



サーバーのブート

- [ブートポリシー, on page 1](#)
- [UEFI ブートモード \(2 ページ\)](#)
- [UEFI セキュアブート \(3 ページ\)](#)
- [CIMC セキュアブート \(5 ページ\)](#)
- [ブートポリシーの作成, on page 6](#)
- [SAN ブート \(8 ページ\)](#)
- [iSCSI ブート \(9 ページ\)](#)
- [LAN ブート \(38 ページ\)](#)
- [ローカルデバイスブート \(38 ページ\)](#)
- [ブートポリシーの削除, on page 46](#)
- [UEFI ブートパラメータ \(46 ページ\)](#)

ブートポリシー

Cisco UCS Manager では、ブレードサーバーとラックサーバーのブートポリシーを作成できます。

Cisco UCS Manager ブートポリシーは、BIOS 設定メニューのブート順序をオーバーライドし、次のことを決定します。

- ブートデバイスの選択
- サーバのブート元
- ブートデバイスの起動順序

たとえば、関連付けられたサーバーをローカルディスクやCD-ROM（仮想メディア（VMedia））などのローカルデバイスからブートしたり、SAN ブートやLAN（PXE）ブートを選択したりすることができます。

1つ以上のサービスプロファイルに関連付ける名前付きブートポリシーを作成するか、または特定のサービスプロファイルに対するブートポリシーを作成できます。ブートポリシーを有効にするには、ブートポリシーをサービスプロファイルに含め、このサービスプロファイル

をサーバーに関連付ける必要があります。サービス プロファイルにブート ポリシーを含めない場合、Cisco UCS Manager によってデフォルトのブート ポリシーが適用されます。



Note ブート ポリシーに対する変更は、そのブート ポリシーを含んでいる、更新中のサービス プロファイル テンプレートを使って作成されたすべてのサーバーに伝播されます。BIOS にブート 順序情報を再書き込みするためのサービス プロファイルとサーバーとの再関連付けは自動的にトリガーされます。

また、ブート ポリシーに次を指定することもできます。

- ローカル LUN の名前指定された名前は、展開される名前ではなく、ストレージ プロファイル内の論理名です。プライマリ名のみを指定します。セカンダリ名を指定すると、設定エラーが発生します。
- JBOD ディスクからブートするための特定の JBOD ディスク番号。
- 下位互換性のための任意の LUN。ただし、これは非推奨です。その他のデバイスでは、正常なブートを確保するために、ブート可能なイメージを保持している必要はありません。

UEFI ブートモード

Unified Extensible Firmware Interface (UEFI) は、オペレーティング システムとプラットフォームファームウェア間のソフトウェア インターフェイスを定義する仕様です。Cisco UCS Manager では、BIOS ファームウェア インターフェイスの代わりに UEFI が使用されます。これにより、BIOS はレガシー サポートを提供する一方で UEFI で動作できるようになります。

ブート ポリシーを作成する際は、レガシー ブート モードまたは UEFI ブート モードのいずれかを選択できます。レガシー ブート モードは、Cisco UCS C125 M5 サーバ以外のすべての Cisco UCS サーバでサポートされます。UEFI ブート モードは M4 以降のサーバーでのみサポートされ、このモードで UEFI セキュア ブート モードを有効にできます。Cisco UCS C125 M5 サーバは UEFI ブート モードのみサポートしています。

UEFI PXE ブートは、Cisco UCS Manager リリース 2.2(4) 以降と統合された Cisco UCS ラック サーバー上のすべての Cisco VIC アダプタでサポートされています。Cisco UCS Manager リリース 2.2(1) 以降では、すべての Cisco ブレード サーバーで UEFI PXE ブートがサポートされます。

次の制限は、UEFI ブート モードに適用されます。

- UEFI ブート モードは、次の組み合わせではサポートされません。
 - Cisco UCS Manager と統合された Cisco UCS ブレード サーバーおよびラック サーバー上の Gen-3 Emulex アダプタと QLogic アダプタ。
 - Cisco UCS Manager と統合された Cisco UCS ラック サーバー上の Broadcom アダプタに対する iSCSI ブート。

- 2つの iSCSI LUN で UEFI ブート モードを使用する場合は、Cisco UCS Manager に IQN 接尾辞プールからの名前を選択を許可するのではなく、基礎となる両方の iSCSI eNIC に適用されるサービスプロファイルに共通の iSCSI イニシエータ名を手動で指定する必要があります。共通の名前を指定しない場合、Cisco UCS Manager は 2 番目の iSCSI LUN を検出できません。
- 同じサーバーで UEFI とレガシー ブート モードを混在させることはできません。
- ブート ポリシーに設定されているブート デバイスに UEFI 対応オペレーティング システムがインストールされている場合にのみ、サーバーは UEFI モードで正常に起動します。互換性のある OS が存在しない場合、ブート デバイスは [Boot Order Details] 領域の [Actual Boot Order] タブに表示されません。
- ごくまれですが、UEFI ブート マネージャ エントリが BIOS NVRAM に正しく保存されなかったため、UEFI ブートが成功しない場合があります。UEFI シェルを使用すると、UEFI ブート マネージャ エントリを手動で入力することができます。この状況は、以下の場合に発生する可能性があります。
 - UEFI ブート モードが有効なブレードサーバーがサービスプロファイルから関連付けを解除され、[Equipment] タブまたは前面パネルを使用してブレードの電源を手動でオンにする場合。
 - UEFI ブート モードが有効なブレードサーバーがサービスプロファイルから関連付けを解除され、直接の VIC ファームウェア アップグレードが試行される場合。
 - UEFI ブート モードが有効なブレードサーバーまたはラック サーバーが SAN LUN からブートされ、サービス プロファイルが移行される場合。

Cisco UCS Manager で UEFI ブート パラメータを作成できます。詳細については「[UEFI ブート パラメータ \(46 ページ\)](#)」を参照してください。

UEFI セキュア ブート

Cisco UCS Manager は、Cisco UCS B シリーズ M4 以降のブレードサーバー、Cisco UCS C シリーズ M4 以降のラック サーバー、および Cisco UCS S シリーズ M4 ラック サーバー、および Cisco UCS C125 M5 サーバで UEFI セキュア ブートをサポートしています。Linux セキュア ブートは、リリース 4.0 (4a) 以降の SLES 15、SLES 13 SP4、Red Hat Linux 7.6 オペレーティングシステムでサポートされています。UEFI セキュア ブートがイネーブルの場合、すべての実行可能ファイル (ブート ローダ、アダプタ ドライバなど) はロードされる前に BIOS によって認証されます。認証されるには、そのイメージに Cisco 認証局 (CA) または Microsoft CA による署名が必要です。

UEFI セキュア ブートには次の制限が適用されます。

- UEFI ブート モードは、ブート ポリシーで有効にする必要があります。
- UEFI ブート モードは、ドライブでのみ使用可能です。

- Cisco UCS Manager ソフトウェアと BIOS ファームウェアは、リリース 2.2 以上である必要があります。



(注) UEFI ブートモードは、リリース 2.2(3a)以降の Cisco UCS C シリーズおよび S シリーズ ラック サーバーでサポートされます。

- ユーザー生成された暗号キーはサポートされません。
- UEFI セキュア ブートは、Cisco UCS Manager でのみ制御できます。
- サーバーがセキュアブートモードのときに Cisco UCS Manager を以前のバージョンにダウングレードする場合は、ダウングレードする前に、サーバーの関連付けを解除し、再び関連付ける必要があります。これを行わないと、サーバー ディスカバリは失敗します。
- Cisco UCS Manager リリース 4.0 では、次のオペレーティング システムで UEFI セキュア ブートがサポートされています。
 - Cisco UCS Manager リリース 4.0(1) では、windows 2016 および Windows 2012 R2 でのみ UEFI セキュア ブートがサポートされています。
 - Cisco UCS Manager リリース 4.0(1) では、windows 2016 および Windows 2019 でのみ UEFI セキュア ブートがサポートされています。
 - Cisco UCS Manager リリース 4.0 では、次で UEFI セキュア ブートがサポートされています。

表 1: Linux オペレーティング システム

Linux OS	eNIC/nNIC	fNIC
RHEL 7.5	3.2.210.18.738.12	1.6.0.50
RHEL 7.6	3.2.210.18.738.12	2.0.0.37
Centos 7.5	3.2.210.18.738.12	1.6.0.50
CentOS 7.6	3.2.210.18.738.12	1.6.0.50
SLES 12.4	3.2.210.18.738.12	2.0.0.32
SLES 15	3.2.210.18.738.12	2.0.0.39-71.0
ESXi	受信トレイの動作	受信トレイの動作



- (注)
- ESXi の場合、受信トレイのドライバは署名され、機能します。非同期ドライバは署名されておらず、機能しません。
 - Oracle OS は IPv6 をサポートしていません。
 - XEN OS は IPv6 をサポートしていません。

表 2: Windows オペレーティングシステム

Windows OS	neNIC	Nfsd Nic
Windows 2016	5.3.25.4	3.2.0.3
Windows 2019	5.3.25.4	3.2.0.3

CIMC セキュア ブート

CIMC セキュア ブートでは、署名済みのシスコファームウェアイメージのみをサーバーにインストールし、実行できます。CIMC が更新されると、イメージは、ファームウェアがフラッシュされる前に認証されます。認証に失敗すると、ファームウェアはフラッシュされません。これにより、CIMC ファームウェアへの不正アクセスを防止します。

CIMC セキュア ブートの注意事項と制約事項

- CIMC セキュア ブートは、Cisco UCS M4、M5、および M6 ラック サーバーでサポートされています。



- (注)
- CIMC セキュア ブートは Cisco UCS C220 M4/M5/M6、C240 M4/M5/M6、C480 M5/C480 M5 ML、C225 M6、および C245 M6 ラック サーバーではデフォルトで有効になっており、Cisco UCS C460 M4 ラック サーバーでは CIMC ファームウェア リリース 2.2(3) 以降へのアップグレード後に自動的に有効になります。
- CIMC セキュア ブートがイネーブルになると、それをディセーブルにすることはできません。
 - CIMC セキュア ブートがサーバー上で有効になると、2.1(3) より前の CIMC ファームウェアイメージにダウングレードすることはできません。

