仮想インターフェイス カード（VIC）アダプタ用のイーサネットおよびファイバ チャネルを設定します。

（注） このポリシーを、Intersight 管理のファブリック接続サーバに割り当てられているサーバ プロファイルに適用しても、無視されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [アダプターの構成（Adapter Configuration）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. [ポリシーの詳細（Policy Details）] ページで、[VIC アダプタ設定の追加（Add VIC Adapter Configuration）] をクリックし、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
VIC アダプタ設定の追加	
[PCI スロット（PCI Slot）]	アダプタが装着されている PCI スロット。 有効な範囲は 1～15 および MLOM です。
[LLDP]	アダプタ インターフェイスの LLDP プロトコルのステータス。 オンにした場合、リンク レイヤー検出プロトコル（Link Layer Discovery Protocol、LLDP）により、データセンターブリッジ機能交換（Data Center Bridging Capability Exchange、DCBX）プロトコルの全機能が有効になります。それには、FCoE、フロー制御に基づく優先度が含まれます。 （注） LLDP を使用できるのは一部の UCS C シリーズ サーバだけです。 LLDP オプションを無効にすると、DCBX の機能がすべて無効になるため、無効にしないようにお勧めします。
[FIP]	アダプタ インターフェイスの FIP プロトコルのステータス。 オンにすると、FCoE 初期化プロトコル（FCoE Initialization Protocol、FIP）モードが有効になります。FIP モードは、アダプタが現在の FCoE 標準との互換性を保つことを保証します。 （注） FIP オプションは、テクニカル サポートの担当者から明示的に指示された場合にだけ使用してください。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ポート チャネル （Port Channel）]	アダプタ インターフェイスのポート チャネル ステータス。 ポートチ ャネルを有効にすると、アダプタカードで 2 つの vNIC と 2 つの vHBA を使用できます。無効にすると、4 つの vNIC と 4 つの vHBA をアダプタカードで使用できます。ポート チャネルを無効にすると、サーバがリブートします。 （注） ポート チャネルは、Cisco VIC 1455/1457 アダプタでのみサポートされます。

[プロパティ（Property）]	[基本情報（Essential Information）]
物理 NIC モードの有効化	

[プロパティ（Property）]	[基本情報（Essential Information）]
	物理 NIC モードが有効になっている場合、VIC のアップリンク ポートはパススルー モードに設定されます。これにより、ホストは変更を行わずにパケットを送信できます。VIC ASIC は、vNIC の VLAN と CoS の設定に基づいてパケットの VLAN タグをリライトしません。 （注） • 物理 NIC モードを有効にすると、サーバーが再起動します。 • 物理 NIC モードは、UCS VIC 1400 シリーズおよび VIC 15000 シリーズアダプタをサポートします。 • サポートされている最小の Cisco サーバー ファームウェア バージョン 4.2(2a) 以降およびアダプタ ファームウェア バージョン 5.2(2a)。 • この機能は、Cisco Intersight Managed FI Attached サーバーではサポートされていません。 • 物理 NIC モードが有効になっている場合は、デフォルトの vNIC のみが追加されます。 • 次のようなアダプタでは、このオプションを有効にすることはできません。 • **[ポート チャネル モード (Port Channel mode)]** が有効になっています • **[VNTAG モード (VNTAG mode)]** が有効になっているもの • **[LLDP]** が有効になっているもの • **[FIP モード (FIP mode)]** が有効になっているもの • **[CISCO IMC**

[プロパティ（Property）]	[基本情報（Essential Information）]
	管理が有効 (Cisco IMC Management Enabled)] 値が **[はい (Yes)]** に設定されています 物理 NIC モードが有効になっている場合、ポップアップ ウィンドウに次のメッセージが表示されます。 **物理 nic-mode が切り替わった後、vNIC構成は失われて新しいデフォルトvNICが作成されます。** [OK] をクリックします。
[DCE インターフェイス（DCE Interface）]	アダプタの DCE インターフェイスの転送エラー訂正（FEC）モード設定。 （注） FEC モード設定は、Cisco VIC 14xx アダプタでのみサポートされます。FEC モード「cl74」は Cisco VIC 1495/1497 ではサポートされていません。この設定は、サポートされていないアダプタおよび使用できない DCE インターフェイスでは無視されます。

7. **[追加（Add）]** をクリックします。
8. **[作成（Create）]** をクリックします。

LAN 接続ポリシーの作成

LAN接続ポリシーは、ネットワーク上のサーバとLANの接続およびネットワーク通信リソースを決定します。MAC アドレスプールまたは静的 MAC アドレスを指定して MAC アドレスをサーバに割り当て、サーバがネットワークとの通信に使用する vNIC を識別します。

前提条件

LAN 接続ポリシーを作成するには、要件に従って次のサブポリシーまたはプールを選択します。

- **[イーサネット ネットワーク ポリシー（Ethernet Network Policy）]**：ポートが単一の VLAN（アクセス）トラフィックを伝送するか、複数の VLAN（トランク）トラフィックを伝送

するかを指定します。タグが見つからない場合にイーサネット パケットに関連付ける VLAN を指定できます。

- **[イーサネット QoS ポリシー（Ethernet QoS Policy）]**：仮想インターフェイスがサポートする$1 $2フレームペイロードの最大サイズを設定し、仮想インターフェイスのデータレートを制限し、サービス クラスを仮想インターフェイスのトラフィックに関連付けます。
- **[イーサネット アダプタ ポリシー（Ethernet Adapter Policy）]**：アダプタのホスト側の動作を制御するVXLAN、NVGRE、ARFS、割り込み設定、RoCE、TCPオフロード設定のような機能を構成します。
- **[IQN プール（IQN Pool）]**：IQNブロックのプレフィックスとサフィックス、ブロックの最初のサフィックス番号、およびブロックが保持できるIDの数を設定できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[LAN 接続（LAN Connectivity）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、以下の情報を設定します。
   - **[名前（Name）]**：ポリシーの名前です。
   - **[ターゲット プラットフォーム（Target Platform）]**： ポリシーが適用されるターゲットプラットフォームです。これは、**[スタンドアロン（Standalone）]** サーバまたは **[FI 接続サーバ（FI Attached）]** サーバのいずれかです。

     スタンドアロン サーバ用に作成された LAN 接続ポリシーは、FI 接続サーバに展開できません。同様に、FI 接続サーバ用に作成された LAN 接続ポリシーは、スタンドアロン サーバには展開できません。
   - **[説明（Description）]**：ポリシーの識別に役立つ説明です。
   - **[タグ（Tag）]**：ポリシーのタグです。タグはkey：value形式である必要があります。たとえば、Org: IT または Site: APJ などです。
6. **[ポリシーの詳細（Policy Details）]** ページで、次を設定します。
   - FI 接続サーバの場合、**[Azure スタックホスト QoS の有効化（Enable Azure Stack Host QoS）]** ボタンをオンにして、RDMA が有効になっているアダプタに Azure Stack QoS 機能を正常に展開します。

     [有効（Enabled）]：アダプタでAzureStack-Host QoSを有効にすると、ユーザはRDMAトラフィックのトラフィック クラスを分割し、帯域幅の必要な部分を確実に割り当てることができます。

     [無効（Disabled）]：アダプタの Azure Stack Host QoS 機能を無効にします。

- **[なし（None）]**、**[プール（Pool）]**、または **[静的（Static）]** を選択して、IQN を関連付けないか、IQN プールまたは一意の IQN ID をポリシーに関連付けるかどうかを指定します。
  - **[なし（None）]**：このオプションを選択した場合、IQN の詳細を指定する必要はありません。
  - **[プール（Pool）]**：このオプションを選択した場合は、LAN 接続ポリシーに関連付ける IQN プールを選択します。
  - **[静的（Static）]**：このオプションを選択すると、ファブリック インターコネクト ドメインの iSCSI vNIC がイニシエータ ID として使用するスタティック IQN を入力します。

- 各 vNIC の配置オプション（**[手動（Manual）]** または **[自動（Auto）]**）を選択します。
  - **[手動 vNIC 配置（Manual vNIC Placement）]**：このオプションを選択した場合は、各 vNIC の配置を手動で指定する必要があります。また、**[グラフィック vNIC エディタ（Graphic vNICs Editor）]** を使用して、vNIC とスロットを追加し、それらの間の接続を定義することによって、各 vNIC の配置を手動で作成および指定することもできます。

（注）
- 手動配置の場合、**[PCI リンク（PCI Link）]** は UCS VIC 1400 シリーズアダプタではサポートされません。
- LAN 接続ポリシーに簡易配置と拡張配置の両方がある場合は、サーバー プロファイルの展開の失敗を防ぐために、PCI 順序で指定された番号が適切であることを確認してください。

  - **[自動 vNIC 配置（Auto vNIC Placement）]**：このオプションを選択すると、vNIC 配置はプロファイルの展開時に自動的に実行されます。このオプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。

（注）
- Cisco UCS VIC 1300 シリーズ アダプタの自動アップグレードは、Cisco サーバ ファームウェア バージョン 4.2（2e）以降を搭載した B シリーズ サーバーでサポートされています。
- Cisco UCS VIC 1300 シリーズ アダプタを搭載したサーバの Cisco サーバ ファームウェア バージョンが 4.2（2g）よりも古い場合、C シリーズ サーバの検出はトリガーされません。Cisco サーバ ファームウェアを 4.2（2g）にアップグレードして、サーバ検出を有効にします。

7. **[vNIC の追加（Add vNIC）]** をクリックし、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[vNIC の追加（Add vNIC）] 構成する各 VIC アダプタの eth0 と eth1 のインターフェイスを構成したことを確認します。ネットワークの要件に応じて、その他の vNIC を追加できます。	
[名前（Name）]	vNIC 名です。
ピングループ名	特定のポート/ポートチャネルを含むピン グループの名前。vNIC からのすべてのトラフィックは、指定されたアップリンク イーサネット ポートまたはポート チャネルに固定されます。 （注） 個人識別番号グループは、ポート ポリシーを作成する間に定義できます。 vNIC に対してピン グループが割り当てられていない場合、アップリンク イーサネット ポートまたはポート チャネルがサーバー インターフェイスから動的に選択されます。この選択は永続的ではありません。インターフェイス フラップまたはサーバのリブートの後は、そのサーバ インターフェイスからのトラフィックに対して別のアップリンク イーサネット ポートまたはポート チャネルが使用される可能性があります。
[MAC アドレス プール（MAC Address Poo）]	**[プールの選択（Select Pool）]** をクリックし、MAC アドレス割り当ての MAC アドレス プールを選択します。
[静的（Static）]	**[静的（Static）]** をクリックし、MAC アドレス割り当ての静的MACアドレスを入力します。このオプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。
[配置（Placement）] 仮想インターフェイスの配置の設定。	

プロパティ（Property）	基本情報（Essential Information）
Simple 簡易配置を選択すると、スロット ID と PCI Link はシステムによって自動的に決定されます。最初の VIC に nVIC が展開されます。スロット識別子によって最初の VIC が決まります。スロット識別子の番号付けは MLOM で始まり、その後は 1 から始まり、1 ずつ増加し続けます。PCI リンクは常に 0 に設定されます。	
[スイッチ ID（Switch ID）]	vNIC トラフィックを伝送するファブリック インターコネクトを指します。
[PCI の順序（PCI Order）]	仮想インターフェイスが起動される順序です。インターフェイスに割り当てられる順序は、VIC アダプタの各 PCI リンク上のすべてのイーサネットおよびファイバ チャネル インターフェイスに対して「0」から始めて順に一意である必要があります。PCI順序の最大値は、VIC アダプタの各 PCI リンク上の仮想インターフェイス（イーサネットおよびファイバ チャネル）の数によって制限されます。 （注） 2 つの vNIC の PCI順序を変更するには、vNIC を削除して再作成する必要があります。
詳細設定	
自動スロット ID 割り当て	有効にすると、スロット ID はシステムによって自動的に決定されます。
[スロット ID（Slot ID）]	自動スロット ID割り当てが無効になっている場合は、スロット ID を手動で入力する必要があります。 サポートされている値は（1～15）で、MLOM です
PCI リンク 仮想インターフェイスのトランスポートとして使用される PCI リンク。 PCI リンクは、2 つの PCI リンクをサポートする一部の Cisco UCS VIC 1300 シリーズ モデル（UCSC-PCIE-C40Q-03、UCSB-MLOM-40G-03、UCSB-VIC-M83-8P）にのみ適用されます。他の VIC モデルの値が指定されている場合、その値は無視されます。 （注） ホスト デバイスの順序は、PCI リンクの両方を使用している場合、および vNIC を追加または削除している場合に影響を受ける可能性があります。	

プロパティ（**Property**）	基本情報（**Essential Information**）
PCI リンクの自動割り当て	有効にすると、PCI リンクはシステムによって自動的に決定されます。 （注） • スロット ID と PCI リンクの両方で自動割り当てが有効になっている場合、動作は単純な配置と同じです。すべての vNIC は同じ PCI リンク（リンク 0）に配置されます。 • 自動スロット ID 割り当てが無効で、自動 PCI リンク割り当てが有効になっている場合は、スロット ID を指定する必要があり、vNIC は PCI リンク 0 に配置されます。
ロード バランシング	[自動 PCI リンク割り当て（Automatic PCI link Assignment）] が無効で [ロード バランシング（Load Balanced）] が有効になっている場合、システムは PCI リンク全体にインターフェイスを均等に分散します。 • 自動 PCI リンク割り当てが無効で、自動スロット ID が有効になっている場合は、vNIC をロードバランシングするために PCI 順序を指定する必要があります。 • 自動 PCI リンク割り当てと自動スロット ID の両方が無効になっている場合は、スロットと PCI 順序を指定して vNIC のロードバランシングを行う必要があります。 （注） vNIC を削除して再作成しないと、2 つの vNIC の PCI リンク モードをロードバランシング モードからカスタム モードに変更することはできません。

プロパティ（Property）	基本情報（Essential Information）
Custom	• 自動 PCI リンク割り当てが無効で、自動スロット ID が有効になっている場合は、PCI 順序、PCI リンク、およびスイッチ ID の値を指定する必要があります。 • 自動 PCI リンク割り当てと自動スロット ID 割り当ての両方が無効になっている場合は、スロット ID、PCI 順序、および PCI リンクの値を指定する必要があります。 （注） vNIC を削除して再作成しないと、2 つの vNIC の PCI リンク モードをカスタム モードからロードバランシング モードに変更することはできません。
[コンシステント デバイス名（Consistent Device Naming、CDN）] 仮想 NIC のコンシステント デバイス名（CDN）の設定。	
[ソース（Source）]	CDN 名のソースが vNIC インスタンスの名前であるか、ユーザ定義の名前であるかです。
[フェールオーバー（Failover）] フェールオーバーを有効にすると、アップリンクで障害が発生した場合に、トラフィックが自動的に 1 つのアップリンクから別のアップリンクにフェールオーバーします。	
イーサネット ネットワーク ポリシー	イーサネット ネットワーク ポリシーを選択するか、作成します。 （注） このサブポリシーは、スタンドアロン サーバーの LAN 接続ポリシーにのみ適用されます。
イーサネット ネットワーク グループ ポリシー	イーサネット ネットワーク グループ ポリシーを選択するか、作成します。 （注） このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。

プロパティ（**Property**）	基本情報（**Essential Information**）
[イーサネット ネットワーク制御ポリシー（Ethernet Network Control Policy）]	イーサネット ネットワーック制御ポリシーを選択または作成します。 （注） このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。
イーサネット QoS ポリシー	イーサネット QoS ポリシーを選択するか、作成します。
イーサネット アダプタ ポリシー	イーサネット アダプタ ポリシーを選択するか、作成します。
[iSCSI ブート ポリシー（iSCSI Boot Policy）]	iSCSI ブート ポリシーを選択するか、作成します。 （注） このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。
接続：Disabled/usNIC/VMQ/SR-IOV	
[無効（Disabled）]	接続ポリシーを設定しません。
usNIC パケットの送信/受信時にカーネル層をバイパスすることによって低遅延および高スループットを実現する、ユーザ スペース NIC の設定。	
[usNIC の数（Number of usNICs）]	作成される usNIC インターフェイスの数。
[usNIC アダプタ ポリシー（usNIC Adapter Policy）]	usNIC に関連付けられるイーサネット アダプタ ポリシーを選択します。
[サービス クラス（Class of Service）]	UsNIC 上のトラフィックに使用されるサービス クラス。
[VMQ] ゲスト オペレーティング システムへの効率的なネットワーク トラフィックの転送を実現する、仮想インターフェイスの仮想マシンキューの設定。	
[マルチ キュー サポートの有効化（Enable Multi Queue Support）]	仮想マシン マルチ キュー（VMMQ）がポリシーで有効かどうか。VMMQ を使用して、複数のキューが 1 つの VM に割り当てられます。
[サブ vNIC 数（Number of Sub vNICs）]	マルチ キューで使用可能なサブ vNIC の数。

プロパティ（Property）	基本情報（Essential Information）
[Roce 設定の有効化（Enable RoCE Settings）]	この仮想インターフェイスでリモート ダイレクト メモリ アクセス（RDMA）over Converged Ethernet（RoCE）が有効になっているかどうか。
[メモリ領域（Memory Regions）]	アダプタ当たりのメモリ リージョンの数。 1 ～ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[キューペア（Queue Pairs）]	アダプタ当たりのキュー ペアの数。 1 ～ 8192 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[リソース グループ（Resource Groups）]	アダプタ当たりのリソース グループの数。 1 ～ 128 の整数を入力します。 最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。
[Version（バージョン）]	RDMA プロトコルのバージョン バージョン 1 は、リンク層プロトコルです。同じイーサネット ブロードキャスト ドメインの 2 つのホスト間で通信できるようにします。 RoCEv2 は、インターネット層プロトコルです。RoCEv2 パケットをルーティングできます。RoCEv2 パケットに IP および UDP ヘッダーが含まれるようになったため可能です。
SR-IOV Single Root Input/Output Virtualization（SR-IOV）により、さまざまな Linux ゲスト オペレーティング システムを実行している複数の VM が、ホスト サーバー内の単一の PCIe ネットワーク アダプタを共有できるようになります。SR-IOV では、VM が vNIC との間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。	
VF の数	作成する VF の数。1～64 の値を入力してください。デフォルト値は 64 です。

プロパティ（Property）	基本情報（Essential Information）
VFごとの受信キュー数	各VFに設定する受信キューリソースの数。1 ～ 8 の値を入力します。デフォルト値は4です。
VFごとの送信キュー数	各VFに設定する送信キューリソースの数。1 ～ 8 の値を入力します。デフォルト値は 1 です。
VFごとの完了キュー数	各VFに設定する完了キューリソースの数。1～16の値を入力してください。デフォルト値は 5 です。
VFごとの割り込み数	各 VF に設定する割り込みカウントの数。1～16 の値を入力してください。デフォルト値は 8 です。

8. vNICテンプレートを使用してFI接続サーバーのvNICを取得するには、**[追加（Add）]** ドロップダウンリストから **[テンプレート（Template）] から [vNIC]** を選択します。vNICテンプレートの作成の詳細については、「*vNIC* または *vHBA* テンプレートの作成」を参照してください。

（注）
- テンプレートからvNICを取得する場合、vNIC設定はテンプレート設定から自動的に入力されます。vNIC テンプレートを使用して設定のオーバーライドが有効になっているパラメータを編集または削除できます。オーバーライドが有効になっていないパラメータの場合は、[目（Eye）] アイコンを使用して設定を表示することしかできません。
- オーバーライドされたパラメータは、[オーバーライド（Overridden）] ラベルを使用して示されます。オーバーライドが有効なパラメータの場合、テンプレートに適用された変更は、派生 vNIC に反映されません。
- テンプレートに含まれていない派生 vNIC インスタンスでは、これらのパラメータのみを変更できます。
- プロファイルの展開中にテンプレートから vNIC を取得しようとすると、プロファイルの展開が完了するまでタスクが再試行されます。これらの詳細は、[リクエスト（Requests）] タブで確認できます。

9. **[作成（Create）]** をクリックします。

[IMM でサポートされるアダプタの構成機能マトリックス（Configuration Feature Matrix for Supported Adapters in IMM）]

次の表は、Intersight管理モードのさまざまなアダプタでサポートされている機能を示しています。

機能	Cisco UCS 1300 シリーズ アダプタ	Cisco UCS 1400/14000 シリーズ アダプタ	Cisco UCS 15000 シリーズ アダプタ
usNIC	はい	はい	はい
VMQ	はい	はい	はい
VMMQ	いいえ	はい	はい
SR-IOV	いいえ	はい	はい
NetQueue	はい	はい	はい
RoCEv1	はい	いいえ	いいえ
RoCEv2	いいえ	はい	はい
Geneveオフロード	いいえ	はい	はい
アズールQoS	いいえ	はい	はい
RSSRSS	はい	はい	はい
RSSv2	いいえ	いいえ	はい
NVGRE	はい	はい	はい
ARFS	はい	はい	はい
VIC Q-in-Q トンネリング	いいえ	はい	はい
VXLAN	はい	はい	はい
Advance Filter	はい	はい	はい
割り込みスケーリング/グループ割り込み	はい	はい	はい
ホストポート構成	はい	いいえ	いいえ
vHBAタイプ	はい	はい	はい
16K リング サイズ	いいえ	いいえ	はい
高精度時間プロトコル	いいえ	いいえ	はい
FC MQ	はい	はい	はい
FC NVMe	はい	はい	はい
ENS	いいえ	はい	はい

イーサネット アダプタ ポリシーの作成

イーサネットアダプタポリシーは、アダプタのトラフィック処理方法など、アダプタのホスト側の動作を制御します。VIC 仮想イーサネットインターフェイスごとにさまざまな機能を設定できます。設定可能な機能には Virtual Extensible LAN（VXLAN）、Generic Routing Encapsulation（NVGRE）を使用したネットワーク仮想化、Accelerated Receive Flow Steering（ARFS）、割り込み設定、TCP オフロード設定などがあります。

イーサネット アダプタ ポリシーには、サポートされているサーバ オペレーティング システムごとの、仮想イーサネットインターフェイスの推奨設定が含まれています。オペレーティングシステムはこれらのポリシーの影響を受けます。一般に、ストレージベンダーでは、デフォルト以外のアダプタ設定を要求します。必須設定の詳細については、ベンダーが提供しているサポート リストで確認できます。

GENEVE オフロード

Cisco Intersight は、ESXi プラットフォームで汎用ネットワーク仮想カプセル化（Generic Network Virtualization Encapsulation、GENEVE）オフロードをサポートするようになりました。これにより、基本的にすべての情報をパケットにエンコードし、トンネルエンドポイント間で渡すことができます。GENEVE は、1400 シリーズ アダプタのデータセンター ファブリック全体で分離されたマルチテナント ブロードキャスト ドメインを作成するためのオーバーレイ機能を提供します。GENEVE プロトコルを使用すると、物理ネットワークの境界にまたがる論理ネットワークを作成できます。

GENEVE オフロードは、すべてのイーサネット アダプタ ポリシーに存在しますが、デフォルトでは無効になっています。VMWare ESXi GENEVE を使用する場合は推奨設定です。

GENEVE オフロードのエンドツーエンド設定の実装方法については、NSX-T のマニュアルを参照してください。

GENEVE オフロードが有効になっている場合は、イーサネット アダプタ ポリシーで次の値を設定することを推奨します。

- 送信キュー : 1
- TX リング サイズ : 4096
- 受信キュー : 8
- RX リング サイズ : 4096
- 完了キュー : 16
- 割り込み : 32

次の機能は、いずれかのインターフェイスで GENEVE オフロードが有効になっている場合はサポートされません。

- Azure QoS

- RoCEv2：ある vNIC で GENEVE を有効にし、別の vNIC で RoCEv2 を有効にすることはできません。
- 高度なフィルタ
- VIC Q-in-Q トンネリング

インターフェイスでの usNIC および VIC QinQ トンネリング機能のサポート：

（注）
- usNIC または VMQ は、1400 シリーズアダプタのみの同じインターフェイス上の GENEVE オフロードと互換性がありません。
- usNIC または VMQ は、1400 シリーズアダプタのさまざまなインターフェイスで GENEVE オフロードと互換性があります。
- usNIC と VMQ は、1500 シリーズアダプタの同じインターフェイスと異なるインターフェイスの両方で GENEVE オフロードと互換性があります。

（注）
GENEVE オフロード機能から Azure Stack QoS 機能へ、またはその逆に切り替える場合は、次の手順を実行します。

1. 現在の機能を無効にする
2. サーバのリブート
3. 必要機能の有効化

GENEVE オフロードには、次のような制限もあります。

- 外部外部 IPV6 は、GENEVE Offload ではサポートされていません。
- GENEVE オフロードは、ESX 7.0（NSX-T 3.0）および ESX 6.7U3（NSX-T 2.5）でサポートされています。
- GENEVE オフロードは、14xx シリーズ アダプタと 15xx シリーズ アダプタでのみサポートされます。UCS VIC 13xx シリーズまたは 12xx シリーズアダプタではサポートされていません。
- Cisco では、サポートされていないリリースにダウングレードする前に、 GENEVE オフロードの設定を削除することを推奨しています。

GENEVEオフロードでサポートされる機能マトリックスの詳細については、次の表を参照してください。

表 *4 : GENEVE* オフロードのサポート機能マトリックス

	KVM VMFEX	VXLAN	NVGRE	RoCEv2	usNIC	NetFlow	高度なフィルタ	VMQ/ VMMQ/ netqueue	arfs	Azure QoS
インターフェイス vnic1 で GENEVE オフロードを有効した場合、機能は vnic1 で有効にされる	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
インターフェイス vnic1 で GENEVE オフロードを有効した場合、機能は vnic2 で有効にされる	はい	はい	はい	いいえ	はい	○	○	○	はい	いいえ

（注） 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。シスコのテクニカル サポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

表 *5 : 1500* シリーズ アダプタ の *GENEVE* オフロードのサポート機能マトリックス

	VXLAN	NVGRE	RoCEv2	usNIC	NetFlow	高度なフィルタ	VMQ/ VMMQ/ netqueue	arfs	アダプタごとのクワッドポート	アダプタごとの物理 NIC ノード
同じインターフェイス（vnic1）で GENEVE オフロードを有効した場合、機能は vnic1 で有効にされる	はい	はい	いいえ	はい	○	○	はい	いいえ	はい	はい
異なるインターフェイス（vnic1）で GENEVE オフロードを有効した場合、機能は vnic2 で有効にされる	はい	はい	いいえ	はい	○	○	○	○	○	○

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット アダプタ（Ethernet Adapter）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。
[イーサネットアダプタのデフォルト設定（Ethernet Adapter Default Configuration）]	
デフォルト設定を選択します	クリックして、デフォルト設定を表示し、インポートします。ポリシーは現在 16 のデフォルト設定をサポートしています。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[仮想拡張 LAN の有効化（Enable Virtual Extensible LAN）]	仮想イーサネット インターフェイスで、仮想拡張可能 LAN プロトコルを有効にします。
[汎用ルーティングカプセル化を使用したネットワーク仮想化の有効化（Enable Network Virtualization using Generic Routing Encapsulation）]	仮想イーサネット インターフェイスで汎用ルーティング カプセル化を使用して、ネットワーク仮想化を有効にします。 （注） NVGRE オフロードを有効にするには、送信チェックサム オフロードと TSO をイネーブルにする必要があります。
[加速受信フロー処理の有効化（Enable Accelerated Receive Flow Steering）]	仮想イーサネットインターフェイスでの加速受信フロー処理（ARFS）を有効にします。ARFS は、ハードウェアによる受信フロー処理で、CPUデータ キャッシュ ヒット率を向上させることができます。これは、カーネル レベルのパケット処理を、そのパケットを消費するアプリケーション スレッドが動作している CPU に誘導することによって行います。
[高度なフィルタの有効化（Enable Advanced Filter）]	仮想イーサネット インターフェイスでの高度なフィルタを有効にします。
割り込みスケーリングの有効化	仮想イーサネット インターフェイス上のリソースの割り込みスケーリングを有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
Geneve オフロード	GENEVE オーバーレイ ハードウェア オフロードを有効にします。
[RoCE の設定（RoCE Settings）] Intersight サポート Microsoft SMB ダイレクト用 RDMA over Converged Ethernet（RoCE）のサポート。イーサネット アダプタ ポリシーを作成または変更しながら、追加の設定情報をアダプタに送信します。	
RDMA over Converged Ethernet の有効化	この仮想インターイーサネットフェイスで RDMA over Converged Ethernet（RoCE）を有効にします。 RoCE は、イーサネット ネットワーク越しのダイレクト メモリ アクセスを実現します。RoCE はリンク層プロトコルであるため、同じイーサネット ブロードキャスト ドメインにある任意の 2 ホスト間の通信を可能にします。RoCE は、低遅延、低 CPU 使用率、、およびネットワーク帯域幅使用率の高さによって、従来のネットワーク ソケット実装と比較して優れたパフォーマンスを提供します。
[キューペア（Queue Pairs）]	アダプタ当たりのキュー ペアの数。 0 ～ 8192 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。 （注） このプロパティは、**[Enable RDMA over converged Ethernet]** が有効になっている場合にのみ表示されます。
[メモリ領域（Memory Regions）]	アダプタ当たりのメモリ リージョンの数。 0 ～ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。 （注） このプロパティは、**[Enable RDMA over converged Ethernet]** が有効になっている場合にのみ表示されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[リソース グループ（Resource Groups）]	アダプタ当たりのリソース グループの数。最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2のべき乗の整数にすることをお勧めします。 0 ～ 128 の整数を入力します。 （注） このプロパティは、**[Enable RDMA over converged Ethernet]** が有効になっている場合にのみ表示されます。
[Version（バージョン）]	RDMA プロトコルのバージョン バージョン1は、リンク層プロトコルです。同じイーサネット ブロードキャスト ドメインの 2 つのホスト間で通信できるようにします。 （注） このプロパティは、**[Enable RDMA over converged Ethernet]** が有効になっている場合にのみ表示されます。
[割り込み設定（Interrupt Settings）]	
[割り込み（Interrupts）]	割り当てる割り込みリソースの数。通常この値は、完了キュー リソースの数と同じにします。 1 ～ 1024 の整数を入力します。
[割り込みモード（Interrupt Mode）]	以下を含む、優先ドライバ割り込みを選択します。 • [MSIx]：機能拡張メッセージ信号割り込み（Message Signaled Interrupts、MSI）。これが推奨オプションです。 • [MSI]：メッセージ信号割り込み（Message Signaled Interrupts、MSI）のみ • [INTx]：PCI INTx 割り込み

[プロパティ（Property）]	[基本情報（Essential Information）]
[割り込みタイマー、（Interrupt Timer、マイクロ秒)]	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。割り込み調停をオフにするには、このフィールドに0（ゼロ）を入力します。 0 ～ 65535 の整数を入力します。
[割り込み調停タイプ（Interrupt Coalescing Type）]	割り込み調停タイプを選択します。 • [最小（Min）] : システムは、別の割り込みイベントを送信する前に [調停時間（Coalescing Time）] フィールドに指定された時間だけ待機します。 • [アイドル（Idle）] : アクティビティなしの期間が少なくとも [調停時間（Coalescing Time）] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[受信（Receive）] 受信キュー リソースの設定。	
[受信キュー数（Receive Queue Count）]	割り当てるキュー リソースの数。 1 ～ 1000 の整数を入力します。
[受信リングサイズ（Receive Ring Size）]	各キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[送信（Transmit）] 送信キュー リソースの設定	
[送信キュー数（Transmit Queue Count）]	割り当てるキュー リソースの数。 1 ～ 1000 の整数を入力します。
[送信リング サイズ（Transmit Ring Size）]	各キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[完了（Completion）] 完了キューリソースの設定。	

[プロパティ（Property）]	[基本情報（Essential Information）]
[完了キュー数（Completion Queue Count）]	割り当てる完了キューリソースの数。通常、割り当てる完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくします。 1 ～ 2000 の整数を入力します。
[完了リング サイズ（Completion Ring Size）]	各キュー内の記述子の数。 1 ～ 256 の整数を入力します。 （注） このプロパティは、**[Enable RDMA over converged Ethernet]** が有効になっている場合にのみ表示されます。
[アップリンク フェールバック タイムアウト（Uplink Failback Timeout、秒）]	アップリンク フェールオーバーが vNIC に対して有効になっている場合の、アップリンク フェールバック タイムアウト（秒単位）。セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の整数を入力します。
[TCP オフロード（TCP Offload）] TCP オフロードの設定は、TCP 関連したネットワーク機能を CPU からネットワーク ハードウェアにオフロードするかどうかを決定します。これらのオプションは、CPU オーバーヘッドの削減とネットワーク スループットの向上に役立ちます。	
[Tx チェックサム オフロードの有効化（Enable Tx Checksum Offload）]	チェックサムを計算できるように、すべてのパケットを CPU からハードウェアに送信します。
[Rx チェックサム オフロードの有効化（Enable Rx Checksum Offload）]	検証できるように、すべてのパケットを CPU からハードウェアに送信します。
[大規模送信オフロードの有効化（Enable Large Send Offload）]	セグメンテーションのため、大規模なパケットを CPU からハードウェアに送信します。
[大規模受信オフロードの有効化（Enable Large Receive Offload）]	セグメント化されたパケットを、ハードウェアで再構成してから、CPU に送信します。

