



## サーバーの管理

---

この章は、次の内容で構成されています。

- [ロケータ LED の切り替え \(1 ページ\)](#)
- [シャーシの前面ロケータ LED の切り替え \(2 ページ\)](#)
- [ハードドライブのロケータ LED の切り替え \(3 ページ\)](#)
- [パーソナリティ構成のクリア \(4 ページ\)](#)
- [時間帯の選択 \(4 ページ\)](#)
- [サーバーのブート順の管理 \(7 ページ\)](#)
- [サーバーのリセット \(25 ページ\)](#)
- [サーバーのシャットダウン \(26 ページ\)](#)
- [サーバーの電源管理 \(26 ページ\)](#)
- [電力ポリシーの設定 \(29 ページ\)](#)
- [ファン ポリシーの設定 \(42 ページ\)](#)
- [DIMM のブラックリストの設定 \(46 ページ\)](#)
- [BIOS の設定 \(47 ページ\)](#)
- [BIOS プロファイル \(50 ページ\)](#)
- [セキュアブート証明書の管理 \(54 ページ\)](#)
- [サーバ コンポーネントのファームウェアの更新 \(59 ページ\)](#)
- [製品 ID \(PID\) カタログの詳細の表示 \(60 ページ\)](#)
- [PID カタログのアップロードとアクティブ化 \(62 ページ\)](#)
- [PID カタログを削除 \(64 ページ\)](#)
- [永続メモリ モジュール \(65 ページ\)](#)

## ロケータ LED の切り替え

始める前に

このタスクを実行するには、`user` または `admin` 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>set locator-led {on   off}</b>	シャーシロケータ LED をイネーブルまたはディセーブルにします。
ステップ 3	Server /chassis # <b>commit</b>	トランザクションをシステムの設定にコミットします。

## 例

次に、シャーシロケータ LED をディセーブルにして、トランザクションをコミットする例を示します。

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit

Server /chassis #
```

## シャーシの前面ロケータ LED の切り替え

このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

## 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>set front-locator-led {on   off}</b>	シャーシロケータ LED をイネーブルまたはディセーブルにします。
ステップ 3	Server /chassis # <b>commit</b>	トランザクションをシステムの設定にコミットします。

### 例

次に、シャーシロケータ LED をディセーブルにして、トランザクションをコミットする例を示します。

```
Server# scope chassis
Server /chassis # set front-locator-led off
Server /chassis *# commit

Server /chassis #
```

## ハードドライブのロケータ LED の切り替え

このアクションを使用できるのは一部の UCS C シリーズ サーバだけです。

### 始める前に

このタスクを実行するには、`user` または `admin` 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server/chassis # <b>scope hdd</b>	ハードディスク ドライブ (HDD) コマンド モードを開始します。
ステップ 3	Server /chassis/hdd # <b>locateHDD drivenum</b> {1   2}	ここで、 <i>drivenum</i> は、ロケータ LED を設定するハードドライブの番号です。値 1 は LED が点灯し、値 2 は LED が消灯します。

### 例

次に、HDD 2 のロケータ LED を点灯する例を示します。

```
Server# scope chassis
Server /chassis # scope hdd
Server /chassis/hdd # locateHDD 2 1
HDD Locate LED Status changed to 1
Server /chassis/hdd # show
Name                Status                LocateLEDStatus
-----
HDD1_STATUS         present               TurnOFF
HDD2_STATUS         present               TurnON
HDD3_STATUS         absent                TurnOFF
HDD4_STATUS         absent                TurnOFF
```

```
Server /chassis/hdd #
```

## パーソナリティ構成のクリア

### 始める前に

このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

### 手順

---

#### ステップ 1 Server # **scope chassis**

シャーシ コマンド モードを開始します。

#### ステップ 2 Server chassis # **clear-personality**

パーソナリティ構成をクリアします。

---

## 時間帯の選択

### タイム ゾーン の 選択

タイムゾーンを選択すると、ローカルタイムゾーンを選択できるため、デフォルトのマシンの時刻ではなく、ローカルタイムを表示できます。Cisco IMC Web UI および CLI では、希望するタイムゾーンを選択して設定するオプションが提供されます。

タイムゾーンをローカルタイムに設定すると、システムのタイミングを使用するすべてのサービスにタイムゾーンの変数が適用されます。これは、ロギング情報に影響し、Cisco IMC の次のアプリケーションで利用されます。

- 障害サマリーと障害履歴のログ
- Cisco IMC log
- rsyslog

ローカルタイムを設定すると、表示できるアプリケーションのタイムスタンプが、選択したローカルタイムで更新されます。

## タイムゾーンの選択

### 始める前に

このタスクを実行するには、**user** または **admin** 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope CIMC</b>	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /CIMC # <b>timezone-select</b>	大陸および海洋のリストが表示されます。
ステップ 3	大陸または海洋に対応する番号を入力します。	選択した大陸または海洋のすべての国または地域のリストが表示されます。
ステップ 4	タイムゾーンとして設定する国または地域に対応する番号を入力します。	国または地域に複数のタイムゾーンがある場合は、その国または地域のタイムゾーンのリストが表示されます。
ステップ 5	タイムゾーンに対応する番号を入力します。	「Is the above information OK?」というメッセージが表示されます。
ステップ 6	<b>1</b> と入力します。	「Continue?[y N]:」プロンプトが表示されます。
ステップ 7	選択したタイムゾーンを設定するには、 <b>y</b> を入力します。	選択したタイムゾーンが Cisco IMC サーバのタイムゾーンとして設定されます。

### 例

次に、タイムゾーンを設定する例を示します。

```
Server# scope CIMC
Server /CIMC # timezone-select
```

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
```

```
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
#? 2
```

Please select a country whose clocks agree with yours.

- 1) Anguilla
- 2) Antigua & Barbuda
- 3) Argentina
- 4) Aruba
- 5) Bahamas
- 6) Barbados
- 7) Belize
- 8) Bolivia
- 9) Brazil
- 10) Canada
- 11) Caribbean Netherlands
- 12) Cayman Islands
- 13) Chile
- 14) Colombia
- 15) Costa Rica
- 16) Cuba
- 17) Curacao
- 18) Dominica
- 19) Dominican Republic
- 20) Ecuador
- 21) El Salvador
- 22) French Guiana
- 23) Greenland
- 24) Grenada
- 25) Guadeloupe
- 26) Guatemala
- 27) Guyana
- 28) Haiti
- 29) Honduras
- 30) Jamaica
- 31) Martinique
- 32) Mexico
- 33) Montserrat
- 34) Nicaragua
- 35) Panama
- 36) Paraguay
- 37) Peru
- 38) Puerto Rico
- 39) St Barthelemy
- 40) St Kitts & Nevis
- 41) St Lucia
- 42) St Maarten (Dutch part)
- 43) St Martin (French part)
- 44) St Pierre & Miquelon
- 45) St Vincent
- 46) Suriname
- 47) Trinidad & Tobago
- 48) Turks & Caicos Is
- 49) United States
- 50) Uruguay
- 51) Venezuela
- 52) Virgin Islands (UK)
- 53) Virgin Islands (US)

#? 49

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County

```
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - southeast Alaska panhandle
25) Alaska Time - Alaska panhandle neck
26) Alaska Time - west Alaska
27) Aleutian Islands
28) Metlakatla Time - Annette Island
29) Hawaii
#? 8
```

The following information has been given:

```
United States
Eastern Time - Indiana - Crawford County
```

Is the above information OK?

```
1) Yes
2) No
#? 1
```

You have chosen to set timezone settings to:

```
America/Indiana/Marengo
```

Continue?[y|N]: y

Timezone has been updated.

The local time now is: Sun Jun 1 02:21:15 2014 EST

Server /CIMC #

## サーバーのブート順の管理

### サーバのブート順

Cisco IMC を使用して、使用可能なブートデバイスタイプからサーバがブートを試行する順序を設定できます。レガシーブート順の設定では、Cisco IMC によりデバイスタイプの並び替えが許可されますが、デバイスタイプ内のデバイスの並べ替えはできません。高精度ブート順の設定により、デバイスの線形順序付けができます。Web UI または CLI では、ブート順およびブートモードの変更、各デバイスタイプ下への複数のデバイスの追加、ブート順の並び替え、各デバイスタイプのパラメータの設定ができます。

ブート順の設定を変更すると、Cisco IMC は、サーバが次にリブートされるときに、設定されたブート順を BIOS に送信します。新しいブート順を実装するには、設定の変更後にサーバー

をリブートします。新しいブート順は以降のリブートで反映されます。設定されたブート順は、設定が Cisco IMC または BIOS 設定で再度変更されるまで保持されます。



- (注) 次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。
- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
  - ユーザが BIOS で直接、ブート順を変更した。
  - BIOS が、ホストによって認識されているがユーザーから設定されていないデバイスを追加した。



**重要** Cisco UCS C220 M5 または C480 M5 サーバをリリース 4.1 (1x) にアップグレードする場合は、次の条件に従います。

- 4.0 よりも前のリリースからアップグレードする場合 (4x)
- [レガシー ブート モード (Legacy Boot Mode)] が有効になっていて、[Cisco IMC のブート順序 (Cisco IMC Boot Order)] が設定されていない場合
- サーバが Cisco HWRAID アダプタから起動している場合

その後、アップグレードする前に次のいずれかを実行する必要があります。

- ここに記載されている XML API スクリプトと UCSCFG ベースのスクリプトを実行します。
- または
- Cisco IMC GUI または CLI インターフェイスを使用して、目的のブート順序を手動で設定します。



- (注) ブート順の設定機能を使用して新しいポリシーを作成する場合、BIOS はこの新しいポリシーをシステムのデバイスにマッピングしようとします。実際にマッピングされたデバイス名とポリシー名が [Actual Boot Order] 領域に表示されます。BIOS が Cisco IMC の特定のポリシーにデバイスをマッピングできない場合は、実際のデバイス名が [Actual Boot Order] 領域に [NonPolicyTarget] として示されます。





- (注) Cisco IMC 2.0(x) のアップグレード中に、レガシーブート順は高精度ブート順に移行されます。前のブート順の設定が削除され、バージョン 2.0 にアップグレードする前に設定されたすべてのデバイス タイプが対応する高精度ブート デバイス タイプに変換され、ダミーのデバイスが同じデバイス タイプ用に作成されます。Web UI の **[構成されたブート順序 (Configured Boot Order)]** 領域でこれらのデバイスを確認できます。CLI でこれらのデバイスを確認するには、**show boot-device** コマンドを入力します。この間に、サーバーの実際のブート順が保持され、Web UI と CLI の実際のブート順オプション下で確認できます。

