



アプライアンスの設定準備

- [アプライアンス設定の準備の概要](#) (1 ページ)
- [Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#) (2 ページ)
- [事前設定チェックの実行](#) (7 ページ)
- [ネットワーク インターフェイス カードの無効化](#) (10 ページ)
- [アプライアンスのイメージの再作成](#) (16 ページ)
- [Cisco DNA Center アプライアンスの設定](#) (22 ページ)

アプライアンス設定の準備の概要

Cisco DNA Center アプライアンスを正常に設定するには、まず、次のタスクを実行します。

1. アプライアンスの Cisco IMC に対するアクセスを有効にします（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照）。
2. Cisco IMC を使用して、ハードウェアとスイッチの重要な設定を確認、調整します（「[事前設定チェックの実行](#)」を参照）。
3. アプライアンスに付属する Intel X710-DA4 ネットワーク インターフェイス カード (NIC) が現在有効になっている場合は、これを無効にする必要があります（「[ネットワーク インターフェイス カードの無効化](#) (10 ページ)」を参照）。
4. Cisco DNA Center ソフトウェアはあらかじめアプライアンスにインストールされていますが、状況によってはソフトウェアを再インストールする必要が生じる場合があります（現在のクラスタリンク設定を変更する前など）。このような場合は、「[アプライアンスのイメージの再作成](#)」で説明されているタスクも実行する必要があります。



(注) アプライアンスのイメージを作成しなおす必要がない場合は、使用する設定ウィザードに固有の「アプライアンスの設定の概要」のトピックに進みます。

- [Maglev 設定ウィザード](#)
- [ブラウザベースの設定ウィザード \(44 および 56 コアアプライアンス\)](#)
- [ブラウザベースの設定ウィザード \(112 コアアプライアンス\)](#)


Cisco Integrated Management Controller に対するブラウザアクセスの有効化

「[アプライアンスのインストールワークフロー](#)」の説明に従ってアプライアンスをインストールした後、Cisco IMC 設定ユーティリティを使用して、アプライアンスの CiIMC ポートに IP アドレスとゲートウェイを割り当てます。この操作で Cisco IMC GUI にアクセスできるようになります。これはアプライアンスを設定するとき使用する必要があります。

Cisco IMC の設定が完了したら、Cisco IMC にログインし、「[事前設定チェックの実行](#)」に記載されているタスクを実行して、設定が正しいことを確認します。



ヒント お客様の環境のセキュリティを確保するため、アプライアンスの初回ブート時は、Cisco IMC ユーザのデフォルトパスワードを変更するように求められます。Cisco IMC ユーザパスワードを後で変更するには、次のように Cisco IMC GUI を使用します。

1. GUI の左上隅から **[Toggle Navigation]** アイコン () をクリックし、**[Admin] > [User Management]** を選択します。
[Local User Management] タブがすでに選択されている必要があります。
2. ユーザ**1**のチェックボックスをオンにして、**[Modify user]** をクリックします。
[Modify User Details] ダイアログボックスが開きます。
3. **[Change Password]** チェックボックスをオンにします。
4. 新しいパスワードを入力して確認し、**[Save]** をクリックします。

ステップ 1 次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- アプライアンスの前面パネルにある KVM コネクタ (「[前面パネルと背面パネル](#)」の前面パネル図のコンポーネント 11) に接続する KVM ケーブルか、

- アプライアンスの背面パネルにある USB ポートと VGA ポート（「前面パネルと背面パネル」の背面パネル図のコンポーネント 2 および 5）に接続するキーボードとモニタ。

ステップ 2 アプライアンスの電源コードが接続され、電源がオンになっていることを確認します。

ステップ 3 前面パネルの電源ボタンを押して、アプライアンスをブートします。

Cisco IMC 設定ユーティリティの次のようなブート画面が表示されます。

```

Cisco
CISCO

Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC
<F12> Network Boot

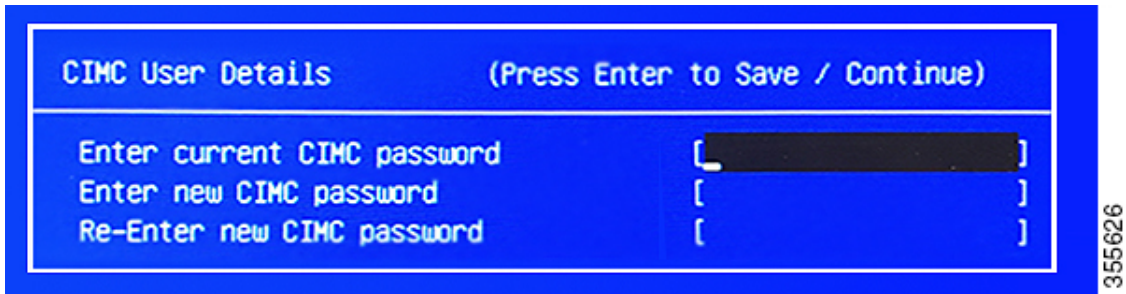
Bios Version : C220M5.3.0.3a.0.0321172055
Platform ID : C220M5

Cisco IMC IPv4 Address : 172.23.1.1
Cisco IMC MAC Address : 40:CE:24:00:00:00

Processor(s) Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz
Total Memory = 256 GB Effective Memory = 256 GB
Memory Operating Speed 2400 Mhz
    
```