[プロパティ（Property）]	[基本情報（Essential Information）]
受信側スケーリング： 受信側スケーリング（RSS）/受信側スケーリング バージョン 2（RSSv2）は、着信データトラフィックを処理するために複数のコアをサポートします。 RSSv2 は Windows 2019 OS 以降のバージョンでサポートされており、Windows NENIC ドライバが必要です。RSS 対応の Windows NENIC ドライバと Cisco UCS VIC アダプタを使用すると、物理機能（PF）で複数のハードウェア受信キューを設定できます。VIC で VMMQ を有効にすると、仮想マシン（VM）ごとに複数のハードウェア受信キューを設定できます。 RSSv2 機能を使用する前に、NENIC ドライバが RSSv2 をサポートしていることを確認してください。一般に、NENIC ドライバは 4 つのキューをサポートします。RSSv2 では、NENIC ドライバに PF または VM のハードウェア キューの数に上限はありません。	
受信側スケーリングを有効にします。	受信側のスケーリングを有効にし、着信トラフィックを複数の CPU コアに分散できるようにします。このプロパティは、RSS と RSSv2 の両方をサポートします。 デフォルトでは、RSS は有効になっています。RSSv2 は RSS と互換性があります。RSS または RSSv2 での NENIC ドライバのサポートに基づいて、このプロパティは適切にサポートされます。 （注） RSSv2 は、次でサポートされています。 • Cisco UCS VIC 15000 シリーズ アダプタ • Cisco UCS M6 および M7 サーバー
[IPv4 ハッシュの有効化（Enable IPv4 Hash）]	トラフィック分散のため、IPv4 アドレスを有効にします。
[IPv6 ハッシュの有効化（Enable IPv6 Hash）]	トラフィック分散のため、IPv6 アドレス拡張を有効にします。
[IPv6 ハッシュの有効化（Enable IPv4 Hash）]	トラフィック分散のため、IPv6 アドレスを有効にします。
[TCP および IPv4 ハッシュの有効化（Enable TCP and IPv4 Hash）]	トラフィック分散のため、IPv4 アドレスと TCP ポート番号の両方を有効にします。
[TCP および IPv6 拡張ハッシュの有効化（Enable TCP and IPv6 Extensions Hash）]	トラフィック分散のため、IPv6 アドレスと TCP ポート番号の両方を有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[TCP および IPv6 ハッシュの有効化（Enable TCP and IPv4 Hash）]	トラフィック分散のため、IPv6 アドレスと TCP ポート番号の両方を有効にします。
[UDP および IPv4 ハッシュの有効化（Enable TCP and IPv4 Hash）]	トラフィック分散のため、IPv4 アドレスと UDP ポート番号の両方を有効にします。
[UDP および IPv6 ハッシュの有効化（Enable TCP and IPv4 Hash）]	トラフィック分散のため、IPv6 アドレスと UDP ポート番号の両方を有効にします。

7. **[作成（Create）]** をクリックします。

イーサネット QoS ポリシーの作成

イーサネットQuality Of Service (QoS)ポリシーは、vNICに向けた発信トラフィックにシステムクラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS が決定されます。一部のアダプタでは、発信トラフィックでバーストやレートなどの付加的な制御を指定することもできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット QoS（Ethernet QoS）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description）]（オプション）	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MTU（バイト）]	仮想インターフェイスが受け入れる最大伝送ユニット（MTU） またはパケットサイズ。 有効範囲は 1500 ～ 9000 です。デフォルト値は 1500 です
[レート制限（Rate Limit、Mbps）]	仮想インターフェイスでのデータレートの制限に使用される Mbps（0ー100000）単位の値。これを 0 に設定すると、レート制限はオフになります。
[サービス クラス（Class of Service）]	仮想インターフェイス上のトラフィックに関連付けられるサービス クラス。 有効範囲は 0 ～ 6 です。デフォルト値は 3 です。 （注） このプロパティは、スタンドアロンサーバでのみサポートされます。
[バースト（Burst）]	vNIC で許可されるバーストトラフィック（バイト単位）。 有効範囲は 1024 ～ 1000000 です。デフォルト値は 1024 です。 （注） このプロパティは、FI 接続サーバでのみサポートされます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[優先度（Priority）]	次を含む、ドメイン プロファイルで定義されたシステムQoSに一致するプライオリティを選択します。 • ベストエフォート • ファイバ チャネル（FC） • プラチナ • ゴールド • シルバー • ブロンズ （注） • デフォルトでは、**[ベストエフォート（Best -Effort）]** システム クラスが有効になっています。 • このプロパティは、FI 接続サーバでのみサポートされます。
[Trust Host CoS の有効化（Enable Trust Host CoS）]	オンにすると、仮想インターフェイス上のトラフィックに関連付けられるサービス クラスの使用が有効になります。。

7. **[作成（Create）]** をクリックします。

イーサネット ネットワーク ポリシーの作成

イーサネット ネットワーク ポリシーは、ネットワーク トラフィックを処理するポートのルールを設定します。このポリシーは、ポートが単一の VLAN (アクセス) または複数の VLAN (トランク) トラフィックを伝送できるようにするかどうかを決定します。

このポリシーは、VIC QinQ トンネリングもサポートします。QinQ（802.1Qin802.1Q）トンネルにより、ネットワーク内の異なる VLAN を分離および分離できます。QinQ VLAN を設定するには、特定のポート、ポート チャネル、または vNIC の VLAN 設定の一部として、目的の VLAN ID を指定できます。これにより、単一の VLAN トランクを介した複数の VLAN の伝送が可能になります。

重要 このポリシーは、C シリーズ スタンドアロン サーバーでのみサポートされます。

イーサネット ネットワーク ポリシーは、ポートが単一の VLAN (アクセス) または複数の VLAN (トランク) トラフィックを伝送できるようにするかどうかを決定します。タグが見つからない場合には、イーサネットパケットに関連付けられた VLAN を指定できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク（Ethernet Network）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value 形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（**Property**）	基本情報（**Essential Information**）
VLAN Mode	

プロパティ（Property）	基本情報（Essential Information）
	ポートが単一の VLAN (アクセス) または複数の VLAN (トランク) トラフィックを伝送できるようにするかどうかを決定する、トラフィック フローを VLAN に割り当てます。 • **アクセス** モード：トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセス ポートに着信したすべての情報は、ポートに割り当てられている VLAN に所属すると見なされます。 アクセス モードでポートを設定してそのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート（アクセス ポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトのVLAN（VLAN1）のトラフィックだけを伝送します。VLAN のアクセス ポート メンバーシップを変更するには、VLAN を構成します。VLAN をアクセス ポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセス ポート上のアクセス VLANを、まだ作成されていないVLANに変更すると、UCS Manager はそのアクセス ポートをシャット ダウンします。 アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元のMACアドレスを学習せずにドロップします。アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応するすべてのアクセス ポートが、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信します。 • **トランク** モード：トランク ポートは、

プロパティ（**Property**）	基本情報（**Essential Information**）
	複数の VLAN がこのトランク リンクを経由してスイッチ間で伝送を行うことを可能にします。トランク ポートは、タグなしのパケットと 802.1Q タグ付きのパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。ネイティブ VLAN ID とは、トランク ポート上でタグなしトラフィックを伝送する VLAN のことです。 トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。 このプロパティは、スタンドアロンサーバにのみ適用され、FI 接続サーバには適用されません。FI接続モードの場合、VLANモードは**トランク**として設定されます。
アクセス モード	
Q-in-Q トンネリングを有効にする	スライドして、VIC QinQ（802.1Qin802.1Q）トンネリングを有効にします。
[デフォルトの VLA（Default VLAN）]	デフォルトで仮想インターフェイスのトラフィックに割り当てられた VLAN ID を指します。デフォルトの VLAN ID の範囲は 0 ～ 4094 です。

プロパティ（**Property**）	基本情報（**Essential Information**）
QinQ VLAN	このプロパティにより、QinQ トンネリングの構成が有効になり、単一の VLAN 内の複数の VLAN のカプセル化が容易になります。サポートされる VLAN ID の範囲は 2 ～ 4093 で、ネットワーク トラフィックを効果的に管理および分離できます。 （注） このプロパティは、*[QinQ トンネリングの有効化（Enable QinQ Tunneling）]* スライダが有効になっている場合にのみ表示されます。
Trunk Mode	
Q-in-Q トンネリングを有効にする	スライドして、VIC QinQ（802.1Qin802.1Q）トンネリングを有効にします。
[デフォルトの VLA（Default VLAN）]	デフォルトで仮想インターフェイスのトラフィックに割り当てられた VLAN ID を指します。デフォルトの VLAN ID の範囲は 0 ～ 4094 です。
QinQ VLAN	このプロパティにより、QinQ トンネリングの構成が有効になり、単一の VLAN 内の複数の VLAN のカプセル化が容易になります。サポートされる VLAN ID の範囲は 2 ～ 4093 で、ネットワーク トラフィックを効果的に管理および分離できます。 （注） このプロパティは、*[QinQ トンネリングの有効化（Enable QinQ Tunneling）]* スライダが有効になっている場合にのみ表示されます。

7. **[作成（Create）]** をクリックします。

イーサネット ネットワーク グループ ポリシーの作成

イーサネット ネットワーク グループ ポリシーを使用すると、UCS サーバ上の VLAN の設定を管理できます。これらの設定には、許可される VLAN の定義、ネイティブ VLAN の指定、QinQ VLAN の指定が含まれます。

（注） イーサネット ネットワーク グループがポート ポリシーに割り当てられている場合、指定された VLAN セットは、他のアップリンク インターフェイスで指定された VLAN セットと同一であるか、または分離されている必要があります。VLAN が VLAN ポリシーで定義されていること、および **[アップリンクでの自動許可（Auto Allow on Uplinks）]** が無効になっていることを確認します。

このポリシーは、VIC QinQ トンネリングもサポートします。QinQ（802.1Qin802.1Q）トンネルにより、ネットワーク内の異なる VLAN を分離および分離できます。QinQ VLAN を設定するには、特定のポート、ポート チャネル、または vNIC の VLAN 設定の一部として、目的の VLAN ID を指定できます。これにより、単一の VLAN トランクを介した複数の VLAN の伝送が可能になります。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク グループ（Ethernet Network Group）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
VLAN 設定	

プロパティ（**Property**）	基本情報（**Essential Information**）
ネイティブ VLAN	このプロパティを使用すると、仮想インターフェイスのネイティブ VLAN ID または対応する vEthernet を 1 ～ 4093 の範囲で指定できます。 • ネイティブ VLAN が許可された VLAN にすでに含まれていない場合は、許可されたVLANのリストに自動的に追加されます。 • QinQ トンネリングが有効になっている場合、ネイティブ VLAN と許可 VLAN のプロパティが組み合わされます。
Q-in-Q トンネリングを有効にする	スライドして、VIC QinQ（802.1Qin802.1Q）トンネリングを有効にします。
[許可された VLAN（Allowed VLAN）]	仮想インターフェイスに許可される VLAN を参照します。カンマ区切りの VLAN ID と VLAN ID 範囲のリストを指定することで、許可された VLAN を指定できます。 たとえば、VLAN ID 10、20、30 ～ 40 を入力して VLAN 10、20、30 ～ 40 の範囲を許可できます。 （注） このプロパティは、*[QinQ* トンネリングの有効化（*Enable QinQ Tunneling*）*]* スライダが無効になっている場合にのみ表示されます。
QinQ VLAN	このプロパティにより、QinQ トンネリングの構成が有効になり、単一の VLAN 内の複数の VLAN のカプセル化が容易になります。サポートされる VLAN ID の範囲は 2 ～ 4093 で、ネットワークトラフィックを効果的に管理および分離できます。 （注） このプロパティは、*[QinQ* トンネリングの有効化（*Enable QinQ Tunneling*）*]* スライダが有効になっている場合にのみ使用できます。

（注） サーバーを隔離ホストまたはコミュニティ ホストにするには、許可VLANとネイティブVLANの両方で隔離 VLAN またはコミュニティ VLAN の ID を指定します。

7. **[作成（Create）]** をクリックします。

イーサネット ネットワーク制御ポリシーの作成

UCS ドメインのネットワーク制御設定を設定するイーサネットネットワーク制御ポリシー。このポリシーは、ポート ポリシーで定義されたアプライアンス ポート、および FI 接続された UCS サーバ上の LAN 接続ポリシーで定義された vNIC にのみ適用されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク コントロール（Ethernet Network Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[CDP の有効化（Enable DNS）]	インターフェイスの Cisco Discovery Protocol（CDP）を有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MAC 登録モード（MAC Register Mode）]	スイッチに登録する必要があるMACアドレスを決定します。次のように指定します。 • [ネイティブ VLAN のみ（Only Native VLAN）]：MACアドレスはネイティブVLAN のみに追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。 • [すべてのホスト VLAN（All Host VLANS）]：MAC アドレスは関連付けられたすべての VLAN に追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
[アップリンク障害時の動作（Action on Uplink Fail）]	スイッチがエンドホスト モードのとき、使用可能なアップリンク ポートがないと、インターフェイスがどのように動作するか決定します。 • [リンク ダウン（Link Down）]：スイッチ上でアップリンク接続が失われたときにvNICの動作状態をダウンに変更します。vNIC のファブリック フェールオーバーが有効になります。これがデフォルトのオプションです。 • [警告（Warning）]：使用可能なアップリンク ポートがない場合であっても、サーバ間の接続を維持します。スイッチ上でアップリンク接続が失われたときのファブリック フェールオーバーは無効になります。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MAC セキュリティ（MAC Security）] **[構築（Forge）]**	パケットがサーバからスイッチに送信される場合に、構築されたMACアドレスが許可されるか、または拒否されるかを決定します。次のように指定します。 • **[許可（Allow）]**：すべてのサーバ パケットは、そのパケットと関連付けられているMACアドレスとは無関係に、スイッチで受け入れられます。これがデフォルトのオプションです。 • **[拒否（Deny）]**：最初のパケットがファブリック インターコネクトに送信された後、それ以降のすべてのパケットは、それと同じMACアドレスを使用する必要があります。そうでなかった場合、スイッチによりメッセージなしで拒否されます。実質的に、このオプションによって、関連する vNIC のポート セキュリティが有効になります。
[LLDP]	インターフェイスが LLDP パケットを送受信できるかどうかを決定します。 • インターフェイス上での LLDP パケットの伝送を有効にするには、**[伝送を有効化（Enable Transmit）]** をクリックします。 • インターフェイス上での LLDP パケットの受信を有効にするには、**[受信を有効化（Enable Receive）]** をクリックします。

7. **[作成（Create）]** をクリックします。

SAN 接続ポリシーの作成

ストレージエリア ネットワーク（SAN）接続ポリシーは、ネットワーク ストレージ リソースと、ネットワーク上のサーバとストレージデバイス間の接続を決定します。このポリシーを使用すると、WWPN アドレスプールの指定や、vHBA を追加する静的 WWPN アドレスの指定ができます。同様に、WWNN プールまたはスタティック WWNN アドレスを指定して、サーバが SAN との通信に使用する vHBA を設定できます。

前提条件

SAN 接続ポリシーを作成するには、次のサブ ポリシーが必要です。

- **[ファイバ チャネル ネットワーク ポリシー（Fibre Channel Network Policy）]**：仮想インターフェイスの VSAN ID を設定します。
- **[ファイバ チャネル QoS ポリシー（Fibre Channel QoS Policy）]**：仮想インターフェイスのデータレートを制限し、仮想インターフェイスがサポートするファイバチャネル フレームのペイロード バイトの最大サイズを設定し、サービス クラスを仮想インターフェイスのトラフィックに関連付けます。
- **[ファイバ チャネル アダプタ ポリシー（Fibre Channel Adapter Policy）]**：アダプタのホスト側の動作を制御します。FCP エラー リカバリを有効にし、キューのデフォルト設定を変更し、割り込み処理を変更して、パフォーマンスを強化することができます。
- ファイバー チャネル ゾーン ポリシー - FC ゾーン ポリシーで直接アクセス ストレージ パス構成を指定して、ホストとストレージ デバイス間のアクセス制御を設定します。FC ストレージ範囲が設定された VSAN 上に、単一のイニシエータの単一のターゲット、または単一のイニシエータの複数のターゲット ゾーンを作成できます。
- **[WWWN プール（WWNN Pool）]**：World Wide Name（WWN）プールは、Cisco UCS ドメイン内のファイバ チャネル vHBA で使用される WWN の集合です。Cisco UCS ドメインのファイバ チャネル vHBA にスタティック WWNN を割り当てることもできます。
- **[WPN プール（WPN Pool）]** World Wide Name（WWN）プールは、Cisco UCS ドメイン内のファイバ チャネル vHBA で使用される、WW ポート名だけを含んでいます。Cisco UCS ドメインのファイバ チャネル vHBA にスタティック WWPN を割り当てることもできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SAN 接続（LAN Connectivity）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、以下の情報を設定します。
   - **[名前（Name）]**：ポリシーの名前です。
   - **[ターゲット プラットフォーム（Target Platform）]**： ポリシーが適用されるターゲット プラットフォームです。これは、**[スタンドアロン（Standalone）]** サーバまたは **[FI 接続サーバ（FI Attached）]** サーバのいずれかです。

     スタンドアロン サーバ用に作成された SAN 接続ポリシーは、FI 接続サーバに展開できません。同様に、FI 接続サーバ用に作成された SAN 接続ポリシーは、スタンドアロン サーバには展開できません。

- **[説明（Description）]**：ポリシーの識別に役立つ説明です。
- **[タグ（Tag）]**：ポリシーのタグです。タグはkey：value形式である必要があります。たとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次を設定します。
   - 配置オプションを **[手動（Manual）]** または **[自動（Auto）]** から選択します。
     - **[vHBA の手動配置（Manual vHBAs Placement）]**：このオプションを選択した場合は、各 vHBA の PCI スロットと PCI の順序を手動で指定する必要があります。また、**[グラフィック vHBA エディタ（Graphic vHBAs Editor）]** を使用して、vHBA とスロットを追加し、それらの間の接続を定義することで、各 vHBA の配置を手動で作成および指定することもできます。

（注）
- 手動配置の場合、**[PCI リンク（PCI Link）]** はUCS VIC 1400シリーズアダプタではサポートされません。
- SAN 接続ポリシーに簡易配置と拡張配置の両方がある場合は、サーバー プロファイルの展開の失敗を防ぐために、PCI順序で指定された番号が適切であることを確認してください。

     - **[自動 vHBA の配置（Auto vHBAs Placement）]**：このオプションを選択すると、vHBAの配置はプロファイルの展開時に自動的に行われます。このオプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。

   - **[WWNN アドレス プール（WWNN Address Pool）]** を作成または選択するか、**[静的（Static）]** を選択して WWNN アドレスを入力します。[静的（Static）] オプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。

7. テンプレートを使用せずにvHBAをセットアップするには、**[vHBAの追加（Add vHBA）]** をクリックし以下のパラメータを構成します。

プロパティ（Property）	基本情報（Essential Information）
[vHBA の追加（Add vHBA）]	
[名前（Name）]	仮想ファイバ チャネル インターフェイスの名前。

プロパティ（**Property**）	基本情報（**Essential Information**）
[vHBA タイプ（vHBA Type）]	

プロパティ（**Property**）	基本情報（**Essential Information**）
	SAN 接続ポリシーの vHBA の設定のタイプ。 • **fc-initiator**：vHBA に設定するファイバ チャネル ゾーン分割のタイプは、イニシエータ タイプです。 • **fc-target**：vHBA に設定するファイバ チャネルゾーン分割のタイプはターゲット タイプです。 • **fc-nvme-initiator**：vHBA タイプはイニシエータであり、NVMe インターフェイスをファイバチャネルに適用します。 • **fc-nvme-target**：vHBA タイプはターゲットで、NVMe インターフェイスをファイバ チャネルに適用します。 NVM Express (NVMe) インターフェイスは、不揮発性メモリ サブシステムとの通信にホスト ソフトウェアを使用できます。これは、PCI Express (PCIe) インターフェイスには通常、登録レベル インターフェイスとして一般的に添付されているエンタープライズ不揮発性ストレージに対して最適化されます。 （注） • この構成は、Cisco VIC 1400 シリーズおよび上位シリーズのアダプタでのみサポートされます。 • 1300 シリーズアダプタは、fc-initiator および fc-nvme-initiator のみをサポートします。 • 接続前に、アダプタとの関連付けに問題はありません。 • アダプタとの接続後、vnic.cfg ファイルの vhba_type を確認します。 **fc-nvme-initiator** タイプの場合、vhba_type は名前を読み取る必要があります。

プロパティ（Property）	基本情報（Essential Information）
	fc-initiator タイプの場合、vhba_type は存在しません。
ピングループ名	特定のポート/ポートチャネルを含むピングループの名前。vHBA からのすべてのトラフィックは、指定された FC/FCoE アップリンク ポートまたはポート チャネルにピンされます。 （注） ピングループは、ポートポリシーの作成中に定義できます。 vHBA に対してピン グループが割り当てられていない場合、アップリンク FC/FCoE ポートまたはポート チャネルがサーバーインターフェイスから動的に選択されます。この選択は永続的ではありません。インターフェイス フラップまたはサーバーのリブートの後は、そのサーバーインターフェイスからのトラフィックに対して別の FC/FCoE アップリンク ポートまたはポートチャネルが使用される可能性があります。
[WWPN アドレスプール（WWPN Address Pool）]	**[プールの選択（Select Pool）]** をクリックし、WWPN アドレスプールを選択します。
[静的（Static）]	**[静的（Static）]** をクリックし、スタティック WWPN アドレスを入力します。このオプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。
[配置（Placement）] 仮想インターフェイスの配置の設定。	
Simple 簡易配置を選択すると、スロット ID と PCI Link はシステムによって自動的に決定されます。最初の VIC に nHBA が展開されます。スロット識別子によって最初の VIC が決まります。スロット識別子の番号付けは MLOM で始まり、その後は 1 から始まり、1 ずつ増加し続けます。PCI リンクは常に 0 に設定されます。	
[スイッチ ID（Switch ID）]	vHBA トラフィックを伝送するファブリック インターコネクトを指します。

プロパティ（Property）	基本情報（Essential Information）
[PCI の順序（PCI Order）]	仮想インターフェイスが起動される順序です。インターフェイスに割り当てられる順序は、VIC アダプタの各 PCI リンク上のすべてのイーサネットおよびファイバ チャネルインターフェイスに対して「0」から始めて順に一意である必要があります。PCI順序の最大値は、VIC アダプタの各 PCI リンク上の仮想インターフェイス（イーサネットおよびファイバ チャネル）の数によって制限されます。 （注） 2 つの vHBA の PCI 順序を変更するには、vHBA を削除して再作成する必要があります。
詳細設定	
自動スロット ID 割り当て	有効にすると、スロット ID はシステムによって自動的に決定されます。
[スロット ID（Slot ID）]	自動スロット ID 割り当てが無効になっている場合は、スロット ID を手動で入力する必要があります。 サポートされている値は（1～15）で、MLOM です
PCI リンク 仮想インターフェイスのトランスポートとして使用される PCI リンク。 PCI リンクは、2 つの PCI リンクをサポートする一部の Cisco UCS VIC 1300 シリーズ モデル（UCSC-PCIE-C40Q-03、UCSB-MLOM-40G-03、UCSB-VIC-M83-8P）にのみ適用されます。他の VIC モデルの値が指定されている場合、その値は無視されます。 （注） 両方の PCI リンクを使用すると、ホストデバイスの順序が影響を受ける可能性があります。	

プロパティ（Property）	基本情報（Essential Information）
PCI リンクの自動割り当て	有効にすると、PCI リンクはシステムによって自動的に決定されます。 （注） • スロット ID と PCI リンクの両方で自動割り当てが有効になっている場合、動作は単純な配置と同じです。すべての vHBA は同じ PCI リンク（リンク 0）に配置されます。 • 自動スロット ID 割り当てが無効で、自動 PCI リンク割り当てが有効になっている場合は、スロット ID を指定する必要があり、vHBA は PCI リンク 0 に配置されます。
ロード バランシング	[自動 PCI リンク割り当て（Automatic PCI link Assignment）] が無効で [ロード バランシング（Load Balanced）] が有効になっている場合、システムは PCI リンク全体にインターフェイスを均等に分散します。 • 自動 PCI リンク割り当てが無効で、自動スロット ID が有効になっている場合は、vHBA をロード バランシングする PCI 順序を指定できます。 • 自動 PCI リンク割り当てと自動スロット ID の両方が無効になっている場合は、スロットと PCI 順序を指定して vHBA のロード バランシングを行うことができます。 （注） vHBA を削除して再作成しないと、2 つの vHBA の PCI リンク モードをロードバランシング モードからカスタム モードに変更することはできません。

プロパティ（**Property**）	基本情報（**Essential Information**）
Custom	• 自動 PCI リンク割り当てが無効で、自動スロット ID が有効になっている場合は、PCI 順序、PCI リンク、およびスイッチ ID の値を指定する必要があります。 • 自動 PCI リンク割り当てと自動スロット ID 割り当ての両方が無効になっている場合は、スロット ID、PCI 順序、および PCI リンクの値を指定する必要があります。 （注） vHBA を削除して再作成しない限り、2 つの vHBA の PCI リンク モードをカスタム モードからロードバランシング モードに変更することはできません。
[永続的 LUN バインド（Persistent LUN Bindings）]	
永続的 LUN バインドを有効にします。	手動でクリアするまで、LUN ID アソシエーションをメモリで保存することを可能にします。
[ファイバ チャネルネットワーク（Fibre Channel Network）]	ファイバ チャネル Network ポリシーを選択または作成します。
[ファイバ チャネル QoS（Fibre Channel QoS）]	ファイバ チャネル QoS ポリシーを選択または作成します。
[ファイバチャネルアダプタ（Fibre Channel Adapter）]	ファイバ チャネルアダプタポリシーを選択または作成します。
FC ゾーン	アタッチする FC ゾーン ポリシーを選択または作成します。

8. vHBA テンプレートを使用して FI 接続サーバーの vHBA を取得するには、**[追加（Add）]** ドロップダウン リストから **[テンプレートから vHBA（vHBA from Template）]** を 選択します。vHBA テンプレートの作成の詳細については、「*vNIC* または *vHBA* テンプレートの作成」を参照してください。

（注）
- テンプレートから vHBA を取得する場合、vHBA 設定はテンプレート設定から自動的に入力されます。vHBA テンプレートを使用して設定のオーバーライドが有効になっているパラメータを編集または削除できます。オーバーライドが有効になっていないパラメータの場合は、**[目（Eye）]** アイコンを使用して設定を表示することしかできません。
- オーバーライドされたパラメータは、**[オーバーライド（Overridden）]** ラベルを使用して示されます。オーバーライドが有効なパラメータの場合、テンプレートに適用された変更は、派生 vHBA に反映されません。
- テンプレートに含まれていない派生 vHBA インスタンスでは、これらのパラメータのみを変更できます。
- プロファイルの展開中にテンプレートから vHBA を取得しようとすると、プロファイルの展開が完了するまでタスクが再試行されます。これらの詳細は、**[リクエスト（Requests）]** タブで確認できます。

9. **[作成（Create）]** をクリックします。

ファイバ チャネル アダプタ ポリシーの作成

ファイバ チャネル アダプタ ポリシーは、アダプタのトラフィック処理方法など、ホスト側のアダプタの動作を制御します。FCPエラーの修復の有効化、キューのデフォルト設定の変更、パフォーマンス強化のための割り込み処理を実行できます。

（注） 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。シスコのテクニカル サポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ファイバ チャネル アダプタ（Fibre Channel Adapter）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。
[ファイバチャネルアダプタのデフォルト設定（Fibre Channel Adapter Default Configuration）]	
デフォルト設定を選択します	クリックして、デフォルト設定を表示し、インポートします。ポリシーは現在 9 つのデフォルト設定をサポートしています。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[エラーリカバリ（Error Recovery）]	
[FCP エラーの修復（FCP Error Recovery）]	仮想インターフェイスで FCP Sequence Level Error Recovery プロトコル（FC-TAPE）の使用をイネーブルにします。
[ポートダウンタイムアウト（Port Down Timeout、ミリ秒）]	リモート ファイバチャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。 0 ～ 240000 の整数を入力します。
[I/O 再試行のタイムアウト（I/O Retry Timeout、秒）]	アダプタが、保留中のコマンドを中止して同じI/O リクエストをを再送信する前に待機する秒数。 1 ～ 59 の整数を入力します。
[リンクダウンタイムアウト（Link Down Timeout、ミリ秒）]	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240000 の整数を入力します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ポートダウン IO 再試行回数（Port Down IO Retry、ミリ秒]	ポートが使用不可能であるとシステムが判断する前に、そのポートへの IO 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。
[エラー検出（Error Detection）]	
[エラー検出タイムアウト（Error Detection Timeout）]	エラー検出タイムアウト値。EDTOV とも呼ばれ、システムが、エラーが発生したと見なす前に待機するミリ秒数です。 1000 ～ 10000 の整数を入力します。
[リソース割り当て（Resource Allocation）]	
[リソース割り当てタイムアウト (Resource Allocation Timeout)]	リソースを適切に割り当てることができないと見なす前にシステムが待機するミリ秒数。 5000 ～ 100000 の整数を入力します。
[Flogi]	
[Flogi Retries（Flogi 再試行数）]	システムがファブリックへのログインを最初に失敗してから再試行する回数。
[Flogi タイムアウト（Flogi Timeout, ms、ミリ秒）]	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。
[Plogi]	
[Plogi 再試行回数（Plogi Retries）]	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。
[Plogi タイムアウト（Plogi Timeout、ミリ秒）]	システムがログインを再試行する前に待機するミリ秒数。 1000～255000 の範囲の整数を入力します。
[割り込み（Interrupt ）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[モード（Mode）]	選択優先ドライバ割り込みモードを選択します。 • [MSIx]：機能拡張メッセージ信号割り込み（Message Signaled Interrupts、MSI）。これが推奨オプションです。 • [MSI]：メッセージ信号割り込み（Message Signaled Interrupts、MSI）のみ • [INTx]：PCI INTx 割り込み
[IO スロットル（IO Throttle）]	
[I/O スロットル数（I/O Throttle Count）]	vHBA 内に同時に保留可能な I/O 操作の数。 1 ～ 1024 の整数を入力します。
[LUN]	
[ターゲットあたりの最大 LUN 数（Maximum LUNs Per Target）]	ドライバでエクスポートされる LUN の最大数。通常は、オペレーティング システム プラットフォームの制限です。 1 ～ 1024 の整数を入力します。 fc-initiator vHBA タイプには、1 ～ 4096 の整数を入力します。 （注） fc-initiator vHBA の最大 LUN 構成には、最小のサーバ ファームウェア バージョン 4.2(3d) が必要です。アダプタでサポートされるファームウェアの詳細については、「サポートされるハードウェア」を参照してください。
[LUN キューの深さ（LUN Queue Depth）]	HBA が 1 回の伝送で送受信できる LUN ごとのコマンドの数です。 1 ～ 254 の整数を入力します。
[受信（Receive）]	
[受信リングサイズ（Receive Ring Size）]	各キュー内の記述子の数。 64 ～ 2048 の整数を入力します。
[送信（Transmit）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[送信リング サイズ（Transmit Ring Size）]	各キュー内の記述子の数。 64 ～ 2048 の整数を入力します。
[SCSI I/O]	
[SCSI I/O キュー（SCSI I/O Queues）]	システムで割り当てる SCSI I/O キュー リソースの数。 1 ～ 245 の整数を入力します。
[SCSI I/O のリングサイズ（SCSI I/O Ring Size）]	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。

7. [作成（Create）] をクリックします。

ファイバ チャネル ネットワーク ポリシーの作成

ファイバ チャネル ネットワーク ポリシーは、仮想インターフェイスの仮想ストレージ エリア ネットワーク（VSAN）設定を制御します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [ファイバ チャネル ネットワーク（Fibre Channel Network）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[デフォルトの VLA（Default VLAN）]	スタンドアロン ラック サーバの仮想インターフェイスのデフォルト VLAN です。Value を 0 に設定すると、[なし（None）] と同じ事になり、デフォルトの VLAN は仮想インターフェイス上のトラフィックに関連付けられません。有効な値は 0 ～ 4094 です。
[VSAN ID]	仮想インターフェイスのデフォルトの VSAN ID。ID を 0 に設定すると、デフォルトの VSAN は仮想インターフェイス上のトラフィックに関連付けられません。

7. [作成（Create）] をクリックします。

ファイバチャネル QoS ポリシーの作成

ファイバチャネル QoS ポリシーは vHBA の発信トラフィックにシステムクラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS が決定されます。一部のアダプタでは、発信トラフィックでバーストやレートなどの付加的な制御を指定することもできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [ファイバ チャネル QoS（Fibre Channel QoS）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description）]（オプション）	簡単な説明を入力します。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
レート制限 (Mbps)	仮想インターフェイスでのデータ レートの制限に使用される値。 有効範囲は 0 ～ 100000 です。デフォルト値はゼロです。
最大データ フィールド サイズ (バイト)	仮想インターフェイスがサポートするファイバチャネル フレームのペイロード バイトの最大サイズ。 有効範囲は 256 ～ 2112 です。デフォルト値は 2112 です。
[サービス クラス（Class of Service）]	仮想インターフェイス上のトラフィックに関連付けられるサービス クラス。 有効範囲は 0 ～ 6 です。デフォルト値は 3 です。 （注） • FCoE トラフィックには、他のタイプのトラフィックで使用できない、予約された QoS システム クラスがあります。他のタイプのトラフィックに FCoE で使用される CoS 値がある場合、その値は 0 にリマークされます。 • このプロパティは、スタンドアロン サーバでのみサポートされます。
[バースト（Burst）]	vNIC で許可されるバースト トラフィック（バイト単位）。 有効範囲は 1024 ～ 1000000 です。デフォルト値は 1024 です。 （注） このプロパティは、FI 接続サーバでのみサポートされます。
[優先度（Priority）]	ドメイン プロファイルで定義されたシステム QoS と一致するプライオリティ。**ファイバチャネル（FC）**はデフォルトで有効になっています。 （注） このプロパティは、FI 接続サーバでのみサポートされます。

