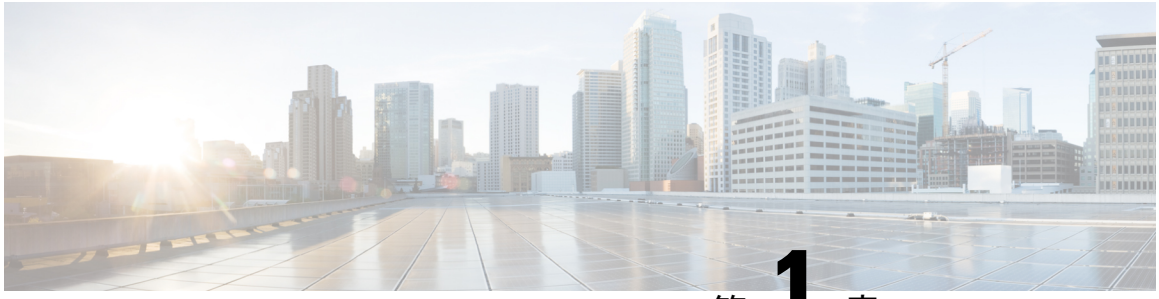
Cisco Application サービス エンジン 入門ガイド、リリース 1.1.3

初版：2020 年 5 月 6 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2020 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

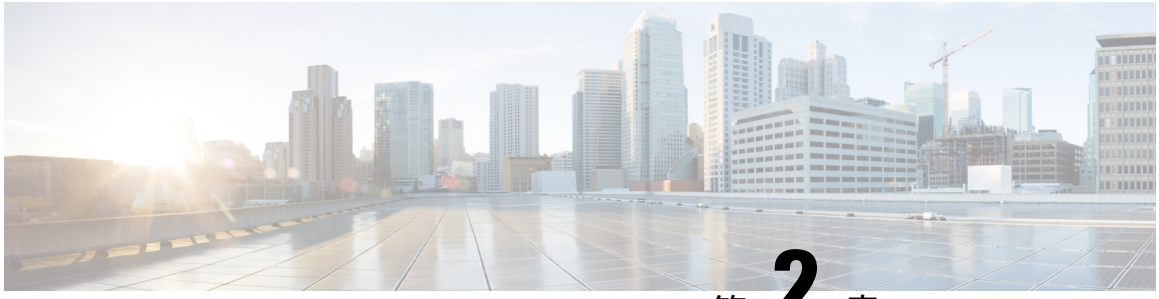
新機能および変更された機能に関する情報

この章では、Cisco Application サービス エンジン、リリース 1.1.3 の新機能および変更された機能に関するリリース固有の情報を示します。

表 *1 : Cisco Application* サービス エンジン リリース *1.1.3* の新機能と動作変更

機能	説明	リリース	参照先
『Cisco Application サービス エンジン Getting Started Guide』	このガイドは最初に発行されました。	1.1.3	

新機能および変更された機能に関する情報



第 2 章

概要

この章は、次の項で構成されています。

Cisco Application サービス エンジン の概要

Cisco Application サービス エンジン は、シスコ データ センター アプリケーションを展開するための共通プラットフォームを提供します。これらのアプリケーションは、ポリシーとインフラストラクチャのリアルタイム分析、可視性、および保証を提供します。

Cisco Data Centerアプリケーションは、最新のテクノロジー スタックに依存するリソース集約型アプリケーションです。Cisco Application サービス エンジン は、共通のプラットフォームでコンテナ化されたアプリケーションをホストできます。

Cisco Application サービス エンジン は、3つのサービス ノードのクラスタとして展開されます。このクラスタリングは、信頼性と高可用性のソフトウェア フレームワークを提供します。

Cisco Application サービス エンジン はファブリック外部モードで展開されます。このモードでは、Cisco ACI ファブリックは Cisco APIC GUI から Cisco Application サービス エンジン クラスタの設定とモニタリングを提供しません。Cisco Application サービス エンジン は、ファブリックエクスターナルモードでは、次のようなさまざまなフォームファクタを使用して導入できます。

- **物理的なアプライアンス フォーム ファクタ:**
  - ISO フォーム ファクタ。

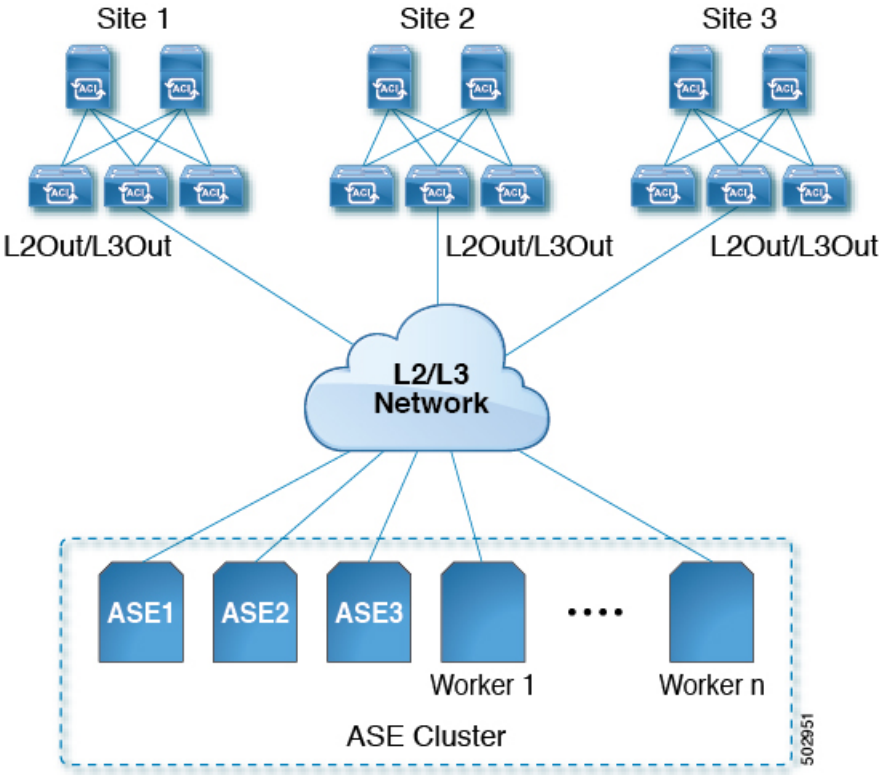
  仮想フォーム ファクタ。
  - AWS-AMIフォームファクタ。
  - OVA フォーム ファクタ。
  - KVM フォーム ファクタ。

（注） Cisco Application サービス エンジン リリース 1.1.3 以降、ファブリック内部モードはサポートされていません。ファブリック内部モードからファブリック外部モードに移行するには、「Fabric Internal Mode（リリース 1.1.2）から Fabric External Mode（リリース 1.1.3）への移行」を参照してください。

（注） Cisco Multisite Orchestrator、Cisco Network Insights Resources アプリケーション、および Cisco Network Insights Advisor アプリケーションがサポートされています。

アーキテクチャ

図 *1 : Cisco Application* サービス エンジン のアーキテクチャ



サービス ノード: サービス ノードは、ネットワークに接続され、Cisco ACI ファブリックを介して情報を作成、受信、または送信できるアプライアンスまたはシステムです。これらはマスター ノードとも呼ばれ、クラスタの状態を管理します。

クラスタ: クラスタは、3 つの接続されたサービス ノードのセットです。アプリのライフ サイクル管理をサポートします。

- 既存のアプリからのサービスを中断することなく、新しいサービス ノードを動的に追加できます。
- サービス ノードは、グレースフル メンテナンスのためにアウトオブサービスにすることができます。サービスを中断することなく、他のノードでアプリを再プロビジョニングできます。

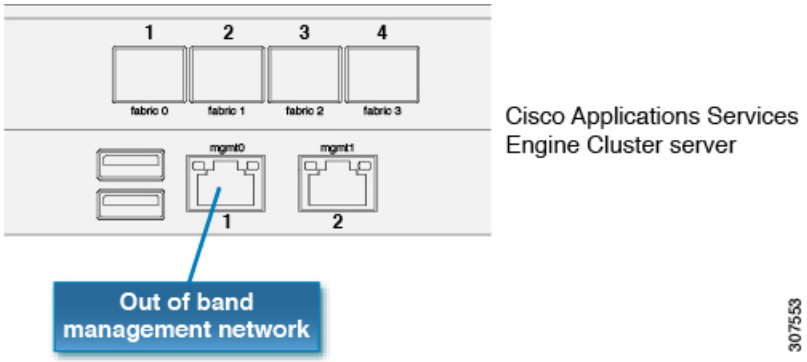
ワーカー ノード: ワーカー ノードは、マスター ノードによって決定されたアプリケーション ワークロードを実行する追加のサービス ノードです。最大 4 つのワーカー ノードを既存のクラスタに追加できます。

管理とネットワークの接続

Cisco Application サービス エンジン は、各サービスノードを 2 つのネットワークに接続するクラスタとして展開されます。

1. 管理インターフェイスを使用した管理ネットワーク。(mgmt0, mgmt1)
2. ファブリック インターフェイスを使用するデータ ネットワーク。(fabric0, fabric1)

図 *2 : Cisco Application Services Engine* のネットワーク接続



管理ネットワーク

- Cisco Application サービス エンジン GUI へのアクセス
- SSH を介した CLI へのアクセス。
- DNS と NTP。
- ファームウェアのアップロード。
- Intersight デバイス コネクタ。

データ ネットワークは次の目的で使用されます。

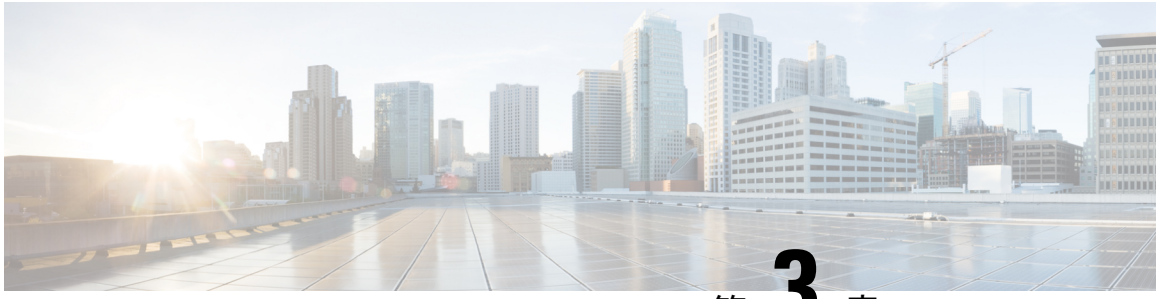
- Cisco Application サービス エンジン クラスタリング。
- アプリ間通信。

- Cisco ACI ファブリックの管理ネットワークにアクセスします。
- ACI ファブリック通信に対するすべてのアプリケーション。

管理とデータ ネットワークは同じサブネットまたは異なるサブネット上に存在することができます。各サービス ノードは、Cisco Application サービス エンジン データ ネットワーク上のすべての Cisco ACI ファブリックに IP で到達可能である必要があります。

Cisco Application サービス エンジン クラスタリングは次の TCP ポートを使用します。これらの TCP ポートはデータ ネットワーク上で許可されます。

- DNS 53
- HTTPS 443
- SSH 22、1022
- NIA 2022、8884
- NIR 5640～5656
- KMS。3379、3380、9969、9979、9989、15223
- Confd 19999
- SEインフラ サービス: 30000～30100
- Kuberentes ノード ポート: 30500～30600



第 3 章

Cisco Application Services Engine の展開

物理アプライアンス（ISO）でのCiscoApplicationServices Engine の展開

前提条件

- サービス ノード データ ネットワーク IP 接続の EPG / L3out を事前に設定する必要があります。
- Cisco ACI インバンド EPG からのネットワーク IP 接続を事前に設定する必要があります。
- サービス ノードからデータ ネットワーク上のリーフおよびスパインへの IP 接続を設定する必要があります（これは Cisco NIR および Cisco NIA にのみ適用されます）。
- 推奨されるデータ ネットワーク接続オプション: Cisco Application Services Engine は、最初の 2 つのファブリック ポートでアクティブ/バックアップ ボンディングを使用します。信頼性のために両方のリンクを接続します。これらのポートは、Cisco ACI ファブリックリーフノードに直接接続することも、外部のレイヤ 2 またはレイヤ 3 ネットワークに接続することもできます。

直接接続:

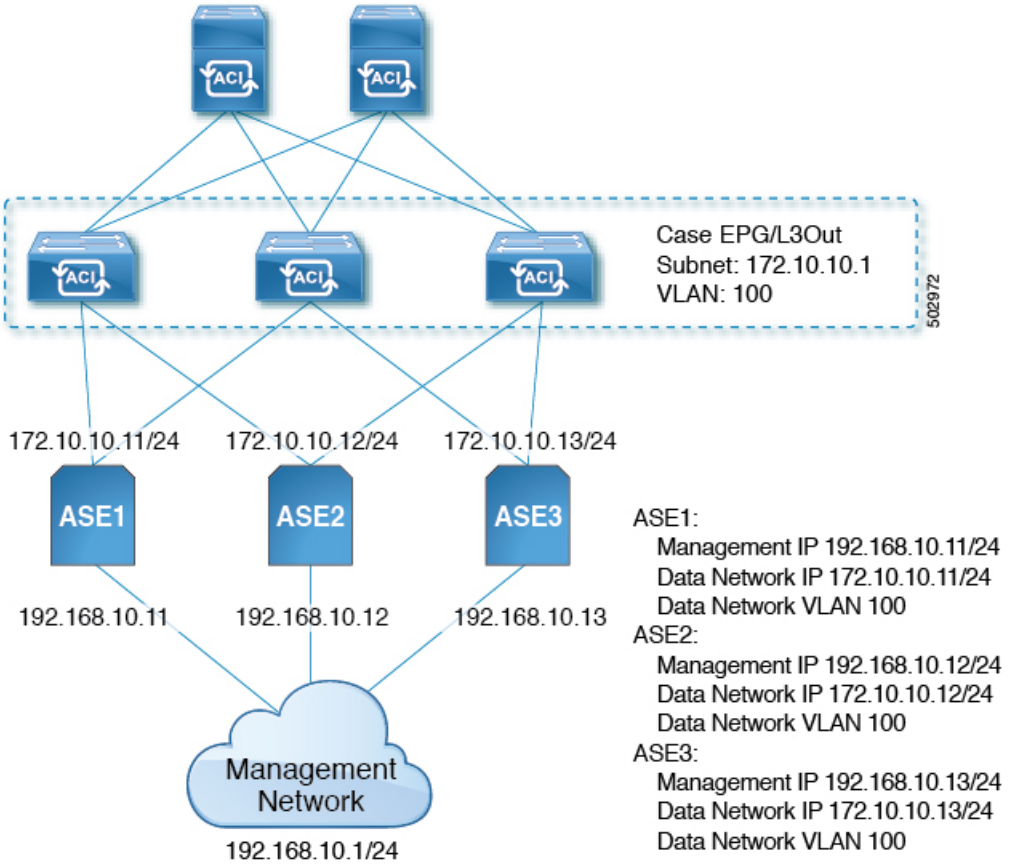
Cisco ACI ファブリックで Cisco Application Services Engine 接続ポートの EPG を設定し、Cisco Application Services Engine EPG とファブリック インバンド ネットワーク EPG 間のコントラクトを作成します。

レイヤ 2 またはレイヤ 3 ネットワークを使用して接続済み:

L2Out または L3out を設定し、Cisco APIC インバンド ネットワーク EPG へのコントラクトを作成します。

Cisco Application Services Engine の展開

Cisco Application Services Engine クラスタのファブリック外部モードを設定するには、次の手順を使用します。



ステップ 1 CIMC 管理 IP を使用して Cisco Application Services Engine コンソールに接続します。

ステップ 2 Application Services Engine-sn セットアップ ユーティリティを開始します。

a) サービス ノードのクラスタ名を入力します。

b) ノードを指定します。ノードがマスターノードであることを指定するには、**y** を入力します。

c) コンフィギュレーション モードを指定します。コンフィギュレーションをピアから取得しないことを指定するには、**n** を入力します。

d) サービス ノードのノード名を入力します。

e) 管理者またはユーザーのパスワードを入力します。

f) パスワードを再入力します。

```
Setup utility for Application Services Engine with SerialNumber WZP23050V5E and running version
1.1.2.168
```

```
Use ^D anytime to start over
Cluster Name: dev-infra12
Master Node? (Y/n): y
Download Config From Peers? (Y/n): n
Node Name: dev-infra12-sn1
Admin Password:
Reenter Password:
```

（注） ワーカーノードを登録するには、**Master Node? (y/n)** プロンプトで「n」を選択します。

```
Master Node? (y/n): n
```

ステップ 3 [データ ネットワークの詳細（Data Nework details）] に入力します。

a) ネットワーク IP アドレスおよびマスクを入力します。

データ ネットワーク IP は、SE クラスタリングおよび Cisco ACI ファブリックへのアクセスに使用されます。

```
IP Address/Mask: 192.168.3.2/24
```

b) ゲートウェイの IP アドレスを入力します。

```
gateway IP address: 192.168.3.1
```

c) サービスノードの VLAN ID を入力します。

VLAN はデータ ネットワークで使用されます。オプションで、VLAN がない場合は空の文字列を入力します。

```
Vlan ID: 100
```

ステップ 4 管理ネットワークの詳細を入力します。

a) 管理ネットワーク IP アドレスおよびマスクを入力します。

```
IP Address/Mask: 172.20.7.125/23
```

b) ゲートウェイの IP アドレスを入力します。

```
gateway IP address: 172.20.6.1
```

ステップ 5 クラスタの他のマスター ノード（マスター ピア）のマスターリスト データ ネットワーク IP アドレスとシリアル番号を入力します。

```
Master List(Space Separated IP,Serialnumber List):192.168.100.2,WZP23380BAT 192.168.100.3,WZP23391QHP
```

ステップ 6 DNS の詳細を入力します。

a) DNS 名プロバイダーの IP アドレスを入力します。

```
Providers(Space Separated IP List):171.70.168.183
```

b) 検索ドメインを入力します。

```
Search Domains(Space Separated List):cisco.com
```

ステップ 7 NTP サーバの IP アドレスを入力します。クラスタ内のすべてのマスター ノード間でクロックを同期する必要があります。

```
NTP Servers (Space Separated IP List): 171.68.38.65
```

ステップ 8 サービス サブネット アドレスとマスクを入力します。

これは、プライベート IP アドレス ブロック、kubernetes、サービスIPなどに使用される /16 ネットワークです。

```
Service Subnet (100.80.0.0/16):
```

ステップ 9 アプリケーション サブネット アドレスとマスクを入力します。

```
App Subnet (172.17.0.1/16):
```

ステップ 10 コンフィギュレーションを見直します。

```
Please review the config:
App Subnet: 1.1.0.0/16
Cluster Name: dev-infra12
Cluster Size: 3
DNS:
  Domain Name: dev-infra12.case.local
  Providers:
  - 171.70.168.183
  Search Domains:
  - atomix.local
Download Config: false
Data Network:
  Gateway: 192.10.10.1
  IP Address/Mask: 192.10.10.2/24
  Vlan ID: 1001
Management Network:
  Gateway: 172.20.6.1
  IP Address/Mask: 172.20.6.147/23
Master List:
- ipAddress: 192.10.12.2
  name: WZP23050V5N
  serialNumber: WZP23050V5N
- ipAddress: 192.10.13.2
  name: WZP23050V68
  serialNumber: WZP23050V68
NTP Servers:
- 171.68.38.65
Node Name: dev-infra12-sn1
Node Role: Master
Node Type: Physical
Password: <hidden>
Service Subnet: 1.2.0.0/16

Re-enter config?(y/N)n

Login with rescue-user & issue acidiag health to check cluster status

CentOS Linux 7 (Core)
Kernel 4.14.174stock-1 on an x86_64
```

ステップ 11 他の 2 つのサービス ノードで手順 1〜11 を実行します。

ノード 2 とノード 3 では、クラスタ内の他のマスターノードの管理IPアドレスとシリアル番号が異なります。

ステップ 12 3 つすべてのサービス ノードがブート ストラップが実行されたら、15〜30 分待ってから次のコマンドを実行します。

```
Server # acidiag health
All components are healthy
```

インストールが正常に実行されたことを示す「正常」ステータスが表示されることを確認します。

（注） リリース1.1.3以降、Cisco Application Services Engine クラスタが機能するには、少なくとも 2 つのマスター ノードが必要です。

ステップ 13 Cisco Application Services Engine は、Cisco Application Services Engine でホストできるアプリケーションの展開に使用できます。

VMware vCenter（OVA）での Cisco Application Services Engine の展開

前提条件

開始する前に、次の 1 回限りの前提条件を完了します。

- NTP サーバが設定され、オーケストレータ VM から到達可能であり、VMware ツールの定期的な時刻同期が無効になっていることを確認します。
- 各 VM サービス ノードに必要なシステム要件があることを確認します。
  - vCPU：16
  - RAM：48GB
  - ディスク領域：25 GB
  - ESX バージョン 5.5 以降
- アウトオブバンド用とファブリック インターフェイス用の 2 つの IP アドレスが必要です（Cisco Application サービス エンジン インバンドは Cisco ACI インバンド IP アドレスとは異なる必要があります）。
- ESXi は、トランク ポート経由でファブリックに接続する必要があります。
- 管理テナントの Cisco Application サービス エンジン 接続用にブリッジドメイン（BD）、サブネット、およびエンドポイントグループ（EPG）を設定します。
- ファブリック インバンド管理 EPG と Cisco Application サービス エンジン EPG 間のコントラクトを作成します。
- Cisco Application Services Engine インバンドIP接続用の EPG/L3Out を事前に設定する必要があります。

（注） EPG/L3Out の設定については、「Cisco APIC Layer 3 ネットワーク設定ガイド」を参照してください。

VMware vCenter（OVA）での Cisco Application Services Engine の展開

ここでは、VMware vCenter で OVA を使用して Cisco Application Services Engine を展開する方法について説明します。

ステップ 1 Cisco Application Services Engine イメージをダウンロードします。

a) [ソフトウェア ダウンロード（Software Download）] ページに移動します。

b) Cisco Application Services Engine OVA イメージ（case-1.1.3a.ova）を選択します。

ステップ 2 VMware vCenter GUI または VMware vSphere Client を使用して OVA を展開します。

a) ホストを右クリックして **[OVF テンプレートの展開 (Deploy OVF Template)]** を選択します。

b) [Deploy OVF Template] ウィザードが表示されます。

ステップ 3 **[OVF テンプレートの選択（Select an OVF Template）]** ページで、送信元の場所を指定し、**[次へ（Next）]** をクリックします。

a) **[ローカル ファイル（local file）]** タブを選択します。

b) **[ファイルの選択（Choose file）]** をクリックし、ステップ 1 でダウンロードしたOVAファイルを選択します。必要なファイルを選択しない場合は、警告メッセージが表示されます。

ステップ 4 Cisco Application Services Engine では、3 つのノードを展開してクラスタを形成する必要があります。**[名前とフォルダの選択（Select a name and folder）]** ページで、最初のノードの一意の名前を入力します。展開場所を選択して、**[次へ（Next）]** をクリックします。

ステップ 5 **[コンピューティング リソースの選択（Select a compute resource）]** ページで、展開された VM テンプレートを実行するリソースを選択し、**[次へ（Next）]** をクリックします。

ステップ 6 **[詳細の確認 (Review details)]** ページで OVF または OVA テンプレートの詳細を確認し、**[次へ (Next)]** をクリックします。

ステップ 7 **[ストレージの選択（Select storage）]** ページで、展開された OVF または OVA テンプレートのファイルを保存する場所と方法を定義します。

a) 仮想マシンの仮想ディスクにディスク形式を選択します。**[シック プロビジョニング（Lazy Zeroed）]** を選択します。

b) OVA を展開するのに十分な容量があるローカル データストアを選択します。

コンフィギュレーション ファイルおよび仮想ディスク ファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスク ファイルを保存できる十分なサイズのデータストアを選択してください。

（注） 各ノードに一意のデータストアを割り当てる必要があります。

ステップ 8 **[ネットワークの選択（Select networks）]** ページで、ソース ネットワークを選択し、それを宛先ネットワークにマップして **[次へ（Next）]** をクリックします。

データネットワーク用の **fabric0** と管理ネットワーク用の **mgmt0** の2つのネットワークがあります。すべてのネットワーク通信は、このポータルを介して行われます。

ステップ 9 **[テンプレートのカスタマイズ（Customize Template）]**ページで、OVA プロパティを設定します。

[ノード設定（Node Configuration）] ダイアログボックスで、各ノードの適切な情報を入力します。

1. **[ノード名（Node Name）]** フィールドに、ノード プール名を入力します。

   `Node1`

2. **[パスワード (Password)]** フィールドに、パスワードを入力します。確認のためにパスワードを再入力します。

3. **[マスター ノード（Master Node）]** フィールド。設定する最初のノードである場合は、[最初のマスター（First Master）] チェックボックスをオンにします。

[ネットワーク設定（Network Configuration）] ダイアログボックスで、各ノードの適切な情報を入力します。

1. **[管理アドレスとサブネット（Management Address and Subnet）]**（ネットワーク アドレス）フィールドに、管理ネットワークアドレスを入力し、IPアドレスとサブネットを入力します。

   （注） 管理 IP アドレスをデータネットワーク IP アドレスと同じにすることはできません。

   `10.197.145.244/24`

   （注） このフィールドは、インストール前に検証されません。このフィールドに無効な値を指定すると、展開が失敗します。

2. **[管理ゲートウェイ IP（Management Gateway IP）]**（ネットワーク ゲートウェイ）フィールドに、管理ネットワーク ゲートウェイの IP アドレスを入力します。

   `10.197.145.1`

3. **[データ ネットワーク アドレスとサブネット（Data Network Address and Subnet）]** フィールドに、データ ネットワーク アドレスと IP/サブネットを入力します。

   `2.2.0.0/16`

   アプリケーションオーバーレイとサービスネットワークは `/16` ネットワークである必要があります。両方のネットワークが管理ネットワークまたは外部ネットワークとオーバーラップしてはなりません。

   （注） このフィールドは、インストール前に検証されません。このフィールドに無効な値を指定すると、展開が失敗します。

4. **[データ ネットワーク ゲートウェイ IP（Data Network Gateway IP）]** フィールドに、データ ネットワーク ゲートウェイの IP アドレスを入力します。IP のみを入力します。

