Cisco Telemetry Broker

仮想アプライアンス導入およびコンフィギュレーション ガイド 1.4.4

目次

はじめに

このガイドでは、Cisco Telemetry Broker（このドキュメントでは CTB と呼ぶ場合があります）のインストール方法について説明します。Cisco Telemetry Broker コンポーネントと、ネットワーク内での配置方法について説明します。

Cisco Telemetry Broker では、次の操作を実行できます。

- Cisco Telemetry Broker のインストール
- の更新 Cisco Telemetry Broker
- 宛先とルールの設定
- Secure Network Analytics UDP Director からの移行
- 接続先の到達不能性を確認する
- IPv4 または IPv6 の宛先の使用
- 10G スループットのパススルー NIC
- 高可用性の使用

対象読者

このガイドは、ネットワーク テレメトリ フローの維持とネットワークテレメトリのモニタリングを担当する担当者を対象としています。

略語

このガイドでは、次の略語が使用されます。

省略形	説明
DNS	ドメイン ネーム サーバ/サービス
FTP	ファイル転送プロトコル
Gbps	ギガビット/秒
HTTPS	Hypertext Transfer Protocol（Secure）
Mbps	メガビット/秒
NAT	ネットワーク アドレス変換
NTP	ネットワーク タイム プロトコル
SSH	セキュア シェル
UDPD	UDP Director

省略形	説明
URL	ユニバーサル リソース ロケータ
VLAN	仮想ローカル エリア ネットワーク

概念とアーキテクチャ

Cisco Telemetry Broker では、多くの入力からネットワークテレメトリを取得し、テレメトリ形式を変換して、それらのテレメトリを 1 つまたは複数の宛先に転送できます。例については、次の表を参照してください。

次のいずれかのテレメトリを取り込むことができます。	そのテレメトリを次の宛先のいずれかまたはすべてに転送します。
• NetFlow、syslog、IPFIX などのオンプレミス ネットワーク テレメトリ • Amazon Web Services（AWS）仮想プライベートクラウド（VPC）フローログなどのクラウドベースのテレメトリ入力	• Cisco Secure Network Analytics、Cisco Secure Cloud Analytics などの分析プラットフォーム • Cisco DNA Center などのネットワーク管理および自動化プラットフォーム • セキュリティ情報とイベント管理（SIEM）プラットフォーム

これを実現するには、1 つ以上の Cisco Telemetry Broker ノードを展開し、UDP 経由でテレメトリを取り込み、設定された宛先に転送します。

Cisco Telemetry Broker は箱から出してすぐ使用でき、次の変換をサポートします。

取り込んだデータ形式	転送されたデータ形式
VPC フローログ	IPFIX
Microsoft ネットワーク セキュリティ グループ（NSG）フローログ	IPFIX
IPFIX、NetFlow v5、NetFlow v9	JSON（SCA 宛先のみ）

ブローカーノードはすべて 1 つの Cisco Telemetry Broker マネージャによって管理されます。このマネージャの Web インターフェイスにログインして、ブローカーノードの管理、転送ルールの設定、ユーザーの作成、使用状況に関するダッシュボードの確認など、さまざまな設定タスクを実行できます。

これらのブローカーノードマネージャを仮想アプライアンスとしてハイパーバイザに展開します。

展開(導入)要件

次に、特定の入力から宛先にテレメトリを転送するためにネットワークに Cisco Telemetry Broker を展開するための前提条件と推奨事項を示します。

ブラウザ要件

Cisco Telemetry Broker は、次のブラウザをサポートします(最新のラピッドリリースおよび 1024 x 768 px の解像度でテスト済み)。

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

ネットワークの要件

展開する前に、次の手順を実行する必要があります。

- 2 つの OVA ファイルをダウンロードし、少なくとも 2 つの仮想マシンを作成します。
- マネージャノード用に 1 つの IP アドレスと、展開する各ブローカーノード用に 2 つの IP アドレスを予約します。

ネットワーク

管理ネットワーク:SSH および HTTPS を介した管理を提供するには、展開内のすべてのノード(マネージャまたはブローカー)に、管理ネットワークに接続された 1 つの IPv4 ネットワーク インターフェイスが必要です(ノードが管理機能を実行している場合)。

テレメトリネットワーク:ブローカノードには、テレメトリネットワークに接続した 2 番目のインターフェイス(IPv4 または IPv6)が必要です。このネットワークでは、ノードは入力からテレメトリを受信し、宛先に転送します。

管理ネットワークとテレメトリネットワークは同じネットワークにすることができます。

管理ネットワーク接続の設定

Cisco Telemetry Broker をインストールする前に、管理ネットワークの次の設定を決定します。

- IPv4 アドレスまたは IPv6 アドレス
- IPv4 サブネットマスクまたは IPv6 サブネットマスク
- IPv4 デフォルトゲートウェイアドレスまたは IPv6 デフォルトゲートウェイアドレス
- IPv4 DNS ネームサーバーまたは IPv6 DNS ネームサーバー

IPv4 アドレスと IPv6 アドレスの両方で同時にアクティブになるようにインターフェイスを設定できます。

テレメトリネットワーク接続の設定

Cisco Telemetry Broker をインストールする前に、テレメトリネットワークの次の設定を決定します。

- IPv4 アドレスまたは IPv6 アドレス
- IPv4 サブネットまたは IPv6 サブネット

- IPv4 デフォルトゲートウェイアドレスまたは IPv6 デフォルトゲートウェイアドレス

IPv4 アドレスと IPv6 アドレスの両方で同時にアクティブになるようにインターフェイスを設定できます。

仮想マシンの要件

KVM の展開の場合、テレメトリブローカはブローカノードで 2 つの CPU のみを使用します。ブローカノードがテレメトリ変換を実行している場合にのみ、追加の CPU を割り当てるとパフォーマンスが向上します。

ハードウェア構成

達成したいパフォーマンスタイプに応じて、次の 3 つの異なるパフォーマンスプロファイルのいずれかを使用してブローカノードを展開できます。

- [1 Gbit/s] このプロファイルを使用して、1 ギガビット/秒 NIC のラインレート パケット ブローカリングを実現します。
- [10 Gbit/s] このプロファイルを使用して、10 ギガビット/秒 NIC のラインレート パケット ブローカリングを実現します。
- [トランスフォーメーション対応(Transformation Capable)] このプロファイルを使用して、テレメトリ変換を実現します(たとえば、IPFIX を Secure Cloud Analytics に送信します)。

設定	マネージャ	ブローカ
CPU	4	1 Gbit/s : 2 10 Gbit/s : 5 トランスフォーメーション対応(Transformation Capable) : 8
メモリ	8GB	1 GBit/s : 12 GB 10 GBit/s : 12 GB トランスフォーメーション対応(Transformation Capable) : 12 GB
ストレージ	80GB	70 GB

ブローカは、次の表に示す情報に従って CPU を使用します。この表を参照として使用して、さまざまな CPU 割り当てが目的のパフォーマンスタイプを達成するのにどのように役立つかを理解してください。

CPU	1 Gbit/s	10 Gbit/s	トランスフォーメーション対応 (Transformation Capable)
1	デグレード	デグレード	デグレード
2	サポート対象	デグレード	デグレード
3	サポート対象	デグレード	デグレード
4	サポート対象	デグレード	デグレード
5	サポート対象	サポート対象	デグレード
6	サポート対象	サポート対象	デグレード
7	サポート対象	サポート対象	デグレード
8	サポート対象	サポート対象	サポート対象

VMware ESXi

リソース	マネージャ	ブローカ
ネットワーク インターフェイス #1 管理ネットワークへ接続	e1000e	e1000e
ネットワーク インターフェイス #2 テレメトリ ネットワークへ接続	インストールされていません	vmxnext

他のすべての値には OVA のデフォルトを使用することを推奨します。ctb v1.4 以降(IOMMU 機能をサポート)を展開するには、ESXi が v6.7 以降である必要があります。

KVM QEMU

リソース	マネージャ	ブローカ
ディスク	virtio-scsi	virtio-scsi
ネットワーク インターフェイス #1 管理ネットワークへ接続	virtio	virtio
ネットワーク インターフェイス #2 テレメトリ ネットワークへ接続	インストールされていません	virtio

時刻の同期

Cisco Telemetry Broker VM はシステム時刻をハイパーバイザと同期します。TLS などの機能が正しく動作するようにするには、ハイパーバイザの時刻が正確である必要があります。

VMware ESXi

ESXi ハイパーバイザで NTP を実行する方法については、この VMware ナレッジベースの記事 [英語] を参照してください。

KVM QEMU

ハイパーバイザとゲストが同期されていることを確認するには、次の図に示すように、ゲストマシンの XML 設定に *track='guest'* 属性が定義されていることを確認します。詳細については、`libvirt` のマニュアルを参照してください。

```
<clock offset='utc'>
    <timer name='rtc' tickpolicy='catchup' track='guest'/>
    <timer name='pit' tickpolicy='delay'/>
    <timer name='hpet' present='no'/>
</clock>
```

これにより、ゲストクロックがホストクロック値に同期されます。ただし、ハイパーバイザ ホスト クロックを正確に維持する必要があります。これを実現するには、NTP デーモンを使用します。

オープンな通信ポート

次の表に、Cisco Telemetry Broker アプライアンスとの間で行われるすべてのネットワーク接続の詳細を示します。ネットワークでこれらの接続が許可されるようにするには、現在設定されている該当するアクセス制御（ファイアウォールなど）を変更する必要があります。

クライアント	サーバ	ポート	説明
ユーザ	ブローカーノードとマネージャノード	22/TCP	コンソールへの SSH アクセス
マネージャ	外部インターネット	443/TCP	スマートライセンスやソフトウェアアップデートなどのセキュアな外部通信用の HTTPS
マネージャ	お客様の syslog サーバー	お客様定義のポート	Cisco Telemetry Broker 通知の syslog テレメトリ
マネージャ	お客様の SMTP サーバー	お客様定義のポート	Cisco Telemetry Broker 通知の SMTP テレメトリ

各ブローカノード	マネージャ	443/TCP	セキュアな管理接続のための HTTPS
各ブローカノード	外部インターネット	443/TCP	AWS S3/Azure SAS ストレージバケットから VPC/NSG フローログをそれぞれ取得するための HTTPS
ユーザ	マネージャ	443/TCP	Web インターフェイスアクセス用の HTTPS
ブローカーノードとマネージャノード	顧客の DNS サーバ	53/UDP	DNS テレメトリ
各ブローカノード	外部インターネット	443/TCP	SCA サーバーへのアクセスを保護し、ファイルを SCA S3 バケットにアップロードするためのブローカノードの HTTPS

さらに、ブローカノードに送信されるテレメトリタイプと、ブローカノードが宛先に送信するテレメトリタイプの両方に基づいてポートを開く必要があります。次の表に、さまざまなテレメトリタイプの共通ポートに関する詳細を示します。

ポート	説明
514/UDP	syslog
2055/UDP	NetFlow v5、NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

新しいシステムへの設定の移行

Cisco Telemetry Broker マネージャで設定した CTB 設定ルールをバックアップおよび復元するには、次のプロセスを実行します。

- UDPD のお客様は、既存の UDPD 設定を Cisco Telemetry Broker に移行できます。詳細については、『Cisco Telemetry Broker User Guide』の「Importing and Exporting UDP Director Configuration」の項を参照してください。

CTB 設定ルールのバックアップ

CTB マネージャノードで次のコマンドを実行します。

```
$ sudo ctb-backup-config -v -f ctb_config.json
```

このプロセスが終了すると、設定ルールは ~/.ctb_config.json のファイルにバックアップされます。その後、設定ルールを別の場所にコピーできます。

- VPC/NSG フローログルールはバックアップされないため、新しいシステムへの移行時に VPC/NSG フローログルールを再作成する必要があります。
- CTB 構成ルールは、同じバージョン内でのみバックアップおよび復元できます。複数のバージョンでこれを行おうとすると、プロセスが失敗する可能性があります。

CTB 設定ルールの復元

> ⚠ マネージャノードで `ctb-install --init` を実行した直後に `ctb-restore-config` を実行する必要があります。GUI ログインアカウントを手動で作成すると、`ctb-restore-config` からのアカウント情報で上書きされます。

次の手順を実行します。

1. *install* ユーザーとしてログインします。
2. 既存のシステムから **ctb-config.json** ファイルをコピーします。
3. *admin* として新しいシステムにログインします。
4. CTB マネージャノードで次のコマンドを実行します。

   ```
   $ sudo ctb-restore-config -v -f ctb_config.json
   ```

   復元のために Cisco Telemetry Broker に追加した入力は、どのノードまたはクラスタにも割り当てられません。必要に応じて、それらを割り当てる必要があります。

ネットワーク設定の決定

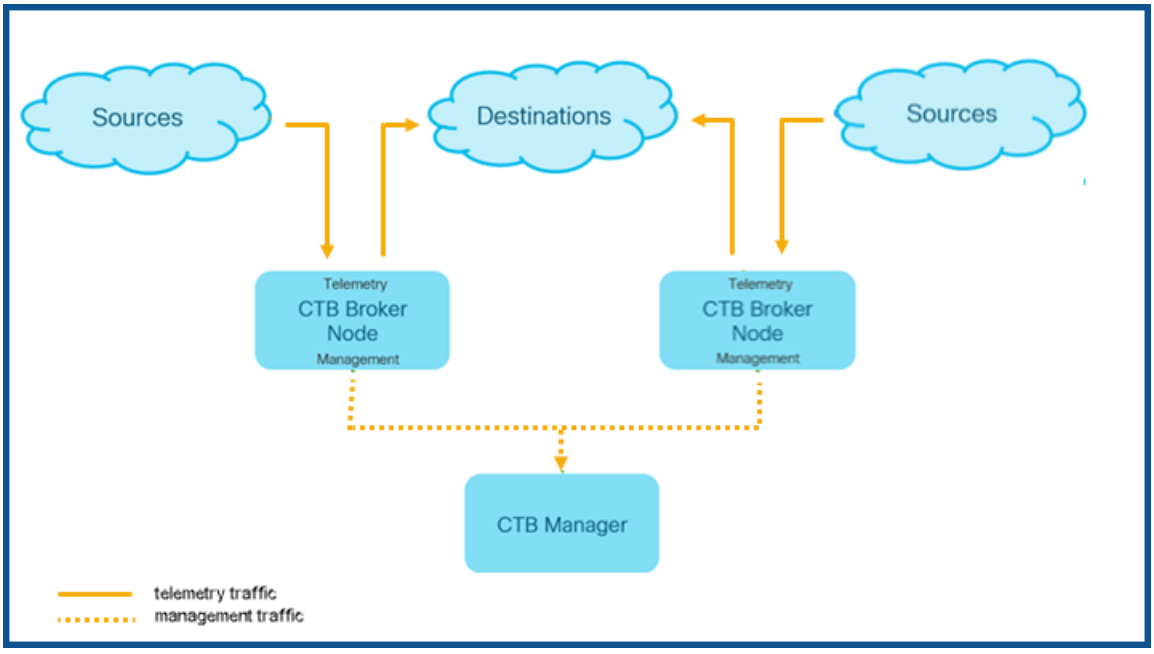
Cisco Telemetry Broker は、単一の Cisco Telemetry Broker マネージャが複数のブローカーノードを管理できるマルチノード設定をサポートします。Cisco Telemetry Broker ではすべてのブローカノードがすべての宛先とルールとともに更新されるため、以下に示すいくつかの一般的な問題を回避するように設定を慎重に計画する必要があります。

- 異なるテレメトリセグメントにブローカノードを展開できます。この場合、各ブローカノードのテレメトリインターフェイスにネットワーク経由でアクセスできない場合があります。特定のノードに到達するエクスポータからのパケットが、そのノードからアクセスできない宛先に転送されないように、ルールを慎重に作成する必要があります。これを実現するには、このルーティングの問題を引き起こす可能性のあるエクスポータを除外するルールを作成する必要があります。1 つの例は、すべての入力に一致するデフォルトルールを使用しないことです。
- すべての宛先が各ブローカノードに関連するとは限りません。ただし、接続先到達可能性チェック機能では、各ブローカーノードが各接続先のアクセシビリティを確認しようとするため、ブローカーノードは競合する情報をマネージャに報告する可能性があります。一部のブローカーノードが一部の接続先に接続できない可能性がある場合は、それらの接続先の接続先到達可能性チェックを無効にします。

UDP Director から Cisco Telemetry Broker に移行する場合は、Cisco Telemetry Broker と UDP Director の構成方法には違いがあるため、マネージャノードとブローカーノードの OVA ファイルを展開する前に、2 つの VM をネットワークに接続する方法を計画する必要があります。

Cisco Telemetry Broker は、テレメトリトラフィックと管理トラフィックを区別します。ブローカーノードには、テレメトリ ネットワーク インターフェイスと管理ネットワーク インターフェイスの 2 つのインターフェイスがあります。マネージャノードには、管理ネットワーク インターフェイスのみがあります。次の図は、マネージャノードとブローカーノードを論理的に展開する方法を示しています。

> このトピックの例は、一般的な導入シナリオを表していることに注意してください。より高度な導入（たとえば、VLAN を使用する導入）を設定する方法については、ネットワーク管理者にお問い合わせください。



Cisco Telemetry Broker は、管理ネットワーク インターフェイスでのみ管理トラフィックを受信します。ブローカーノードとマネージャノード間のすべての通信にこのインターフェイスを使用します。テレメトリトラフィックは、主にブローカーノードのテレメトリ ネットワーク インターフェイスで仲介されます。唯一の例外は、Cisco Telemetry Broker が AWS VPC フローログまたは Azure NSG フローログを取得する場合、もしくは Cisco Telemetry Broker がテレメトリを SCA に送信する場合です。これはどちらも、ブローカーノードの管理ネットワーク インターフェイスで発生します。

マネージャノードは、ネットワークの任意のサブネット上の任意の場所に配置できますが、ポート 443 経由でブローカーノードと TCP 接続する必要があります。

ブローカノードでは、次のいずれかの導入モードを使用できます。

1. テレメトリサブネットと管理サブネットが同じです。このモードでは、ブローカーノードのテレメトリ ネットワーク インターフェイスと管理ネットワーク インターフェイスは同じサブネットに属します。「同じサブネットに属するインターフェイス」を参照してください。
2. テレメトリサブネットと管理サブネットが異なるため、ブローカーノードはテレメトリ ネットワーク インターフェイスと管理ネットワーク インターフェイスを 2 つの異なるサブネットに保持します。「異なるサブネットに属するインターフェイス」を参照してください。

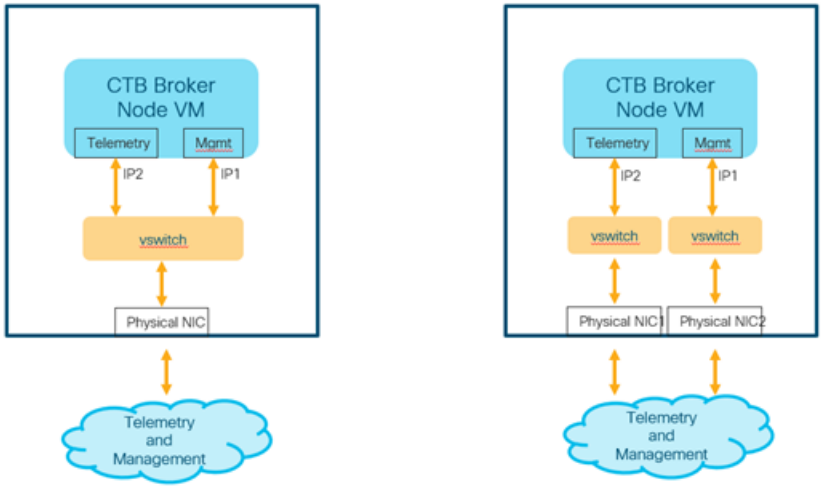
テレメトリトラフィックと管理トラフィックの両方に個別のパスを指定すると、次の利点があります。

- パスを分離すると、トラフィックがリソース（仮想スイッチや物理 NIC など）を共有する必要がないため、特にインターフェイス ライン レートのパフォーマンスに近づいた場合にパフォーマンスが向上します。
- テレメトリトラフィックから管理トラフィックを分離することは、ネットワーク構成に適しています。

同じサブネットに属するインターフェイス

この導入モードは、管理インターフェイスとテレメトリインターフェイスが同じである UDP Director の導入モードと非常によく似ています。この最初の導入モードの唯一の違いは、ブローカノードのインターフェイスに個別の IP アドレスが必要なことです。