7. **[作成（Create）]** をクリックします。

FC ゾーンポリシーの作成

このポリシーは、ホストとストレージデバイスの間のアクセス制御をセットアップできるようにします。

FC ゾーン ポリシーを作成する際の注意事項：

- ドメイン プロファイルを使用してストレージ VSAN を初めて展開すると、ファブリック インターコネクトからすべての管理対象外ゾーンがクリアされます。
- ストレージ VSAN を使用した SAN ブート ターゲットには、ファブリック インターコネクトにゾーン エントリがあります。
- ストレージ VSAN を使用した 1 回限りの SAN ブートには、ファブリック インターコネクトにゾーン エントリがあります。
- FC ゾーン ポリシーを編集すると、サーバー プロファイルのステータスが「変更の保留（Pending Changes）」に変更されます。
- ファブリック インターコネクトが再起動されると、構成内のゾーンが再生されます。
- 構成のドリフトの検出は、FC ゾーン ポリシーではサポートされていません。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[FC ゾーン（FC Zone）]**を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（**Property**）	基本情報（**Essential Information**）
FCターゲットゾーン分割タイプ	FC ゾーニングのタイプ。FC ゾーニングのタイプは次のとおりです。 • 単一イニシエータ単一ターゲット（Single Initiator Single Target） • 単一イニシエータ複数ターゲット（Single Initiator Multiple Target） • なし（None） （注） FC ゾーン分割タイプを **[なし（None）]** として選択すると、ターゲットを追加することも、追加された FC ゾーン セットのテーブルを表示することもできません。
ターゲットの追加	クリックして、FC ゾーン ポリシーのターゲットの詳細を追加します。
名前（Name）	FC ゾーン ポリシーの名前。
WWPN	FC ゾーンのメンバーである WWPN。
[スイッチ ID（Switch ID）]	目標の固有識別子スイッチ ID は A または B です。
[VSAN ID]	FC ゾーンが作成される VSAN の一意の識別子。VSAN ID の有効な値は 1 ～ 4093 です。 （注） VSAN ID の範囲は、ドメインに指定された VSAN ポリシーのストレージである必要があります。

7. **[作成（Create）]** をクリックします。

ファームウェア ポリシーの作成

このポリシーにより、ファームウェアのベースラインと比較して、システムに存在するファームウェアを確認できます。ファームウェア ポリシーを使用すると、システムのファームウェアを目的のバージョンに合わせることができるため、ドライブをコンプライアンスに準拠させることができます。

1. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

2. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
Advanced モード	詳細モードを有効にして、ファームウェアのアップグレード中にコンポーネントを除外します。
ドライブの除外	詳細モードを有効にして、ドライブを除外するチェックボックスを選択して、ファームウェアのアップグレードからドライブを除外します。
ストレージコントローラの除外	詳細モードを有効にして、ストレージ コントローラを除外するチェックボックスを選択して、ファームウェア アップグレードからストレージ コントローラを除外します。
サーバ モデル	ファームウェア アップグレードにサーバ ファミリを選択します。[+] をクリックして、サーバ モデルをさらに追加します。 （注） 最大 6 つのサーバ モデルを選択できます。
Firmware Version	サーバをアップグレードするバンドル バージョンを選択します。

3. **[作成（Create）]** をクリックします。

BIOS ポリシーの作成

BIOS ポリシーは、サーバに対する BIOS 設定の構成を自動化します。1 台のサーバまたはサーバ セットのニーズに適合する特定の BIOS 設定のグループを含む、1 つ以上の BIOS ポリシーを作成できます。サーバの BIOS ポリシーを指定しない場合、BIOS 設定はデフォルト値のセット（新品のベア メタル サーバの場合）、あるいは以前に Cisco IMC を使用して設定した値の

セットになります。BIOS ポリシーを指定すると、それまでにサーバに設定されているすべての値はその値に置き換えられます。

すべての BIOS トークンがすべてのサーバに適用可能なわけではありません。サポートされていないトークンがサーバにプッシュされた場合、それらのトークンは無視されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[BIOS]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。
Cisco 提供の BIOS 構成	
[Cisco 提供の構成の選択（Select Cisco Provided Configuration）]（オプション）	[Cisco 提供の構成の選択（**Select Cisco Provided Configuration**）] をクリックして、定義済みの BIOS 構成のいずれかを検索して選択します。 （注） 構成を選択すると、選択した構成の事前定義された値でポリシーが更新されます。**[詳細（Details）]** ページで値を変更することも、ステップ 6 をスキップして、これらの事前定義された値を使用してポリシーの作成に進むこともできます。

6. **[ポリシーの詳細（Policy Details）]** ページで、次の BIOS ポリシー オプションを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[LOM と PCIe スロット（LOM and PCIe Slots）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[ACS 制御 GPU（ACS Control GPU）*-n]* *n*= 1～8	アクセス コントロール サービス（ACS）を使用すると、プロセッサは、GPU の複数のデバイス間のピアツーピア通信を有効または無効にすることができます。
[ACS 制御スロット（ACS Control Slot）*n]* *n*= 11～14	アクセス コントロール サービス（ACS）を使用すると、プロセッサは、制御スロット n の複数のデバイス間のピアツーピア通信を有効または無効にすることができます。
[LOM の CDN サポート（CDN Support for LOM）]	イーサネット ネットワーキング識別子の命名規則を、Consistent Device Naming（CDN）と従来の命名規則のどちらに準拠させるかを指定します。
[LOM ポート（LOM Port）*n* オプション ROM（OptionROM）] *n*= 0～3	オプション ROM が LOM ポート n で使用できるかどうか
[すべてのオンボード LOM ポート（All Onboard LOM Ports）]	すべてのオンボード LOM ポートを有効または無効にするか
[すべての PCIe スロット オプション ROM（All PCIe Slots OptionROM）]	オプション ROM がすべての PCIe スロットで使用可能かどうか
[PCI ROM CLP]	PCI ROM コマンド ライン プロトコル（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。
[PCIe スロット（PCIe Slot）：*n* リンク速度（Link Speed）] *n*= 1～12	このオプションを使用すると、PCIe スロット n に装着されているアダプタカードの最大速度を制限できます。
[スロット（Slot）*n* の状態（state）] *n*= 1～12	PCIe スロット *n* に取り付けられているアダプタ カードの状態。
PCIe スロット: FLOM リンク速度（PCIe Slot:FLOM Link Speed）	このオプションを使用すると、PCIe FLOM スロットに装着されているアダプタ カードの最大速度を制限できます。
[PCIe スロット：フロント NVMe（PCIe Slot:Front Nvme）*n* リンク速度（ Link Speed）] *n*= 1～2	このオプションでは、フロント PCIe スロット *n* に取り付けられた NVMe カードの最高速度を制限することができます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[PCIe スロット：フロント（PCIe Slot:Front）*n* リンク速度（Link Speed）] *n*= 1～2	このオプションでは、フロント PCIe スロット *n* に取り付けられた アダプタ カードの最高速度を制限することができます。
[GPU *n* オプション ROM（OptionROM）] *n*= 1～8	GPU スロット n でオプション ROM を有効にするかどうか設定します。
PCIe Slot:HBA Link Speed	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。
[PCIe スロット：HBA オプション ROM（PCIe Slot:HBA OptionROM）]	HBA スロットでオプション ROM を有効にするかどうか設定します。
PCIe LOM:*n* リンク（Link） *n*= 1～2	LOM ポートでオプション ROM を使用可能にするかどうか設定します。
[スロット メザニンの状態（Slot Mezz state）]	メザニン カード スロットの状態。
PCIe スロット: MLOM リンク速度（PCIe Slot:FLOM Link Speed）	このオプションを使用すると、PCIe スロットに装着されている MLOM アダプタ カードの最大速度を制限できます。
[PCIe スロット MLOM オプション ROM（PCIe Slot MLOM OptionROM）]	MLOM スロットでオプション ROM を有効にするかどうか設定します。
[MRAID リンク速度（MRAID Link Speed）]	このオプションでは、MRAID の最高速度を制限することができます。
[PCIe スロット MRAID オプション ROM（PCIe Slot MLOM OptionROM）]	MRAID ポートでオプション ROM を使用可能にするかどうか設定。
[PCIe スロット N（PCIe Slot N）*n* オプション ROM（OptionROM）] *n*= 1～24	PCIe スロットでオプション ROM を有効にするかどうか設定します。
[RAID リンク速度（MRAID Link Speed）]	このオプションでは、MRAID の最高速度を制限することができます。
[PCIe スロット RAID オプション ROM（PCIe Slot MLOM OptionROM）]	RAID スロットでオプション ROM を有効にするかどうか設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[PCIe スロット：リア NVMe（PCIe Slot:RearNVMe）*n* リンク速度（ Link Speed）] *n*= 1～2	このオプションでは、リア PCIe スロット *n* に取り付けられた NVMe カードの最高速度を制限することができます。
[PCIe スロット：リア NVMe（PCIe Slot:Rear NVME）*n* オプション ROM（OptionRom）] *n*= 1～8	リア NVMe スロット *n* でオプション ROM を有効にするかどうか設定します。
[PCIe スロット：ライザー（PCIe Slot:Riser）*n* リンク速度（Link Speed）] *n*= 1～2	このオプションを使用すると、PCIe スロットに装着されているライザー カード *n* の最大速度を制限できます。
[PCIe スロット：ライザー 1 スロット（PCIe Slot:Riser1 Slot）*n* リンク速度（Link Speed）] *n*= 1～3	このオプションを使用すると、PCIe スロットに装着されているライザー カード 1 のスロット *n* の最大速度を制限できます。
[PCIe スロット：ライザー 1 スロット（PCIe Slot:Riser2 Slot）*n* リンク速度（Link Speed）] *n*= 4～6	このオプションを使用すると、PCIe スロットに装着されているライザー カード 2 のスロット *n* の最大速度を制限できます。
PCIe スロット：SAS オプション ROM（PCIe Slot:SAS OptionROM）	SAS スロットでオプション ROM を有効にするかどうか設定。
[PCIe スロットフロント PCIe（PCIe Slot:FrontPcie）*n* リンク速度（Link Speed）] *n*= 1～2	このオプションでは、フロント PCIe *n* の最高速度を制限することができます。
[プロセッサ（Processor）]	
X2APICオプトアウトフラグ	OS が x2APIC で動作していないときに、OS が拡張 xAPIC（x2APIC）モードを有効にしないようにします。
[隣接キャッシュ行のプリフェッチ（Adjacent Cache Line Prefetcher）]	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか設定します。
[高度（Altitude）]	物理サーバがインストールされている地点のおよその海抜（m 単位）。

[プロパティ（Property）]	[基本情報（Essential Information）]
[自律コア C-state（Autonomous Core C-state）]	オペレーティングシステムが CPU コア C1 状態を要求すると、システムハードウェアは自動的に要求をコア C6 状態に変更します。
[CPU 自律 C-state（CPU Autonomous Cstate）]	HALT 命令を MWAIT 命令に変換する CPU 自律 C-state を有効にします。
[ブート パフォーマンス モード（Boot Performance Mode）]	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。
[ダウンコア制御（Downcore control）]	AMD プロセッサがコアを無効にすることを許可します。つまり、有効にするコア数を選択できます。
[チャネル インターリーブ（Channel Interleaving）]	CPU がメモリ ブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか設定します。
閉ループ サーマル スロットル [（Closed Loop Therm Throt）]	閉ループ サーマル スロットリングのサポートを可能にします。これにより信頼性が向上し、CPU がアイドル状態の間は自動電圧制御により CPU の電力消費が低減します。
[プロセッサ CMCI（Processor CMCI）]	CMCI の生成を有効にします。
[TDP 設定（Config TDP）]	システムの熱設計電力（TDP）を設定できます。TDP は、過熱イベントを引き起こすことなくアプリケーションを実行できる最大電力量です。
[コア マルチ プロセッシング（Core MultiProcessing）]	パッケージ内の CPU ごとの論理プロセッサ コアの状態を設定します。この設定を無効にすると、Intel ハイパー スレッディング テクノロジーも無効になります。
[エネルギー パフォーマンス（Energy Performance）]	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを決定できるようにします。
[周波数フロア オーバーライド（Frequency Floor Override）]	アイドル状態のときに CPU を最大非ターボ周波数未満にすることができるかどうか設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[CPU パフォーマンス プロファイル（CPU Performance）]	サーバの CPU パフォーマンス プロファイルを設定します。
[電源テクノロジー（Power Technology）]	CPU 電源管理設定を指定できます。
[スクラブを要求（Demand Scrub）]	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか設定します。
[ダイレクト キャッシュ アクセスのサポート（Direct Cache Access Support）]	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。
[DRAM クロック スロットリング（DRAM Clock Throttling）]	メモリ帯域幅と消費電力に関してシステム設定を調整できます。
[エネルギー効率ターボ（Energy Efficient Turbo）]	プロセッサがアイドル状態のときに最小パフォーマンス状態に切り替えることができます。
[エネルギー パフォーマンス チューニング（Energy Performance Tuning）]	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。
[拡張 Intel Speedstep テクノロジー（Enhanced Intel Speedstep\（R\) Technology）]	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。
[EPP プロファイル（EPP Profile）]	プロセッサ拡張パフォーマンス プロファイルを決定します。
[ローカル X2 Apic（Local X2 Apic）]	Application Policy Infrastructure Controller（APIC）アーキテクチャ タイプを設定できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ハードウェア プリフェッチ（Hardware Prefetcher）]	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか設定します。
[CPU ハードウェア パワー管理（CPU Hardware Power Management）]	プロセッサの Hardware Power Management（HWPM）を有効にします。
[IMC インターリーブ（IMC Interleaving）]	この BIOS オプションは、Integrated Memory Controller（IMC）間のインターリーブを制御します。
[インテル ハイパースレッディング テクノロジー（Intel HyperThreading Tech）]	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか設定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。
[インテル Speed Select（Intel Speed Select）]	インテル Speed Select テクノロジーを使用して CPU のパフォーマンスを向上させ、論理プロセッサ コア、頻度、および TDP スレッド設定の数に基づいて、3 つの動作プロファイルのいずれかで実行する CPU を調整し、基本プラットフォームのデフォルト設定でパフォーマンスを向上させます。これらのプロファイルは、高、中、および低コア設定に対応します。
[インテル ターボ ブースト テクノロジー（Intel Turbo Boost Tech）]	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか設定します。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。
Intel(R) VT	プロセッサで Intel Virtualization Technology を使用するかどうか設定します。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[IIO エラー有効化（IIO Error Enable）]	IIO 関連のエラーが出力されるようにします。
[DCU IP プリフェッチ（DCU IP Prefetcher）]	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。
[KTI プリフェッチ（XPT Prefetch）]	KTI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。
LLC プリフェッチ（LLC Prefetch）	プロセッサが LLC プリフェッチ メカニズムを使用してデータを LLC にフェッチするかどうか設定します。
[メモリインターリーブ（Memory Interleaving）]	メモリの更新中に別のメモリにアクセスできるように、CPU が物理メモリをインターリーブするかどうか設定します。
[パッケージ C State リミット（Package C State Limit）]	アイドル時にサーバ コンポーネントが使用できる電力量を設定します。
[パトロール スクラブ（Patrol Scrub）]	システムにサーバのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させるかどうか設定します。
[パトロール スクラブ間隔（Patrol Scrub Interval）]	各パトロール スクラブによるメモリ アクセスの時間間隔を制御します。小さくすると、メモリのスクラブ頻度が高くなりますが、必要なメモリ帯域幅も多くなります。 5 ～ 23 の値を選択します。デフォルト値は 8 です。 このオプションは、[パトロール スクラブ（Patrol Scrub）] が有効な場合にのみ使用します。
[プロセッサ C1E（Processor C1E）]	C1 に入ってプロセッサが最低周波数に遷移できるようにします。この設定は、サーバをリブートするまで有効になりません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[プロセッサ C3 レポート（Processor C3 Report）]	BIOS からオペレーティング システムに C3 レポートを送信するかどうかを設定します。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持します。
[プロセッサ C6 レポート（Processor C3 Report）]	BIOS からオペレーティング システムに C6 レポートを送信するかどうかを設定します。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持します。
[CPU C State]	アイドル期間中にシステムが省電力モードに入ることができるかどうか設定します。
[P-State の調整（P-STATE Coordination)]	BIOS がオペレーティング システムに P-state サポート モデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。
[電力パフォーマンス調整（Power Performance Tuning）]	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。
[ランク インターリーブ（Rank Interleaving）]	1 つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか設定します。
[シングル PCTL（Single PCTL）]	プロセッサの電源管理を向上させるために単一 PCTL サポートを促進します。
[SMT モード（SMT Mode）]	プロセッサで AMD 同時マルチスレッディング（Simultaneous MultiThreading）テクノロジーを使用するかどうかを指定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。
[サブ NUMA クラスタリング（Sub Numa Clustering）]	CPU がサブ NUMA クラスタリングをサポートするかどうか設定します。そのクラスタリングでは、タグ ディレクトリとメモリ チャネルは常に同じ領域になります。

[プロパティ（Property）]	[基本情報（Essential Information）]
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）]	プロセッサでDCUストリーマプリフェッチメカニズムを使用して履歴キャッシュ アクセスパターンを分析し、L1キャッシュ内で最も関連性の高い行をプリロードします。
[SVM モード（SMT Mode）]	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか設定します。
[ワークロード設定（Workload Configuration）]	この機能を使用すると、ワークロードを最適化できます。
[XPT プリフェッチ（XPT Prefetch）]	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリコントローラのプリフェッチャに発行するかどうか設定します。
[USB]	
[すべての USB デバイス（All USB Devices）]	すべての物理および仮想 USB デバイスを有効または無効にします。。
[レガシー USB のサポート（Legacy USB Support）]	システムでレガシー USB デバイスをサポートするかどうか設定します。
[デバイスをブート不可にする（Make Device Non Bootable）]	サーバが USB デバイスからブートできるかどうか設定します。
[xHCI モード（xHCI Mode）]	xHCI モードを有効または無効にします。
[ポート 60/40 エミュレーション（Port 60/64 Emulation）]	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか設定します。
[USB ポート フロント（USB Port Front）]	フロントパネルのUSBデバイスを有効または無効にします。
[USB ポート内部（USB Port Internal）]	内部 USB デバイスを有効または無効にします。
[USB ポート KVM（USB Port KVM）]	KVM ポートを有効または無効にします。
[USB ポート リア（USB Port Rear）]	リアパネルのUSBデバイスを有効または無効にします。
[USB ポート SD カード（USB Port SD Card）]	SD カードドライブを有効または無効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[USB ポート VMedia（USB Port VMedia）]	仮想メディア デバイスを有効または無効にします。
[XHCI レガシーサポート（XHCI Legacy Support）]	レガシー xHCI モードを有効または無効にします。
[プロパティ（Property）]	
[ASPM のサポート（ASPM Support）]	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。
[IOH リソースの割り当て（IOH Resource Allocation）]	システム要件に応じて、IOH0 と IOH1 間で 16 ビット I/O リソースの 64 KB を分配できます。
[4 GB 超のメモリマップド IO（Memory mapped IO above 4GB）]	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O を有効または無効にします。レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[MMCFG ベース（MMCFG BASE）]	4GB 以内の PCIe アダプタに下位のベースアドレスを設定します。
[オンボード 10 Gbit LOM（Onboard 10Gbit LOM）]	サーバ上で 10 Gbit LOM を有効または無効にします。
[オンボード Gbit LOM（Onboard Gbit LOM）]	サーバ上で Gbit LOM を有効または無効にします。
[NVMe SSD ホットプラグサポート（NVMe SSD Hot-Plug Support）]	サーバの電源を切らずに NVMe SSD を交換できるようにします。
[SR-IOV のサポート（SR-IOV Support）]	サーバ上で SR-IOV（Single Root I/O Virtualization）を有効または無効にします。
[VGA の優先順位（VGA Priority）]	システムに複数の VGA デバイスがある場合、VGA グラフィックスデバイスの優先順位を設定できるようにします。
[サーバ管理（Server Management）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[PERR 上の NMI アサート（Assert NMI on PERR）]	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうかを設定します。
[SERR 上の NMI アサート（Assert NMI on SERR）]	システムエラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうかを設定します。
[ボー レート（Baud rate）]	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。
[コンシステント デバイス ネーミング（Consistent Device Naming]）	イーサネット ネットワークの命名規則をコンシステントデバイス ネーミング（CDN）または従来の命名規則のどちらに準拠させるかを設定します。
[適応型メモリ トレーニング（Adaptive Memory Training）]	BIOS は CPU/メモリ設定情報と共にメモリ トレーニング結果（最適化されたタイミング/電圧値）を保存し、それらをその後のリブートで使用して、ブート時間を短縮します。保存済みメモリのトレーニング結果は、最後の保存操作後の 24 時間以内に、リブートが発生した場合にのみ使用されます。
[BIOS Techlog レベル（BIOS Techlog Level）]	より細かい出力レベルで BIOS Tech ログ出力を制御します。これにより、冗長であるか、あまり使用しない BIOS Tech ログ メッセージの数が減少します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[オプション ROM 起動最適化（OptionROM Launch Optimization）]	オプション ROM の起動は PCI スロット レベルで管理されます。デフォルトで有効になっています。多数のネットワーク コントローラおよびオプション ROM をもつストレージ HBA から成る設定では、すべてのオプション ROM は、PCI スロットのオプション ROM コントロールがすべてに対して有効になっている場合に起動できます。ただし、ブート プロセスでは、コントローラのサブセットのみを使用できます。このトークンが有効になっているときに、ブートポリシーに存在するこれらのコントローラでのみ、オプション ROM が起動されます。
[コンソールのリダイレクト（Console Redirection）]	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションの関連性はなくなり、無効になります。
[フロー制御（Flow Control）]	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。
[FRB-2 タイマー（FRB-2 Timer）]	POST 中にシステムがハングした場合に、システムを回復するために FRB-2 タイマーを使用するかどうかを設定します。
[レガシー OS リダイレクト（Legacy OS Redirection）]	シリアルポートでのレガシーなオペレーティング システム（DOS など）からのリダイレクションをイネーブルにするかどうか設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[OS ウォッチドッグ タイマー（OS Boot Watchdog Timer）]	BIOSが、定義済みのタイムアウト値を持つウォッチドッグ タイマーをプログラムするかどうか設定します。タイマーが切れる前にオペレーティング システムのブートが完了しなかった場合、CIMC はシステムをリセットし、エラーがログに記録されます。 （注） OSブートウォッチドッグタイマーの値は 5 分を超えてはなりません。
[OS Boot Watchdog Timer Policy	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout]）	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。
[アウトオブバンド管理ポート（Out-of-Band Mgmt Port）]	Windows の Special Administration Control（SAC）で使用。このオプションを使用すると、Windows 緊急管理サービスに使用できる COM ポート 0 を設定できます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。
[Putty キーパッド（Putty KeyPad）]	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。
[BIOS POST 後のリダイレクション（Redirection After BIOS POST]）	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか設定します。
[ターミナル タイプ（Terminal Type)]	コンソール リダイレクションに使用される文字フォーマットのタイプ。
[ブート順序の規則（Boot Order Rules）]	使用可能な特定タイプのデバイスがない場合、またはユーザがサーバの BIOS セットアップユーティリティを使用して異なるブート順序を定義 で定義されたブート順序リストをサーバがどのように変更するかを設定します。
[メモリ（Memory）]	
[BME DMA 緩和（BME DMA Mitigation）]	不正な外部 DMA からの脅威を緩和するため、PCI BME ビットを無効にできます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[IOMMU]	出入力メモリ管理ユニット（IOMMU）により、AMD プロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。
[バンク グループ スワップ（Bank Group Swap）]	物理アドレスをアプリケーションに割り当てる方法を決定します。
[チップ選択インターリーブ（Chipselect Interleaving）]	ノード 0 に選択した DRAM チップ経由でメモリ ブロックがインターリーブされるかどうか設定します。
[メモリ インターリーブ（Memory interleaving）]	メモリの更新中に別のメモリにアクセスできるように、CPU が物理メモリをインターリーブするかどうか設定します。このオプションは、ファブリック レベルでメモリのインターリーブを制御します。チャネル、ダイ、ソケットの要件はメモリによって異なるため、選択したオプションがメモリでサポートされない場合これらは無視されます。
[メモリインターリーブサイズ（Memory interleaving size）]	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。
[DCPMM ファームウェアのダウングレード（DCPMM Firmware Downgrade）]	DCPMM ファームウェアのダウングレードが有効かどうか設定します。
[SMEE]	プロセッサで、メモリの暗号化サポートを実現するセキュア メモリ暗号化有効（SMEE）機能を使用するかどうかを指定します。
[ブート オプション（Boot Options）]	
[試行数（Number of Retries）]	ブートの試行数。
[クール ダウン時間（Cool Down Time（秒）]	次のブートを試行するまで待機する時間（秒単位）。
[ブートオプション再試行（Boot Option Retry）]	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうかを設定します。
[IPV6 PXE サポート（IPV6 PXE Support）]	PXE の IPv6 サポートを有効または無効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[オンボード SCU ストレージのサポート（Onboard SCU Storage Support）]	オンボード ソフトウェア RAID コントローラをサーバで使用できるかどうかを設定します。
[オンボード SCU ストレージ SW スタック（Onboard SCU Storage SW Stack）]	オンボード ソフトウェア スタックをサーバで使用できるかどうかを設定します。
[電源オンパスワード（Power ON Password）]	このトークンでは、F2 BIOS設定を使用する前にBIOSパスワードを設定する必要があります。有効にすると、BIOS関数（IO設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。
[P-SATA モード（P-SATA mode）]	このオプションでは、P-SATAモードを選択できます。
[SATA モード（SATA mode）]	このオプションでは、SATAモードを選択できます。
[VMD 有効化（VMD Enablement）]	PCIeバスに接続されているNVMe SSDをスワップできるかどうかを指定します。この設定により、これらのドライブのLEDステータス ライトも標準化されます。LEDステータス ライトは、特定の障害インジケータ パターンを表示するようにオプションでプログラムできます。
[電源およびパフォーマンス（Power and Performance）]	
[コア パフォーマンス ブースト（Core Performance Boost）]	AMDプロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。
[グローバル C-State 制御（Global C-state Control）]	AMD プロセッサが IO ベースの C-state ジェネレーションおよびDF C-stateを制御するかどうか設定します。
[L1 ストリーミング HW プリフェッチ（L1 Stream HW Prefetcher）]	プロセッサで、AMD ハードウェア プリフェッチ機構が必要に応じてデータおよび命令ストリームをメモリから取得し、L1キャッシュに入れることを許可するかどうか設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[L2 ストリーミング HW プリフェッチ（L2 Stream HW Prefetcher）]	プロセッサで、AMD ハードウェア プリフェッチ機構が必要に応じてデータおよび命令ストリームをメモリから取得し、L2 キャッシュに入れることを許可するかどうか設定します。
[デタミニズム スライダ（Determinism Slider）]	AMD プロセッサに、動作をパフォーマンスとパワー間で切り替えさせるかどうかを指定します。
[cTDP コントロール（cTDP Control）]	熱設計出力（TDP）のカスタマイズされた値を設定できます。
RAS メモリ	
[CKE Low ポリシー（CKE Low Policy）]	DIMM の省電力モード ポリシーを制御します。
[DRAM リフレッシュ レート（DRAM Refresh Rate）]	内部メモリ用のリフレッシュ間隔。
[低電圧 DDR モード（Low Voltage DDR Mode）]	低電圧と高周波数のどちらのメモリ動作をシステムで優先するかを設定します。。
[ミラーリングモード（Mirroring Mode）]	メモリのミラーリングは、メモリに 2 つの同じデータイメージを保存することにより、システムの信頼性を向上させます。 このオプションは、[メモリ RAS 設定（Memory RAS Config）] で [ミラーリング（mirroring）] オプションを選択したときのみ使用可能です。
[NUMA 最適化（NUMA optimized）]	BIOS で NUMA をサポートするかどうか設定します。
[メモリ RAS 設定の選択（Select Memory RAS configuration）]	サーバに対するメモリの RAS（信頼性、可用性、有用性）の設定方法です。

[プロパティ（Property）]	[基本情報（Essential Information）]
[スペアリング モード（Sparing Mode）]	スペアリングはメモリを予備に保持することで信頼性を最適化し、別の DIMM の障害発生時に使用できるようにします。このオプションは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。使用可能なスペアリング モードは、現在のメモリ容量によって異なります。 このオプションは、[メモリ RAS 設定（Memory RAS Config）] で [スペアリング（sparing）] オプションを選択したときのみ使用可能です。
[Intel Directed IO)	
[Intel VT for directed IO]	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか設定します。
[Intel(R) VT-d Coherency サポート（Intel(R) VT-d Coherency Support）]	プロセッサで Intel VT-d Coherency をサポートするかどうか設定します。
[Intel(R) VT-d Interrupt Remapping]	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか設定します。
[Intel(R) VT-d PassThrough DMA サポート (Intel(R) VT-d PassThrough DMA Support)]	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか設定します。
[Intel VTD ATS サポート（Intel VTD ATS support)]	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか設定します。
[メイン（Main）]	
[POST エラーの一時停止（POST Error Pause）]	POST 中にサーバで重大なエラーが発生した場合の処理を設定します。
[QPI]	
[QPI リンクの周波数選択（QPI Link Frequency Select）]	Intel QuickPath Interconnect（QPI）のリンク周波数で、MT/s（毎秒 100 万転送）単位で選択します。
[QPI スヌープモード（QPI Snoop Mode）]	Intel QuickPath インターコネクト（QPI）のスヌープ モードです。
[シリアル ポート（Serial Port）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[シリアル A 有効化（Serial A Enable）]	シリアル ポート A を有効または無効にします。
[信頼できるプラットフォーム（Trusted Platform）]	
[信頼されたプラットフォーム モジュールの状態（Trusted Platform Module State）]	TPM が初期化され、オペレーティングシステムに接続されているかどうかを判断します。
[Intel Trusted Execution Technology のサポート（Intel Trusted Execution Technology Support）]	Intel Trusted Execution Technology（TXT）を使用すると、ビジネスサーバ上で使用され、保管される情報の保護機能が強化されます。このオプションを使用すると、システムの TXT サポートを制御できます。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）]	このトークンを有効にすると、Windows 2022 カーネル DMA 保護機能が有効になります。OS はこれを、悪意のあるデバイスからの DMA 攻撃を防ぐために IOMMU を有効にする必要があるというヒントとして扱います。
セキュリティデバイスのサポート	セキュリティデバイスの BIOS サポートを有効または無効にします。

7. [作成（Create）] をクリックします。

ブート順序ポリシーの作成

[ブート順序ポリシー（Boot Order Policy）] は、デバイスのブート順序を設定します。ブート順序とブート モードの変更を可能にします。さまざまなデバイス タイプに複数のデバイスを追加し、ブート順序を変更し、各ブート デバイス タイプのパラメータを設定することもできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [ブート順序（Boot Order）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

プロパティ（**Property**）	基本情報（**Essential Information**）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（**Property**）	基本情報（**Essential Information**）
ブート モード（BootMode）	有効なブート モードのタイプ。次のいずれかになります。 • **[レガシー（Legacy）]**：マスター ブート レコード（MBR）パーティション スキームを使用します。 システムが UEFI 対応でない場合に選択します。 • **UEFI**：GUID パーティションテーブル（GPT）を使用します。 システムが UEFI 対応の場合に選択します。統合拡張型ファームウェア インターフェイス（Uified Extensible Firmware Interface）の略です。 （注） レガシーブートモードは現在、Cisco UCS C225 M6、C245 M6、C220 M7、C240 M7、および C245 M8 サーバではサポートされていません。
[セキュア ブート モードの有効化（Enable Secure Boot Mode）]	このオプションは、UEFIブート モードが有効になっている場合にのみ使用できます。 セキュア ブートは、相手先商標製品製造会社（OEM）による信頼済みのソフトウェアのみを使用してデバイスブートを実行します。

プロパティ（**Property**）	基本情報（**Essential Information**）
[ブート デバイスの追加（Add Boot Device）]	

プロパティ（Property）	基本情報（Essential Information）
	ブート デバイスを追加して設定する場合に選択します。設定オプションは、ブート デバイスのタイプによって異なります。UCS スタンドアロンおよび FI 接続サーバでサポートされるブート デバイスとその設定オプションを以下に示します。 • **FlexMMC ブート** （注） • FlexMMC ブートは、 C シリーズスタンドアロンサーバーの **UEFI ブート モード** でのみサポートされます。 • セキュア ブート オプションは、FlexMMC でサポートされています。 HTTP ブートのファームウェア要件の詳細については、「HTTP ブート オプションのファームウェア要件」を参照してください。 **設定オプション**： • **[デバイス名（Device Name）]**：デバイスの名前 • **[サブタイプ（Sub-Type）]**：選択したデバイスのサブタイプ。 • なし • FlexMMCマッピングされた DVD • FlexMMCマッピングされた HDD • **HTTP ブート** （注） HTTP/HTTPS ブートは、IMM サーバーと C シリーズ スタンドアロン サーバーの両方で UEFI ブート モードでのみサポートされます。 HTTP ブートのファームウェア要件の詳細については、「HTTP

プロパティ（**Property**）	基本情報（**Essential Information**）
	ブート オプションのファームウェア要件」を参照してください。 **設定オプション**：

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[デバイス名（Device Name）]**：デバイスの名前 • **[IP タイプ（IP Type）]**：HTTP ブートプロセス中に使用する IP アドレス ファミリの種類を指定します。 • **[IP 構成タイプ（IP Config Type）]**：HTTP ブート プロセス中に使用する IP 構成タイプ。 • **DHCP** • （オプション）**URI**：URI 形式のブート技術情報の場所。 （注） URI を入力しない場合は、DHCP がクライアント拡張機能で設定されていることを確認します。 • **インターフェイス名（Interface Name）**（FI接続された）UCS サーバーに対してのみ）(Only for UCS Server (FI-Attached))）]：HTTP ブート デバイスによって使用される基盤となる vNIC の名前。LAN 接続ポリシーを使用して構成された vNIC を選択できます。詳細については、「LAN 接続ポリシー」の項を参照してください。 • **[静的（Static）]** *IP* 構成タイプが静的で *IP* タイプが *IPv4* の場合： • **DNS IP**DNS サーバーの IP アドレス。 • **ゲートウェイ IP**