CIMCセキュア ブートのステータスの判別

手順

- ステップ1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ2 [Equipment > Rack-Mounts] > [Servers] > [Server Name] の順に展開します。
- ステップ3 [作業 (Work)] 領域の [インベントリ (Inventory)] タブをクリックします。
- ステップ4 [CIMC] サブタブをクリックします。
- ステップ5 [CIMC] 領域の [Secure Boot Operational State] フィールドをメモします。

次のいずれかになります。

- [Unsupported] : CIMC セキュア ブートはサーバーでサポートされていません。
- [Disabled] : CIMC セキュア ブートはサーバーでサポートされていますが、無効になっています。
- [Enabling] : CIMC セキュア ブートはイネーブルで、操作は進行中です。
- [Enabled] : CIMC セキュア ブートはサーバでイネーブルになっています。

ブート ポリシーの作成

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカルブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

Procedure

- ステップ1 [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ2 [サーバ] > [ポリシー]を展開します。
- ステップ3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ4 [Boot Policies] を右クリックし、[Create Boot Policy] を選択します。
[Create Boot Policy] ウィザードが表示されます。
- ステップ5 ポリシーの一意の名前と説明を入力します。

この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。

ステップ 6 (Optional) ブート順序に変更を加えた後、**[Reboot on Boot Order Change]** チェック ボックスを確認して、このブートポリシーを使用するすべてのサーバを再起動します。

シスコ以外の VIC アダプタがあるサーバに適用されるブートポリシーの場合、**[Reboot on Boot Order Change]** チェックボックスがオフでも、SAN デバイスが追加、削除または順序の変更がなされると、ブートポリシーの変更の保存時にサーバは常にリブートします。

ステップ 7 (Optional) 必要に応じて、**[Enforce vNIC/vHBA/iSCSI Name]** チェック ボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーと、**[Boot Order]** テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかのレポートとを表示します。
- オフにした場合は、Cisco UCS Manager がサービス プロファイルから (ブート オプションに応じて) vNIC または vHBA を使用します。

ステップ 8 **[Boot Mode]** フィールドで **[Legacy]** または **[UEFI]** オプション ボタンをオンにします。

Note Cisco UCS C125 M5 サーバは UEFI ブート モードのみをサポートします。

ステップ 9 **[UEFI]** を選択した場合、UEFI ブートセキュリティを有効にするには **[ブートセキュリティ (Boot Security)]** チェックボックスをオンにします。

ステップ 10 次の 1 つ以上のオプションをブートポリシーに設定し、ブート順序を設定します。

- **[Local Devices boot]** : サーバのローカル ディスクなどのローカル デバイスから、仮想メディアまたはリモート仮想ディスクを起動するには、[ブートポリシー用ローカルディスクブートの設定, on page 40](#) に進みます。
- **[SAN boot]** : SAN のオペレーティング システム イメージから起動するには、[ブートポリシー用 SAN ブートポリシー設定, on page 8](#) に進みます。
プライマリおよびセカンダリ SAN ブートを指定できます。プライマリブートが失敗した場合、サーバはセカンダリからのブートを試行します。
- **[LAN boot]** : 集中型プロビジョニングサーバから起動するには、[ブートポリシー用 LAN ブートポリシー設定, on page 38](#) に進みます。
- **[iSCSI ブート (iSCSI boot)]** : iSCSI LUN から起動するには、[iSCSI ブートポリシーの作成, on page 21](#) に進みます。

What to do next

ブートポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられると、サーバの [General] タブの [Boot Order Details] 領域でブート順序を確認できます。

SAN ブート

SAN 上のオペレーティング システム イメージから 1 つ以上のサーバがブートするように、ブートポリシーを設定できます。ブートポリシーにはプライマリとセカンダリの SAN ブートを含めることができます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。

シスコでは、システム内で最高のサービス プロファイル モビリティを提供する SAN ブートの使用を推奨しています。SAN からブートした場合、あるサーバから別のサーバにサービス プロファイルを移動すると、新しいサーバは、同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、新しいサーバは同じサーバと認識されます。

SAN ブートを使用するには、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージデバイスと通信できること。
- オペレーティング システム イメージが置かれているデバイス上のブートターゲット LUN (論理ユニット番号)。



(注) SAN ブートは、Cisco UCS ブレードおよびラック サーバー上の Gen-3 Emulex アダプタではサポートされていません。

ブートポリシー用 SAN ブートポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカルブートポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。



Tip ローカル ディスクと SAN LUN の両方がブート順序のストレージタイプに設定されていて、オペレーティング システムまたは論理ボリューム マネージャ (LVM) の設定が誤っている場合、サーバが SAN LUN ではなくローカル ディスクからブートする場合があります。

たとえば、Red Hat Linux がインストールされているサーバで、LVM にデフォルトの LVM が設定されていて、ブート順序に SAN LUN とローカル ディスクが設定されている場合、Linux は同じ名前の LV が 2 つあるという通知を生成し、SCSI ID の値が最も小さい LV (ローカル ディスクの可能性がありますが) からブートします。

この手順は、[ブート ポリシーの作成, on page 6](#) から直接続いています。

Procedure

ステップ 1 下矢印をクリックして [vHBAs] 領域を展開します。

ステップ 2 [Add SAN Boot] リンクをクリックします。

ステップ 3 [Add San Boot] ダイアログ ボックスで、vHBA とタイプを指定して、[OK] をクリックします。

[Primary] または [Secondary] の SAN ブートを指定できます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。[Any] オプションは、SAN ストレージデバイスに直接接続し、UCS Manager をバイパスしているサポート対象外のアダプタに使用します。UCSM が管理するサポート対象の一連のアダプタの場合の SAN ブートには [Any] を使用しないでください。サポート対象外のアダプタについては、ベンダーの指示に従ってブート用のアダプタを設定します。

ステップ 4 この vHBA がブート可能な SAN イメージを参照する場合は、[Add SAN Boot Target] リンクをクリックし、[Add SAN Boot Target] ダイアログボックスで、ブート ターゲット LUN、ブート ターゲット WWPN、およびタイプを指定して、[OK] をクリックします。

ステップ 5 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブート デバイスを追加します。
- [OK] をクリックして終了します。

What to do next

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

iSCSI ブート

iSCSI ブートを利用すると、サーバはネットワークにリモートに配置されている iSCSI ターゲット マシンからオペレーティング システムを起動できます。

iSCSI ブートは次の Cisco UCS VIC アダプタでサポートされます：

- Cisco UCS VIC 1200 シリーズ
- Cisco UCS VIC 1300 シリーズ
- Cisco UCS VIC 1400 シリーズ

iSCSI ブートを設定する前に満たさなければならない前提条件があります。これらの前提条件のリストについては、[iSCSI ブートのガイドラインと前提条件 \(11 ページ\)](#) を参照してください。

iSCSI ブートを実装するための手順の概要については、[iSCSI ブートの設定 \(14 ページ\)](#) を参照してください。

iSCSI ブート プロセス

Cisco UCS Manager は、サーバーにあるアダプタをプログラムするための関連付けプロセスで、サービス プロファイル用に作成された iSCSI vNIC と iSCSI のブート情報を使用します。アダプタのプログラミング後に、サーバーは最新のサービスプロファイル値で再起動します。電源投入時セルフテスト (POST) の後、アダプタは、それらのサービスプロファイル値を使用して初期化を試みます。値を使用して指定されたターゲットにログインできる場合、アダプタは iSCSI ブート ファームウェア テーブル (iBFT) を初期化してホスト メモリにポスト紙、有効なブート可能 LUN をシステム BIOS にポストします。ホスト メモリにポストされる iBFT には、プライマリ iSCSI vNIC にプログラミングされた、イニシエータとターゲットの設定が含まれています。



- (注) 以前は、ホストは LUN 検出が最初に終了したパスに応じて、設定されたブートパスのうち 1 つだけを参照し、そのパスから起動していました。現在は、設定された iSCSI ブート vNIC が 2 つある場合、ホストは両方のブートパスを参照するようになりました。そのため、マルチパス構成では、両方のブート vNIC に単一の IQN を設定する必要があります。ホスト上のブート vNIC に設定された異なる IQN が存在する場合、ホストは PCI 順序が低いブート vNIC に設定された IQN を使用して起動します。

次の手順であるオペレーティングシステム (OS) のインストールでは、iBFT 対応の OS が必要です。OS のインストール時に、OS インストーラは iBFT テーブルのホストのメモリをスキャンし、iBFT テーブルの情報を使用してブートデバイスの検出とターゲット LUN への iSCSI パス作成を行います。OS によっては、このパスを完了するために NIC ドライバが必要です。このステップが成功した場合、OS インストーラが OS をインストールする iSCSI ターゲット LUN を検出します。