Cisco IMC を 2.0(x) よりも前のバージョンにダウングレードすると、サーバの最後のブート順が保持され、それを **[Actual Boot Order]** 領域で確認できます。次に例を示します。

- 2.0(x) バージョンでレガシーブート順でサーバを設定した場合、ダウングレードすると、レガシーブート順の設定が保持されます。
- 2.0(x) で高精度ブート順でサーバを設定した場合、ダウングレードすると、最後に設定したレガシーブート順が保持されます。



#### 重要

- 2.0(x) より前のブート順の設定がレガシーブート順と見なされます。実行中のバージョンが 2.0(x) の場合、Web UI でレガシーブート順を設定できませんが、CLI および XML API を介して設定できます。CLI で、**set boot-order HDD,PXE** コマンドを使用してこれを設定できます。CLI または XML API を介してレガシーブート順を設定できますが、Web UI では設定されたこのブート順は表示されません。
- レガシーブート順の機能と高精度ブート順の機能は相互に排他的です。レガシーブート順または高精度ブート順のどちらかを設定できます。レガシーブート順を設定すると、設定されたすべての高精度ブートデバイスがディセーブルになります。高精度ブート順を設定すると、レガシーブート順の設定が消去されます。

## ブートデバイスの詳細の表示



- (注) ホストが BIOS 電源投入時自己診断テスト (POST) を実行している間は、ブート順を変更しないでください。

#### 始める前に

このタスクを実行するには、**user** または **admin** 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>show boot-device [detail]</b>	ブート デバイスの詳細情報を表示します。

## 例

次に、作成したブート可能デバイスの詳細情報を表示する例を示します。

```
Server# scope bios
Server /bios # show boot-device
Boot Device          Device Type  Device State  Device Order
-----
TestUSB              USB         Enabled      1
TestPXE              PXE         Enabled      2
Server /bios # show boot-device detail
Boot Device TestUSB:
  Device Type: USB
  Device State: Enabled
  Device Order: 1
  Sub Type: HDD
Boot Device TestPXE:
  Device Type: PXE
  Device State: Enabled
  Device Order: 2
  Slot Id: L
  Port Number: 1
```

## 高精度ブート順の設定



- (注) ホストがBIOS電源投入時自己診断テスト (POST) を実行している間は、ブート順を変更しないでください。

## 始める前に

リリース 4.1(3b) 以降、Cisco IMC は HTTP ブート機能をサポートしています。HTTP ブートは、UEFI ブート モードでのみサポートされます。

このタスクを実行するには、`user` または `admin` 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>create-boot-device</b> [ <i>device name</i> ] [ <i>device type</i> ].	<p>BIOS がブートするブート可能デバイスを作成します。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [HDD] : ハードディスク ドライブ</li> <li>• [PXE] : PXE ブート</li> <li>• <b>SAN</b> ブート</li> <li>• <b>iSCSI</b> ブート</li> <li>• <b>SD</b> カード</li> </ul> <p>(注) SD カード オプションを使用できるのは一部の UCS C シリーズ サーバだけです。</p> <ul style="list-style-type: none"> <li>• <b>USB</b></li> <li>• 仮想メディア</li> <li>• <b>PCHStorage</b></li> <li>• <b>UEFISHELL</b></li> <li>• <b>HTTP</b></li> </ul>
ステップ 3	Server /bios # <b>scope boot-device</b> はブートデバイス名を作成しました。	作成したブート可能デバイスの管理を入力します。
ステップ 4	Server /bios /boot-device # <b>set values</b>	<p>特定のブート可能なデバイスにプロパティ値を指定します。次のいずれか、または複数を設定できます。</p> <ul style="list-style-type: none"> <li>• <b>cli</b> : CLI オプション</li> <li>• <b>state</b> : BIOS がデバイスを認識するかどうか。デフォルトでは、デバイスはディセーブルにされています。</li> </ul> <p>(注) イネーブルである場合、デバイスはレガシーのブート順序の設定を上書きします。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• slot : デバイスが差し込まれるスロットの ID。</li> <li>• port : デバイスが装着されているスロットのポート。</li> <li>• LUN : デバイスが装着されているスロットの論理ユニット。</li> <li>• sub-type : 特定のデバイスタイプの下位のサブデバイスタイプ。</li> <li>• order : デバイスの使用可能なリストにおけるそのデバイスの順序。</li> <li>• macaddress : ネットワーク イーサネットインターフェイスの MAC アドレス</li> <li>• iptype : IP タイプ 必要な値のいずれかを入力します : IPv4 または IPv6</li> <li>• ipconfig-type : IP 構成のタイプ 必要な値のいずれかを入力します : DHCP または 静的</li> <li>• uri : すべての OS iso および EFI ファイルが配置されている URI パス</li> </ul>
ステップ 5	Server /bios /boot-device # <b>commit</b>	トランザクションをシステムの設定にコミットします。

### 例

次に、ブート順序を設定し、ブートデバイスを作成し、新しいデバイスの属性を設定し、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # create boot-device TestPXE PXE
Server /bios # scope boot-device TestPXE
Server /bios /boot-device # set state Enabled
Server /bios /boot-device # set slot L
Server /bios /boot-device # set port 1
Server /bios /boot-device # set order 1
Server /bios /boot-device # commit
Enabling boot device will overwrite Legacy Boot Order configuration
Continue?[y|N]y
Server /bios /boot-device # y
```

```
Committing device configuration
Server /bios/boot-device # show detail
BIOS:
  BIOS Version: "C240M3.2.0.0.15 (Build Date: 03/16/2014)"
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: None
  Actual Boot Mode: Legacy
  Last Configured Boot Order Source: CIMC
```

```
Server /bios/boot-device # show boot-device detail
Boot Device TestPXE:
  Device Type: PXE
  Device State: Enabled
  Device Order: 1
  Slot Id: L
  Port Number: 1
```

次に、ブート順序を構成し、IPタイプ：**[DHCP]**にHTTPブートデバイスを作成し、新しいデバイスの属性を設定し、トランザクションをコミットする例を示します。

```
Server# scope server 1
Server /server # scope bios
Server /server/bios # create boot-device HTTP-Test HTTP
Server /server/bios # scope boot-device HTTP-Test
Server /server/bios/boot-device # set status enabled
Server /server/bios/boot-device # set port 10
Server /server/server/bios /boot-device # set order 1
Server /server/bios /boot-device # set slot MLOM
Server /server/bios/boot-device # set iptype IPv4
Server /server/bios/boot-device # set macaddress 00:25:B5:00:01:2b
Server /server/bios/boot-device # set ipconfig-type DHCP
Server /server/bios/boot-device # set uri http://www.cloudboot.com:80/EFI/rhel_82_dvd.iso
Server /bios /boot-device # commit
Committing device configuration
Server /server/bios/boot-device # show detail
BBIOS:
  BIOS Version: server-name.2.0.7c.0.071620151216
  Backup BIOS Version: server-name.2.0.7c.0.071620151216
  Boot Order: (none)
  Boot Override Priority:
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: Enabled
  Last Configured Boot Order Source: CIMC

Server /server/bios/boot-device # show boot-device detail
Boot Device HTTP-Test:
  Device Type: HTTP-Test
  Device State: Enabled
  Device Order: 1
  Slot Id: MLOM
  Port Number: 10
  MAC Address: 00:25:B5:00:01:2b
  IP Type: IPv4
  IP Config Type: DHCP
  URI: http://www.cloudboot.com:80/EFI/rhel_82_dvd.iso
```

次に、ブート順序を構成し、IPタイプ:[静的 (Static)]にHTTPブートデバイスを作成し、新しいデバイスの属性を設定し、トランザクションをコミットする例を示します。

```
Server# scope server 1
Server /server # scope bios
Server /server/bios # create boot-device HTTP-Test HTTP
Server /server/bios # scope boot-device HTTP-Test
Server /server/bios/boot-device # set status enabled
Server /server/bios/boot-device # set port 10
Server /server/server/bios /boot-device # set order 1
Server /server/bios /boot-device # set slot MLOM
Server /server/bios/boot-device # set macaddress 00:25:B5:00:01:2b
Server /server/bios/boot-device # set ipconfig-type Static
Server /server/bios/boot-device # set iptype IPv6C240-WZP21360Z1B /bios/boot-device *#
set ipaddress 2001:420:5446:2014::330:12
Server /server/bios/boot-device *# set netmask_or_ipv6prefix 64
Server /server/bios/boot-device *# set gateway 2001:420:5446:2014::330:1
Server /server/bios/boot-device *# set dnsserver 2001:420:c0e0:1008::118
Server /server/bios/boot-device *# commit
Server /server/bios/boot-device *# set uri http://cisco.com/a.iso
Server /server/bios/boot-device *# commit
Server /server/bios/boot-device # show detail
Boot Device http_test:
  Device Type: HTTP
  Device State: Disabled
  Device Order: 1
  Slot Id: MLOM
  Port Number: 10
  MAC Address: aa:aa:aa:aa:aa:aa
  IP Type: IPv6
  IP Config Type: Static
  URI: http://cisco.com/a.iso
  IP Address: 2001:420:5446:2014::330:12
  Netmask/IPV6 Prefix: 64
  Gateway: 2001:420:5446:2014::330:1
  DNS Server: 2001:420:c0e0:1008::118
Server /server/bios/boot-device #
```

### 次のタスク

サーバーを再起動して、新しいブート順でブートします。

## ブートデバイスの属性の変更



- (注) ホストがBIOS電源投入時自己診断テスト (POST) を実行している間は、ブート順を変更しないでください。

### 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>scope boot-device</b> はブート デバイス名を作成しました。	作成したブート可能デバイスの管理を入力します。
ステップ 3	Server /bios /boot-device # <b>set state</b> { <i>Enabled</i>   <i>Disabled</i> }.	デバイスをイネーブルまたはディセーブルにしますデフォルトのステータスはディセーブルです。  (注) イネーブルである場合、デバイスはレガシーのブート順序の設定を上書きします。
ステップ 4	Server /bios /boot-device* # <b>set order</b> { <i>Index</i>   1-50}	デバイス リストの特定のデバイスのブート順序を指定します。作成したデバイスの総数に基づいて、1 ~ 50 の範囲の数字を入力します。  (注) ブートデバイス順序を個別に設定すると、設定したとおり順序が表示されるかの保証はありません。そのため、1 回の実行で複数のデバイスの順序を設定する場合は、 <b>re-arrange-boot-device</b> コマンドを使用することを推奨します。
ステップ 5	Server /bios /boot-device* # <b>set port</b> { <i>value</i>   1-255 }	デバイスが装着されているスロットのポートを指定します。1 ~ 255 の範囲内の数を入力してください。
ステップ 6	Server /server/bios /boot-device* # <b>set iptype</b> { <i>value</i>   <i>IPv4</i>   <i>IPv6</i> }.	デバイスの IP タイプを指定します。
ステップ 7	Server /server/bios /boot-device* # <b>set macaddress</b> { <i>value</i> }.	ネットワーク イーサネット インターフェイスの MAC アドレスを設定します。
ステップ 8	Server /server/bios /boot-device* # <b>set ipconfig-type</b> { <i>value</i>   <i>DHCP</i>   <i>Static</i> }.	デバイスの IP 構成タイプを指定します。

	コマンドまたはアクション	目的
ステップ 9	Server /server/bios /boot-device* # <b>set uri</b> {value}.	すべての OS iso および EFI ファイルが置かれている URI パスを指定します。
ステップ 10	Server /bios /boot-device* # <b>commit</b>	トランザクションをシステムの設定にコミットします。

## 例

次に、既存のデバイスの属性を変更する例を示します。