プロパティ（**Property**）	基本情報（**Essential Information**）
	（**Gateway IP**）：デフォルト ゲートウェイの IP アドレス。 • **静的 IP**：IPv4 または IPv6 の静的インターネット プロトコル アドレス。 • **ネットワーク マスク**（**Network Mask**）：IPv4 アドレスのネットワーク マスク。 • **URI**：URI形式のブート技術情報の場所。 • **インターフェイス名**（**Interface Name**）：HTTP ブート デバイスによって使用される基盤となる vNIC の名前。LAN 接続ポリシーを使用して設定された vNIC を選択できます。 *IP* 構成タイプが静的で *IP* タイプが *IPv6* の場合：

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **DNS IP**DNS サーバーの IP アドレス。 • **ゲートウェイ IP**（**Gateway IP**）：デフォルト ゲートウェイの IP アドレス。 • **静的 IP**：IPv4 または IPv6 の静的インターネット プロトコル アドレス。 • **プレフィックス長**（**Prefix Length**）：IP アドレスをマスクし、IP アドレスをネットワーク アドレスとホスト アドレスに分割するプレフィックス長。 • **URI**：URI形式のブート技術情報の場所。 • **インターフェイス名**（**Interface Name**）：HTTP ブート デバイスによって使用される基盤となる vNIC の名前。LAN 接続ポリシーを使用して設定された vNIC を選択できます。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• プロトコル（**Protocol**）：HTTP ブートに使用されるプロトコル。 HTTPS プロトコルを使用するには、認証用の有効なルートCA証明書が必要です。証明書管理ポリシーを使用してルートCA証明書を展開できます。詳細については、「証明書管理ポリシーの作成」を参照してください。 （注） 証明書管理ポリシーは、単一の証明書の追加、削除、および変更をサポートしていません。いずれかの証明書がポリシーで追加、削除、または変更された場合でも、証明書の変更を有効にするには、サーバープロファイルを再展開するか、サーバーアクションを実行する必要があります。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[インターフェイス ソース（Interface Source）]（C シリーズ スタンドアロン サーバーのみ）**：HTTPデバイスでサポートされているインターフェイス ソースを一覧表示します。 • **インターフェイス名（VIC アダプタのみ）** • **スロット**：基盤となる仮想イーサネット インターフェイスが存在するアダプタのスロットID。 • **インターフェイス名**：HTTPブートデバイスで使用される基盤となる仮想イーサネット インターフェイスの名前。 • **ポート（VIC アダプタのみ）** • **スロット**：基盤となる仮想イーサネット インターフェイスが存在するアダプタのスロットID。 • **スロット**：基盤となる仮想イーサネット インターフェイスが存在するアダプタのポート ID。ポートが指定されていない場合、デフォルト値は -1 です。サポートされる値は 0 ～ 255 です。 • **MAC アドレス（MAC Address）** • **スロット**：基盤となる仮想イーサネット インターフェイスが存在するアダプタのスロット ID。 • **MAC**：HTTP ブートデバイスによって使用される、

プロパティ（**Property**）	基本情報（**Essential Information**）
	基盤となる仮想イーサネット インターフェイスの MAC アドレス。 • **[iSCSI ブート（iSCSI Boot）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[スロット（Slot）]**：ブートデバイスのスロット ID。 • **[ポート（Port）]**：ブートデバイスのポート ID。 device. • **[ローカル CDD（Local CDD）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[ローカル ディスク（Local Disk）]** （注） このデバイスを使用すると、ホストは仮想ドライブをブート可能なデバイスとして使用できます。 • **[デバイス名（Device Name）]**：デバイスの名前 • **[スロット（Slot）]**：ブートデバイスのスロット ID。

プロパティ（**Property**）	基本情報（**Essential Information**）

	• **[NVMe]**
	  • **[デバイス名（Device Name）]**：デバイスの名前
	  • **[ブートローダ名（Bootloader Name）]**：ブートローダ イメージの名前。
	  • **[ブートローダの説明（Bootloader Description）]**：ブートローダの説明。
	  • **[ブートローダ パス（Bootloader Path）]**：ブートローダ イメージのパス名。
	（注） NVMeデバイスは、UEFIモードでのみ構成できます。
	• **[PCH ストレージ（PCH Storage）]**
	  • **[デバイス名（Device Name）]**：デバイスの名前
	  • **[LUN]**：ブート デバイスの論理ユニット番号（LUN）で、0 ～ 255。
	（注） UEFI ブート モードのみがソフトウェア RAID 構成でサポートされています。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[PXE ブート（PXE Boot）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[IP タイプ（IP Type）]**：PXE ブートプロセス中に使用する IP アドレス ファミリの種類を指定します。 • **[スロット（Slot）]**：仮想イーサネット インターフェイスが存在するアダプタのスロット ID。 • **[インターフェイス名/ポート/MAC アドレス（Interface Name/Port/MAC Address）]**：PXE ブートデバイスによって使用される、基盤となる仮想イーサネット インターフェイスの名前またはアドレス。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[SAN ブート（SAN Boot）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[LUN]**：ブート デバイスの論理ユニット番号（LUN）で、0 ～ 255。 • **[スロット（Slot）]**：ブート デバイスのスロット ID。このフィールドは、スタンドアロン サーバにのみ適用されます。 • **[インターフェイス名（Interface Name）]**：基盤となる vHBA インターフェイスの名前。 • **[ターゲット WWPN（Target WWPN）]**：基板となるファイバ チャネル インターフェイスの WWPN アドレス。 • **[ブート ローダ名（Bootloader Name）]**：ブートローダ イメージの名前。このフィールドは、UEFI モードでのみ使用できます。 • **[ブートローダの説明（Bootloader Description）]**：ブートローダ イメージの詳細。このフィールドは、UEFI モードでのみ使用できます。 • **[ブートローダ パス（Bootloader Path）]**：ブートローダ イメージのパス名。このフィールドは、UEFI モードでのみ使用できます。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[SD カード（SD Card）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[LUN]**：ブート デバイスの論理ユニット番号（LUN）で、0 ～ 255。 • **[サブタイプ（Sub-Type）]**：選択したデバイスのサブタイプ。 • [FlexUtil] • [FlexFlash] • [SDCard] • **[UEFI シェル（UEFI Shell）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[USB]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[サブタイプ（Sub-Type）]**：選択したデバイスのサブタイプ。 • [CD] • [FDD] • [HDD]

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[仮想メディア（Virtual Media）]** • **[デバイス名（Device Name）]**：デバイスの名前 • **[サブタイプ（Sub-Type）]**：選択したデバイスのサブタイプ。 • [なし（None）] （注） このオプションは、UCS FI 接続サーバではサポートされていません。 • [CIMC マップされた DVD（CIMC Mapped DVD）] • [CIMC マップされた HDD(CIMC Mapped HDD）] • [KVM マップされた DVD（KVM Mapped DVD）] • [KVM マップされた HDD（KVM Mapped HDD] • [KVM マップされた FDD（KVM Mapped FDD）] （注） ブートデバイスのデバイス名は、以下の制限を満たしていれば、どのような文字列にすることもできます。最初と最後の文字は英数字にする必要があります。アンダースコアとハイフンを含めることができます。30 文字以内である必要があります。

7. **[作成（Create）]** をクリックします。

iSCSI ブート ポリシーの設定

iSCSI ブートのサポートにより、ストレージエリアネットワークを介してリモートディスクからFI接続ブレードおよびラックサーバのオペレーティングシステムを初期化できます。リモー

トディスク（ターゲット）は、TCP / IP および iSCSI ブートファームウェアを使用してアクセスされます。

前提条件

iSCSI ブートデバイスを設定するには、次のものが必要です。

- **iSCSI Static Target Policy**iSCSI スタティックターゲットポリシー：iSCSI ブートポリシーを設定するためのモードとして**[スタティック（Static）]**を選択すると、iSCSI スタティックターゲットポリシーを使用してプライマリターゲットの詳細を指定できます。必要に応じて、セカンダリターゲットの詳細を指定することもできます。
- **[iSCSI アダプタポリシー（iSCSI Adapter Policy）]**：このポリシーを使用して、ブートデバイスの論理ユニット番号がビジーの場合の TCP および DHCP 接続タイムアウトと再試行回数を指定できます。
- **IQN プールの作成**：このポリシーを使用して、ブートデバイスの論理ユニット番号がビジーの場合の TCP および DHCP 接続タイムアウトと再試行回数を指定できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[iSCSI ブート（iSCSI Boot）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
ターゲットインターフェイス ターゲットインターフェイスは [自動（Auto）] または [静的（Static）] です。	

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP ベンダー ID / IQN	ターゲットインターフェイスに **[自動（Auto）]** を選択した場合は、イニシエータ名または DHCP ベンダー ID を指定します。ベンダー ID には、最大 32 文字の英数字を指定できます。
[静的（Static）] ターゲットインターフェイスが**スタティック**の場合は、次のパラメータを指定します。	
主なターゲット	[プライマリターゲット（Primary Target）] ポリシーを選択します。 iSCSI ターゲットは、オペレーティングシステムが初期化されるストレージエリアネットワーク内のリモートディスクです。このポリシーは、ターゲット名、ターゲットの IP アドレス、ポート、および LUN ID を指定します。
セカンダリターゲット	[セカンダリターゲット（Secondary Target）] ポリシーを選択します。セカンダリターゲットはオプションです
アダプタ ポリシー	iSCSI ブートデバイスのアダプタポリシーを選択します。アダプタポリシーは、TCP と DHCP のタイムアウト、および LUN ID がビジーの場合の再試行回数を指定します。
認証 認証方式として **CHAP** または **相互 CHAP** を選択し、パラメータを指定できます。CHAP を選択した場合は、iSCSI ターゲットの CHAP 認証パラメータを指定します。相互 CHAP は双方向 DHCP メカニズムであり、より安全です。	

[プロパティ（Property）]	[基本情報（Essential Information）]
CHAP	CHAP 認証の場合は、次のように入力します。 • **[ユーザ名（Username）]**：イニシエータ/ターゲットインターフェイスのユーザ ID。1 ～ 128 文字の文字、スペース、特殊文字を入力します。 • **[パスワード（Password）]**：イニシエータまたはターゲット インターフェイスのパスワード。12 ～ 16 文字で入力します。スペース、タブ、改行以外の文字を含めます。 • **[パスワードの確認入力（Password Confirmation）]**：入力したパスワードを再入力しますパスワードとパスワードの確認入力は一致する必要があります。
相互 CHAP	相互 CHAP は、双方向 CHAP メカニズムです。相互 CHAP 認証の場合は、次のように入力します。 • **[ユーザ名（Username）]**：イニシエータ/ターゲットインターフェイスのユーザ ID。1 ～ 128 文字の文字、スペース、特殊文字を入力します。 • **[パスワード（Password）]**：イニシエータまたはターゲット インターフェイスのパスワード。12 ～ 16 文字で入力します。スペース、タブ、改行以外の文字を含めます。 • **[パスワードの確認入力（Password Confirmation）]**：入力したパスワードを再入力しますパスワードとパスワードの確認入力は一致する必要があります。

[プロパティ（Property）]	[基本情報（Essential Information）]
[イニシエータ IP ソース（Initiator IP Source）]	イニシエータ IP ソースを決定する方法を選択します。イニシエータ IP ソースを決定する方法は次のとおりです。 • **[プール（Pool）]**: : IP プールを選択できます。 • **[自動（Auto）]** : IP は自動的に決定されます。 • **[静的（Static）** : イニシエータ IP として静的 IP アドレスを指定できます。[静的（Static）] を選択した場合は、次を指定します。 • **[IP アドレス（IP Address）]** : iSCSI イニシエータに提供される静的 IP アドレスを入力します。 • **[サブネット マスク（Subnet Mask）」** : IP アドレスをマスクし、IP アドレスをネットワークアドレスとホストアドレスに分割する 32 ビットの数値を入力します。 • **[デフォルト ゲートウェイ（Default Gateway）]:** デフォルト IPv4 ゲートウェイの IP アドレスを入力します。 • **[Primary DNS（プライマリ DNS）]:** プライマリ ドメイン ネーム システム サーバの IP アドレスを入力します。 • **[セカンダリ DNS（Secondary DNS）]** : セカンダリ ドメイン ネーム システム サーバの IP アドレスを入力します。

7. **[作成（Create）]** をクリックします。

iSCSI アダプタ ポリシーの作成

iSCSIアダプタポリシーは、TCP接続タイムアウト、DHCPタイムアウト、および指定LUN IDがビジーの場合の再試行回数といった値を設定するために使用します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[iSCSI アダプタ（iSCSI Adapter）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[TCP 接続タイムアウト（TCP Connection Timeout）]	TCP 接続がタイムアウトになるまでの時間（秒単位）を入力します。
[DHCP タイムアウト（DHCP Timeout）]	DHCPがタイムアウトになるまでの時間（秒単位）を入力します。
[LUN 再試行回数値（LUN Busy Retry Count）]	LUN IDがビジーのときに接続を試行する回数を入力します。

7. **[作成（Create）]** をクリックします。

iSCSI スタティック ターゲット ポリシーの作成

iSCSI スタティック ターゲット ポリシーでは、iSCSI ブートのプライマリ ターゲットの名前、IP アドレス、ポート、および論理ユニット番号を指定します。オプションで、セカンダリ ターゲットにもこれらの詳細を指定できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[iSCSI 静的ターゲット（iSCSI Static Target）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ターゲット名（Target Name）]	ターゲットの名前を入力します。
[IP アドレス（IP Address）]	ターゲット IP アドレスを入力します。
[ポート（Port）]	ターゲットのポート番号を入力します。
LUN ID	ブート論理ユニット番号の ID を入力します。

7. **[作成（Create）]** をクリックします。

デバイス コネクタ ポリシーの作成

デバイス コネクタ ポリシーによって、**[Intersight のみから設定（Configuration from Intersight only）]** オプションを選択することができ、Cisco IMC に許可される設定変更を制御できます。[Intersight のみから設定（Configuration from Intersight only）] オプションは、デフォルトで有効になっています。Intersight でデバイス コネクタ ポリシーを展開すると、次の変更を確認できるようになります。

- 次の場合は検証タスクが失敗します。
  - Intersight の [読み取り専用（Read-only）] モードが要求済みデバイスで有効になっている場合。
  - Cisco UCS のスタンドアロン C シリーズ サーバーのファームウェアが 4.0(1) よりも前のバージョンの場合。
- Intersight の読み取り専用モードが有効になっている場合は、Intersight から実行された場合にのみファームウェアのアップグレードが成功します。Cisco IMC からローカルで実行されたファームウェア アップグレードは失敗します。
- IPMI over LAN の権限は、[Intersight のみから構成（Configuration from Intersight only）] がデバイス接続ポリシーを介して有効にされたか、または Cisco IMC のデバイス コネクタで同じ構成が有効になっている場合は、読み取り専用レベルにリセットされます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[デバイス コネクタ（Device Connector）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、**[Intersight からの設定のみ（Configuration from Intersight only）]** を有効または無効にします。このオプションは、デフォルトで有効です。
7. **[作成（Create）]** をクリックします。

ドライブ セキュリティ ポリシーの作成

Intersight 管理モードでは、ドライブ セキュリティ ポリシーにより、KMIP サーバの詳細を指定し、ポリシーをサーバ プロファイルに添付できます。

1. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

2. **[ポリシーの詳細（Policy Details）]** ページで、
   1. 切り替えボタンを使用して、プライマリ KMIP サーバを有効にします。
   2. 次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[ホスト名/IP アドレス（Hostname/IP Address）]	使用する KMIP サーバの IP アドレスを入力します。
ポート	KMIP サーバ用のポート番号を入力します。デフォルトのポートは 5696 です。
タイムアウト（Timeout）	KMIP クライアントが接続する必要がある経過時間を入力します。 推奨されるタイムアウト間隔は、最大 65 秒です。

   3. [オプション（Optional）] フォールバック KMIP サーバを構成するには、**セカンダリ KMIP サーバ**の下に追加の KMIP サーバの詳細を追加します。
   4. **[サーバのパブリック ルート CA 証明書（Server Public Root CA Certificate）]** フィールドに、KMIP サーバからのルート証明書をコピーして貼り付けます。

5. [オプション（Optional）] KMIP サーバが認証をサポートしている場合は、セキュリティを強化するために **[認証を有効にする（Enable Authentication）]** オプションをクリックし、ユーザー名とパスワードを入力します。

（注） 認証は、KMIP サーバがサポートしている場合にのみ使用できます。

3. **[作成（Create）]** をクリックします。

新しく作成されたポリシーは、**[ポリシーの詳細（Policy Details）]** ページのテーブル ビューに表示されます。

ディスク グループ ポリシーの作成

ディスク グループ ポリシーは、ディスク グループ（仮想ドライブの作成に使用される物理ディスクのグループ）の作成および構成方法を定義し、ディスク グループに使用される RAID レベルを指定します。このポリシーでは、ディスク グループの一部である必要がある物理ディスクを選択できます。ディスク グループ ポリシーがストレージ ポリシーで複数の仮想ドライブと関連付けられている場合、それらの仮想ドライブは同じディスク グループ スペースを共有します。

（注） このポリシーは、Cisco ブート最適化 M.2 RAID コントローラの仮想ドライブには適用されません。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ディスク グループ（Disk Group）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

[プロパティ（Property）]	[基本情報（Essential Information）]
[説明（Description、オプション）]	簡単な説明を入力します。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[仮想ドライブ設定（Virtual Drive Configuration）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[RAID レベル（RAID Level）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
	データの可用性と冗長性、および I / O パフォーマンスを確保するために、Redundant Array of Inexensive Disks（RAID）レベルを設定します。 ディスク グループでサポートされている RAID レベル: • RAID0：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。 • RAID 1：データが 2 つのディスクに書き込まれ、1つのディスクで障害が発生した場合に完全なデータ冗長性を提供します。最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。 • RAID5：データはアレイのすべてのディスクにストライピングされます。各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。 • RAID 6：アレイのすべてのディスクにデータをストライプ化し、2 つのパリティ データ セットを使用して、最大 2 台の物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。 • RAID 10：この RAID は、ミラー化されたディスクのペアを使用して、完全なデータ冗長性を提供し、ブロック レベル ストライピングによって高いスループット レートを実現します。RAID 10 は、パリティおよびブロック レベルのストライピングを使用しないミラーリ

[プロパティ（Property）]	[基本情報（Essential Information）]
	ングを行います。RAID 10 には 4 台以上のディスクが必要です。 • RAID 50：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。 • RAID 60：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。
[ローカル ディスク構成（Local Disk Configuration）-ディスク グループ（スパン 0）（Disk Group（Span 0））]	
[ドライブ番号（Drive Number）]	RAID コントローラに関連付けられたディスク グループのドライブ番号を指定します。
[専用ホットスペア（Dedicated Hot Spares）]	
[専用ホットスペア（Dedicated Hot Spares）]	ディスク グループでディスク障害が発生した場合にホットスペア ドライブを使用するには、**[有効（Enable）]** を選択します。
[ドライブ番号（Drive Number）]	ディスク グループの専用ホット スペアとして機能するドライブ数を指定します。
[JBOD 状態のディスクを未構成で良好に設定（Set Disks in JBOD state to Unconfigured good）]	ユーザが JBOD 内の任意のディスクを RAID グループで使用できるように未設定の正常なディスクに変換できるようにする場合に選択します。

注目 ディスク グループ内のすべての仮想ドライブは、同じ 1 つのディスク グループ ポリシーを使用して管理する必要があります。

7. **[作成（Create）]** をクリックします。

IMC アクセス ポリシーの作成

IMC アクセス ポリシーを使用すると、ネットワークを構成し、IP プールからの IP アドレスをサーバに関連付けることができます。インバンド IP アドレス、アウトオブバンド IP アドレス、またはインバンドとアウトオブバンドの両方の IP アドレスは、IMC アクセスポリシーを

使用して設定でき、ドライブ セキュリティ、SNMP、Syslog、および vMedia ポリシーでサポートされます。

（注）
- SNMP ポリシーのアウトオブバンド IP アドレスのサポートは、インフラストラクチャ ファームウェア 4.3(2.230129) 以降のバージョンで実行されているファブリック インターコネクトでのみ使用できます。
- SNMP ポリシーのアウトオブバンド IPアドレスのサポートは、Cisco UCS X シリーズ ダイレクト システムのサーバーでは使用できません。
- 分離レイヤ 2 ルールは、同じシャーシ内のブレードで設定されたインバンド VLAN に適用されます。VLAN が同じ分離グループに属し、同じアップリンクで許可されている場合、同じシャーシ内のブレードに複数のインバンド VLAN を設定できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[IMC アクセス（IMC Access）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）		基本情報（Essential Information）
[インバンド設定（In-Band Configuration）]	有効にすると、アップリンク ポートを使用してサーバー管理サービスを使用できるようになります。	
	[VLAN ID]	入力インバンドネットワークを介したサーバアクセスに使用される VLAN ID を入力します。フィールド値は 4ー4093 です。
	IPv4 アドレス設定	このポリシーのネットワークのタイプを決定する場合に選択します。 （注） IPv4 アドレス設定のみ、または IPv4 と IPv6 の両方の設定を選択できます。
	IPv6 アドレス設定	このポリシーのネットワークのタイプを決定する場合に選択します。 （注） IPv6 アドレス設定のみ、または IPv4 と IPv6 の両方の設定を選択できます。
	IP プール	
	IP プールの選択	クリックして使用可能な IP プールのリストを表示し、インバンド構成用の IP プールを選択します。 （注） IMC アクセス ポリシーに使用される IP プールで、指定されたデフォルト ゲートウェイに Cisco IMC への接続があることを確認します。詳細については、「*IP* プールの作成」セクションを参照してください。

プロパティ（Property）		基本情報（Essential Information）
アウトオブバンド設定	有効にすると、管理ポートを使用してサーバー管理サービスを使用できるようになります。	
	IP プール	
	IP プールの選択	クリックして使用可能な IP プールのリストを表示し、アウトオブバンド構成用の IP プールを選択します。 （注） アウトオブバンド構成では、IPv4 アドレスのみがサポートされています。

IPMI Over LAN ポリシーの作成

IPMI Over LAN ポリシーは、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイス用のプロトコルを定義します。Intelligent Platform Management Interface（IPMI）を使用すると、オペレーティング システムはシステムの正常性と制御システムのハードウェアに関する情報を取得し、適切なアクションを実行するよう Cisco IMC に指示します。IPMI メッセージを管理するための IPMI Over LAN ポリシーは、Cisco Intersight で作成できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[IPMI オーバー LAN（IPMI Over LAN）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[IPMI Over LAN の有効化（Enable IPMI Over LAN）]	エンドポイントでの IPMI Over LAN サービスの状態。
[権限レベル（Privilege Level）]	サーバ上の IPMI セッションに次の権限を割り当てることができます。 • 管理者：「管理者」ユーザ ロールにより、サーバ上で管理者、ユーザ、および読み取り専用セッションを作成できます。 • 読み取り専用：「読み取り専用」ユーザ ロールにより、サーバで読み取り専用 IPMI セッションのみを作成できます。 • ユーザ：「ユーザ」ロールでは、サーバでユーザ セッションと読み取り専用セッションを作成できますが、管理者セッションは作成できません。 （注） • この構成は、Cisco UCS C シリーズ スタンドアロンおよび C シリーズ Intersight 管理モード サーバでのみサポートされます。 • [権限レベル（Privilege Level）] フィールドの値は、ログインを試行するユーザーに割り当てられているロールと正確に一致している必要があります。たとえば、このフィールドを読み取り専用に設定した場合、管理者ロールを持つユーザーが IPMI を使用してログインを試みても、ログインできません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[暗号化キー（Encryption Key）]	IPMI通信に使用する暗号キー。偶数桁の 16 進数を含めます。40 文字を超えないようにする必要があります。「00」を使用して、暗号化キーの使用を無効にすることができます。指定された暗号化キーが 40 文字未満の場合、IPMI コマンドは暗号化キーにゼロを追加して、40 文字の長さにする必要があります。 （注） この暗号化キー構成は、Cisco UCS C シリーズ スタンドアロンおよびC シリーズ Intersight 管理モード サーバでのみサポートされます。Intersight 管理モードサーバでこの構成をサポートするには、最小ファームウェア バージョン 4.2(3a) が必要です。

7. **[作成（Create）]** をクリックします。

LDAP ポリシーの作成

Lightweight Directory Access Protocol（LDAP）は、ネットワークでディレクトリ情報を保管し、保守します。シスコ IMC で LDAP が有効になっている場合、ユーザ アカウントがローカル ユーザ データベース内に見つからないと、そのユーザ認証とロール許可はLDAP サーバによって実行されます。LDAP を有効にして設定し、LDAP サーバと LDAP グループを設定できます。

（注） このポリシーは、Intersight Managed FI が接続された UCS サーバに割り当てられているサーバ プロファイルに適用されている場合、無視されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[LDAP]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[LDAP の有効化（Enable DHCP）]	エンドポイントでのLDAPサービスの状態。
[基本設定（Base Settings）]	
[ベース DN（Base DN）]	ベース識別名。このフィールドは、ユーザーおよびグループのロード元を示します。 Active Directory サーバーでは、これは dc=domain,dc=com という形式でなければなりません。
[ドメイン（Domain）」	すべてのユーザーが属する必要のある IPv4 ドメイン。 グローバル カタログ サーバーのアドレスを少なくとも 1 つ指定していない限り、このフィールドは必須です。
[タイムアウト（Timeout）]	LDAP 検索操作がタイムアウトするまで Intersight が待機する秒数。 検索操作がタイムアウトになった場合、Intersight はこのタブで次にリストされているサーバ（存在する場合）への接続を試行します。 （注） このフィールドに指定する値は、全体的な時間に影響を及ぼす可能性があります。
[暗号化の有効化（Enable Encryption）]	これを有効にした場合、サーバはLDAPサーバに送るすべての情報を暗号化します。
[バインド パラメータ（Binding Parameters）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[バインドメソッド（Bind Method）]	次のいずれかを指定できます。 [匿名（Anonymous）]：ユーザ名とパスワードを NULL にする必要があります。このオプションが選択され、LDAP サーバで匿名ログインが設定されている場合は、ユーザがアクセスできます。 [設定済みクレデンシャル（Configured Credentials）]：初期バインドプロセスで既知のクレデンシャル セットを指定する必要があります。初期バインド プロセスが成功した場合、ユーザ名の識別名（DN）が照会されて、その DN が再バインディング プロセスで再利用されます。再バインド プロセスが失敗すると、ユーザはアクセスを拒否されます。 [ログイン クレデンシャル（Login Credentials）]：ユーザ クレデンシャルが必要です。バインド プロセスが失敗すると、ユーザーはアクセスを拒否されます。デフォルトでは、[ログイン クレデンシャル（Login Credentials）] オプションが選択されます。
[バインド DN（Bind DN）]	ユーザーの識別名（DN）。このフィールドは、バインディング方式として [設定済みクレデンシャル（Configured Credentials）] オプションを選択した場合にのみ編集可能になります。
[バインドパスワード（Bind Password）]	ユーザーのパスワード。このフィールドは、バインディング方式として [Configured Credentials] オプションを選択した場合にのみ編集可能になります。
[検索パラメータ（Search Parameters）]	
[フィルタ（Filter）]	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致している必要があります。 デフォルトでは、このフィールドには sAMAccountName と表示されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[グループ属性（Group Attribute）]	このフィールドは、LDAPサーバ上のスキーマの設定済み属性に一致している必要があります。 デフォルトでは、このフィールドにはmemberOfと表示されます。
[属性（Attribute）]	ユーザのロールとロケール情報を保持するLDAP属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP属性では、Cisco IMCユーザ ロールおよびロケールにマップされる既存のLDAP属性を使用することも、スキーマを変更して新しいLDAP属性を作成することもできます。（たとえばCiscoAvPairなど）。 （注） このプロパティを指定しない場合、ユーザーはログインできません。オブジェクトはLDAPサーバー上に存在していますが、このフィールドで指定される属性と正確に一致する必要があります。
[グループ認証（Group Authorization）]	
[グループ認証（Group Authorization）]	これを選択した場合、ローカル ユーザ データベースにないLDAPユーザに関しても、グループ レベルでユーザ認証が実行されます。
[検索するグループのネスト レベル（Nested Group Search Depth）]	LDAPグループ マップで別の定義済みグループ内にネストされたLDAPグループを検索するパラメータ。このパラメータでは、ネストされたグループ検索の深さを定義します。
LDAP サーバの設定	
[DNS の有効化（Enable DNS）]	これを選択した場合、DNSを使ってLDAPサーバへのアクセスを設定できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ソース（Source）]	DNS SRV 要求に使われるドメイン名を取得する方法を指定します。次のいずれかを指定できます。 • [抽出済み（Extracted）]：ログイン ID からのドメイン名抽出ドメインを使用することを指定します。 • [設定済み（Configured）]：設定された検索ドメインを使用することを指定します。 • [設定済み - 抽出済み（Configured-Extracted）]：設定された検索ドメインよりも、ログイン ID から抽出されるドメイン名を優先することを指定します。
[サーバ（Server）]	LDAP サーバの IP アドレスまたはホスト名。
[ポート（Port）]	LDAP サーバのポート番号。
[ユーザ検索の優先順位（User Search Precedence）]	ローカル ユーザ データベースと LDAP ユーザ データベースの間の検索の順序を指定できます。次のいずれかになります。 • [ローカル ユーザ データベース（Local User Database）]（デフォルト設定） • [LDAP ユーザ データベース（LDAP User Database）]
[新しい LDAP グループの追加（Add New LDAP Group）]	
[名前（Name）]	サーバへのアクセスが許可された LDAP サーバ データベース内のグループの名前。
[ドメイン（Domain）」	グループを所属させる LDAP サーバ ドメイン。

[プロパティ（Property）]	[基本情報（Essential Information）]

[ロール（Role）]	すべてのユーザーに割り当てられているこの LDAP サーバー グループのロール。次のいずれかになります。
	• [読み取りのみ（read-only）]：このロールのユーザは情報を表示できますが、変更することはできません。
	• [ユーザ（user）]：このロールのユーザは、次のタスクを実行できます。
	  • すべての情報を表示する
	  • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する
	  • KVM コンソールと仮想メディアを起動する
	  • すべてのログをクリアする
	  • ロケータ LED の点灯・消灯（リモート作業者に場所を示す）
	  • タイムゾーンの設定
	  • ping
	• [管理者（admin）]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。

[ポート（Port）]	LDAP サーバのポート番号。
[ユーザ検索の優先順位（User Search Precedence）]	ローカル ユーザ データベースと LDAP ユーザ データベースの間の検索の順序を指定できます。次のいずれかになります。 • [ローカル ユーザ データベース（Local User Database）]（デフォルト設定） • [LDAP ユーザ データベース（LDAP User Database）]

7. [作成（Create）] をクリックします。

ローカル ユーザ ポリシーの作成

ローカル ユーザ ポリシーは、ローカル ユーザ設定の構成を自動化します。設定する必要があるローカル ユーザのリストを含む、1 つ以上のローカル ユーザ ポリシーを作成できます。

（注） デフォルトでは、IPMI サポートはすべてのユーザーに対して有効になっています

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ローカル ユーザー（Local User）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[パスワードプロパティ (Password Properties)]	パスワードプロパティはラックサーバにのみ適用され、ブレードサーバには適用されません。
[強力なパスワードの適用（Enforce Strong Password）]	強力なパスワードポリシーを有効にします。
パスワードの変更	既存のパスワードの変更を有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[パスワード有効期限の有効化（Enable Password Expiry）]	エンドポイントのパスワード有効期限を有効にします。 （注） 管理者により一度設定されたパスワード有効期限は、その後に作成されるすべてのユーザに適用されます。有効な [パスワードの有効期間（Password Expiry Duration）] は、[通知期間（Notification Period）] および [猶予期間（Grace Period）] より長い必要があります。そうでない場合、[ユーザ パスワードの有効期限ポリシーの設定エラー（User Password Expiry Policy configuration error）] が表示されます。
[パスワードの有効期間（Password Expiry Duration）]	既存のパスワードに設定できる有効期間（その時間以後、新しいパスワードを設定するか、または既存のパスワードを変更します）。範囲は 1 ～ 3650 日です。
[通知期間（Notification Period）]	パスワードの期限が切れる時間を通知します。0 日から 15 日までの値を入力します。0 を入力すると、このフィールドが無効になります。
[猶予期間（Grace Period）]	既存のパスワードをまだ使用できる期間。この期間の後、パスワードは期限切れになります。0 日から 5 日までの値を入力します。0 を入力すると、このフィールドが無効になります。
[パスワード履歴（Password History）]	パスワードが入力された回数。このフィールドを有効にすると、指定された回数を超えてパスワードを繰り返し使用することができなくなります。0 ～ 5 の間の値を入力します。0 を入力すると、このフィールドが無効になります。

[プロパティ（Property）]	[基本情報（Essential Information）]
[常にユーザパスワードを送信（Always Send User Password）]	有効にすると、ユーザパスワードは常にエンドポイントデバイスに送信されます。有効にしていない状態では、ユーザ パスワードがエンドポイント デバイスに送信されるのは、ユーザが新規作成された場合、および既存のユーザのパスワードが変更された場合になります。
[新規ユーザを追加（Add New User）]	
有効	エンドポイントでユーザーアカウントを有効にします。
[新規ユーザ（New User）]	新しいユーザ設定を有効にします。
[ユーザ名（Username）]	ユーザーのユーザー名。 1 ～ 16 文字の範囲で入力します。