- (注) iBFT は OS インストールのソフトウェア レベルで動作し、HBA モード (別名 TCP オフロード) では動作しない場合があります。iBFT が HBA モードで動作するかどうかは、インストール中の OS の機能によって異なります。また、Cisco UCS M51KR-B Broadcom BCM57711 アダプタを含むサーバーについては、iBFT は MTU ジャンボ設定に関係なく、最大伝送単位 (MTU) サイズ 1500 で正常に動作します。OS が HBA モードをサポートする場合、iSCSI インストールプロセスの後に HBA モード、デュアルファブリックのサポートおよびジャンボ MTU サイズの設定が必要な場合があります。

iSCSI ブートのガイドラインと前提条件

iSCSI ブートを設定する前に、これらのガイドラインと前提条件を満たす必要があります。

- iSCSI ブート ポリシーの作成後、`ls-compute` 権限を持つユーザーは、そのポリシーをサービスプロファイルまたはサービスプロファイルテンプレートに組み込むことができます。ただし、`ls-compute` 権限しかないユーザーは iSCSI ブート ポリシーを作成できません。
- セカンド vNIC (フェールオーバー vNIC) が iSCSI LUN から起動する必要がある Windows 2008 サーバーからの iSCSI ブートを設定するには、[Microsoft Knowledge Base Article 976042](#) を参照してください。Microsoft には、ネットワーク ハードウェアが変更されたときに、Windows が iSCSI ドライブからの起動に失敗するか、`bugcheck` エラーが発生する可能性がある、という既知の問題があります。この問題を回避するには、Microsoft が推奨する解決方法に従ってください。
- ストレージアレイは、iSCSI ブートのライセンスが付与され、アレイ サイド LUN マスキングが正しく設定されている必要があります。
- 各 iSCSI イニシエータに 1 つずつ、2 つの IP アドレスを決定する必要があります。IP アドレスは、ストレージアレイと同じサブネット上にある必要があります (可能な場合)。IP アドレスは、Dynamic Host Configuration Protocol (DHCP) を使用して静的または動的に割り当てられます。
- グローバル ブート ポリシーのブートパラメータは設定できません。代わりに、ブートパラメータを設定した後、ブートポリシーを適切なサービス プロファイルに含めます。
- オペレーティングシステム (OS) は iSCSI Boot Firmware Table (iBFT) 互換である必要があります。
 - RHEL 7.x の場合は、インストールの前にカーネルパラメータ「`rd.iscsi.ibft=1`」が必須となります。パラメータを入力しないと、iSCSI ブートに失敗することがあります。
 - SLES 12.x の場合は、次のガイドラインに従う必要があります。
 - カーネルをロードする前に、インストールディスクで「`e`」を押し、`linuxefi` (EFI を使用している場合) またはカーネル (レガシーを使用している場合) を編集して、カーネルパラメータ「`rd.iscsi.ibft=1 rd.iscsi.firmware=1 rd.neednet=1`」を追加します。パラメータを入力しないと、iSCSI ブートに失敗することがあります。
 - iSCSI を使用する既存のシステムで、`/etc/iscsi/iscsid.conf` has `node.startup=automatic` (manual ではない) であることを確認します。このパラメータを `/etc/default/grub/` に追加してから、`grub2-mkconfig -o /boot/grub2/grub.cfg` を実行して `grub` 設定を再構築します。
- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタの場合：
 - iSCSI ブートを使用するサーバーは、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタを含んでいる必要があります。アダプタカードの取り付け方法や交換方法については、『*Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*』を参照してください。サービスノートは、

<http://www.cisco.com/go/unifiedcomputing/b-series-doc> の『Cisco UCS B-Series Servers Documentation Roadmap』からアクセスできます。

- iSCSI デバイスの MAC アドレスを設定します。
- DHCP Vendor ID (オプション 43) を使用している場合は、iSCSI デバイスの MAC アドレスを `/etc/dhcpd.conf` に設定します。
- HBA モード (別名 TCP オフロード) および Boot to Target 設定がサポートされます。ただし、インストール中の HBA モードは Windows OS だけがサポートします。
- OS をインストールする前に、iSCSI のアダプタ ポリシーで Boot to Target 設定を無効にし、OS をインストールした後で、Boot to Target 設定を再度有効にします。



(注) アダプタ ポリシーの設定を変更するたびに、アダプタはリブートして新しい設定を適用します。

- iSCSI ターゲットに OS をインストールするときは、iSCSI ターゲットの順番を OS イメージが存在するデバイスよりも前にしておく必要があります。たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に iSCSI ターゲット、その後 CD とする必要があります。
 - サーバーが iSCSI ブートされた後は、イニシエータ名、ターゲット名、LUN、iSCSI デバイス IP、ネットマスクやゲートウェイを Broadcom ツールで変更しないでください。
 - POST (電源投入時自己診断テスト) プロセスを中断しないでください。中断すると、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタは初期化に失敗します。
- Cisco UCS M81KR 仮想インターフェイス カード および Cisco UCS VIC-1240 仮想インターフェイス カード の場合 :
- Cisco UCS VIC-1240 仮想インターフェイス カード の場合 :
- iSCSI デバイスの MAC アドレスを設定しないでください。
 - HBA モードおよび Boot to Target 設定はサポートされていません。
 - iSCSI ターゲットに OS をインストールするときは、iSCSI ターゲットの順番を OS イメージが存在するデバイスよりも後にしておく必要があります。たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に CD、その後 iSCSI ターゲットとする必要があります。
 - DHCP Vendor ID (オプション 43) を使用している場合、オーバーレイ vNIC の MAC アドレスを `/etc/dhcpd.conf` に設定する必要があります。
 - サーバーの iSCSI ブート後は、オーバーレイ vNIC の IP 詳細を変更しないでください。

- VMware ESX/ESXi オペレーティングシステムは、iSCSI ブート ターゲット LUN へのコアダンプ ファイルの保存をサポートしていません。ダンプ ファイルはローカル ディスクに書き込む必要があります。

イニシエータ IQN の設定

Cisco UCS は、サービス プロファイルが物理サーバーに関連付けられた時点で、以下のルールを使用してアダプタ iSCSI vNIC のイニシエータ IQN を決定します。

- サービス プロファイル レベルのイニシエータ IQN と iSCSI vNIC レベルのイニシエータ IQN を、1つのサービス プロファイルと一緒に使用することはできません。
- イニシエータ IQN をサービス プロファイル レベルで指定すると、DHCP オプション 43 の場合（イニシエータ IQN はアダプタ iSCSI vNIC で空に設定される）を除き、すべてのアダプタ iSCSI vNIC が同じイニシエータ IQN を使用するように設定されます。
- イニシエータ IQN を iSCSI vNIC レベルで設定すると、サービス プロファイル レベルのイニシエータ IQN は削除されます（存在する場合）。
- サービス プロファイルに 2つの iSCSI vNIC があり、一方にだけイニシエータ IQN が設定されている場合、もう一方にはデフォルトの IQN プールが設定されます。この設定は後で変更できます。唯一の例外は、DHCP オプション 43 が設定されている場合です。その場合、もう一方の iSCSI vNIC のイニシエータ IQN は、サービス プロファイルに関連付けるときに削除されます。



- (注) ベンダー ID を設定して、DHCP オプション 43 を使用するように iSCSI vNIC を変更した場合、サービス プロファイル レベルで設定したイニシエータ IQN は削除されません。サービス プロファイル レベルのイニシエータ IQN は、DHCP オプション 43 を使用しない別の iSCSI vNIC で使用できます。

Windows での MPIO のイネーブル化

ストレージアレイで接続を最適化するには、MPIOをイネーブルにします。



- (注) ネットワーク ハードウェアを変更すると、Windows が iSCSI ドライブからの起動に失敗する場合があります。詳細については、『[Microsoft support Article ID: 976042](#)』を参照してください。

始める前に

Microsoft Multipath I/O (MPIO) を有効化するサーバーには、Cisco VIC ドライバが必要です。

ブート LUN に設定されたパスが複数ある場合、LUN がインストールされるときにイネーブルにするパスは 1 つのみです。

手順

- ステップ 1** サーバーに関連付けられたサービス プロファイルで、プライマリ iSCSI vNIC を設定します。詳細については、[サービス プロファイル用 iSCSI vNIC の作成 \(22 ページ\)](#) を参照してください。
- ステップ 2** プライマリ iSCSI vNIC を使用して、iSCSI ターゲット LUN に Windows オペレーティング システムをインストールします。
- ステップ 3** Windows のインストールが完了したら、ホスト上で MPIO をイネーブルにします。
- ステップ 4** サーバーに関連付けられたサービス プロファイルで、ブート ポリシーにセカンダリ iSCSI vNIC を追加します。詳細については、[iSCSI ブート ポリシーの作成 \(21 ページ\)](#) を参照してください。

iSCSI ブートの設定

LUN ターゲットから iSCSI ブートするよう Cisco UCS でアダプタまたはブレードを設定する場合、次のすべてのステップを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	(任意) iSCSI ブートのアダプタ ポリシーを設定します。	詳細については、 iSCSI ブート ポリシーの作成 (21 ページ) を参照してください。
ステップ 2	(任意) イニシエータとターゲットの認証プロファイルを設定します。	詳細については、 iSCSI 認証プロファイルの作成 (18 ページ) を参照してください。
ステップ 3	(任意) IP アドレス プールの IP アドレスを使用するよう iSCSI イニシエータを設定するには、iSCSI イニシエータ プールに IP アドレスのブロックを追加します。	詳細については、 iSCSI イニシエータ IP プールの作成 (20 ページ) を参照してください。
ステップ 4	すべてのサービス プロファイルで利用できるブート ポリシーを作成します。または、特定のサービス ポリシーに対してのみローカルブート ポリシーを作	すべてのサービス プロファイルで利用できるブート ポリシーの作成の詳細については、 iSCSI ブート ポリシーの作成 (21 ページ) を参照してください。

	コマンドまたはアクション	目的
	成できます。ただし、複数のサービスプロファイルと共有できるブートポリシーを作成することを推奨します。	
ステップ 5	すべてのサービスプロファイルで使用できるブートポリシーを作成した場合は、それをサービスプロファイルに割り当てます。それ以外の場合は、次のステップに進みます。	ステップ 7 において、サービスプロファイルで iSCSI ブートおよび vNIC パラメータを設定するときに、サービスプロファイルにブートポリシーを割り当てることができます。
ステップ 6	サービスプロファイルで iSCSI vNIC を作成します。	詳細については、 サービスプロファイル用 iSCSI vNIC の作成 (22 ページ) を参照してください。
ステップ 7	expert モードでサービスプロファイルにおいて、またはサービスプロファイルテンプレートにおいて、iSCSI ブートパラメータ (iSCSI 修飾子名 (IQN)、イニシエータ、ターゲットインターフェイスなど) および iSCSI vNIC パラメータを設定します。	詳細については、 [Expert] ウィザードを使用したサービスプロファイルの作成 または サービスプロファイルテンプレートの作成 を参照してください。
ステップ 8	iSCSI ブート動作を確認します。	詳細については、「 Verifying iSCSI Boot 」を参照してください。
ステップ 9	OS をインストールする前に、OS が iSCSI ブートファームウェアテーブル (iBFT) と互換性があることを確認します。 <ul style="list-style-type: none"> • RHEL 7.x の場合は、OS をインストールする前にカーネルパラメータ「rd.iscsi.ibft=1」が必須となります。 • SLES 12.x については、カーネルをロードする前に、インストールディスクで「e」を押し、linuxefi (EFI を使用している場合) またはカーネル (レガシーを使用している場合) を編集して、カーネルパラメータ「rd.iscsi.ibft=1 rd.iscsi.firmware=1 rd.neednet=1」を追加します。 	適切なパラメータを入力しないと、iSCSI ブート操作に失敗することがあります。
ステップ 10	サーバーに OS をインストールします。	詳細については、次のいずれかのドキュメントを参照してください。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> 『Cisco UCS B シリーズ ブレード サーバー VMware インストール ガイド』 『Cisco UCS B シリーズ ブレード サーバー Linux インストール ガイド』 『Cisco UCS B シリーズ ブレード サーバー Windows インストール ガイド』
ステップ 11	サーバーをブートします。	

iSCSI アダプタ ポリシーの作成

Procedure

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 [サーバ] > [ポリシー]を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、**[root]** ノードを展開します。