ステップ 4 ブート画面が表示されたら、すぐに **F8** キーを押して Cisco IMC 設定を実行してください。

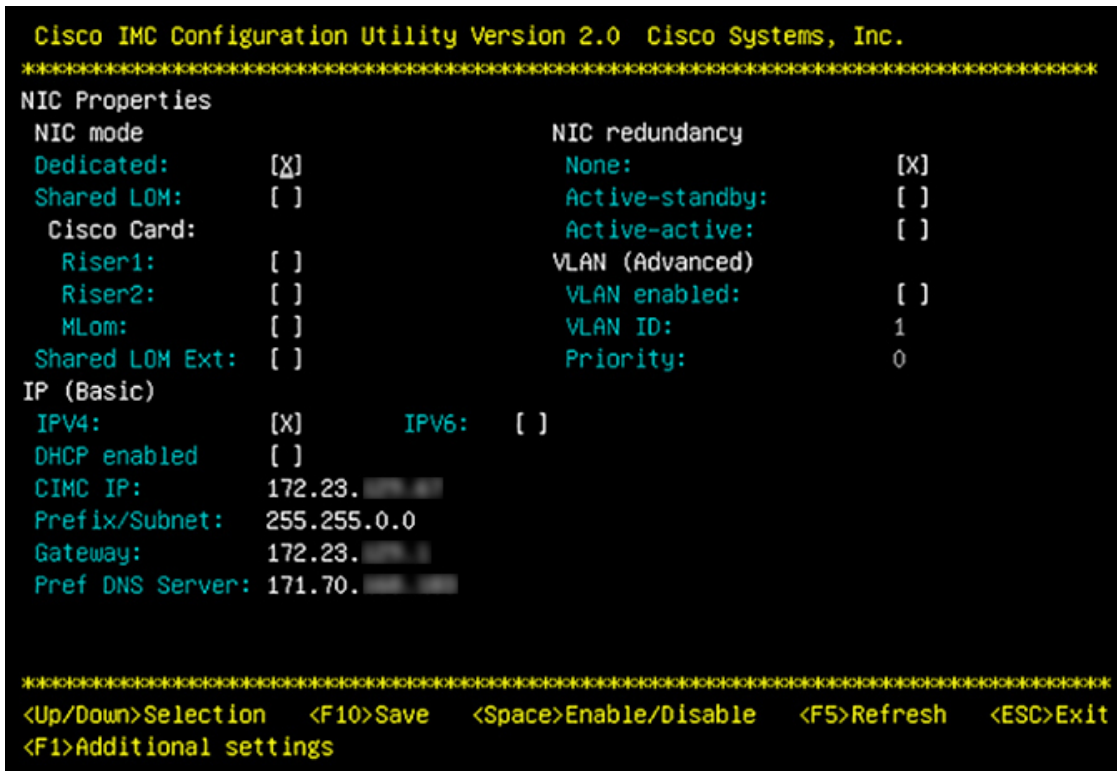
次に示すように、Cisco IMC 設定ユーティリティに **[CIMC User Details]** 画面が表示されます。



ステップ5 デフォルトの CIMC ユーザパスワード（新規アプライアンスで付与されるデフォルトのパスワードは「password」）を [Enter current CIMC Password] フィールドに入力します。

ステップ6 次に [Enter New CIMC Password] フィールドと [Re-Enter New CIMC Password] フィールドに新しい CIMC ユーザパスワードを入力して確認します。

[Re-Enter New CIMC Password] フィールドで **Enter** を押すと、次に示すように、Cisco IMC 設定ユーティリティに [NIC Properties] 画面が表示されます。



ステップ7 次のアクションを実行します。

- **NIC モード (NIC mode)** : [Dedicated] を選択します。
- **IP (基本)** : [IPV4] を選択します。
- **CIMC IP** : CIMC ポートの IP アドレスを入力します。

- プレフィックス/サブネット (Prefix/Subnet) : CIMC ポート IP アドレスのサブネットマスクを入力します。
- ゲートウェイ (Gateway) : 優先するデフォルトゲートウェイの IP アドレスを入力します。
- 優先DNSサーバ (Pref DNS Server) : 優先 DNS サーバの IP アドレスを入力します。
- NIC 冗長性 (NIC Redundancy) : [なし (None)] を選択します。

ステップ 8 F1 を押して [Additional Settings] を指定します。

次に示すように、Cisco IMC 設定ユーティリティに [Common Properties] 画面が表示されます。

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
Hostname:      C220-FCH212
Dynamic DNS:   [ ]
DDNS Domain:
FactoryDefaults
Factory Default: [ ]
Default User(Basic)
Default password:
Reenter password:
Port Properties
Auto Negotiation: [X]
                Admin Mode      Operation Mode
Speed [1000/100/10Mbps]:      Auto          1000
Duplex mode[half/full]:      Auto          full
Port Profiles
Reset: [ ]
Name:
*****
<Up/Down>Selection <F10>Save <Space>Enable/Disable <F5>Refresh <ESC>Exit
<F2>PreviousPageettings
    