このタイプの導入の設定方法については、次の図を参照してください。



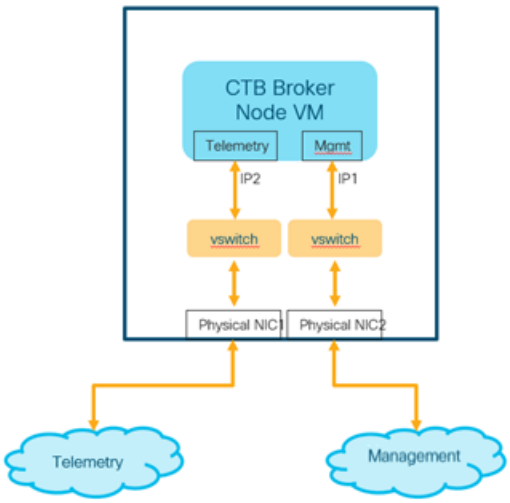
仮想環境では、次の 2 つの方法のいずれかで実行できます。

1. ブローカーノードのテレメトリ ネットワーク インターフェイスと管理ネットワーク インターフェイスをハイパーバイザ内の同じ仮想スイッチに接続します。
2. ブローカーノードのテレメトリ ネットワーク インターフェイスと管理ネットワーク インターフェイスを異なる仮想スイッチに接続しますが、基盤となる NIC は同じ物理スイッチに接続するため、同じサブネットに接続します。

異なるサブネットに属するインターフェイス

この導入モードでは、テレメトリ ネットワーク インターフェイスと管理ネットワーク インターフェイスは異なるサブネット上にあります。この場合、通常は 2 つのインターフェイスに個別の仮想スイッチが必要です。

このタイプの導入の設定方法については、次の図を参照してください。



Cisco Telemetry Broker の展開

次に、ブローカノードをネットワークに展開し、入力からテレメトリを取り込み、宛先にテレメトリをエクスポートするようにブローカノードを設定する手順の概要を示します。

- マネージャノードと 1 つ以上のブローカーノードをハイパーバイザに展開します
- Cisco Telemetry Broker スマートライセンスを設定します
- ブローカーノードを管理するためのマネージャノードを設定します
- ブローカノードがテレメトリを取り込み、エクスポートする方法を制御する 1 つ以上のルールを設定します
- ダッシュボードから展開のパフォーマンスの状態を確認します

なお、ブローカノードはテレメトリインターフェイス NIC を継続的にポーリングして着信テレメトリを検出するため、CPU 使用率が高くなります。ブローカーノードの CPU 使用率が高くなるのは正常な動作です。

技術的な制限

- 1 つの Cisco Telemetry Broker 環境では、入力ごとに最大 10 の宛先がサポートされ、マネージャノードごとに 10 のブローカノードがサポートされます。
- エクスポータの追跡を無効にすると、各ブローカノードは、最大 100,000 のエクスポータをサポートします。1 つ以上の入力についてエクスポータの追跡を有効にする場合は、パフォーマンスが低下する可能性があるため、1,000 を超えるエクスポータ（すべての入力の合計）を追跡しないことをお勧めします。

  （エクスポータの追跡の無効化および有効化については、Cisco Telemetry Brokerのユーザーガイドにある「UDP 入力」のトピックを参照してください）
- 宛先は、最大 1,000 のサブネットをサポートします（その宛先に関するすべてのルールでの合計）。1,000 を超えるサブネットを追加すると、データが失われる可能性があります。

VMware のセットアップ

VMware ESXi 6.7 で次の手順をテストしました。

> ブローカーノードをインストールする前に、マネージャノードをインストールして設定する必要があります。

VMware：マネージャノードのインストール

次の手順を順番に実行します。

1. マネージャノード OVA ファイルをダウンロードします。
2. マネージャノードを展開します。
3. リソース予約の設定
4. VM 時間設定を確認します。
5. インストールユーザとしてログインします。
6. sudo ctb-install --init コマンドを実行します。
7. 最初のスーパーユーザアカウントを設定します。
8. ログアウトします。

> ブローカーノードをインストールする前に、マネージャノードをインストールして設定する必要があります。

1. マネージャノード OVA ファイルのダウンロード

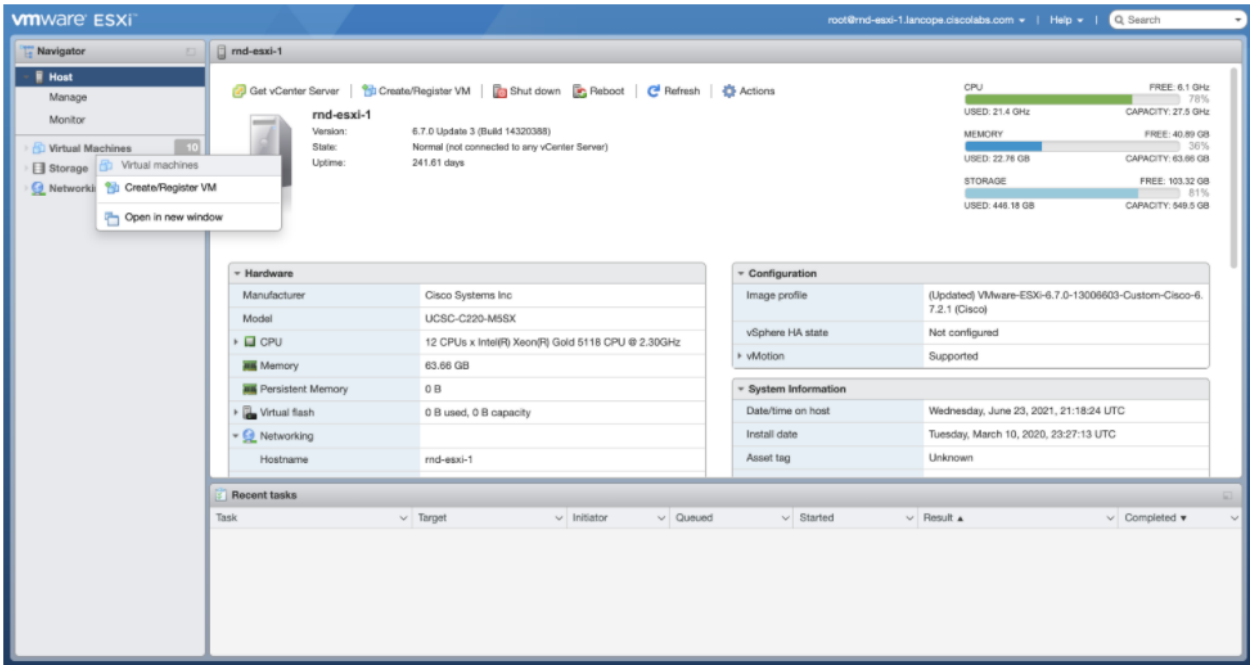
1. マネージャノード OVA ファイルをダウンロードします。
2. software.cisco.com で、OVA ファイルの SHA512sum 値を確認します。
3. OVA ファイルをダウンロードしたら、OVA ファイルの SHA512sum 値が software.cisco.com の SHA512 チェックサム値と一致することを確認します。これを行うには、次のコマンドを実行します。

   ```
   sha512sum <path/to/file>
   ```

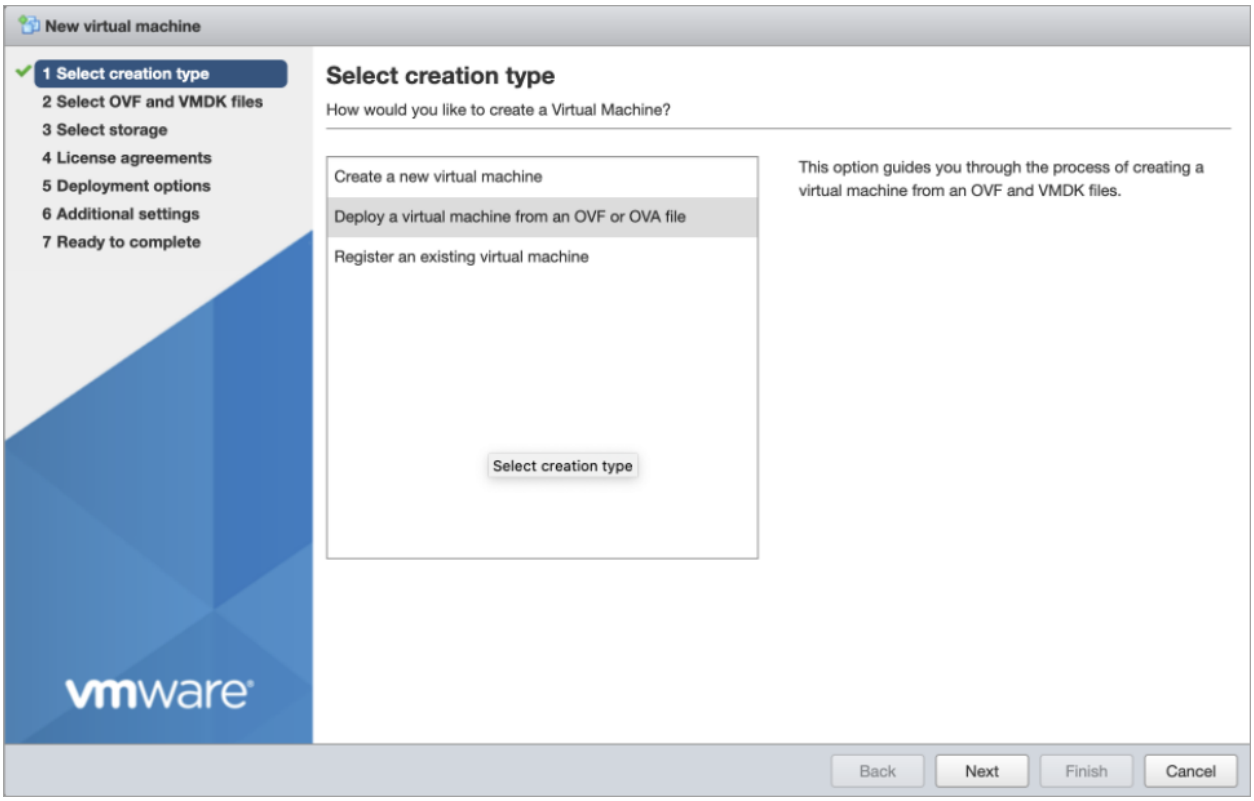
   software.cisco.com では、リンクのツールチップにカーソルを合わせると、SHA512sum 値が表示されます。

2. マネージャノードの展開

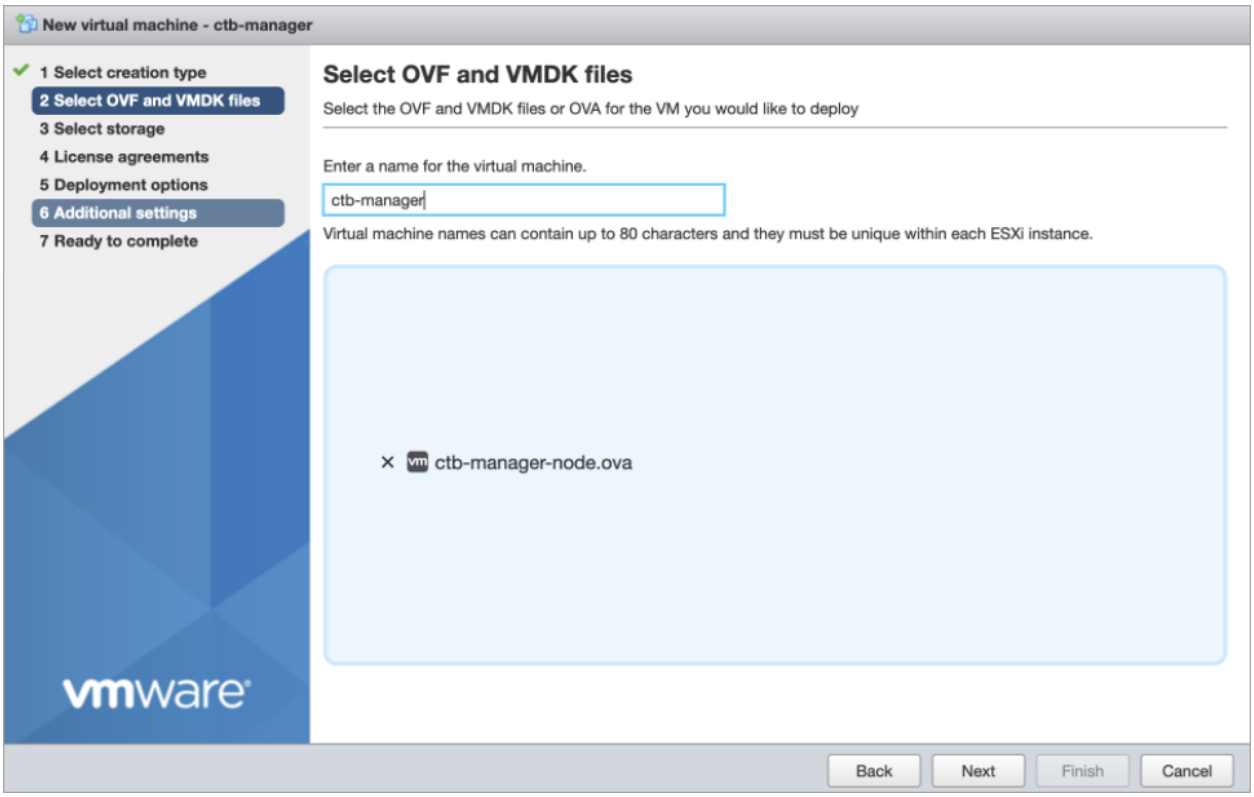
1. VMware vSphere の Web ユーザ インターフェイス コンソールにログインします。
2. サイドメニューから [仮想マシン（Virtual Machine）] を右クリックし、[VMの作成/登録（Create/Register VM）] を選択します。



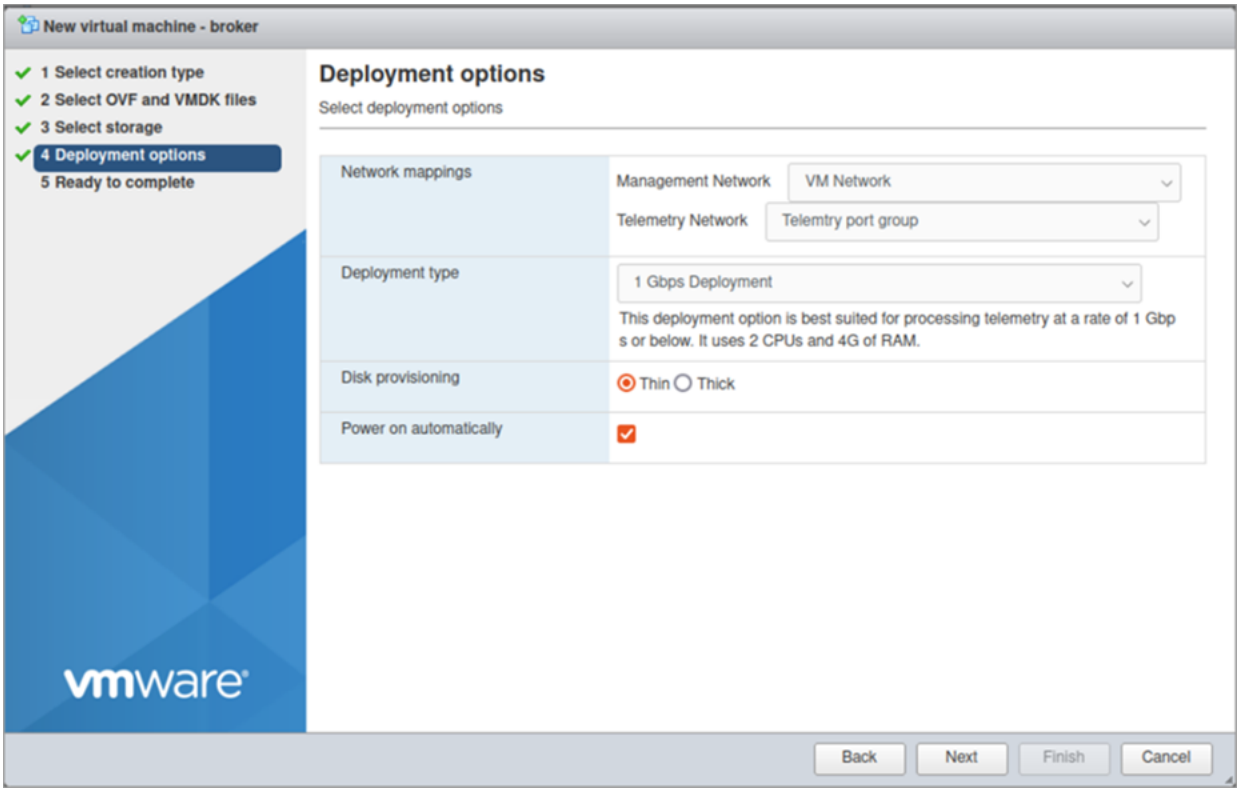
3. [OVFまたはOVAファイルから仮想マシンを展開する（Deploy a virtual machine from a OVF or OVA file）] を選択します。



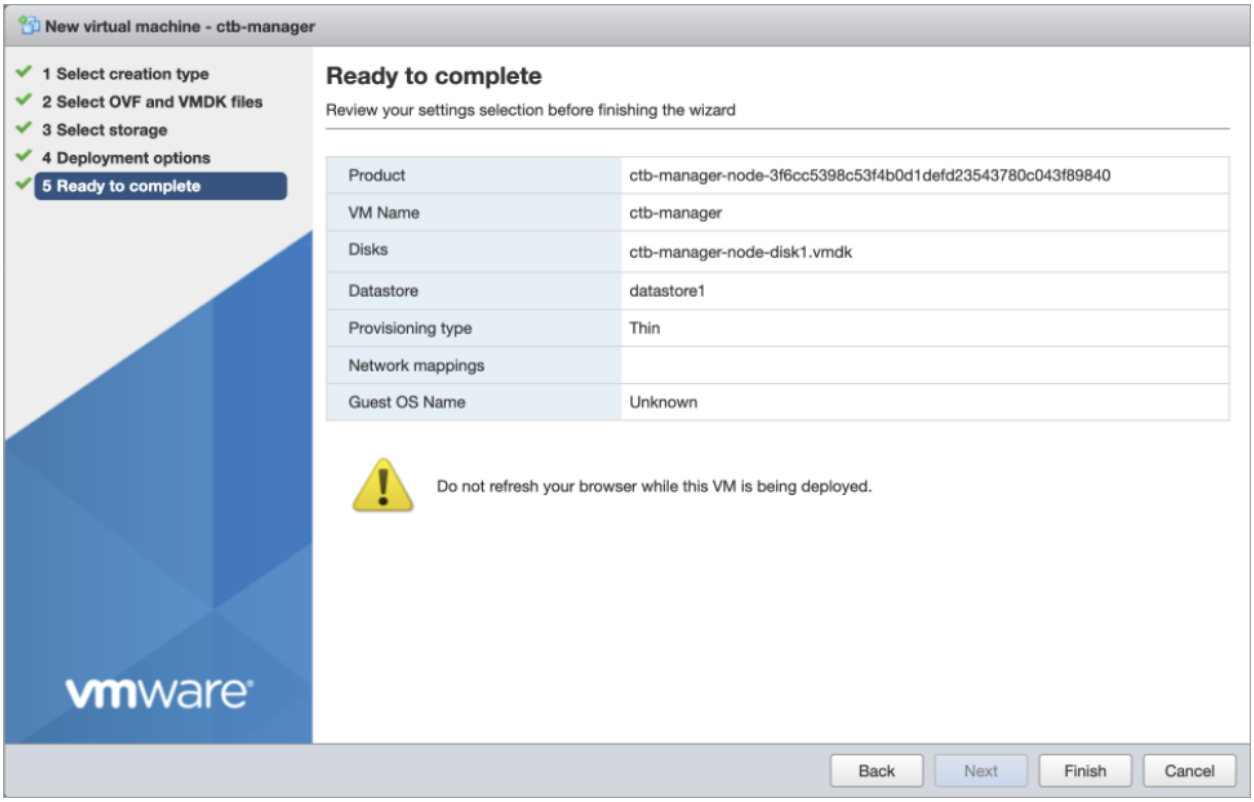
4. **OVA ファイルの名前**を入力します。



5. 次の図に示すように、設定を構成します。



6. [終了(Finish)]をクリックします。システムが起動し、ログインするように求められます。



3. リソース予約の設定

> 「**展開(導入)要件**」に従って、推奨される仮想マシンリソースを予約してください。そうしないと、実際に割り当てられるリソースが推奨値より少なくなり、次のアラートのいずれかまたは両方を受け取る可能性があります。
>
> - 不十分な CPU 割り当て(Insufficient CPU Allocated)
> - 不十分なメモリ割り当て(Insufficient Memory Allocated)