ステップ 4 [Adapter Policies] を右クリックし、[Create iSCSI Adapter Policy] を選択します。

ステップ 5 [Create iSCSI Adapter Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[名前 (Name)] フィールド	<p>ポリシーの名前。</p> <p>この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。</p>
[Connection Timeout] フィールド	<p>Cisco UCS が、最初のログインに失敗し、iSCSI アダプタが使用できないと見なすまで待機する秒数。</p> <p>0～255の整数を入力します。0を入力すると、Cisco UCS はアダプタ ファームウェアの値セットを使用します (デフォルト: 15 秒)。</p>

名前	説明
[LUN Busy Retry Count] フィールド	<p>iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。</p> <p>0 ～ 60 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアの値セットを使用します（デフォルト：15 秒）。</p>
[DHCP Timeout] フィールド	<p>イニシエータが DHCP サーバーが使用できないと判断するまでに待機する秒数。</p> <p>60 ～ 300 の整数を入力します（デフォルト：60 秒）。</p>
[Enable TCP Timestamp] チェックボックス	<p>TCP タイムスタンプを使用する場合は、このボックスをオンにします。この設定では、必要に応じてパケットのラウンドトリップ時間を計算できるように、送信パケットにはパケット送信時のタイムスタンプが付きます。</p> <p>Note このオプションは、Cisco UCS NIC M51KR-B アダプタを備えたサーバーだけに適用されます。</p>
[HBA Mode] チェックボックス	<p>HBA モード（別名 TCP オフロード）をイネーブルにするには、このボックスをオンにします。</p> <p>Important このオプションは、Windows オペレーティングシステムを実行する Cisco UCS NIC M51KR-B アダプタがあるサーバーに対してのみ有効にするようにします。</p>
[Boot to Target] チェックボックス	<p>iSCSI ターゲットから起動する場合は、このボックスをオンにします。</p> <p>Note このオプションは、Cisco UCS NIC M51KR-B アダプタを備えたサーバーだけに適用されます。このオプションは、サーバにオペレーティングシステムをインストールするまで無効にしておく必要があります。</p>

名前	説明
[Owner] フィールド	次のいずれかになります。 <ul style="list-style-type: none"> • [ローカル (Local)] : このポリシーは、この Cisco UCS ドメイン内のサービスプロファイルとサービスプロファイルテンプレートでのみ使用できます。 • [グローバル移行中 (Pending Global)] : このポリシーの制御は、Cisco UCS Centralに移行中です。移行が完了すると、このポリシーは (Cisco UCS Centralに登録されている) すべての Cisco UCS ドメインで使用可能になります。 • [グローバル (Global)] : このポリシーは Cisco UCS Central で管理されます。このポリシーを変更する場合は、必ず Cisco UCS Central を使用してください。

ステップ 6 [OK] をクリックします。

What to do next

アダプタ ポリシーをサービス プロファイルとテンプレートに含めます。

iSCSI アダプタ ポリシーの削除

手順

ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ] > [ポリシー] を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Adapter Policies] ノードを展開します。

ステップ 5 アダプタ ポリシーを右クリックし、[Delete] を選択します。

ステップ 6 確認ダイアログボックスが表示されたら、[はい] をクリックします。

iSCSI 認証プロファイルの作成

iSCSI ブートの場合、イニシエータおよびターゲットの iSCSI 認証プロファイルを作成する必要があります。

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 [サーバ]>[ポリシー]を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [iSCSI Authentication Profiles] を右クリックし、[iSCSI Authentication Profile] を選択します。

ステップ 5 [Create Authentication Profile] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[名前 (Name)] フィールド	認証プロファイルの名前。 この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[ユーザ ID (User ID)] フィールド	このプロファイルに関連付けられたユーザ ID。 1～128文字の文字、スペース、特殊文字を入力します。
[Password] フィールド	このプロファイルに関連付けられたパスワード。 12～16文字 (特殊文字を含む) を入力します。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

ステップ 6 [OK] をクリックします。

次のタスク

認証プロファイルをサービス プロファイルとテンプレートに含めます。

iSCSI 認証プロファイルの削除

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 [サーバ]>[ポリシー]を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、**[root]** ノードを展開します。

- ステップ 4 [iSCSI Authentication Profiles] ノードを展開します。
- ステップ 5 削除する IP プールを右クリックし、[Delete] を選択します。
- ステップ 6 確認ダイアログボックスが表示されたら、**[はい]** をクリックします。

iSCSI イニシエータ IP プールの作成

iSCSI ブートに使用する IP アドレスのグループを作成できます。Cisco UCS Manager は指定した IPv4 アドレスのブロックを予約します。

サーバまたはサービスプロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、IP プールに含まれてはなりません。

手順

- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2 [LAN] > [プール] を展開します。
- ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、**[root]** ノードを展開します。
- ステップ 4 [IP Pools] ノードを展開します。
- ステップ 5 [IP Pool iscsi-initiator-pool] を右クリックし、[Create Block of IPv4 Addresses] を選択します。
- ステップ 6 [Create a Block of IPv4 Addresses] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[名前 (Name)] カラム	ブロックに割り当てる IPv4 アドレスの範囲。
[開始 (From)] カラム	ブロック内の最初の IPv4 アドレス。
[終了 (To)] カラム	ブロック内の最後の IPv4 アドレス。
[サブネット (Subnet)] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネットマスク。
[デフォルト ゲートウェイ (Default Gateway)] カラム	ブロック内の IPv4 アドレスに関連付けられたデフォルトゲートウェイ。
[プライマリ DSN (Primary DNS)] カラム	この IPv4 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[セカンダリ DNS (Secondary DNS)] カラム	この IPv4 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

ステップ7 [OK] をクリックします。

次のタスク

1 つ以上のサービス プロファイルまたはサービス プロファイル テンプレートを設定し、iSCSI イニシエータ IP プールから iSCSI イニシエータ IP アドレスを取得します。

iSCSI ブート ポリシーの作成

ブート ポリシーあたり最大 2 つの iSCSI vNIC を追加できます。一方の vNIC はプライマリ iSCSI ブート ソースとして動作し、もう一方はセカンダリ iSCSI ブート ソースとして動作します。

手順

ステップ1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ2 [サーバ] > [ポリシー] を展開します。

ステップ3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ4 [Boot Policies] を右クリックし、[Create Boot Policy] を選択します。

[Create Boot Policy] ウィザードが表示されます。

ステップ5 ポリシーの一意の名前と説明を入力します。

この名前には、1～16 文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。

ステップ6 (任意) ブート順序の変更後にこのブート ポリシーを使用するサーバをリブートするには、[Reboot on Boot Order Change] チェック ボックス をオンにします。

Cisco UCS Manager GUI で、ブート ポリシーの [順序を変更したときにリブートする (Reboot on Boot Order Change)] チェックボックスがオンになっていて、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスを削除または追加してもブート順序には直接影響せず、サーバは再起動しません。

(注) これは、標準のブート順序を使用しているサーバにのみ適用されます。

ステップ7 (任意) 必要に応じて、[Enforce vNIC/vHBA/iSCSI Name] チェック ボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーと、[Boot Order] テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかのレポートとを表示します。

- オフにした場合は、Cisco UCS Manager がサービス プロファイルから（ブート オプションに応じて）vNIC または vHBA を使用します。

ステップ 8 iSCSI ブートをブート ポリシーに追加するには、次の手順を実行します。

- 下矢印をクリックして [iSCSI vNICs] 領域を展開します。
- [Add iSCSI Boot] リンクをクリックします。
- [Add iSCSI Boot] ダイアログボックスで、iSCSI vNIC の名前を入力し、[OK] をクリックします。
- 別の iSCSI vNIC を作成するには、ステップ b、c を繰り返します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの **[一般 (General)]** タブの **[ブート順序の詳細 (Boot Order Details)]** 領域で実際のブート順序を確認できます。

サービス プロファイル用 iSCSI vNIC の作成

手順

- ステップ 1** [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2** [サーバ] > [サービス プロファイル] を展開します。
- ステップ 3** iSCSI vNIC を作成するサービス プロファイルが含まれている組織のノードを展開します。
- ステップ 4** iSCSI vNIC を作成するサービス プロファイルを展開します。
- ステップ 5** [iSCSI vNICs] ノードを右クリックし、[Create vNICs] を選択します。
- ステップ 6** [Create iSCSI vNIC] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[名前 (Name)] フィールド	iSCSI vNIC の名前。 この名前には、1～16 文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC (存在する場合)。

名前	説明
[iSCSI Adapter Policy] ドロップダウンリスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー (存在する場合)。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。
[MAC Address] フィールド	この iSCSI vNIC に関連付けられた MAC アドレス (存在する場合)。MAC アドレスが設定されていない場合、Cisco UCS Manager GUI は [Derived] と表示します。
[MAC Pool] フィールド	この iSCSI vNIC に関連付けられた MAC プール (存在する場合)。
[VLAN] ドロップダウンリスト	この iSCSI vNIC に関連付けられた仮想 LAN。デフォルトの VLAN は [default] です。 (注) Cisco UCS M81KR 仮想インターフェイス カード および Cisco UCS VIC-1240 仮想インターフェイス カード の場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。 Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

ステップ 7 [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。

- MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。このサービス プロファイルに関連付けられるサーバが Cisco UCS M81KR 仮想インターフェイス カードアダプタまたは Cisco UCS VIC-1240 仮想インターフェイス カードを含む場合、このオプションを選択します。

重要 このサービスプロファイルに関連付けられたサーバに Cisco UCS NIC M51KR-B アダプタが含まれる場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[00:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。
- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。各プール名の後には、数字のペアが括弧で囲まれています。最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番目の数字はそのプール内の MAC アドレスの合計数です。