```
Server# scope bios
Server /bios *# scope boot-device scu-device-hdd
Server /bios/boot-device # set status enabled
Server /bios/boot-device *# set order 2
Server /bios/boot-device *# set port 1
Server /bios/boot-device *# commit
Enabling boot device will overwrite boot order Level 1 configuration
Continue?[y|N]y
Server /bios/boot-device #
```

次に、既存の HTTP ブートデバイスの属性を変更する例を示します。

```
Server# scope server 1
Server /server # scope bios
Server /server/bios *# scope boot-device http-test
Server /server/bios/boot-device # show detail
Boot Device http-test:
  Device Type: HTTP
  Device State: Disabled
  Device Order: 3
  Slot Id: 1
  Port Number: 10
  MAC Address: 00:25:B5:00:01:2b
  IP Type: IPv4
  IP Config Type: DHCP
  URI: http://www.cloudboot.com:80/EFI/rhel_82_dvd.iso

Server /server/bios/boot-device # set iptype IPv6
Server /server/bios/boot-device *# set slot 34
Server /server/server/bios /boot-device # set order 1
Server /server/bios/boot-device *# set macaddress 00:25:B5:00:01:2c
Server /server/bios/boot-device *# set uri http://www.cloudboot.com:80/dvd.iso
Server /server/bios/boot-device *# commit
Server /server/bios/boot-device # show detail
Boot Device http-test:
  Device Type: HTTP
  Device State: Disabled
  Device Order: 3
  Slot Id: 34
  Port Number: 10
  MAC Address: 00:25:B5:00:01:2c
  IP Type: IPv6
  IP Config Type: DHCP
  URI: http://www.cloudboot.com:80/dvd.iso

Server /server/bios/boot-device #
```



## デバイスのブート順序の並べ替え



(注) ホストが BIOS 電源投入時自己診断テスト (POST) を実行している間は、ブート順を変更しないでください。

### 始める前に

このタスクを実行するには、`user` または `admin` 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンドモードを開始します。
ステップ 2	Server /bios # <b>rearrange boot-device</b> <i>[device name]:[position]</i>	選択したブート デバイスの順序を 1 回の実行で変更します。

### 例

次に、選択したブート デバイスの順序を変更する例を示します。

```
Server# scope bios
Server /bios # rearrange-boot-device TestPXE:1,TestUSB:2
Server /bios # show boot-device
Boot Device          Device Type  Device State  Device Order
-----
TestPXE              PXE         Disabled     1
TestUSB              USB         Disabled     2

Server /bios #
```

## ブート順序の設定の再適用



(注) ホストが BIOS 電源投入時自己診断テスト (POST) を実行している間は、ブート順を変更しないでください。

### 始める前に

このタスクを実行するには、`user` または `admin` 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>re-apply</b>	最後に設定されたブート順の送信元が BIOS の場合は、ブート順序を BIOS に再適用します。

## 例

次に、BIOS にブート順序を再適用する例を示します。

```
Server# scope bios
Server /bios # re-apply
Server /bios #
```

## 次のタスク

BIOS にブート順序を再適用した後に、ホストをリブートします。

## 既存のブートデバイスの削除



(注) ホストが BIOS 電源投入時自己診断テスト (POST) を実行している間は、ブート順を変更しないでください。

## 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>remove-boot-device device name</b>	特定のデバイスをブート順序から削除します。

## 例

次に、選択したデバイスをデバイス リストから削除する例を示します。

```
Server# scope bios
Server /bios # remove-boot-device scu-device-hdd
Server /bios #
```

## UEFI セキュア ブートの概要

オペレーティングシステムをロードし実行する前に、ロードおよび実行前のすべてのEFI ドライバ、EFI アプリケーション、オプション ROM またはオペレーティング システムが確実に署名され信頼性と整合性が確認されるために、Unified Extensible Firmware Interface (UEFI) のセキュア ブートを使用できます。Web UI または CLI を使用して、このオプションをイネーブルにできます。UEFI のセキュア ブート モードをイネーブルにすると、ブート モードは UEFI モードに設定され、UEFI のブート モードがディセーブルになるまで、設定されているブート モードを変更できません。



- (注) サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとする、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。



- 重要** また、サポートされていないアダプタを使用すると、Cisco IMC SEL のエラー ログ イベントが記録されます。エラー メッセージが次のように表示されます。

```
System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .
```

UEFI のセキュア ブートは次のコンポーネントでサポートされます。

コンポーネント	種類
サポートされている OS	<ul style="list-style-type: none"> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• ESX 6.7</li> <li>• ESX 6.5</li> <li>• ESXi 7.0</li> <li>• Linux</li> </ul>

コンポーネント	種類
<b>Broadcom PCI アダプタ</b>	<ul style="list-style-type: none"> <li>• 5709 デュアルおよびクアドポートアダプタ</li> <li>• 57712 10GBASE-T アダプタ</li> <li>• 57810 CNA</li> <li>• 57712 SFP ポート</li> </ul>
<b>Intel PCI アダプタ</b>	<ul style="list-style-type: none"> <li>• i350 クアドポートアダプタ</li> <li>• X520 アダプタ</li> <li>• X540 アダプタ</li> <li>• LOM</li> </ul>
<b>QLogic PCI アダプタ</b>	<ul style="list-style-type: none"> <li>• 8362 デュアルポートアダプタ</li> <li>• 2672 デュアルポートアダプタ</li> </ul>
<b>Fusion-io</b>	
<b>LSI</b>	<ul style="list-style-type: none"> <li>• LSI MegaRAID SAS 9240-8i</li> <li>• LSI MegaRAID SAS 9220-8i</li> <li>• LSI MegaRAID SAS 9265CV-8i</li> <li>• LSI MegaRAID SAS 9285CV-8e</li> <li>• LSI MegaRAID SAS 9285CV-8e</li> <li>• LSI MegaRAID SAS 9266-8i</li> <li>• LSI SAS2008-8i mezz</li> <li>• LSI Nytro カード</li> </ul>

## UEFI セキュア ブート モードのイネーブル化

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server/ BIOS # <b>set secure-boot enable   disable</b>	UEFI セキュアブートを有効または無効にします。

	コマンドまたはアクション	目的
		<p>(注) 有効にすると、ブートモードが UEFI セキュア モードに設定されます。UEFI セキュア ブートモードがディセーブルになるまでブートモードの設定は変更できません。</p> <p>(注) RFD (Reset Factory Default) の場合は、UEFI セキュア ブートを再度有効にする必要があります。</p>

例

次に、UEFI セキュア ブート モードをイネーブルにして、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # set secure-boot enable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

次のタスク

サーバーを再起動してコンフィギュレーションブートモード設定を有効にします。

## UEFI セキュア ブートのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# scope bios	BIOS コマンドモードを開始します。
ステップ 2	Server/ BIOS # set secure-boot enable   disable	UEFI セキュア ブートを有効または無効にします。

例

次に、UEFI セキュア ブート モードを無効にして、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # set secure-boot disable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

次のタスク

サーバーを再起動してコンフィギュレーションブートモード設定を有効にします。

## サーバーの実際のブート順の表示

サーバーの実際のブート順とは、サーバーが最後にブートされたときに BIOS によって実際に使用されたブート順です。実際のブート順は、Cisco IMC で設定されたブート順とは異なる場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	bios コマンドモードを開始します。
ステップ 2	Server /bios # <b>show actual-boot-order [detail]</b>	サーバーが最後に起動したときに実際に BIOS で使用されたブート順序を表示します。

例

次に、最後のブート以降のレガシーブート順序の実際のブート順序を表示する例を示します。

```
Server# scope bios
Server /bios # show actual-boot-order

Boot Order  Type                               Boot Device
-----
1           CD/DVD                                    CD-ROM
2           CD/DVD                                    Cisco Virtual CD/DVD 1.18
3           Network Device (PXE)                     Cisco NIC 23:0.0
4           Network Device (PXE)                     MBA v5.0.5 Slot 0100
5           Network Device (PXE)                     MBA v5.0.5 Slot 0101
6           Network Device (PXE)                     MBA v5.0.5 Slot 0200
7           Network Device (PXE)                     MBA v5.0.5 Slot 0201
8           Network Device (PXE)                     Cisco NIC 22:0.0
```

```

9           Internal EFI Shell           Internal EFI Shell
10          FDD                          Cisco   Virtual HDD    1.18
11          FDD                          Cisco   Virtual Floppy   1.18
    
```

Server /bios #

次に、最後のブート以降の高精度ブート順序の実際のブート順序を表示する例を示します。

Server /bios # **show actual-boot-order**

```

Boot Order  Boot Device                               Device Type      Boot Policy
-----
1           IBA GE Slot 0201 v1398                 PXE              TestPXE
2           IBA GE Slot 0200 v1398                 PXE              NonPolicyTarget
3           IBA GE Slot 0202 v1398                 PXE              NonPolicyTarget
4           IBA GE Slot 0203 v1398                 PXE              NonPolicyTarget
5           "UEFI: Built-in EFI Shell "           EFI              NonPolicyTarget
    
```

Server /bios #

## ワンタイム ブート デバイスでブートするようにサーバーを設定する

現在設定されているブート順序を中断することなく、次回のサーバーのブートに対してのみ、特定のデバイスから起動するようにサーバーを設定できます。ワンタイム ブート デバイスからサーバーを起動すると、事前に設定されているブート順で以降のすべてのリブートが行われます。

### 始める前に

このタスクを実行するには、`user` または `admin` 権限でログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios <b>show boot-device</b>	使用可能なブート ドライブのリストを表示します。
ステップ 3	Server #/bios <b>set one-time-boot-device device-order</b>	サーバのブート順を設定します。  (注) 無効になっている拡張ブート デバイスで設定されている場合でも、ホストはワンタイムブートデバイスに対して起動します。
ステップ 4	Server# /bios * <b>commit</b>	トランザクションをコミットします。
ステップ 5	(任意) Server# /bios <b>show detail</b>	BIOS の詳細を表示します。

## 例

次に、ワンタイム ブート デバイスで起動するサーバを設定する例を示します。