[ロール（Role）]	エンドポイントのユーザに関連付けられているロール。
	• **[read-only]**：このロールのユーザは情報を表示できますが、変更することはできません。
	• **[user]**：ユーザロールタイプはラックでのみサポートされます。このロールのユーザは、次のタスクを実行できます。
	  • すべての情報を表示する
	  • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する
	  • KVM コンソールと仮想メディアを起動する
	  • すべてのログをクリアする
	  • ping
	• [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。

[プロパティ（Property）]	[基本情報（Essential Information）]

Password	このユーザー名のパスワード。このフィールドの横にあるヘルプ アイコン上にマウスを移動すると、パスワード設定に関する以下のガイドラインが表示されます。
	• パスワードは 8 ～ 20 文字とすること。これは Intersight プラットフォームの制限です。
	• パスワードにユーザ名を含めないこと。
	• パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。
	  • 英大文字（A から Z まで）。
	  • 英小文字（a から z まで）。
	  • 10 進数の数字（0 ～ 9）。
	  • アルファベット以外の文字（!、@、#、$、%、^、&、*、-、_、=、'）。
	
	これらのルールは、セキュリティ上の理由からユーザーに強力なパスワードを定義するように意図されています。ただし、これらのガイドラインを無視して希望するパスワードを設定する場合は**[強力なパスワードの無効化（Disable Strong Password）]** ボタン（、**[ローカル ユーザ（Local Users）]** タブ）をクリックします。強力なパスワードのオプションが無効になっている場合にパスワードを設定する場合、1 文字以上、20 文字以下のものを使用できます。
	（注） ポリシーを編集することで、ローカルユーザーポリシーのパスワードを変更できます。ただし、ポリシーが展開されると、パスワードの変更オプションは無効になります。

パスワードの確認入力	確認のためのパスワードの再入力。

7. **[作成（Create）]** をクリックします。

NTP ポリシの作成

NTP ポリシーは、Cisco Intersight によって管理される UCS システムが NTP サーバの時刻と同期するように設定するために、NTP サービスを有効にします。NTP サービスを有効化するには、NTP サーバとして動作する 1 ～ 4 台のサーバの IP/DNS アドレスを指定する必要があります。NTP サービスを有効にすると、Cisco Intersight によりエンドポイント側で NTP の詳細が設定されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[NTP]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[Enable NTP]	NTP ポリシー設定をイネーブルにします。
NTP サーバ （NTP Servers）	NTP サーバの IP アドレスまたはホスト名のコレクション。
[タイム ゾーン（Time Zone）]	エンドポイントのタイムゾーンを選択できるタイムゾーンのコレクション。 このプロパティは、スイッチおよび Cisco IMC（スタンドアロン）サーバに適用されます。

NTP の設定にホスト名を使用する場合は、ネットワーク接続ポリシーで DNS サーバ情報を設定する必要があります。

7. **[作成（Create）]** をクリックします。

SD カード ポリシーの作成

Cisco Intersight の SD カード ポリシーは、Cisco Intersight が管理するファブリック インターコネクト ドメイン内にある、Cisco UCS C シリーズ スタンドアロン M4、M5 サーバ、および Cisco UCS C シリーズ M5 サーバの Cisco FlexFlash と FlexUtil セキュアデジタル（SD）カードを設定します。このポリシーは、SD カードの仮想ドライブの詳細を指定します。SD カードは、オペレーティングシステムのみ、ユーティリティのみ、またはオペレーティングシステム+ユーティリティのモードで設定できます。

Cisco FlexFlash コントローラに 2 つのカードがあり、SD カードポリシーでオペレーティングシステムが選択されている場合、設定された OS パーティションがミラーリングされます。Cisco FlexFlash コントローラで使用できるカードが 1 つだけの場合、設定されている OS パーティションは非 RAID です。ユーティリティパーティションは常に非 RAID として設定されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SD カード（SD Card）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[オペレーティングシステムのみ（Operating System Only）]	
[オペレーティング システム（Operating System）]	オペレーティングシステムパーティションを有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[オペレーティングシステムパーティション名（Operating System Partition Name）]	オペレーティングシステムパーティションの名前。
[ユーティリティのみ（Utility Only）]	
[診断（Diagnostics）]	オペレーティングシステムのヘルス診断ユーティリティを有効にします。
[ドライバ（Drivers）]	仮想ドライバユーティリティを有効にします。
[ホスト アップグレード ユーティリティ（Host Upgrade Utility）]	ホスト アップグレード ユーティリティ（HUU）を有効にします。
[サーバ設定ユーティリティ （Server Configuration Utility）]	サーバ設定ユーティリティ（SCU）を有効にします。
[ユーザパーティション（User Partition）]	ユーザパーティションを有効にします。
[ユーザパーティション名（User Partition Name）]	ユーザパーティション名。
[オペレーティングシステムとユーティリティ（Operating System + Utility）]	
[診断（Diagnostics）]	オペレーティングシステムのヘルス診断ユーティリティを有効にします。
[ドライバ（Drivers）]	仮想ドライバユーティリティを有効にします。
[ホスト アップグレード ユーティリティ（Host Upgrade Utility）]	ホスト アップグレード ユーティリティ（HUU）を有効にします。
[サーバ設定ユーティリティ （Server Configuration Utility）]	サーバ設定ユーティリティ（SCU）を有効にします。
[ユーザパーティション（User Partition）]	ユーザパーティションを有効にします。
[ユーザパーティション名（User Partition Name）]	ユーザパーティション名。
[オペレーティングシステムパーティション（Operating System Partition）]	オペレーティングシステムパーティションを有効にします。
[オペレーティングシステムパーティション名（Operating System Partition Name）]	オペレーティングシステムパーティションの名前。

7. **[作成（Create）]** をクリックします。

例外

- **SD カードポリシーは M6 サーバではサポートされていません。**
- SD カードがサーバに存在しない場合には、SD カードポリシーがサーバ プロファイルとともにインポートされることはありません。
- 診断は M5 シリーズのみに適用されます。
- オペレーティングシステム+ユーティリティモードの場合、M5 サーバには少なくとも 1 つの FlexFlash + 1 つの FlexUtil カードが必要です。

Serial over LAN ポリシーの作成

Serial over LAN ポリシーを使用すると、管理対象システムのシリアルポートの入出力を IP 経由でリダイレクトできます。サーバ/サーバ群のニーズを条件に特定の Serial over LAN 属性を分類する Serial over LAN ポリシーを 1 つ以上作成できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[シリアル オーバー LAN（Serial Over LAN）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[Serial over LAN を有効にする（Enable Serial Over LAN）]	エンドポイントでの Serial Over LAN サービスの状態。

[プロパティ（Property）]	[基本情報（Essential Information）]
[COM ポート（COM Port）]	システムが Serial over LAN 通信のルーティングに使用するシリアル ポート。 • **[com0]**：SoL 通信は、外部デバイスへの物理 RJ45 接続またはネットワーク デバイスへの仮想 SoL 接続をサポートする、外部からアクセス可能なシリアル ポートである COM ポート 0 を介してルーティングされます。 このオプションを選択すると、システムは、SoL を有効にして、RJ45 接続を無効にします。これは、サーバが外部シリアル デバイスをサポートできなくなることを意味します。 • **[com1]**：SoL 通信は COM ポート 1 経由でルーティングされます。このポートは、SoL のみを介してアクセスできる内部ポートです。 このオプションを選択した場合、COM ポート 1 上の SoL および COM ポート 0 上の物理 RJ45 接続を使用できます。 （注） • これは、Cisco UCS C シリーズ スタンドアロン サーバにのみ適用されます。 • シリアルポートは、一部の Cisco UCS C シリーズサーバでのみ使用できます。利用できない場合、サーバはデフォルトで COM ポート 0 を使用します。COM ポートの設定を変更すると、既存のすべての SoL セッションが切断されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ボーレート（Baud Rate）]	Serial Over LAN 通信に適用されるボーレート。レートは次のいずれかになります。 • **[9600 bps]** • **[19.2 kbps]** • **[38.4 kbps]** • **[57.6 kbps]** • **[115.2 kbps]** （注） • このボーレートは、サーバのシリアル コンソールで設定したボーレートと一致する必要があります。 • Cisco UCS X シリーズ ダイレクトのボーレートは 115.2 kbps です。
[SSH ポート（SSH Port）]	Serial over LAN への直接アクセスに使用される SSH ポート。Cisco IMC シェルをバイパスして Serial over LAN に直接アクセスできるようにします。 有効な範囲は 1024 ～ 65535 です。デフォルト値は 2400 です。 （注） • これは、Cisco UCS C シリーズ スタンドアロンサーバにのみ適用されます。 • SSH ポートの設定を変更すると、既存のすべての SSH セッションが切断されます。

7. **[作成（Create）]** をクリックします。

SSH ポリシーの作成

[SSH ポリシー（SSH Policy）] は、SSH クライアントを有効にし、暗号化されたセキュアな接続を確立します。サーバ/サーバ群の SSH プロパティの分類方法を含む SSH ポリシーを 1 つ以上作成できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SSH]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SSH ポリシーの有効化（Enable SSH Policy）]	SSH を有効にします。
[SSH ポート（SSH Port）]	セキュア シェル アクセスで使用するポート。
[SSH タイムアウト（SSH Timeout）（秒）]	SSH 要求がタイムアウトしたものとシステムが判断するまでの待機秒数。 60 ～ 10,800 の範囲の整数を入力します。デフォルトは 1,800 秒です。

7. **[作成（Create）]** をクリックします。

仮想 KVM ポリシーの作成

KVM コンソールは、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレート可能なインターフェイスです。これにより、リモート ロケーションからサーバーを制御し、この KVM セッション中にサーバーからアクセスできる仮想ドライブに物理ロケーションをマッピングすることができます。

仮想 KVM プロパティを特定のグループとしてまとめることができます。このポリシーにより、許可される同時 KVM セッション、ポート情報、およびビデオ暗号化オプションを指定できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[仮想 KVM（Virtual KVM）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[仮想 KVM の有効化（Enable Virtual KVM）]	エンドポイントでのvKVMサービスの状態。
[最大セッション数（Max Sessions）]	許可されているKVMの同時セッションの最大数。
[リモート ポート（Remote Port）]	リモートKVM通信に使用するポート。ポートの範囲は 1024ー49151 です。デフォルトは 2068 です。
[ビデオ暗号化の有効化（Enable Video Encryption）]	KVMを介して送信されるすべてのビデオ情報を暗号化します。ビデオ暗号化はデフォルトで有効です。 （注） ファームウェアバージョン4.2（1a）以降では、この暗号化パラメータは廃止されました。暗号化を無効にすると、サーバプロファイルの展開中に検証が失敗します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ローカル サーバ ビデオの有効化（Enable Local Server Video）]	オンにすると、KVMセッションはサーバに接続されているすべてのモニタに表示されます。 （注） これは、Cisco UCS C シリーズ スタンドアロン サーバにのみ適用されます。
[トンネル化 vKVM の許可（Allow Tunneled vKVM）]	エンドポイントでトンネリングされたvKVMを許可するには、これを有効にします。 （注） トンネルvKVMをサポートするデバイス コネクタにのみ適用されます。

7. **[作成（Create）]** をクリックします。

例外

- 仮想メディア ビューアには KVM を使用してアクセスします。KVM コンソールを無効にすると、Cisco IMC はホストに接続されているすべての仮想メディア デバイスへのアクセスも無効にします。
- KVM仮想メディア（vMedia）セッションがマッピングされた後、KVM管理ポリシーを変更すると、仮想メディア（vMedia）セッションは失われます。KVM仮想メディア（vMedia）セッションを再度マッピングする必要があります。

仮想メディア ポリシーの作成

仮想メディアポリシーを使用すると、KVM コンソールと仮想メディアを使用してサーバにオペレーティングシステムをインストールし、リモートファイル共有からホストにファイルをマウントして、仮想メディア暗号化を有効化できます。別の OS イメージの仮想メディアマッピングを含む1つ以上の仮想メディアポリシーを作成し、最大2つの仮想メディアマッピングを設定できます。1つは ISO ファイル（CDD 経由）、もう1つは IMG ファイル（HDD 経由）です。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[仮想メディア（Virtual Media）]** を選択し、**[スタート（Start）]** をクリックします。

5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[仮想メディアの有効化（Enable Virtual Media）]	仮想メディアポリシーを有効にするには、このオプションを選択します。このプロパティは、デフォルトで有効になっています。
[仮想メディア暗号化の有効化（Enable Virtual Media Encryption）]	仮想メディア通信の暗号化を有効にするには、このオプションを選択します。このプロパティは、デフォルトで有効になっています。 （注） ファームウェア バージョン 4.2(1a) 以降では、この暗号化パラメータは廃止されました。暗号化を無効にすると、サーバプロファイルの展開中に検証が失敗します。
[省電力 USB の有効化（Enable Low Power USB）]	有効にして、イメージをマッピングしてホストを再起動すると、ブート選択メニューに仮想ドライブが表示されます。このプロパティは、デフォルトで有効になっています。
[仮想メディアの追加（Add Virtual Media）]	
[仮想メディアのタイプ（Virtual Media Type）]	リモートの仮想メディアのタイプを選択します • [CDD] • [HDD]
[NFS/CIFS/HTTP/HTTPS] 以下のプロパティは、選択したタブによって異なります。	

プロパティ（**Property**）	基本情報（**Essential Information**）
[名前（Name）]	仮想メディア マッピング用のイメージ ID。
[ファイルの場所（File Location）]	リモート ファイルの場所のパスを **ホスト名または IP アドレス/ファイル パス/ファイル名**で指定します。 • **[IP アドレス（IP Address）]**：リモート サーバの IP アドレスまたはホスト名。 • **[ファイル パス（File Path）]**：リモート サーバ上のイメージの場所へのパス。 • **[ファイル名（File Name）]**：**.iso** または **.img** フォーマットのリモート ファイルの名前。 仮想メディア マッピングでのリモート ファイルのロケーション パスには、以下のオプションを含められます。 • [HDD 仮想メディア（HDD Virtual Media]：<ホスト名>または<IP アドレス>/<ファイルパス>/<ファイル名>.img。 • [CDD 仮想メディア（CDD Virtual Media）]：<ホスト名>または<IP アドレス>/<ファイルパス>/<ファイル名>.iso。 • HTTP の HDD 仮想メディア：http://<サーバのホスト名>または<IP>/<ファイルパス>/<ファイル名>.img。 • HTTP の CDD 仮想メディア：http://<サーバのホスト名>または<IP>/<ファイルパス>/<ファイル名>.iso。 • HTTPS の HDD 仮想メディア：https://<サーバのホスト名>または<IP>/<ファイルパス>/<ファイル名>.img 。 • HTTPS の CDD 仮想メディア：https://<サーバのホスト名>または<IP>/<ファイルパス>/<ファイル名>.iso。
[ユーザ名（Username）]	リモートサーバにログインするためのユーザ名。このフィールドは、CIFS、HTTP、または HTTPS を選択すると表示されます。

プロパティ（**Property**）	基本情報（**Essential Information**）
Password	ユーザ名に関連付けられたパスワードです。このフィールドは、CIFS、HTTP、または HTTPS を選択すると表示されます。
[マウントオプション（Mount Options）]	仮想メディアマッピングのマウントオプション。フィールドは空白のままにするか、またはカンマ区切りリストで次のオプションを指定することができます。 • NFS の場合、サポートされているオプションは、**ro**、**rw**、**nolock**、**noexec**、**soft**、**port=VALUE**、**timeo=VALUE**、**retry=VALUE** です。 • CIFS の場合、サポートされているオプションは、**soft**、**nounix**、**noserverino**、**guest**、**ver=3.0**、または **ver=2.0** です。 （注） ファームウェア バージョンが 4.1 以上で、CIFS バージョンが 3.0 未満の場合、マウント オプション フィールドにバージョン値（vers = VALUE）を入力する必要があります。たとえば、vers = 2.0 です。 • HTTP および HTTPS の場合、サポートされているオプションは **noauto** だけです。

プロパティ（**Property**）	基本情報（**Essential Information**）
[認証プロトコル（Authentication Protocol）]	CIFS がリモートサーバとの通信に使用される際の認証プロトコルを選択します。このフィールドは、CIFS を選択すると表示されます。 • **[なし（None）]**：認証は使用されません。 • **[ntlm]**：—NT LAN Manager（NTLM）セキュリティプロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • **[ntlmi]**：NTLMi のセキュリティプロトコル。このオプションは、CIFS Windows サーバーでデジタル署名が有効な場合のみ使用します。 • **[ntlmv2]**：NTLMv2 セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • [ntlmv2i]：NTLMv2i のセキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • **[ntlmssp]**：NT LAN Manager のセキュリティ サポートプロバイダ（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • **[ntlmsspi]**：NT LAN Manager のセキュリティ サポート プロバイダ（NTLMSSPI）プロトコル。このオプションは、CIFS Windows サーバでデジタル署名を有効にした場合にのみ使用します。
[追加（Add）]	**[追加（Add）]**をクリックして、仮想メディアの追加を確認します。

7. **[作成（Create）]** をクリックします。

[例外（Exceptions）]

- 応答ファイルが OS ISO に組み込まれている場合、ブートモードが UEFI に設定されていると、vMedia からの起動に失敗し、Cisco UCS C シリーズスタンドアロン M4 サーバでの OS のインストールが失敗します。
- HTTPS ベースの共有の OS イメージの vMedia マッピングが失敗します。

ネットワーク接続ポリシーの作成

ネットワーク接続ポリシーを使用すると、IPv4 アドレスと IPv6 アドレスを設定して割り当てることができます。

[ダイナミック DNS（Dynamic DNS）]

ダイナミック DNS（DDNS）は、 DNS サーバのリソース レコードを追加または更新するために使用されます。DDNS オプションを有効にすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、DNS サーバのリソース レコードを更新します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ネットワーク 接続（Network Connectivity）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のプロパティを設定します。

[共通プロパティ（Common Properties）]

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[ダイナミック DNS の有効化]（Enable Dynamic DNS）	ダイナミック DNS を有効化します。 このプロパティは、ファブリック インターコネクトには適用されません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ダイナミック DNS 更新ドメイン（Dynamic DNS Update Domain）]	ダイナミック DNS ドメインを指定します。このドメインは、メイン ドメインまたはサブ ドメインのどちらにもできます。 このプロパティは、ファブリックインターコネクトには適用されません。

IPv4 のプロパティ

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP から IPv4 DNS サーバアドレスを取得	IPv4 アドレスが Dynamic Host Configuration Protocol（DHCP）から取得されるか、または特定の DNS サーバのセットから取得されるか。 • [有効（Enabled）]：Intersight は DHCP を使用します • [無効（Disabled）]：Intersight は IPv4 DNS サーバの設定済みセットを使用します。 このプロパティは、ファブリック インターコネクトには適用されません。
[優先 IPv4 DNS サーバ（Preferred IPv4 DNS Server）]	プライマリ DNS サーバの IP アドレス。このプロパティは、**[IPv4 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。
[代替 IPv4 DNS サーバ（Alternate IPv4 DNS Server）]	セカンダリ DNS サーバの IP アドレス。このプロパティは、**[IPv4 DNS サーバ アドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[IPv6 の有効化（Enable IPv6）]	IPv6 を有効にするかどうかを指定します。IPv6 プロパティは、このプロパティが有効になっている場合にのみ設定できます。

[IPv6 のプロパティ（IPv6 Properties）]

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP から IPv6 DNS サーバアドレスを取得	IPv6 アドレスが Dynamic Host Configuration Protocol（DHCP）から取得されるか、または特定の DNS サーバのセットから取得されるか。 • [有効（Enabled）]：Intersight は DHCP を使用します • [無効（Disabled）]：Intersight は IPv6 DNS サーバの設定済みセットを使用します。 このプロパティは、ファブリック インターコネクトには適用されません。
[優先 IPv6 DNS サーバ（Preferred IPv4 DNS Server）]	プライマリ DNS サーバの IP アドレス。このプロパティは、**[IPv6 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。
[代替 IPv6 DNS サーバ（Alternate IPv4 DNS Server）]	セカンダリ DNS サーバの IP アドレス。このプロパティは、**[IPv6 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。

7. **[作成（Create）]** をクリックします。

SMTP ポリシーの作成

簡易メール転送プロトコル（SMTP）は、サーバの障害が発生すると、設定されている SMTP サーバに電子メール アラートとして送信します。

ポリシーは、管理対象デバイスの SMTP クライアントの状態を設定します。発信通信の優先設定を指定し、報告する障害のシビラティ（重大度）とその報告を受け取る受信者を選択できます。

（注） このポリシーは、Intersight Managed FI が接続された UCS サーバに割り当てられているサーバ プロファイルに適用されている場合、無視されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SMTP]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
SMTP を有効にする	SMTPポリシーをイネーブルまたはディセーブルにします。
SMTP サーバ アドレス（SMTP Server Address）	SMTPサーバのIPアドレスまたはホスト名。
SMTP ポート	SMTP サーバで発信 SMTP 通信で使用するポート番号。 値の範囲は 1 ～ 65535 です。デフォルトは 25 です。
最小のシビラティ（重大度）	電子メール通知を受信する、障害シビラティ（重大度）レベルの最小値。選択したシビラティ（重大度）以上のすべての障害に関して電子メール通知が送信されます。
SMTP アラートの送信元アドレス	すべての SMTP メールアラートの送信者 IP アドレスまたはホスト名。
メールアラートの受信者	障害の通知を受け取る電子メールアドレスのリスト。

7. **[作成（Create）]** をクリックします。

SNMP ポリシーの作成

SNMPポリシーでは、管理対象デバイスからSNMPトラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。このポリシーは、SNMPv1、SNMPv2（v2c を含む）、SNMPv3 などのSNMPバージョンをサポートします。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、サーバ上の既存のユーザやトラップは削除されます。

SNMP ポリシーを使用すると、SNMP を有効または無効にしたり、アクセスおよびコミュニティ ストリングを指定したり、データの取得に使用する SNMP ユーザの詳細を指定したりできます。

（注）
- SNMP ポリシーのアウトオブバンド IP アドレスのサポートは、インフラストラクチャ ファームウェア 4.3(2.230129) 以降のバージョンで実行されているファブリック インターコネクトでのみ使用できます。
- SNMP ポリシーのアウトオブバンド IPアドレスのサポートは、Cisco UCS X シリーズ ダイレクト システムのサーバでは使用できません。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SNTP]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value 形式でタグを入力します
[説明（Description）]（オプション）	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP の有効化（Enable DNS）]	エンドポイントでの SNMP ポリシーの状態を表示します。エンドポイントから指定ホストに SNMP トラップを送信するには、このオプションを有効にします。
[SNMP ポート（SNMP Port）]	Cisco IMC SNMP エージェントを実行するポート。
[アクセス コミュニティ ストリング（Access Community String）]	SNMPv1、SNMPv2 コミュニティストリング、またはSNMPv3ユーザ名を入力します。フィールドには 18 文字まで入力できます。 （注） フィールドが空の場合は、SNMPv1 およびSNMPv2cユーザが無効になっていることを示します。
[SNMP コミュニティアクセス（SNMP Community Access）]	インベントリテーブル内の情報へのアクセスを制御します。SNMPv1 および SNMPv2c ユーザにのみ適用されます。 （注） このプロパティは、UCS スタンドアロン C シリーズ M6 サーバでのみサポートされます。
[トラップ コミュニティ ストリング（Trap Community String）]	他のデバイスに SNMP トラップを送信する際に使用する SNMP コミュニティ グループの名前を入力します。 （注） このフィールドは、SNMPv2c トラップホストまたは宛先にのみ適用されます。
[システム連絡先（System Contact）]	SNMP の実装担当者の連絡先。電子メールアドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。 （注） このプロパティは、UCS スタンドアロン C シリーズ サーバでのみサポートされます。
[システムの場所（System Location）]	SNMP エージェント（サーバ）が動作するホストの場所。 （注） このプロパティは、UCS スタンドアロン C シリーズ サーバでのみサポートされます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP エンジン入力 ID（SNMP Engine Input ID）]	ユーザ定義の一意の静的エンジン ID。 （注） このプロパティは、UCS スタンドアロン C シリーズ サーバでのみサポートされます。
[SNMP ユーザ（SNMP Users）]	
[名前（Name）]	SNMPv3 ユーザ名を入力します。このフィールドは 1～31 文字で指定する必要があります。
[セキュリティ レベル（Security Level）]	エージェントとマネージャーの間での通信で使用するセキュリティ メカニズムを選択します。 • AuthPriv • AuthNoPriv
[認証タイプ（Auth Type）]	ユーザの許可プロトコルとして [SHA] を選択します。 （注） MD5 認証プロトコルはサポートされていません。
[認証パスワード（Auth Password）]	ユーザの認証パスワードを入力します。
[認証パスワードの確認（Auth Password Confirmation）]	ユーザの認証パスワードを確認のため入力します。
[プライバシータイプ（Privacy Type）]	ユーザのプライバシープロトコルとして [AES] を選択します。 （注） [DES] プライバシータイプは、セキュリティ標準を満たすために廃止されました。
[プライバシー パスワード（Privacy Password）]	ユーザのプライバシー パスワードを入力します。
[プライバシーパスワードの確認（Privacy Password Confirmation）]	ユーザのプライバシー パスワードを確認のため入力します。
[SNMP トラップの宛先（SNMP Trap Destinations）]	
[有効化（Enable）]	SNMP ポリシーを使用するには、このオプションを有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP バージョン（SNMP Version）]	トラップの SNMP バージョンとして [v2] または [v3] を選択します。
[ユーザ（User）]	トラップの SNMP ユーザを選択します。最大 15 のトラップ ユーザを定義できます。 （注） このフィールドは SNMPv3 にのみ適用されます。
[トラップ タイプ（Trap Type）]	宛先にトラップが送信されたとき、どのタイプであれば通知を受信するかを選択します: • [トラップ（Trap）] • [情報（Inform）]
[宛先アドレス（Destination Address）]	SNMP トラップ情報の送信先アドレスを指定します。最大 15 のトラップ宛先を定義できます。
[ポート（Port）]	入力のサーバーがトラップの宛先と通信するために使用するポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 162 です。

7. [作成（Create）] をクリックします。

ストレージ ポリシーの作成

ストレージポリシーでは、ドライブグループ、仮想ドライブの作成、仮想ドライブのストレージ容量の設定、および M.2 RAID コントローラの設定を行うことができます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [ストレージ（Storage）] を選択して、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[一般設定（General Configuration）]	
[仮想ドライブの作成に JBOD ドライブを使用する（Use JBOD Drives for Virtual Drive creation）]	仮想ドライブの作成に JBOD 状態のディスクを使用するには、このオプションを有効にします。
[未使用のディスクの状態（Unused Disks State）]	このポリシーの未使用ディスクの移動先の状態を選択します。状態は、[UnconfiguredGood]、または [JBOD] のいずれかになります。 [No Change] を選択すると、状態は変更されません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[デフォルトのドライブモード（Default Drive Mode）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
	新しく挿入されたドライブまたは再起動時に、サポートされているストレージ コントローラーに設定する必要があるデフォルトのディスク状態を選択します。状態は、**UnconfiguredGood**、**JBOD** または **RAID0** のいずれかになります。 **[デフォルトのドライブ モード（Default Drive Mode）]**が **JBOD** または **RAID0** に設定されている場合、**[未使用ディスクの状態（Unused Disks State）]**は**[変更なし（No Change）]**に設定するべきです。 （注） デフォルトのドライブ モードは、M6 サーバーと次のストレージ コントローラでのみサポートされます。 • UCSC-RAID-M6T • UCSC-RAID-M6HD • UCSC-RAID-M6SD • UCSX-X10C-RAIDF **[設定の制限値（Configuration Limitation）]** : • Default Drive State が **JBOD** または **RAID0** の場合、**[未使用ディスクの状態（Unused Disks State）]** は **[変更なし（No Change）]** である必要があります。 • **[デフォルトのドライブ モード（Default Drive Mode）]**が **JBOD** の場合、**[VD 作成に JBOD を使用（Use JBOD for VD creation）]** を有効にすることはできません。 • Default Drive State が **UnconfiguredGood** の場合、ドライブの状態は再起動時に変更されません。 さまざまな **[デフォルト ドライブ モード シ**

[プロパティ（Property）]	[基本情報（Essential Information）]
	ナリオ（Default Drive Mode Scenarios）] については、表デフォルト ドライブ モード シナリオを参照してください。
セキュアな JBOD ディスク スロット	暗号化する JBOD ドライブ スロットを指定します。コンマまたはハイフンで区切られた番号範囲を入力できます。例: 1、3 または 4-6、8。
M.2 RAID 構成	**仮想ドライブ名と仮想ドライブを作成するための M.2 RAID コントローラのスロット**を指定するには、このオプションを有効にします。 M.2 コントローラが使用するディスク スロットは自動的に追加されます。
[仮想ドライブ名（Virtual Drive Name）]	このフィールドには、デフォルト名が事前に入力されています。任意の名前に変更できます。選択したコントローラ スロットに基づいて、優先する名前にサフィックスが追加されます。 名前の長さは 1 ～ 15 文字で、文字、数字、特殊文字のハイフン（-）、アンダースコア（_）、コロン（:）、およびピリオド（.）を使用できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[仮想ドライブ作成用の M.2 RAID コントローラのスロット（Slot of the M.2 RAID Controller for Virtual Drive Creation）]	仮想ドライブを作成する M.2 RAID コントローラのスロットを選択します。選択できるスロットは次のとおりです。 • **[MSTOR-RAID-1]**：M.2 RAID コントローラ スロットが 1 つしかない場合、または M.2 RAID コントローラ用に 2 つのスロットがあり、仮想ドライブを最初のスロットのコントローラに作成する必要がある場合は、このオプションを選択します。 • **[MSTOR-RAID-2]**：M.2 RAID コントローラ用の 2 つのスロットがあり、2 番目のスロットのコントローラに仮想ドライブを作成する必要がある場合は、このオプションを選択します。 • **[MSTOR-RAID-1,MSTOR-RAID-2]**：いずれかまたは両方のスロットのコントローラに仮想ドライブを作成します。
[ドライブグループの設定（Drive Group Configuration）]	仮想ドライブの作成に使用できる RAID ドライブグループを追加できるようにします。グローバルホットスペア情報を指定することもできます。 この構成は、M.2 RAID コントローラには適用されません。
[グローバルホットスペア（Global Hot Spares）]	ホットスペアとして使用するディスクを、すべての RAID グループに対してグローバルに指定します。 許可される値は、カンマまたはハイフンで区切られた数値範囲です。
[ドライブグループの追加（Add Drive Group）]	クリックしてドライブ グループを追加します。
[ドライブグループ名（Drive Group Name）]	ドライブ グループの名前を入力します。 名前の長さは 1 ～ 15 文字で、文字、数字、特殊文字のハイフン（-）、アンダースコア（_）、コロン（:）、およびピリオド（.）を使用できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[RAID レベル（RAID Level）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
	ディスク グループの RAID レベルは、可用性、データの冗長性、およびI/Oパフォーマンスの確保を目的とした、ディスク グループでのデータの編成方法を表します。レベルは次のとおりです。 • **[RAID0]**：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。 • **[RAID1]**：データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合に完全なデータ冗長性を提供します。最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。 • **[RAID5]**：データはアレイのすべてのディスクにストライピングされます。各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。 • **[RAID6]**：アレイのすべてのディスクにデータをストライプ化し、2 つのパリティ データ セットを使用して、最大 2 台の物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。 • **[RAID10]**：この RAID は、ミラー化されたディスクのペアを使用して、完全なデータ冗長性を提供し、ブロック レベルストライピングによって高いスループット レートを実現します。RAID 10 は、パリティおよびブロック レベルのストライピングを使用しないミラーリングを行います。RAID 10 には 4 台以上のディスクが必要です。