マネージャノードでは、すべてのコンピュータリソースが VM 専用である必要があります。これが確実に行われるようにするには、次の手順を実行します。

1. VMware インターフェイスで、前のセクション「マネージャノードの展開」で展開した マネージャノード VM をクリックします。
2. [編集(Edit)]をクリックして、VM の設定を編集するウィンドウを開きます。
3. [仮想ハードウェア(Virtual Hardware)]>[CPU]>[予約(Reservations)]を選択します。
4. [予約(Reservations)]の値を決定するには、VM の CPU 数にハイパーバイザのプロセッサタイプ(ハイパーバイザの[概要(Summary)]>[CPU]>[プロセッサタイプ(Processor Type)]画面で確認できます)の GHz 値を掛けます。
   - たとえば、ハイパーバイザでプロセッサタイプが @2.40 GHz と表示されていて、VM に 8 個の CPU が割り当てられている場合、次の式を使用します:8 x 2.40 GHz = 19200 MHz。この場合、[予約(Reservations)]の値として **19200 MHz** を指定する必要があり

ます。

- 一部の VMware 製品（VCenter など）では、事前に計算された値を反映する［最大（Maximum）］というラベルの付いた値を含むドロップダウンリストが提供されます。

5. ［仮想ハードウェア（Virtual Hardware）］>［メモリ（Memory）］>［予約（Reservations）］を選択します。
6. ［すべてのゲストメモリを予約（すべてロック）（Reserve all guest memory (all locked)）］チェックボックスをオンにします。
7. ［保存（Save）］をクリックして、設定を保存します。

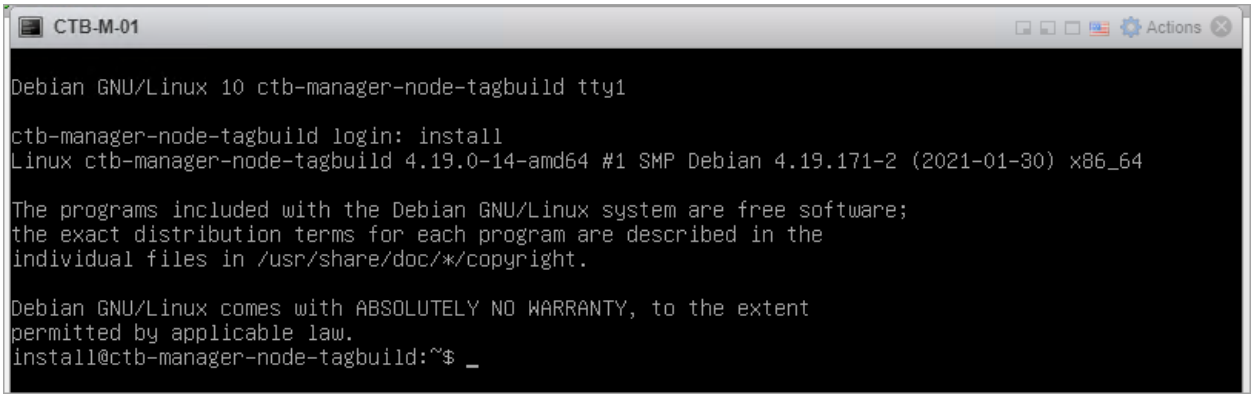
4. VM 時間設定の確認

VM はハイパーバイザに依存して正確な時刻を提供し、デフォルト設定で、これが確実に行われるはずです。しかし、次の手順を実行してこれを確認することをお勧めします。

1. VMware インターフェイスで、前のセクション「マネージャノードの展開」で展開した マネージャノード VM をクリックします。
2. ［編集（Edit）］をクリックして、VM の設定を編集するウィンドウを開きます。
3. ［VMオプション（VM Options）］>［VMwareツール（VMware Tools）］>［時間（Time）］を選択します。
4. ［ゲストの時間をホストと同期する（Synchronize guest time with host）］チェックボックスがオンになっていることを確認します。
5. ［保存（Save）］をクリックして、設定を保存します。

5. インストールユーザとしてログインする

vmware ユーザーインターフェイス内のマネージャノード仮想マシンから、Web コンソールを開き、仮想マシンにログインします（ユーザー名は **install**、パスワードはありません）。



6. sudo ctb-install --init コマンドを実行します。

> ⚠ 別の CTB 導入から設定を復元する場合は、`ctb-install --init` を実行して、*install* ユーザーとしてログアウトした後に `ctb-restore-config` を実行する必要があります。詳細については、「**新しいシステムへの設定の移行**」を参照してください。

1. `sudo ctb-install --init` コマンドを実行します。
2. 次の情報を入力します。
    - **管理者**ユーザのパスワード

      パスワードは次の要件を満たしている必要があります。
        - 8 文字以上
        - 少なくとも 1 つの小文字を含む
        - 少なくとも 1 つの大文字を含む
        - 少なくとも 1 つの数字を含む
        - 少なくとも 1 つの特殊文字を含む（@ # $ % ^ & * ! + ?）
        - 一般的に使用されるフレーズやシーケンスにはできません
        - ユーザの識別属性（ユーザ名など）と同じにすることはできません
    - ホスト名（最大 255 文字、文字と数字のみ）
    - 次の IP アドレスパラメータの 1 つまたは両方を入力できます。
        - 管理ネットワーク インターフェイスの IPv4 アドレス、サブネットマスク、デフォルト ゲートウェイ アドレス
        - 管理ネットワーク インターフェイスの IPv6 アドレス、サブネットマスク、デフォルト ゲートウェイ アドレス
    - 仮想マシンから到達可能な有効な DNS ネームサーバーの IP アドレス（1 つまたは 2 つ入力可能）

> 今後、個々のパラメーターを変更するには、`sudo ctb-install --config` コマンドを実行します。

7. 最初のスーパーユーザアカウントの設定

マネージャ Web インターフェイスに初めてログインする場合は、最初のスーパーユーザーアカウントを作成してから、ブローカーノードをインストールする必要があります。**webadmin** のユーザ名を、**admin** ユーザと混同しないように割り当てることをお勧めします。

- Web ブラウザで、次のサイトに移動して作成します。https://<manager_ip_address>。

8. ログアウト

ログアウトするには、「`exit`」と入力します。

VMware：ブローカノードのインストール

次の手順を順番に実行します。

1. ブローカノード OVA ファイルをダウンロードします。
2. ブローカノードを展開します。
3. リソース予約を設定します。
4. VM 時間設定を確認します。

5. インストールユーザとしてログインします。
6. sudo ctb-install --init コマンドを実行します。
7. sudo ctb-manage コマンドを実行します。
8. ログアウトします。
9. テレメトリインターフェイスを設定します。

> ブローカーノードをインストールする前に、マネージャノードをインストールして設定する必要があります。

1. ブローカノード OVA ファイルのダウンロード

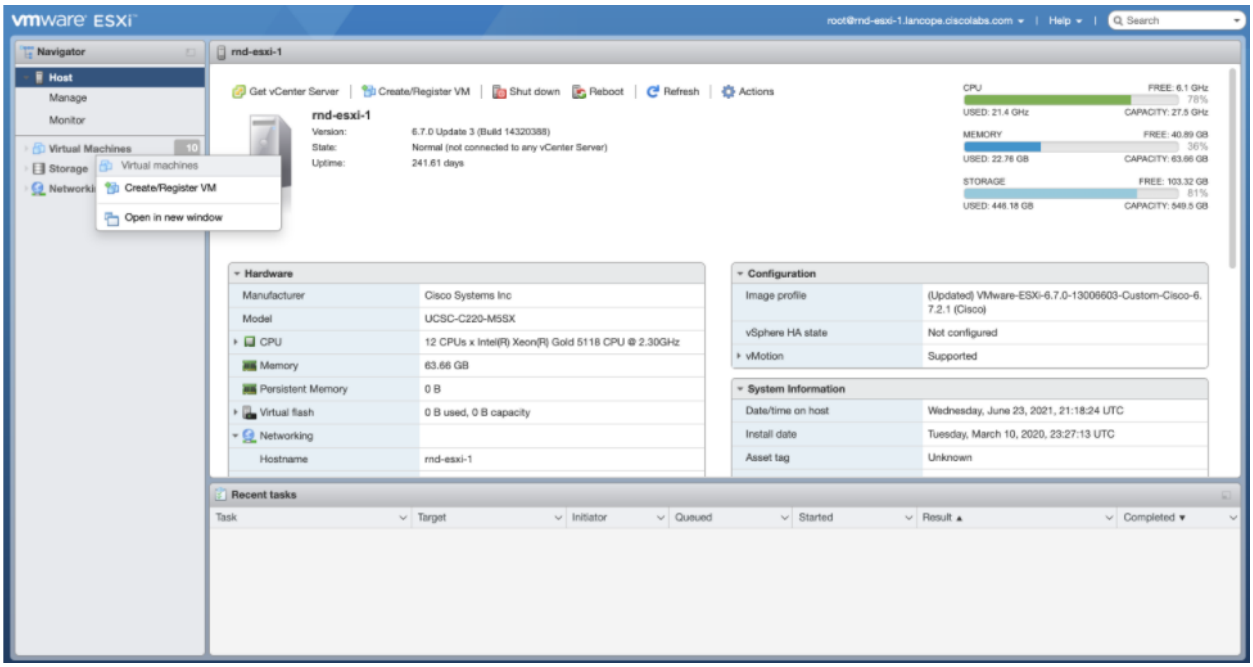
1. ブローカノード OVA ファイルをダウンロードします。
2. software.cisco.com で、OVA ファイルの SHA512sum 値を確認します。
3. OVA ファイルをダウンロードしたら、OVA ファイルの SHA512sum 値が software.cisco.com の SHA512 チェックサム値と一致することを確認します。これを行うには、次のコマンドを実行します。

   ```
   sha512sum <path/to/file>
   ```

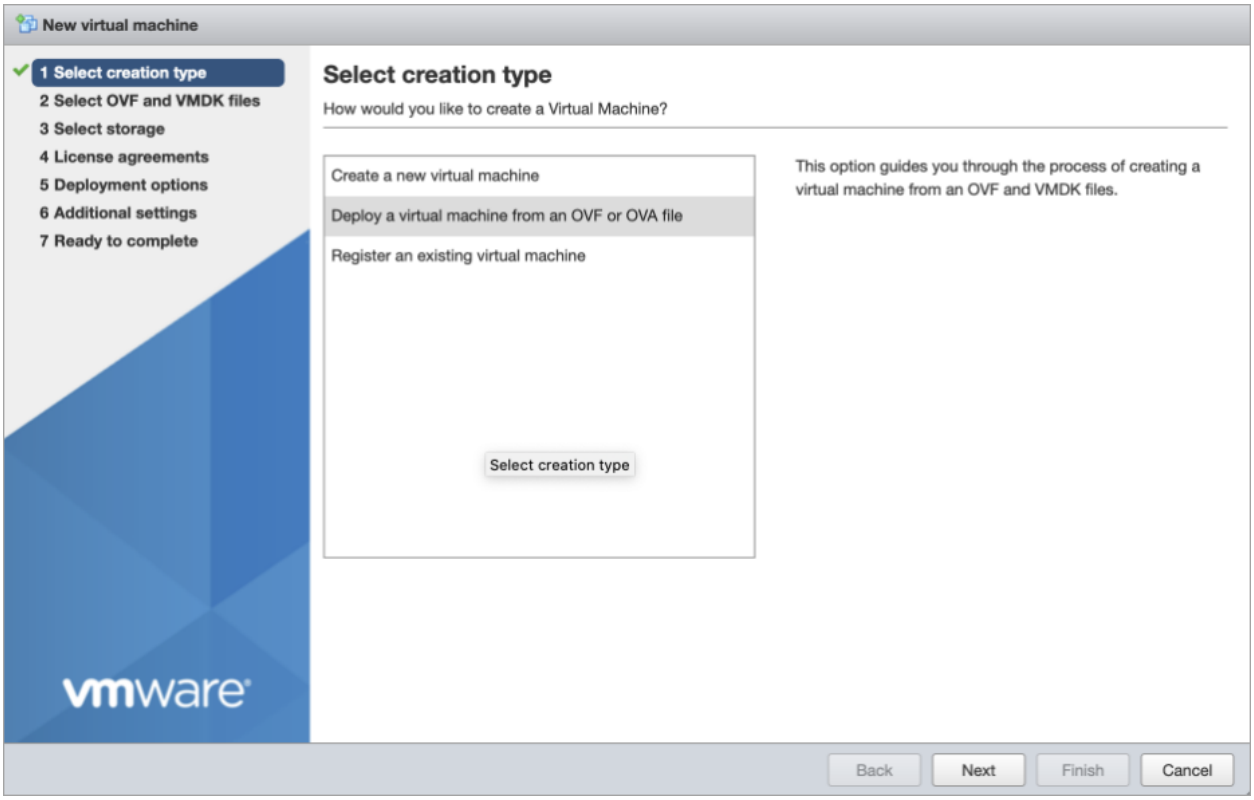
   software.cisco.com では、リンクのツールチップにカーソルを合わせると、SHA512sum 値が表示されます。

2. ブローカノードの展開

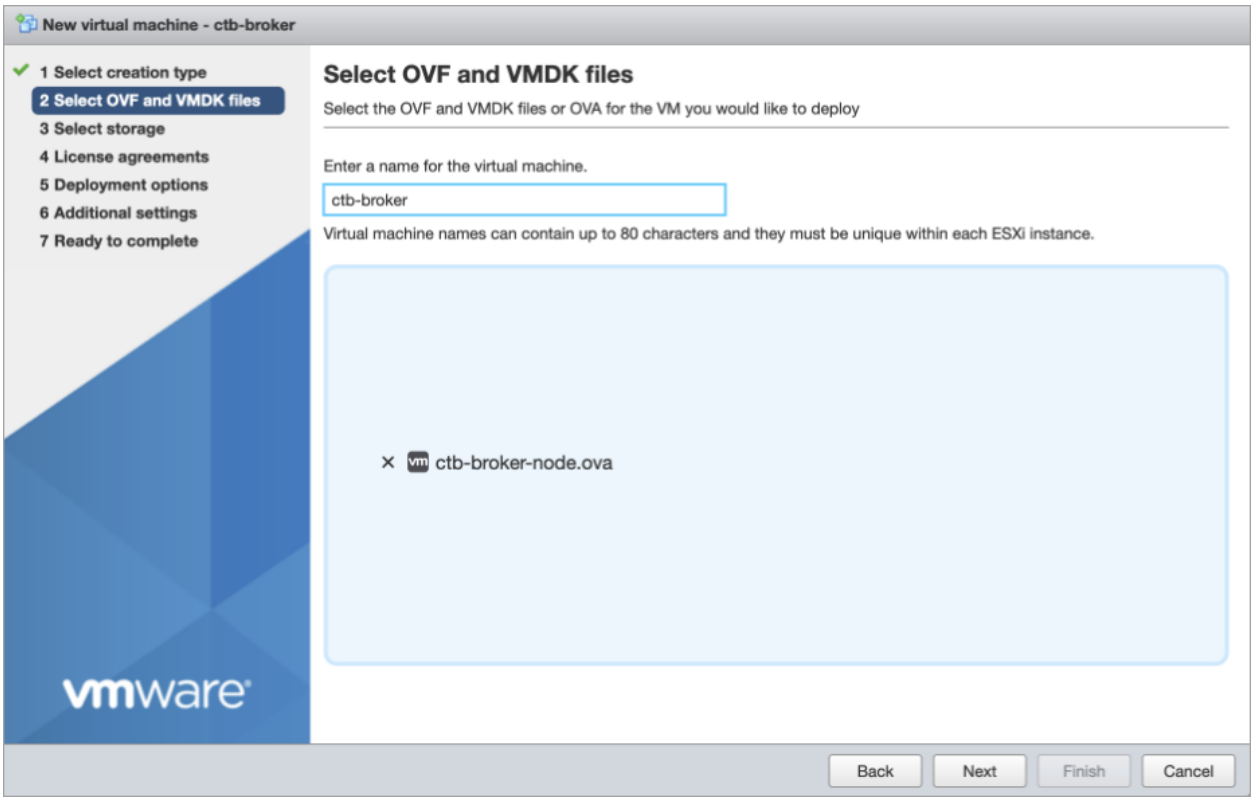
1. VMware vSphere の Web ユーザ インターフェイス コンソールにログインします。
2. サイドメニューから [仮想マシン（Virtual Machine）] を右クリックし、[VMの作成/登録（Create/Register VM）] を選択します。



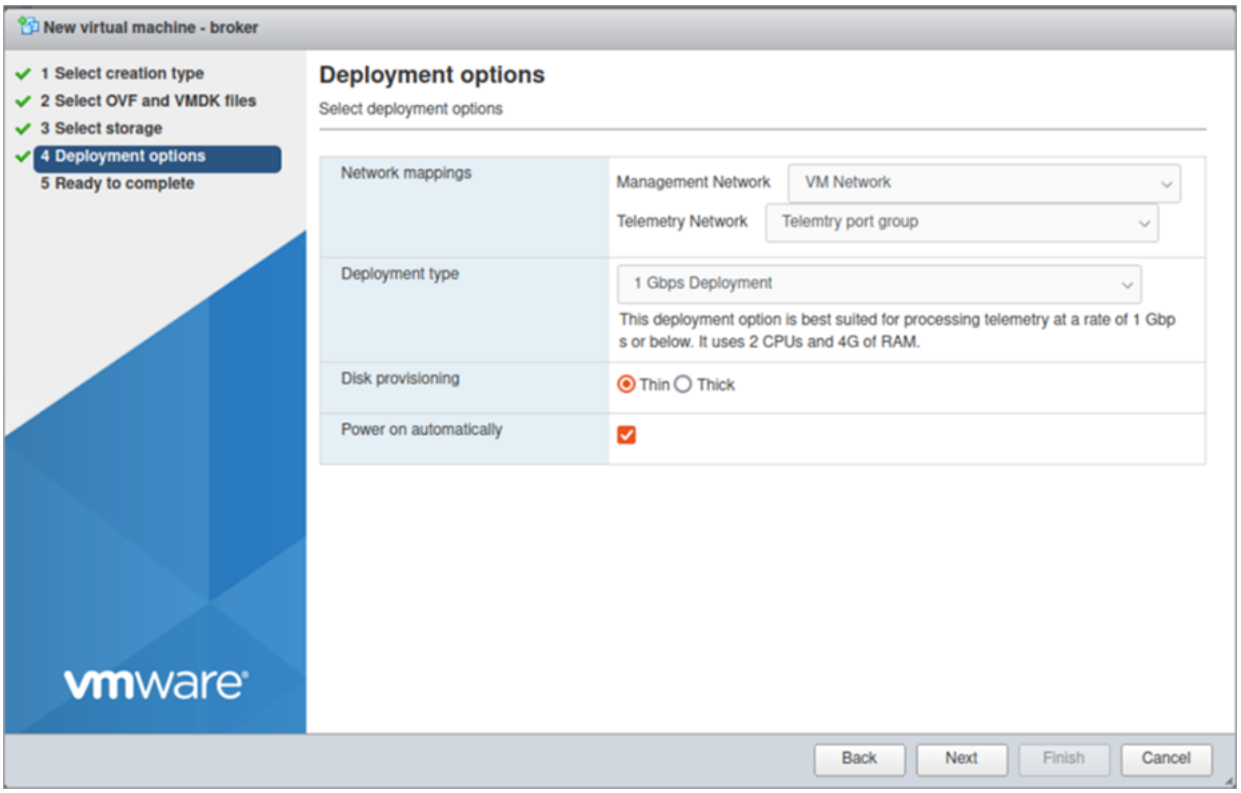
3. [OVFまたはOVAファイルから仮想マシンを展開する（Deploy a virtual machine from a OVF or OVA file）] を選択します。