```

ステップ 9 次のアクションを実行します。

- ホスト名 (Hostname) : このアプライアンスで使用する CIMC のホスト名を入力します。
- ダイナミックDNS (Dynamic DNS) : チェックボックスをオフにすると、この機能が無効になります。
- 出荷時の初期状態 (Factory Defaults) : チェックボックスをオフにして、この機能を無効にします。
- デフォルトのユーザ (基本設定) (Default User (Basic)) : フィールドを空白のままにします。
- ポートのプロパティ (Port Properties) : 新しい設定を入力するか、フィールドに表示されるデフォルト値を受け入れます。

- **ポートプロファイル (Port Profiles)** : チェックボックスをオフにすると、この機能が無効になります。

ステップ 10 F10 を押して、設定を保存します。

ステップ 11 **Esc** キーを押して終了し、アプライアンスをリブートします。

ステップ 12 設定が保存され、アプライアンスのリブートが完了したら、アプライアンスがインストールされているサブネットへのアクセスが可能なクライアントマシンで互換性のあるブラウザを開き、次の URL を入力します。

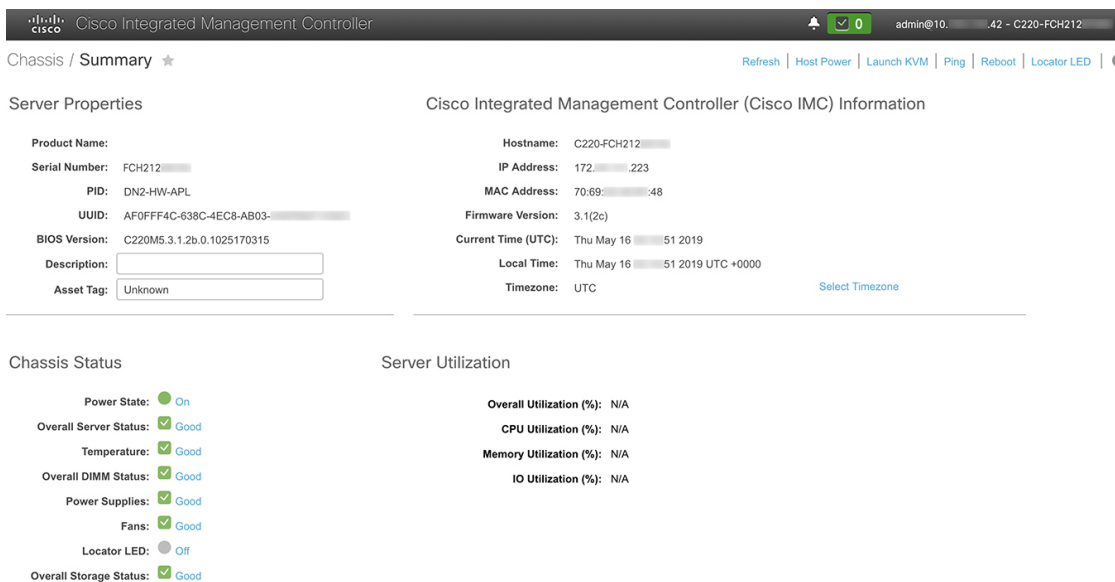
https://CIMC_ip_address (この **CIMC_ip_address** は先ほどステップ 7 で入力した Cisco IMC ポート IP アドレスです。

次に示すような Cisco IMC GUI のメインログインウィンドウがブラウザに表示されます。



ステップ 13 ステップ 5 で設定した Cisco IMC ユーザのユーザ ID とパスワードを使用してログインします。

ログインに成功すると、以下と同じような **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウがブラウザに表示されます。



事前設定チェックの実行

アプライアンスをインストール（「[アプライアンスのインストールワークフロー](#)」の説明どおり）し、Cisco IMC の GUI へのアクセスを設定（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」の説明どおり）した後、Cisco IMC を使用して次の事前設定タスクを実行します。この操作は、正しい設定と展開の確実な実行に役立ちます。

1. アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol (NTP) サーバと同期します。同期する NTP サーバは、「[必要な IP アドレスおよびサブネット](#)」で説明されているように、実装の計画時に収集したホスト名または IP を持つ NTP サーバである必要があります。Cisco DNA Center データがネットワーク全体で正しく同期されるよう徹底するには、このタスクが不可欠です。
2. 10 Gbps アプライアンスポートに接続されているスイッチを再設定して、高スループット設定がサポートされるようにします。

ステップ 1 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」で設定した CISCO imc IP アドレス、ユーザ ID、パスワードを使用して、アプライアンスの Cisco IMC にログインします。

ログインに成功すると、次に示すような **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウがブラウザに表示されます。

The screenshot shows the Cisco IMC Chassis Summary page. It is divided into two main sections: Server Properties and Cisco Integrated Management Controller (Cisco IMC) Information. Below these are Chassis Status and Server Utilization.

Server Properties:

- Product Name: C220-FCH212
- Serial Number: FCH212
- PID: DN2-HW-APL
- UUID: AF0FFF4C-638C-4EC8-AB03-
- BIOS Version: C220M5.3.1.2b.0.1025170315
- Description: [Empty field]
- Asset Tag: Unknown

Cisco Integrated Management Controller (Cisco IMC) Information:

- Hostname: C220-FCH212
- IP Address: 172.20.1.223
- MAC Address: 70:69:00:00:00:48
- Firmware Version: 3.1(2c)
- Current Time (UTC): Thu May 16 10:51 2019
- Local Time: Thu May 16 10:51 2019 UTC +0000
- Timezone: UTC

Chassis Status:

- Power State: On
- Overall Server Status: Good
- Temperature: Good
- Overall DIMM Status: Good
- Power Supplies: Good
- Fans: Good
- Locator LED: Off
- Overall Storage Status: Good

Server Utilization:

- Overall Utilization (%): N/A
- CPU Utilization (%): N/A
- Memory Utilization (%): N/A
- IO Utilization (%): N/A

ステップ 2 次に示すように、アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol (NTP) サーバと同期します。

- Cisco IMC GUI の左上隅から、[Toggle Navigation] アイコン (☰) をクリックします。
- Cisco IMC メニューから [Admin] > [Networking] を選択し、[NTP Setting] タブを選択します。
- [NTP Enabled] チェックボックスがオンになっていることを確認してから、次に示す例のように、4つの番号付きサーバフィールドに最大4つの NTP サーバホスト名またはアドレスを入力します。

The screenshot shows the Cisco IMC NTP Setting page. The breadcrumb is Network > Network Security > NTP Setting. The NTP Properties section is active.

NTP Properties:

- NTP Enabled:
- Server 1: 1.ntp.example.com
- Server 2: 2.ntp.example.com
- Server 3: 3.ntp.example.com
- Server 4: [Empty field]
- Status: NTP service disabled

At the bottom right, there are buttons for "Save Changes" and "Reset Values".

- [Save Changes] をクリックします。Cisco IMC はエントリを検証した後、アプライアンスハードウェアの時刻と NTP サーバの時刻の同期を開始します。

- (注) 第1世代の Cisco DNA Center アプライアンスとは異なり、第2世代のアプライアンスでは仮想インターフェイスカード (VIC) が使用されません。Cisco IMC で高スループットをサポートするために、第2世代アプライアンスにインストールされているネットワークインターフェイスカード (NIC) を設定する必要はありません。すでにデフォルトで有効になっているためです。

ステップ3 アプライアンスの高スループット設定と一致するようにスイッチを再設定します。

- a) セキュアシェル (SSH) クライアントを使用して、設定するスイッチにログインし、スイッチプロンプトで EXEC モードを開始します。
- b) スイッチポートを設定します。

Cisco Catalyst スイッチで、次のコマンドを入力します。次に例を示します。

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport mode access
MySwitch(config-if)#switchport access vlan 99
MySwitch(config-if)#speed auto
MySwitch(config-if)#duplex full
MySwitch(config-if)#mtu 1500
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

Cisco Nexus スイッチで、次のコマンドを入力して、Link Layer Discovery Protocol (LLDP) およびプライオリティフロー制御 (PFC) を無効にします。次に例を示します。

```
N7K2# configure terminal
N7K2(config)# interface eth 3/4
N7K2(config-if)# no priority-flow-control mode auto
N7K2(config-if)# no lldp transmit
N7K2(config-if)# no lldp receive
```

次の点に注意してください。

- これらのコマンドは単なる例です。
 - 正常に機能させるには、第2世代 Cisco DNA Center アプライアンスのスイッチポートをアクセスモードに設定する必要があります。トランクモードは、第1世代のアプライアンスのモードであるため、サポートされていません。
- c) `show interface tengigabitethernet` という *portID* コマンドを実行して、ポートが接続されて動作していること、正しい MTU、デュプレックス、リンクタイプが設定されていることをコマンド出力で確認します。次に例を示します。

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia XXX.310.8000)
MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

- d) `show run interface tengigabitethernet` という *portID* コマンドを実行して、X710-DA2 NIC ポートからのケーブルが接続されているスイッチポートを設定します。次に例を示します。

```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
! interface TenGigabitEthernet1/1/3
  switchport access vlan 99
  ip device tracking maximum 10
end
```

MySwitch#

- e) `show mac address-table interface tengigabitethernet` という portID コマンドを実行して、コマンド出力で MAC アドレスを確認します。次に例を示します。