[プロパティ（Property）]	[基本情報（Essential Information）]
	• **[RAID50]**：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。 • **[RAID60]**：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。
セキュアなドライブ グループ	このオプションを有効にして、仮想ドライブの一部であるドライブの暗号化を構成します。
[スパン数（Number of Spans）]	RAID グループ用に作成されるスパングループの数。ネストのない RAID レベルには、単一のスパンがあります。 （注） [スパン数（Number of spans）] は、スパンのある RAID レベルが選択されている場合にのみ表示されます。
[ドライブの選択（Drive Selection）]	
[ドライブアレイスパン 0（Drive Array Span 0）]	ドライブアレイスパンを入力します。スパンを持たない RAID レベル RAID0、RAID1、RAID5、および RAID6 には、ディスクグループが 1 つだけあります。スパンを持つ RAID レベルには複数のディスクグループがあり、各ディスクグループがスパンを表します。 スパンのない RAID レベルには 1 つのスパングループがあり、スパンのある RAID レベルには 2ー8 つのスパングループがあります。 （注） スパンのない RAID レベルを選択した場合は、[Drive Array Span 0] フィールドのみが表示されます。スパンのある RAID レベルを選択した場合は、スパンの数を指定する必要があります。このシナリオでは、スパンと同じ数のドライブアレイスパン フィールドが表示され、詳細を指定できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[専用ホットスペア（Dedicated Hot Spares）]	このドライブグループのホットスペアとして使用するドライブのコレクションを指定します。 許可される値は、カンマまたはハイフンで区切られた数値範囲です。
[追加（Add）]	[追加（Add）] をクリックしてドライブ グループを追加します。
[仮想ドライブの追加（Add Virtual Drive）]	
[ドライブグループ（Drive Groups）]	仮想ドライブを作成するドライブグループを選択します。
[コピー数（Number of Copies）]	作成する仮想ドライブのコピー数を入力します。最大で 10 コピーを作成できます。
[仮想ドライブ設定（Virtual Drive Configuration）]	
[仮想ドライブ名（Virtual Drive Name）]	仮想ドライブの名前を入力します。 名前は1ー15文字で、英数字、特殊文字「-」（ハイフン）、「_」（アンダースコア、「:」（コロン）、および「.」（ピリオド）が使用できます。
[サイズ (MiB)（Size）]	MebiByte 単位での仮想ドライブのサイズです。[拡張して使用可能] オプションが有効になっている場合を除き、サイズは必須フィールドです。
保護済み	仮想ドライブの暗号化を有効にするには、これを設定します。 （注） このコントローラでサポートされているSEDドライブがないため、このオプションはUCS-M2-NVRAID（M.2 NVMe コントローラ）ではサポートされません。
RAID タイプ	RAID タイプを選択します。
[拡張して使用可能（Expand to Available）]	フラグを設定すると、ディスクグループ内で使用可能なすべての領域をこの仮想ドライブで使用できるようになります。有効にした場合、サイズプロパティは無視されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ブート ドライブとして設定（Set as Boot Drive）]	仮想ドライブをブート ドライブとして使用できるようにします。 （注） スタンドアロンラックの場合、ネイティブ ブロック サイズが 4K のドライブをブートドライブとして設定することはできません。
[ストリップ サイズ（Strip Size）]	必要なストリップサイズを選択します。指定できる値は、64KiB、128KiB、256KiB、512KiB、1 MiB です。
[アクセスポリシー（Access Policy）]	この仮想ドライブに対するホストのアクセスタイプを選択します。 • [読み取り/書き込み（Read/Write）]：ホスト仮想ドライブ で読み取り/書き込みを実行できます。 • [読み取り専用（Read Only）]：ホストは 仮想ドライブ から読み取りのみ行うことができます。 • [ブロック済み（Blocked）]：ホストは仮想ドライブ の読み取りおよび書き込みができません。
[読み取りポリシー（Read Policy）]	この仮想ドライブの先読みモードを選択します。 • [常に先読み（Always Read Ahead）] • [先読みしない（No Read Ahead）]

[プロパティ（Property）]	[基本情報（Essential Information）]
[書き込みポリシー（Write Policy）]	この仮想ドライブにを書き込むために使用するモードを選択します。 • [ライトスルー（Write Through）]：データはキャッシュによって物理ドライブに書き込まれます。以降はキャッシュからデータを読み取ることができるため、パフォーマンスが向上します。 • [BBU が良好でもライトバック（Write Back Good BBU）]：このポリシーでは、バッテリ バックアップ ユニット（BBU）が良好な場合でも、書き込みキャッシングは [ライトバック（Write Back）] のままにします。 • [書き込みバック（ライトバック）]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。
[ディスクキャッシュ（Disk Cache）]	この仮想ドライブのディスクキャッシュポリシーを選択します。値は次のとおりです。 • [変更なし（Unchanged）] • 有効 • 無効
[追加（Add）]	[追加（Add）] をクリックして仮想ドライブを追加します。
[シングルドライブの RAID 構成（Single Drive RAID Configuration）]	各物理ドライブに RAID0 仮想ドライブを作成できるようにします。
[ドライブスロット（Drive Slots）]	RAID0 仮想ドライブを作成するドライブスロットのセットを指定します。 （注） 単一ドライブ RAID では、将来ディスクを挿入する予定の場所にのみスロットを追加できます。
[ストリップ サイズ（Strip Size）]	必要なストリップサイズを選択します。指定できる値は、64KiB、128KiB、256KiB、512KiB、1 MiB です。

[プロパティ（Property）]	[基本情報（Essential Information）]
[アクセスポリシー（Access Policy）]	この仮想ドライブに対するホストのアクセスタイプを選択します。 • [読み取り/書き込み（Read/Write）]：ホスト仮想ドライブ で読み取り/書き込みを実行できます。 • [読み取り専用（Read Only）]：ホストは 仮想ドライブ から読み取りのみ行うことができます。 • [ブロック済み（Blocked）]：ホストは仮想ドライブ の読み取りおよび書き込みができません。
[読み取りポリシー（Read Policy）]	この仮想ドライブの先読みモードを選択します。 • [常に先読み（Always Read Ahead）] • [先読みしない（No Read Ahead）]
[書き込みポリシー（Write Policy）]	この仮想ドライブにを書き込むために使用するモードを選択します。 • [ライトスルー（Write Through）]：データはキャッシュによって物理ドライブに書き込まれます。以降はキャッシュからデータを読み取ることができるため、パフォーマンスが向上します。 • [BBU が良好でもライトバック（Write BackGood BBU）]：このポリシーでは、バッテリ バックアップ ユニット（BBU）が良好な場合でも、書き込みキャッシングは [ライトバック（Write Back）] のままにします。 • [書き込みバック（ライトバック）]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ディスクキャッシュ（Disk Cache）]	この仮想ドライブのディスクキャッシュポリシーを選択します。値は次のとおりです。 • [変更なし（Unchanged）] • 有効 • 無効
ハイブリッド スロット構成	ハイブリッド ドライブ スロット構成をサポートするサーバーの次のモードを選択します。 • 直接接続 NVMe スロット（Direct Attached NVMe Slots）：スロット範囲で指定された NVMe ドライブは、直接接続モードに移行されます。 • RAID 接続 NVMe スロット（RAID Attached NVMe Slots）：スロット範囲で指定された NVMe ドライブが RAID 接続モードに移行されます。 （注） • NVMe ハイブリッド スロットは、スタンドアロンモードおよび Intersight 管理モードの UCSC-C240-M7、UCSC-C220-M7 および UCSC-C245-M8 サーバでのみサポートされます。 • ハイブリッドスロットのサポートは、スロット 1 ～ 4 およびスロット 101 ～ 104 で使用できます。 • エンドポイントに PID UCSC-RAID-HP および Micron 7450 4GC キャッシュドライブを備えた Trimode 24G SAS RAID コントローラがある場合、RAID 接続された NVMe スロットを使用して RAID 構成を作成できます。 • ハイブリッドスロットでは、U.2 と U.3 ドライブ PID の組み合わせは推奨されません。

7. **[作成（Create）]** をクリックします。

（注） [仮想ドライブの削除（Delete Virtual Drive）] オプションは、ストレージ ポリシーでは使用できません。[ストレージ コントローラ（Storage Controllers）] ページを使用して仮想ドライブを削除する

（注） デコミッションまたは再稼働操作では、ディスク上の RAID またはデータは削除されません。

次の表は、さまざまなシナリオでのデフォルトのドライブ状態の動作を示しています。

表 *6 :* デフォルトのドライブ モードのシナリオ

[デフォルトのドライブ状態（Default Drive State）]	**[ホストの再起動/ホストの起動（Host Reboot/ Host Boot）]**	**ホットプラグ**	**[ユーザー アクション (デフォルトのドライブ状態でのサービス プロファイルの展開)（User Action (Service Profile deployment with Default Drive State)）]**
UnconfiguredGood（オフ）	• すべての UnconfiguredGood ドライブは、UnconfiguredGood のままです。 • 以前に変換されたすべての JBOD は、引き続き JBOD です。	• 挿入されたドライブは UnconfiguredGood のままです • 別のサーバーからの JBOD は、このコントローラで UnconfiguredGood のままです。	• UnconfiguredGood を設定しても、既存の構成には影響しません。 • すべての JBOD デバイスは、コントローラの起動後も JBOD のままになります。 • UnconfiguredGood は、コントローラーの起動後も UnconfiguredGood のままです。

[デフォルトのドライブ状態（Default Drive State）]	[ホストの再起動/ホストの起動（Host Reboot/Host Boot）]	ホットプラグ	[ユーザー アクション (デフォルトのドライブ状態でのサービス プロファイルの展開)（User Action (Service Profile deployment with Default Drive State)）]
JBOD	すべての未構成のドライブ（ユーザーが作成したものではない）は、JBOD に変換されます。	新しく挿入された未構成のドライブは、JBOD に変換されます。	• コントローラ上のすべての未構成のドライブ（ユーザーが作成したものではないドライブ）は、JBOD に変換されます。 • ユーザーが作成した UnconfiguredGood ドライブは、UnconfiguredGood のままです。
RAID0（RAID0 ライトバック）	すべての未構成ドライブは、RAID0 WriteBack（WB） に変換されます。 （注） 未構成のドライブは、ユーザーの操作によって状態が変更されないドライブです。	新しく挿入された未構成のドライブは、RAID0 WB に変換されます。	• コントローラー上のすべての未構成のドライブ（ユーザーが作成しない UnconfiguredGood）は、RAID0 WriteBack（WB）に変換されます。 • ユーザーが作成した UnconfiguredGood は、コントローラの再起動後も UnconfiguredGood のままです。 • すべての RAID0 ライトバック デバイスは、コントローラの起動/再起動後も RAID0 WB として残ります。

（注） デフォルトのドライブ状態が **RAID0** であるためにシステムによって作成された仮想ドライブの**[サーバー プロファイル派生（Server Profile Derived）]**は、**No** です。

次の表は、さまざまなデフォルト ドライブ状態シナリオのサンプル ユース ケースを示しています。

表 *7:* さまざまなドライブ モードの使用例

ユースケースのシナリオ	**[デフォルトのドライブ状態（Default Drive State）]**
サーバーを JBOD のみに使用する（例: ハイパーコンバージド、Hadoop データノードなど）	JBOD
サーバーを RAID ボリュームに使用する (例: SAP HANA データベース)	UnconfiguredGood
JBOD と RAID ボリュームが混在するサーバーの使用	UnconfiguredGood
ドライブの ROWB ごとにサーバーを使用する（例: Hadoop データノード）	RAID0 ライトバック

Syslog ポリシーの作成

Syslog ポリシーは、エンドポイントから収集したログファイルをレポートするログレベル (最低限のシビラティ（重大度）)、Syslog メッセージを保存する宛先、ホスト名/IP アドレス、ポート情報、リモートロギングサーバ用の通信プロトコルを定義します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[Syslog]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
ローカルロギング（Local Logging）	
[報告する最小シビラティ（重大度）（Minimum Severity to Report）]	リモート ログで報告する最低のシビラティ（重大度）レベルを選択します。シビラティ（重大度）は次のとおりです。 • 0 緊急 • 1 アラート • 2 重大 • 3 エラー • 4 警告 • 5 通知 • 6 情報 • 7 デバッグ
[リモートロギング：Syslog サーバ 1 および Syslog サーバ 2（Remote Logging - Syslog Server 1 and Syslog Server 2）]	
[有効化（Enable）]	Syslog ポリシーを有効または無効にするには、このオプションを選択します。 （注） Syslog サーバ 1 を無効にして Syslog サーバ 2 を有効にして Syslog ポリシーを作成すると、エンドポイント サーバで常に最初に Syslog サーバ 1 が有効になることがわかります。
[ホスト名/IP アドレス（Hostname/IP Address）]	Cisco IMC ログを保存する Syslog サーバのホスト名または IP アドレスを入力します。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ポート（Port）]	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルト ポート番号は、514 です。
[プロトコル（Protocol）]	Syslog サーバにログ メッセージを送信するためのトランスポート層プロトコルを選択します。。次のオプションがあります。 • TCP • UDP
[報告する最小シビラティ（重大度）（Minimum Severity to Report）]	リモート ログで報告する最低のシビラティ（重大度）レベルを選択します。シビラティ（重大度）は次のとおりです。 • 0 緊急 • 1 アラート • 2 重大 • 3 エラー • 4 警告 • 5 通知 • 6 情報 • 7 デバッグ

7. [作成（Create）] をクリックします。

サーバの電源ポリシーの作成

このポリシーは、サーバの電源冗長性、電源プロファイリング、および電源復元の設定を有効にします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [電源（Power）] を選択し、[スタート（Start）] をクリックします。

5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

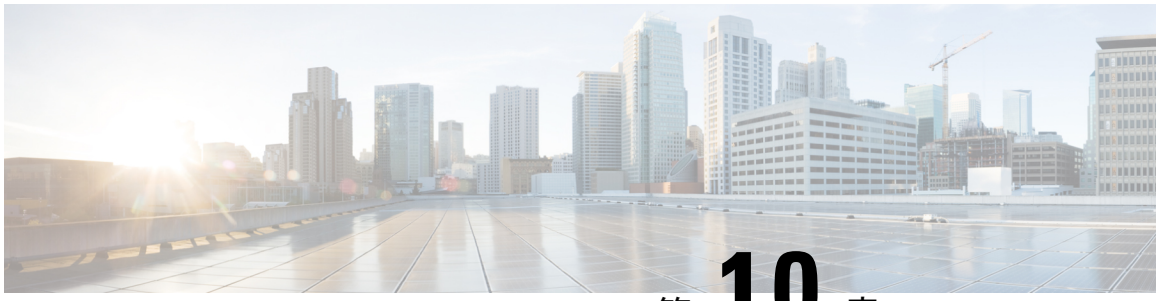
6. **[ポリシーの詳細（Policy Details）]** ページで、**[すべてのプラットフォーム（All Platforms）]** タブに移動します。

7. 次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[電力プロファイル（Power Profiling）]	システムの電力プロファイリングを有効または無効にします。 **[有効（Enabled）]**：有効にすると、CIMC は BIOS ブート中に電力プロファイリングユーティリティを実行して、サーバの電力ニーズを判断できます。 **[無効（Disabled）]**：無効にすると、電力プロファイリングは実行されません。 （注） このプロパティは、Cisco UCS X シリーズ サーバーでのみサポートされます。

プロパティ（**Property**）	基本情報（**Essential Information**）
電源のプライオリティ	各サーバーには、**高**、**中**、または**低**の電力優先度が割り当てられます。サーバーに割り当てられる電力は、サーバーの電力優先度によって異なります。優先度の高いサーバーは、より高い電力バジェットを取得します。デフォルトの電力優先度は**低**です。 （**注**） このプロパティは、次でサポートされています。 • 最小 Cisco IMC ファームウェア バージョン 4.2(1e) を搭載した Cisco-UCSX-9508 シャーシ内のサーバー。 • 最小 Cisco IMC ファームウェア バージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ内のサーバー。
[電源復元（Power Restore）] CIMC でサーバの電源復元状態を設定できます。IMM 接続がない場合、CIMC はこのポリシーを使用して、電力損失イベント後にホストの電力を回復します。 （**注**） このプロパティは、以下でサポートされています。 • 最小 Cisco IMC ファームウェア バージョン 4.2(1e) を搭載した Cisco-UCSX-9508 シャーシ内の Cisco UCS X シリーズ IMM サーバー。 • 最小 Cisco IMC ファームウェア バージョン 4.2(1d) を搭載した Cisco-UCSB-5108 シャーシ内の Cisco UCS B シリーズ IMM サーバー。	
[前回の状態（Last State）]	電力損失イベントが発生する前の状態にホストの電力を設定します。
[常時オン（Always On）]	電力損失イベント後は常にホストの電源をオンにします。
[常にオフ（Always Off）]	電力損失イベント後は、必ずホストの電源をオフにします。

8. **[作成（Create）]** をクリックします。



第 10 章

UCS シャーシ ポリシーの設定

- シャーシ ポリシー （317 ページ）
- IMC アクセス ポリシーの作成 （318 ページ）
- SNMP ポリシーの作成 （319 ページ）
- シャーシの電源ポリシーの作成 （322 ページ）
- 温度ポリシーの作成 （325 ページ）

シャーシ ポリシー

Cisco Intersight のシャーシポリシーでは、IP プール設定、VLAN 設定、SNMP 認証、SNMP トラップ設定など、シャーシのさまざまなパラメータを構成できます。シャーシポリシーは、任意の数のシャーシプロファイルに割り当てることで、シャーシの構成基準を提供できます。

Chassis Policies テーブル ビューを表示するには、**Service Selector** ドロップダウン リストから **[サービスとしてのインフラストラクチャ（Infrastructure Service）]** を選択します。**[構成（Configure）> ポリシー（Policies）]** の順に選択します。

Cisco Intersight のシャーシポリシー作成ウィザードには、次の 2 つのページがあります。

- **[全般（General）]**：組織を選択し、ポリシーの名前を入力できます。オプションで、ポリシーの識別に役立つ短い説明とタグ情報を含められます。タグは key：value 形式である必要があります。たとえば、Org:IT または Site:APJ などです。
- **[ポリシーの詳細（Policy Details）]**：ポリシーの詳細ページには、UCS シャーシポリシーに適用可能なプロパティがあります。

シャーシ ポリシーは、既存のポリシーと同様のプロパティで **[ポリシー クローン（Policy Clone）]** ウィザードを使用して複製することもできます。ポリシーの複製アクションは、ポリシー リストと詳細ビューの両方で使用できます。詳細については、「ポリシーの複製」を参照してください。

Cisco Intersight で設定できるシャーシ ポリシーは次のとおりです。

- **[IMC アクセス ポリシー（IMC Access Policy）]**：IP プールとシャーシプロファイルのマッピングによって、ネットワークを構成し、管理できます。このポリシーを使用すると、VLAN を構成し、IP プールを使用して IP アドレスと関連付けることができます。

（注） シャーシ IMC アクセス ポリシーでは、インバンド構成のみがサポートされます。

- **[SNMP ポリシー（SNMP Policy）]**：管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。管理対象デバイスですでに構成されている SNMP ユーザーまたは SNMP トラップは削除され、このポリシーで構成するユーザーまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、入出力モジュール（IOM）上の既存のユーザやトラップは削除されます。
- **[電源ポリシー（Power Policy）]**：シャーシの電源使用の管理を有効にします。このポリシーでは、シャーシ電源装置（PSU）の冗長モードを設定し、シャーシに電力を割り当てることができます。[シャーシの詳細（Chassis details）] ビューページの **[全般（General）]** タブのプロパティセクションで、冗長の正常性、冗長モード、入力電源の正常性、および出力電源の正常性を表示できます。Cisco UCS X9508 シャーシの場合、省電力モードと動的電力再割り当てを設定できます。
- **[温度ポリシー（Thermal Policy）]**：シャーシのファン制御モードの値を設定できます。ファン制御モードは、最適なサーバ冷却を維持するためにシャーシファンの速度を制御します。

IMC アクセス ポリシーの作成

IMC アクセスポリシーでは、VLAN ID を提供し、選択した IP プールからの IP アドレスと関連付けることができます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[IMC アクセス（IMC Access）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value 形式でタグを入力します

[プロパティ（Property）]	[基本情報（Essential Information）]
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]	
[VLAN ID]	入力インバンドネットワークを介したサーバアクセスに使用される VLAN ID を入力します。フィールド値は 4ー4093 です。	
IPv4 アドレス設定	このポリシーのネットワークのタイプを決定する場合に選択します。 （注） IPv4 アドレス設定のみ、または IPv4 と IPv6 の両方の設定を選択できます。	
IPv6 アドレス設定	このポリシーのネットワークのタイプを決定する場合に選択します。IPv6 アドレス設定のみ、または IPv4 と IPv6 の両方の設定を選択できます。 重要 IPv6 は UCS-IOM-2408 でのみサポートされます。	
IP プール	IP プールの選択	クリックして、右側のペインで IP プールリストを表示して選択します。

7. **[作成（Create）]** をクリックします。

（注） IMC アクセス ポリシーは、現在、Cisco UCS X シリーズ ダイレクトシャーシ（UCSX-9508）ではサポートされていません。

SNMP ポリシーの作成

SNMP ポリシーでは、管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。このポリシーは、SNMPv1、SNMPv2（v2c を含む）、SNMPv3 などの SNMP バージョンをサポートします。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、入出力モジュール（IOM）上の既存のユーザやトラップは削除されます。

SNMP ポリシーを使用すると、SNMP を有効または無効にしたり、アクセスおよびコミュニティ ストリングを指定したり、データの取得に使用する SNMP ユーザの詳細を指定したりできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SNTP]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value 形式でタグを入力します
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP の有効化（Enable DNS）]	エンドポイントでの SNMP ポリシーの状態を表示します。エンドポイントから指定ホストに SNMP トラップを送信するには、このオプションを有効にします。
[アクセス コミュニティ ストリング（Access Community String）]	SNMPv1、SNMPv2 コミュニティストリング、またはSNMPv3ユーザ名を入力します。フィールドには 18 文字まで入力できます。 （注） フィールドが空の場合は、SNMPv1およびSNMPv2cユーザが無効になっていることを示します。
[トラップ コミュニティ ストリング（Trap Community String）]	他のデバイスに SNMP トラップを送信する際に使用する SNMP コミュニティ グループの名前を入力します。 （注） このフィールドは、SNMPv2c トラップホストまたは宛先にのみ適用されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP ユーザ（SNMP Users）]	
[名前（Name）]	SNMPv3ユーザ名を入力します。このフィールドは 1〜31 文字で指定する必要があります。
[セキュリティ レベル（Security Level）]	エージェントとマネージャーの間での通信で使用するセキュリティ メカニズムを選択します。 • AuthPriv • AuthNoPriv
[認証タイプ（Auth Type）]	ユーザの認証プロトコルとして **[SHA]** を選択します （注） **[MD5]** 認証プロトコルはサポートされていません。
[認証パスワード（Auth Password）]	ユーザの認証パスワードを入力します。
[認証パスワードの確認（Auth Password Confirmation）]	ユーザの認証パスワードを確認のため入力します。
[プライバシータイプ（Privacy Type）]	ユーザのプライバシープロトコルとして **[AES]** を選択します。
[プライバシー パスワード（Privacy Password）]	ユーザのプライバシー パスワードを入力します。
[プライバシーパスワードの確認（Privacy Password Confirmation）]	ユーザのプライバシー パスワードを確認のため入力します。
[SNMP トラップの宛先（SNMP Trap Destinations）]	
[有効化（Enable）]	SNMP ポリシーを許可して展開するには、このオプションを有効にします。
[SNMP バージョン（SNMP Version）]	トラップの SNMP バージョンとして **[v2]** または **[v3]** を選択します。
[ユーザ（User）]	トラップの SNMP ユーザを選択します。最大 15 のトラップ ユーザを定義できます。 （注） このフィールドはSNMPv3 にのみ適用されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[トラップ タイプ（Trap Type）]	宛先にトラップが送信されたとき、どのタイプであれば通知を受信するかを選択します: • [トラップ（Trap）] • [情報（Inform）]
[宛先アドレス（Destination Address）]	SNMP トラップ情報の送信先アドレスを指定します。最大 15 のトラップ宛先を定義できます。
[ポート（Port）]	入力のサーバーがトラップの宛先と通信するために使用するポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 162 です。

7. [作成（Create）] をクリックします。

（注） SNMP ポリシーは現在、Cisco UCS X シリーズ ダイレクト シャーシ（UCSX-9508）ではサポートされていません。

シャーシの電源ポリシーの作成

このポリシーは、シャーシの電源冗長性と電源割り当ての設定を有効にします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ（Service Selector）] ドロップダウン リストから、[インフラストラクチャ サービス（Infrastructure Service）] を選択します。
3. [ポリシーの構成（Configure > Policies）] に移動し、[ポリシーの作成（Create Policy）] をクリックします。
4. [電源（Power）] を選択し、[スタート（Start）] をクリックします。
5. [全般（General）] ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

プロパティ（Property）	基本情報（Essential Information）
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、**[UCS シャーシ（UCS Chassis）]** タブに移動します。
7. 次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[電源の冗長性（Power Redundancy）] シャーシ電源の冗長モードを設定します。	
[グリッド（Grid）]	グリッドモードには2つの電源が必要です。一方の電源がダウンすると、もう一方の電源装置がシャーシに電源を供給します。
[非冗長（Not Redundant）]	Power Managerは、シャーシの電力要件をサポートするために必要な最小数の PSU をオンにします。冗長 PSU は維持されません。
[N+1]	Power Managerは、シャーシの電源要件をサポートするために必要な最小数の PSU と、冗長性のために 1 つの追加 PSU をオンにします。
[N+2]	Power Managerは、シャーシの電源要件と冗長性のための 2 つの追加 PSU をサポートするために必要な最小数の PSU をオンにします。 （注） このモードは、Cisco-UCSX-9508 シャーシでのみサポートされています。

プロパティ（Property）	基本情報（Essential Information）
Power Saveモード	要求された電力が利用可能な電力よりも少ない場合に、追加の PSU 容量を省電力モードにすることができます。 （注） このプロパティは、以下でサポートされています。 • 最小 Cisco IMC ファームウェア バージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシ。 • 最小 Cisco IMC ファームウェア バージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ。
動的パワー リバランス	サーバに電力を動的に再割り当てできるようにします。 有効にすると、ブレード、ファン、IOM/IFM、XFM などのさまざまなシャーシ コンポーネント間で電力が再バランスされます。 （注） このプロパティは、以下でサポートされています。 • 最小 Cisco IMC ファームウェア バージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシ。 • 最小 Cisco IMC ファームウェア バージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ。
拡張電力容量	シャーシの拡張電力容量を設定します。このモードを有効にすると、冗長電源から電力が借りられ、シャーシが利用できる電力が増加します。 （注） このプロパティは、最小 Cisco IMC ファームウェア バージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシでのみサポートされます。

プロパティ（Property）	基本情報（Essential Information）
[電力割り当て（ワット）（Power Allocation (Watts)）]	シャーシが消費できる最大電力を設定できます。 この値は、最小システム要件から最大使用可能電力までの範囲で指定できます。 電力割り当てが0のポリシーを展開すると、シャーシバジェットのキャップが解除されます。つまり、シャーシは使用可能なすべての電力を消費できます。 （注） このプロパティは、以下でサポートされています。 • 最小 Cisco IMC ファームウェア バージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシ。 • 最小 Cisco IMC ファームウェア バージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ。

8. **[作成（Create）]** をクリックします。

温度ポリシーの作成

このポリシーにより、シャーシ ファンの速度を制御できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[サーマル（Thermal）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

プロパティ（Property）	基本情報（Essential Information）
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[ファン制御モード（Fan Control Mode）] シャーシのファン速度を制御します。	
[バランス（Balanced）]	サーバで多量の熱が発生すると、ファンはその必要に応じてより高速で稼働します。可能な場合、ファンは必要な最低速度に戻ります。
[ロー パワー（Low Power）]	ファンは、**[バランス（Balanced）]**モードよりもわずかに低い最小速度で動作し、可能な場合は電力消費を抑えます。
[ハイ パワー High Power）]	ファンは電力消費よりパフォーマンスを重視した、より高い速度を動作します。 （注） このモードは、UCS X シリーズ シャーシでのみサポートされます。
[最大パワー（Maximum Power）]	ファンは常に最大速度に維持されます。このオプションでは冷却効果は最大になりますが、電力消費も最大になります。 （注） このモードは、UCS X シリーズ シャーシでのみサポートされます。
[音響（Acoustic）]	大きな音響が問題となる環境でのノイズレベルを減らすために、ファン速度を遅くします。 （注） このモードは、UCS X シリーズ シャーシでのみサポートされます。

7. **[作成（Create）]** をクリックします。

第 11 章

プールの設定

- プール （327 ページ）
- ID プール （327 ページ）
- プールの割り当て （328 ページ）
- プールの削除 （328 ページ）
- 予約済みの識別子 （329 ページ）
- IP プール （330 ページ）
- MAC プール （334 ページ）
- UUID プール （337 ページ）
- WWN プール （339 ページ）
- IQN プール （343 ページ）
- リソース プール （346 ページ）
- 仮想ルーティングおよび転送 （350 ページ）

プール

プールは、ハードウェアリソースを一意に識別するための基本的な構成要素です。これらは UCS 管理モデルの基盤を形成し、アップストリーム LAN または SAN に対して同じ ID とプレゼンテーションを維持しながら、サーバー プロファイルとブレード サーバーの関連付けを可能にします。

プールは、リソースプールとアイデンティティ（ID）プールに分類されます。

プール テーブル ビューを使用すると、サーバー プールの使用率をモニターし、使用可能 ID および使用済み ID を追跡し、プールの容量と割り当てに関して情報に基づいた決定を行うことができます。

ID プール

ID プールはさらに、次のカテゴリに分類されます。

- **IP プール**： ネットワーク要素で実行されているサービスに IP アドレスを動的に割り当てる柔軟性を提供します。
- **MAC アドレス プール**：ネットワーク インターフェイス ポートの一意の ID を提供します。
- **UUID プール**：サーバー プロファイルに関連付けられた各サーバーに一意の ID を提供します。
- **WWNN および WWPN プール**：サーバ上のファイバ チャネル リソースの一意の ID を提供します（ファイバ チャネル ノードおよびポート）。
- **IQN プール**：iSCSI vNIC によってイニシエータ ID として使用される iSCSI 修飾名（IQN）の集合です。

プールの割り当て

複数の割り当て反復で一貫した反復可能な ID 割り当てを確保するために、プール割り当ての反復中に使用可能な最小の ID が順番に割り当てられます。

たとえば、ID の範囲が 1 ～ 20 のプールがあるとします。次の表では、ID の割り当てと再割り当ての反復について説明します。

使用例	動作
プールから 5 つのIDが要求されます	ID 1 ～ 5 が割り当てられます
1 ～ 5 個の ID がリリースされます	ID 1 ～ 5 がリリースされました
プールから 5 つのIDが要求されます	ID 1 ～ 5 が割り当てられます

一部の ID が組織の異なるプール間で共有される、重複するプールを持つことができます。ID はアカウント全体で一意であるため、異なる組織で使用されているかどうかにかかわらず、ID が 1 つのプールで使用されている場合は、使用されているすべてのプールでも **[使用済み（Used）]** としてマークされます。プール テーブル表示には、割り当てられた ID の概要が表示され、組織全体のプールの ID 使用状況を追跡できます。[プール テーブル表示（Pools Table View）] の [ソース（Source）] 列は、ID が割り当てられているプールを示します。ID が現在のプールから割り当てられている場合、[ソース（Source）] 列は [セルフ（Self）] としてマークされます。ID が別のプールから割り当てられている場合、[ソース（Source）] 列は [その他（Other）] とマークされます。

プールの削除

ID が割り当てられていない組織内のプールまたはアドレス ブロックを削除できます。別の組織のプールの割り当てには影響しません。

ステップ 1 ID が現在サーバプロファイルに関連付けられていないことを確認します。

a) **[プール テーブル表示（Pools Table View）]**で、**[ソース（Source）]** 列を確認してプールの使用状況を分析します。

b) **[ソース（Source）]** が **[その他（Other）]** とマークされている場合は、重複する他のプールから割り当てられている ID の削除に進むことができます。

c) **Source = Self** としてマークされたプールは、いずれかのプロファイルで使用されているため削除できないため、削除しないでください。

ステップ 2 [削除（Delete）] をクリックします。

予約済みの識別子

IP アドレス、MAC アドレス、IQN、UUID、WWNN、および WWPN は、物理サーバーがサーバー プロファイルから取得する一般的な識別子です。

Intersight は、ポリシー、プロファイル、またはテンプレートを変更するときに、MAC、IQN、iSCSI IP などの LAN 接続ポリシー（LCP）ID、および WWPN や WWNN などの SAN 接続ポリシー（SCP）識別子を保持するためにベストエフォートを使用します。 。

LCP または SCP を、重複しない ID を持つ異なるプールにアクセスする新しいポリシーに変更する場合は、すべての ID が変更されることを想定してください。さらに、新しいプールに使用可能な正確な ID がない場合は、変更が予想されます。

次のシナリオでは、編集または変更中に ID の保持が期待できます。

- vNIC または vHBA を LCP または SCP に追加する場合。
- ポリシー LCP1/SCP1 を、同じプール参照を使用する LCP2/SCP2 に変更する場合。
- ポリシー LCP1/SCP1 を、異なるプール参照を使用するが、同じ ID が使用可能な LCP2/SCP2 に変更する場合。
- 静的識別子を使用するポリシー LCP1/SCP1 を、使用可能な同じ ID を持つプール参照を使用する LCP2/SCP2 に変更する場合。
- テンプレート T1 からサーバー プロファイルを切り離し、同じ ID を使用してサーバー プロファイルをテンプレート T2 に接続する場合。
- 上記のように、サーバー プロファイル テンプレートを編集し、LCP1/SCP1 を LCP2/SCP2 に変更する場合。
- 既存の LCP/SCP ポリシーを編集し、識別子参照を静的から使用可能な同じ ID を持つプールに変更する場合。

アイデンティティ予約

環境間の移行などの目的で、プールから特定の値を選択できるように、割り当ての前にアイデンティティ を予約できます。たとえば、Cisco UCSM から IMM などです。

予約済み識別子のガイドライン

- 識別子は、 IMM 移行ツール（IMM Transition Tool） を介して、または https://intersight.com/apidocs/apirefs/macpool/Reservations/model/ などの使用可能なプール予約 API を使用してのみ予約できます。
- 識別子の予約は、ファブリック インターコネクト接続サーバーに対してのみ実行できます。
- 予約済み識別子は1回限りの使用を目的としており、消費されると予約プールから削除されます。

予約済みIDは、ポリシー（予約済みIDを含む）がサーバープロファイルに接続されたとき、またはサーバー プロファイルが展開されたときに消費されます。

[予約済み識別子（Reserved Identifiers）] タブには、予約済み識別子の値、そのタイプ、および対応するプール メンバーシップのリストが表示されます。割り当てタイプが静的の場合、プール メンバーシップは空白で表示されます。予約済みの識別子を選択して削除できます。

IP プール

IP プールには、1 つ以上の IP ブロックを含めることができます。これらのブロックは、最も低いブロックから順番に使用されます。IP プールは、IPv4 アドレスと IPv6 アドレスの両方をサポートします。

IP プールのサブネット構成

すべての IP ブロックに共通のサブネット構成（プールレベル）または IP ブロックごとに異なるサブネット構成（ブロック レベル）のいずれかで IP プールを作成できます。