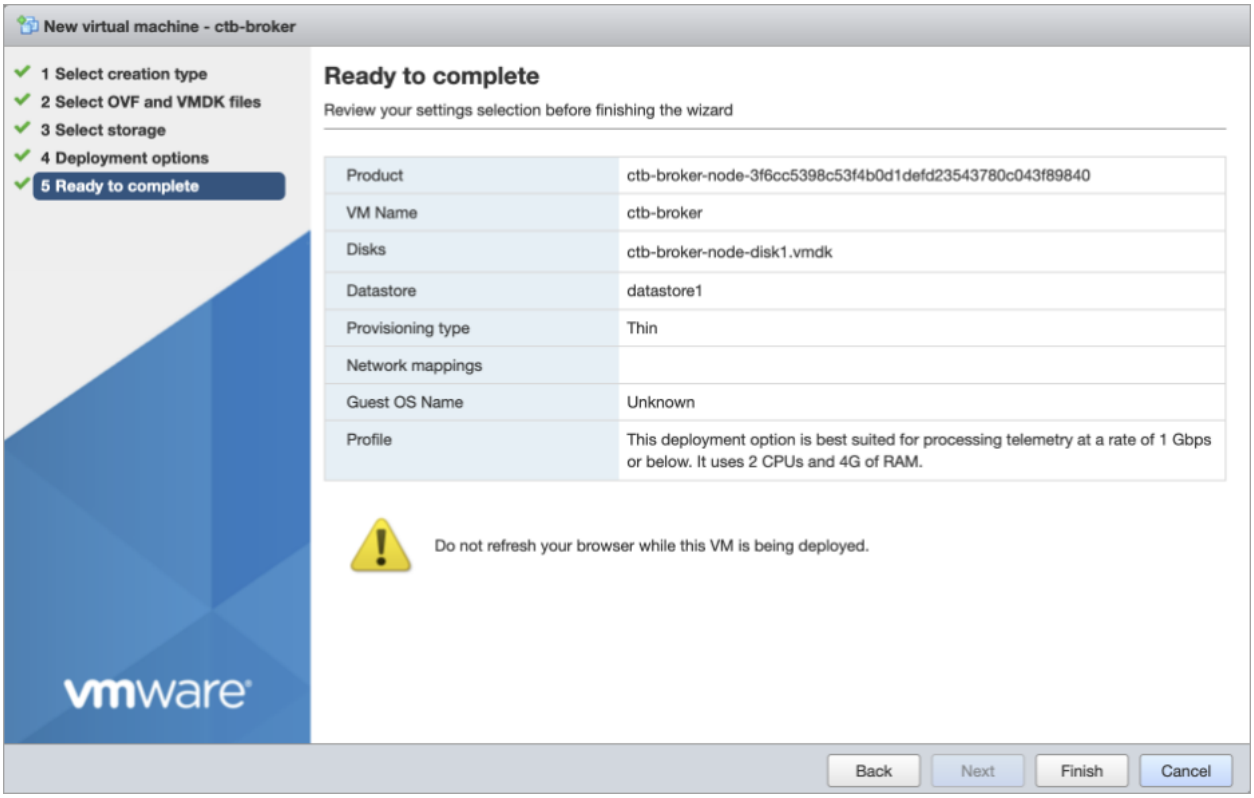
4. ステップ 3 でダウンロードした **OVA ファイルの名前**を入力します。



5. インストールに応じて [デフォルトタイプ（Default type）] を [1 Gbps]、[10 Gbps]、または [トランスフォーメーション対応（Transformation Capable）] に設定します。次の図に示すように、残りの設定を構成します。



6. ［終了（Finish）］をクリックします。



3. リソース予約の設定

> 「**展開（導入）要件**」に従って、推奨される仮想マシンリソースを予約してください。そうしないと、実際に割り当てられるリソースが推奨値より少なくなり、次のアラートのいずれかまたは両方を受け取る可能性があります。
>
> - 不十分な CPU 割り当て（Insufficient CPU Allocated）
> - 不十分なメモリ割り当て（Insufficient Memory Allocated）

ブローカノードでは、すべてのコンピュータリソースが VM 専用である必要があります。これが確実に行われるようにするには、次の手順を実行します。

1. VMware インターフェイスで、前のセクション「ブローカノードの展開」で展開したブローカノード VM をクリックします。
2. [編集（Edit）] をクリックして、VM の設定を編集するウィンドウを開きます。
3. [仮想ハードウェア（Virtual Hardware）] > [CPU] > [予約（Reservations）] を選択します。
4. [予約（Reservations）] の値を決定するには、VM の CPU 数にハイパーバイザのプロセッサタイプ（ハイパーバイザの [概要（Summary）] > [CPU] > [プロセッサタイプ（Processor Type）] 画面で確認できます）の GHz 値を掛けます。
   - たとえば、ハイパーバイザでプロセッサタイプが @2.40 GHz と表示されていて、VM に 8 個の CPU が割り当てられている場合、次の式を使用します：8 x 2.40 GHz = 19200 MHz。この場合、[予約（Reservations）] の値として **19200 MHz** を指定する必要があります。
   - 一部の VMware 製品（VCenter など）では、事前に計算された値を反映する [最大（Maximum）] というラベルの付いた値を含むドロップダウンリストが提供されます。
5. [仮想ハードウェア（Virtual Hardware）] > [メモリ（Memory）] > [予約（Reservations）] を選択します。
6. [すべてのゲストメモリを予約（すべてロック）（Reserve all guest memory (all locked)）] チェックボックスをオンにします。
7. [保存（Save）] をクリックして、設定を保存します。

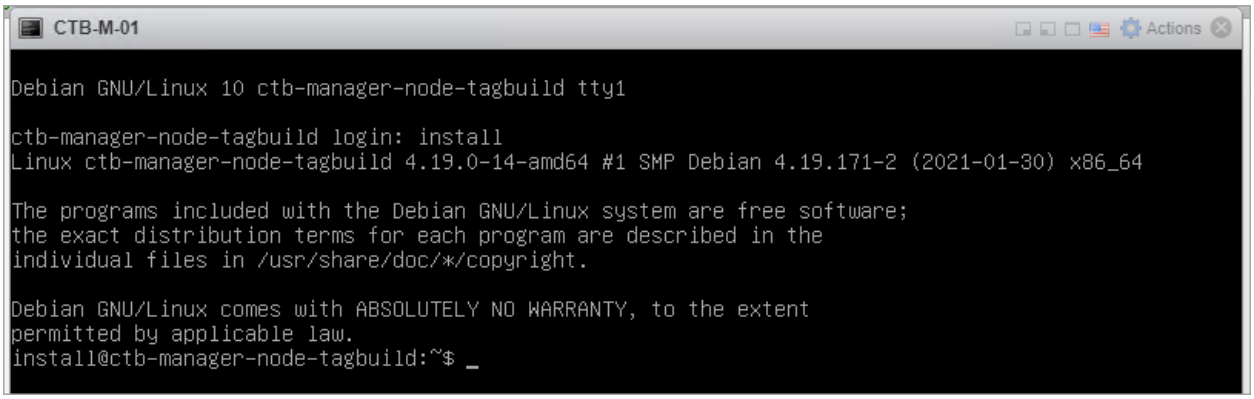
4. VM 時間設定の確認

VM はハイパーバイザに依存して正確な時刻を提供し、デフォルト設定で、これが確実に行われるはずです。しかし、次の手順を実行してこれを確認することをお勧めします。

1. VMware インターフェイスで、セクション 2「ブローカノードの展開」で展開したブローカノード VM をクリックします。
2. [編集（Edit）] をクリックして、VM の設定を編集するウィンドウを開きます。
3. [VMオプション（VM Options）] > [VMwareツール（VMware Tools）] > [時間（Time）] を選択します。
4. [ゲストの時間をホストと同期する（Synchronize guest time with host）] チェックボックスがオンになっていることを確認します。
5. [保存（Save）] をクリックして、設定を保存します。

5. インストールユーザとしてログインする

vmware ユーザインターフェイス内のブローカノード仮想マシンから、Web コンソールを開き、仮想マシンにログインします（ユーザ名は **install**、パスワードはありません）。



6. sudo ctb-install --init コマンドを実行します。

1. `sudo ctb-install --init` コマンドを実行します。
2. 次の情報を入力します。
   - **管理者**ユーザのパスワード

     パスワードは次の要件を満たしている必要があります。
     - 8 文字以上
     - 少なくとも 1 つの小文字を含む
     - 少なくとも 1 つの大文字を含む
     - 少なくとも 1 つの数字を含む
     - 少なくとも 1 つの特殊文字を含む（@ # $ % ^ & * ! + ?）
     - 一般的に使用されるフレーズやシーケンスにはできません
     - ユーザの識別属性（ユーザ名など）と同じにすることはできません
   - ホスト名（最大 255 文字、文字と数字のみ）
   - 次の IP アドレスパラメータの 1 つまたは両方を入力できます。
     - 管理ネットワーク インターフェイスの IPv4 アドレス、サブネットマスク、デフォルト ゲートウェイ アドレス
     - 管理ネットワーク インターフェイスの IPv6 アドレス、サブネットマスク、デフォルト ゲートウェイ アドレス
   - 仮想マシンから到達可能な有効な DNS ネームサーバーの IP アドレス（1 つまたは 2 つ入力可能）

> 今後、個々のパラメーターを変更するには、`sudo ctb-install --config` コマンドを実行します。

7. sudo ctb-manage コマンドの実行

1. `sudo ctb-manage` コマンドを実行します。
2. 次の情報を入力します。
    - マネージャノードの IP アドレス
    - マネージャノードで作成するスーパーユーザーアカウントのユーザー名
    - マネージャノードで作成するスーパーユーザーアカウントのパスワード

8. ログアウト

ログアウトするには、「`exit`」と入力します。

9. テレメトリインターフェイスの設定

「**テレメトリインターフェイスの設定**」に移動します。

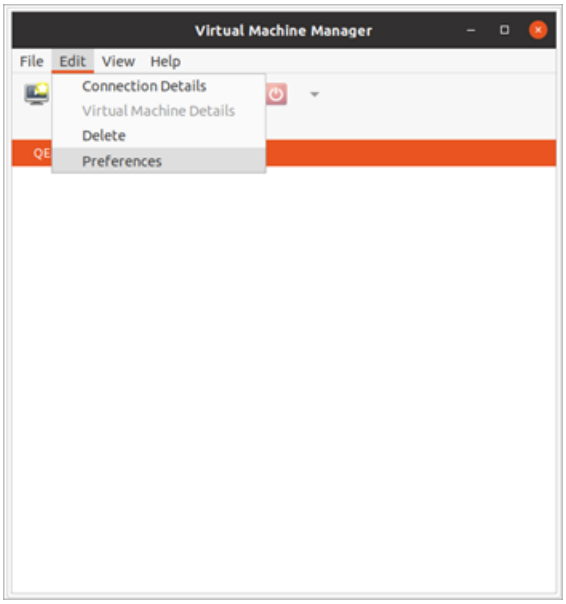
KVM のセットアップ

KVM（カーネル（ベースの）仮想マシン）を設定するための次の手順は、以下に基づいています。

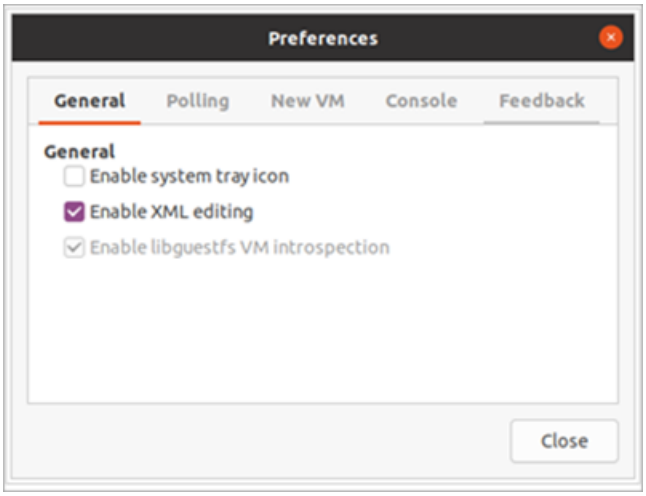
- libvirt 7.1.0
- qemu-kvm 5.2.0
- Linux Kernel 5.10.26
- Virtual Machine Manager（virt-manager）Ubuntu 2.2.1

> 続行する前に、Virtual Machine Manager で［XML編集の有効化（Enable XML Editing）］オプションを選択したことを確認します。ご使用の Virtual Machine Manager のバージョンが XML 編集をサポートしていない場合は、KVM ホストで *virsh edit* コマンドを使用して同じ手順を実行できます。

1. VM Manager を開き、［編集（Edit）］>［設定（Preferences）］の順に選択します。



2. ［XML編集の有効化（Enable XML Editing）］チェックボックスをオンにして、［閉じる（Close）］をクリックします。



KVM：マネージャノードのインストール

次の手順を順番に実行します。

1. マネージャノード QCOW2 ファイルをダウンロードします。
2. 仮想マシンを起動します。
3. インストールユーザとしてログインします。
4. sudo ctb-install --init コマンドを実行します。
5. 最初のスーパーユーザアカウントを設定します。
6. ログアウトします。

> ブローカーノードをインストールする前に、マネージャノードをインストールして設定する必要があります。

1. マネージャノード QCOW2 ファイルのダウンロード

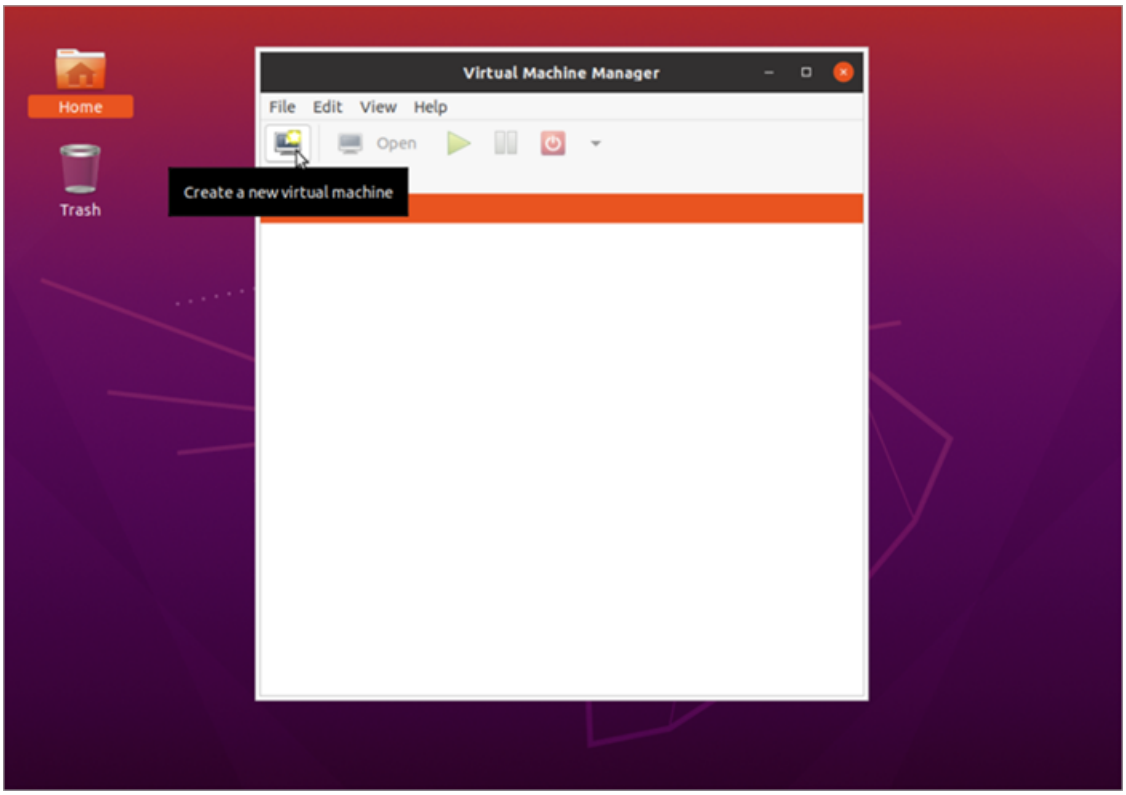
1. マネージャノード QCOW2 ファイルをダウンロードします。
2. software.cisco.com で、QCOW2 ファイルの SHA512sum 値を確認します。
3. QCOW2 ファイルをダウンロードしたら、QCOW2 ファイルの SHA512sum 値が software.cisco.com の SHA512 チェックサム値と一致することを確認します。これを行うには、次のコマンドを実行します。

   ```
   sha512sum <path/to/file>
   ```

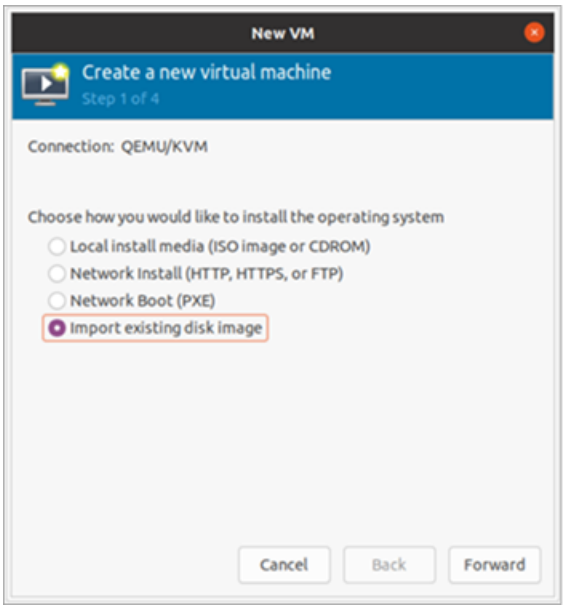
   software.cisco.com では、リンクのツールチップにカーソルを合わせると、SHA512sum 値が表示されます。

2. 仮想マシンの起動

1. KVM を実行している Linux システムで仮想マシンマネージャを開き、[新しい仮想マシンの作成（Create a new virtual machine）] をクリックします。

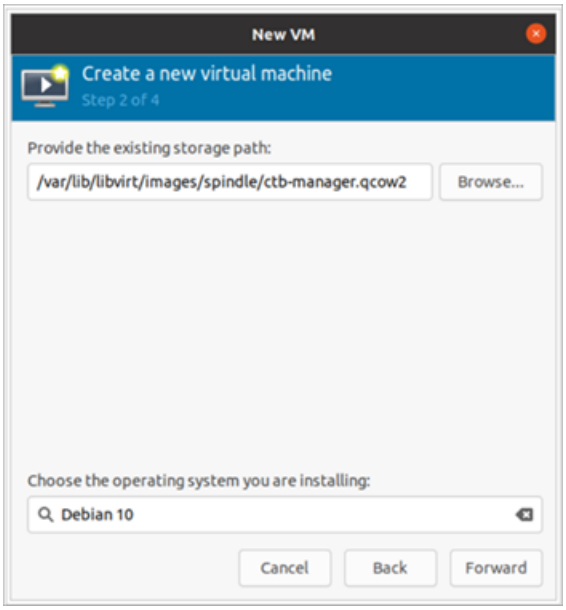


2. [新しい仮想マシンの作成(Create a new virtual machine)] ダイアログのステップ 1 で、[既存のディスクイメージをインポート(Import existing disk image)] オプションをオンにします。[続行(Forward)] をクリックします。



3. [新しい仮想マシンの作成(Create a new virtual machine)] ダイアログボックスのステップ 2 で、次を実行します。

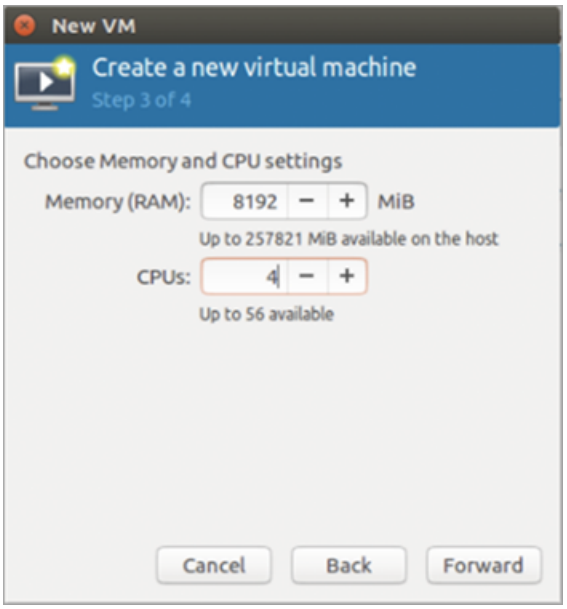
a. ステップ 1 でダウンロードした QCOW2 ファイルへの既存のストレージパスを入力します。
b. オペレーティングシステムには、[Debian Buster] を選択します。
c. [続行（Forward）] をクリックします。



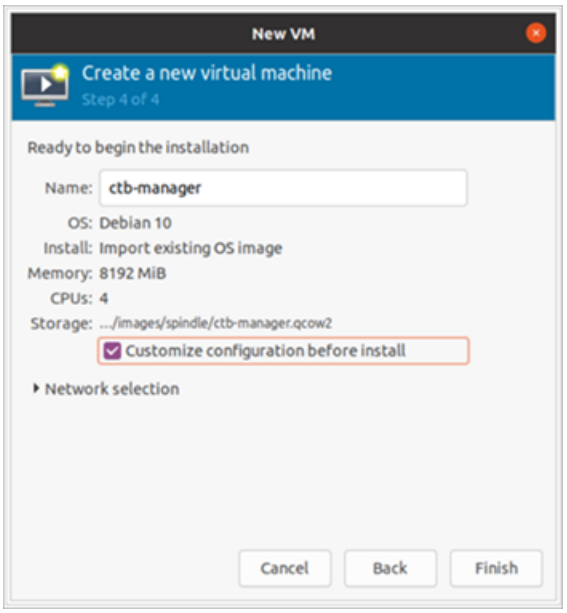
「**展開（導入）要件**」に従って、推奨される仮想マシンリソースを予約してください。そうしないと、実際に割り当てられるリソースが推奨値より少なくなり、次のアラートのいずれかまたは両方を受け取る可能性があります。