```
Server scope bios
Server /bios # show boot-device
Boot Device                               Device Type  Device State  Device Order
-----
KVMDVD                                    VMEDIA      Enabled       1
vkvm                                       VMEDIA      Enabled       2

Server /bios # set one-time-boot-device KVMDVD
Server /bios *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]n
Changes will be applied on next reboot.
Server /bios # show detail
BIOS:
  BIOS Version: "C240M3.3.0.0.9 (Build Date: 10/02/16)"
  Boot Order: (none)
  FW Update/Recovery Status: None, OK
  UEFI Secure Boot: disabled
  Configured Boot Mode: Legacy
  Actual Boot Mode: Legacy
  Last Configured Boot Order Source: CIMC
  One time boot device: KVMDVD
Server /bios #
```

## ユーザ定義のサーバの説明とアセットタグの割り当て

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>set description</b> <Server Description>	サーバの説明を入力します。
ステップ 3	Server /chassis* # <b>set asset-tag</b> <Asset Tag>	アセット タグを入力します。
ステップ 4	Server /chassis* # <b>commit</b>	トランザクションをコミットします。
ステップ 5	(任意) Server /chassis # <b>show detail</b>	サーバの詳細を表示します。

## 例

この例は、ユーザ定義のサーバの説明とアセットタグを割り当てる方法を示しています。

```
Server# scope chassis
Server/chassis # set description DN1-server
```



```

Server/chassis* # set asset-tag powerpolicy
Server /chassis* # commit
Server /chassis # show detail
Chassis:
  Power: on
  Serial Number: FCH1834V23X
  Product Name: UCS C220 M4S
  PID : UCSC-C220-M4S
  UUID: 414949AC-22D6-4D0D-B0C0-F7950E9217C1
  Locator LED: off
  Description: DN1-server
  Asset Tag: powerpolicy
Server /chassis #

```

## サーバーのリセット



**重要** ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをリセットしないでください。

### 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>power hard-reset</b>	確認プロンプトの後に、サーバーがリセットされます。

### 例

次に、サーバーをリセットする例を示します。

```

Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
Continue?[y|N]

```

# サーバーのシャットダウン



**重要** ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをシャットダウンしないでください。

## 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシモードを開始します。
ステップ 2	Server /chassis # <b>power shutdown</b>	サーバをシャットダウンします。

## 例

次に、サーバをシャットダウンする例を示します。

```
Server# scope chassis
Server /chassis # power shutdown
```

# サーバーの電源管理

## サーバーの電源投入



(注) サーバの電源が Cisco IMC 経由以外の何らかの方法でオフにされた場合、サーバは電源をオンにしてもすぐにはアクティブになりません。この場合、Cisco IMC が初期化を完了するまで、サーバはスタンバイモードに入ります。



**重要** ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源を変更しないでください。

### 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>power on</b>	サーバの電源をオンにします。
ステップ 3	プロンプトで、 <b>y</b> を入力して確認します。	サーバの電源をオンにします。

### 例

次に、サーバの電源をオンにする例を示します。

```
Server# scope chassis
Server /chassis # power on
Warning: System is already powered ON, this action is ineffective.
Do you want to continue?[y|N]y
```

## サーバーの電源オフ



**重要** ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源をオフにしないでください。

### 始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>power off</b>	サーバーの電源をオフにします。

**例**

次に、サーバーの電源をオフにする例を示します。

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name  UUID
-----
off   Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

## サーバー電源の再投入



**重要** ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源を再投入しないでください。

**始める前に**

このタスクを実行するには、**user** または **admin** 権限を持つユーザとしてログインする必要があります。

**手順**

	コマンドまたはアクション	目的
<b>ステップ 1</b>	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
<b>ステップ 2</b>	Server /chassis # <b>power cycle</b>	サーバ電源を再投入します。

**例**

次に、サーバ電源を再投入する例を示します。

```
Server# scope chassis
Server /chassis # power cycle
```

# 電力ポリシーの設定

## 電力制限



**重要** このセクションは、一部の UCS C シリーズのサーバでのみ利用可能です。

パワー キャッピングによって、サーバの電力消費をアクティブに管理する方法が決定されます。パワー キャッピング オプションを有効にすると、システムにより電力消費がモニタされ、割り当てられている電力制限を超えないように電力が維持されます。サーバが電力制限を維持できない場合、またはプラットフォームの電力を修正時間内に指定の電力制限に戻すことができない場合、[電力プロファイル (Power Profile)] 領域の [アクション (Action)] フィールドに指定したアクションがパワー キャッピングにより実行されます。

パワー キャッピングが有効になったら、定義された属性を持つ標準電力プロファイルまたは詳細電力プロファイルを使用できるように複数の電力プロファイルを設定できます。標準電力プロファイルを選択する場合は、電力制限、修正時間、修正アクション、中断期間、ハードキャップ、ポリシー状態 (有効な場合) を設定できます。詳細電力プロファイルを選択する場合は、標準電力プロファイルの属性の他に、ドメイン固有の電力制限、安全スロットルレベル、周囲温度に基づくパワー キャッピング属性も設定できます。



(注) 次に示す変更は、Cisco UCS C シリーズ リリース 2.0(13) 以降に適用されます。

- 2.0(13) リリースへのアップグレード後、ホストの電源を初めてオンにするときに、電力特性評価が自動的に実行されます。それ以降は、電力特性評価は [電力特性評価の実行 (Run Power Characterization)] セクションで指定されているとおりに開始する場合にのみ実行されます。
- また、サーバへの電源再投入が行われ、CPU または DIMM の設定が変更されている場合にも、初回ホスト ブート時に電力特性評価が自動的に実行されます。PCIe アダプタ、GPU、HDD などのハードウェアが変更されている場合は、電力特性評価は実行されません。特性評価された電力範囲は、ホストの電源再投入後に存在するコンポーネントに応じて変更されます。

Web UI の [パワー キャッピング設定 (Power Cap Configuration)] タブの [電力特性評価の実行 (Run Power Characterization)] オプションを選択すると、ホストの電源が再投入され、電力特性評価が開始されます。

## 電源の冗長性ポリシーの設定

### 始める前に

このアクションを実行するには、**admin**権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope sensor</b>	センサー コマンドを入力します。
ステップ 2	Server /sensor # <b>scope psu-redundancy-policy</b>	psu 冗長性ポリシー コマンドを入力します。
ステップ 3	Server /sensor/psu-redundancy-policy # <b>set psu-redundancy-policyvalue</b>	<p>設定する次の冗長性値のいずれか1つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>non-redundant</b> - N（使用可能な PSU 出力性能）は、インストールされている PSU の数に等しくなります。この場合、PSU のエラー、またはグリッドのエラーはサポートされません。</li> <li>• <b>[N+1] : N</b>（使用可能な PSU 出力性能）は、インストールされている PSU の数から 1 を引いた数に等しくなります。この場合、単一の PSU のエラーはサポートされますが、グリッドのエラーはサポートされません。</li> <li>• <b>grid</b> - N（使用可能な PSU 出力性能）は、インストールされている PSU の数の半分に等しくなります。この場合、N 個の PSU のエラー、またはグリッドのエラーがサポートされます。このポリシーは、N 個の PSU を 1 つのフィードに接続し、別の N 個の PSU を別のフィードに接続したことを暗黙的に示しています。</li> </ul>
ステップ 4	Server /sensor/psu-redundancy-policy* # <b>commit</b>	トランザクションをサーバにコミットします。

	コマンドまたはアクション	目的
ステップ 5	(任意) Server /sensor/psu-redundancy-policy #show detail	パワー冗長性ステータスを表示します。

例

次に、サーバのパワー冗長性を設定する例を示します。

```
Server / #scope sensor
Server /sensor #scope psu-redundancy-policy
Server /sensor/psu-redundancy-policy # set psu-redundancy-policy grid
Server /sensor/psu-redundancy-policy* # commit
Server /sensor/psu-redundancy-policy # show detail
PSU Redundancy Policy: grid
Server /sensor/psu-redundancy-policy #
```

## 電力特性評価の有効化

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# scope chassis	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # scope power-cap-config	電力制限コマンドモードを開始します。
ステップ 3	Server /chassis # run-pow-char-at-boot	ブート時に電力特性評価を実行します。
ステップ 4	Server /chassis # commit	トランザクションをシステムにコミットします。

例

次に、ホスト リブート時に電力特性評価を自動的に呼び出す例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # run-pow-char-at-boot
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

## 電力制限ポリシーの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

### 始める前に

このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope power-cap-config</b>	電力制限コマンドモードを開始します。
ステップ 3	Server /chassis /power-cap-config# <b>set pow-cap-enable {yes   no}</b>	サーバへの電力制限をイネーブルまたはディセーブルにします。
ステップ 4	Server /chassis /power-cap-config# <b>commit</b>	トランザクションをシステムの設定にコミットします。

### 例

次に、電力制限ポリシーをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

## Power Cap 範囲の確認

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

### 始める前に

このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Chassis power-cap-config # <b>show detail</b>	power cap 範囲の詳細の表示します。 [プラットフォーム最小値 (スロットリングを許可)] - CPU のスロットリング



	コマンドまたはアクション	目的
		<p>が有効になっているときのシャーシの電力の下限です。プラットフォーム最小値としてこれを使用するには、標準または高度な電力プロファイル範囲 <b>allow-throttle</b> フィールドを <b>enabled</b> に設定します。</p> <p><b>[プラットフォーム最小値 (効率的)]</b> - CPU のスロットリングが無効になっているときのシャーシの電力の下限です。</p> <p><b>[CPU 最小値 (スロットリングを許可)]</b> - スロットリングが有効になっているときに CPU ドメインの電力の下限です。CPU 最小値としてこれを使用するには、標準または高度な電力プロファイル範囲内の <b>allow-throttle</b> フィールドを <b>enabled</b> に設定します。</p> <p><b>[CPU 最小値 (効率的)]</b> - これは、スロットリングが無効になっているときの、CPU ドメインの電力の下限です。</p>

例