ブロック レベルでサブネット構成を使用してプールを定義した後、プール レベルのサブネット構成に移行できます。その逆も可能です。プールレベルからブロックレベルのサブネット構成に移行する場合、サブネット構成は既存の各 IP ブロックに複製されます。ブロックレベルからプールレベルのサブネット構成に移行する場合は、プールレベルで共通のサブネット構成を再構成する必要があります。

IP ブロックに既存のリースがある場合、移行は次のシナリオでのみ許可されます。

- **既存のリースを使用したプールレベルからブロックレベルの構成への移行**：

  既存のリースを使用してプールレベルの構成からブロックレベルの構成に移行すると、サブネット構成は変更なしでブロックレベルに移動されます。これは、プール レベルで以前に構成された同じサブネット構成が各ブロックにコピーされることを意味します。このような場合、既存のリースがあっても移行は許可されます。移行後、どのブロックのサブネット構成も変更できない場合は、既存のアクティブなリースがあることが原因である可

能性があります。すでにアクティブなリースがある場合は、ブロックのサブネット構成を変更できないことに注意してください。

- **既存のリースを使用したブロックレベルからプールレベルの構成への移行**：

  既存のリースを使用してブロックレベルからプールレベルの構成に移行する場合は、プールレベルでサブネット構成を指定する必要があります。以前のすべてのブロックレベルのサブネット構成が新しいプールレベルのサブネット構成と同じである場合、移行は許可されます。このシナリオでは、既存のリースがある場合でも移行が許可されます。

IP プールの作成

IP プールは、サーバ プロファイルなどの設定エンティティに割り当てることができる IP アドレスの集合を表します。IPv4 プールまたは IPv6 プール、あるいは両方を作成できます。

ステップ 1 左側のナビゲーションパネルで、**[プールの作成（Create Pools）]** > **[IP]** > **[開始（Start）]**をクリックします。

[IP Pool] ウィザードが表示されます。

ステップ 2 **[General]** ページで次の情報を追加します。

- **[Organization]**：IP プールの組織。
- **[Name]**：IP プールの名前。
- **[Add Tag]**：IP プールを識別して検索するためのタグ。
- **[Description]**：IP プールの説明。
- **[ブロック レベルでのサブネットの構成（Configure Subnet at Block Level）]**：IPv4 および IPv6 プール内の各 IP ブロックのサブネット構成を有効にするには、このチェックボックスをオンにします。

ステップ 3 **[次へ（Next）]** をクリックします。

ステップ 4 （オプション）IPv4 プールを設定します。

a) **[IPv4 プールの設定（Configure IPv4 Pool）]** トグル ボタンを使用して、IPv4 プールの構成を有効にします。デフォルトでは有効に設定されています。後で IPv4 プールを構成することもできます。

b) プールレベルで**[ネットマスク（Netmask）]**、**[ゲートウェイ（Gateway）]**、**[プライマリDNS（Primary DNS）]**、および **[セカンダリ DNS（Secondary DNS）]** フィールドを設定することを選択した場合は、**[構成（Configuration）]** でこれらの詳細を入力します。これらのフィールドをブロック レベルで設定することを選択した場合は、IP ブロックの構成時にこれらの詳細を入力します。

c) **[IP ブロック（IP Blocks）]** で、1 つ以上の IP ブロックを設定します。

1. **[IP ブロックの追加（Add IP Blocks）]** をクリックして、IP ブロックを追加します。
2. IP ブロックの次のパラメータを入力します。

   （注） プールレベルまたはブロックレベルで [ネットマスク（Netmask）]、[ゲートウェイ（Gateway）]、[プライマリ DNS（Primary DNS）]、および [セカンダリ DNS（Secondary DNS）] フィールドを設定できます。

- **[開始（From）]**：IP プールの開始 IP アドレス。
- **[サイズ（Size）]**：IP プールに割り当てられた IP アドレスの数。
- **[ネットマスク（Netmask）]**：IP プールに関連付けられたネットマスク。
- **[ゲートウェイ（Gateway）]**：IP プールのゲートウェイの IP アドレス。

  （注） IP プールを IMC アクセス ポリシーに使用する場合は、IP プールで指定されたゲートウェイ IP アドレスに Cisco IMC への接続があることを確認してください。

- **[プライマリ DNS（Primary DNS）]**：この IP アドレスのブロックがアクセスするプライマリ DNS サーバです。
- **[セカンダリ DNS（Secondary DNS）]**：この IP アドレスのブロックがアクセスするセカンダリ DNS サーバです。

ステップ 5 （オプション）IPv6 プールを構成します。

a) **[IPv6 プールの構成（Configure IPv6 Pool）]** トグルボタンを使用して、IPv6 プールの構成を有効にします。デフォルトでは有効に設定されています。後で IPv6 プールを構成することもできます。

b) プール レベルで **[プレフィックス（Prefix）]**、**[ゲートウェイ（Gateway）]**、**[プライマリ DNS（Primary DNS）]**、および **[セカンダリ DNS（Secondary DNS）]** フィールドを構成することを選択した場合は、**[設定（Configuration）]** でこれらの詳細を入力します。これらのフィールドをブロック レベルで設定することを選択した場合は、IP ブロックの構成時にこれらの詳細を入力します。

c) **[IP ブロック（IP Blocks）]** で、1 つ以上の IP ブロックを設定します。

1. **[IP ブロックの追加（Add IP Blocks）]** をクリックして、IP ブロックを追加します。
2. IP ブロックの次のパラメータを入力します。

   （注） [プレフィックス（Prefix）]、[ゲートウェイ（Gateway）]、[プライマリ DNS（Primary DNS）]、および [セカンダリ DNS（Secondary DNS）] フィールドは、プール レベルまたはブロック レベルで構成できます。

   - **[開始（From）]**：IP プールの開始 IP アドレス。
   - **[サイズ（Size）]**：IP プールに割り当てられた IP アドレスの数。
   - **[プレフィックス（Prefix）]**：IP プールに関連付けられたプレフィックス。
   - **[ゲートウェイ（Gateway）]**：IP プールのゲートウェイの IP アドレス。

     （注） IP プールを IMC アクセス ポリシーに使用する場合は、IP プールで指定されたゲートウェイ IP アドレスに Cisco IMC への接続があることを確認してください。

   - **[プライマリ DNS（Primary DNS）]**：この IP アドレスのブロックがアクセスするプライマリ DNS サーバです。
   - **[セカンダリ DNS（Secondary DNS）]**：この IP アドレスのブロックがアクセスするセカンダリ DNS サーバです。

ステップ 6 **[作成（Create）]** をクリックします。

新しく作成された IP プールが IP プールのリストに表示されます。

IP プールの詳細

詳細

IP プールのリストを表示します。

プロパティ（Property）	基本情報（Essential Information）
[詳細（Details）]	
[名前（Name）]	IP プールの名前を表示します。
[タイプ（Type）]	プールのタイプを表示します。
[サイズ（サイズ）]	IP プールに含まれる ID の総数を表示します。
[使用済み（Used）]	使用されて使用できなくなった IP プール内の識別子の総数を表示します。
予約済み	後で使用するために予約されている IP プール内の識別子の総数を表示します。
[応答可能（Available）]	使用可能な IP プール内の識別子の総数を表示します。
[説明（Description）]	IP プールの説明。
[最終更新（Last Update）]	IP プールが最後に更新された日時。
[組織（Organization）]	**[デフォルト（Default）]**組織のユーザは、ユーザアカウントで使用可能なすべてのリソースにアクセスできます。
設定	
IPv4	サブネットがプール レベルで構成されるとき、サブネット マスク、デフォルト ゲートウェイ、プライマリ DNS、セカンダリ DNS など、プールの IPv4 構成を表示します。
IPv6	サブネットがプール レベルで構成されているとき、プレフィックス、デフォルト ゲートウェイ、プライマリ DNS、セカンダリ DNS など、プールの IPv6 構成を表示します。

プロパティ（**Property**）	基本情報（**Essential Information**）
移行前	プールの開始 IP を表示します。 **Note** Cisco Intersight は、ID を順番に選択します。つまり、プールから使用可能な最も低い ID を選択します。
[保持数（To）]	ブロック サイズの範囲を表示します。 **Note** この値は、IP プール サイズ プロパティに依存します。
[サイズ（Size）]	IP プール サイズを表示します。
目の記号	サブネットがブロック レベルで設定されている場合に、サブネット マスク、プレフィックス、デフォルト ゲートウェイ、プライマリ DNS、セカンダリ DNS などのプールの設定を表示します。
使用量	
IP、VRF、サーバー プロファイル、およびソース	IP アドレス、VRF インスタンス、使用状況（予約済みまたは使用済み）、および関連するサーバー プロファイルを表示します。 Source は **Self** または **Other**にできます。ここで、 **Self** はこのプールによって使用または予約されている ID であり、 **Other** は静的にまたは別のプールによって使用または予約されている ID です。
[アクション（Actions）]	
[編集（Edit）]	IP プールの設定の詳細を追加または変更できます。
[削除（Delete）]	IP プールを削除できます。

MAC プール

MAC プールは、ネットワーク ID（MAC アドレス）の集合です。MAC アドレスはレイヤ 2 環境では一意で、サーバの vNIC に割り当てることができます。サーバプロファイルで MAC プールを使用する場合は、サーバ プロファイルに関連付けられたサーバで使用できるように MAC アドレスを手動で設定する必要はありません。

サーバに MAC アドレスを割り当てるには、vNIC を LAN 接続ポリシーに追加すると同時に MAC プールを含める必要があります。その後、LAN 接続ポリシーは、そのサーバに割り当てられたサーバ プロファイルに取り込まれます。

MAC プールの作成

MAC プールは、サーバ プロファイルの vNIC に割り当てることができる MAC アドレスの集合を表します。

ステップ 1 左側のナビゲーションパネルで **[プール（Pools）]** > **[MAC]** > **[MAC プールの作成（Create MAC Pool）]** をクリックします。

[MAC Pool] ウィザードが表示されます。

ステップ 2 **[General]** ページで次の情報を追加します。

- **[Name]**：MAC プールの名前
- **Description**MAC プールの説明。
- **Organization**：MAC プールが属する組織。
- **[タグの追加（Add Tag）]**：MAC プールを識別して検索するためのタグ。

ステップ 3 **[次へ（Next）]** をクリックします。**[プール詳細（User Details）]** ページが表示されます。

ステップ 4 **[MAC Blocks]** 領域に次の設定情報を追加します。

- **[From]**：ブロック内の最初の MAC アドレスを示します。
- **[Size]**：ブロック内の MAC アドレスの数。

ステップ 5 ブロックを追加するには、**[+]** をクリックして、新しいブロックの開始 MAC アドレスと MAC アドレスの総数を追加します。

ステップ 6 **[作成（Create）]** をクリックします。

新しく作成された MAC プールが MAC プールのリストに表示されます。

MAC プールの詳細

詳細

MAC プールのリストを表示します。

プロパティ（Property）	基本情報（Essential Information）
[名前（Name）]	MAC プールの名前。
[サイズ（Size）]	プール内の MAC アドレスの数。

プロパティ（**Property**）	基本情報（**Essential Information**）
[使用済み（Used）]	プール内の使用済みのため使用不可能なMACアドレスの数。
予約済み	後で使用するために予約されているMACプール内の識別子の総数を表示します。
応対可	使用可能なMACプール内の識別子の総数を表示します。
[説明（Description）]	MAC プールの説明。
[最終更新（Last Update）]	MAC プールが最後に更新された日時。
設定	
移行前	プールの MAC プレフィックス値を表示します。 **Note** Cisco Intersight は、ID を順番に選択します。つまり、プールから使用可能な最も低い ID を選択します。
[保持数（To）]	プールのMACサフィックス値を表示します。
[サイズ（Size）]	MAC プール サイズを表示します。
使用量	
MAC アドレス、ステータス、サーバー プロファイルおよびソース（MAC Address, Status, Server Profile, and Source）]	MACアドレス、使用状況（予約済みまたは使用済み）、および関連するサーバー プロファイルを表示します。 Source は **Self** または **Other**にできます。ここで、 **Self** はこのプールによって使用または予約されている ID であり、 **Other** は静的にまたは別のプールによって使用または予約されている ID です。
[アクション（Actions）]	
[編集（Edit）]	MACプールの設定の詳細を追加または変更できます。
削除	MAC プールを削除できます。

UUID プール

Universally Unique Identifier (UUID) プールは、サーバーに割り当てられる UUID のコレクションです。UUID のプレフィックスとサフィックスは可変値です。UUID プールは、特定のプールを使用するサーバープロファイルに関連づけられた各サーバーについて、これらの変数が一意であることを保証して競合を回避します。

（注）

- サポートされているサーバーと、UUID プールに必要な最小ファームウェアまたは Cisco IMC バージョンを以下に示します。

サーバ	ファームウェアの最小バージョン
Cisco UCS-B200-M5、UCS-B480-M5、Cisco UCS UCS-B200-M6	4.2(1b)
Cisco UCS-C220-M6、UCS-C240-M6	4.2(1b)
Cisco UCS-C225-M6、UCS-C245-M6	4.2(1i)
Cisco UCSX-210C-M6	5.0(1a)

- UUIDプールを使用したサーバープロファイルの関連付けの詳細については、「サーバープロファイルの構成」を参照してください。

UUID プールの作成

UUID プールは、サーバー プロファイルに割り当てることができる UUID アイテムのコレクションを表します。

ステップ 1 左側のナビゲーションパネルで **[プール（Pools）]** > **[UUID]** > **[UUID プールの作成（Create UUID Pool）]** をクリックします。

[UUID プール(UUID Pool)] ウィザードが表示されます。

ステップ 2 **[全般（Genera）l]** ページで次の情報を追加します。

- **[組織（Organization）]**：UUID プールが属する組織。
- **[名前（Name）]**：UUID プールの名前。
- **[セット タグ（Set Tags）]**：UUID プールの識別と検索のためのオプションのタグ。
- **[説明（Description）]**：UUUD プールのオプションの説明。

ステップ 3 **[次へ（Next）]** をクリックします。**[プール詳細（User Details）]** ページが表示されます。

ステップ 4 **[構成（Configuration）]** セクションで、UUID プレフィックス番号を 16 進形式で追加します。例、1728E8C7-7B40-47E8

ステップ 5 **[UUID ブロック（UUID Blocks）]** セクションで、次の構成の詳細を追加します。

- **[開始（From）]**：ブロックの UUID サフィックス番号を 16 進形式で示します。例、9EDE-0E52924AC87A
- **[サイズ（Size）]**：このブロックの UUID 識別子の数を示します。範囲は 1 ～ 1000 です。

ステップ 6 さらにブロックを追加するには、**[+]** をクリックし、開始 UUID サフィックスと UUID 識別子の総数を新しいブロックに追加します。

ステップ 7 **[作成（Create）]** をクリックします。

新しく作成された UUID プールが UUID プールのリストに表示されます。

UUID プールの詳細

詳細

UUID プールのリストを表示します。

プロパティ（Property）	基本情報（Essential Information）
[詳細（Details）]	
[名前（Name）]	UUID プールの名前を表示します。
[タイプ（Type）]	プールのタイプを表示します。
[サイズ（サイズ）]	UUID プールに含まれる ID の総数を表示します。
[使用済み（Used）]	プールから既に使用されている UUID の数を表示します。
予約済み	後で使用するために予約されている UUID の総数を表示します。
[応答可能（Available）]	使用可能な UUID の数を表示します。
[最終更新（Last Update）]	UUID プールが最後に更新された日時。
説明	UUID プールの説明。
[組織（Organization）]	UUID プールが作成される組織を表示します。
コンフィギュレーション	
UUIDプレフィクス	プールの UUID プレフィックス値を表示します。

プロパティ（Property）	基本情報（Essential Information）
[先頭（From）]	プールのUUIDサフィックス値を表示します。 **Note** Cisco Intersight は、ID を順番に選択します。つまり、プールから使用可能な最も低い ID を選択します。
[保持数（To）]	ブロック サイズの範囲を表示します。 **Note** この値は、UUID プール サイズ プロパティに依存します。
[サイズ（Size）]	UUID プール サイズを表示します。
使用量	
UUID、ステータス、サーバー プロファイル、およびソース	サーバー プロファイルに割り当てられた UUID、使用状況（予約済みまたは使用済み）、および関連するサーバー プロファイルを表示します。 ソース（Source）は **セルフ（Self）** または **その他（Other）**にできます。ここで、 **セルフ（Self）** はこのプールによって使用または予約されている ID であり、 **その他（Other）** は静的にまたは別のプールによって使用または予約されている ID です。

WWN プール

World Wide Name（WWN）プールは、Cisco UCS ドメイン内のファイバチャネル vHBA で使用される WWN の集合です。次の独立したプールを作成します。

- サーバに割り当てられる WW ノード名
- サーバに割り当てられる WW ポート名

（注） WWN ID は、WWPN および WWNN プール間で再利用できません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするために、Cisco Intersight では、プールのすべてのブロックに WWN プレフィックス20:00:00:25:B5:xx:xx:xx を使用します。

サーバ プロファイルで WWN プールを使用する場合は、サーバ プロファイルに関連付けられたサーバで使用される WWN を手動で設定する必要はありません。複数のテナントを実装する

システムでは、WWN プールを使用して、各組織で使用される WWN を制御できます。WWN をブロック単位でプールに割り当てます。

WWNN プール

WWNNプールは、WWノード名だけを含むWWNプールです。サーバプロファイルにWWNNのプールを含める場合、関連付けられたサーバには、そのプールから WWNN が割り当てられます。

WWPN プール

WWPNプールは、WWポート名だけを含むWWNプールです。サーバプロファイルにWWPNプールを含めると、関連付けられているサーバの各 vHBA のポートには、そのプールから WWPN が割り当てられます。

WWNN プールの作成

SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするために、Cisco Intersight では、プールのすべてのブロックに WWN プレフィックス20:00:00:25:B5:xx:xx:xx を使用します。

ステップ 1 左側のナビゲーションパネルで、**[プール（Pools）]** > **[WWNN]** > **[WWNN プールの作成（WWNN Pool）]** をクリックします。

[WWNN Pool] ウィザードが表示されます。

ステップ 2 **[General]** ページで次の情報を追加します。

- **Name**：WWNN プールの名前
- **Description**WWNN プールの説明。
- **Organization**：WWNN プールが属する組織のオプション エントリ。
- **[タグの追加（Add Tag）]**：WWNN プールを識別して検索するためのタグ。

ステップ 3 **[次へ（Next）]** をクリックします。**[プール詳細（User Details）]** ページが表示されます。

ステップ 4 **[イニシエータ ブロック（Initiator Blocks）]** 領域に次の設定情報を追加します。

- **[開始（From）]**：ブロックの最初の WWN ID を示します。
- **[サイズ（Size）]**：ブロックに含めることができる識別子の最大数を示します。

ステップ 5 ブロックを追加するには、**[+]** をクリックし、ブロックに含めることができる開始 WWN ID と ID の最大数を追加します。

ステップ 6 **[作成（Create）]** をクリックします。

新しく作成された WWNN プールが WWNN プールのリストに表示されます。

WWNN プールの詳細

詳細

WWNN プールのリストを表示します。SAN ファブリックで Cisco UCS WWN の一意性を確保するために、20:00:00:25:b5:0:00:01 という形の WWN プレフィックスを使用することをお勧めします。

プロパティ（Property）	基本情報（Essential Information）
[名前（Name）]	WWNN プールの名前
[サイズ（Size）]	プール内の WWNN の総数。
[使用済み（Used）]	プール内で使用済みのため使用できない WWNN の数。
予約済み	後で使用するために予約されているプール内の WWNN の総数を表示します。
応対可	使用可能なプール ハット内の WWNN の総数を表示します。
[説明（Description）]	WWNN プールの説明。
[最終更新（Last Update）]	WWNN プールが最後に更新された日時。
設定	
移行前	プールの WWNN プレフィックス値を表示します。 **Note** Cisco Intersight は、ID を順番に選択します。つまり、プールから使用可能な最も低い ID を選択します。
[保持数（To）]	プールの WWNN サフィックス値を表示します。
[サイズ（サイズ）]	WWNN プール サイズを表示します。
Usage	

プロパティ（**Property**）	基本情報（**Essential Information**）
識別子、ステータス、サーバープロファイル、およびソース	WWNN、使用状況(予約済みまたは使用済み)、および関連するサーバー プロファイルを表示します。 Source は **Self** または **Other**にできます。ここで、 **Self** はこのプールによって使用または予約されている ID であり、 **Other** は静的にまたは別のプールによって使用または予約されている ID です。
[アクション（Actions）]	
[編集（Edit）]	WWNN プールの構成の詳細を追加または変更できます。
削除	WWNN プールを削除できます。

WWPN プールの作成

SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするために、Cisco Intersight では、プールのすべてのブロックに WWN プレフィックス20:00:00:25:B5:xx:xx:xx を使用します。

ステップ 1 左側のナビゲーションパネルで、**[プール（Pools）]** > **[WWNN]** > **[WWPN プールの作成（WWPN Pool）]** をクリックします。

[WWPN プール（WWPN Pool）] ウィザードが表示されます。

ステップ 2 **[全般（Genera）l]** ページで次の情報を追加します。

- **[名前（Name）]**：WWPN プールの名前
- **[説明（Description）]**：WWPN プールの説明。
- **[組織（Organization）]**：WWPN プールが属する組織のエントリ（オプション）。
- **[タグの追加（Add Tag）]**：WWPN プールを識別して検索するためのタグ。

ステップ 3 **[次へ（Next）]** をクリックします。**[プール詳細（User Details）]** ページが表示されます。

ステップ 4 **[イニシエータブロック（Initiator Blocks）]** 領域に次の設定情報を追加します。

- **[開始（From）]**：ブロックの最初の WWN ID を示します。
- **[サイズ（Size）]**：ブロックに含めることができる識別子の最大数を示します。

ステップ 5 ブロックを追加するには、**[+]** をクリックし、ブロックに含めることができる開始 WWN ID と ID の最大数を追加します。

ステップ 6 **[作成（Create）]** をクリックします。

新しく作成された WWPN プールが WWPN プールのリストに表示されます。

WWPN プールの詳細

詳細

WWPN プールのリストを表示します。SAN ファブリックで Cisco UCS WWPN の一意性を確保するために、20:00:00:25:b5:0:00:01 という形の WWN プレフィックスを使用することをお勧めします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[名前（Name）]	ワールドワイドポート名（WWPN）プールの名前。
[サイズ（サイズ）]	プール内の WWPN の総数。
[使用済み（Used）]	プール内で使用済みのため使用できない WWPN の数。
[説明（Description）]	WWPN プールの説明。
[最終更新（Last Update）]	WWPN プールが最後に更新された日時。

IQN プール

IQN プールは、iSCSI vNIC によってイニシエータ ID として使用される iSCSI 修飾名（IQN）の集合です。IQN プール メンバの形式は、*prefix: suffix: number* であり、接頭辞、接尾辞、および番号のブロック（範囲）を指定できます。

IQN プールには、番号の範囲やサフィックスが異なる（ただし、プレフィクスは共通している）複数の IQN ブロックを含めることができます。

IQN プールの作成

IQN プールは、イニシエータ ID として使用される iSCSI 修飾名（IQN）の集合です。IQN プールの詳細は、IQN 識別子のブロックを設定するために使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	左側のナビゲーションパネルで、[プールの作成（Create Pools）] > [IQN] > [開始（Start）]をクリックします。	[IQN プール（IQN Pool）] ウィザードが表示されます。

	コマンドまたはアクション	目的
ステップ 2	**[全般（Genera）l]**ページで次の情報を追加します。 • **[組織（Organization）]**：IQN プールの組織。 • **[名前（Name）]**：IQN プールの名前。 • **[タグの追加（Add Tag）]**：IQN プールを識別して検索するためのタグ。 • **[説明（Description）]**：IQN プールの説明。	
ステップ 3	**[次へ（Next）]** をクリックします。**[プール詳細（User Details）]** ページが表示されます。	
ステップ 4	**[設定（Configuration）]** 領域で、IQN プールに関する次の設定情報を追加します。 • **[プレフィックス（Prefix）]**：このプール用に作成された IQN ブロックのプレフィックス。IQN プレフィックスは「iqn-yyyy-mm.<命名機関>」の形式にする必要があります。通常、命名機関は、命名機関のインターネットドメインの逆構文です。例、iqn1.2021-01.alpha.com • **[サフィックス（Suffix）]**：IQN のこのブロックのサフィックス。 1 ～ 64 文字を入力します。任意の文字や数字、および次の特殊文字を使用できます：（ピリオド）、:（コロン）、-（ハイフン）。 • **[開始（From）**：ブロック内の最初の iSCSI Qualified Name（IQN）サフィックス。 • **[サイズ（Size）]**：このブロックが保持できる識別子の数。	

新しく作成された IQN プールが IQN プールのリストに表示されます。

IQN プールの詳細

詳細

IQN プールのリストを表示します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[詳細（Details）]	
[名前（Name）]	IQN プールの名前を表示します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[タイプ（Type）]	プールのタイプを表示します。
[サイズ（サイズ）]	IQN プールに含まれる識別子の総数を表示します。
[使用済み（Used）]	プールから既に使用されている識別子の数を表示します。
予約済み	後で使用するために予約されている識別子の総数を表示します。
応対可	使用可能な識別子の数を表示します。
[説明（Description）]	IQN プールの説明。
[最終更新（Last Update）]	IQN プールが最後に更新された日時。
[組織（Organization）]	[デフォルト（Default）]組織のユーザは、ユーザアカウントで使用可能なすべてのリソースにアクセスできます。
[タグ（Tags）]	プールのタグを表示します。
[設定（Configuration）]	
[プレフィックス（Prefix）]	このプール用に作成された IQN ブロックのプレフィックスを表示します。
[サフィックス（Suffix）]	この IQN ブロックのサフィックスを表示します。
[先頭（From）]	ブロック内の最初の接尾辞番号。 （注） Cisco Intersight は、ID を順番に選択します。つまり、プールから使用可能な最も低い ID を選択します。
[保持数（To）]	ブロックが保持できる識別子の数。
[使用（Usage）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
IQN アドレス、ステータス、サーバー プロファイルおよびソース（IQN Address, Status, Server Profile, and Source）]	IQN アドレス、使用状況（予約済みまたは使用済み）、および関連するサーバー プロファイルを表示します。 Source は **Self** または **Other**にできます。ここで、 **Self** はこのプールによって使用または予約されている ID であり、 **Other** は静的にまたは別のプールによって使用または予約されている ID です。
[アクション（Actions）]	
[編集（Edit）]	IQN プールの設定の詳細を追加または変更できます。
[削除（Delete）]	IQN プールを削除できます。

リソース プール

プールを使用すると、リソース（サーバーおよびその他のエンドポイント）をより効率的に論理的にグループ化し、管理することができます。サーバーをリソース プールに割り当て、サーバー プロファイルの自動割り当てを続行できます。リソース プールを使用したサーバー プロファイルの関連付けの詳細については、「サーバー プロファイルの構成」を参照してください。

永続的なリソース プールの割り当て

プールの一部であるサーバーがデコミッションされると、**[リソース プールの詳細（Resource Pool Details）] ビュー** および **[サーバーの詳細（Server Details）] ビュー** の **[デコミッションされたリソース（Decommissioned Resources）]** セクションに表示されます。サーバーが再稼働すると、同じプールに再度割り当てられます。サーバーを停止し、別のシャーシまたはスロットに移動してから再稼働した場合も、同じ動作が発生します。したがって、展開環境で物理的な変更が発生した場合に、そのサーバーのプールの再割り当てを管理する必要はありません。

（注） 既存のリソース プールを永続的なリソース プールに変換するには、[リソース プール（Resource Pool）] を編集します。

API または Terraform ユーザーの動作の変更

API または Terraform ユーザーは、API を使用して、管理対象オブジェクト ID（MOID）またはシリアル セレクタを使用して新しいリソース プールを作成できます。

ただし、API ユーザーが UI から MOID を使用するリソース プールを編集して、永続的なリソース プールの割り当てを有効にすると、システムはこれらの MOID セレクタをシリアル セ

レクタに内部的に変換し、MOID は API を介してアクセスできなくなります。リソース プールを作成するためのペイロードの詳細については、 API ドキュメントを参照してください。

（注） リソースプールの編集オプションを使用する際、リースがアクティブであるリソースはリソース プールから削除できません。

リソース プールの作成

リソース プールは、サーバー プロファイルなどの設定エンティティに割り当てることができるリソース アドレスの集合を表します。

ステップ 1 左側のナビゲーションパネルで、**[プールの作成（Create Pools）]**>**[リソース（Resource）]**>**[開始（Start）]** をクリックします。

[リソース プール（Resource Pool）] ウィザードが表示されます。

ステップ 2 **[全般（Genera）l]** ページで次の情報を追加します。

- **[組織（Organization）]**：リソース プールの組織。
- **[名前（Name）]**：リソース プールの名前。
- **[ターゲット プラットフォーム（Target Platform）]**：UCS スタンドアロン サーバーまたは UCS FI アタッチ サーバーとしてのターゲット プラットフォーム タイプ。
- **[セット タグ（Set Tags）]**：リソース プールを識別して検索するためのタグ。
- **[説明（Description）]**：リソース プールの説明。

ステップ 3 [次へ（Next)] をクリックします。**[リソース プールの詳細（Resource Pool Details）]** ページに、ターゲット プラットフォーム タイプに基づいて検出されたサーバーのリストが表示されます。

ステップ 4 **[リソース選択（Resource Selection）]** テーブルからサーバーを選択します。

ステップ 5 **[作成（Create）]** をクリックします。

新しく作成されたリソース プールがリソース プールのリストに表示されます。

リソース プールの詳細

[詳細（Details）] - リソース プールの詳細を表示します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[詳細（Details）]	
[名前（Name）]	リソース プールの名前を表示します。
[タイプ（Type）]	プールのタイプを表示します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[サイズ（サイズ）]	リソース プールに含まれるリソースの総数を表示します。
[使用済み（Used）]	使用済みで使用できないリソースの数を表示します。
[応答可能（Available）]	使用可能なリソースプールの数を表示します。
[最終更新（Last Update）]	リソース プールが最後に更新された日時。
リソース	
タイプ（Type）	リソース プールのタイプを表示します。 （注） 現在、Intersightは、リソース プールのリソースとしてサーバー タイプのみをサポートしています。
選択項目	リソース プールの選択タイプを表示します。現在、手動（静的）選択のみがサポートされています。
ターゲットプラットフォーム	ターゲット名を表示します。これには、次のいずれかがあり得ます。 • スタンドアロン • FI接続
説明	リソース プールの説明。
[組織（Organization）]	リソース プールが作成される組織を表示します
コンフィギュレーション （注） リソース プールの構成プロパティは、関連付けられているリソース タイプによって異なります。	
ステータス（Status）	リソースの状態を表示します。次のいずれかが考えられます。 • [使用可能（Available）] — リソースが使用可能であることを示します。 • [使用済み（Used）] — リソースがリソース プールですでに使用されていることを示します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[デコミッションされたリソース（**Decommissioned Resources**）]：このセクションには、デコミッションされたサーバーの詳細が表示されます。 （注） このセクションは、サーバーがデコミッションされ、すでにリソースプールの一部になっている場合にのみ表示されます。	
名前	デコミッションされたサーバーの名前を表示します。
[タイプ（Type）]	サーバーが Cisco UCS C シリーズ サーバーか Cisco UCS B シリーズ サーバーかを表示します。
ID	デコミッションされたサーバーに割り当てられた一意の ID を表示します。このフィールドは、Cisco UCS C シリーズ サーバーにのみ適用されます。
モデル（Model）	サーバーのモデルを表示します。
シリアル番号	サーバーのシリアル番号を表示します。
廃止日	サーバーがデコミッションされたときのタイム スタンプを表示します。
[使用（Usage）]	
リソース名（Resource Name）	リソース名を表示します。
リースエンティティ	構成エンティティを表示します。 （注） リソースはさまざまなプールの一部にすることができますが、1 つのリースエンティティにのみ関連付けることができます。
使用例	リソースのコンシューマーを表示します。例、サーバー プロファイル。

[プロパティ（Property）]	[基本情報（Essential Information）]
リソース使用状況	リソース消費タイプを表示します。次のタイプがあります。 • 現在（Current） — リソースは、現在のリソース プールに関連付けられて使用されています。 • 他のプール（Other Pool） — リソースは他のプールに関連付けられて使用されています。 • 直接（Direct） — リソースは、リソース プールを使用せずにサーバー プロファイルに直接関連付けられます。

（注） リソース プールの編集オプションを使用する際、リースがアクティブであるリソースはリソース プールから削除できません。

仮想ルーティングおよび転送

仮想ルーティングおよびフォワーディング（VRF）は、同じルータ上で同時に複数のインスタンスのルーティング テーブルを共存させるための IP テクノロジーです。ルーティング インスタンスが互いに独立しているため、同じ（重複する）IP アドレスを競合することなく使用できます。VRF は、IP アドレス管理用の名前空間を作成します。Cisco Intersight では、IP プールは VRF に対応しています。

VRF ガイドライン

VRF インスタンスには、次の注意事項と制限が適用されます。

- Intersight は、アカウントのデフォルト VRF を作成し、このデフォルト VRF のコンテキスト内で IP アドレスの割り当てを管理します。
- 単一の VRF インスタンス内では、各 IP アドレスが一意である必要があります。異なる VRF インスタンス間では IP アドレスが重複してもかまいません。
- VRF インスタンス間で IP プールを共有する場合は、IP アドレスが重複していないことを確認してください。

VRF インスタンスの作成

仮想ルーティングおよびフォワーディング（Virtual Routing and Forwarding、VRF）は、単一のネットワーク エンティティ内に複数の仮想ネットワークを作成する技術です。

ステップ 1 左側のナビゲーションパネルで、**[仮想ルーティングおよびフォワーディング（Virtual Routing And Forwarding）]** > **[VRFs]** > **[VRF の作成（Create VRF）]** をクリックします。