- 不十分な CPU 割り当て（Insufficient CPU Allocated）
- 不十分なメモリ割り当て（Insufficient Memory Allocated）

4. [新しい仮想マシンの作成（Create a new virtual machine）] ダイアログボックスのステップ 3 で、次を実行します。
   a. [メモリ（RAM）（Memory（RAM））] フィールドで、エントリを **8 GB** 以上に設定します。
   b. [CPU] フィールドで、エントリを **4** 以上に設定します。
   c. [続行（Forward）] をクリックします。



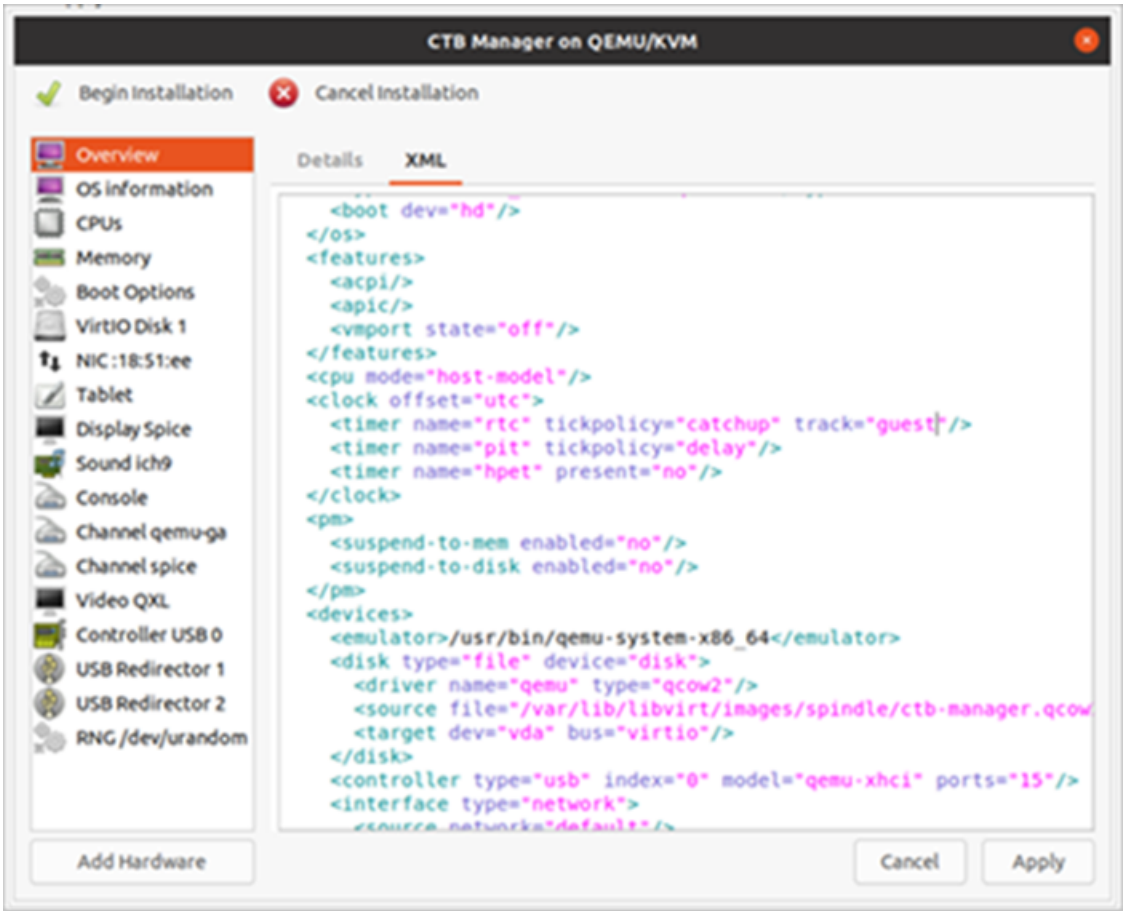
5. [新しい仮想マシンの作成（Create a new virtual machine）] ダイアログボックスのステップ 4 で、次を実行します。
   a. [名前（Name）] フィールドに、**ctb-manager** と入力します。
   b. [インストール前に構成をカスタマイズ（Customize configuration before install）] チェックボックスをオンにします。
   c. [終了（Finish）] をクリックします。



6. 次の手順を実行します。
   a. サイドメニューから、[概要（Overview）] を選択します。
   b. [XML] タブをクリックします。

c. `<timer name="rtc" tickpolicy="catchup"/>` の行を `<timer name="rtc" tickpolicy="catchup" track="guest"/>` に変更します

d. [適用（Apply）] をクリックします。

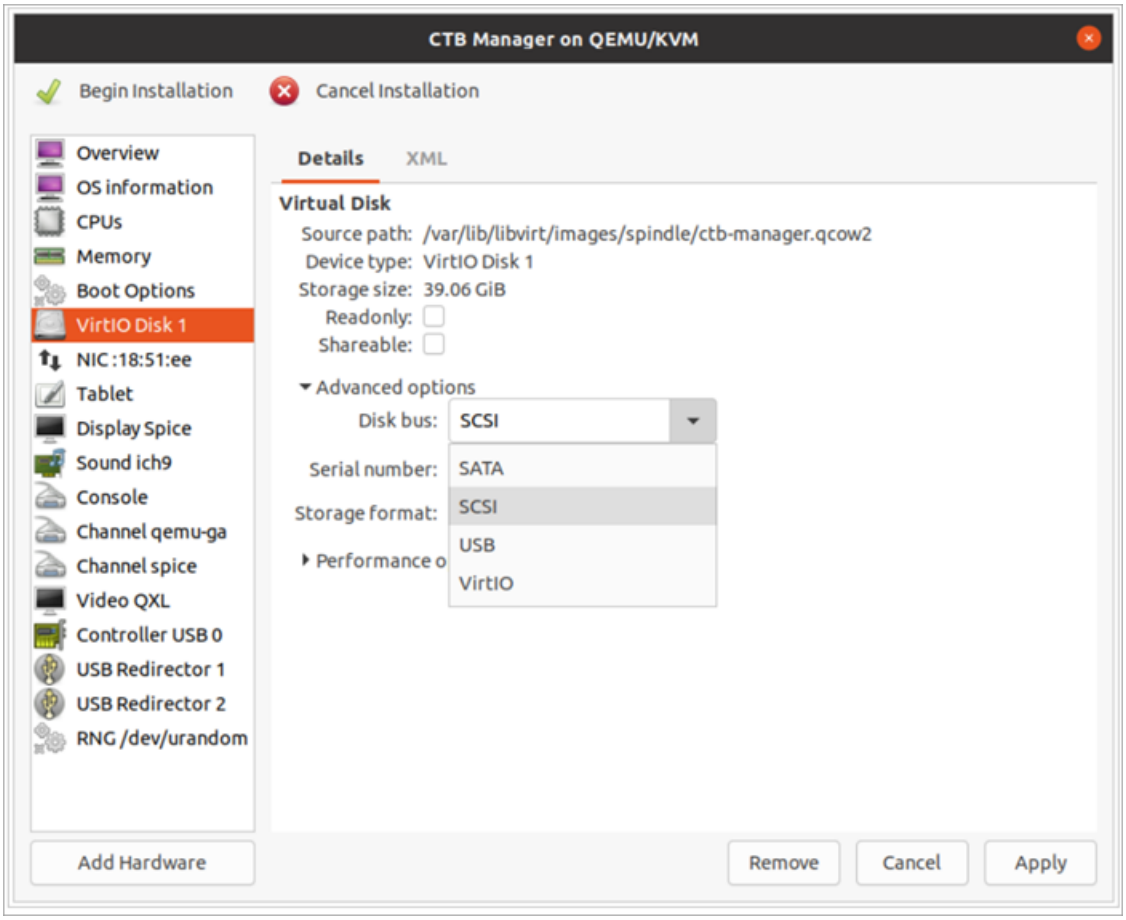


7. 次の手順を実行します。

a. サイドメニューから [VirtIOディスク1（VirtIO Disk 1）] を選択します。

b. [詳細（Details）] タブで、[詳細オプション（Advanced Options）] の [ディスクバス（Disk Bus）] ドロップダウンリストから [SCSI] を選択します。

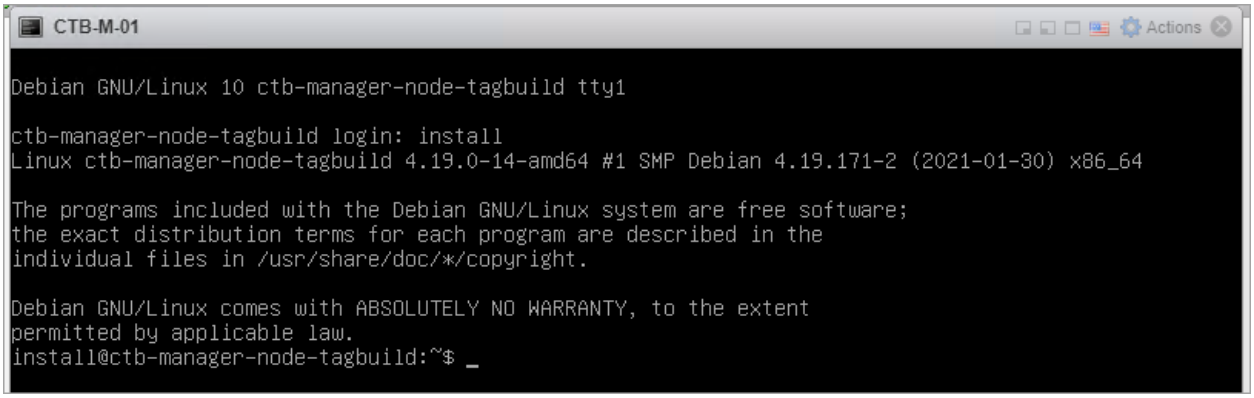
c. [適用] をクリックします。



8. ページの左上隅にある［インストールの開始（Begin Installation）］をクリックします。

3. インストールユーザとしてログインする

vmware ユーザーインターフェイス内のマネージャノード仮想マシンから、Web コンソールを開き、仮想マシンにログインします（ユーザー名は **install**、パスワードはありません）。



4. sudo ctb-install --init コマンドを実行します。

> ⚠ 別の CTB 導入から設定を復元する場合は、`ctb-install --init` を実行して、*install* ユーザーとしてログアウトした後に `ctb-restore-config` を実行する必要があります。詳細については、「**新しいシステムへの設定の移行**」を参照してください。

1. `sudo ctb-install --init` コマンドを実行します。
2. 次の情報を入力します。
   - **管理者**ユーザのパスワード

     パスワードは次の要件を満たしている必要があります。
     - 8 文字以上
     - 少なくとも 1 つの小文字を含む
     - 少なくとも 1 つの大文字を含む
     - 少なくとも 1 つの数字を含む
     - 少なくとも 1 つの特殊文字を含む（@ # $ % ^ & * ! + ?）
     - 一般的に使用されるフレーズやシーケンスにはできません
     - ユーザの識別属性（ユーザ名など）と同じにすることはできません
   - ホスト名（最大 255 文字、文字と数字のみ）
   - デフォルト名 default mgmt = 'ens160' および default telem = 'ens192' と異なる場合は、インターフェイス名を指定します。

```
== Setting up network interfaces:

The following NICs were discovered:
Interface    Bus Info            Size          Description
=========================================================
enp1s0       pci@0000:01:00.0    0             Virtio network device
enp8s0       pci@0000:08:00.0    0             Virtio network device


Please select management interface (options: enp1s0,enp8s0):enp1s0


Please select telemetry interface (options: enp8s0):enp8s0_
```

   - 次の IP アドレスパラメータの 1 つまたは両方を入力できます。
     - 管理ネットワーク インターフェイスの IPv4 アドレス、サブネットマスク、デフォルト ゲートウェイ アドレス
     - 管理ネットワーク インターフェイスの IPv6 アドレス、サブネットマスク、デフォルト ゲートウェイ アドレス
   - 仮想マシンから到達可能な有効な DNS ネームサーバーの IP アドレス（1 つまたは 2 つ入力可能）

> ℹ 今後、個々のパラメーターを変更するには、`sudo ctb-install --config` コマンドを実行します。

5. 最初のスーパーユーザアカウントの設定

マネージャ Web インターフェイスに初めてログインする場合は、最初のスーパーユーザーアカウントを作成してから、ブローカーノードをインストールする必要があります。**webadmin** のユーザ名を、**admin** ユーザと混同しないように割り当てることをお勧めします。

- Web ブラウザで、次のサイトに移動して作成します。https://<manager_ip_address>。

6. ログアウト

ログアウトするには、「`exit`」と入力します。

KVM：ブローカノードのインストール

次の手順を順番に実行します。

1. ブローカノード QCOW2 ファイルをダウンロードします。
2. 仮想マシンを起動します。
3. インストールユーザとしてログインします。
4. sudo ctb-install コマンドを実行します。
5. sudo ctb-manage コマンドを実行します。
6. ログアウトします。
7. テレメトリインターフェイスを設定します。

> ブローカーノードをインストールする前に、マネージャノードをインストールして設定する必要があります。

1. ブローカノード QCOW2 ファイルのダウンロード

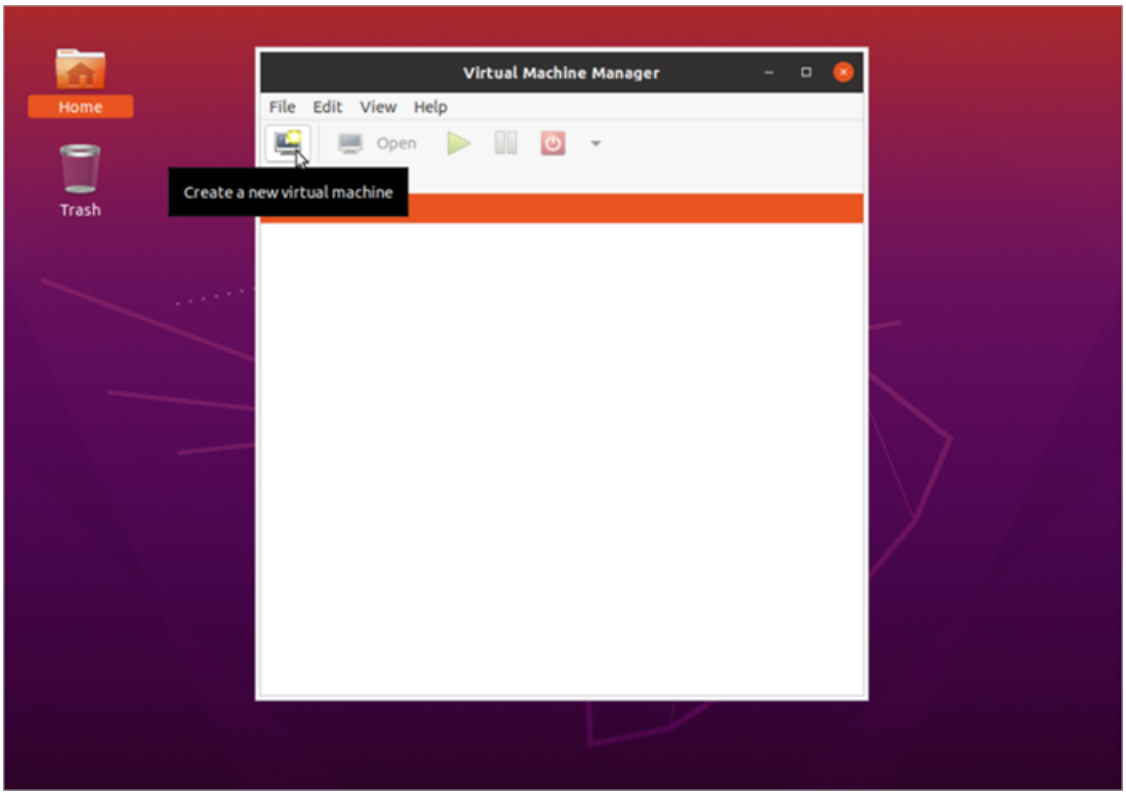
1. ブローカノード QCOW2 ファイルをダウンロードします。
2. software.cisco.com で、QCOW2 ファイルの SHA512sum 値を確認します。
3. OVA ファイルをダウンロードしたら、OVA ファイルの SHA512sum 値が software.cisco.com の SHA512 チェックサム値と一致することを確認します。これを行うには、次のコマンドを実行します。

   ```
   sha512sum <path/to/file>
   ```

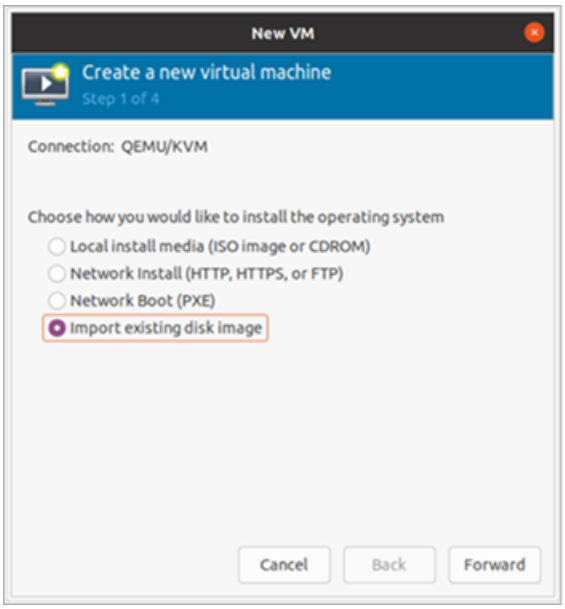
   software.cisco.com では、リンクのツールチップにカーソルを合わせると、SHA512sum 値が表示されます。

2. 仮想マシンの起動

1. KVM を実行している Linux システムで仮想マシンマネージャを開き、[新しい仮想マシンの作成（Create a new virtual machine）] をクリックします。



2. [新しい仮想マシンの作成(Create a new virtual machine)] ダイアログのステップ 1 で、[既存のディスクイメージをインポート(Import existing disk image)] オプションをオンにします。[続行(Forward)] をクリックします。

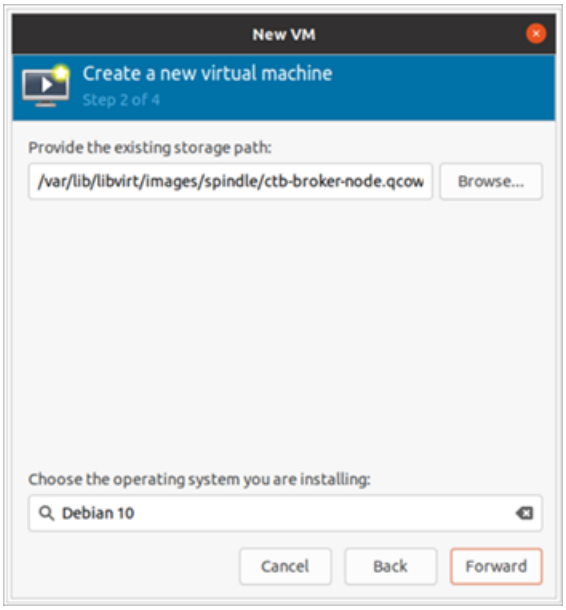


3. [新しい仮想マシンの作成(Create a new virtual machine)] ダイアログボックスのステップ 2 で、次を実行します。

a. ステップ 1 でダウンロードした QCOW2 ファイルへの既存のストレージパスを入力します。
b. オペレーティングシステムには、[Debian Buster] を選択します。
c. [続行（Forward）] をクリックします。

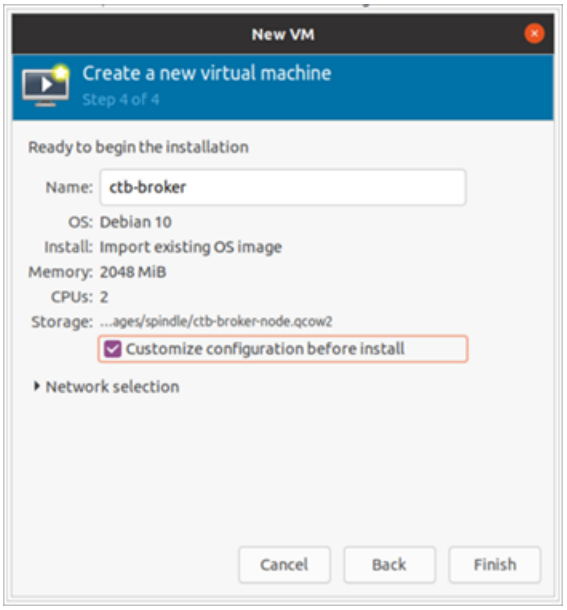
「**展開（導入）要件**」に従って、推奨される仮想マシンリソースを予約してください。そうしないと、実際に割り当てられるリソースが推奨値より少なくなり、次のアラートのいずれかまたは両方を受け取る可能性があります。