```
Power Characterization Enabled: yes
  Power Capping: yes
  Power Characterization Status: Completed
  Platform Min (Allow-Throttle) (W): 164
  Platform Min (Efficient) (W): 286
  Platform Max (W): 582
  Memory Min (W): 2
  Memory Max (W): 5
  CPU Min (Allow-Throttle) (W): 64
  CPU Min (Efficient) (W): 177
  CPU Max (W): 330
```

## 標準の電力プロファイルの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

始める前に

- 電力制限が有効にされている必要があります。
- このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope power-cap-config</b>	電力制限コマンド モードを開始します。
ステップ 3	Server /chassis /power-cap-config# <b>set pow-cap-enable {yes   no}</b>	システムの電力制限機能をイネーブルまたはディセーブルにします。
ステップ 4	Server /chassis /power-cap-config# <b>scope power-profile standard</b>	電力プロファイルの標準のコマンドモードを開始します。
ステップ 5	Server /chassis /power-cap-config# <b>set allow-throttle yes   no</b>	スロットリング状態 (T 状態) とメモリスロットルをプロセッサで強制的に使用させるために電力制限を維持するようにシステムを有効または無効にします。
ステップ 6	Server /chassis /power-cap-config# <b>set corr-time value</b>	<b>Action</b> モードで指定したアクションが実行される前に、プラットフォームの電力が指定された電力制限に戻る必要のある時間を設定します。  有効な範囲は 3 ~ 600 秒です。デフォルトは 3 秒です。
ステップ 7	Server /chassis /power-cap-config# <b>set except-action alert   shutdown</b>	指定した電力制限が修正用の時間内に維持されない場合に実行されるアクションを指定します。次のいずれかになります。  <ul style="list-style-type: none"> <li>• <b>Alert</b> : Cisco IMC SEL にイベントを記録します。</li> <li>• <b>Shutdown</b> : ホストをグレースフルシャットダウンします。</li> <li>• <b>None</b> : アクションは実行されません。</li> </ul>
ステップ 8	Server /chassis /power-cap-config# <b>set hard-cap yes   no</b>	電力消費を指定した電力制限未満の値に維持するようにシステムを有効または無効にします。
ステップ 9	Server /chassis /power-cap-config# <b>set pow-limit value</b>	電力制限を指定します。

	コマンドまたはアクション	目的
		指定した範囲内の値を入力します。
ステップ 10	Server /chassis /power-cap-config# <b>set susp-pd</b> {h:m-h:m   /All,Mo,Tu,We,Th,Fr,Sa,Su. }	電力制限プロファイルがアクティブにならない時間を指定します。
ステップ 11	Server /chassis /power-cap-config# <b>commit</b>	トランザクションをシステムにコミットします。

### 例

次に、標準の電力プロファイルを設定する例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advance
Server /chassis/power-cap-config # set allow-throttle yes
Server /chassis/power-cap-config* # set corr-time 6
Server /chassis/power-cap-config* # set except-action alert
Server /chassis/power-cap-config* # set hard-cap yes
Server /chassis/power-cap-config* # set pow-limit 360
Server /chassis/power-cap-config* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config* # commit
Server /chassis/power-cap-config # show detail
Power Cap Config:
  Power Characterization Enabled: yes
  Power Capping: no
  Power Characterization Status: Completed
  Platform Min (Allow-Throttle) (W): 164
  Platform Min (Efficient) (W): 290
  Platform Max (W): 581
  Memory Min (W): 2
  Memory Max (W): 5
  CPU Min (Allow-Throttle) (W): 64
  CPU Min (Efficient) (W): 177
  CPU Max (W): 330
```

## 詳細電力プロファイルの設定

これらの設定は、一部の UCS C シリーズ サーバでのみ行うことができます。

### 始める前に

- パワー キャッシングをイネーブルにする必要があります。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope power-cap-config</b>	電力制限コマンド モードを開始します。
ステップ 3	Server /chassis /power-cap-config # <b>set pow-cap-enable {yes   no}</b>	サーバの電力制限機能をイネーブルまたはディセーブルにします。
ステップ 4	Server /chassis /power-cap-config # <b>commit</b>	トランザクションをシステムにコミットします。
ステップ 5	Server /chassis /power-cap-config # <b>scope power-profile advanced</b>	電力プロファイルの高度なコマンドモードを開始します。
ステップ 6	Server/chassis/power-cap-config/power-profile # <b>set allow-throttle {yes   no}</b>	スロットリング状態 (T 状態) とメモリスロットルをプロセッサで強制的に使用させるために電力制限を維持するようにシステムを有効または無効にします。
ステップ 7	Server/chassis/power-cap-config/power-profile # <b>set corr-time value</b>	<b>Action</b> モードで指定したアクションをとる前に、プラットフォームを指定した電力制限に戻すための是正処置を実行する際の最大時間を設定します。  有効な範囲は 3 ~ 600 秒です。デフォルトは 3 秒です。
ステップ 8	Server /chassis /power-cap-config/power-profile # <b>set cpu-power-limit value</b>	CPU の電力制限を指定します。  指定された範囲内の電力 (ワット単位) を入力します。
ステップ 9	Server/chassis/power-cap-config/power-profile # <b>set except-action {alert   shutdown}</b>	指定した電力制限が修正用の時間内に維持されない場合に実行されるアクションを指定します。次のいずれかになります。  <ul style="list-style-type: none"> <li>• <b>Alert</b> : Cisco IMC SEL にイベントを報告します。</li> <li>• <b>Shutdown</b> : ホストをグレースフルシャットダウンします。</li> <li>• <b>None</b> : アクションは実行されません。</li> </ul>

	コマンドまたはアクション	目的
ステップ 10	Server/chassis/power-cap-config/power-profile # <b>set hard-cap</b> {yes no}	電力消費を指定した電力制限未満の値に維持するようにシステムを有効または無効にします。
ステップ 11	Server /chassis /power-cap-config/power-profile # <b>set mem-pow-limit</b> value	メモリの電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 12	Server /chassis /power-cap-config/power-profile # <b>set fail-safe-timeout</b> value	プラットフォームやCPUの電力読み取りの消失などの内部的な障害で電力制限機能が影響を受けた場合の安全なスロットルポリシーを指定します。 有効な範囲は1～10秒です。
ステップ 13	Server /chassis /power-cap-config/power-profile # <b>set plat-safe-Tlvl</b> value	プラットフォームのスロットリングレベルをパーセンテージで指定します。 範囲は、0～100です。
ステップ 14	Server /chassis /power-cap-config/power-profile # <b>set plat-temp</b> value	差し込み口の温度センサーを指定します。 摂氏（°C）で値を入力します
ステップ 15	Server /chassis /power-cap-config/power-profile # <b>set pow-limit</b> value	電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 16	Server /chassis /power-cap-config/power-profile # <b>set susp-pd</b> {h:m-h:m   /All,Mo,Tu,We,Th,Fr,Sa,Su. }	電力制限プロファイルがアクティブにならない時間を指定します。
ステップ 17	Server /chassis /power-cap-config/power-profile # <b>set thermal-power-limit</b> value	維持する電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 18	Server /power-cap-config/power-profile # <b>commit</b>	トランザクションをシステムの設定にコミットします。

例

次に、高度な電力プロファイル設定を行う例を示します。

```
Server# scope chassis
```

```

Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advanced
Server /chassis/power-cap-config/power-profile # set allow-throttle yes
Server /chassis/power-cap-config/power-profile* # set corr-time 6
Server /chassis/power-cap-config/power-profile* # set cpu-power-limit 259
Server /chassis/power-cap-config/power-profile* # set except-action alert
Server /chassis/power-cap-config/power-profile* # set hard-cap yes
Server /chassis/power-cap-config/power-profile* # set mem-pow-limit 259
Server /chassis/power-cap-config/power-profile* # set fail-safe-timeout 10
Server /chassis/power-cap-config/power-profile* # set plat-safe-Tlvl 50
Server /chassis/power-cap-config/power-profile* # set plat-temp 35
Server /chassis/power-cap-config/power-profile* # set pow-limit 360
Server /chassis/power-cap-config/power-profile* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config/power-profile* # set thermal-power-limit 354
Server /chassis/power-cap-config/power-profile* # commit
Server /chassis/power-cap-config/power-profile #

```

## 電力プロファイルのデフォルトへのリセット

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

### 始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope power-cap-config</b>	電力制限コマンドモードを開始します。
ステップ 3	Server /chassis # <b>reset-power-profile-to-defaults</b>	電力プロファイルの設定を工場出荷時のデフォルト値にリセットし、電力制限を無効にします。
ステップ 4	Server /chassis # <b>commit</b>	トランザクションをシステムにコミットします。

### 例

次に、電力プロファイルをデフォルトの設定値にリセットする例を示します。

```

Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # reset-power-profile-to-defaults
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #

```

## 電力制限設定の表示

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

### 始める前に

このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope power-cap-config</b>	電力制限設定コマンド モードを開始します。
ステップ 3	Server /chassis/power-cap-config# <b>showdetail</b>	電力特性評価に関する情報を表示します。

### 例

次に、電力制限設定に関する情報を表示する例を示します。

```
Server #scope chassis
Server/chassis # scope power-cap-config
Server /chassis/power-cap-config # show detail
Power Cap Config:
  Power Characterization Enabled: yes
  Power Capping: no
  Power Characterization Status: Completed
  Platform Min (Allow-Throttle) (W): 164
  Platform Min (Efficient) (W): 290
  Platform Max (W): 581
  Memory Min (W): 2
  Memory Max (W): 5
  CPU Min (Allow-Throttle) (W): 64
  CPU Min (Efficient) (W): 177
  CPU Max (W): 330
Server /chassis/power-cap-config #
```

## 電力統計情報の表示

このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

### 始める前に

このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>show power-monitoring</b>	最後にリブートされてから、サーバ、CPU、およびメモリが使用した電力が表示されます。

## 例

次に、個々のドメインの電力統計情報を表示する例を示します。

```
Server #scope chassis
Server /chassis # show power-monitoring
Domain      Current (W)  Minimum (W)  Maximum (W)  Average (W)
-----
Platform    180           160           504           180
CPU          53            33            275           53
Memory      2             2             6             2
Server /chassis #
```

## 電力復元ポリシーの設定

電力復元ポリシーによって、シャーシの電力供給が失われた後、サーバに電力を復元する方法が決定されます。

## 始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>Scope CIMC</b>	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /CIMC # <b>Scope power-restore-policy</b>	電力復元ポリシー コマンドを入力します。
ステップ 3	Server /CIMC/power-restore-policy # <b>set policy {power-off   power-on   restore-last-state}</b>	シャーシの電源が復旧した場合に実行するアクションを指定します。次のいずれかを選択します。 <ul style="list-style-type: none"> <li>• <b>power-off</b> : サーバーの電源は、手で投入されるまでオフのままになる</li> </ul>