   `1.1.0.0`

5. **[データ ネットワーク VLAN（Data Network VLAN）]** フィールドに、データネットワークVLAN ID を入力します。

   `10.197.145.2`

[必須クラスタ設定（Cluster Configuration Mandatory）] ダイアログボックスで、各ノードに適切な情報を入力します。

1. **[クラスタ名（Cluster Name）]** フィールドに、クラスタの名前を入力します。

   `se-ova`

2. **[マスターリスト（Master List）]** フィールドに、クラスタ内のピア ノードの IP アドレスのリストをスペースで区切って入力します。

   `10.197.145.245 10.197.145.246`

3. **[クラスタのマスター ノードから最新の dgbtokenを入力する（Enter the latest dgbtoken from the master node in the cluster）]** フィールドに、マスターノードの長さ 11 文字以上の任意の文字列を入力します。ピアノードの場合は、マスターノードから最新の dgb トークンを入力します。

   （注） 3 つすべてのノードをマスターノードとして設定します。

   `aaabbbcccdd`

4. **[ピアから設定をダウンロード（Download Config From Peers）]** で、設定する最初のノードである場合は、このチェックボックスを**オンにしません**。

   （注） このボックスをオンにすると、**[任意クラスタ設定（Cluster Configuration Optional）]** の情報が他のノードからダウンロードされます。他のノードから同期されるため、**[任意クラスタ設定（Cluster Configuration Optional）]** フィールドの設定をスキップします。ボックスがチェックされていない場合、**[任意クラスタ設定（Cluster Configuration Optional）]** フィールドが使用されます。

[任意クラスタ設定（Cluster Configuration Optional）] ダイアログボックスで、各ノードの適切な情報を入力します。

1. **[アプリ サブネット（App Subnet）]** フィールドに、Docker 内部ブリッジ ネットワークに使用するアプリケーション IP/サブネットを入力します。

   `172.17.0.1/16`

2. **[サービス サブネット（Service Subnet）]** フィールドに、IP/サブネットを入力します。

   `1.0.0.0`

3. **[NTP-servers]** フィールドに、スペースで区切られたネットワーク タイム プロトコル サーバを入力します。

   `10.197.145.2 10.197.146.2`

4. **[ネーム サーバ IP（Name Server IP）]** リストで、ネーム サーバの IP アドレスを入力します。

   `10.197.145.3`

5. **[ドメインの検索（Search Domains）]** フィールドに、デバイスの検索ドメインのカンマ区切りのリストを入力します。

```
cisco.com
```

ステップ 10 クラスタ内の 2 番目と 3 番目のノードも同様に設定する必要があります。

ステップ 11 **[終了準備の完了（Ready to Complete）]** ページで設定を確認し、**[完了（Finish）]** をクリックします。

ステップ 12 すべての VM を再起動してクラスタを形成します。

ステップ 13 3 つすべてのノードがブートストラップされたら、15〜30 分待ってから SSH にログインし、次のコマンドを実行します。

```
Server # acidiag health
cluster is healthy
```

インストールが正常に実行されたことを示す「正常」ステータスが表示されることを確認します。

ステップ 14 Cisco Application Services Engine は、Cisco Application Services Engine でホストできるアプリケーションの展開に使用できます。

AWS での Cisco Application Services Engine の展開

前提条件

開始する前に、次の 1 回限りの前提条件を完了します。

1. VPC（仮想プライベート クラウド）を作成します。

   VPC は、Amazon EC2インスタンスなどの AWS オブジェクトによって入力される AWS クラウドの分離された部分です。

   - **[ネットワークとコンテンツ配信ツール（Networking＆Content Delivery Tools）]** の **[VPC]** を選択します。
   - **[VPC]** をクリックします。**[VPCの作成（Create VPC）]** > **[作成（Create）]** をクリックします。
   - **[名前タグ（Tag Name）]** に入力します。これにより、「Name」のキーと指定した値を持つタグが作成されます。
   - **IPv4 CIDR ブロック**をブロック形式で入力します。CIDR ブロック形式の VPC の IPv4 アドレスの範囲です。ブロック サイズは、/16 ネットマスクと /28 ネットマスクの間である必要があります。たとえば、「10.0.0.0/24」と入力します。

2. **インターネット ゲートウェイ**を作成します。インターネット ゲートウェイは、VPC がインターネットに接続できるようにする仮想ルータです。

   - [**VPC** ダッシュボード（VPC Dashboard）] > **[インターネット ゲートウェイ（Internet Gateway）]**を選択します。**[インターネット ゲートウェイの作成（Create Internet Gateway）]** > **[作成（Create）]** をクリックします。

- **[名前タグ（Tag Name）]** に入力します。新しいインターネット ゲートウェイを作成するには、ゲートウェイの名前を指定します。これにより、「Name」のキーで指定された値を持つタグが作成されます。
- [Actions] をクリックします。前の手順で作成した**名前タグ**を選択します。ドロップダウン メニューから **[VPCにアタッチ（attach to VPC）]** を選択します。ステップ 1 で作成したVPCを選択して、インターネット ゲートウェイを作成します。

3. **ルート テーブル**を作成します。VPC、インターネット、およびインターネット ゲートウェイ内のサブネットを Cisco Application Services Engine に接続するためのルート テーブルを作成します。
   - [**VPC** ダッシュボード（VPC Dashboard）] > **[ルートテーブル（Route Tables）]** をクリックします。ステップ 1 で VPC 用に作成済みのルート テーブルを選択します。
   - **[ルート（Routes）]** > **[ルートの編集（Edit routes）]** をクリックします。
   - **[ルートを追加（Add Route）]** をクリックします。**[宛先（Destination）]** フィールドに外部サブネットを入力します。ステップ 2 で作成したインターネット ゲートウェイを **[ターゲット（Target）]** フィールドに入力します。**[ルートの保存（Save Routes）]** をクリックします。

AWS 展開の一部として次のリソースが必要です。

- Cisco Application Services Engine Amazon マシン イメージ（AMI）にアクセスします。
- AWS で完全な管理者アクセス権があることを確認します。
- Elastic Compute Cloud (m5. 2 x大規模EC2) を起動するための権限があります。これは、クラウドで実行されているアプリケーションの仮想マシン（VM）として機能します。Cisco Application Services Engine クラスタをインストールするために、3 つ以上のインスタンスを起動する権限が推奨されます。

AWS での Cisco Application Services Engine の展開

Cisco Application Services Engine は、AWS の CFT テンプレートを使用して、ファブリック外部モードで展開できます。

ステップ 1 Amazon Web Services アカウントにログインし、AWS Management Console に移動します。

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

ステップ 2 [AWS 管理コンソール (AWS Management Console)] 画面の右上隅で、リージョンが表示されている領域を見つけ、Cisco Application Services Engine AMI イメージが呼び出されるで管理する AWS のリージョンを選択します 。

ステップ 3 Amazon EC2 SSH キーペアを作成します。

a) **[サービス（Services）]** をクリックし、**EC2** リンクをクリックします。
b) **[リソース（Resources）]** の下の **[キーペア（Key Pairs）]** をクリックします。

プライベート キーとパブリック キーで構成されるキー ペアは、インスタンスへの接続時に ID を証明するために使用されるセキュリティ クレデンシャルのセットです。

c) **[キー ペアの作成 (Create Key Pair)]** をクリックします。
d) キー ペアの一意の名前を入力します。

名前には、最大 255 文字を含めることができます。有効な文字には、_、-、a～z、A～Z、0～9 が含まれます。

e) （OpenSSHで使用する）**pem**ファイル形式を選択し、**[キー ペアの作成（Create Key Pairs）]** をクリックします。秘密キー PEM ファイルをシステム上の安全な場所に移動し、場所をメモします。

これらの手順の後の部分で、この場所に置かれたプライベート キー PEM ファイルに戻ります。

ステップ 4 AWS Marketplaceで、Cisco Application Services Engine ページを検索します。

AWS の Cisco Application Services Engine ページが表示されます。

ステップ 5 **[引き続きサブスクライブする（Continue to Subscribe）]** をクリックして登録します。

ステップ 6 エンド ユーザ ライセンス契約（EULA）を確認して、**[条件に同意 (Accept Terms)]** ボタンをクリックして同意します。

ステップ 7 1 分後、サブスクリプションを処理する必要がありますというメッセージが表示され、**[ソフトウェアのサブスクライブ（Subscribe to the Software）]**ページが表示されます。**[設定を続行 (Continue to Configuration)]** をクリックします。

[このソフトウェアを設定 (Configure this software)] ページが表示されます。

ステップ 8 以下のパラメータを選択します。

- **[履行（Fulfillment）]** オプション: クラウド形成テンプレートを選択し、Cisco Application Services Engine クラウドを選択します。
- **ソフトウェア バージョン**: 該当するリリースを選択します。
- **[リージョン（Region）]**: クラウド形成テンプレート用の Cisco Application Services Engine が展開されるリージョン。

ステップ 9 **[引き続き起動する（Continue to Launch）]** をクリックします。

[このソフトウェアの起動（Launch this software）] ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 10 **[アクションの選択（Choose Action）]** から、**[CloudFormation の起動（Launch CloudFormation）]** を選択し、**[起動（Launch）]** をクリックします。

ステップ 11 **[Create Stack（スタックの作成）]** ページが表示されます。

ステップ 12 **[テンプレートの指定（Specify Template）]** フィールドで、テンプレート ソースとして **[Amazon S3 URL]** を選択します。これは、自動的に入力されます。

ステップ 13 [Next] をクリックします。

ステップ 14 **[スタック詳細の指定 (Specify Stack Details)]** ページに、以下の情報を入力します。

- **スタック名**
  - **スタック名:** スタック名には、文字（A〜Zおよびa〜z）、数字（0〜9）、およびダッシュ（-）を含めることができます。

    `SE-Cluster`

- **SE クラスタ設定パラメータ**
  - **VPC ID:** Cisco Application Services Engineクラスタに必要なVPC IDです。VPCは前提条件として作成されました。

    `vpc-038f83026b6a48e98(10.21.0.0/16)`

  - **SE クラスタ サブネット-CIDR:** Cisco Application Services Engine クラスタでの起動に必要な VPC サブネット CIDR ブロックです。

    `10.21.1.0/24`

  - **アベイラビリティ– ゾーン (Availability Zone):** スクロールダウン メニューから、Cisco Application Services Engine サブネットのアベイラビリティ ゾーンを選択します。

    Cisco Application Services Engine ノードの起動に使用されるアベイラビリティ ゾーンのリスト。高可用性のために 3 つのアベイラビリティゾーンを選択します。2 つのアベイラビリティ ゾーンのみをサポートするリージョンの場合、2つのアベイラビリティゾーンを選択します（2番目と3 番目の Cisco Application Services Engine は 2 番目のアベイラビリティ ゾーンで起動されます）。**[AZ の数（Number Of AZs）]** パラメータの値が選択数と一致することを確認します。

  - **[AZ の数（Number of AZs）]**: アベイラビリティ ゾーンの数を入力します。有効値は「2」または「3」です。

    （注） この数は、アベイラビリティ ゾーン パラメータから選択した AZ の数と一致する必要があります。一致しない場合、展開は失敗します。

  - **[インスタンス タイプ（Instance Type）]**: 可能な EC2 インスタンス タイプの 1 つを選択します。
  - **ノード名**: サービス ノード名は、「-」で区切った英数字にする必要があります。

    `aws-se-node`

  - **ノード ドメイン**: ノード ドメイン名は、「-」または「。」で区切られた英数字である必要があります。

    `user.local`

  - **NTP サーバ**: NTP サーバの IP アドレスは xxxx 形式である必要があります。

    `192.168.100.100`

  - **DNS サーバ**: DNS サーバの IP アドレスは xxxx の形式である必要があります。

    `2.2.2.2`

  - **検索ドメイン**: DNS 検索ドメインの長さは 6〜128 文字である必要があります。

```
domain.com
```

- **アプリ ネットワーク（App Network）:** Cisco Application Services Engine アプリケーションオーバーレイ IP サブネットの形式は xxxx/x である必要があります。

```
10.101.0.0/16
```

- **サービス ネットワーク（Service Network）:** Cisco Application Services Engine サービスのIPサブネットは xxxx/x の形式である必要があります。

```
10.102.0.0/16
```

- **外部ネット（External Net）:** Cisco Application Services Engineクラスタへのアクセスを許可された外部ネットワーク。xxxx/x 形式の有効な IP サブネットである必要があります。
- **パスワード:** サービスノードのRescueユーザパスワード。パスワードには、少なくとも1文字、数字、および特殊文字（@ $! %* # ? & 長さ: 8ー64文字）を含める必要があります。
- **[パスワードの確認（Confirm Password）]:** サービス ノードのレスキュー ユーザー パスワードを再入力します。
- **SSH キー ペア（SSH Key Pair）:** Cisco Application Services Engine への SSH アクセスを有効にする既存の SSH KeyPair の名前。

```
keypair
```