- 不十分な CPU 割り当て（Insufficient CPU Allocated）
- 不十分なメモリ割り当て（Insufficient Memory Allocated）



4. [新しい仮想マシンの作成（Create a new virtual machine）] ダイアログボックスのステップ 3 で、次を実行します。
   a. [メモリ（RAM）（Memory（RAM））] フィールドで、エントリを **2 GB** 以上に設定します。
   b. [CPU] フィールドで、エントリを **2** に設定します（ブローカに追加の CPU を割り当てても、KVM のパフォーマンスは必ずしも向上しません）。
   c. [続行（Forward）] をクリックします。

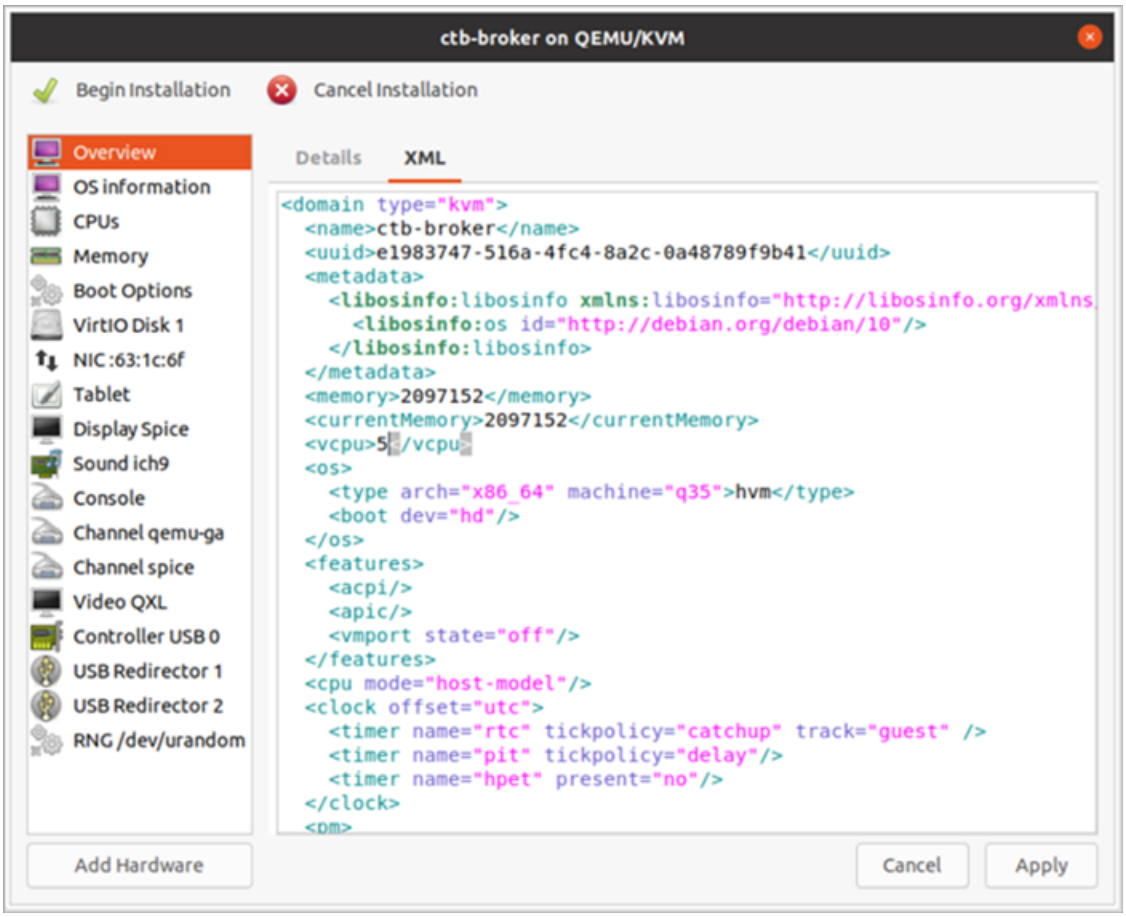
5. [新しい仮想マシンの作成（Create a new virtual machine）] ダイアログボックスのステップ 4 で、次を実行します。
   a. [名前（Name）] フィールドに、**ctb-broker** と入力します。
   b. [インストール前に構成をカスタマイズ（Customize configuration before install）] チェックボックスをオンにします。
   c. [終了（Finish）] をクリックします。



6. 次の手順を実行します。
   a. サイドメニューから、[概要（Overview）] を選択します。
   b. [XML] タブをクリックします。

c. `<timer name="rtc" tickpolicy="catchup"/>` の行を `<timer name="rtc" tickpolicy="catchup" track="guest"/>` に変更します

d. [適用（Apply）] をクリックします。

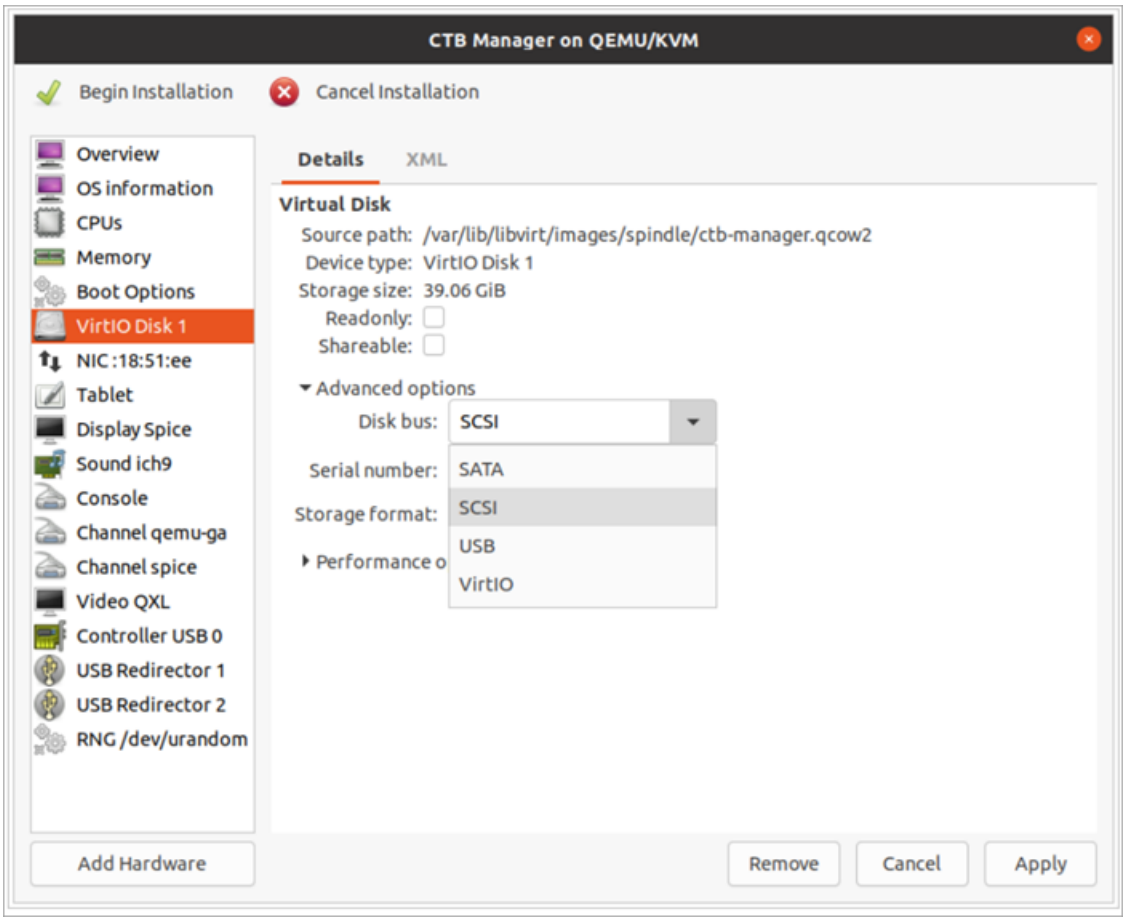


7. 次の手順を実行します。

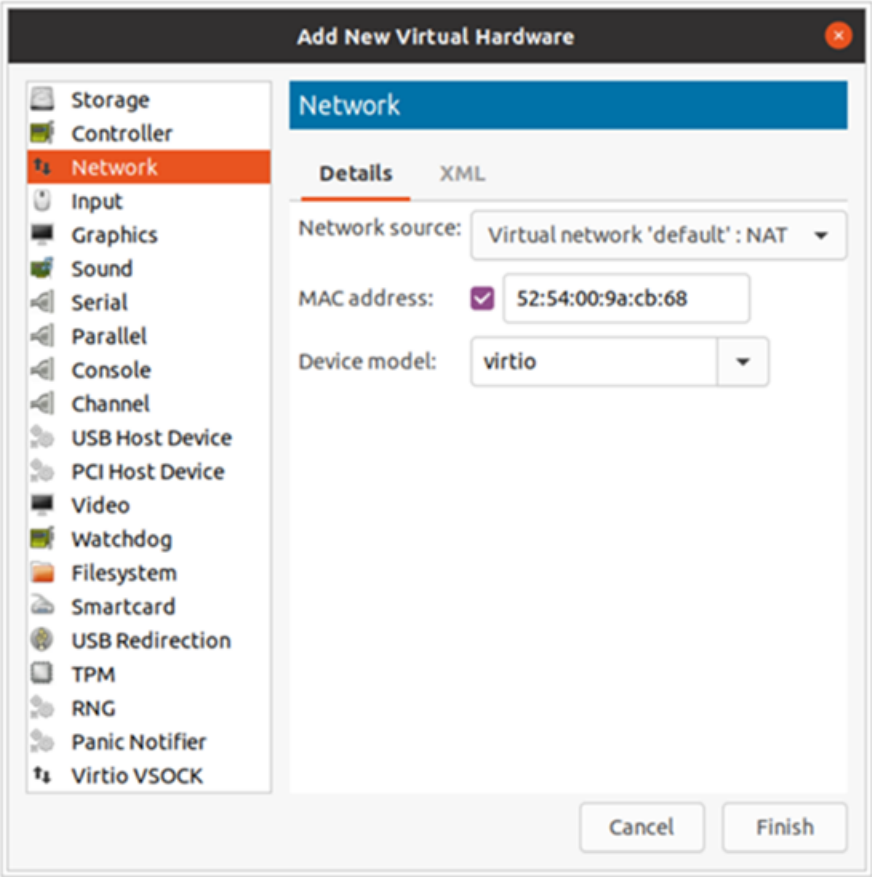
a. サイドメニューから [VirtIOディスク1（VirtIO Disk 1）] を選択します。

b. [詳細（Details）] タブで、[詳細オプション（Advanced Options）] の [ディスクバス（Disk Bus）] ドロップダウンリストから [SCSI] を選択します。

c. [適用（Apply）] をクリックします。



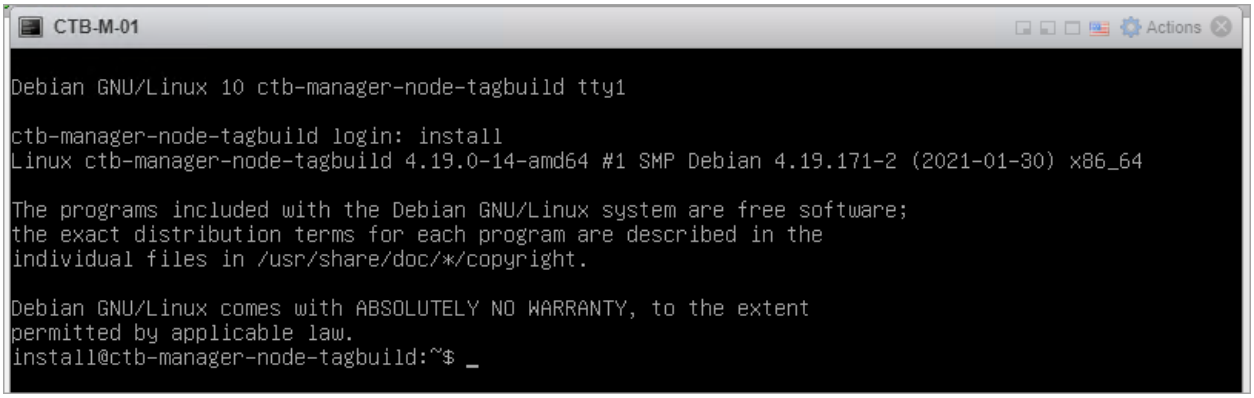
8. サイドメニューから、[ハードウェアの追加（Add Hardware）] > [ネットワーク（Network）] の順に選択します。[終了（Finish）] をクリックします。



9. [インストールの開始(Begin Installation)]をクリックします。

3. インストールユーザとしてログインする

vmware ユーザインターフェイス内のブローカノード仮想マシンから、Web コンソールを開き、仮想マシンにログインします(ユーザ名は **install**、パスワードはありません)。



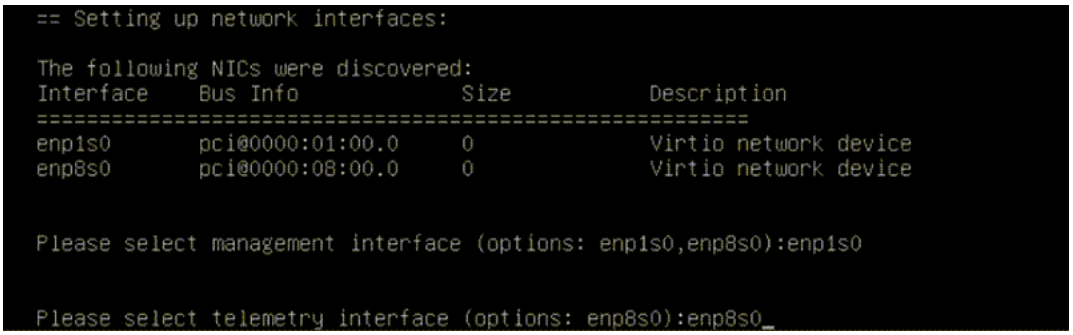
4. sudo ctb-install --init コマンドを実行します。

1. `sudo ctb-install --init` コマンドを実行します。
2. 次の情報を入力します。

- **管理者**ユーザのパスワード

  パスワードは次の要件を満たしている必要があります。

  - 8 文字以上
  - 少なくとも 1 つの小文字を含む
  - 少なくとも 1 つの大文字を含む
  - 少なくとも 1 つの数字を含む
  - 少なくとも 1 つの特殊文字を含む（@ # $ % ^ & * ! + ?）
  - 一般的に使用されるフレーズやシーケンスにはできません
  - ユーザの識別属性（ユーザ名など）と同じにすることはできません
- ホスト名（最大 255 文字、文字と数字のみ）
- デフォルト名 default mgmt = 'ens160' および default telem = 'ens192' と異なる場合は、インターフェイス名を指定します。



- 次の IP アドレスパラメータの 1 つまたは両方を入力できます。
  - 管理ネットワーク インターフェイスの IPv4 アドレス、サブネットマスク、デフォルトゲートウェイ アドレス
  - 管理ネットワーク インターフェイスの IPv6 アドレス、サブネットマスク、デフォルトゲートウェイ アドレス
- 仮想マシンから到達可能な有効な DNS ネームサーバーの IP アドレス（1 つまたは 2 つ入力可能）

> 今後、個々のパラメーターを変更するには、`sudo ctb-install --config` コマンドを実行します。

5. sudo ctb-manage コマンドの実行

1. `sudo ctb-manage` コマンドを実行します。
2. 次の情報を入力します。
   - マネージャノードの IP アドレス
   - マネージャノードで作成するスーパーユーザーアカウントのユーザー名
   - マネージャノードで作成するスーパーユーザーアカウントのパスワード

6. ログアウト

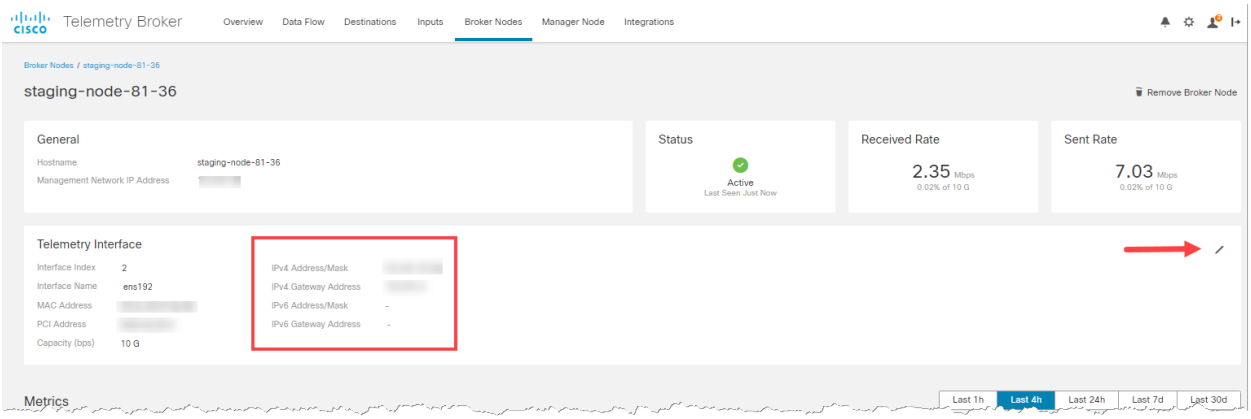
ログアウトするには、「`exit`」と入力します。

7. テレメトリインターフェイスの設定

「**テレメトリインターフェイスの設定**」に移動します。

テレメトリインターフェイスの設定

1. Cisco Telemetry Broker にログインします。Web ブラウザで、マネージャの管理インターフェイスの IP アドレスを入力し、**Enter** を押してマネージャの Web インターフェイスのログインに移動します。
2. メインメニューから [ブローカーノード（Broker Nodes）] を選択します。
3. [ブローカノード（Broker Nodes）] テーブルで、該当するブローカノードをクリックします。
4. [テレメトリインターフェイス（Telemetry Interface）] セクションで、（**編集**）アイコンをクリックします（次の図の矢印で示されています）。



5. IP アドレスとゲートウェイアドレスを設定します（赤い枠で囲まれています）。

高可用性クラスタの管理

Cisco Telemetry Broker ハイアベイラビリティにより、高い可用性を持つ IPv4 および IPv6 仮想 IP アドレスが入力のターゲットとして提供され、入力から宛先への信頼性の高いテレメトリ配信が保証されます。

ハイ アベイラビリティ クラスタを複数作成し、それぞれのクラスタに複数のブローカノードを割り当てることで、ブローカノードの高可用性を確立することができます。各クラスタでは、1 つのブローカノードがアクティブに指定されます。これは、テレメトリを受け渡し、メトリックを Cisco Telemetry Broker に提供することを意味します。残りのノードは、パッシブに指定されます。これは、現時点でテレメトリを渡さず、メトリックを提供しないことを意味します。アクティブなブローカノードがテレメトリの受け渡しを停止するか、Telemetry Broker との接続を失うと、いずれかのパッシブブローカノードがアクティブなブローカノードに昇格し、テレメトリの受け渡しを開始します。

クラスタについては、次の点に注意してください。

- 各ブローカノードは、同時に 1 つのクラスタのみに属することができます。
- 特定のクラスタでどのブローカノードがアクティブであるかを選択することはできません。
- 特定の仮想 IP アドレスのアクティブブローカノードに障害が発生すると、同じクラスタ内のパッシブブローカノードの 1 つがその仮想 IP アドレスのアクティブブローカノードになります。障害が発生したブローカノードが復帰すると、パッシブブローカノードの状態を維持します。そのノードを再度アクティブにする場合は、提供されているコマンドを使用して手動で操作する必要があります。
- ブローカノードを 1 つのみ持つクラスタを作成できますが、このブローカノードに障害が発生した場合、アクティブなブローカノードに昇格できるブローカノード内のクラスタがありません。同様に、クラスタ内のすべてのブローカノードに障害が発生した場合は、アクティブなブローカノードに昇格できるブローカノードはありません。ブローカノードに障害が発生した場合は、できるだけ早くオンラインに復帰させてください。
- ブローカノードを持たないクラスタを作成し、後でブローカノードを追加できます。
- 仮想 IPv4 または仮想 IPv6 アドレスのいずれか、または両方をクラスタに割り当てることができます。Telemetry Broker は、この仮想 IP アドレスを使用してクラスタと通信し、アクティブなブローカノードと Telemetry Broker の接続が失われた場合にパッシブのブローカノードをアクティブなブローカノードに昇格させます。