```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
99      xxXe.3161.1000  DYNAMIC Te1/1/3
Total Mac Addresses for this criterion: 1
```

MySwitch#

次のタスク

このタスクが完了したら、次のいずれかを実行します。

- アプライアンスを設定する前に Cisco DNA Center ソフトウェアを再インストールする必要がある場合は、「[アプライアンスのイメージの再作成](#)」を参照してください。
- アプライアンスを設定する準備ができている場合は、使用する設定ウィザードに固有の「アプライアンス設定の概要」のトピックに進みます。
 - [Maglev 設定ウィザード](#)
 - [ブラウザベースの設定ウィザード \(44 および 56 コアアプライアンス\)](#)

ネットワーク インターフェイス カードの無効化

アプライアンスが Intel X710-DA4 ネットワーク インターフェイス カード (NIC) を有効にした状態で出荷されている場合は、次の手順を実行して無効にする必要があります。カードを無効にしない場合、アプライアンスには4つの追加インターフェイスが含まれているため、設定に悪影響を及ぼす可能性があります。

ステップ 1 Cisco DNA Center アプライアンスがあること、INTEL X710-DA4 NIC がインストールされていることを確認します。

- アプライアンスの Cisco IMC にログインします。
- [概要 (Summary)]** ウィンドウの **[サーバプロパティ (Server Properties)]** エリアに次の値が設定されていることを確認します。

- PID : 44 コアアプライアンスの場合は **DN2-HW-APL**、56 コアアプライアンスの場合は **DN2-HW-APL-L**、112 コアアプライアンスの場合は **DN2-X-HW-APL-XL**です（次の例を参照）。
- BIOS バージョン : この値は 44 および 56 コアアプライアンスの **C220M5**、または 112 コアアプライアンスの **C480M5** のいずれかで開始する必要があります（次の例を参照）。

Server Properties

Product Name:
 Serial Number: FCH224
PID: DN2-HW-APL-XL
 UUID: 6FF202AA-EEF9-4DF4-9FE4-
 BIOS Version: **C480M5** 4.0.1c.0.0706181854
 Description:
 Asset Tag: Unknown

Cisco Integrated Management Controller

Hostname: C480-FCH224
 IP Address: 10.195.
 MAC Address: A8:B4:56:
 Firmware Version: 4.0(1a)
 Current Time (UTC): Wed Nov 6 18:51:54 2019
 Local Time: Wed Nov 6 10:51:54 2019 PST -08
 Timezone: America/Los_Angeles

- >[シャーシ (Chassis)]>[インベントリ (Inventory)]>[ネットワークアダプタ (Network Adaptor)] を選択します。
- [ネットワークアダプタ (Network Adapters)]表で、次のスロットのいずれかに INTEL X710-DA4 Quad Port ネットワークアダプタが表示されていることを確認します。
 - 44 または 56 コアアプライアンスの場合はスロット 2。
 - 112 コアアプライアンスの場合はスロット 12（次の例を参照）。

Cisco Integrated Management Controller

/ ... / Inventory / Network Adapters ★

CPU Memory PCI Adapters Power Supplies Cisco VIC Adapters **Network Adapters** Storage SAS Expan

Network Adapters Total 3 ⚙️

Slot	Product Name	Number Of Interfaces	External Ethernet Interfaces	
			ID	MAC Address
9	Intel X710-DA2 Dual Port 10Gb SFP+ conver...	2	1	3c:fd:fe:...
			2	3c:fd:fe:...
			4	3c:fd:fe:...
			3	3c:fd:fe:...
12	Intel X710-DA4 Quad Port 10Gb SFP+ conver...	4	1	3c:fd:fe:...