ステップ 15 [Next] をクリックします。

ステップ 16 **[デフォルトの設定（Configure Defaults）]** ページが表示されます。[Next] をクリックします。

ステップ 17 **[確認（Review）]** ページが表示されます。**[確認（Review）]** ページのすべての情報が正しいことを確認します。

[確認（Review）]ページにエラーが表示された場合は、**[前へ（Previous）]**をクリックして情報を更新します。

ステップ 18 **[スタックの作成（Create Stack）]** をクリックします。

[CloudFormation] ページが再表示されます。作成した Cisco Application Services Engine テンプレートは、**[ステータス（Status）]** 列にテキストとともに表示されます。作成したCisco Application Services Engine テンプレートが、**CREATE_IN_PROGRESS** というテキストとともに表示されます。

ステップ 19 続行する前に、**CREATE_COMPLETE** メッセージが表示されるまで 5ー10 分待ちます。

a) **[サービス（Services）]** をクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード（EC2 Dashboard）] ページが表示されます。

b) **[EC2ダッシュボード（EC2 Dashboard）]** ページで、**[リソース（Resources）]** 領域の実行中のインスタンスの数を含むテキストに移動します。この**実行中のインスタンス**のリンクをクリックします。

[インスタンス（Instances）] ページが表示されます。

c) Cisco Application Services Engine インスタンスの準備が整うまで、5ー10 分待ってから続行します。インスタンスの準備ができると、**[ステータスチェック（Status Checks）]** タブに 2/2 チェックが表示されます。3 つの Cisco Application Services Engine インスタンスすべてに 2/2 チェックが表示されます。

ステップ 20 3 つの Cisco Application Services Engine インスタンスすべてに 2/2 チェックが表示された後で、5〜10 分待ちます。コマンド **ssh -i** *pem-filename* を使用して、Cisco Application Services Engine インスタンスのパブリック IP アドレスを使用して SSH ノードにログインします。**pem rescue-user**@*service-engine-ip*

ステップ 21 SSH にログインした後、次のコマンドを実行します。

```
bash-4.2$ acidiag health
All components are healthy
bash-4.2$
```

インストールが正常に実行されたことを示す「healthy」ステータスが表示されることを確認します。

ステップ 22 Cisco Application Services Engine は、Cisco Application Services Engine でホストできるアプリケーションの展開に使用できます。

（注） Cisco Application Services Engine リリース 1.1.2 では、Cisco ACI Multi-Site Orchestrator アプリケーション（リリース 2.2（3）以降）のみの展開がサポートされています。詳細については、『ACI Multi-Site Orchestrator Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide』を参照してください。

ユーザー名とパスワードに基づいた認証の有効化

Cisco Application Services EngineをAWS（`.ami`）に導入する場合は、Cisco Application Services Engineの導入時に作成した証明書（`.pem` ファイル）を使用してログインする必要があります。

```
ssh -i pem-filename.pem rescue-user@service-engine-ip
```

デフォルトでは、証明書ベースの認証のみが AMI サービス ノードで許可されます。

次のコマンドを実行して、各サービスノードで個別にユーザー名/パスワード認証を有効にします。

acidiag loginprompt enable / disable

KVM での Cisco Application Services Engine の展開

前提条件

開始する前に、次の 1 回限りの前提条件を完了します。

- CentOS、Ubuntu、RedHat などの Linux オペレーティング システムでサポートされている Cisco Application Services Engine の展開。
- 次の要件が満たされていることを確認します。
  - Linux カーネル: 3.10.0-957.el7.x86_64
  - Virsh: libvirt-4.5.0-23.el7_7.1.x86_64

- 各クラスタ ノードには、専用のディスク パーティションと 800 GB 以上のディスク領域が必要です。
- ディスクの I/O 遅延は 20 ミリ秒未満である必要があります。/home がディスク/パーティションの場合、

```
# mkdir /home/test_data
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data_with_se --size=22m
 --bs=2300 --name=mytest
```

  99.00th=[<VALUE>] under **fsync/fdatasync/sync_file_range** セクションを確認します。20 ミリ秒未満である必要があります。
- メモリ：サービスノードごとに 48G
- vCPU：サービスノードごとに 16 個
- QEMU-KVM サポートに必要なすべてのパッケージをインストールしました。

KVM での Cisco Application Services Engine の展開

この手順は、Linux KVM で Cisco Application Services Engine クラスタを設定するために使用されます。

ステップ 1 Cisco Application Services Engine ISOイメージ イメージを選択します。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

b) KVM の Cisco Application Services Engine イメージ（apic-sn-dk9.1.1.2(x).qcow2）を選択します。

ステップ 2 サービスノードベースqcow2イメージのディレクトリを作成し、**apic-sn-dk9.1.1.2h.qcow2** ファイルをダウンロードします。

（注） すべてのクラスタ ノードのすべての KVM ホストでこれを実行します。

（注） 各ノードは、一意のディスク パーティション上に qcow2 パスを持つ必要があります。

```
[ node1 ] # mkdir -p /home/sn_base/qcow2
[ node1 ] # cd /home/sn_base/qcow2
[ node1 ] # <wget/scp file from CCO to this location>
[ node1 ] # ls
apic-sn-dk9.1.1.2h.qcow2
[ node1 ] #
```

ステップ 3 各ホストでサービス ノードのデータ パスのディレクトリを作成し、ベースイメージのスナップショットを作成します。サービス ノードは常にこのスナップショットに書き込みます。

（注） クラスタ内のすべてのサービス ノードでこのアクションを実行します。

```
[ node1 ] # mkdir -p /home/mso-node1/
[ node1 ] # cd /home/mso-node1
[ node1 ] # qemu-img create -f qcow2 -b /home/sn_base/qcow2/apic-sn-dk9.1.1.2h.qcow2
/home/mso-node1/disk0.qcow2
```

ステップ 4 KVM コンソールを開き、**[新しい仮想マシン（New Virtual Machine）]** をクリックします。

ステップ 5 **[新しい VM（New VM）]** で、**[既存のディスク イメージのインポート（import existing disk image）]** オプションを選択します。[Forward] をクリックします。

ステップ 6 **[既存のストレージパスの提供（provid existing storage path）]** タブで、**/home/mso-node1/disk0.qcow2** ファイルを選択します。

（注） 各ノードは、一意のディスク パーティション上に qcow2 パスを持つ必要があります。

ステップ 7 オペレーティング システムとバージョンの**汎用**値を選択します。[Forward] をクリックします。

ステップ 8 メモリには、値 48000 を選択します。CPUには、値 16 を選択します。[Forward] をクリックします。

ステップ 9 仮想マシン **`mso-node1`** の名前を入力します。**[インストール前に設定をカスタマイズ（Customize configuration before install）]** チェックボックスをオンにします。**[ネットワーク選択（Network selection）]** から適切なオプションを選択し、**[終了（Finish）]** をクリックします。

ステップ 10 **QEMU/KVM の mso-node1** ウィンドウで、**[ネットワーク選択（Network selection）]** から適切なオプションを選択します。

a) **仮想ネットワーク インターフェイス** の NIC を選択し、デバイス モデルとして **e1000** を選択します。
b) デフォルトの **MAC アドレス** のままにします。
c) [Apply] をクリックします。
d) [Begin Installation] をクリックします。

仮想マシンが **disk0.qcow2** から起動します。最初のブート プロンプトが表示されます。

a) モードを指定します。Cisco APIC クラスタから設定を取得しないことを指定するには、**n** を入力します。
b) サービス ノードのシリアル番号と一意のホスト名を入力します。
c) サービス ノードのドメイン名を入力します。ドメイン名は、クラスタの名前またはファブリックのドメイン名と同じです。

```
Setup utility for apic-sn with SerialNumber Not Specified and running version 1.1.2h
Is this running in ACI mode? (y/n) n
Enter node serialnumber: Mynode01
Enter node hostname: mso-node1
Enter node domain: example.com
Enter the password for rescue-user:
Reenter the password for rescue-user:
```

ステップ 11 [データ ネットワークの詳細（Data Nework details）] に入力します。

a) ネットワーク IP アドレスおよびマスクを入力します。

データ ネットワーク IP は、SE クラスタリングおよび Cisco ACI ファブリックへのアクセスに使用されます。

```
IP Address/Mask: 192.168.3.2/24
```

b) ゲートウェイの IP アドレスを入力します。

```
gateway IP address: 192.168.3.1
```

c) サービスノードの VLAN ID を入力します。

VLAN はデータ ネットワークで使用されます。オプションで、VLAN がない場合は空の文字列を入力します。

```
Vlan ID: 100
```

ステップ 12 管理ネットワークの詳細を入力します。

a) 管理ネットワーク IP アドレスおよびマスクを入力します。

```
IP Address/Mask: 172.20.7.125/23
```

b) ゲートウェイの IP アドレスを入力します。

```
gateway IP address: 172.20.6.1
```

ステップ 13 クラスタの他のマスター ノード（マスター ピア）のマスターリスト データ ネットワーク IP アドレスとシリアル番号を入力します。

```
Master List(Space Separated IP,Serialnumber List):192.168.100.2,WZP23380BAT 192.168.100.3,WZP23391QHP
```

ステップ 14 DNS の詳細を入力します。

a) DNS 名プロバイダーの IP アドレスを入力します。

```
Providers(Space Separated IP List):171.70.168.183
```

b) 検索ドメインを入力します。

```
Search Domains(Space Separated List):cisco.com
```

ステップ 15 NTP サーバの IP アドレスを入力します。クラスタ内のすべてのマスター ノード間でクロックを同期する必要があります。

```
NTP Servers (Space Separated IP List): 171.68.38.65
```

ステップ 16 サービス サブネット アドレスとマスクを入力します。

これは、プライベート IP アドレス ブロック、kubernetes、サービスIPなどに使用される /16 ネットワークです。

```
Service Subnet (100.80.0.0/16):
```

ステップ 17 アプリケーション サブネット アドレスとマスクを入力します。

```
App Subnet (172.17.0.1/16):
```

ステップ 18 コンフィギュレーションを見直します。

```
Please review the config:
App Subnet: 1.1.0.0/16
Cluster Name: dev-infra12
Cluster Size: 3
DNS:
  Domain Name: dev-infra12.case.local
  Providers:
  - 171.70.168.183
  Search Domains:
  - atomix.local
Download Config: false
Data Network:
  Gateway: 192.10.10.1
  IP Address/Mask: 192.10.10.2/24
  Vlan ID: 1001
```

```
Management Network:
  Gateway: 172.20.6.1
  IP Address/Mask: 172.20.6.147/23
Master List:
- ipAddress: 192.10.12.2
  name: WZP23050V5N
  serialNumber: WZP23050V5N
- ipAddress: 192.10.13.2
  name: WZP23050V68
  serialNumber: WZP23050V68
NTP Servers:
- 171.68.38.65
Node Name: dev-infra12-sn1
Node Role: Master
Node Type: Physical
Password: <hidden>
Service Subnet: 1.2.0.0/16

Re-enter config?(y/N)n

Login with rescue-user & issue acidiag health to check cluster status

CentOS Linux 7 (Core)
Kernel 4.14.174stock-1 on an x86_64
```

ステップ 19 他の 2 つのサービス ノードで手順 1〜11 を実行します。

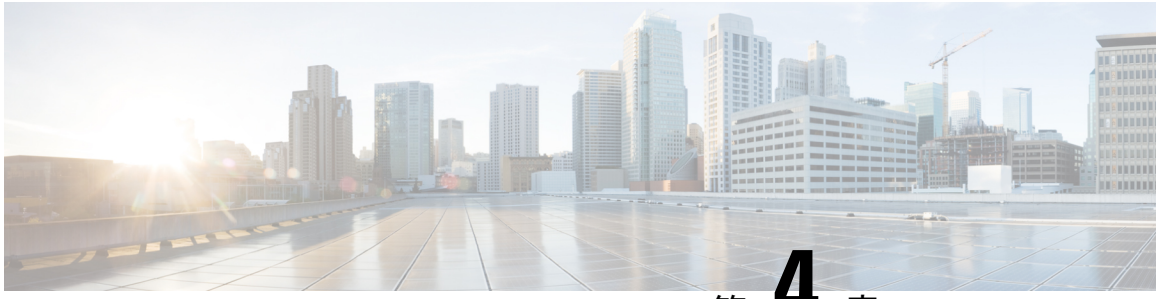
ノード 2 とノード 3 では、クラスタ内の他のマスターノードの管理IPアドレスとシリアル番号が異なります。

ステップ 20 3 つすべてのサービス ノードがブート ストラップが実行されたら、15〜30 分待ってから次のコマンドを実行します。

```
Server # acidiag health
cluster is healthy
```

インストールが正常に実行されたことを示す「正常」ステータスが表示されることを確認します。

ステップ 21 Cisco Application Services Engine は、Cisco Application Services Engine でホストできるアプリケーションの展開に使用できます。



第 4 章

マルチファブリック展開

マルチファブリックのサポート

Cisco Application Services Engine はマルチファブリックをサポートします。マルチファブリック展開では、サービス ノードをファブリック全体にスパンできます。

マルチファブリックのサポートにより、複数の Cisco ACI ファブリックを単一の Cisco Application Services Engine クラスタにオンボードできます。Cisco ACI ファブリックがサイトとして Cisco Application Services Engine クラスタにオンボーディングされると、Cisco Application Services Engine クラスタで実行されているアプリはこのサイトにアクセスできます。

サイトをオンボードするには、Cisco APIC データネットワーク IP と管理者ログイン情報が必要です。Cisco Application Services Engine には、Cisco APIC インバンド管理 IP への IP 到達可能性が必要です。Cisco APIC の管理者ログイン情報は Cisco Application Services Engine クラスタに保存されず、SSL キーを Cisco APIC にコピーするために一度だけ使用されます。Cisco Application Services Engine クラスタに追加されたサイトは、デフォルトではアプリで有効になっていません。それぞれの GUI でアプリごとに明示的に有効にする必要があります。