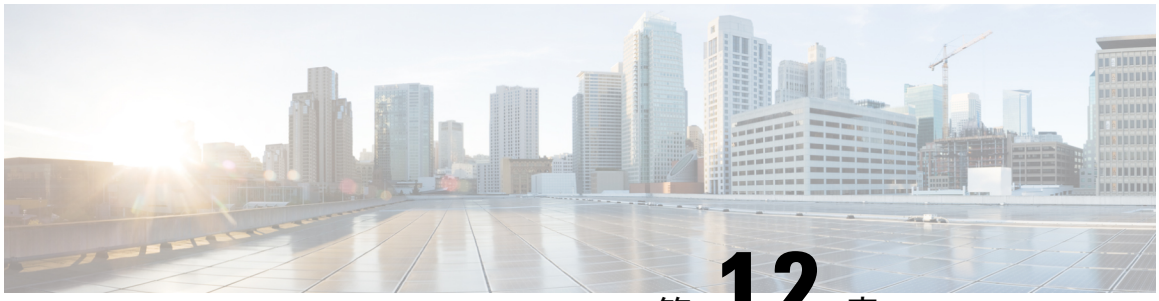
[VRF] ウィザードが表示されます。

ステップ 2 **[全般（Genera）l]** ページで次の情報を追加します。

- **[名前（Name）]**：VRF インスタンスの名前。
- **[説明（Description）]**：VRF インスタンスの説明（オプション）。
- **[組織（Organization）]**：VRF インスタンスが属する組織（オプション）。
- **[タグの追加（Add Tag）]**：VRF プールを識別して検索するためのタグ。

ステップ 3 **[作成（Create）]** をクリックします。

新しく作成された VRF インスタンスが VRF のリストに表示されます。



第 12 章

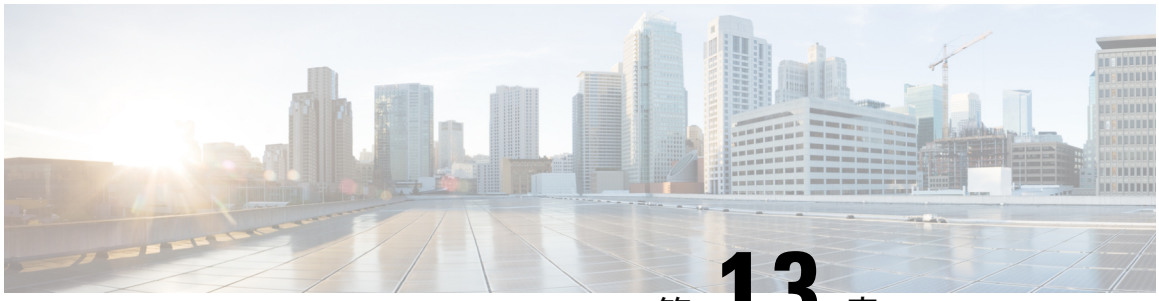
デバイス コンソールの管理

• デバイス コンソール （353 ページ）

デバイス コンソール

ファブリック インターコネクトにインストールされているデバイス コンソールを使用すると、デバイスの正常性と、各デバイスから Intersight への接続ステータスを監視できます。デバイスをトラブルシューティングする場合、またはデバイスが Cisco Intersight に接続されていない場合は、デバイス コンソール GUI または CLI インターフェイスを使用できます。

デバイス コンソールのユーザー インターフェイスにアクセスするには、管理 IP アドレスを使用してファブリック インターコネクトにログインします。デバイス コンソール UI にアクセスするには、管理者権限が必要です。詳細については、『Cisco Intersight に管理モード ファブリック インターコネクト管理ガイド』を参照してください。



第 13 章

ファームウェアの管理

- Intersight を使用した Cisco UCS ドメインでのファームウェアアップグレード （355 ページ）
- ファブリック インターコネクト ファームウェアのアップグレード （358 ページ）
- サーバ ファームウェアのアップグレード （360 ページ）
- RMA でのサーバおよびファブリック インターコネクトのアップグレードおよび交換 （362 ページ）

Intersight を使用した Cisco UCS ドメインでのファームウェアアップグレード

次のいずれかのアップグレードオプションを選択して、Cisco Intersight から Cisco UCS ドメインのさまざまなコンポーネントのファームウェアをアップグレードできます。

ファブリックファームウェアのアップグレード

このプロセスにより、2 つのファブリックインターコネクトと I/O モジュールを含む、Cisco UCS ドメイン内のすべてのファブリックコンポーネントをアップグレードできます。これらのコンポーネントは、選択したファブリック ファームウェア バンドルに含まれるファームウェアバージョンにアップグレードされます。ファブリック ファームウェアのアップグレードは、Cisco UCS ドメインの一部のコンポーネントだけを対象にした、部分アップグレードをサポートしていません。1ファブリックファームウェアのアップグレードプロセスは、Cisco UCS 6400 シリーズファブリックインターコネクトでのみ有効です。

ファブリックファームウェアバンドルは Cisco Intersight リポジトリで入手でき、2 つのコンポーネントイメージがあります。

- NXOS イメージ
- CMC イメージ

次のワークフローは、ファブリックファームウェアのアップグレードプロセスを示しています。

1. **ファブリックの選択**：ファブリックインターコネクトを選択し、ファームウェアのアップグレードアクションを実行することで、ファブリック**ファームウェアのアップグレード**プロセスを開始できます。ファブリックインターコネクトは常にペアとしてアップグレードされ、ファブリックインターコネクトAの前にファブリックインターコネクトBがアップグレードされます。
2. **バンドルの選択**：アップグレードするファブリックインターコネクトペアを選択した後、ファブリックインターコネクトをアップグレードする必要があるファブリックファームウェアバンドルを選択する必要があります。ファームウェア選択画面には、使用可能なファームウェアバンドルのリストと、それらのファームウェアバージョン、サイズ、リリース日、および説明に関する情報が表示されます。選択したファームウェアバンドルがCisco Intersight のレポジトリからダウンロードされます。
3. **影響の推定**：[概要（Summary）] 画面には、選択したスイッチの概要、スイッチで実行されているファームウェアバージョン、およびアップグレード先のファームウェアバージョンが表示されます。**[アップグレード（Upgrade）]**をクリックしてアップグレードするか、**[戻る（Back）]** をクリックして設定を変更するかを選択できます。
4. **アップグレード要求の送信**：**[アップグレード（Upgrade）]**,をクリックした後、アップグレード要求を確認します。

次のワークフローは、アップグレード要求を送信した後に自動的に実行されるタスクを示しています。

1. システムは、ファームウェアバンドルに十分なストレージ領域があるかどうかを検証します。ファブリックインターコネクトのスペースが不足している場合、アップグレードは失敗します。
2. 選択したファームウェアバンドルがすでにファブリックインターコネクトキャッシュにあるかどうかがチェックされます。ファームウェアバンドルが存在しない場合は、ファブリックインターコネクトキャッシュにダウンロードされます。
3. 両方の IO モジュールが更新され、接続されているすべてのシャーシでアクティブ化されます。IO モジュールの再起動時に IO モジュールのアップグレードが完了します。
4. **[続行（Continue）]** をクリックして、ファブリックインターコネクトB のファームウェアアップグレードを確認し、開始します。ファブリックインターコネクトBのアップグレードが完了すると、ファブリックインターコネクトがリブートし、新しいイメージが表示されます。IOM-BがファブリックインターコネクトBとともにリブートされ、アップグレードされたイメージが表示されます。
5. **[続行（Continue）]** をクリックして、ファブリックインターコネクトA のファームウェアアップグレードを確認し、開始します。ファブリックインターコネクトAのアップグレードが完了すると、ファブリックインターコネクトがリブートし、新しいイメージが表示されます。IOM-AがファブリックインターコネクトAとともにリブートされ、アップグレードされたイメージが表示されます。

ホスト ファームウェア アップグレード

このプロセスにより、Intersight 管理モードの Cisco UCS B シリーズおよび C シリーズ FI 接続サーバのすべてのサーバコンポーネントをアップグレードできます。これらのコンポーネントは、選択したホスト ファームウェア バンドルに含まれるファームウェア バージョンにアップグレードされます。

サーバファームウェアバンドルは Cisco Intersight リポジトリで入手でき、次のコンポーネントイメージがあります。

- CIMC イメージ
- BIOS イメージ
- ネットワーク アダプタ イメージ

（注） UCS VIC 1400 シリーズアダプタのみがサポートされます。

- ストレージ コントローラ イメージ
- ボード コントローラ イメージ
- ディスク イメージ
- GPU イメージ
- メモリカードイメージ
- M-Switch および PLX イメージ

次のワークフローは、ホストファームウェアのアップグレードプロセスを示しています。

1. **サーバの選択**：サーバを選択し、そのサーバで**[ファームウェアのアップグレード（Upgrade Firmware）]** アクションを実行することで、ホストファームウェアのアップグレードプロセスを開始できます。
2. **バンドルの選択**：アップグレードするサーバを確認した後、サーバをアップグレードする必要があるホストファームウェアバンドルを選択する必要があります。ファームウェア選択画面には、使用可能なファームウェアバンドルのリストと、それらのファームウェアバージョン、サイズ、リリース日、および説明に関する情報が表示されます。選択したファームウェア バンドルが Cisco Intersight レポジトリからダウンロードされます。
3. **影響の推定**：[概要（Summary）] 画面には、選択したサーバの概要、サーバで実行されているファームウェアバージョン、およびアップグレード先のファームウェアバージョンが表示されます。**[アップグレード（Upgrade）]** をクリックしてアップグレードするか、**[戻る（Back）]**.をクリックして、ファームウェアバージョンを変更するかを選択できます。
4. **アップグレード要求の送信**：**[アップグレード（Upgrade）]** をクリックした後、ファームウェアをすぐにインストールするか、デバイスを再起動するかを選択します。アップグレードのリクエストを確認します。

デフォルトでは、ファームウェアはデバイスの次回起動時にインストールされます。

次のワークフローは、アップグレード要求を送信した後に自動的に実行されるタスクを示しています。

1. システムは、ファームウェアバンドルに十分なストレージ領域があるかどうかを検証します。ファブリックインターコネクトのスペースが不足している場合、アップグレードは失敗します。
2. 選択したファームウェアバンドルがすでにファブリックインターコネクトキャッシュにあるかどうかがチェックされます。ファームウェアバンドルが存在しない場合は、ファブリックインターコネクトキャッシュにダウンロードされます。
3. サーバファームウェアは次のようにアップグレードされます。
   - B シリーズ サーバ:
     1. アダプタファームウェアが更新され、アクティブになります。サーバの再起動時にアダプタのアップグレードが完了します。
     2. Host Service Utility（HSU）は、ただちにアップグレードされるか、サーバがリブートされたときにアップグレードされます。
     3. すべてのサーバコンポーネントがアップグレードされます。
   - C シリーズ サーバ:
     1. HSU は、ただちに、またはサーバの再起動時にアップグレードされます。
     2. すべてのサーバコンポーネントがアップグレードされます。
4. **[続行（Continue）]** をクリックして確認し、ファームウェアアップグレードを開始します。

ファブリックインターコネクトファームウェアのアップグレード

Cisco Intersight を使用して、Intersight マネージド ファブリック インターコネクトをアップグレードできます。

始める前に

Intersight 管理ファブリック インターコネクト ファームウェアをアップグレードする前に、次の前提条件を考慮してください。

- Cisco UCS ドメイン内の Cisco UCS 6400 シリーズ ファブリック インターコネクトのみをアップグレードできます。

- ファームウェア バンドルをダウンロードするには、ファブリック インターコネクト パーティションに少なくとも次の使用可能なストレージが必要です。
  - /var/tmp に 90％の 空き領域
  - /va /sysmgr に 20％ の空き領域
  - /mnt/pss に 30％ の空き領域
  - /bootflash に 18％ の空き領域
- Intersight を介して要求された Cisco UCS ドメインのみをアップグレードできます。
- Cisco UCS ドメイン内のすべてのサーバは、Essentials 以上のライセンス階層である必要があります。

ステップ 1 左側のナビゲーション ペインで、**[ファブリック インターコネクト（Fabric Interconnects）]** をクリックし、ファブリック インターコネクトを選択して、**[ファームウェアのアップグレード（Upgrade Firmware）]** アクションを実行します。

ステップ 2 **[ファームウェアのアップグレード（Upgrade Firmware）]** ページで、**[開始（Start）]** をクリックします。

ステップ 3 **[全般（General）]** ページで、スイッチ ドメインの選択を確認し、**[次へ（Next）]** をクリックします。

ステップ 4 **[バージョン（Version）]** ページで、ファブリック インターコネクトをアップグレードするファブリック ファームウェア バンドルを選択し、**[次へ（Next）]** をクリックします。

このページには、使用可能なファームウェア バンドルのリストと、そのファームウェア バージョン、サイズ、リリース日、および説明に関する情報が表示されます。選択したファームウェア バンドルが Intersight のレポジトリからダウンロードされます。

Intersightの管理対象のファブリック インターコネクトのアップグレード中には、ファブリック インターコネクト トラフィックの待避はデフォルトで有効になります。ファブリック インターコネクト トラフィックの待避では、システムのアップグレードの間、ファブリック インターコネクトに接続されているすべてのサーバからファブリック インターコネクトを通るすべてのトラフィックを待避します。トラフィックはフェールオーバー vNIC のピア ファブリック インターコネクトにフェールオーバーします。ファブリック インターコネクトでのトラフィック待避の前に、ユーザはピア ファブリック インターコネクトでのリプレイが完了し、すべての vEth が起動していることを確認する必要があります。NXOS からそれぞれの vEth の vEth ステータスを確認するには、*[インターフェイスの仮想ステータスを表示（show interface virtual status）]* コマンドを使用します。

トラフィックの退避の前に、ホスト インターフェイス（HIF）の送信（Tx）および受信（Rx）統計情報を表示して、ファブリック インターコネクトを通過するトラフィックを確認できます。トラフィックの退避後、ネットワーク インターフェイス（NIF）の送信（Tx）および受信（Rx）統計情報を表示して、ファブリック インターコネクト（FI）を通過するトラフィックを確認できます。

（注） ファブリック インターコネクト トラフィックの退避を機能させるには、LAN 接続ポリシーで vNIC フェールオーバーを有効にする必要があります。

ファブリック インターコネクト トラフィックの退避をディセーブルにするには、**拡張モード**を選択します。

ステップ 5 **[サマリー（Summary）]** 画面で、選択したスイッチのサマリー、スイッチで実行されているファームウェア バージョン、およびアップグレード先のファームウェア バージョンを確認し、**[アップグレード（Upgrade）]** をクリックします。

[戻る（Back）] をクリックして、ファームウェア バージョンを変更できます。

ステップ 6 アップグレードのリクエストを確認します。

ファームウェア アップグレード ワークフローが開始されます。**[実行フロー（Execution Flow）]** ペインでアップグレードワークフローのステータスを確認できます。**[実行フロー（Execution Flow）]** ペインのメッセージを確認し、**[続行（Continue）]** をクリックしてアップグレードを続行します。

サーバ ファームウェアのアップグレード

始める前に

サーバをアップグレードする前に、次の前提条件を考慮してください。

- アップグレードできるのは、Intersight 経由で要求された Cisco UCS B シリーズ M5、M6、M8 および C シリーズ M5、M6、M7、および X シリーズ M6 と M7 サーバのみです。
- サーバーは、少なくとも Cisco UCS HSU バンドルリリースバージョン 4.1（2a）からアップグレードできます
- Cisco UCS ドメイン内のすべてのサーバーは、ライセンス階層が Essentials 以上である必要があります

ステップ 1 左側のナビゲーションペインで、**[サーバ（Servers）]** をクリックしてサーバを選択し、**ファームウェアのアップグレード** アクションを実行します。

（注） 複数のサーバをアップグレードするには、次の手順を実行します。

- 複数のサーバをアップグレードするには、選択したサーバが同じモデルと管理モードであることを確認します。有効な選択の例を次に示します。
  - 1 台以上の B200 M5 サーバ
  - 1 台以上の C220 M5 サーバ

  無効な選択の例を次に示します。
  - C220 M5 および C240 M5 サーバ
  - C220 M5 および B200 M5 サーバ
- アップグレードするすべてのサーバーを選択し、リストビューの下部にあるその他のメニューをクリックして、それらのサーバーに対して **[ファームウェアのアップグレード（Upgrade Firmware）]** アクションを実行します。

ステップ 2 **[ファームウェアのアップグレード（Upgrade Firmware）]** ページで、**[開始（Start）]** をクリックします。

ステップ 3 **[全般（General）]** ページで、サーバの選択を確認し、**[次へ（Next）]** をクリックします。

ステップ 4 **[バージョン（Version）]** ページで、サーバをアップグレードする必要がある Cisco UCS HSU バンドルを選択し、**[次へ（Next）]** をクリックします。

このページには、使用できるファームウェアバンドルの一覧と、そのファームウェアのバージョン、サイズ、リリース日、ファームウェアの説明が表示されます。選択したファームウェアバンドルがシスコのリポジトリからダウンロードされます。デフォルトではドライブコントローラやストレージコントローラを含むすべてのサーバコンポーネントがアップグレードされます。

一部のドライブやストレージ コントローラをアップグレードから除外するには、**[アドバンスト モード（Advanced Mode）]** を選択します。

ステップ 5 **[概要（Summary）]** 画面で、選択したサーバの概要、サーバで実行されているファームウェアバージョン、およびアップグレード先のファームウェアバージョンを確認します。

[戻る（Back）] をクリックして、設定を変更できます。

ステップ 6 **[アップグレード（Upgrade）]** をクリックします。

ステップ 7 **[ファームウェアのアップグレード（Upgrade Firmware）]** ダイアログボックスで、次のいずれかのオプションを選択します。

a) **[直ちにリブートしてアップグレードを開始（Reboot Immediately To Begin Upgrade）]** デフォルトでは、次回の起動時にサーバファームウェアがアップグレードされます。すぐにリブートしてファームウェアのアップグレードを開始する場合は、このオプションを有効にします。

b) **[アップグレード（Upgrade）]** をクリックして、アップグレード要求を確認します。

ファームウェア アップグレード ワークフローが開始されます。**[実行フロー（Execution Flow）]** ペインでアップグレードワークフローのステータスを確認できます。**[実行フロー（Execution Flow）]** ペインのメッセージを確認し、**[続行（Continue）]** をクリックしてアップグレードを続行します。

RMAでのサーバおよびファブリックインターコネクトのアップグレードおよび交換

RMA のアップグレード

RMA はカスタマー エクスペリエンスを向上させる返品許可プロセスです。

RMA でのサーバのアップグレード

新しいブレード サーバを挿入するか、古いブレード サーバを交換すると、RMA プロセスによって自動検出ワークフローがトリガーされます。ブレードサーバのファームウェアが古い場合、検出ワークフローによってアラームが発生し、アップグレードワークフローをトリガーするように求められます。

1. **[シャーシ（Chassis）]**、**[インベントリ（Inventory）]**、**[サーバー（Servers）] の順**に選択します。
2. アップグレードするサーバをセレクトします。
3. [アップグレード] をクリックします。
4. サーバをアップグレードするためのファームウェアのバージョンを選択します。

Cisco IMC やアダプタなどの関連するエンドポイントはアップグレードされて、サーバが Intersight 管理モードで起動し、サーバ リスト ページで利用可能になり、使用できるようになります。標準のファームウェア アップグレード方法を使用して、残りのエンドポイントをアップグレードできます。

（注） CMC バージョンは 4.1（3b）以降である必要があります。

RMA サポートは、Intersight 管理モードの FI 接続の C シリーズ サーバーでは利用できません。まず、IMM の C シリーズ サーバをスタンドアロン モードに変換し、ファームウェアを確認してから、HUU を使用してアップグレードする必要があります。

サーバーを IMM からスタンドアロン モードに変換するには、「Intersight 管理モードのサーバーをスタンドアロン モードに変換する（Converting a Server in Intersight Managed Mode to Standalone Mode）」を参照してください。

詳細については、UCS C シリーズ スタンドアロン サーバー ファームウェアのアップグレードおよびUCS C シリーズ スタンドアロン サーバー ファームウェアのアップグレード（Upgrading UCS C-Series Standalone Servers Firmware）]を参照してください。

RMA でのファブリック インターコネクトの交換

単一のファブリック インターコネクトまたはファブリック インターコネクト クラスタに問題があり、同じモデルのファブリック インターコネクトが交換された場合、古いファブリック インターコネクトの設定を新しいファブリック インターコネクトに移行するために [交換（Replace）]オプションを使用できます。単一のファブリックインターコネクトとファブリック インターコネクトクラスタの両方を交換するワークフローについては、以降の項で詳しく説明します。

Cisco UCS 6400 シリーズの単一のファブリック インターコネクトと Cisco UC5 6500 シリーズのファブリック インターコネクトの置き換え

1. 古いファブリック インターコネクトを取り外し、同じモデルの新しいファブリック インターコネクトを接続します。
2. サーバ、FEX ファブリック、およびブレードシャーシを含むすべてのケーブル接続を、古いファブリック インターコネクトから新しいファブリック インターコネクトに移動します。
3. 「置換」アクションをトリガーする前に、クラスタに参加するように新しいモジュールを設定します。
4. **[操作] > [ファブリック インターコネクト]** に移動して、交換されたファブリック インターコネクトのリストを表示し、「交換」オプションが有効になっているファブリック インターコネクトを特定します。
5. [ファブリック インターコネクトの交換（Replace Fabric Interconnect）] オプションを選択します。
6. 確認ページで [交換（Replace）] をクリックして、交換ワークフローをトリガーします。

ワークフローの一部として：

- 接続解除されたファブリック インターコネクトがインベントリから削除されます。
- ドメインプロファイルが新しいファブリック インターコネクトに再割り当てされ、展開されます。
- サーバー、シャーシ、および FEX がインベントリに登録され、新しいファブリック インターコネクトで検出されます。
- サーバおよびシャーシ プロファイルは、ファブリック インターコネクト関連のポリシーを使用して再展開されます。

Cisco UCS ファブリック インターコネクト 9108 100G のシングル ファブリック インターコネクトの交換

1. 古いファブリック インターコネクトを取り外し、スロットに同じモデルの新しいファブリック インターコネクトを挿入します。

交換用ファブリック インターコネクトに既存の設定がある場合は、交換用に使用する前に、デバイスで設定の消去を実行してください。

2. すべてのケーブル接続を新しいファブリック インターコネクトに再接続します。
3. 「置換」アクションをトリガーする前に、クラスタに接続するように新しいモジュールを設定します。
4. **[操作] > [ファブリック インターコネクト]** に移動して、交換されたファブリック インターコネクトのリストを表示し、「交換」オプションが有効になっているファブリック インターコネクトを特定します。
5. [ファブリック インターコネクトの交換（Replace Fabric Interconnect）] オプションを選択します。
6. 確認ページで [交換（Replace）] をクリックして、交換ワークフローをトリガーします。

ワークフローの一部として：

- 接続解除されたファブリック インターコネクトがインベントリから削除されます。
- ドメインプロファイルが新しいファブリックインターコネクトに再割り当てされ、展開されます。
- サーバおよびシャーシがインベントリに登録され、新しいファブリックインターコネクトで検出されます。
- サーバおよびシャーシ プロファイルは、ファブリック インターコネクト関連のポリシーを使用して再展開されます。

Cisco UCS 6400 シリーズのファブリック インターコネクト クラスタと Cisco UC5 6500 シリーズ のファブリック インターコネクトの置き換え

1. 古いファブリックインターコネクトクラスタを取り外し、同じモデルの新しいファブリック インターコネクト クラスタを接続します。
2. 古いファブリック インターコネクトから新しいファブリック インターコネクトに、サーバ、FEX ファブリック、およびブレードシャーシを含むすべてのケーブル接続を移動します。
3. Intersight で新しいファブリック インターコネクトを要求します。
4. [ファブリック インターコネクト（Fabric Interconnects）] ページの古いクラスタの横に表示される [UCS ドメインの置換（Replace UCS Domain）] オプションをセレクトします。
5. 古いファブリック インターコネクト クラスタを置き換える新しいファブリック インターコネクト クラスタを選択します。

ワークフローの一部として：

- 古いデバイス登録が新しいデバイス登録にマージされます。

- 接続解除されたファブリック インターコネクト クラスタがインベントリから削除されます。
- ドメイン プロファイルが新しいファブリック インターコネクト クラスタに再割り当てされ、展開されます。
- サーバー、シャーシ、および FEX がインベントリに登録され、新しいファブリック インターコネクト クラスタで検出されます。
- サーバおよびシャーシ プロファイルは、ファブリック インターコネクト関連のポリシーを使用して再展開されます。

Cisco UCS ファブリック インターコネクト 9108 100G のファブリック インターコネクト クラスタの交換

1. 古いファブリック インターコネクト クラスタを取り外し、スロットに同じモデルの新しいファブリック インターコネクト クラスタを挿入します。

   既存の構成を持つファブリックインターコネクトを交換に使用する場合は、交換に使用する前に、デバイスで必ず消去構成を実行してください。

2. すべてのケーブル接続を新しいファブリック インターコネクトに再接続します。
3. Intersight で新しいファブリック インターコネクトを要求します。

   プライマリ シャーシ検出ワークフローが実行されて失敗し、シャーシ識別子が同じであることが判明したため、「UCS ドメインの置換」アクションを実行するようWarning（注意）が表示されます。

4. [ファブリック インターコネクト（Fabric Interconnects）]ページの古いクラスタの横に表示される [UCS ドメインの置換（Replace UCS Domain）] オプションをセレクトします。
5. 古いファブリック インターコネクトクラスタを置き換える新しいファブリック インターコネクト クラスタを選択します。

ワークフローの一部として：

- 古いデバイス登録が新しいデバイス登録にマージされます。
- 接続解除されたファブリック インターコネクト クラスタがインベントリから削除されます。
- ドメイン プロファイルが新しいファブリック インターコネクト クラスタに再割り当てされ、展開されます。
- サーバー、シャーシ、および FEX がインベントリに登録され、新しいファブリック インターコネクト クラスタで検出されます。
- サーバおよびシャーシ プロファイルは、ファブリック インターコネクト関連のポリシーを使用して再展開されます。

（注） スロット間のファブリック インターコネクトのスワップはサポートされていません。

Cisco UCS X シリーズ ダイレクトでのシャーシの交換

Cisco UCS X シリーズ ダイレクトは、UCSX-9508 のシャーシRMA もサポートします。手順は次のとおりです。

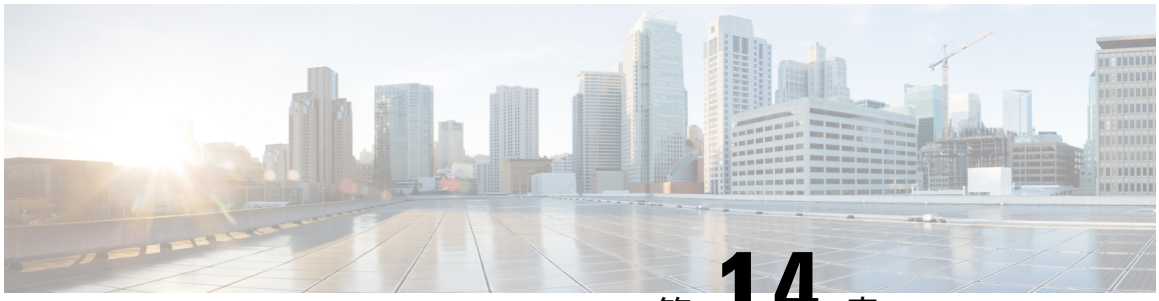
1. モジュールを新しいシャーシに挿入します。
2. シャーシの電源を入れます。

ワークフローの一部として：

- シャーシの検出が自動的に開始されます。
- サーバーとシャーシがインベントリされ、検出されます。
- Intersight インベントリで新しいシャーシのシリアル番号が更新されます。

Cisco Intersight による IOM の自動アップグレードのサポート

CMC が 4.1（3b）よりも前である IOM のファームウェアは、手動で更新する必要はありません。シャーシがファブリック インターコネクトに接続されると、ファームウェアが自動的に更新され、サーバ ポートがポート ポリシーで設定され、ポート ポリシーがドメイン プロファイルに関連付けられ、ドメイン プロファイルが展開されます。



第 14 章

テクニカル サポートの管理

- Cisco TAC との統合 （367 ページ）
- テクニカル サポートの診断ファイル収集 （368 ページ）

Cisco TAC との統合

重要

- テクニカルサポートの診断ファイルはエンドポイントでローカルに生成されるため、どの時点でもそれらのファイルにアクセスできません。現時点では、Intersight はテクニカルサポートファイルやその他のケース関連のアクティビティに関する通知は送信しません。
- Connected TAC は、Cisco TAC で直接オープンされたケースでのみ使用できます。
- パートナーサポートの場合、Connected TAC は次の場合にのみ期待どおりに動作します。
  - パートナーが Intersight ユーザに代わってケースをオープンします。

    （または）
  - パートナーは、Intersight ユーザが Cisco TAC に直接ケースをオープンすることを許可しています。

Cisco TAC サービス リクエスト（SR）は、Intersight から直接作成できます。そのためには、次の手順で、**Cisco Support Case Manager** を起動します。

- テーブル ビューと詳細ビューからの **HyperFlex クラスタ**。
- テーブル ビューと詳細ビューからの **IWE クラスタ**。
- テーブル ビューと詳細ビューからの **サーバー**。
- テーブルビューからの **ファブリック インターコネクト**。

Intersight モバイルアプリから Cisco TAC ケースを開くこともできます。

ケースをオープンする前に、次の要件を満たしていることを確認してください。

- ハードウェアに有効なサービス契約（権限付与）が存在している。
- Cisco ID がサービス契約に関連付けられている。

Cisco TAC ケースをオープンするには、次の手順を実行します。

1. 対応するテーブル ビューから **[HyperFlex クラスター（HyperFlex Cluster）]**、または**[IWE クラスター（IWE Cluster）]**、または **[サーバー（Server）]**、または **[ファブリック インターコネクト（Fabric Interconnect）]** を選択し、右のアクション列で省略記号 **(…)** をクリックします。また、TAC ケースを、**[アクション（Actions）]** メニューを **[HyperFlex クラスタ（ClusterHyperFlex Cluster）]**、または **[IWE クラスタ (IWE Cluster)]**、または**[サーバーの詳細（Server Details）]** ページから開くことができます。
2. [TAC ケースのオープン（Open TAC Case）] を選択します。選択した HyperFlex クラスタまたはサーバーまたはファブリック インターコネクトの名前とシリアル番号が含まれた [TAC ケースを開く（Open a TAC Case）] ウィンドウが表示されます。
3. **[続行（Continue）]** をクリックして **Cisco Support Case Manager** を起動します。**Cisco Support Case Manager** の UI で、自動的に挿入されたケースの詳細を確認し、TAC ケースの説明とタイトルを追加し、[送信（Submit）] をクリックします。

プロアクティブサポートワークフロー、詳細オプションの設定、およびプロアクティブ RMA のオプトアウトの詳細については、Proactive RMA for Intersight Connected Devices を参照してください。

プロアクティブ RMA の要件と利点については、Proactive Support Enable Through Intersight を参照してください。

テクニカル サポートの診断ファイル収集

Cisco TAC でケースをオープンすると、Intersight はテクニカル サポートの診断ファイルを収集して、オープン サポート ケースを支援します。収集されたデータには、ハードウェア テレメトリ、システム設定、および TAC ケースのアクティブなトラブルシューティングに役立つその他の詳細情報が含まれることがあります。指定したデータ収集オプションに関係なく、テクニカル サポートの収集が実行されます。ただし、この情報は任意で収集されるわけではありませんが、システムに対してケースをオープンする場合に限り、システム サポートの支援が必要になります。

（注） テクニカルサポート診断ファイルの収集は、要求されていない Intersight 管理対象デバイスではサポートされません。

アカウント管理者ユーザーは、[テクニカル サポート バンドルを追加（Add Tech Support Bundle）] をクリックし、デバイスの PID、シリアル番号、およびプラットフォーム タイプを提供することにより、[テクニカル サポート バンドル（Tech Support Bundles）] ページからテクニカル サポート コレクション リクエストを送信することもできます。

Intersight マネージド FI 接続デバイスのテクニカルサポート診断ファイルの収集を開始するには、デバイスの PID とシリアル番号を入力し、でプラットフォームタイプとして **[Intersight 管理対象ドメイン（Intersight Managed Domain）]** を選択します（**[テクニカルサポートバンドルの追加（Add Tech Support Bundle）]** ウィンドウ）。

- IMM デバイスの場合、テクニカル サポート コレクションは、バンドル内のすべてのエンドポイント ログがコレクションに含まれるベスト エフォート戦略に従います。
- 少なくとも 1 つのエンドポイントのログがバンドルで収集されると、最終的な収集ステータスは **[完了（Completed）]** と表示されます。
- 最終的なテクニカル サポート バンドルの *tech_support.log* および *peer_tech_support.log* ファイルには、欠落しているエンドポイント ログと収集の失敗に関する情報が含まれています。

次の表に、テクニカルサポート診断ファイルの収集を開始するために必要な入力の組み合わせを示します。

テクニカル サポート バンドルのタイプ	PID とシリアル番号
シャーシ	IOM-1、IOM-2、またはシャーシ
ファブリック インターコネクト（FI）	FI-A または FI-B
ブレード サーバ	ブレードまたはブレードに接続されたアダプタ

Intersight Managed FI Attached デバイスの場合、テクニカルサポート診断ファイルの収集は次のエンドポイントでサポートされます。

- ブレード BMC
- ブレードアダプタ
- ブレード シャーシ
- ファブリック インターコネクト
- IO モジュール
- ラック サーバ
- ラック サーバ アダプタ
- サーバ バンドル
- ファブリック エクステンダ

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。