	コマンドまたはアクション	目的
		<p>ります。これがデフォルトのアクションになります。</p> <ul style="list-style-type: none"> <li>• <b>power-on</b> : サーバの電源は、シャーシの電源が回復したときにオンになります。</li> <li>• <b>restore-last-state</b> : サーバの電源は、シャーシの電源が切断される前の状態に戻ります。</li> </ul> <p>選択したアクションが <b>power-on</b> の場合は、サーバに対して電源を回復するまでの遅延を選択できます。</p>
ステップ 4	(任意) Server /CIMC/power-restore-policy # <b>set delay</b> { <b>fixed</b>   <b>random</b> }	サーバの電源復元までの時間を固定するか、ランダムにするかを指定します。デフォルトは <b>fixed</b> です。このコマンドは、電力復元アクションが <b>power-on</b> の場合のみ使用可能です。
ステップ 5	(任意) Server /CIMC/power-restore-policy # <b>set delay-value</b> <i>delay</i>	遅延時間を秒単位で指定します。指定できる値の範囲は0～240です。デフォルトは0です。
ステップ 6	Server /CIMC/power-restore-policy # <b>commit</b>	トランザクションをシステムの設定にコミットします。

例

次に、180秒（3分）の固定遅延で電源をオンにする電力復元ポリシーを設定し、トランザクションをコミットする例を示します。

```

Server# scope CIMC
Server /CIMC # Scope power-restore-policy
Server /CIMC/power-restore-policy # set policy power-on
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy # set delay fixed
Server /CIMC/power-restore-policy *# set delay-value 180
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy # show detail
Power Restore Policy:
  Power Restore Policy: power-on
  Power Delay Type: fixed
  Power Delay Value(sec): 180

Server /CIMC/power-restore-policy #
    
```

# ファンポリシーの設定

## ファン制御ポリシー

ファン制御ポリシーを使ってファンの速度を制御することにより、サーバの消費電力を削減し、ノイズレベルを下げることができます。これらのファンポリシーが導入される前は、いずれかのサーバコンポーネントの温度が設定済みしきい値を超過した場合に、ファン速度が自動的に増加しました。ファン速度を低く抑えるために、通常、コンポーネントのしきい値温度を高い値に設定しました。この動作はほとんどのサーバ構成に最適でしたが、次のような状況に対処できませんでした。

- 最大の CPU パフォーマンス

高パフォーマンスを得るには、いくつかの CPU を設定済みしきい値よりもかなり低い温度に冷却する必要があります。これは非常に高速なファン速度を必要とし、結果として電力消費とノイズレベルが増大しました。

- 低電力消費

電力消費を最も低く抑えるにはファンを非常に遅くする必要があり、場合によっては、ファン停止をサポートするサーバで完全に停止する必要があります。ただし、ファンの速度を遅くすると、結果としてサーバが過熱します。この状況を回避するには、可能な最低速度よりもやや速くファンを作動させる必要があります。

ファンポリシーを導入すると、サーバ内のコンポーネントに基づき、そのサーバに適したファン速度を決定できます。さらに、最大の CPU パフォーマンスと低消費電力に関連する問題に対処するために、ファン速度を設定することができます。

次のファンポリシーの中から選択できます。

- **[バランス (Balanced)]** : この設定はほとんどのサーバ構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバには適していない可能性があります。
- **[低電力 (Low Power)]** : この設定は、PCIe カードが含まれない最小構成のサーバに最適です。
- **[高電力 (High Power)]** : このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバに最適です。
- **[最大電力 (Maximum Power)]** : この設定は、非常に高いファン速度を必要とするサーバ構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。
- **Acoustic** : この設定は、ファンのノイズレベルを設定するために使用できます。これにより、サーバのノイズリダクションが可能になります。

このポリシーを適用すると、システムパフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンスイベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断のない変更です。



- (注) このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C245 M6、C225 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。これらのサーバーでは、**[音響 (Acoustic)]** がデフォルトのファンポリシーです。

他のサーバーの場合、デフォルトのファンポリシーは、サーバー構成とサーバーに存在する PCIe カードの数によって異なります。



- (注) Cisco UCS M5 サーバーの場合、Cisco IMC でファンポリシーを設定することはできますが、実際のファン作動速度はサーバーの構成要件により決定されます。PCIe カードには、温度要件に応じて最小ファン速度のタグが付けられています。サーバーにこれらの PCIe カードが装備されている場合、タグ付けされた要件を下回るファンポリシーを構成することはできません。

**[構成ステータス (Configuration Status)]** には、Cisco UCS M5 サーバーで構成されたファンポリシーのステータスが表示されます。次のいずれかになります。

- **[SUCCESS]** : 選択されたファンポリシーはサーバで実行されている実際のファン速度に一致します。
- **[PENDING]** : 設定されたファンポリシーはまだ有効になっていません。この原因として、以下が考えられます。
  - サーバの電源がオフになっている
  - BIOS POST が完了していない
- **[ファンポリシーの上書き (FAN POLICY OVERRIDE)]** : 指定されたファン速度を、サーバーの設定要件によって決定された実際の速度で上書きします。



- (注)
- Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480-M5ML の場合、**[適用されるファンポリシー (Applied fan policy)]** は、サーバーに存在する PCIe カードによって異なります。
  - Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファンポリシー (Applied fan policy)]** は、サーバーに存在する PCIe カードまたは特定の CPU タイプによって異なります。

## ファンポリシーの設定

ファンポリシーは、サーバの冷却要件を決定します。ファンポリシーを設定する前に、容易に加熱する PCIe カードがサーバ内にあるかどうかを確認します。

### 始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope fan-policy</b>	ファンポリシー コマンド モードを開始します。
ステップ 3	Server /chassis/fan-policy # <b>set fan-policy</b>	<p>サーバのファンポリシーを設定します。次のいずれかを指定できます。</p> <ul style="list-style-type: none"> <li>• <b>[バランス (Balanced)]</b> : この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。</li> <li>• <b>[低電力 (Low Power)]</b> : この設定は、PCIe カードが含まれない最小構成のサーバに最適です。</li> <li>• <b>[高電力 (High Power)]</b> : このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバーに最適です。</li> <li>• <b>[最大電力 (Maximum Power)]</b> : この設定は、非常に高いファン速度を必要とするサーバー構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。</li> <li>• <b>Acoustic</b> : この設定は、ファンのノイズレベルを設定するために使用できます。これにより、サーバのノ</li> </ul>

	コマンドまたはアクション	目的
		<p>イズリダクションが可能になります。</p> <p>このポリシーを適用すると、システムパフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンス イベントがイベント ログに記録されている場合は、<b>低電力</b>などの標準のファン制御ポリシーを選択します。これは、中断のない変更です。</p> <p>(注) このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C245 M6、C225 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。これらのサーバーでは、<b>[Acoustic]</b>がデフォルトのファンポリシーです。</p> <p>他のサーバーの場合、デフォルトのファンポリシーは、サーバー構成とサーバーに存在する PCIe カードの数によって異なります。</p>
<p>ステップ 4</p>	<p>Server /chassis/fan-policy # <b>set aggressive-cooling</b><i>no</i>/<i>yes</i></p>	<p>このオプションを使用して、積極的な冷却を有効にします。</p>
<p>ステップ 5</p>	<p>Server /chassis/fan-policy # <b>commit</b></p>	<p>サーバへの変更をコミットします。</p>

例

次に、サーバのファンポリシーを最大電力に設定する例を示します。

```
server # scope chassis
server /chassis # scope fan-policy
server /chassis/fan-policy # set fan-policy maximum-power
server /chassis/fan-policy # set aggressive-cooling yes
```

```
server /chassis/fan-policy* # commit
server /chassis/fan-policy # show detail
  Fan Policy: maximum-power
  Applied Fan Policy: Max Power
  Configuration Status: SUCCESS
server /chassis/fan-policy #
```

## DIMM のブラックリストの設定

### DIMM のブラックリスト化

Cisco IMC で、デュアルインラインメモリモジュール (DIMM) の状態は、SEL イベントレコードに基づいています。BIOS が BIOS ポスト中のメモリテスト実行時に 16000 のエラー件数を伴う修正不可能なメモリエラーまたは修正可能なメモリエラーに遭遇した場合、DIMM は不良と判断されます。不良とマークされた DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco IMC はメモリテスト実行メッセージをモニタし、あらゆる時点で DIMM SPD データ内でメモリエラーに遭遇した DIMM をブラックリストに載せません。これにより、ホストはこれらの DIMM をマップから外すことができます。

DIMM がマップから外されるかまたはブラックリストに追加されるのは、修正不可能なエラーが発生した場合だけです。DIMM がブラックリスト化されると、同じチャンネル上にある他の DIMM が無視されるかディセーブルとなり、その DIMM は不良として見なされなくなります。



(注) 16000 修正可能エラーの場合、DIMM がマップから外されることや、ブラックリストに追加されることはありません。

### DIMM のブラックリストのイネーブル化

始める前に

管理者としてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope dimm-blacklisting</b> /	DIMM ブラックリストモードを開始します。
ステップ 2	Server /dimm-blacklisting # <b>set enabled</b> { <b>yes</b>   <b>no</b> }	DIMM ブラックリストをイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	Server /dimm-blacklisting* # <b>commit</b>	トランザクションをシステムの設定にコミットします。

例

次に、DIMM のブラックリストをイネーブルにする例を示します。

```
Server# scope dimm-blacklisting
Server /dimm-blacklisting # set enabled yes
Server /dimm-blacklisting* # commit
Server /dimm-blacklisting #
Server /dimm-blacklisting # show detail
```

```
DIMM Blacklisting:
  Enabled: yes
```

# BIOS の設定

## BIOS ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>show detail</b>	BIOS ステータスの詳細を表示します。

BIOS ステータス情報には、次のフィールドが含まれます。

名前	説明
BIOS Version	実行中の BIOS のバージョン文字列。
Boot Order	サーバが使用を試行する、ブート可能なターゲット タイプのレガシー ブート順序。
Boot Override Priority	None または HV のいずれかを選択できます。
FW Update/Recovery Status	保留中のファームウェア アップデートまたは回復アクションのステータス。
UEFI Secure Boot	UEFI セキュアブートを有効または無効にします。

名前	説明
Configured Boot Mode	BIOS がデバイスのブートを試行するブートモード。
Actual Boot Mode	BIOS がデバイスを起動した実際のブートモード。
Last Configured Boot Order Source	BIOS が最後に設定したブート順序送信元。

## Configuring BIOS Settings

### 始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンドモードを開始します。
ステップ 2	Server /bios # <b>scope input-output</b> <b>input-output power-up-manages-key-override</b>	設定コマンドモードを開始します。 各 BIOS 設定のオプションに関する説明および情報については、次のトピックを参照してください。 <a href="#">サーバー モデル別 BIOS パラメータ</a> 各設定タイプ間の変更をコミットする必要があります。 Server /bios/ # <b>commit</b>