Cisco Application Services Engine リリース 1.1.3 では、Cisco NIR および Cisco NIA のみが Cisco APIC にオンボードされたサイトを使用します。Cisco ACI Multi-Site Orchestrator はこれらのサイトを使用しません。

サイトの作成

[Sites Details] ページで、次の手順に従います。

始める前に

1. Cisco ACI ファブリック インバンド管理は事前に設定する必要があります。

2. Cisco Application Services Engine データ ネットワーク IP 接続の EPG/L3Out を事前に設定する必要があります。

（注） EPG/L3Out の設定については、『Cisco APIC Layer 3 Networking Configuration Guide』を参照してください。

3. データネットワークを介した Cisco Application Services Engine から Cisco APIC への IP 接続を設定する必要があります。
4. Cisco Application Services Engine からリーフ ノードまたはスパイン ノードへの IP 接続を設定する必要があります。

（注） ポイント 3 および 4 は、Cisco NIR アプリにのみ適用されます。

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > **[サイト（Sites）]**.を選択します。

ステップ 2 [Actions] をクリックします。**[サイトの追加（Add Site）]** をクリックします。

ステップ 3 サイト名を入力します。任意の文字列を指定できます。

ステップ 4 **APIC のホスト名/データネットワーク IP アドレス**を入力します。

ステップ 5 **ユーザー名** を入力します。

ステップ 6 **パスワード**を作成して入力します。パスワードを確認します。

ステップ 7 **ドメイン名**を入力します。

ステップ 8 **[ログイン ドメイン（Login Domain）]** フィールドで、サイトのドメイン名を入力します。

ステップ 9 [作成（Create）] をクリックします。

サイトは、Cisco Application Services Engine に追加されます。

ステップ 10 サイトを追加するには、これらの手順を繰り返します。

（注） サイトが削除された場合、サイトの設定をインポートしても、サイトの回復には役立ちません。サイトは手動で作成する必要があります。

サイトの削除 Cisco Application サービス エンジン

Cisco Application サービス エンジン からサイトを削除または削除するには、次の手順を実行します。

ステップ 1 Cisco Application サービス エンジン GUI にログインします。

ステップ 2 サイトの削除を試みる前に、どのスキーマからもサイトがアンバインドされていることを確認します。

（注） Cisco ACIファブリックを Cisco Application サービス エンジン にサイトとして追加すると、一部のポリシーがCisco APICで作成されます。オンボードサイトを削除せずに Cisco Application サービス エンジン がクリーン リブートされた場合、Cisco APICで作成されたポリシーは削除されません。Cisco APIC でこれらのポリシーをクリーンアップするには、サイトを再度追加して削除する必要があります。

（注） サイトを削除すると、このサイトで実行されているすべてのアプリケーションが中断されます。この操作は取り消すことができません。

ステップ 3 **[インフラストラクチャ（Infrastracture）]** > **[サイト（Sites）]**.を選択します。

ステップ 4 **[サイト（Site）]** リスト ページで、削除するサイトにマウスを合わせて **[アクション（Action）]** > **[削除（Delete）]** を選択します。

ステップ 5 [Submit] をクリックします。`

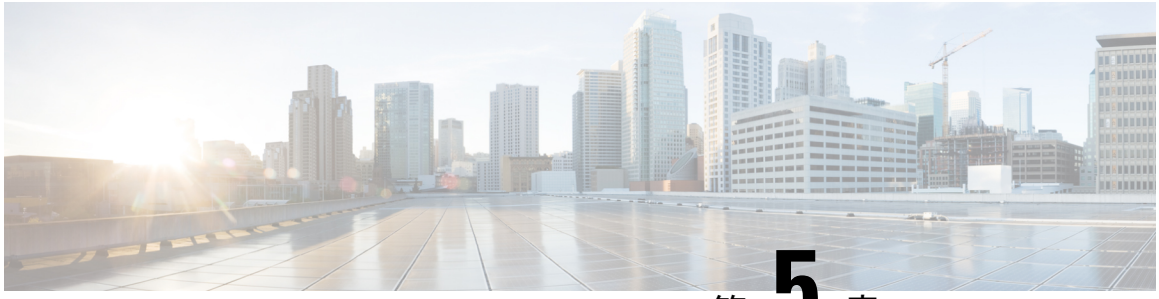
ステップ 6 **[削除の確認（Confirm Delete）]** ダイアログボックスが表示されます。

a) **ユーザー名** を入力します。
b) **パスワード**を作成して入力します。パスワードを確認します。
c) **[ログイン ドメイン（Login Domain）]** フィールドで、サイトのドメイン名を入力します。
d)

ステップ 7 **[強制削除（Force Delete）]** のボックスの横にあるチェックボックスをオンにします。

（注） アプリがサイトを使用しており、アプリからサイトを削除する推奨アクションを実行できない場合、またはサイトに到達できない場合は、**[Force Delete (強制削除)]**オプションを使用します。

ステップ 8 [OK] をクリックします。



第 5 章

Cisco Application Services Engine GUI の概要

この章では、Cisco Application サービス エンジン のグラフィカル ユーザー インターフェイスについて説明します。

この章の内容は、次のとおりです。

Cisco Application Services Engine GUI

Cisco Application サービス エンジン がブートストラップされると、Cisco Application サービス エンジン GUIを使用して残りのアクションを実行できます。

Cisco Application Services Engine GUIにアクセスするには、任意のマスターノードの管理ネットワークIPを使用します。 https://<node-mgmt-ip>

ダッシュボード

ダッシュボードには、Cisco Application サービス エンジン の全体像が表示されます。管理者はこのビューを使用して、システムの健全性、サイトとアプリケーションの接続ステータス、およびリソース使用率をモニターできます。

ダッシュボードには次の情報が表示されます。

- **[概要（Overview）]**タイルには、システムステータス、クラスタ ステータス、およびCisco Intersight ステータスが表示されます。

- **[サイト、アプリ、インフラサービス（Sites、Apps、and Infra Services）]** タイルには、接続別のサイト、ステータス別のアプリケーション、およびステータス別のインフラストラクチャ サービスが表示されます。
- **[インベントリ（Inventory）]** タイルには、ノードタイプ、ノード、コンテナ、ポッド、展開、ステートフル セット、デーモン セット、およびサービスの詳細が表示されます。
- **[サービス ノード ストレージ（Service Node Storage）]** タイルには、登録されたサービス ノードの詳細が表示されます。
- **[使用率（Utilization）]** タイルには、CPU 使用率に関する詳細が表示されます。
- **[メモリ（Memory）]** タイルには、メモリ使用量の詳細が表示されます。

機能

左側のナビゲーションペインの **[Apps]** コンポーネントには、Cisco Application サービス エンジン でホストされているアプリケーションが表示されます。

クリックすると、アプリの作業ウィンドウに、選択したアプリで実行されている**説明**、**バージョン**、**ポッド**、**コンテナ**などのアプリの詳細が表示されます。

- **[コンテナ（Containers）]** タブには、設定済みのすべてのコンテナ、コンテナのステータス、IP アドレス、および設定済みのサービス ノードが表示されます。
- **[ポッド（Pods）]** タブには、選択したアプリで実行されている設定済みポッドが表示されます。
- **[バージョン（Version）]** タブには、アプリのバージョン番号が表示されます。

[有効（Enable）] を選択すると、選択したアプリが有効になります。

[アプリケーションの起動（Lauch App）] では、有効なアプリを起動できます。これにより、アプリが起動する新しいウィンドウが開きます。Cisco Application サービス エンジン にログインして、その他の操作を実行します。

リソースの概要

左側のナビゲーションペインの[システムリソース（System Resources）]コンポーネントには、サービスノードで設定されているアプリケーションリソースが表示されます。

[システム リソース（System Resources）]タブでは、ノードで実行中の**ノード**、**ポッド**、**コンテナ**、**展開**、**ステートフルセット**、**ドメインセット**、および**ネームスペース**を表示するナビゲーション作業ウィンドウが開きます。

ナビゲーション作業ペインの **[ノード（Nodes）]** タブには、選択したアプリで設定され、実行されているサービス ノードの詳細が表示されます。クラスタでは最大7つのノードが許可されます。 3 つのマスターノードと 4 つのワーカーノード。

（注） GUI を使用して登録できるのは、ワーカー ノードのみです。マスター ノードは、「Cisco Application Services Engineの導入」セクションで指定されているコマンド ラインを使用して起動されます。

ナビゲーション作業ウィンドウの **[ポッド（Pods）]** タブには、選択したアプリケーションで実行されている設定済みポッドが表示されます。

ナビゲーション作業ウィンドウの **[コンテナ（Containers）]** タブには、設定されているすべてのコンテナ、コンテナのステータス、IPアドレス、および設定されているサービスノードが表示されます。

ナビゲーション作業ウィンドウの **[展開（Deployments）]** タブには、すべての展開、ステータス、IP アドレス、および設定されたサービス ノードが表示されます。

ナビゲーション作業ペインの **[ステートフルセット（Statefulsets）]** タブには、設定されているすべてのステートフルセット、ステータス、IP アドレス、および設定済みのサービス ノードが表示されます。

ナビゲーション作業ウィンドウの **[Deamonsets]** タブには、設定されているすべての deamonsets、ステータス、ネームスペース、IPアドレスが表示されます。

ナビゲーション作業ペインの **[サービス（Services）]** タブには、サービス名、クラスタIP、設定済みポート、およびアプリのセレクタが表示されます。

ナビゲーション作業ペインの **[名前空間（Namespaces）]** タブには、アプリケーションのサービス、ポッド、コンテナ、展開、およびレプリカセットが表示されます。

オペレーション

左側のナビゲーション ペインの **[操作（Operations）]** コンポーネントに、Cisco Application サービス エンジン に実行できるアクションが表示されます。**[操作（Operations）]** で実行できる 4 つのアクション:

ファームウェア管理

ファームウェア管理は、クラスタ（ファームウェア）のアップグレードまたはダウングレードを実行するために使用されます。

（注） 詳細は Firmware アップグレード （45 ページ） を参照してください。

テクニカルサポート

管理者は、テクニカルサポートの収集を実行できます。

監査ログ

監査ログは、ユーザがトリガーする設定変更です。

バックアップと復元

[バックアップと復元（Backup and Restore）]に、バックアップおよび復元された設定が表示されます。

[テクニカルサポート（Tech Support）]

テクニカル サポートにより、ユーザーは Cisco TAC による詳細なトラブルシューティングのためにシステムのログとアクティビティを収集できるようになります。Cisco Application Services Engine は、ベストエフォートのテクニカルサポートコレクションを提供し、個々のノードまたは統合されたノードのテクニカルサポートをダウンロードできるようになります。テクニカル サポート ファイルは Cisco Application Services Engine でホストされ、いつでもダウンロードできます。

テクニカル サポートを収集するには、次の手順を使用します。

ステップ 1 テクニカル サポートを収集するには、**[テクニカルサポート（Tech Support）]** > **[アクション（Actions）]** > **[テクニカルサポートの収集（Collect Tech Support）]** をクリックします。

ステップ 2 問題の説明を入力し、**[収集（Collect）]** をクリックします。

ステップ 3 テクニカル サポートを削除するには、**[テクニカルサポート（Tech Support）]** をクリックします。削除するテクニカル サポート ログをオンにします。**[アクション（Actions）]**をクリックし、**[テクニカルサポートの削除（Delete Tech Support）]** をクリックします。

ステップ 4 テクニカル サポートが完了したら、ユーザーはトラブルシューティング用のファイルをダウンロードできます。

監査ログ

監査ログを表示するには、次の手順を使用します。

ステップ 1 **[オペレーション（Operations）]**、**[監査ログ（Audit Logs）]**の順に選択します。

ステップ 2 [Audit Logs] をクリックします。

管理者は、**[監査ログ（Audit Logs）]** ビューで設定の変更をモニタできます。監査ログはデフォルトではソートされません。ソートするには、任意の列をクリックします。

アクションの詳細を確認するには、行をクリックすると、特定のアクションで変更された設定を確認できます。

バックアップと復元

クラスタ設定の詳細をバックアップおよび復元するには、次の手順を使用します。

ステップ 1 **[バックアップと復元（Backup and Restore）]** > **[アクション（Actions）]** をクリックします。

ステップ 2 この設定をバックアップするには、**[設定のバックアップ（Back up configuration）]** をクリックします。

ステップ 3 暗号化キー（データを暗号化するためのキー）とファイル名を入力します。**[ダウンロード（download）]** をクリックします。設定がバックアップされ、**[Backup and Restore（バックアップと復元）]** ページに詳細が表示されます。

ステップ 4 設定を復元するには、**[アクション（Actions）]** と **[設定の復元（Restore configuration）]** をクリックします。

ステップ 5 [設定の復元（Restore configuration）] ウィンドウで、インポート タイプを入力します。実行する必要があるアクションに基づいて、**置換** または **マージ** を選択します。