この Cisco UCS ドメインが Cisco UCS Central に登録されている場合は、プール カテゴリが2つ存在することがあります。[ドメイン プール (Domain Pools)] は Cisco UCS ドメインでローカルに定義され、[グローバル プール (Global Pools)] は Cisco UCS Central で定義されます。

ステップ 8 (任意) すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。

詳細については、『』『Cisco UCS Manager Network Management Guide, Release 3.2』の「Creating a MAC Pool」セクションを参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 (任意) イニシエータ名を設定または変更する場合は、[iSCSI vNIC (iSCSI vNICs)] タブから [イニシエータ名のリセット (Reset Initiator Name)] または [イニシエータ名の変更 (Change Initiator Name)] をクリックし、[イニシエータ名の変更 (Change Initiator Name)] ダイアログボックスのフィールドを入力するかクリックします。詳細については、[サービス プロファイル レベルでのイニシエータ IQN の設定 \(24 ページ\)](#) を参照してください。

サービス プロファイルからの iSCSI vNIC の削除

手順

ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ] > [サービス プロファイル] を展開します。

ステップ 3 iSCSI vNIC を削除するサービス プロファイルが含まれている組織のノードを展開します。

ステップ 4 iSCSI vNIC を削除するサービス プロファイルを展開します。

ステップ 5 [iSCSI vNICs] ノードを展開します。

ステップ 6 削除する iSCSI vNIC を右クリックし、[Delete] を選択します。

ステップ 7 確認ダイアログボックスが表示されたら、[はい] をクリックします。

サービス プロファイル レベルでのイニシエータ IQN の設定

手順

ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ] > [サービス プロファイル] を展開します。

ステップ 3 編成の対象となるノードを展開します。

- ステップ4 変更する iSCSI vNIC のサービス プロファイルをクリックします。
- ステップ5 [作業 (Work)] ペインで、[iSCSI vNIC (iSCSI vNICs)] タブをクリックします。
- ステップ6 [Reset Initiator Name] をクリックします。
- ステップ7 確認ダイアログボックスが表示されたら、[はい]をクリックします。

サービス プロファイル レベルでのイニシエータ IQN の変更

手順

- ステップ1 [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ2 [サーバ]>[サービスプロファイル]を展開します。
- ステップ3 編成の対象となるノードを展開します。
- ステップ4 変更する iSCSI vNIC のサービス プロファイルをクリックします。
- ステップ5 [作業 (Work)] ペインで、[iSCSI vNIC (iSCSI vNICs)] タブをクリックします。
- ステップ6 [アクション (Actions)] エリアで、[イニシエータ名の変更 (Change Initiator Name)] をクリックします。
- ステップ7 [Change Initiator Name] ダイアログボックスで、次のフィールドの値を変更します。

名前	説明
[イニシエータ名の割り当て (Initiator Name Assignment)] ドロップダウン リスト	ドロップダウンリストから、使用する IQN イニシエータ名を選択します。
[イニシエータ名] フィールド	手動によるイニシエータ名の割り当てを選択した場合は、イニシエータ名を入力します。
[IQN サフィックス プールの作成 (Create IQN Suffix Pool)] リンク	これをクリックして、新しい IQN 接尾辞プールを作成します。

- ステップ8 [OK] をクリックします。

iSCSI ブート パラメータの設定

iSCSI vNIC のブート順序、ブートポリシー、iSCSI 認証プロファイル、イニシエータインターフェイス、ターゲットインターフェイスなど、iSCSI ブート パラメータを設定できます。

手順

- ステップ1 [ナビゲーション]ペインで、[サーバ]をクリックします。

- ステップ 2** [サーバ]>[サービスプロファイル]を展開します。
- ステップ 3** iSCSIブートパラメータを作成するサービスプロファイルを含む組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** iSCSI ブート パラメータを作成するサービス プロファイルをクリックします。
- ステップ 5** [Boot Order] タブをクリックします。
- ステップ 6** [Specific Boot Policy] 領域で、下矢印をクリックして [iSCSI vNICs] 領域を展開します。
- ステップ 7** [iSCSI vNICs] 領域で、サーバのブート元の iSCSI vNIC をダブルクリックしてそれらを [Boot Order] テーブルに追加します。
- ステップ 8** [iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。
2つの iSCSI vNIC がある場合は、ブートパラメータを設定する方を選択します。
- ステップ 9** [Set iSCSI Boot Parameters] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[名前 (Name)] フィールド	ブートパラメータを設定している iSCSI vNIC の名前。
[認証プロファイル (Authentication Profile)] ドロップダウンリスト	関連する iSCSI 認証プロファイルの名前。
[認証プロファイルの作成 (Create Authentication Profile)] リンク	このリンクをクリックして、すべての iSCSI vNIC で使用可能となる新しい iSCSI 認証プロファイルを作成します。

- ステップ 10** [Initiator Name] 領域で、次のフィールドに入力します。

名前	説明
[イニシエータ名の割り当て (Initiator Name Assignment)] ドロップダウンリスト	<p>iSCSI ブート イニシエータ名の割り当て方法を選択します。次の方法の中から 1 つを選択してください。</p> <ul style="list-style-type: none"> • [手動 (Manual)] : [イニシエータ名 (Initiator Name)] フィールドに名前を入力します。イニシエータ名は最大 223 文字です。 • [Pools] : IQN 接尾辞プールを選択します。このプールから名前が割り当てられます。 <p>(注) [iSCSI ブートパラメータの設定 (Set iSCSI Boot Parameters)] ダイアログボックスでイニシエータ名を設定すると、サービスプロファイルレベルではなく、iSCSI vNIC レベルでイニシエータ IQN が設定されます。複数のパスが設定されている場合は、[iSCSI vNICs] タブから、またはサービスプロファイルの作成時に、イニシエータ IQN を設定する必要があります。</p> <p>必要に応じて、イニシエータ名を変更またはリセットできます。詳細については、サービスプロファイルレベルでのイニシエータ IQN の変更 (25 ページ) を参照してください。</p>
[IQN サフィックスプールの作成 (Create IQN Suffix Pool)] リンク	すべての iSCSI vNIC で使用可能な新しい IQN 接尾辞プールを作成するには、このリンクをクリックします。
[Initiator Name] フィールド	<p>iSCSI イニシエータ名を定義する正規表現。</p> <p>任意の英数字および次の特殊文字を入力できます。</p> <ul style="list-style-type: none"> • . (ピリオド) • : (コロン) • - (ダッシュ)

ステップ 11 [Initiator IP Address Policy] ドロップダウンリストで、次のいずれかを選択します。

オプション	説明
[Select (DHCP used by default)]	<p>システムが DHCP を使用してインターフェイスを自動的に選択します。</p> <p>ステップ 13 に進みます。</p>
Static	<p>スタティック IPv4 アドレスが、この領域に入力された情報に基づいて iSCSI ブート vNIC に割り当てられます。</p>

オプション	説明
	ステップ 12 に進みます。
Pool	IPv4 アドレスが管理 IP アドレス プールから iSCSI ブート vNIC に割り当てられます。 ステップ 13 に進みます。

ステップ 12 [Initiator IP Address Policy] ドロップダウン リストから [Static] を選択した場合は、次のフィールドに値を入力します。

名前	説明
[IPv4 Address] フィールド	iSCSI ブート vNIC に割り当てられた IPv4 アドレス。 このアドレスを指定する場合は、[Initiator IP Address Policy] ドロップダウン リストで [Static] を選択する必要があります。
[Subnet Mask] フィールド	IPv4 アドレスに関連付けられたサブネットマスク。
[デフォルトゲートウェイ (Default Gateway)] フィールド	IPv4 アドレスに関連付けられたデフォルトゲートウェイ。
[プライマリ DNS (Primary DNS)] フィールド	プライマリ DNS サーバーのアドレス。
[セカンダリ DNS (Secondary DNS)] フィールド	セカンダリ DNS サーバー アドレス。

ステップ 13 iSCSI ターゲット インターフェイスでは、次のいずれかのオプション ボタンを選択します。

オプション	説明
[iSCSI Static Target Interface]	システムにより、設定する必要があるスタティック ターゲット インターフェイスが作成されます。 ステップ 14 に進みます。
[iSCSI Auto Target Interface]	システムにより、自動ターゲット インターフェイスが作成されます。自動ターゲットがイニシエータと DHCP ベンダー ID のどちらを使用するか指定する必要があります。 ステップ 16 に進みます。

ステップ 14 [iSCSI Static Target Interface] を選択した場合、[Static Target Interface] テーブルで [Add] をクリックします。

ステップ 15 [Create iSCSI Static Target] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[iSCSI Target Name] フィールド	<p>iSCSI ターゲットの iSCSI 修飾名 (IQN) または拡張固有識別子 (EUI) の名前を定義する正規表現。</p> <p>任意の英数字および次の特殊文字を入力することができます。</p> <ul style="list-style-type: none"> • . (ピリオド) • : (コロン) • - (ダッシュ) <p>重要 この名前は、標準の IQN または EUI のガイドラインに従って適切な形式にする必要があります。</p> <p>以下に、正しい形式の iSCSI ターゲット名の例を示します。</p> <ul style="list-style-type: none"> • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 • iqn.2001-04.com.example:storage.tape1.sys1.xyz • iqn.2001-04.com.example:storage.disk2.sys1.xyz • eui.02004567A425678D
[Priority] フィールド	システムによって iSCSI ターゲットに割り当てられたプライオリティ。
[Port] フィールド	<p>iSCSI ターゲットに関連付けられたポート。</p> <p>1 ~ 65535 の整数を入力します。デフォルトは 3260 です。</p>
[認証プロファイル (Authentication Profile)] ドロップダウンリスト	関連する iSCSI 認証プロファイルの名前。
[iSCSI 認証プロファイルの作成 (Create iSCSI Authentication Profile)] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。
[IPv4 Address] フィールド	iSCSI ターゲットに割り当てられた IPv4 アドレス。
[LUN Id] フィールド	iSCSI ターゲットの LUN 識別子です。