VIP とルーティング

高可用性は、VIP アドレスブローカノードのテレメトリ ネットワーク インターフェイスを設定します。クラスタ内の各ブローカノードのテレメトリ ネットワーク インターフェイスには、プライマリ IPv4 または IPv6 の IP アドレス、およびサブネットマスクとゲートウェイがすでに設定されている必要があります。これらは、テレメトリ ネットワーク インターフェイスで設定できます。

IPv4 または IPv6 の VIP IP アドレスは、クラスタ内のプライマリ IP アドレスと同じサブネットに設定する必要があります。これは、VIP も同じサブネットに存在する必要があるためです。これにより、事前設定されたゲートウェイを介した適切なルーティングと高速フェールオーバーが保証されます。

VIP アドレスがテレメトリ ネットワーク インターフェイスのプライマリ IP アドレスと同じサブネットにない場合、またはクラスタ内のテレメトリ ネットワーク インターフェイスが異なるサブネットで設定されている場合は、高可用性が機能しない可能性があります。

クラスタの管理

Cisco Telemetry Broker の実装では、一般的に使用される 2 つの Linux パッケージを使用して、基盤となる高可用性インフラストラクチャを提供します。

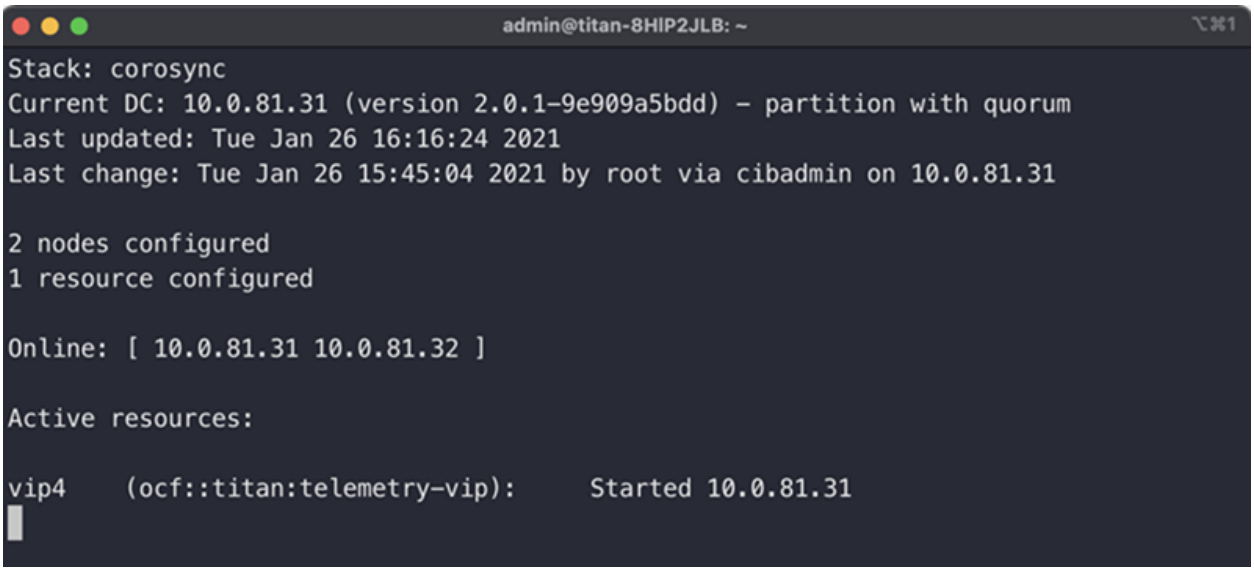
Corosync：これは、クラスタノード間の基盤となる通信を提供する低レベルのクラスタエンジンです。また、各ノードのロール（アクティブまたはスタンバイ）を決定するクォーラム機能も提供します。

Pacemaker：これは、マシンとアプリケーション間のすべての関係を管理するクラスタリソースマネージャです。Corosync を使用して通信します。

現在のクラスタステータスの表示

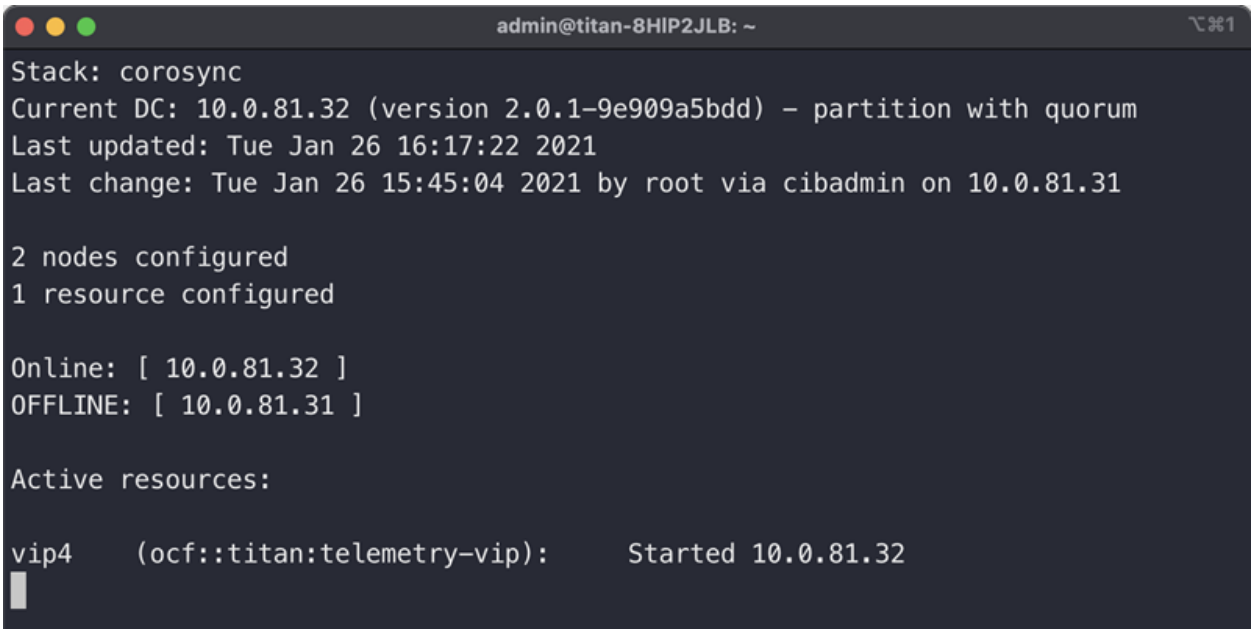
各ノードのステータス（オフラインまたはオンライン）と、IPv4 VIP（vip4）および IPv6 VIP（vip6）IP アドレスの場所を含む、クラスタの現在のステータスを表示するには、次の手順を実行します。

1. コンソールから VMware vCenter によって提供される仮想マシンに、または SSH 経由で、クラスタ内の任意のブローカノードに**管理者**としてログインします。ノードのインストール時に指定したパスワードを使用します。
2. `sudo crm_mon` コマンドを実行します。これにより、クラスタに現在設定されている属性のビューが表示されます。このコマンドの詳細については、こちらを参照してください。
3. **Ctrl+C** を押してツールを終了します。



前の図は、10.0.81.31 と 10.0.81.32 の 2 つのノードのクラスタを示しています。両方のノードのステータスは *Online* です。IPv4 VIP（vip4）は現在 10.0.81.31 で実行されています。IPv6 VIP（vip6）は設定されていないため表示されません。

10.0.81.31 が失敗した場合、そのステータスは次のようになります。

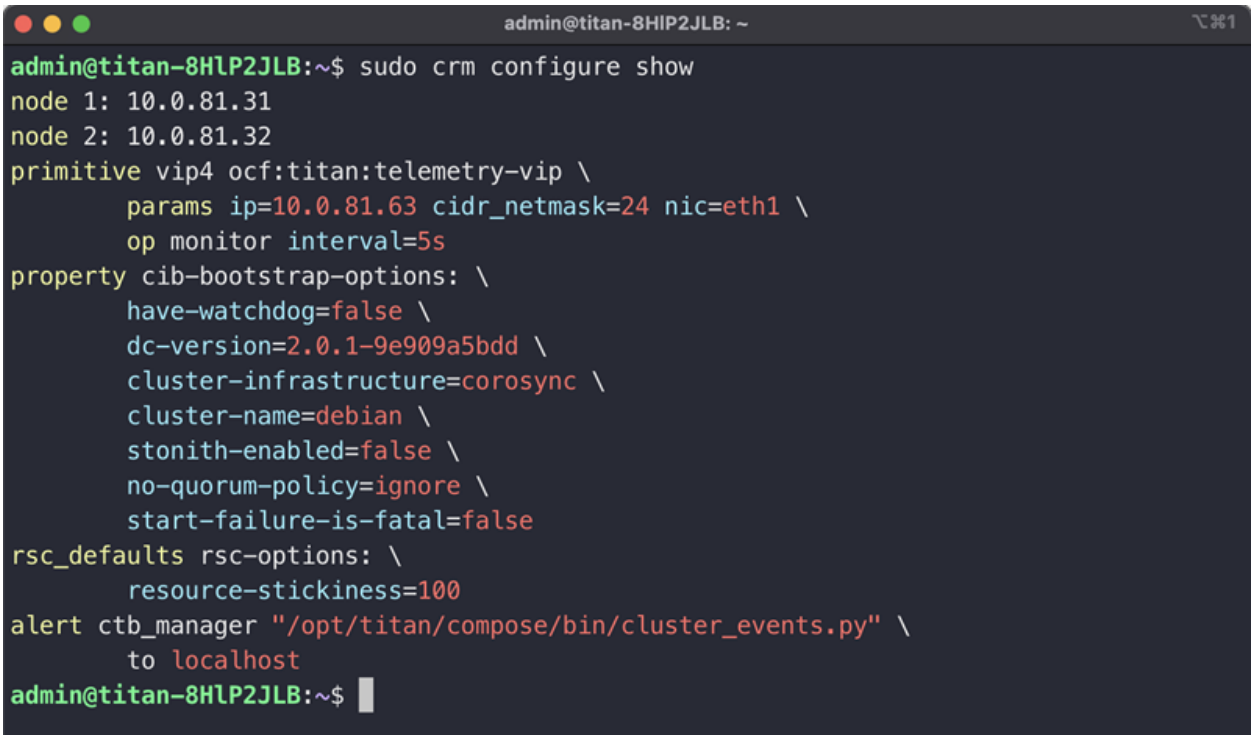


10.0.81.31 が *OFFLINE* と表示され、vip4 が 10.0.81.32 に移動したことに注目してください。

現在のクラスタ設定の表示

クラスタの現在の設定を表示して、Corosync と Pacemaker の設定が正しいことを確認するには、次の手順を実行します。

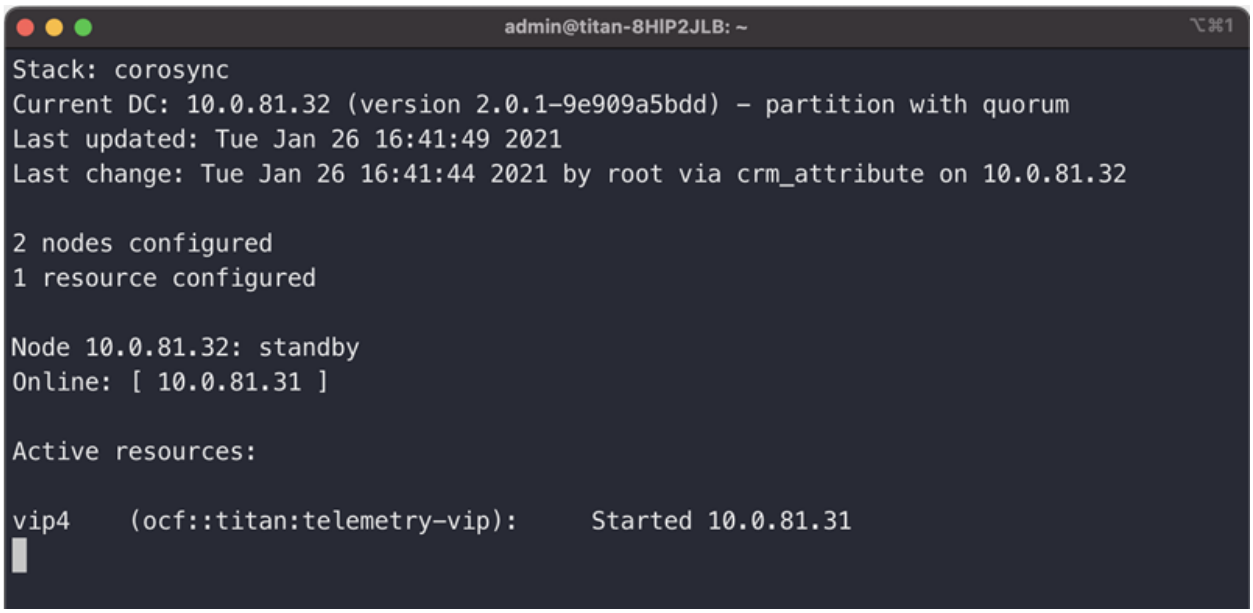
1. コンソールから VMware vCenter によって提供される仮想マシンに、または SSH 経由で、クラスタ内の任意のブローカノードに**管理者**としてログインします。ノードのインストール時に指定したパスワードを使用します。
2. `sudo crm configure show` コマンドを実行します。これにより、クラスタに現在設定されている属性のビューが表示されます。このコマンドの詳細については、こちらを参照してください。



ノードスタンバイモードの有効化と無効化

スタンバイモードでは、ノードは IPv4 または IPv6 仮想 IP アドレスをホストできません。

1. コンソールから VMware vCenter によって提供される仮想マシンに、または SSH 経由で、クラスタ内の任意のブローカノードに**管理者**としてログインします。ノードのインストール時に指定したパスワードを使用します。
2. `sudo crm node standby 10.0.81.32` コマンドを実行します。対象のノードでこのコマンドを実行している場合は、ノード名を省略できます。このコマンドの詳細については、こちらを参照してください。
3. `sudo crm node online 10.0.81.32` コマンドを実行して、ノードのスタンバイステータスを解除します。コマンドの詳細については、こちらを参照してください。



ご覧のように、*crm_mon* は 10.0.81.32 ノードのスタンバイステータスを表示します。

特定のノードへの VIP の移動

IPv4 または IPv6 仮想 IP アドレスを実行しているノードを指定する必要がある場合があります。その場合は次の手順を実行します。

1. コンソールから VMware vCenter によって提供される仮想マシンに、または SSH 経由で、クラスタ内の任意のブローカノードに**管理者**としてログインします。ノードのインストール時に指定したパスワードを使用します。
2. `sudo crm resource move vip4 10.0.81.32` コマンドを実行します。このコマンドの詳細については、こちらを参照してください。
3. `sudo crm resource unmove vip4` コマンドを実行して、VIP がターゲットノードに留まるようにします。そうしないと、VIP は次の機会に以前の（移動前の）ノードに戻ります。

物理 NIC を使用するための仮想マシンの設定

vmxnet3 仮想ドライバを使用して、テレメトリ ネットワーク インターフェイスで ctb-node OVA ファイルを事前設定しました。vmxnet3 ドライバは、最大約 1 Gbps のワークロードまでは正常に動作しますが、約 1 Gbps を超えるワークロードでは遅延し始めます。

フル 10 Gbps テレメトリをサポートするには、物理 NIC を使用するように VM を設定する必要があります。これは、VMware では VMDirectPath I/O パススルーと呼ばれます。VMDirect I / O パススルーのナレッジベースの設定の記事では、物理 NIC をパススルーデバイスとして設定する方法について説明しています。

パススルーデバイスを使用して ESXi サーバーを設定したら、次の手順を実行して ctb-node VM に追加します。

1. OVA ファイルをインポートしたら、VM をシャットダウンします。
2. vSphere Client で、**仮想マシン**を右クリックし、[設定の編集(Edit Settings)] を選択します。
    a. [新規デバイスの追加(Add New Device)] をクリックします。
    b. [PCIデバイス(PCI Device)] を選択します。
    c. 設定した PCI パススルーデバイスを選択します。
    d. VM メモリの設定を更新するには、[すべてのゲストメモリを予約(すべてロック済み)(Reserve all guest memory (All locked))] チェックボックスをオンにします。
    e. [OK] をクリックします。
3. VM を起動し、上記のインストールプロセスを実行します。パスワードを入力すると、3 つの異なる NIC のリストから**管理ネットワーク インターフェイス**と**テレメトリ ネットワーク インターフェイス**を選択するように求められます。
    a. **82574L ギガビットネットワーク接続** NIC を管理ネットワーク インターフェイスとして使用します。
    b. テレメトリ ネットワーク インターフェイスとして**パススルー NIC** を使用します(説明にはおそらく(*10Gbps*)と書かれています)。

これで、仮想マシンがパススルーインターフェイスで実行されます。

Telemetry Broker ライセンスの有効化

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマート ライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

アシスタンス

Cisco スマートアカウントとスマートライセンシングのサポートについては、次のいずれかのリソースを通じてお問い合わせください。

- Support Case Manager（https://mycase.cloudapps.cisco.com/case）に移動し、[ソフトウェアライセンス（Software Licensing）] でケースタイプとして [セキュリティ関連ライセンス（Security Related Licensing）] を選択します。
- TAC ワールドワイドサポート番号（https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html）に連絡し、ライセンス要求を依頼します。

ライセンスの概要

マネージャを導入したら、次の操作を実行します。

1. 最初のスーパーユーザアカウントを作成します。
2. Cisco スマートアカウントを作成します。
3. Telemetry Broker でスマートライセンシングを開きます。
4. 評価モードのステータスを確認します。
5. 製品インスタンスを登録します。

Cisco Telemetry Broker が Cisco スマートアカウントに直接アクセスできず、Smart Software Manager（トランスポートゲートウェイとも呼ばれる）または Smart Software Manager のオンプレミスで通信する場合は、転送設定に [トランスポートゲートウェイ（Transport Gateway）] を選択します。

> Cisco Telemetry Broker には、Smart Software Manager のオンプレミス v8-202010 以降が必要です。

次のオンプレミスガイドを確認して、インストールおよび設定を完了します。

- **スマート ソフトウェア オンプレミス**:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/smart-software-manager-satellite/tsd-products-support-series-home.html

1. 最初のスーパーユーザアカウントの作成

Cisco Telemetry Broker を評価モードで使用すると、90 日間使用できます。評価モードは、Cisco Telemetry Broker のアクティブな使用状況に基づいています。たとえば、Cisco Telemetry Broker をシャットダウンした場合、再度オンになるとカウントダウンが再開されます。

Cisco Telemetry Broker のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマートライセンシングで Smart Software Manager に製品インスタンスを登録します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、Cisco Telemetry Broker は入力からのテレメトリの受信を停止し、宛先へのテレメトリの送信を停止します。機能を再開するには、製品インスタンスを登録します。

1. Web ブラウザで、マネージャの管理インターフェイスの IP アドレスを入力し、**Enter** を押してマネージャの Web インターフェイスのログインに移動します。
2. 姓名、電子メールアドレス、ユーザー名（**admin** ユーザーと混同しないように **webadmin** のユーザー名を割り当てることを推奨します）とパスワードを入力し、[作成（Create）] をクリックして最初のスーパーユーザーアカウントを作成します。

2. Cisco スマートアカウントの作成

Cisco スマートアカウントを使用すると、ソフトウェア、サービス、およびデバイスを 1 つのポータル（Cisco Smart Software Manager とも呼ばれる）で表示できます。

Cisco Telemetry Broker でスマートライセンシングを使用するには、Cisco スマートアカウントが必要です。Cisco スマートアカウントを使用すると、ソフトウェア、サービス、およびデバイスを 1 つのポータル（Cisco Smart Software Manager とも呼ばれる）で表示できます。

Cisco Telemetry Broker のライセンスを取得するには、スマートアカウントを使用して製品インスタンスを登録し、ライセンスを管理し、レポートを実行し、通知を設定します。詳細については、cisco.com のスマートライセンシングを参照してください。

- **チュートリアル**：ビデオチュートリアルについては、「スマートライセンシングのリソース」を参照してください。
- **手順**：Cisco スマートアカウントの使用に関する詳細な手順については、Cisco スマートアカウントにログインしてください。[ヘルプ（Help）] をクリックするか、オンラインアシスタントを使用します。

3. Telemetry Broker でスマート ソフトウェア ライセンシングを開く

1. Cisco Telemetry Broker にログインします。
2. 任意のページの右上隅にあるツールバーで、⚙（[グローバル設定（Global Settings）]）アイコン をクリックし、[設定（Settings）] を選択します。
3. [スマートライセンシング（Smart Licensing）] タブをクリックします。