（注） Cisco Application Services Engineは設定のバックアップを保存しないため、ユーザーはバックアップをダウンロードしてローカル環境で維持する必要があります。

replace は、既存の設定をバックアップされた設定に置き換えます。**merge** は、既存の設定とバックアップされた設定のマージを試みます。

ステップ 6 暗号化キー（設定のバックアップに使用）を入力し、インポートするファイルを選択して、**[インポート（Import）]** をクリックします。

クラスタの管理

インフラストラクチャ コンポーネントは、Cisco Application サービス エンジン にサイト、クラスタ設定、および Cisco Intersight の追加または削除を可能にする組み込み管理コントローラです。

サイト:

ACI 領域および可用性ゾーンと見なされる APIC クラスタ ドメイン、または単一のファブリックです。その他のサイトと同じメトロ領域に配置することも、ワールドワイドに配置することもできます。

クラスタの設定:

[クラスタの設定（Cluster Configuration）]には、名前、アプリ サブネット、サービス サブネットなどのクラスタの詳細が表示されます。また、NTP および DNS サーバの詳細も提供します。

Intersight:

デバイス コネクタは、クラウドベース管理プラットフォームである Cisco Intersight の機能を実現する組み込み管理コントローラです。

（注） Cisco NIA アプリは、サービス ノードで設定され、使用可能なアプリの Intersight デバイス コネクタに依存します。

ユーザ管理

左側のナビゲーションペインの**管理**コンポーネントに、Cisco Application サービス エンジン のユーザが表示されます。[ユーザー（Users）]タブでは、管理者が他のユーザーにアクセス権を付与できます。

ユーザの作成

他のユーザーにアクセス権を付与するには、次の手順を使用します。

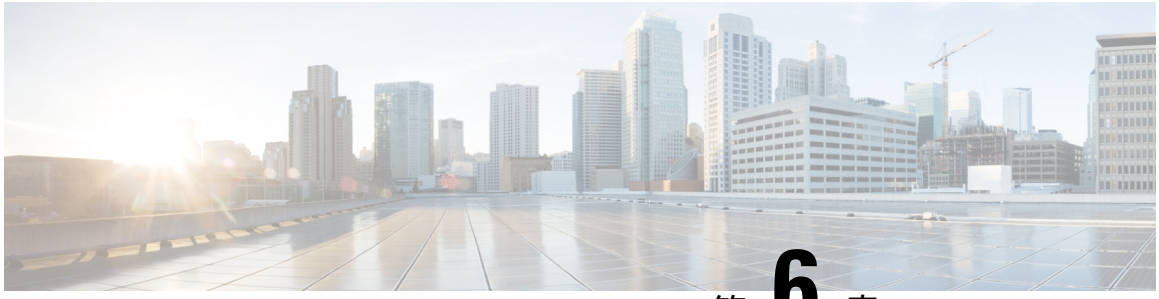
ステップ 1 **[管理（Administrative）]** > **[ユーザー（Users）]** の順に選択します。

（注） ユーザーは、管理ユーザーまたは読み取り専用ユーザーのいずれかになります。

ステップ 2 **[アクション（Actions）]** をクリックし、**[ローカル ユーザーの作成（Create local user）]** をクリックしてユーザを作成します。

ステップ 3 **[アクション（Actions）]** をクリックし、**[ローカル ユーザーの削除（Delete local user）]** をクリックしてユーザーを削除します。

ステップ 4 タイルには、ユーザーのユーザーID、ステータス、名、姓、電子メールID、および権限が表示されます。



第 6 章

アプリケーション管理

Cisco Application Services Engine でのアプリのホスト

Cisco Application サービス エンジン にアプリをアップロードするには、次の手順を実行します。

始める前に

- Cisco Data Center からアプリをダウンロードし、ダウンロードしたアプリ ファイルを http サーバに移動しました。
- アプリをインストールするには管理者のログイン情報が必要です。

ステップ 1 Cisco Application サービス エンジン にログインします。

ステップ 2 サイドのナビゲーション バーから **[アプリ（Apps）]** をクリックします。

ステップ 3 [Actions] をクリックします。

ステップ 4 作業ウィンドウの右端にある **[アプリケーションのアップロード（Upload App）]** をクリックします。

アプリを Cisco Application サービス エンジン にアップロードする**ローカル**タブを選択します。アプリをコンピュータにダウンロードして保存します。Cisco Application サービス エンジン にアップロードする場所を参照します。

ステップ 5 大きなアプリケーションをアップロードするには、**リモート**アップロードオプションを使用します。Cisco App Center からダウンロードし、アプリケーションファイルをホストしたアプリケーションの URL を http サーバにコピーします。

ステップ 6 **[URL]** フィールドにコピーした http アドレスを入力し、**[送信（Submit）]** をクリックします。

[更新（Refresh）] をクリックして、アップロード ステータスを確認します。アプリケーションがホストされると、**[アプリ（Apps）]** タブが表示されます。

ステップ 7 **[アプリ（Apps）]** タブをクリックします。作業ウィンドウに、**[アプリケーションのインストール中]** が表示されます。

ステップ 8 インストールが完了したら、**[有効にする（Enable）]** をクリックして Cisco Application サービス エンジンでアプリケーションを有効にします。

GUI を使用した Cisco Application Services Engine でのサイトのオンボード

GUI を使用して Cisco Application Services Engine にサイトをオンボードするには、次の手順を使用します。Cisco Application Services Engine にインストールされているすべてのアプリケーションは、オンボードされたサイトにアクセスできます。

始める前に

Cisco Application Services Engine をインストールして設定しました。

アプリケーションをインストールするには、管理者のクレデンシャルが必要です。

ステップ 1 管理者権限で Cisco Application Services Engine GUI にログインします。

ステップ 2 サイトの作成 （25 ページ） の手順を使用してサイトを作成し、追加します。

ステップ 3 サイトを作成すると、サイトがノードにオンボードされます。Cisco Application Services Engine にインストールされているすべてのアプリケーションは、オンボードされたサイトにアクセスできます。

ステップ 4 引き続き、GUI を使用して Cisco Application Services Engine にアプリケーションをインストールします。アプリのアップロードについては、Cisco Application Services Engine でのアプリのホスト （35 ページ） を参照してください。

ステップ 5 アプリが起動したら、アプリのユーザー ガイドに従ってサイトを設定します。

アプリのアンインストール

Cisco Application Services Engine のアプリケーションを削除するには、次の手順を使用します。

管理者権限を持つユーザーとして Cisco APIC GUI にログインします。

始める前に

Cisco Application Services Engine でアプリを削除する前に、アプリを無効にする必要があります。

ステップ 1 Cisco Application Services Engine GUI にログインします。

ステップ 2 **[アプリ（Apps）]** をクリックします。

ステップ 3 アプリケーション ダイアログの右上隅にある **[削除（Delete）]** をクリックします。

ステップ 4 アプリケーションの削除ダイアログで **[Yes]** をクリックします。

アプリの無効化

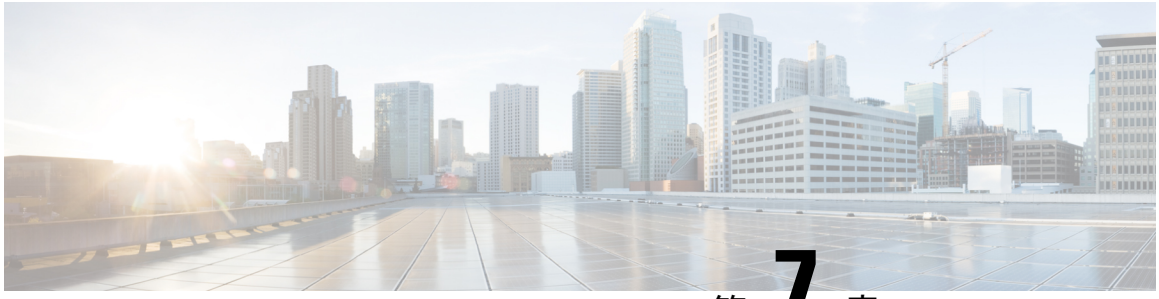
Cisco Application Services Engineでアプリケーションを無効にするには、次の手順を使用します。

ステップ 1 Cisco Application Services Engine GUI にログインします。

ステップ 2 **[アプリ（Apps）]** をクリックします。アプリ ページが表示されます。

ステップ 3 削除するアプリケーションとアプリケーションタイルを選択します。アプリケーションダイアログの右上隅にある **[無効化（Disable）]** をクリックします。

ステップ 4 [アプリケーションの無効化（disable application）] ダイアログで **[はい（Yes）]** をクリックします。



第 7 章

Cisco Application Services Engine の水平スケーリング

ワーカー ノードの追加

既存のクラスタにワーカーノードを追加するには、この手順を使用します。

（注） ワーカー ノードのみが GUI を使用して登録できます。

始める前に

3 つすべてのサービス ノードがブートストラップされていることを確認してください。

ステップ 1 新しいワーカーノードの電源をオンにし、ブートストラップを完了します。このノードのシリアル番号を書き留めます。

ノードのブートストラップについては、Cisco Application Services Engine の展開 （8 ページ） を参照してください。最大 4 つのワーカーノードをクラスタに含めることができます。

（注） ワーカーノードがコマンドラインを使用してブートストラップされると、Cisco Application Services Engine はワーカーノードを検出します。ユーザーは登録アクションをクリックして、追加情報を入力する必要なく、このノードを既存のケース クラスタに追加できます。

ステップ 2 Cisco Application Services Engine GUI にログインします。

ステップ 3 **[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。

GUIでは、ワーカー ノード エントリが **[Register]** として表示されます。シリアル ナンバーが新しいノードのものと一致することを確認します。

ワーカー ノードの事前登録

ワーカーノードを登録するには、次の手順を使用します。

始める前に

3 つすべてのサービス ノードがブートストラップされていることを確認します。

ステップ 1 ノードの**名前**と**シリアル番号**を入力します。

ステップ 2 ノードの**データ ネットワーク IP アドレス**と**データ ネットワーク ゲートウェイ** を入力します。

ステップ 3 ノードの**管理 IP アドレス**と**管理ゲートウェイ**を入力します。

ステップ 4 **[保存（Save）]** をクリックして、**[終了（Finish）]** をクリックします。

ワーカーノードはブートストラップ時に登録されます。

ワーカー ノードの登録

ワーカーノードを登録するには、次の手順を使用します。

始める前に

3 つすべてのサービス ノードがブートストラップされていることを確認します。

ステップ 1 GUI では、ブートストラップしたワーカー ノードの隣のチェックボックスを選択します。ワーカーノードを許可するには、**[アクション（Actions）]** > **[登録（Register）]** をクリックします。

ステップ 2 ノードの**データ ネットワーク IP アドレス**と**データ ネットワーク ゲートウェイ** が自動入力されます。

ステップ 3 ノードの**管理 IP アドレス**と**管理ゲートウェイ**が自動入力されます。

ステップ 4 **[保存（Save）]** をクリックして、**[終了（Finish）]** をクリックします。

ワーカーノードはブートストラップ時に登録されます。

ワーカー ノードの削除

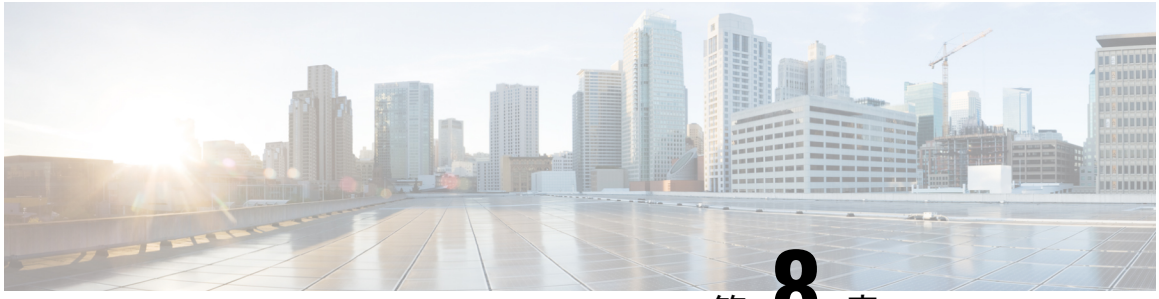
ワーカー ノードを削除するには、次の手順を使用します。

始める前に

1. 3 つすべてのサービス ノードがブートストラップされていることを確認します。
2. 新しいワーカー ノードが事前登録または登録されている。

ステップ 1 GUIで、ブートストラップされたワーカー ノードの横にあるチェックボックスをオンにします。ワーカー ノードを削除するには、**[アクション（Actions）]** > **[削除（Delete）]** をクリックします。

ステップ 2 **[削除（Delete）]** と **[終了 (Finish)]** を順にクリックします。



第 8 章

Cisco Application Services Engine のアップグレード

Fabric Internal Mode（リリース 1.1.2）から Fabric External Mode（リリース 1.1.3）への移行

この手順を使用して、Cisco Application サービス エンジン をバージョン 1.1.2 から 1.1.3 にアップグレードできます。

（注） ステートフル移行はサポートされません。1.1.2 から 1.1.3 にアップグレードしても、アプリデータは保持されません。移行後にすべてのアプリを再インストールする必要があります。

（注） 同じ手順を各サービスノードで個別に実行する必要があります。

始める前に

- Cisco Application Services Engineがインストールされ、クラスタが設定されている必要があります。
- アップグレード用の動作中のソフトウェア イメージがあることを確認します。