ステップ 16 [iSCSI Auto Target Interface] を選択した場合、[DHCP Vendor Id] フィールドにインシエータ名または DHCP ベンダー ID を入力します。インシエータがすでに設定済みである必要があります。ベンダー ID には、最大 32 文字の英数字を指定できます。

ステップ 17 [OK] をクリックします。

iSCSI ブートパラメータの変更

iSCSI vNIC のブート順序、ブートポリシー、iSCSI 認証プロファイル、イニシエータインターフェイス、ターゲットインターフェイスなど、iSCSI ブートパラメータを変更できます。

手順

- ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ 2** [サーバ]>[サービスプロファイル]を展開します。
- ステップ 3** iSCSI ブートパラメータを変更するサービスプロファイルを含む組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** iSCSI ブートパラメータを変更するサービスプロファイルをクリックします。
- ステップ 5** [Boot Order] タブをクリックします。
- ステップ 6** [Specific Boot Policy] 領域で、下矢印をクリックして [iSCSI vNICs] 領域を展開します。
- ステップ 7** ブート順序の iSCSI vNIC を追加または削除する、またはブート順序を変更するには、次のいずれかを実行します。
- iSCSI vNIC を追加するには、[iSCSI vNICs] 領域で、iSCSI vNIC をダブルクリックして [Boot Order] テーブルに追加します。
 - ブート順序から iSCSI vNIC を削除するには、[Boot Order] テーブルで、iSCSI vNIC を選択して [Delete] をクリックします。
 - iSCSI vNIC のブート順序を変更するには、[Boot Order] テーブルで、iSCSI vNIC を選択して [Move Up] または [Move Down] をクリックします。
- ステップ 8** ブートパラメータを変更するには、[iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。
- 2つの iSCSI vNIC がある場合は、ブートパラメータを変更する方を選択します。
- ステップ 9** [Set iSCSI Boot Parameters] ダイアログボックスで、次のいずれかのフィールドの値を変更します。

名前	説明
[名前 (Name)] フィールド	ブートパラメータを設定している iSCSI vNIC の名前。
[認証プロファイル (Authentication Profile)] ドロップダウンリスト	関連する iSCSI 認証プロファイルの名前。
[認証プロファイルの作成 (Create Authentication Profile)] リンク	このリンクをクリックして、すべての iSCSI vNIC で使用可能となる新しい iSCSI 認証プロファイルを作成します。

- ステップ 10** [Initiator Name] 領域で、次のフィールドに入力します。

名前	説明
[イニシエータ名の割り当て (Initiator Name Assignment)] ドロップダウンリスト	<p>iSCSI ブート イニシエータ名の割り当て方法を選択します。次の方法の中から 1 つを選択してください。</p> <ul style="list-style-type: none"> • [手動 (Manual)] : [イニシエータ名 (Initiator Name)] フィールドに名前を入力します。イニシエータ名は最大 223 文字です。 • [Pools] : IQN 接尾辞プールを選択します。このプールから名前が割り当てられます。 <p>(注) [iSCSI ブートパラメータの設定 (Set iSCSI Boot Parameters)] ダイアログボックスでイニシエータ名を設定すると、サービスプロファイルレベルではなく、iSCSI vNIC レベルでイニシエータ IQN が設定されます。複数のパスが設定されている場合は、[iSCSI vNICs] タブから、またはサービスプロファイルの作成時に、イニシエータ IQN を設定する必要があります。</p> <p>必要に応じて、イニシエータ名を変更またはリセットできます。詳細については、サービスプロファイルレベルでのイニシエータ IQN の変更 (25 ページ) を参照してください。</p>
[IQN サフィックスプールの作成 (Create IQN Suffix Pool)] リンク	すべての iSCSI vNIC で使用可能な新しい IQN 接尾辞プールを作成するには、このリンクをクリックします。
[Initiator Name] フィールド	<p>iSCSI イニシエータ名を定義する正規表現。</p> <p>任意の英数字および次の特殊文字を入力できます。</p> <ul style="list-style-type: none"> • . (ピリオド) • : (コロン) • - (ダッシュ)

ステップ 11 [Initiator IP Address Policy] ドロップダウンリストの選択を、次のいずれかに変更します。

オプション	説明
[Select (DHCP used by default)]	<p>システムが DHCP を使用してインターフェイスを自動的に選択します。</p> <p>ステップ 13 に進みます。</p>
Static	<p>スタティック IPv4 アドレスが、この領域に入力された情報に基づいて iSCSI ブート vNIC に割り当てられます。</p>

オプション	説明
	ステップ 12 に進みます。
Pool	IPv4 アドレスが管理 IP アドレス プールから iSCSI ブート vNIC に割り当てられます。 ステップ 13 に進みます。

ステップ 12 [Initiator IP Address Policy] ドロップダウン リストで [Static] を選択した場合、次のフィールドを入力するか変更してください。

名前	説明
[IPv4 Address] フィールド	iSCSI ブート vNIC に割り当てられた IPv4 アドレス。 このアドレスを指定する場合は、[Initiator IP Address Policy] ドロップダウン リストで [Static] を選択する必要があります。
[Subnet Mask] フィールド	IPv4 アドレスに関連付けられたサブネット マスク。
[デフォルトゲートウェイ (Default Gateway)] フィールド	IPv4 アドレスに関連付けられたデフォルトゲートウェイ。
[プライマリ DNS (Primary DNS)] フィールド	プライマリ DNS サーバーのアドレス。
[セカンダリ DNS (Secondary DNS)] フィールド	セカンダリ DNS サーバー アドレス。

ステップ 13 iSCSI ターゲット インターフェイスでは、次のいずれかのオプション ボタンを選択します。

オプション	説明
[iSCSI Static Target Interface]	システムにより、設定する必要があるスタティック ターゲット インターフェイスが作成されます。 ステップ 14 に進みます。
[iSCSI Auto Target Interface]	システムにより、自動ターゲット インターフェイスが作成されます。自動ターゲットがイニシエータと DHCP ベンダー ID のどちらを使用するか指定する必要があります。 ステップ 15 に進みます。

ステップ 14 [iSCSI Static Target Interface] を選択した場合は、[Static Target Interface] テーブルで次のいずれかを実行します。

- iSCSI スタティック ターゲット インターフェイスを追加するには、[Add] をクリックします。iSCSI ターゲット インターフェイスを変更するには、変更する iSCSI ターゲットイン

ターフェイスを選択して [Modify] をクリックします。次に、[Create iSCSI Static Target] ダイアログボックスで、次のフィールドを入力または変更します。

名前	説明
[iSCSI Target Name] フィールド	<p>iSCSI ターゲットの iSCSI 修飾名 (IQN) または拡張固有識別子 (EUI) の名前を定義する正規表現。</p> <p>任意の英数字および次の特殊文字を入力することができます。</p> <ul style="list-style-type: none"> • . (ピリオド) • : (コロン) • - (ダッシュ) <p>重要 この名前は、標準の IQN または EUI のガイドラインに従って適切な形式にする必要があります。</p> <p>以下に、正しい形式の iSCSI ターゲット名の例を示します。</p> <ul style="list-style-type: none"> • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 • iqn.2001-04.com.example:storage.tape1.sys1.xyz • iqn.2001-04.com.example:storage.disk2.sys1.xyz • eui.02004567A425678D
[Priority] フィールド	システムによって iSCSI ターゲットに割り当てられたプライオリティ。
[Port] フィールド	iSCSI ターゲットに関連付けられたポート。 1 ~ 65535 の整数を入力します。デフォルトは 3260 です。
[認証プロファイル (Authentication Profile)] ドロップダウンリスト	関連する iSCSI 認証プロファイルの名前。
[iSCSI 認証プロファイルの作成 (Create iSCSI Authentication Profile)] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。
[IPv4 Address] フィールド	iSCSI ターゲットに割り当てられた IPv4 アドレス。
[LUN Id] フィールド	iSCSI ターゲットの LUN 識別子です。

- iSCSI ターゲット インターフェイスを削除するには、削除する iSCSI ターゲット インターフェイスを選択して [Delete] をクリックします。

(注) 2つの iSCSI スタティック ターゲットがあり、優先順位 1 位のターゲットを削除すると、優先順位 2 位のターゲットが優先順位 1 位のターゲットになります。ただし、このターゲットは、Cisco UCS Manager では、引き続き優先順位 2 位のターゲットとして表示されます。

ステップ 15 [iSCSI Auto Target Interface] を選択した場合、[DHCP Vendor Id] フィールドのエントリをイニシエータ名または DHCP ベンダー ID に変更します。イニシエータがすでに設定済みである必要があります。ベンダー ID には、最大 32 文字の英数字を指定できます。

ステップ 16 [OK] をクリックします。

IQN プール

IQN プールは、Cisco UCS ドメイン内の iSCSI vNIC によって発信側 ID として使用される iSCSI 修飾名 (IQN) の集合です。

IQN プールのメンバは、プレフィックス:サフィックス:数字の形式になります。これで、プレフィックス、サフィックス、および数字のブロック (範囲) を指定することができます。

IQN プールには、番号の範囲やサフィックスが異なる (ただし、プレフィックスは共通している) 複数の IQN ブロックを含めることができます。

IQN プールの作成



(注) ほとんどの場合、最大 IQN サイズ (プレフィックス + サフィックス + 追加文字) は 223 文字です。Cisco UCS NIC M51KR-B アダプタを使用する場合、IQN サイズを 128 文字に制限する必要があります。

手順

ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ 2 [SAN] > [プール] を展開します。

ステップ 3 プールを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [IQN Pools] を右クリックし、[Create IQN Suffix Pool] を選択します。

ステップ 5 [Create IQN Suffix Pool] ウィザードの [Define Name and Description] ページで、次のフィールドに値を入力します。

フィールド	説明
名前	iSCSI 修飾名 (IQN) プールの名前。 この名前には、1～32文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[Description]	プールのユーザ定義による説明。 256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または' (一重引用符) は使用できません。
Prefix	このプール用に作成された任意の IQN ブロックのプレフィックス。 1～150文字を入力します。任意の文字や数字、および次の特殊文字を使用できます: (ピリオド)、: (コロン)、- (ハイフン)。たとえば、 iqn1.alpha.com を使用できます。
[割り当て順序 (Assignment Order)] フィールド	次のいずれかになります。 <ul style="list-style-type: none"> • [デフォルト (Default)] : Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル (Sequential)] : Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Create IQN Suffix Pool] ウィザードの [Add IQN Blocks] ページで、[Add] をクリックします。