			2	3c:fd:fe:...
			1	2c:f8:9b:...
			2	2c:f8:9b:...
L	Cisco(R) LOM X550-T2	2	1	2c:f8:9b:...
			2	2c:f8:9b:...

ステップ 2 次の要領でアプライアンスの PCIe カードが無効になっていることを確認します。

- >[コンピューティング (Compute)] を選択します。
 [BIOS > BIOS の設定 (Configure BIOS) > I/O] タブが開きます。

b) 次のパラメータを[Disabled (無効)]に設定してから、[保存 (Save)]をクリックします。

- 44 または 56 コアアプライアンスの場合、**PCIe スロット 2 OptionROM** と **PCIe スロット 2 リンク速度**。
- 112 コアアプライアンスの場合は **PCIe スロット 12 OptionROM** および **PCIe スロット 12 リンク速度** (次の例を参照)。

Note: Default values are shown in bold.

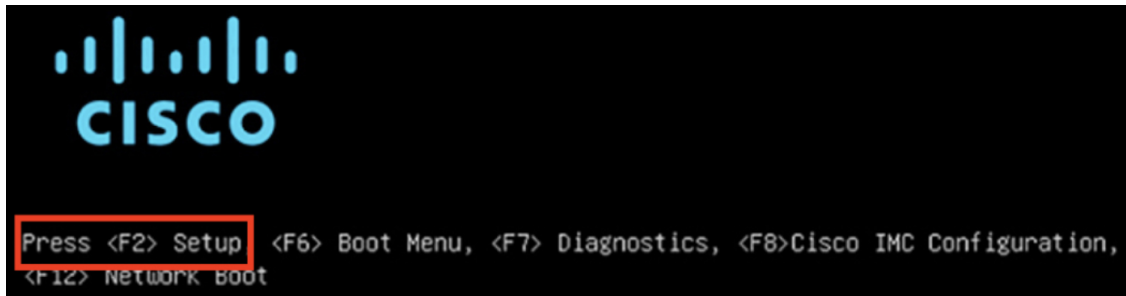
Reboot Host Immediately:	<input type="checkbox"/>
Intel VT for directed IO:	Enabled
Intel VTD ATS support:	Enabled
LOM Port 1 OptionRom:	Enabled
Pcie Slot 1 OptionRom:	Enabled
Pcie Slot 3 OptionRom:	Enabled
Pcie Slot 5 OptionRom:	Enabled
Pcie Slot 7 OptionRom:	Enabled
Pcie Slot 9 OptionRom:	Enabled
Pcie Slot 11 OptionRom:	Enabled
RAID OptionRom:	Enabled
Front NVME 2 OptionRom:	Enabled
Front NVME 12 OptionRom:	Enabled
Front NVME 14 OptionRom:	Enabled
Front NVME 16 OptionRom:	Enabled
Front NVME 18 OptionRom:	Enabled
Front NVME 20 OptionRom:	Enabled
Legacy USB Support:	Enabled
Intel VTD coherency support:	Disabled
All Onboard LOM Ports:	Enabled
LOM Port 2 OptionRom:	Enabled
Pcie Slot 2 OptionRom:	Enabled
Pcie Slot 4 OptionRom:	Enabled
Pcie Slot 6 OptionRom:	Enabled
Pcie Slot 8 OptionRom:	Enabled
Pcie Slot 10 OptionRom:	Enabled
Pcie Slot 12 OptionRom:	Disabled
Front NVME 1 OptionRom:	Enabled
Front NVME 11 OptionRom:	Enabled
Front NVME 13 OptionRom:	Enabled
Front NVME 15 OptionRom:	Enabled
Front NVME 17 OptionRom:	Enabled
Pcie Slot 12 Link Speed:	Disabled

c) 次のいずれかを実行します。

- アプライアンスでこれらの2つのパラメータを**無効**に設定できる場合は、アプライアンスをリブートして、設定を続行します。この手順の残りを実行する必要はありません。
- お使いの 112 コアアプライアンスで [I/O] タブにこれらのパラメータのいずれか1つのみ表示される場合は、ステップ 3 に進み、残りの手順を実行します。

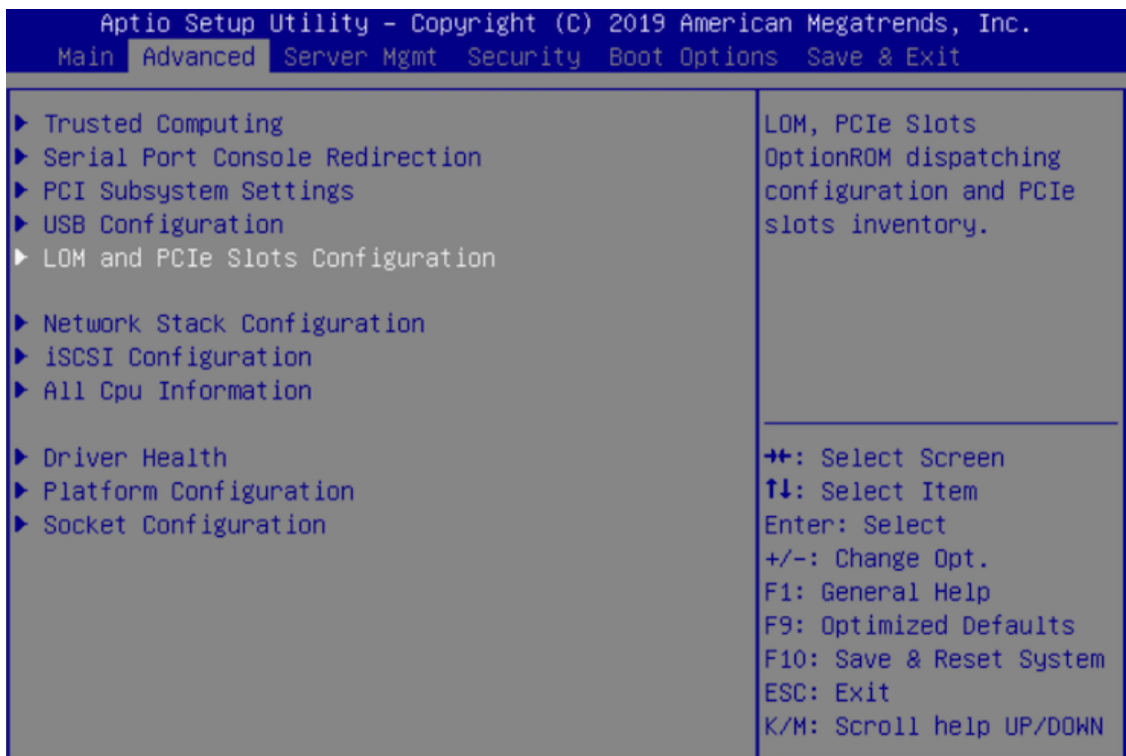
ステップ 3 アプライアンスの BIOS を起動します。

- Cisco IMC から KVM セッションを開始します。
- [**ホスト電源 (Host Power)**] リンクをクリックしてから [**電源の再投入 (Power Cycle)**] を選択し、アプライアンスの電源を再投入します。
- 起動時に、次の画面が表示されたらすぐに**F2**キーを押してアプライアンスの BIOS を起動し、Aptio セットアップユーティリティを開きます。

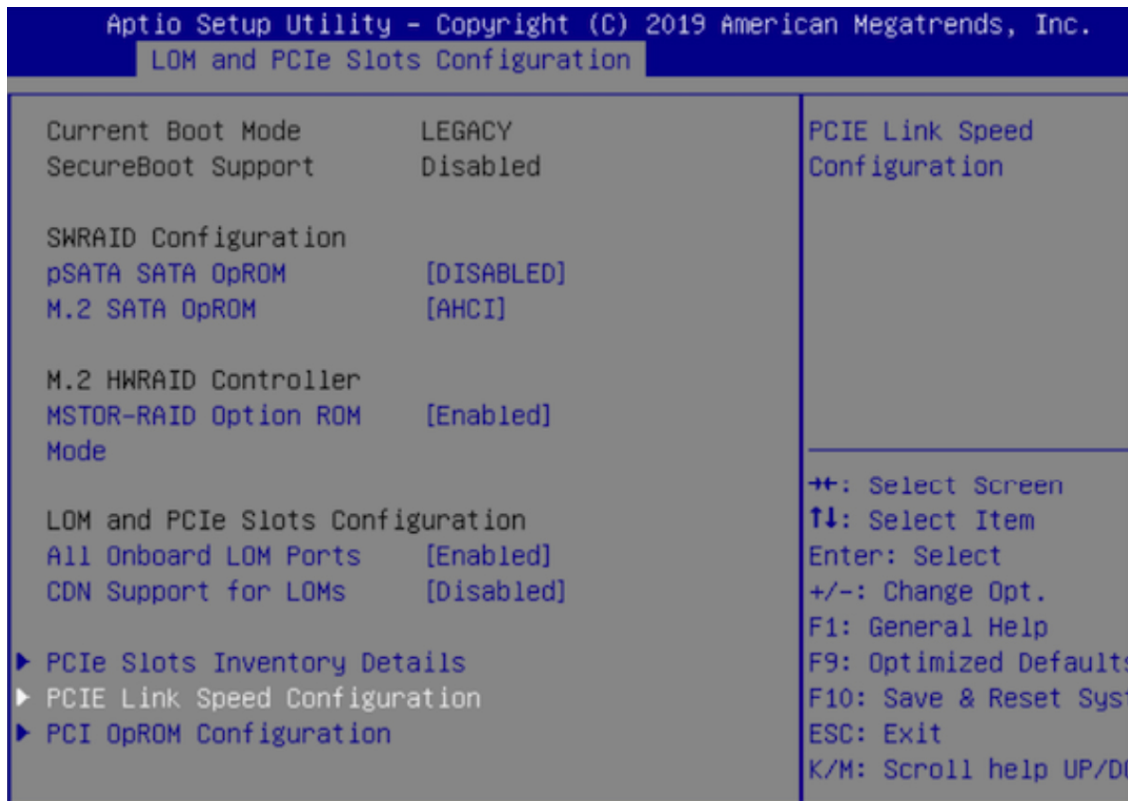


ステップ 4 次の要領で PCIe カードを無効にします。