ステップ 1 Cisco Application サービス エンジン GUI にログインします。

ステップ 2 Cisco APIC で Cisco NIR および Cisco NIA アプリを無効にします。

ステップ 3 Cisco Application サービス エンジン データ ネットワーク サブネットと Cisco Application サービス エンジン 接続ポートを書き留めます。

ステップ 4 Cisco APIC からサービス ノード関連の設定を消去します。次のクリーン スクリプトを実行します。

```
import requests
import json
import xml
import urllib3
import argparse
urllib3.disable_warnings()
```

ステップ 5 Cisco Application サービス エンジン アプリを無効にして削除します。

ステップ 6 ステップ 3 の情報を使用して、管理テナントの Cisco Application サービス エンジン 接続用のブリッジ ドメイン（BD）、サブネット、およびエンドポイント グループ（EPG）を設定します。

（注） EPG/L3Out の設定については、「Cisco APIC Layer 3 ネットワーク設定ガイド」を参照してください。

ステップ 7 ファブリック データ ネットワーク EPGと Cisco Application サービス エンジン EPG間のコントラクトを作成します。

ステップ 8 すべてのサービスノードをリリース 1.1.3 にアップグレードします。

ステップ 9 **acidiag installer update** -f *iso_filepath* コマンドを使用して、アップグレードを開始します。

```
node # acidiag installer update -f /tmp/apic-sn-dk9.1.1.3.iso
```

すべてのノードでコマンドを個別に実行します。コマンドが正常に実行されたら、サービス ノードを再起動します。

ステップ 10 **acidiag touch setup** コマンド を使用して、以前のバージョンの展開をクリーンアップします。

```
node # acidiag touch setup
```

ステップ 11 **acidiag reboot** コマンドを使用して個々のノードをリブートします。

```
node # acidiag reboot
```

ステップ 12 Cisco Application Services Engine の展開 （8 ページ） の説明に従って、3つすべてのノードで最初のセットアップを完了します。

ステップ 13 **acidiag version** コマンドを使用して、アップグレード後のバージョンを確認します。

```
node # acidiag version
```

ステップ 14 サイトの作成 （25 ページ） に記載されている手順を使用して、新しいサイトを追加します。

ステップ 15 Cisco NIR および Cisco NIA アプリを再インストールし、Cisco Application サービス エンジン GUIでサイトを有効にします。

Firmware アップグレード

ファームウェア管理は、クラスタ（ファームウェア）のアップグレードまたはダウングレードを実行するために使用されます。同じワークフローを使用してクラスタ（ファームウェア）のダウングレードを実現することもできます。ファームウェアをアップグレードまたはダウングレードするには、次の手順を使用します。

始める前に

注目 この手順は、1.1.3 以降のリリースにアップグレードする場合にのみ適用されます。以前のリリースからアップグレードするには、Cisco Application Services Engine のアップグレード （43 ページ） を参照してください。

ステップ 1 左側のナビゲーション ペインで **[Operations（オペレーション）]** コンポーネントに移動します。

ステップ 2 **[Operations（オペレーション）]** > **[ファームウェア管理（Firmware Management）]** に移動します。

[ファームウェア管理（Firmware Management）]タブには、現在のファームウェアバージョン、ノード数、ファームウェアで行われた最後の更新など、ノードの詳細が表示されます。

ステップ 3 **[イメージ（images）]** タブをクリックし、新しいイメージをダウンロードします。

ステップ 4 **[ファームウェア管理（Firmware Management）]**をクリックし、**[更新の設定（Set an update）]** をクリックします。

ステップ 5 **[使用可能なターゲット ファームウェア バージョン（Available Target Firmware Versions）]** をクリックし、該当するバージョンを選択して **[確認（confirm）]** をクリックします。

ステップ 6 **[インストール（Install）]** をクリックし、**[次へ（Next）]** をクリックします。

ステップ 7 インストールが完了したら、**[アクティベート（Activate）]**をクリックし、アクティベーションが完了したら、**[完了（Complete）]** をクリックします。

手動アップグレード手順

サービス ノードを手動でアップグレードするには、この手順を使用します。

ステップ 1 Cisco Application Services Engine サーバにレスキューユーザーとしてログインします。

ステップ 2 ISOイメージ ファイルをすべてのノードの / tmp ディレクトリにコピーします。

ステップ 3 **acidiag installer update** コマンドを使用して、アップグレードを開始します。

すべてのノードでコマンドを個別に実行します。コマンドが正常に実行されたら、サービス ノードを再起動します。ステップ 4 に進む前に、すべてのノードで成功メッセージが表示されるまで待ちます。

```
[rescue-user@node1 ~]$ acidiag installer update -f /tmp/case-dk9.1.1.3a.iso
Warning: This command will initiate node update to new version. Proceed? (y/n): y
Update in Progress ... Do not press Ctrl^C
Update succeeded, reboot your host
```

ステップ 4 **acidiag reboot** コマンドを使用してノードを再起動します。

次のノードに進む前に、各ノードが新しいバージョンと正常な状態になるまで待ちます。

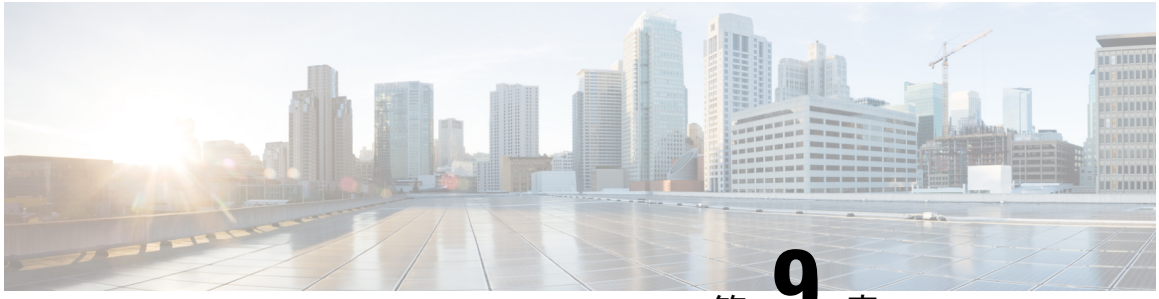
```
[rescue-user@node1 ~]$ acidiag reboot
This command will restart this device, Proceed? (y/n): y
Connection to 172.20.6.119 closed.

[rescue-user@node1 ~]$ acidiag version
APIC-SN 1.1.3a

[rescue-user@node1 ~]$ acidiag health
All components are healthy
```

（注） これをノードで次々に実行します。複数のノードを使用不可にすることはできません。

ステップ 5 すべてのノードが新しいバージョンで稼働し、正常になったら、すべてのノードで並行して **acidiag installer post-update** を実行します。

```
[rescue-user@node1 ~]$ acidiag installer post-update
Warning: This command will run the post-update scripts. Proceed? (y/n): y
Update in Progress ... Do not press Ctrl^C
Post-update succeeded
```

ステップ 6 これでアップグレードは完了です。サービスが新しいバージョンに更新される際のクラスタの状態をモニタするために **acidiag health** を使用します。



第 9 章

Cisco Application Services Engine のメンテナンス

シングル マスターノードのRMA

マスター ノードの RMA にこの手順を使用します。

ステップ 1 正常なマスター ノードの1つでUIにログインします。**[システム リソース（System Resources）]** < **[ノード（Nodes）]** を選択します。

ステップ 2 削除する古いマスター ノードの電源をオフにします。UIで、このノードのステータスが **[非アクティブ（Inactive）]** に変更されていることを確認します。削除する必要があるノードのシリアル番号と一致することを確認します。

ステップ 3 新しいノードの電源をオンにし、ブートストラップを完了します。古いノードの設定に使用したものと同じパラメータ（名前とネットワーク情報を含む）を使用します。このノードのシリアル番号を書き留めます。

ステップ 4 UIで、非アクティブなマスターノードの横にあるチェックボックスをオンにします。**[アクション（Actions）]** をクリックし、**[置換（Replace）]** を選択します。プロンプトが表示されたら、[New Serial Number]の下に新しいノードのシリアル番号を入力して続行します。

ステップ 5 UIで、シリアル番号が更新されるのがわかります。マスターがクラスタに正常に参加すると、ステータスが **[アクティブ（Active）]** に変わります。

2 つのマスターノードの RMA

マスター ノードの RMA にこの手順を使用します。

ステップ 1 障害が発生した 2 つのマスター ノードの電源を切ります。

ステップ 2 古いノードのブートストラップに使用したパラメータと同じパラメータを使用して、2 つの新しいノードの電源をオンにし、ブートストラップします。

ノードのブートストラップについては、Cisco Application Services Engine の展開 （8 ページ） を参照してください。最大 4 つのワーカーノードをクラスタに含めることができます。

ステップ 3 正常なマスター（CLI）にログインし、**acidiag recover save** コマンドを実行します。

```
[rescue-user@node1 ~]$ acidiag recover save
Warning: Cluster recovery can be a disruptive operation and should only
be performed as last resort option to recover cluster from disasters
where two master nodes have lost their state due to hardware faults. Proceed? (y/n): y

cluster snapshot '/tmp/cluster_snapshot.tar.gz' generated successfully.
Copy to other devices as '/tmp/cluster_snapshot.tar.gz' before performing restore.
```

ステップ 4 前の手順で生成された `.tar` ファイルを 2 つの新しいノードに `/tmp/cluster_snapshot.tar.gz` としてコピーし、すべてのノードで **acidiag recover restore** コマンドを実行します。ノードが再起動します。

```
[rescue-user@node1 ~]$ acidiag recover restore
Warning: This command will restart this device to perform recovery.
Make sure, you have copied cluster snapshot to other devices
if you are recovering the cluster from this device. Proceed? (y/n): y
Connection to 172.20.6.119 closed.
```

ステップ 5 すべてのノードがクラスタを形成し、それらのステータスが正常と表示されるまで待ちます。クラスタ全体のヘルスを確認するには、**acidiag health** コマンドを使用します。

シングル ワーカー RMA

障害が発生したワーカーノードを置換するには、次の手順を使用します。

（注） 不正なソフトウェア状態のノードをクリーンアップまたはリカバリするには、**acidiag touch clean** または **acidiag touch setup** を使用してから、**acidiag reboot** が続きます。

（注） 物理的に交換する必要があるハードウェアの問題に対してノードを RMA できるように、**[削除（Delete）]** オプションが提供されていないことを確認してください。ワーカーノードを **削除** する場合は、同じブートストラップ情報で新しいノードを **登録** する必要があります。

ステップ 1 正常なマスターノードのいずれかの GUI にログインします。**[システム リソース（System Resources）]** < **[ノード（Nodes）]** を選択します。

ステップ 2 削除する古いワーカーノードの電源をオフにします。GUIで、このノードのステータスが **[Inactive]** に変更されていることを確認します。シリアル番号が、交換する必要があるノードのシリアル番号と一致していることを確認します。

ステップ 3 GUIで、削除する必要があるワーカーノードの横にあるチェックボックスをオンにします。**[アクション（Actions）]** < **[削除（Delete）]** をクリックします。このノードのエントリが **[ノード（Nodes）]** ページから削除されます。

ステップ 4 新しいワーカーノードの電源をオンにし、ブートストラップを完了します。古いワーカーノードの設定に使用したものと同じパラメータを使用します。このノードのシリアル番号を書き留めます。

ステップ 5 GUI では、ワーカーノードエントリは **[登録解除（Unregistered）]** として表示されます。シリアル番号が新しいノードのシリアル番号と一致していることを確認します。

ステップ 6 GUIで、このワーカーノードの横にあるチェックボックスをオンにします。**[アクション（Actions）]** をクリックし、**[登録（Register）]** を選択します。次の画面で詳細を確認し、**[保存（Save）]** を選択します。

ステップ 7 GUIで、ノードのステータスが[**Discovering]** に変わり、その後、**[Active]** に変わります。

第 10 章

Cisco Application サービス エンジンのトラブルシューティング

この章の内容は、次のとおりです。

Cisco Application Services Engine の操作

次のコマンドを使用して、Cisco Application Services Engineでさまざまな操作を実行できます。

アプリ操作用のコマンド:

- **acidiag cluster get config**クラスタリング設定を確認します。

  ```
  acidiag cluster get config
  ```

- **acidiag cluster get masters**: クラスタ マスターのステータスを確認します。

  ```
  acidiag cluster get masters
  ```

- **acidiag cluster get workers**: クラスタ ワーカーのステータスを確認します。

  ```
  acidiag cluster get workers
  ```

- **acidiag health**: クラスタ ヘルスのステータスを確認します。

  ```
  acidiag health
  ```

- **acidiag app show**: インストールされているアプリケーションのステータスを表示します。

  ```
  acidiag app show
  ```

- **acidiag app install**: アプリケーションをインストールします。

  ```
  acidiag app install <filepath or url>
  ```

- **acidiag app enable**: インストール済み（または無効化済み）のアプリケーションを有効にします。

  ```
  acidiag app enable <application id>
  bash-4.2$ acidiag app
  [ { 'adminState': 'Enabled',
  'apiEntrypoint': '/query',
  ```

```
'appID': 'MSO',
'creationTimestamp': '2019-12-08T22:02:08.513217541Z',
'description': 'Multi-Site Orchestrator application',
'displayName': 'cisco-mso',
'id': 'cisco-mso:2.2.3',
'name': 'cisco-mso',
'operStage': 'Enable',
'operState': 'Running',
'schemaversion': '',
'uiEntrypoint': '/ui/app-start.html',
'vendorID': 'Cisco',
'version': '2.2.3'}]
bash-4.2$
```