### 例

次に、USB レガシー サポートを有効にするように BIOS を設定し、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # scope input-output
Server /bios/input-output # set UsbLegacySupport enabled
Server /bios/input-output *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/input-output #
```



## BIOS デフォルトの復元

### 始める前に

このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>bios-setup-default</b>	BIOS のデフォルト設定を復元します。 このコマンドでは、リブートが開始されます。

### 例

次の例は、BIOS デフォルト設定を復元します。

```
Server# scope bios
Server /bios # bios-setup-default
This operation will reset the BIOS set-up tokens to factory defaults.
All your configuration will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

## BIOS セットアップの開始

### 始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、**admin** 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>enter-bios-setup</b>	リブート時に BIOS セットアップを開始します。

### 例

次に、BIOS セットアップを開始できるようにする例を示します。

```
Server# scope bios
Server /bios # enter-bios-setup
This operation will enable Enter BIOS Setup option.
Host must be rebooted for this option to be enabled.
Continue?[y|N]y
```

## BIOS の工場出荷時のデフォルト設定への復元

BIOS のコンポーネントが正常に動作しない場合、BIOS セットアップ トークンを工場出荷時のデフォルト値に復元できます。



(注) このアクションは、一部の C シリーズ サーバに対してのみ使用できます。

### 始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- サーバの電源をオフにする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # <b>restore-mfg-defaults</b>	セットアップ トークンを工場出荷時のデフォルト値に復元します。

### 例

次に、BIOS セットアップ トークンを工場出荷時のデフォルト値に復元する例を示します。

```
Server # scope bios
Server /bios # restore-mfg-defaults
This operation will reset the BIOS set-up tokens to manufacturing defaults.
The system will be powered on.
Continue? [y|n] N
Server /bios #
```

## BIOS プロファイル

Cisco UCS サーバでは、デフォルトのトークン ファイルはすべての S3260 サーバプラットフォームで使用可能で、グラフィックユーザインターフェイス (GUI)、CLI インターフェイス、および XML API インターフェイスを使用して、これらのトークンの値を設定できます。

サーバーパフォーマンスを最適化するには、これらのトークン値を特定の組み合わせで設定する必要があります。

BIOS プロファイルを設定することで、正しい組み合わせのトークン値が設定された事前設定トークンファイルを使用することができます。利用可能な事前設定プロファイルには、仮想化、高性能、低電力などがあります。シスコの Web サイトから事前設定トークンファイルのさまざまなオプションをダウンロードし、BMC を介してサーバに適用できます。

ダウンロードしたプロファイルを編集し、トークンの値を変更したり、新しいトークンを追加したりできます。これにより、応答時間なしで、要件に合わせてプロファイルをカスタマイズできます。

## BIOS プロファイルの有効化

### 始める前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンドモードを開始します。
ステップ 2	Server# /bios <b>scope bios-profile</b>	BIOS プロファイルコマンドモードを開始します。
ステップ 3	Server# /bios/bios-profile <b>activate virtualization</b>	BIOS の設定をバックアップするように求めるメッセージが表示されます。y と入力します。
ステップ 4	BIOS のセットアップパラメータの変更を適用するためシステムを再起動するように求められます。y と入力します。	システムの再起動を開始します。

### 例

次に、指定した BIOS プロファイルをアクティブにする例を示します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # activate virtualization
It is recommended to take a backup before activating a profile.
Do you want to take backup of BIOS configuration?[y/n] y
backup-bios-profile succeeded.
bios profile "virtualization" deleted
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.
Server /bios/bios-profile #
```

## BIOS プロファイルのバックアップの取得

### 始める前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンドモードを開始します。
ステップ 2	Server# /bios <b>scope bios-profile</b>	BIOS プロファイルコマンドモードを開始します。
ステップ 3	Server# /bios/bios-profile <b>backup</b>	BIOS プロファイルのバックアップが成功したというメッセージが表示されます。

### 例

この例は、BIOS プロファイルをバックアップします。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # backup
backup-bios-profile succeeded.
Server /bios #
```

## BIOS プロファイルの削除

### 始める前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンドモードを開始します。
ステップ 2	Server# /bios <b>scope bios-profile</b>	BIOS プロファイルコマンドモードを開始します。
ステップ 3	Server# /bios/bios-profile <b>delete BIOS profile</b>	指定した BIOS プロファイルを削除します。

例

この例では、指定した BIOS プロファイルを削除します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # delete performance
Server /bios/bios-profile #
```

## BIOS プロファイルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios <b>show bios-profile</b>	すべての BIOS プロファイルを表示します。

例

次に、BIOS プロファイルを表示する例を示します。

```
Server # scope bios
Server /bios # show bios-profile
ID      Name          Active
-----
1       performance      yes
2       virtualization   no
3       none              no
4       cisco_backup     no
Server /bios #scope bios-profile
Server /bios #
```

## BIOS プロファイルの情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios <b>scope bios-profile</b>	すべての BIOS プロファイルを表示します。
ステップ 3	Server# /bios/bios-profile <b>info performance</b>	トークンの名前、プロファイル値、およびアクティブな値など BIOS プロファイルの情報を表示します。

## 例

この例では、指定した BIOS プロファイルの情報を表示します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # info performance
```

TOKEN NAME	PROFILE VALUE	ACTUAL VALUE
TPMAdminCtrl	Enabled	Enabled
ASPMsupport	Disabled	Disabled

```
Server /bios/bios-profile #
```

## BIOS プロファイルの詳細の表示

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios <b>scope bios-profile</b>	BIOS プロファイルコマンドモードを開始します。
ステップ 3	Server# /bios/bios-profile <b>show detail</b>	BIOS プロファイルの詳細が表示されます。

## 例

次に、BIOS プロファイルの詳細を表示する例を示します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # show detail
Active Profile: Virtualization
Install Status: bios profile install done
Server /bios/bios-profile #
```

## セキュアブート証明書の管理

4.2 (2a) リリース以降、Cisco IMC では、設定されたセキュア HTTP ブート デバイス用に最大 10 個の証明書をアップロードできます。構成された特定のブート デバイスの新しい証明書を削除してアップロードすることもできます。Cisco IMC では、最大 10 個のルート CA 証明書をアップロードできます。

## セキュアブート証明書の表示

### 始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server / bios # <b>scope secure-boot-certificate certificate_ID</b>	ここで、 <i>certificate_ID</i> は Cisco IMC によって割り当てられた ID です。
ステップ 3	Server / bios / secure-boot-certificate # <b>show detail</b>	証明書の詳細が表示されます。

### 例

この例は、セキュアブート証明書の詳細を表示する方法を示しています。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
server /bios/secure-boot-certificate # show detail
Secure Boot CA Certificate:
  Certificate ID: 3
  Serial Number: 04
  Subject Country Code (CC): XX
  Subject State (S): XX
  Subject Locality (L): XX
  Subject Organization (O): XX
  Subject Organizational Unit (OU): XX
  Subject Common Name (CN): *.XX
  Issuer Country Code (CC): XX
  Issuer State (S): XX
  Issuer Locality (L): XX
  Issuer Organization (O): XX
  Issuer Organizational Unit (OU): XX
  Issuer Common Name (CN): .XX
  Valid From: Month Date Time_Stamp 20xx GMT
  Valid To: Month Date Time_Stamp 20xx GMT
```

## 貼り付けオプションをしようしてセキュアブート証明書をアップロードする

### 始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server / bios # <b>scope secure-boot-certificate certificate_ID</b>	ここで、 <i>certificate_ID</i> は Cisco IMC によって割り当てられた ID です。  証明書がこの ID に既にアップロードされている場合は、証明書の詳細のみを表示できます。ステータスを確認するには、 <b>show detail</b> コマンドを使用します。
ステップ 3	Server / bios / secure-boot-certificate # <b>upload-paste-secure-boot-certificate</b>	証明書を貼り付けるように求められます。  ここに証明書を貼り付けてください。完了したら、CTRL+D を押します。

証明書が正常にアップロードされると、次のメッセージが表示されます。

セキュアブート証明書が正常に貼り付けられました。

## 例

この例は、貼り付けオプションを使用してセキュアブート証明書をアップロードする方法を示しています。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
server /bios/secure-boot-certificate # upload-paste-secure-boot-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDzCCAreAwIBAgIBBDANBgkqhkiG9w0BAQsFADCBnTELMakGA1UEBhMCMVVMx
EzARBgNVBAgMCkNhbm3JuaWEwEDAOBgNVBAMCMB05ld3lvcmsxETAPBgNVBAoM
CERpZ21jZXJOMRAwDgYDVQQLEAdTU0xERVBUmR8wHQYDVQQDDBYqLmNhLnRlc3Rp
bmcuY28uYmxyLm1uMSEwHwYJKoZIhvcNAQkBFhJhbm1pY2hhZUBjaXNjby5jb20w
HhcNMjAwNDI4MDQyNTM2WhcNMjIwNDI4MDQyNTM2WjCBODELMakGA1UEBhMCMCU4x
EjAQBgNVBAgMCUJlbmdhbHVydTESMBAGA1UEBwwJa2FybmF0YWthMQ8wDQYDVQQK
DAZPUkdDU1IxZzARBgNVBAwMCk9SR1VOSVRDU1IxIDAeBgNVBAMMFyouY3NyLnRl
c3RpbmcyYmxyLm1uMSEwHwYJKoZIhvcNAQkBFhJhbm1pY2hhZUBjaXNjby5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4oBCGcFmw/wcHkitn
TshWSc15+yI2aCmiCcVCUfRCX96erde+4QKW1UqCl291pL8CqnhKkKTWV154mcw2
RcZto+SpDrCJLJNgcuVmaU1sIoafNmc3DTLCDJvrlxE0ooJP8SgXdEngAm44DXz
Uw3/8nu3I7WLXu//tOxd0edHHv4V2ktFx5mLaU/QlRRBEyRuXtGyiRSE5h5YWWd0
TAZ0R2NzFhN7ymYg2GGMjEFKfDSK0mfsPbfQI5SMNLVieA3SqI98Y95o6y9UUbG0
2DQH409Z/F9w0NuNjz5vhtxS13ScNFQwRMLho/1JErV0SvV9vtuio+j3btQ+1CsF
VM91AgMBAAGjFTATMBEGCWCsAGG+EIBAQQEAWIGQDANBgkqhkiG9w0BAQsFAAOC
AQEAUzW7p3YhiEZfgBvR8D4iNsuV4J18BdzZmhDqA852tLprnh4HoWgMRt1YBO5B
7D5wJ7mgQn/TCqI1l1rNX8KUBDs+UYyDQBTxCuRZcM2QNaFogOJiQqHFugtjJZ4H
kUX06s9JmTns68dySQVJhHrY0b3sQdvWhzL8ryxDyg5EUu/m+O/FnxqU9CTEWEf
7E8ATB4dH82NlecRCbh2su4bC1PnMMi5g/w6pIMahMKHPVvVRQBw/0PsB0r1Rw2j
J6o61UR1J6L7bc8ij5ExX+UjYc1mR555jflNG+1Sty5H8oJtZDLoxNgOPzyb4U6C
1jPN+QPSVZOcLUjIMZYjB8qSDw==
```