- a) Aptio セットアップユーティリティの [メイン (Main)] タブで [詳細 (Advanced)] タブを選択し、[LOM と PCIe スロットの設定 (LOM and PCIe Slots Configuration)] を選択します。

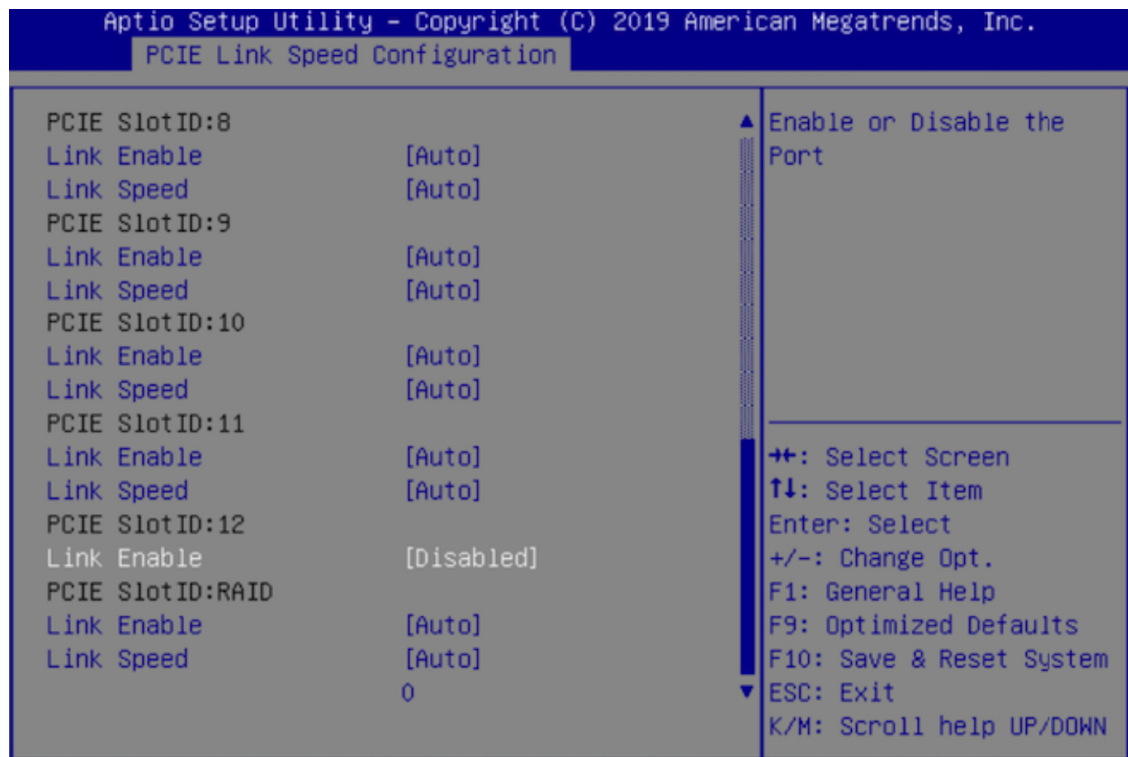


- b) [LOM および PCIe スロットの設定 (LOM and PCIe Slots Configuration)] タブで [PCIe リンク速度の設定 (PCIe Link Speed Configuration)] を選択します。

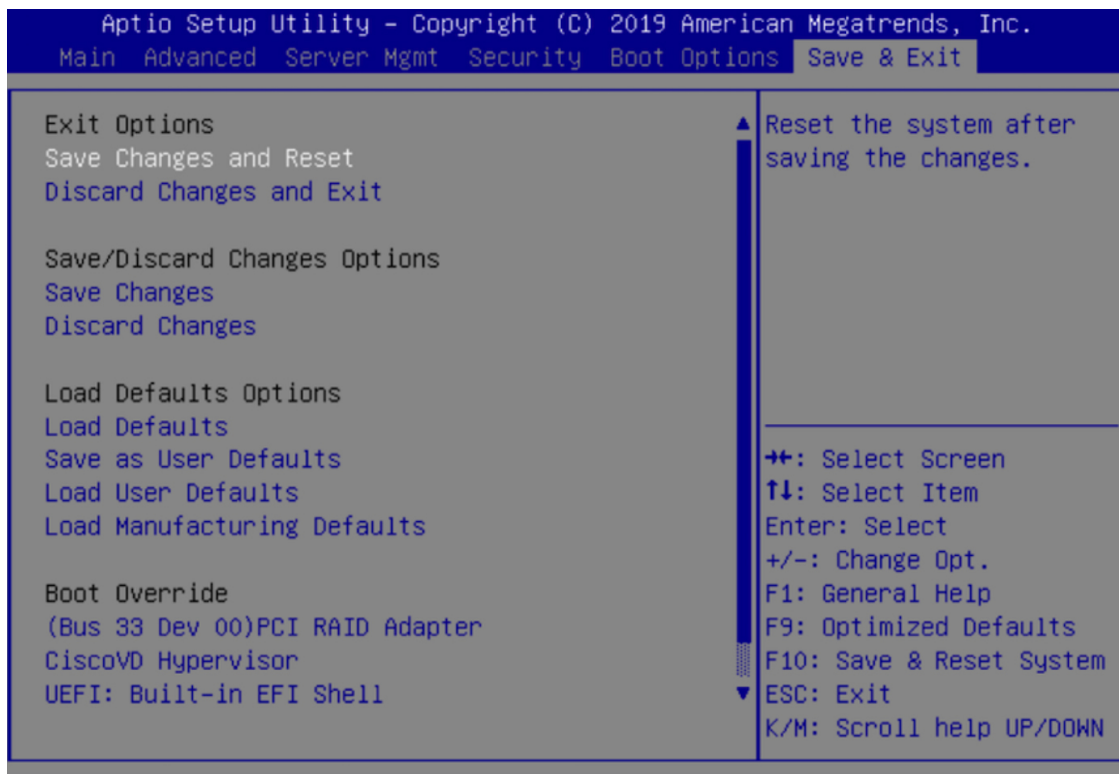


- c) [PCIe リンク速度の設定 (PCIe Link Speed Configuration)] タブを下向きにスクロールして PCIe SlotID : 12 の [リンク有効化 (Link Enable)] オプションを見つけ、**Enter** を押します。
- d) [無効化 (Disable)] を選択し、**Enter** を押します。


次の例のような画面が表示されます。



- e) **ESC**キーを2回押してメインの BIOS メニューに戻り、[保存して終了 (Save & Exit)] タブを開きます。
- f) [変更を保存してリセット (Save Changes And Reset)] オプションを選択し、**Enter** を押します。



アプライアンスがリブートし、設定ウィザードが開きます。アプライアンスの設定を続けます。

重要 アプライアンスのNICを無効にした後、アプライアンスをCisco IMCのデフォルト設定にリセットした場合（ > 管理者 > ユーティリティが > 工場出荷時のデフォルトにリセットされた場合）、この手順をもう一度実行する必要があります。

アプライアンスのイメージの再作成

バックアップからの回復やクラスターリンク設定の変更など、Cisco DNA Center アプライアンスイメージの再作成が必要な状況が発生する場合があります。これを行うには、次の手順を実行します。

ステップ 1 Cisco DNA Center ISO イメージをダウンロードし、それが正規のCiscoイメージであることを確認します。

「[Cisco DNA Center ISO イメージの確認](#)」を参照してください。

ステップ 2 Cisco DNA Center ISO イメージを含むブート可能USBドライブを作成します。

「[ブート可能なUSBドライブの作成](#)」を参照してください。

ステップ 3 アプライアンスのRAIDコントローラによって管理されている仮想ドライブを再初期化します。

「[Cisco DNA Center アプライアンスの仮想ドライブの再初期化 \(20 ページ\)](#)」を参照してください。

ステップ 4 アプライアンスに Cisco DNA Center を再インストールします。

「[Cisco DNA Center ISO イメージのインストール](#)」を参照してください。

Cisco DNA Center ISO イメージの確認

Cisco DNA Center を展開する前に、ダウンロードした ISO イメージが正規の Cisco イメージであることを確認するよう強くお勧めします。

始める前に

Cisco DNA Center ISO イメージの場所を把握します（電子メールを使用するか、シスコサポートチームと連絡を取る方法で）。

- ステップ 1** シスコによって指定された場所から Cisco DNA Center ISO イメージ (.iso) をダウンロードします。
- ステップ 2** シスコの指定した場所から署名検証用のシスコ公開キー (cisco_image_verification_key.pub) をダウンロードします。
- ステップ 3** シスコが指定した場所から ISO イメージのセキュア ハッシュ アルゴリズム (SHA512) チェックサム ファイルをダウンロードします。
- ステップ 4** シスコサポートから電子メールで、またはセキュアなシスコの Web サイト（利用可能な場合）からダウンロードして、ISO イメージのシグニチャファイル (.sig) を入手します。
- ステップ 5** （任意）SHA 検証を実行して、不完全なダウンロードによって ISO イメージが破損していないかどうかを判定します。

（オペレーティングシステムに応じて）次のコマンドのいずれかを実行します。

- Linux システムの場合：**sha512sum ISO-image-filename**
- Mac システムの場合：**shasum -a 512 ISO-image-filename**

Microsoft Windows には組み込みのチェックサムユーティリティはありませんが、certutil ツールを使用できます。

