サーバ ポリシーの設定

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	M5	M6	M7	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
デバイス コネクタ ポリシー	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
LDAP ポリシー	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
NTP ポリシー	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	—	—	—	—	—	—	—
永続メモリ ポリシー	—	はい	はい	はい	—	—	—	—	—	—	—
電源ポリシー	—	—	—	—	—	—	—	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	M5	M6	M7	M5	M6	M6	M7
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	—	—	—	—	—	—	—
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
SSH ポリシー	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
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
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
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
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

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	M5	M6	M7	M5	M6	M6	M7
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
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
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
アダプタ設定ポリシー	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
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
IMC アクセス ポリシー	—	—	—	—	はい	はい	はい	はい	はい	はい	はい
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

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	M5	M6	M7	M5	M6	M6	M7
イーサネット ネットワーク ポリシー	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
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
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
FC ゾーン ポリシー	—	—	—	—	はい	はい	はい	はい	はい	はい	はい
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

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	M5	M6	M7	M5	M6	M6	M7
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
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
iSCSI ブート ポリシー	—	—	—	—	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
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
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

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。
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。

[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、[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。 • 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

[プロパティ（Property）]	[基本情報（Essential Information）]
	• **[CISCO IMC 管理が有効 (Cisco IMC Management Enabled)]** 値が **[はい (Yes)]** に設定されています • 複数のユーザーが作成した vNIC 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 IMC 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 IMC バージョンが 4.2（2g）よりも古い場合、C シリーズ サーバーの検出はトリガーされません。Cisco IMC ファームウェアを 4.2（2g）にアップグレードして、サーバ ディスカバリを有効にします。

- **[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。

プロパティ（Property）	基本情報（Essential Information）
[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。	
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 インターフェイスで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。

プロパティ（Property）	基本情報（Essential Information）
[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。	
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。

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

プロパティ（Property）	基本情報（Essential Information）
[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 アダプタ（Ethernet Adapter）]	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します。
[イーサネット QoS（Ethernet QoS）]	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 ネットワーク	イーサネット ネットワーック ポリシーを選択するか、作成します。
[接続（Connection）]	
[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。

プロパティ（Property）	基本情報（Essential Information）
[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。
[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。

- **[追加（Add）]** をクリックします。

7. **[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
NetQueue	はい	はい	はい
RoCEv1	はい	非対応	いいえ
RoCEv2	いいえ	はい	はい
GeneveOffload	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
Q-in-Q	はい	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	非対応	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
- usNIC
- VMQ

（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 *1: 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 で有効にされるか	いいえ	はい	はい	非対応	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

	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 vnic2 で有効にされるか	はい	はい	はい	非対応	はい	はい	はい	はい	はい	非対応

（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. **[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。
[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。
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。	

[プロパティ（Property）]	[基本情報（Essential Information）]
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（VLAN 1）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。

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	
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。

プロパティ（**Property**）	基本情報（**Essential Information**）
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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
- **[vHBA の追加（Add vHBA）]** 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）
[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

プロパティ（**Property**）	基本情報（**Essential Information**）
	取る必要があります。 **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。	

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 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。
[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 インターフェイスで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。

- **[追加（Add）]** をクリックします。

7. **[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）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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 ）]	
[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]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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）]	
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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 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）]	
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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）。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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）]	
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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）]	
[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、C245 M6、C220 M7、および C240 M7 サーバー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）]	UEFI セキュア ブートを有効にすると、ブート モードはデフォルトで UEFI に設定されます。 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。 • **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 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 • **[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。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• 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。

プロパティ（**Property**）	基本情報（**Essential Information**）
	• **[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（Gateway IP）**：デフォルト ゲートウェイの IP アドレス。 • **静的 IP（Static 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： • **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。

プロパティ（Property）	基本情報（Essential Information）
	• **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。	
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。

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	

プロパティ（Property）		基本情報（Essential Information）
		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。
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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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 M4、M5、および M6 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。
[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 M4、M5、および M6 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 M4、M5、および M6 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]

プロパティ（**Property**）	基本情報（**Essential Information**）
[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。	
[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。

プロパティ（**Property**）	基本情報（**Essential Information**）
[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。
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。

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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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 M4、M5、および 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 M4、M5、および M6 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 M4、M5、および M6 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 M4、M5、および M6 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）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[プロパティ（Property）]	[基本情報（Essential Information）]
	さまざまな **[デフォルト ドライブ モード シナリオ（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 構成（M.2 Configuration）]	M.2 RAID コントローラのスロットを指定できるようにします。スロットは仮想ドライブの作成に必要です。 これは、M.2 ドライブに仮想ドライブを作成するために必要な唯一の構成です。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。

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。

[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）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[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。
[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。

[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
[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。
[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 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。
[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

[プロパティ（Property）]	[基本情報（Essential Information）]
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 および UCSC-C220-M7 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 *2:* 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 *3:* 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。

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。