ステップ 8 [Create a Block of IQN Suffixes] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Suffix] フィールド	iSCSI 修飾名 (IQN) のこのブロックの接尾辞。 1～64文字を入力します。任意の文字や数字、および次の特殊文字を使用できます: (ピリオド)、: (コロン)、- (ハイフン)。たとえば、 alphadc-1 を使用できます。
[From] フィールド	ブロック内の最初の接尾辞番号。
[Size] フィールド	ブロック内の接尾辞の数。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックして、ウィザードを終了します。

次のタスク

IQN サフィックスプールをサービスプロファイルとテンプレートに含めます。

IQN プールへのブロックの追加

手順

ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ 2 [SAN] > [プール] を展開します。

ステップ 3 プールを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [IQN Pools] ノードを展開します。

ステップ 5 目的の IQN プールを右クリックし、[Create a Block of IQN Suffixes] を選択します。

ステップ 6 [Create a Block of IQN Suffixes] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Suffix] フィールド	iSCSI 修飾名 (IQN) のこのブロックの接尾辞。 1 ~ 64 文字を入力します。任意の文字や数字、および次の特殊文字を使用できます: (ピリオド)、: (コロン)、- (ハイフン)。たとえば、 alphadc-1 を使用できます。
[From] フィールド	ブロック内の最初の接尾辞番号。
[Size] フィールド	ブロック内の接尾辞の数。

ステップ 7 [OK] をクリックします。

IQN プールからのブロックの削除

プールからアドレスブロックを削除すると、Cisco UCS Managerはそのブロックの中のvNICまたはvHBAに割り当てられたアドレスを再割り当てしません。削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられたvNICまたはvHBAに残ります。

- 関連付けられたサービスプロファイルが削除される。
- アドレスが割り当てられたvNICまたはvHBAが削除される。

- vNIC または vHBA が異なるプールに割り当てられる。

手順

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 [SAN]>[プール]を展開します。

ステップ 3 プールを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [IQN Pools] ノードを展開します。

ステップ 5 IQN 接尾辞のブロックを削除する IQN プールを選択します。

ステップ 6 [Work] ペインで、[IQN Blocks] タブをクリックします。

ステップ 7 削除するブロックを右クリックし、[Delete] を選択します。

ステップ 8 [はい (Yes)] をクリックして削除を確認します。

ステップ 9 [Save Changes] をクリックします。

IQN プールの削除

プールを削除した場合、Cisco UCS Managerは、に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みアドレスは、次のいずれかが起きるまで、vNIC または vHBA に割り当てられた状態のままになります。

- 関連付けられたサービス プロファイルが削除される。
- アドレスが割り当てられた vNIC または vHBA が削除される。
- vNIC または vHBA が異なるプールに割り当てられる。

手順

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 [SAN]>[プール]を展開します。

ステップ 3 プールを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [IQN Pools] ノードを展開します。

ステップ 5 削除するプールを右クリックして、[削除]を選択します。

ステップ 6 確認ダイアログボックスが表示されたら、[はい]をクリックします。

LAN ブート

LAN の集中プロビジョニング サーバーから 1 つまたは複数のサーバーをブートするブート ポリシーを設定できます。LAN (または PXE) ブートは、その LAN サーバーからサーバーに OS をインストールする際に頻繁に使用されます。

LAN ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、ローカル ディスクや仮想メディア ブートをセカンダリ ブート デバイスとして追加できます。

ブート ポリシー用 LAN ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカルブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。たとえば、セカンダリブート デバイスとしてローカル ディスクや仮想メディアのブートを追加できます。

この手順は、[ブートポリシーの作成 \(6 ページ\)](#) から直接続いています。

手順

-
- ステップ 1 下矢印をクリックして [vNICs] 領域を展開します。
 - ステップ 2 **[Add LAN Boot]** リンクをクリックします。
 - ステップ 3 **[Add LAN Boot]** ダイアログボックスで、LAN ブートに使用する vNIC の名前を [vNIC] フィールドに入力して、[OK] をクリックします。
 - ステップ 4 次のどちらかを実行します。
 - **[Boot Order]** テーブルに別のブート デバイスを追加します。
 - **[OK]** をクリックして終了します。
-

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ローカル デバイス ブート

Cisco UCS Manager 異なるローカル デバイスから起動することができます。



(注) 拡張ブート順序を使用しているCisco UCS M4 以降のブレードサーバーとラックサーバーの場合、トップレベルと第2レベルのどちらのブートデバイスも選択できます。



(注) 同じコントローラで複数のブートオプションが提供されている場合、ブートオプションは、Cisco UCS Manager で設定されたブート順序ではなく、次のように扱われます。

- OS がインストールまたはブートされると、UEFI ブートの場合、インストールされた OS は、Cisco UCS Manager で設定されているブートオプションに関係なく、ブートオプションを 0 優先度（最優先）にプッシュします。
- 起動順序は、BIOS によって設定された起動デバイスの列挙と、コントローラがデバイスをホストに公開する方法（または Cisco UCS Manager で提供）に基づいています。

ローカル ディスク ブート

サーバーにローカルドライブがある場合、ブートポリシーを設定して、トップレベルのローカルディスクデバイスまたは第2レベルのデバイスのいずれかからサーバーを起動できます。

- [Local LUN] : ローカルディスクまたはローカル LUN からの起動を有効にします。
- [Local JBOD] : ブート可能な JBOD からの起動を有効にします。
- [SD card] : SD カードからの起動を有効にします。
- [Internal USB] : 内部 USB からの起動を有効にします。
- [External USB] : 外部 USB からの起動を有効にします。
- [内蔵ローカル LUN (Embedded Local LUN)] : すべての Cisco UCS C240 M4、M5、および M6 サーバー上の内蔵ローカル LUN からの起動を有効にします。
- [内蔵ローカルディスク (Embedded Local Disk)] : すべての Cisco UCS C240 M4、M5、および M6 サーバー上の内蔵ローカルディスクからの起動を有効にします。



(注) Cisco UCS C125 M5 サーバでは、別の PCIe ストレージコントローラがない場合、このオプションを使用しないでください。代わりに、[Add Local Disk] オプションを使用します。



(注) 第2レベルのデバイスは、拡張ブート順序を使用している Cisco UCS M4 M4 以降のブレードサーバーとラックサーバーでのみ使用できます。

仮想メディア ブート

ブートポリシーを設定して、サーバーからアクセスできる仮想メディア デバイスから1つ以上のサーバーを起動できます。仮想メディア デバイスは、物理 CD/DVD ディスク（読み取り専用）またはフロッピーディスク（読み取りと書き込み）のサーバーへの挿入を疑似的に実行します。このタイプのサーバーブートは、通常、サーバーに手動でオペレーティングシステムをインストールするために使用されます。



(注) 第2レベルのデバイスは、拡張ブート順序を使用している Cisco UCS M4 以降のブレードサーバーとラックサーバーでのみ使用できます。

リモート仮想ドライブのブート

ブートポリシーを設定して、サーバーからアクセスできるリモート仮想ドライブから1つ以上のサーバーを起動できます。

NVMe のブート

リリース 3.2(1) 以降、Cisco UCS Manager には NVMe デバイスを M5 および M6 ブレードサーバーやラックサーバーのブートポリシーに追加するオプションが備わっています。BIOS は、存在する NVMe デバイスを列挙し、UEFI 対応 OS がインストールされている最初の NVMe デバイスで起動します。

Cisco ブート最適化 M.2 RAID コントローラ

4.0(4a) 以降、Cisco UCS Manager は Marvell 88SE92xx PCIe から SATA 6Gb/s コントローラ (UCS-M2-HWRAID) を搭載した Cisco ブート最適化 M.2 コントローラをサポートしています。BIOS は、このコントローラにインストールされている M.2 SATA ドライブを列挙し、その後前面パネルの SATA ドライブが UEFI 対応 OS がインストールされている最初の SATA デバイスから起動します。

ブートポリシー用ローカル ディスク ブートの設定

サービスプロファイルまたはサービスプロファイルテンプレートに制限されたローカルブートポリシーを作成することもできます。しかし、複数のサービスプロファイルまたはサービスプロファイルテンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブートポリシーには複数のタイプのブートデバイスを追加できます。たとえば、セカンダリブートデバイスとして SD カードのブートを追加できます。

この手順は、[ブートポリシーの作成 \(6 ページ\)](#) から直接続いています。

手順

ステップ 1 [ローカル デバイス (Local Devices)] 領域を展開します。

ステップ 2 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [ローカル ディスクの追加 (Add Local Disk)] または
 - [Add Local LUN]
 - [Add Local JBOD (ローカル JBOD の追加)]
 - [Add SD Card]
 - [Add Internal USB]
 - [Add External USB]
 - [Add Embedded Local LUN (内蔵ローカルLUNの追加)]
 - [Add Embedded Local Disk (内蔵ローカルディスクの追加)]

重要 Cisco Boot 最適化 M. 2 RAID コントローラ (HWRAID) が設定されている場合は、[Add Embedded Local Disk (組み込みローカル ディスクを追加)] ダイアログ ボックスで、[いずれか (Any)] を選択してディスクを追加します。[プライマリ (Primary)] または [セカンダリ (Secondary)] を選択しないでください。

(注) 拡張ブート順序を使用している Cisco UCS M4 以降のブレード サーバーとラックサーバーの場合、トップレベルと第2レベルのどちらのブートデバイスも選択できます。

ステップ 3 次のどちらかを実行します。

- [Boot Order] テーブルに別のブート デバイスを追加します。
- [OK] をクリックして終了します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ブート ポリシー用仮想メディア ブートの設定

サービス プロファイルまたはサービス プロファイルテンプレートに制限されたローカルブートポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービ

スプロファイルテンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブートポリシーには複数のタイプのブートデバイスを追加できます。ローカルディスクブートをセカンダリブートデバイスとして追加できます。



(注) 仮想メディアでは、USBを有効にする必要があります。USBの機能に影響するBIOS設定を変更した場合は、仮想メディアにも影響します。したがって、最適なパフォーマンスを実現するためには、次のUSB BIOSをデフォルト設定のままにしておくことをお勧めします。