```
certutil -hashfile <filename> sha256 | md5
```

次に例を示します。

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

Windows では、[Windows PowerShell](#) を使用してダイジェストを生成することもできます。次に例を示します。

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

実行したコマンドの出力とダウンロードした SHA512 チェックサムファイルを比較します。コマンド出力が一致しない場合は、ISO イメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 6 署名を確認し、ISO イメージが正規の製品でありシスコ製であることを確認します。

openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature signature-filename ISO-image-filename

(注) このコマンドは MAC と Linux の両方の環境で動作します。まだ OpenSSL をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります ([こちらから入手可能](#))。

ISO イメージが純正であれば、このコマンドを実行すると、「問題がないことを確認 (Verified OK)」というメッセージが表示されます。このメッセージが表示されない場合は、ISO イメージをインストールせず、シスコサポートにお問い合わせください。

ステップ 7 Cisco ISO イメージをダウンロードしたことを確認してから、Cisco DNA Center ISO イメージを含むブート可能 USB ドライブを作成します。「[ブート可能な USB ドライブの作成](#)」を参照してください。

ブート可能な USB ドライブの作成

Cisco DNA Center ISO イメージをインストールできるブート可能 USB ドライブを作成するには、次のいずれかの手順を実行します。

始める前に

- Cisco DNA Center ISO イメージのコピーをダウンロードして確認します。「[Cisco DNA Center ISO イメージの確認](#)」を参照してください。
- 使用している USB フラッシュドライブの容量が少なくとも 32 GB であることを確認します。

Etcher の使用

ステップ 1 ラップトップまたはデスクトップでのブート可能 USB ドライブの作成を可能にする、オープンソースのフリーウェアユーティリティ Etcher (バージョン 1.3.1 以降) をダウンロードしてインストールします。

現在、Linux、macOS、Windows バージョンの Etcher を使用できます。<https://www.balena.io/etcher/> からダウンロードできます。

(注) Windows 10 を実行しているマシンでは Etcher の Windows バージョンのみを使用してください。古いバージョンの Windows との互換性に関する既知の問題があるためです。

ステップ 2 Etcher をインストールしたマシンに USB ドライブを接続し、Etcher を起動します。

ステップ 3 ウィンドウの右上隅にある  をクリックし、Etcher が次のように設定されていることを確認します。

- 成功時に自動マウント解除する

- 成功時に書き込みを検証する

ステップ 4 [Back] をクリックして、メインウィンドウに戻ります。

ステップ 5 [Select Image] をクリックします。

ステップ 6 以前にダウンロードした Cisco DNA Center ISO イメージに移動し、そのイメージを選択して [Open] をクリックします。

接続した USB ドライブの名前がドライブアイコン () の下に表示されます。表示されない場合には、次の操作を実行します。

1. [Select drive] をクリックします。
2. 正しい USB ドライブのオプションボタンをクリックしてから、[Continue] をクリックします。

ステップ 7 [Flash!] をクリックして、ISO イメージを USB ドライブにコピーします。

Etcher では、インストールされた Cisco DNA Center ISO イメージを使用して、ブート可能ドライブとして USB ドライブが設定されます。

Linux CLI の使用

ステップ 1 次のとおり、ご使用のマシンで USB フラッシュドライブが認識されていることを確認します。

- a) フラッシュドライブをマシンの USB ポートに挿入します。
- b) Linux シェルを開き、次のコマンドを実行します。 **lsblk**

次の例に示すように、このコマンドでは、マシンに現在設定されているディスクパーティションが一覧表示されます。

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 446.1G 0 disk
├─sda1 8:1 0 1M 0 part
├─sda2 8:2 0 28.6G 0 part /
├─sda3 8:3 0 28.6G 0 part /install2
├─sda4 8:4 0 9.5G 0 part /var
├─sda5 8:5 0 30.5G 0 part [SWAP]
└─sda6 8:6 0 348.8G 0 part /data
sdb 8:16 0 1.8T 0 disk
├─sdb1 8:17 0 426.1G 0 part /data/maglev/srv/fusion
└─sdb2 8:18 0 1.3T 0 part /data/maglev/srv/maglev-system
sdc 8:32 0 3.5T 0 disk
└─sdc1 8:33 0 3.5T 0 part /data/maglev/srv/ndp
sdd 8:48 1 28.7G 0 disk
└─sdd1 8:49 1 12G 0 part
```