4. 評価モードのステータスの確認

1. Cisco Telemetry Broker でスマートライセンシングを開きます。
2. 任意のページの右上隅にあるツールバーで、[グローバル設定（Global Settings）] アイコンをクリックし、[設定（Settings）] を選択します。
3. [スマートライセンシング（Smart Licensing）] タブをクリックします。
4. [スマート ソフトウェア ライセンシングのステータス（Smart Software Licensing Status）] セクションで、[登録ステータス（Registration Status）] と [ライセンス認証ステータス（License Authorization Status）] を確認します。

	ステータス	詳細
登録ステータス	未登録（Unregistered）	製品インスタンスが Cisco スマートアカウントに登録されていません。評価期間が満了する前に製品インスタンスを登録します。 評価期間が終了すると、Cisco Telemetry Broker は入力からのテレメトリの受信を停止し、宛先へのテレメトリの送信を停止します。機能を再開するには、製品インスタンスを登録します。
ライセンス認証ステータス	使用中のライセンスはありません（No Licenses in Use）	Cisco Telemetry Broker の導入を開始し、テレメトリの処理を開始した後、Cisco Telemetry Broker が契約適応資格の使用状況を計算して報告するまでに 24 時間かかります。
	評価モード（Evaluation Mode）	製品インスタンスは評価モードを使用しており、残りの日数が表示されます。より詳細な情報を表示するには、ステータスの上にポインタを置きます。

5. 製品インスタンスの登録

Cisco Telemetry Broker でスマートライセンシングを使用するには、Cisco スマートアカウントが必要です。Cisco スマートアカウントを使用すると、ソフトウェア、サービス、およびデバイスを 1 つのポータル（Cisco Smart Software Manager とも呼ばれる）で表示できます。

Cisco Telemetry Broker のライセンスを取得するには、スマートアカウントを使用して製品インスタンスを登録し、ライセンスを管理し、レポートを実行し、通知を設定します。詳細については、cisco.com のスマートライセンシングを参照してください。

- **チュートリアル**：ビデオチュートリアルについては、「スマートライセンシングのリソース」を参照してください。

- **手順**：Cisco スマートアカウントの使用に関する詳細な手順については、Cisco スマートアカウントにログインしてください。[ヘルプ（Help）] をクリックするか、オンラインアシスタントを使用します。

評価期間が終了する前に、以下の手順に次の順序でしたがって製品インスタンスを登録してください。

a. Cisco Smart Software Manager にログインします。
b. 転送設定を構成します。
c. 登録トークンを作成します。
d. Telemetry Broker に登録します。
e. （必要に応じて）製品インスタンスの登録を変更します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、Cisco Telemetry Broker は入力からのテレメトリの受信を停止し、宛先へのテレメトリの送信を停止します。機能を再開するには、製品インスタンスを登録します。

a. Cisco Smart Software Manager へのログイン

Cisco Telemetry Broker のデフォルト機能を最大限に活用して購入ライセンスと機能をアカウントに追加するには、Cisco スマートアカウントにログインし、スマートライセンシングで Smart Software Manager に製品インスタンスを登録します。

1. Cisco Software Central（https://software.cisco.com）に移動します。
2. 👤（[ユーザ（User）]）アイコン をクリックします。
3. CCOID クレデンシャルを使用してログインします。

   - **ログイン**：アカウントを持っている場合は、[ログイン（Log In）] をクリックします。
   - **アカウントの作成**：アカウントがない場合は、[アカウントの作成（Create an Account）] をクリックします。画面に表示される指示に従って、アカウントを設定します。

4. [ライセンス（License）] セクションで、[スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

b. 転送設定の構成

Cisco Telemetry Broker が Cisco スマートアカウント（Cisco Smart Software Manager）と通信する方法を設定します。ここで設定を変更すると、これらの変更は、このサービスを使用する Smart Call Home およびその他の機能に適用されます。

1. Cisco Telemetry Broker にログインします。
2. [スマートライセンシング（Smart Licensing）] タブをクリックします。
3. [シスコ スマート ソフトウェア ライセンシングのステータス（Smart Software Licensing Status）] セクションで、[転送設定（Transport Settings）] を見つけます。
4. [表示/編集（View/Edit）] をクリックします。

> ⚠ 製品インスタンスがすでに登録されている場合は、転送設定を変更する前に登録解除してください。詳細については、「**登録解除**」を参照してください。

5. 転送設定を選択します。

転送設定	説明
直接（Direct）	Cisco Telemetry Broker が Cisco スマートアカウントに直接アクセスでき、ファイアウォールによってブロックされていない場合は、このオプションを使用します。Cisco Telemetry Broker は Cisco Telemetry Broker が直接アクセスを試みる URL をリストします。
トランスポートゲートウェイ（Transport Gateway）	Cisco Telemetry Broker が Cisco スマートアカウントに直接アクセスできず、トランスポートゲートウェイまたは Smart Software Manager のオンプレミスで通信する場合は、[トランスポートゲートウェイ（Transport Gateway）] を選択します。 [URL] フィールドに、製品インスタンスのライセンスを含む Smart Software Manager On-Prem の URL を入力します。 **例：** https://<SSM-ON-PREM-URL>SmartTransport
HTTPS プロキシ（HTTPS Proxy）	このオプションは、プロキシを使用するように Cisco Telemetry Broker を構成した場合にのみ使用できます。その場合は、[HTTPSプロキシ（HTTPS Proxy）] オプションを選択して、Cisco Smart Licensing サーバーとの通信にプロキシを使用するように Cisco Telemetry Broker に指示できます。プロキシを設定するには、次のセクションを参照し、「**c. インターネットプロキシの設定**」で手順を確認してください。

6. [保存（Save）] を選択します。

c. インターネットプロキシの設定

Cisco Telemetry Brokerトランスポート設定で HTTPS プロキシオプションを有効にするには、インターネットプロキシが設定されていることを確認します。

1. Cisco Telemetry Broker にログインします。
2. 任意のページの右上隅にあるツールバーで、[グローバル設定（Global Settings）] アイコンをクリックします。
3. [HTTPSプロキシを使用する（Use HTTPS proxy）] 切り替えアイコンをクリックして、HTTPS プロキシ機能を有効にします（アイコンバーが青色に変わります）。
4. [IP アドレス（IP Address）] フィールドに、プロキシ サーバの IP アドレスを入力します。

5. [ポート(Port)] フィールドに、Cisco Telemetry Broker がプロキシサーバとの通信に使用するポート番号を入力します。
6. [保存(Save)] をクリックします。

d. 登録トークンの作成

1. https://software.cisco.com にある Cisco スマートアカウントにログインします。
2. [ライセンス(License)] セクションで、[スマートソフトウェアライセンシング(Smart Software Licensing)] を選択します。
3. [インベントリ(Iventory)] を選択します。
4. [製品インスタンス登録トークン(Product Instance Registration Tokens)] セクションで、[新規トークン(New Token)] をクリックします。
5. [登録トークンの作成(Create Registration Token)] ダイアログボックスのフィールドに入力して、アカウントのトークンを特定し、使用方法を指定します。
6. [トークンの作成(Create Token)] をクリックします。
7. [製品インスタンス登録トークン(Product Instance Registration Tokens)] リストでトークンを見つけます。
8. **トークンのコピー**:トークン名をクリックしてコピーするか、次のいずれかを選択します。

    - **コピー**:トークンをコピーするには、[アクション(Actions)] > [コピー(copy)] の順にクリックします
    - **ダウンロード**:テキストファイルとしてトークンをダウンロードするには、[アクション(Actions)] > [ダウンロード(Download)] の順にクリックします。

e. Cisco Telemetry Broker への登録

1. Cisco Telemetry Broker でスマートライセンシングを開きます。
2. [登録(Register)] をクリックします。
3. トークンをプレーンテキストとして貼り付けるか、または [製品インスタンス登録トークン(Product Instance Registration Token)] ウィンドウに入力します。
4. [登録(Register)] をクリックします。

> 登録中に通信がタイムアウトした場合は、転送設定を確認します。

5. [スマート ソフトウェア ライセンシングのステータス(Smart Software Licensing Status)] セクションを確認し、次のことを確認します。

    - **登録ステータス**:登録済み
    - **ライセンス認証のステータス**:認証済み
    - **コンプライアンス違反**:ステータスがコンプライアンス違反として表示されている場合は、アカウントにライセンスを追加する必要があります。詳細については、「**ライセンスのトラブルシューティング**」を参照してください。

6. [スマートライセンスの使用状況（Smart License Usage）] セクションを確認します。すべてのライセンスが承認済みとして表示されていることを確認します。
    - **ステータスの詳細**：Cisco Telemetry Broker でスマートライセンシングを開き、スマートライセンスの使用状況を確認して、どのライセンスが準拠していないかを判断します。
    - **コンプライアンス違反**：ライセンスがコンプライアンス違反として表示されている場合は、アカウントにライセンスを追加する必要があります。詳細については、「**ライセンスのトラブルシューティング**」を参照してください。

f.（必要に応じて）製品インスタンスの登録を変更

スマートライセンシングで Smart Software Manager への製品インスタンスの登録を変更または更新するには、次の手順を使用します。

登録解除

Cisco スマートアカウントから製品インスタンスを削除するには、次の手順を使用します。製品インスタンスの登録を解除する場合は、次の点に注意してください。

- **バーチャル アカウント インベントリ**：使用していたライセンスはバーチャルアカウントに返され、アカウント内の他の製品インスタンスはそれらのライセンスを使用できます。
- **評価モード**：評価期間の残り日数がある場合、製品インスタンスは評価モードに戻ります。

転送設定を変更する、またはトラブルシューティングを行う前に、登録解除を使用してください。

1. Cisco Telemetry Broker でスマートライセンシングを開きます。
2. [アクション（Actions）] をクリックします。
3. [登録解除（Deregister）] を選択します。

再登録

製品インスタンスが接続解除されたか、または Cisco Telemetry Broker が再試行後に Cisco スマートアカウントに接続できなかった場合は、ライセンス認証ステータスに [登録期限切れ（Registration Expired）] と表示されます。次の手順を使用して通信の問題を解決し、製品インスタンスを再登録します。

1. Cisco Telemetry Broker でスマートライセンシングを開きます。
2. 転送設定と Cisco スマートアカウントを確認して通信を確認してください。

> ⚠ 転送設定を変更する必要がある場合は、最初に製品インスタンスを登録解除します。

3. [アクション（Actions）] > [再登録（Reregister）] の順にクリックします。
4. https://software.cisco.com にある Cisco スマートアカウントにログインします。
5. [ライセンス（License）] セクションで、[スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。
6. [インベントリ（Iventory）] を選択します。
7. [製品インスタンス登録トークン（Product Instance Registration Tokens）] セクションで、[新しいトークン（New Token）] をクリックするか、または [製品インスタンス登録トークン（Product Instance Registration Tokens）] リストでトークンを見つけます。

8. トークンをコピーして、Cisco Telemetry Broker の [製品インスタンス登録トークン（Product Instance Registration Token）] ウィンドウに貼り付けます。
9. [再登録（Reregister）] をクリックします。
10. スマート ソフトウェア ライセンシングのステータスを確認して確定します。
    - **登録ステータス**：登録済み
    - **ライセンス認証のステータス**：認証済み

ステータスと使用状況の確認

スマートライセンスで Smart Software Manager に製品インスタンスを登録すると、[Cisco Telemetry Brokerスマートライセンシング（Cisco Telemetry Broker Smart Licensing）] ページに Cisco スマートアカウントと製品インスタンスの詳細が表示されます。これには次のものが含まれます。

製品インスタンスの詳細

情報	詳細
登録ステータス	詳細については、「**登録ステータス**」を参照してください。
ライセンス認証ステータス	詳細については、「**ライセンス認証ステータス**」を参照してください。
輸出管理機能	Cisco スマートアカウントのオンラインヘルプを参照してください。
スマート アカウント	Cisco スマートアカウントのオンラインヘルプを参照してください。
バーチャル アカウント	Cisco スマートアカウントのオンラインヘルプを参照してください。
製品インスタンス名	製品インスタンス名は、お客様の Cisco Telemetry Broker の製品インスタンスに使用する識別子であり、Cisco Telemetry Broker マネージャノードとブローカノードが含まれます。製品インスタンス名を使用して、Cisco スマートアカウントの製品インスタンスを特定します。
転送設定	詳細については、「**Telemetry Broker ライセンスの有効化**」の「製品インスタンスの登録」セクションのステップ 2 を参照してください。

登録ステータス

Cisco Telemetry Broker は Cisco スマートアカウントに接続し、ライセンスのステータスと使用状況をレポートします。

1. Telemetry Broker でスマートライセンシングを開きます。
2. [スマート ソフトウェア ライセンシングのステータス（Smart Software Licensing Status）] セクションを確認します。

ステータス	詳細
登録済み（Registered）	製品インスタンスが登録され、ライセンスの使用状況が Cisco スマートアカウントにレポートされます。更新と有効期限の詳細を表示するには、ステータスの上にポインタを置きます。
未登録（Unregistered）	製品インスタンスが Cisco スマートアカウントに登録されていません。評価期間が満了する前に製品インスタンスを登録します。 詳細については、「Telemetry Broker ライセンスの有効化」の「評価モード（90 日間）」および「製品インスタンスの登録」を参照してください。

ライセンス認証ステータス

ステータス	詳細
許可の期限切れ（Authorization Expired）	Cisco Telemetry Broker が Cisco スマートアカウントとの通信を失う場合は、許可が期限切れになっている可能性があります。 [許可の期限切れ（Authorization Expired）] は、通信ステータスを示します。これは、ライセンスステータスを示すものではありません。ライセンスステータス（購入済み、期限切れ、使用状況）を確認するには、「Cisco スマートアカウント」を確認します。
承認済み（Authorized）	製品インスタンスが登録されており、ライセンスが承認されます。 承認の試みと詳細を表示するには、ステータスの上にポインタを置きます。
評価期間が期限切れ（Evaluation Period Expired）	評価期間が終了し、テレメトリの処理が停止しました。より詳細な情報を表示するには、ステータスの上にポインタを置きます。 詳細については、「Telemetry Broker ライセンスの有効化」の「評価モード（90 日間）」および「製品インスタンスの登録」を参照してください。
評価モード（Evaluation Mode）	製品インスタンスは評価モードを使用しており、残りの日数が表示されます。より詳細な情報を表示するには、ステータスの上にポインタを置きます。 詳細については、「Telemetry Broker ライセンスの有効化」の「評価モード（90 日間）」および「製品インスタンスの登録」セクションを参照してください。
コンプライアンス違反（Out of Compliance）	Cisco Telemetry Broker に対してライセンスが不足している場合は、コンプライアンス違反になります。 詳細については、「ライセンスのトラブルシューティング」の「コンプライアンス違反の解決」を参照してください。

スマート ライセンスの使用状況の確認

Cisco Telemetry Broker は、ライセンスの使用状況を Cisco スマートアカウントにレポートします。

スマートライセンスのステータスがコンプライアンス違反を示している場合は、Cisco Telemetry Broker のライセンスが不足していて、Cisco スマートアカウントに割り当てられているよりも多くのライセンスを使用していることを示します。詳細については、「**ライセンスのトラブルシューティング**」の「コンプライアンス違反の解決」のセクションを参照してください。

ライセンスのトラブルシューティング

[スマートライセンシング（Smart Licensing）] に示されているライセンス関連のエラーを解決するには、次の手順を使用します。

コンプライアンス違反の解決

ライセンス認証ステータスまたはスマートライセンスの使用がコンプライアンス違反を示している場合、アプライアンスまたは機能のライセンスが不足していて、Cisco スマートアカウントに割り当てられているよりも多くのライセンスを使用しています。

ライセンスの確認

次のことを確認します。

- Cisco Telemetry Broker でスマートライセンシングを開き、スマートライセンスの使用状況を確認して、どのライセンスが準拠していないかを判断します。
- バーチャルアカウントに十分なライセンスが割り当てられていることを確認してください。詳細については、「Cisco スマートアカウント」を参照してください。
- 追加のライセンスを購入する必要がある場合は、アカウントマネージャに問い合わせるか、stealthwatch-sales@cisco.com で Cisco Telemetry Broker 販売チームにご連絡ください。

Cisco Telemetry Broker の更新

バーチャルアカウントにライセンスを追加または移動した後、次の手順を使用して Telemetry Broker のステータスを更新します。

認証を今すぐ更新

Cisco Telemetry Broker は、ライセンスの使用状況を Cisco スマートアカウントにレポートします。[認証を今すぐ更新（Renew Authorization Now）] を使用してアカウントに接続し、ライセンスの使用状況のテレメトリをただちに更新します。Cisco スマートアカウントのライセンスを変更したにもかかわらず、[スマートライセンシング（Smart Licensing）] ページに表示されない場合は、次の手順を使用します。

1. Cisco Telemetry Broker でスマートライセンシングを開きます。
2. [アクション（Actions）] > [認証を今すぐ更新（Renew Authorization Now）] の順にクリックします。

登録を今すぐ更新

製品インスタンスが接続解除されたか、または Cisco Telemetry Broker が再試行後に Cisco スマートアカウントに接続できなかった場合は、ライセンス認証ステータスに［登録期限切れ（Registration Expired）］と表示されます。アカウントに接続して登録ステータスを更新するには、［登録を今すぐ更新（Renew Registration Now）］を使用します。

1. ［アクション（Actions）］メニューを選択します。
2. ［登録を今すぐ更新（Renew Registration Now）］を選択します。

登録の有効期限切れ：ライセンス認証ステータスが引き続き［登録の有効期限切れ（Registration Expired）］と表示される場合は、製品インスタンスを再登録する必要がある場合があります。詳細については、「**Telemetry Broker ライセンスの有効化**」の「登録」を参照してください。

ライセンスの有効期限のステータスの確認

購入したライセンス、割り当て、有効期限のステータス、および使用状況が Cisco スマートアカウントに表示されます。詳細については、「**Telemetry Broker ライセンスの有効化**」の「Cisco スマートアカウント」を参照してください。

Cisco Telemetry Broker のトラブルシューティング

一般：アプライアンスは標準の Debian 10 オペレーティングシステムを実行しているため、ほとんどの一般的な Linux システム管理のプラクティスをトラブルシューティングに適用できます。

管理ネットワーキング：アプライアンスの管理ネットワーク インターフェイスは、使い慣れた ifup、ifdown、または ifconfig ツールではなく、systemd-networkd サービスによって管理されます。Cisco Telemetry Broker のインストールが完了したら、次のファイルで設定情報を確認できます。

/etc/systemd/network/management.network

テレメトリネットワーキング：マネージャノードは、アプライアンスのテレメトリ ネットワーク インターフェイスを管理します。インストール後、テレメトリ ネットワーク インターフェイスはほとんどオペレーティングシステムに表示されません。したがって、Cisco Telemetry Broker 管理レイヤを使用して設定を行う必要があります。

テレメトリ パケット キャプチャ：設定と同様に、オペレーティング システム ユーティリティの代わりに、カスタム Cisco Telemetry Broker ツールを使用してテレメトリ ネットワーク インターフェイスでパケットをキャプチャします。これを行うには、アプライアンスに SSH で接続し、次のコマンドを実行します。

```
$ sudo ctb-pcap -V -n 1000 -t 15 -s 10.203.3.3 -o test_tx_src.pcap
rx
```

このコマンドは、キャプチャされた出力を /var/lib/titan/pcap/test_tx_src.pcap に書き込みます。使用可能なすべてのオプションを表示するには、**–help** オプションを使用します。

診断：アプライアンスには、Cisco Telemetry Broker エンジニアリングチームのデバッグ情報をキャプチャできる *Mayday* という名前の診断ツールが含まれています。この役立つ情報をバグレポートに含める必要があります。

Mayday で診断パックを作成するには、アプライアンスに SSH で接続し、次のコマンドを実行します。

```
sudo mayday
```

これにより、関連するシステム情報が tar ball にコンパイルされ、SCP ツールを使用してノードから別の場所にコピーできるようになります。結果の tar ball の場所は、Mayday ログに含まれます。

例：

```
$ ssh admin@<ctb-node-ip>

ctb-node> sudo mayday

<output-redacted>

2020/08/05 19:04:45 Output saved in /tmp/mayday-ctb-5SWVTpSx-
202008051904.677025165.tar.gz

2020/08/05 19:04:45 All done!
```

システムの設定の完了

システムの設定を完了するには、「Cisco Telemetry Brokerユーザーガイド」の次のセクションを参照してください。

- [宛先（Destinations）]
- 入力
- ブローカーノード

サポートに連絡

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りの Cisco Telemetry Broker パートナーにご連絡ください。
- Cisco Telemetry Broker サポートにご連絡ください。
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリックドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

このドキュメントのすべての印刷版と複製ソフトは管理対象外と見なされます。最新版については、現在のオンライン バージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。住所と電話番号は、シスコの Web サイト（https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html）に記載されています。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。（1721R）