- [デバイスをブート不可能にする (Make Device Non Bootable)] : [無効 (disabled)] に設定します。
- [USBアイドル電源最適化設定 (USB Idle Power Optimizing Setting)] : [ハイパフォーマンス (high-performance)] に設定します。

この手順は、[ブートポリシーの作成 \(6 ページ\)](#) から直接続いています。

手順

ステップ1 下矢印をクリックして [Local Devices] 領域を展開します。

ステップ2 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [Add CD/DVD] または

- [Add Local CD/DVD]

- [Add Remote CD/DVD] (ラックサーバのKVM CD/DVD用)

M5 ブレードサーバを使用した設定で、ISOをKVMコンソールにマッピングしている場合は、ブート順序には [Remote CD/DVD] のみを使用してください。

- [Add Floppy] または

- [Add Local Floppy]

- [Add Remote Floppy]

- [Add Remote Virtual Drive]

(注) 拡張ブート順序を使用しているCisco UCS M4以降のブレードサーバとラックサーバの場合、トップレベルと第2レベルのどちらのブートデバイスも選択できます。

ステップ3 次のどちらかを実行します。

- [Boot Order] テーブルに別のブートデバイスを追加します。

- [OK] をクリックして終了します。

次のタスク

ブートポリシーをサービスプロファイルとテンプレートに含めます。

このブートポリシーを含むサービスプロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ブートポリシー用 NVMe ブートの設定

サービスプロファイルまたはサービスプロファイルテンプレートに制限されたローカルブートポリシーを作成することもできます。しかし、複数のサービスプロファイルまたはサービスプロファイルテンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブートポリシーには複数のタイプのブートデバイスを追加できます。たとえば、セカンダリブートデバイスとして SD カードのブートを追加できます。

この手順は、[ブートポリシーの作成 \(6 ページ\)](#) から直接続いています。

手順

ステップ 1 下矢印をクリックして [Local Devices] 領域を展開します。

ステップ 2 [Add NVMe] をクリックし、デバイスを [Boot Order] テーブルに追加します。

(注) NVMe ブートポリシーは、[Uefi] ブートモードでのみ使用できます。

ステップ 3 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブートデバイスを追加します。
- [OK] をクリックして終了します。

次のタスク

ブートポリシーをサービスプロファイルとテンプレートに含めます。

このブートポリシーを含むサービスプロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

vMedia サービスプロファイルへのブートポリシーの追加

この手順では、[Create Service Profile (expert)] ウィザードの [Server Boot Order] ページで、vMedia のブートポリシーのオプションを設定する方法について説明します。

手順

- ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ 2** [サーバ]>[サービスプロファイル]を展開します。
- ステップ 3** サービス プロファイルを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** 組織を右クリックし、[Create Service Profile (expert)] を選択します。
[Unified Computing System Manager] ペインが表示されます。
- ステップ 5** [名前 (Name)]フィールドに、サービス プロファイルの識別に使用できる一意の名前を入力します。
この名前には、2～32文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。
この名前は、サービスプロファイルを作成する組織またはサブ組織内で一意である必要があります。
- ステップ 6** **[UUID Assignment]** ドロップダウン リストで、次のいずれかの手順を実行します。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。 ステップ 8 に進みます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUID はサービス プロファイルがサーバと関連付けられるまで割り当てられません。この時点で、UUID は製造元によってサーバに割り当てられた UUID 値に設定されます。サービス プロファイルを後で別のサーバに移動すると、UUID は新しいサーバに一致するように変更されます。 ステップ 8 に進みます。
	手動で割り当てる UUID を使用します。 ステップ 7 に進みます。
Pools Pool_Name	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。 各プール名の後には、プール内で利用可能な UUID の数および UUID の合計数を示す、括弧に囲まれた 2 つの数字が表示されます。 既存のプールを使用するのではなく、すべてのサービス プロファイルがアクセスできるプールを作成する場合は、ステップ 4 に進みます。それ以外の場合はステップ 8 に進みます。

- ステップ 7** (任意) オプションを選択した場合は、次の手順を実行します。
- a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。
- ステップ 8** (任意) このサービス プロファイルで使用する新しい UUID サフィックス プールを作成する場合は、[Create UUID Suffix Pool] をクリックし、[Create UUID Suffix Pool] ウィザードのフィールドに値を入力します。
- 詳細については、[UUID 接尾辞プールの作成](#)を参照してください。
- ステップ 9** (任意) テキストボックスに、このサービス プロファイルの説明を入力します。
- このサービス プロファイルのユーザ定義による説明。
- 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または' (一重引用符) は使用できません。
- ステップ 10** [Next] をクリックします。
- ステップ 11** [Create Service Profile (expert)] に移動し、[Server Boot Order] をクリックします。
[Boot Policy] ペインが表示されます。
- ステップ 12** [Boot Policy] ドロップダウン リストから、次のいずれかを選択します。

オプション	説明
Select Boot Policy to use	このサービス プロファイルにデフォルトのブート ポリシーを割り当てます。 ステップ 13 に進みます。
[特定のブート ポリシーを作成 (Create a Specific Boot Policy)]	このサービス プロファイル テンプレートだけがアクセスできるローカルブート ポリシーを作成できます。
Boot Policies <i>Policy_Name</i>	サービス プロファイルに既存のブート ポリシーを割り当てます。このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create Boot Policy] をクリックします。それ以外の場合は、リストでポリシーを選択し、ステップ 13 に進みます。

- ステップ 13** すべてのサービス プロファイルおよびテンプレートにアクセスできる新しいブート ポリシーを作成したら、[Boot Policy] ドロップダウン リストからそのポリシーを選択します。
- ステップ 14** [Next] をクリックします。

次のタスク

サービス プロファイルを Cisco UCS サーバに関連付けます。

ブートポリシーの削除

Procedure

- ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ 2 [サーバ (Servers)] > [ポリシー (Policies)] > [Organization_Name] の順に展開します。
- ステップ 3 [Boot Policies] ノードを展開します。
- ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
- ステップ 5 確認ダイアログボックスが表示されたら、[はい]をクリックします。

UEFI ブートパラメータ

サーバーの UEFI ブートモードは、プラットフォームハードウェアに保存されている情報によって決まります。UEFI OS ブートローダに関する情報を含むブートエントリは、サーバーの BIOS フラッシュに保存されます。2.2(4) より前の Cisco UCS Manager リリースでは、サービスプロファイルがあるサーバーから別のサーバーに移行されると、ブートローダ情報は宛先サーバーで使用できなくなります。そのため、BIOS は、サーバーを UEFI ブートモードでブートするためのブートローダ情報をロードできません。

Cisco UCSM リリース 2.2(4) では、宛先サーバー上の UEFI OS ブートローダの位置に関する情報を BIOS に提供する UEFI ブートパラメータが導入され、BIOS はその位置からブートローダをロードできます。サーバーは、そのブートローダ情報を使用して、UEFI ブートモードでブートできます。

UEFI ブートパラメータに関する注意事項と制約事項

- ブートモードが UEFI の場合のみ、UEFI ブートパラメータを設定できます。
- Cisco UCS Manager をリリース 2.2(4) 以降にアップグレードする場合は、サービスプロファイルの移行中に UEFI ブートが失敗しても自動的に処理されません。UEFI 対応 OS で正常にブートするには、ターゲットデバイスで UEFI ブートパラメータを明示的に作成しておく必要があります。
- UEFI ブートパラメータは、セカンドレベルのブート順序をサポートする、M4 以降のすべてのサーバーでサポートされています。
- 次のデバイスタイプの UEFI ブートパラメータを指定できます。

- SAN LUN
 - iSCSI LUN
 - ローカル LUN
- UEFI ブートパラメータは各オペレーティングシステム固有のパラメータです。次のオペレーティングシステムの UEFI ブートパラメータを指定できます。
- VMware ESX
 - SUSE Linux
 - Microsoft Windows
 - Red Hat Enterprise Linux 7

UEFI ブートパラメータの設定

始める前に

ブートポリシーの [Boot Mode] が [Uefi] であることを確認します。

手順

ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ] > [ポリシー] を展開します。

ステップ 3 [Boot Policies] を展開し、UEFI ブートパラメータを設定するブートポリシーを選択します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 LUN の UEFI ブートパラメータを設定するには、[Boot Order] 領域の LUN を選択し、[Set Uefi Boot Parameters] をクリックします。

重要 ローカル LUN、SAN LUN、iSCSI LUN に対してのみ UEFI ブートパラメータを設定できます。

ステップ 6 [Set Uefi Boot Parameters] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Boot Loader Name]	ブートローダの名前を指定します。これは必須フィールドです。 例 : grub.efi
[Boot Loader Path]	ブートローダがある場所のパスを指定します。これは必須フィールドです。ブートローダの名前をこのフィールドに入力しないでください。パスだけを指定する必要があります。 例 : \EFI\RedHat

フィールド	説明
[Boot Loader Description]	ブートローダの詳細です。これは、F6ブートメニューに表示される可読形式の名前です。

ステップ7 [OK] をクリックします。

ステップ8 [Save Changes] をクリックします。

UEFI ブートパラメータの変更

始める前に

ブートポリシーの [Boot Mode] が [Uefi] であることを確認します。

手順

ステップ1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ2 [サーバ] > [ポリシー] を展開します。

ステップ3 [Boot Policies] を展開し、UEFI ブートパラメータを変更するブートポリシーを選択します。

ステップ4 [Work] ペインで、[General] タブをクリックします。

ステップ5 UEFI ブートパラメータを使用して、LUN の UEFI ブートパラメータを変更するには、[Boot Order] 領域で LUN を選択し、[Modify Uefi Boot Parameters] をクリックします。

重要 ローカル LUN、SAN LUN、および iSCSI LUN に対してのみ UEFI ブートパラメータを設定できます。

ステップ6 [Modify Uefi Boot Parameters] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Boot Loader Name]	ブートローダの名前を指定します。これは必須フィールドです。
[Boot Loader Path]	ブートローダがある場所のパスを指定します。これは必須フィールドです。
[Boot Loader Description]	ブートローダの詳細です。

ステップ7 [OK] をクリックします。

ステップ8 [Save Changes] 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。