```
-----END CERTIFICATE-----
Secure Boot Certificate pasted successfully.
```

次のタスク

**show detail** コマンドを使用して、証明書の詳細を確認できます。

## リモートの場所からセキュアブート証明書をアップロードする

始める前に

- このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。
- 生成された証明書のタイプが [Server] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。
ステップ 2	Server / bios # <b>scope secure-boot-certificate certificate_ID</b>	ここで、 <i>certificate_ID</i> は Cisco IMC によって割り当てられた ID です。  証明書がこの ID に既にアップロードされている場合は、証明書の詳細のみを表示できます。ステータスを確認するには、 <b>show detail</b> コマンドを使用します。
ステップ 3	Server / bios / secure-boot-certificate # <b>upload-remote-secure-boot-certificate tftp   ftp   sftp   scp   http IP_address/Hostname Remote_server_path_filename</b>	値は次のとおりです。  • <b>[tftp]、[ftp]、[sftp]、[scp]、[http]</b> はファイル転送用のプロトコルです  • <b>[サーバー IP アドレスまたはホスト名 (Server IP Address or Hostname) ]</b> : 証明書ファイルの保管先とするサーバーの IP アドレスまたはホスト名。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• [パスおよびファイル名 (Path and Filename) ]: リモート サーバーにファイルをアップロードする際に Cisco IMC が使用する必要があるパスおよびファイル名。</li> </ul> <p>ファイル転送プロトコルによっては、ユーザー名とパスワードの入力を求められる場合があります</p>

証明書が正常にアップロードされると、次のメッセージが表示されます。

セキュアブート証明書が正常にアップロードされました

### 例

次の例は、リモートロケーションオプションを使用してセキュアブート証明書をアップロードする方法を示しています (scp ファイル転送プロトコルを使用)。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
server /bios/secure-boot-certificate # upload-remote-secure-boot-certificate scp
10.10.10.10
/home/username/certificate.pem
Server (RSA) key fingerprint is xx:xx:8b:36:5a:53:14:d3:85:d0:xx:xx:e0:xx:24:51
Do you wish to continue? [y/N]y
Username: username
Password: password
Secure Boot Certificate uploaded successfully
```

### 次のタスク

**show detail** コマンドを使用して、証明書の詳細を確認できます。

## セキュアブート証明書の削除

### 始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope bios</b>	BIOS コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server / bios # <b>scope secure-boot-certificate</b> <i>certificate_ID</i>	ここで、 <i>certificate_ID</i> は Cisco IMC によって割り当てられた ID です。
ステップ 3	Server / bios / secure-boot-certificate # <b>delete-secure-boot-certificate</b>	[y] と入力して [Enter] を押して確定します。

次のメッセージが表示されます。

セキュアブート証明書: *ID* は削除されました

**例**

この例は、セキュアブート証明書を削除する方法を示しています。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
Server /bios/secure-boot-certificate # delete-secure-boot-certificate
Do you want to delete the existing secure boot certificate? [y|N]y
Secure Boot Certificate - 3 is deleted
```

## サーバコンポーネントのファームウェアの更新



**重要** ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをリセットしないでください。

**始める前に**

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

サーバの電源をオフにする必要があります。

**手順**

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>scope firmware</b>	ファームウェア コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis/firmware # <b>show detail</b>	一部のコンポーネント メッセージで必要なファームウェアの更新を表示します。
ステップ 4	Server /chassis/firmware # <b>update-all</b>	サーバ コンポーネントのファームウェアを更新します。

### 例

次に、サーバをリセットする例を示します。

```
Server# scope chassis
Server /chassis # scope firmware
Server /chassis / firmware # show detail

Firmware update required on some components,
please run update-all (under chassis/firmware scope).

Server /chassis / firmware # update-all
```

## 製品 ID (PID) カタログの詳細の表示

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server # <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # <b>show cpu-pid</b>	CPU PID の詳細を表示します。
ステップ 3	Server /chassis # <b>show dimm-pid</b>	メモリ PID の詳細を表示します。
ステップ 4	Server /chassis # <b>show pciadapter-pid</b>	PCIアダプタ PIDの詳細を表示します。
ステップ 5	Server /chassis # <b>show hdd-pid</b>	HDD PID の詳細を表示します。

### 例

次に、PID の詳細を表示する例を示します

```
Server # scope chassis
Viewing CPU PID details
Server /chassis # show cpu-pid
Socket Product ID Model
-----
```

```
CPU1 UCS-CPU-E52660B Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
CPU2 UCS-CPU-E52660B Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
```

**Viewing memory PID details**

Server /chassis # **show dimm-pid**

Name	Product ID	Vendor ID	Capacity	Speed
DIMM_A1	UNKNOWN	NA	Failed	NA
DIMM_A2	UNKNOWN	NA	Ignore...	NA
DIMM_B1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_B2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_C1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_C2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_D1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_D2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_E1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_E2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_F1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_F2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_G1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_G2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_H1	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866
DIMM_H2	UCS-MR-1X162RZ-A	0xCE00	16384 MB	1866

**Viewing PCI adapters PID details**

Server /chassis # **show pciadapter-pid**

Slot	Product ID	Vendor ID	Device ID	SubVendor ID	SubDevice ID
1	UCSC-MLOM-CSC-02	0x1137	0x0042	0x1137	0x012e

**Viewing HDD PID details**

Server /chassis # **show hdd-pid**

Disk	Controller	Product ID	Vendor	Model
1	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
2	SLOT-MEZZ	UCS-C3X60-HD4TB	SEAGATE	ST4000NM0023
3	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
4	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
5	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
6	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
7	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
8	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
9	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
10	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
11	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
12	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
13	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
14	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
15	SLOT-MEZZ	UCS-C3X60-HD4TB	SEAGATE	ST4000NM0023
16	SLOT-MEZZ	UCS-C3X60-HD4TB	SEAGATE	ST4000NM0023
19	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
28	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
54	SLOT-MEZZ	UCSC-C3X60-HD6TB	SEAGATE	ST6000NM0014
55	SLOT-MEZZ	UCSC-C3X60-HD6TB	SEAGATE	ST6000NM0014
56	SLOT-MEZZ	UCSC-C3X60-HD4TB	TOSHIBA	MG03SCA400
57	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...
58	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...
59	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...
60	SLOT-MEZZ	UCS-HD4T7KS3-E	WD	WD4001FYY...

Server /chassis #

## PID カタログのアップロードとアクティブ化



**注意** PID カタログがアクティブになると、BMC が自動的に再起動します。

PID カタログをアクティブ化した後、サーバを再起動する必要があります。

### 始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server# /chassis <b>scope pid-catalog</b>	PID カタログ コマンド モードを開始します。
ステップ 3	Server /chassis/pid-catalog # <b>upload-pid-catalog remote-protocol IP Address PID Catalog file</b>	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 <ul style="list-style-type: none"> <li>• TFTP</li> <li>• FTP</li> <li>• SFTP</li> <li>• SCP</li> <li>• HTTP</li> </ul>

	コマンドまたはアクション	目的
		<p>(注) Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。</p> <p>このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is &lt;server_finger_print_ID&gt; Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。</p> <p>フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。</p>
ステップ 4	(任意) Server# /chassis/pid-catalog show detail	アップロードのステータスが表示されます。
ステップ 5	Server# /chassis/pid-catalog activate	アップロードされた PID カタログをアクティブにします。
ステップ 6	Server# /chassis/pid-catalog show detail	アクティベーションのステータスが表示されます。

例

次に、PID カタログをアップロードし、アクティブにする例を示します。

```
Server # scope chassis
Server /chassis # scope pid-catalog
Uploading PID Catalog
Server /chassis/pid-catalog # upload-pid-catalog tftp 10.10.10.10
```

```

pid-ctlg-2_0_12_78_01.tar.gz
upload-pid-catalog initialized.
Please check the status using "show detail".
Server /chassis/pid-catalog #
Server /chassis/pid-catalog # show detail
    Upload Status: Upload Successful
    Activation Status: Please Activate Catalog
    Current Activated Version: N/A
Activating the uploaded PID catalog
Server /chassis/pid-catalog # activate
Successfully activated PID catalog
Server /chassis/pid-catalog # show detail
    Upload Status:
    Activation Status: Activation Successful
    Current Activated Version: 2.0(12.78).01
Server /chassis/pid-catalog #

```

## PID カタログを削除



**注意** PID カタログが削除されると、BMC が自動的に再起動します。

PID カタログを削除した後、サーバを再起動する必要があります。

### 始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope chassis</b>	シャーシ コマンド モードを開始します。
ステップ 2	Server#/chassis <b>scopepid-catalog</b>	PID カタログ コマンド モードを開始します。
ステップ 3	Server /chassis/pid-catalog # <b>delete</b>	確認プロンプトで <b>y</b> と入力し、PID カタログを削除します。  (注) PID カタログは、以前に更新およびアクティブ化されている場合にのみ削除できます。
ステップ 4	(任意) Server#/chassis/pid-catalog <b>show detail</b>	PID カタログのステータスを表示します。



## 例

次に、PID カタログをアップロードし、アクティブにする例を示します。

```
Server # scope chassis
Server /chassis # scope pid-catalog
Server /chassis/pid-catalog # delete
CIMC will be automatically rebooted after successful deletion of the uploaded catalog
file.
Once this is complete, a host reboot will be required for the catalog changes to be
reflected in
the BIOS and host Operating System Continue?[y|N]y
Server /chassis/pid-catalog # show detail
PID Catalog:
  Upload Status: N/A
  Activation Status: N/A
  Current Activated Version: 4.1(0.41)
Server /chassis/pid-catalog #
```

# 永続メモリ モジュール

## 永続メモリ モジュール

Cisco UCS C シリーズ リリース 4.0(4) は、Intel® Optane™ Data Center 永続メモリ モジュール (第二世代インテル® Xeon® Scalable プロセッサに基づく UCM M5 サーバ上) のサポートを導入します。永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

永続メモリ モジュールは、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。永続メモリ モジュールに保存されているデータは、他のストレージデバイスに比べてすぐにアクセスでき、電源サイクルで保持されます。

永続メモリ モジュールの設定の詳細については、『[Cisco UCS: Intel® Optane™ Data Center 永続メモリモジュールの設定と管理](#)』を参照してください。



## 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。