- c) SDDパーティション (USB フラッシュドライブの存在を示す) が表示されていることを確認します。

ステップ 2 以前にダウンロードした Cisco DNA Center ISO イメージを USB フラッシュドライブに書き込みます。 **time sudo dd if=/data/tmp/ISO-image-filename of=/dev/flash-drive-partition bs=4M && sync**

たとえば `cdnac-sw-1.330` という名前の ISO イメージを使用してブート可能な USB ドライブを作成するには、次のコマンドを実行します。 **`time sudo dd if=/data/tmp/CDNAC-SW-1.330.iso of=/dev/sdd bs=4M && sync`**

Mac CLI の使用

ステップ 1 USB フラッシュドライブに関連付けられているディスクパーティションを確認します。

a) ターミナルウィンドウを開き、次のコマンドを実行します。 **`diskutil list`**

このコマンドでは、マシンに現在設定されているディスクパーティションが一覧表示されます。

b) フラッシュドライブをマシンの USB ポートに挿入し、 **`diskutil list`** コマンドをもう一度実行します。

このコマンドを最初に行ったときリストの表示されなかったパーティションは、フラッシュドライブです。たとえば `/dev/disk2` がフラッシュドライブのパーティションだと仮定します。

ステップ 2 このコマンドでフラッシュドライブのパーティションをマウント解除します。 **`diskutil unmountDisk flash-drive-partition`**

この例ではこの先、次のように入力します **`diskutil unmountDisk /dev/disk2`**

ステップ 3 以前ユーザがダウンロードした Cisco DNA Center ISO イメージを使用してディスクイメージを作成します。 **`hdiutil convert -format UDRW -o Cisco-DNA-Center-version ISO-image-filename`**

この例を続け、 `cdnac-sw-1.330.iso` という Cisco DNA Center ISO イメージを使用して作業しているとしましょう。次のコマンドを実行すると、 `cdnac-1.330.dmg` という名前の macOS ディスクイメージが作成されます。 **`hdiutil convert -format UDRW -o CDNAC-1.330 CDNAC-SW-1.330.iso`**

重要 ISO イメージがボックスパーティションに存在しないことを確認します。

ステップ 4 ブート可能な USB ドライブを作成します。 **`sudo dd if=macOS-disk-image-filename of=flash-drive-partition bs=1m`**

この例を続け、次のコマンドを実行します。 **`sudo dd if=CDNAC-1.330.dmg of=/dev/disk2 bs=1m`**

ISO イメージのサイズは約 18 GB であるため、完了までに時間がかかることがあります。

Cisco DNA Center アプライアンスの仮想ドライブの再初期化

Cisco DNA Center アプライアンスの仮想ドライブを再初期化するには、次の手順を実行します。

ステップ 1 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」で設定した CISCO imc IP アドレス、ユーザ ID、パスワードを使用して、アプライアンスの Cisco IMC にログインします。

ステップ 2 Cisco IMC GUI の左上隅から、**[Toggle Navigation]** アイコン () をクリックします。

- ステップ3 Cisco IMC メニューから、**[Storage]** > **[Cisco 12G Modular Raid Controller]** を選択します。
- ステップ4 **[Virtual Drive Info]** タブをクリックします。
- ステップ5 リストされている最初の仮想ドライブ（ドライブ番号 0）のチェックボックスをオンにして、**[Initialize]** をクリックします。
- ステップ6 **[Initialize Type]** ドロップダウンリストから **[Full initialize]** を選択します。
- ステップ7 **[Initialize VD]** をクリックします。
- ステップ8 アプライアンスの残りの仮想ドライブにそれぞれステップ 5～7 を繰り返します。

Cisco DNA Center ISO イメージのインストール

アプライアンスに Cisco DNA Center ISO イメージをインストールするには、次の手順を実行します。

始める前に

Cisco DNA Center ISO イメージのインストール元となるブート可能 USB ドライブを作成します。「[ブート可能な USB ドライブの作成](#)」を参照してください。

-
- ステップ1 Cisco DNA Center ISO イメージを含むブート可能 USB ドライブをアプライアンスに接続します。
- ステップ2 Cisco IMC にログインし、KVM セッションを開始します。
- ステップ3 アプライアンスの電源を投入または再投入します。
- アプライアンスが実行されていない場合には、**[Power]** > **[Power On System]** を選択します。
 - アプライアンスがすでに実行されている場合には、**[Power]** > **[Power Cycle System (cold boot)]** を選択します。
- ステップ4 表示されたポップアップウィンドウで **[Yes]** をクリックして、サーバ制御アクションを実行しようとしていることを確認します。
- ステップ5 シスコのロゴが表示されたら、**F6** キーを押すか、**[KVM]** メニューから **[Macros]** > **[User Defined Macros]** > **[F6]** を選択します。
- ブートデバイス選択メニューが表示されます。
- ステップ6 USB ドライブを選択してから、**Enter** を押します。
- ステップ7 **[GNU GRUB]** ブートローダウィンドウで、**[Cisco DNAアプライアンスの作成 (Manufacture Cisco DNA appliance)]** を選択してから、**Enter** を押します。
- (注) 30 秒以内に選択しなかった場合、ブートローダが自動的に Maglev インストーラを起動します。

Cisco DNA Centerアプライアンスの設定

Cisco DNA Center ISO イメージのインストールが完了すると、インストーラがリブートし、Maglev 設定ウィザードの初期画面が開きます。アプライアンスの再イメージ化を完了するには、[Maglev ウィザードを使用したアプライアンスの設定](#)の手順を実行します。