- **acidiag app disable**: 有効なアプリケーションを無効にします。

```
acidiag app disable <application id>
```

- **acidiag app delete**: アプリケーションを削除します。

```
acidiag app delete <application id>
```

アプリ イメージ操作用のコマンド:

- **acidiag image show**: 存在するすべてのアプリケーション イメージを表示します。

```
acidiag image show
```

- **acidiag image show <image file name>**: 指定されたアプリケーション イメージに関する情報を表示します。

```
acidiag image show <image file name>
```

アプリのインポート操作のコマンド:

- **acidiag import show**: Cisco Application Services Engine に対して行われたすべてのアプリケーションインポートに関する情報を表示します。

```
acidiag import show
```

- **acidiag import show <import id>**: 指定したインポートに関する情報を表示します。インポート ID はオプションのパラメータです。

```
acidiag import show <import id>
```

テクニカル サポートのコマンド:

- **acidiag techsupport collect**

```
acidiag techsupport collect
Started: TS collection may take 15-20 minutes to complete. Monitor /techsupport/ for
 the file
```

第 11 章

デバイス コネクタの設定

この章では、Cisco Application サービス エンジン プラットフォームで Cisco Intersight Device Connector を設定および要求するタスクについて説明します。

この章の内容は、次のとおりです。

Intersight デバイス コネクタの概要

デバイスは、各システムの管理コントローラに組み込まれているデバイス コネクタを介して Cisco Intersight ポータルに接続されます。デバイス コネクタは、接続されているデバイスに対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight ポータルから制御命令を受信できる安全な方法を提供します。

Intersight 対応のデバイスまたはアプリケーションが起動すると、デフォルトではブート時にデバイスコネクタが起動してクラウドサービスに接続しようとします。**[自動更新（Auto Update）]** オプションが有効になっている場合、Cisco Intersight に接続するときに、Intersight サービスによる更新を介して、デバイス コネクタは最新のバージョンに自動的に更新されます。**[自動更新（Auto Update）]** オプションの詳細については、デバイス コネクタの設定 （53 ページ） を参照してください。

デバイス コネクタの設定

Cisco NIA アプリなどのデータセンター アプリは、Cisco Application サービス エンジン プラットフォームの管理コントローラに組み込まれているデバイス コネクタを介して Cisco Intersight クラウド ポータルに接続されます。

Cisco Intersight は、他のインテリジェントシステムによって拡張される Software-as-a-Service（SaaS）インフラストラクチャ管理プラットフォームです。Cisco Unified Computing System（Cisco UCS）およびCisco HyperFlex ハイパーコンバージド インフラストラクチャ、Cisco APIC、および Cisco Application サービス エンジン を含むその他のプラットフォームのグロー

バル管理を提供します。デバイス コネクタは、接続されている Cisco Application サービス エンジンに対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight クラウドから情報送受信できる安全な方法を提供します。

デバイス コネクタを設定するには、次の手順を実行します。

ステップ 1 Cisco Application サービス エンジン GUIを開きます。

ステップ 2 **[ナビゲーション（Navigation）]**ペインで、**[インフラストラクチャ（Infrastructure）]**、**[Intersight]** の順にクリックします。

- **[デバイス コネクタ（Device Connector）]**ページで**インターネット**を **Intersight** に接続する緑色の点線と、**[要求（Claimed）]** というテキストが表示されている場合、Intersightデバイスコネクタはすでに設定されており、Intersight クラウド サービスに接続されています。
- **[デバイス コネクタ（Device Connector）]**ページに黄色い点線と**インターネット**を **Intersight** に接続する注意アイコンと、テキスト **[要求されていない（Not Claimed）]** が表示されている場合、Intersight デバイス コネクタはまだ設定されておらず、Intersightサービスに接続されていないため、デバイスはまだ要求されていません。次の手順に従って、Intersight デバイス コネクタを設定し、Intersight クラウド サービスに接続し、デバイスを要求します。

（注） **[デバイス コネクタ（Device Connector）]** ページで**インターネット**を **Intersight** に接続する赤い点線は、手順 8 でプロキシが正しく設定されていないことを示します。

ステップ 3 使用可能な新しいデバイス コネクタ ソフトウェア バージョンがある場合は、この時点でソフトウェアを更新するかどうかを決定します。

使用可能な新しいデバイス コネクタ ソフトウェアバージョンがあり、**[自動更新（Auto Update）]** オプションが有効になっていない場合は、画面上部に、デバイス コネクタに重要な更新プログラムがあることを通知するメッセージが表示されます（ステップ 5c を参照）。

- この時点でソフトウェアを更新しない場合は、手順 5 に進み、Intersight デバイス コネクタ設定を開始します。
- この時点でソフトウェアを更新する場合は、ソフトウェアの更新方法に応じて、ページ上部にある黄色のバーの 2 つのリンクのいずれかをクリックします。
  - **[今すぐ更新（Update Now）]**: デバイスコネクタソフトウェアをすぐに更新するには、このリンクをクリックします。
  - **[自動更新の有効化（Enable Auto Update）]**: **[一般（General）]**ページに移動するには、このリンクをクリックします。**[自動更新（Auto Update）]** フィールドを [オン（On）] に切り替えると、システムはデバイス コネクタ ソフトウェアを自動的に更新できます。詳細については、ステップ6cを参照してください。

ステップ 4 **[デバイス コネクタ（Device Connector）]** 見出しの右側にある **[設定（Settings）]** リンクを見つけ、**[設定（Settings）]** リンクをクリックします。

[設定（Settings）] ページが表示され、**[General（設定）]** タブがデフォルトで選択されています。

ステップ 5 **[全般（General）]** ページで、次の設定を行います。

a) **[デバイス コネクタ（Device Connector）]**フィールドで、デバイスと Cisco Intersight 間の通信を許可するかどうかを決定します。

[デバイス コネクタ（Device Connector）] オプション（デフォルトで有効）を使用すると、デバイスを要求し、Intersight の機能を活用できます。オフになっている場合、Cisco Intersight への通信は許可されません。

b) **[アクセスモード（Access Mode）]** フィールドで、Intersight がこのデバイスに変更を加えることを許可するかどうかを決定します。

アクセス モードでは、クラウドからの完全な読み取りまたは書き込み操作を許可したり、Cisco Intersight からこのデバイスに加えられた変更を制限したりできます。

- **[コントロールを許可（Allow Control）]**オプション（デフォルトで選択）を使用すると、Cisco Intersight で使用可能な機能に基づいて、クラウドからすべての読み取り/書き込み操作を実行します。
- **[読み取り専用（Read-only）]** オプションは、Intersight からこのデバイスに変更が加えられないことを保証します。たとえば、ファームウェアのアップグレードやプロファイルの展開などのアクションは読み取り専用モードでは許可されません。ただし、アクションは特定のシステムで使用可能な機能によって異なります。

c) **[自動更新（Auto Update）]** フィールドで、システムによるソフトウェアの自動更新を許可するかどうかを決定します。

システムがソフトウェアを自動的に更新するように、**[自動更新（Auto Update）]** オプションを [オン（ON）] に切り替えることを推奨します。**[自動更新（Auto Update）]** オプションを [オン（ON）] に切り替えると、Intersight からのアップグレード プッシュがあるたびに、デバイス コネクタがそのイメージを自動的にアップグレードします。

- システムがソフトウェアを自動的に更新できるようにするには、[オン（ON）] を切り替えます。
- 必要に応じて手動でソフトウェアを更新できるように、[オフ（OFF）] に切り替えます。この場合、新しいリリースが利用可能になると、ソフトウェアを手動で更新するように求められます。

（注） **[自動更新（Auto Update）]** オプションをオフにすると、デバイス コネクタが定期的に期限切れになり、デバイス コネクタが Cisco Intersight に接続できなくなる可能性があります。

ステップ 6 **[全般（General）]** ページの設定を完了したら **[Save（保存）]** をクリックします。

[Intersight - デバイス コネクタ] の概要ページが再度表示されます。この時点で、Intersight デバイス コネクタのいくつかの設定を行うか、確認できます。

- デバイス コネクタが Cisco Intersight クラウドとの通信に使用するプロキシを設定する場合は、ステップ 8 に進みます。
- デバイス コネクタを使用して証明書を管理する場合は、ステップ 11 に進みます。

（注） Cisco Application サービス エンジン では、Intersight デバイス コネクタのプロキシ設定を構成する必要があります。

ステップ 7 デバイス コネクタが Cisco Intersight クラウドとの通信に使用するプロキシを設定する場合は、**[設定（Settings）]** をクリックし、**[プロキシ設定（Proxy Configuration）]** をクリックします。

[プロキシ設定（Proxy Configuration）] ページが表示されます。

ステップ 8 **[プロキシ設定（Proxy Configuration）]** ページで、次の設定を行います。

このページでは、デバイス コネクタが Cisco Intersight クラウドとの通信に使用するプロキシを設定できます。

（注） デバイス コネクタで必須となるログイン情報のフォーマットはなく、入力したクレデンシャルがそのまま構成済み HTTP プロキシ サーバに渡されます。ドメイン名でユーザー名を限定する必要があるかどうかは、HTTP プロキシ サーバの設定によって異なります。

a) **[プロキシの有効化（Enable Proxy）]** フィールドで、オプションを [オン（ON）] に切り替えてプロキシ設定を行います。
b) **[プロキシ ホスト名/IP（Proxy Hostname/IP）]** フィールドに、プロキシ ホスト名または IP アドレスを入力します。
c) **[プロキシ ポート（Proxy Port）]** フィールドで、プロキシ ポート番号を指定します。
d) **[認証（Authentication）]** フィールドで、**[認証（Authentication）]** オプションを [オン（ON）] に切り替えてプロキシ認証設定を行い、認証用のプロキシ ユーザー名とパスワードを入力します。

ステップ 9 **[プロキシ設定（Proxy Configuration）]** ページで設定が完了したら、**[保存（Save）]** をクリックします。

[Intersight - デバイス コネクタ] の概要ページが再度表示されます。

デバイス コネクタで証明書を管理する場合は、次の手順に進みます。

ステップ 10 デバイス コネクタを使用して証明書を管理する場合は、**[設定（Settings）]** をクリックし、**[証明書マネージャ（Certificate Manager）]** をクリックします。

[証明書マネージャ（Certificate Manager）] ページが表示されます。

ステップ 11 **[証明書マネージャ（Certificate Manager）]** ページで、次の設定を行います。

デフォルトでは、デバイス コネクタが信頼するのは組み込まれている svc.ucs-connect.com 証明書のみです。デバイス コネクタが TLS 接続を確立し、サーバが組み込まれている svc.ucs-connect.com 証明書に一致しない証明書を送信すると、デバイス コネクタはそのサーバが信頼できるデバイスかどうかを判断できないため、TLS 接続を終了します。

[インポート（Import）] をクリックして、CA 署名付き証明書をインポートします。インポートされた証明書が *.pem (base64 エンコード) 形式である必要があります。証明書が正常にインポートされると、**信頼できる証明書**のリストに記載され、証明書が正しければ **[使用中（In-Use）]** に表示されます。

svc.ucs-connect.com（intersight.com）への接続に使用する証明書のリストの次の詳細を表示します。

- **[名前 (Name)]**—CA 証明書の共通名。
- **[使用中 (In Use)]** - 信頼ストアで証明書を正常にリモート サーバの確認に使用されたかどうか。

- **[発行者 (Issued By)]**: 証明書の発行認証局。
- **[有効期限 (Expires)]**—証明書の有効期限。

信頼できる証明書 のリストから証明書を削除します。ただし、バンドルされている証明書（root + 中間証明書）はリストから削除できません。ロック アイコンは、バンドルされた証明書を表します。

ステップ 12 **[証明書マネージャ（Certificate Manager）]** ページで設定が完了したら、**[閉じる（Close）]**をクリックします。

デバイスの要求 （57 ページ） に記載されている手順を使用してデバイスを要求できます。

デバイスの要求

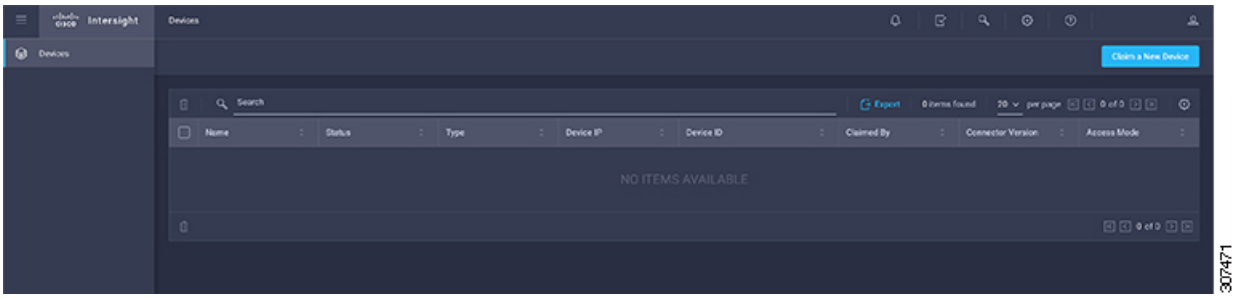
始める前に

Cisco Application Services Engine から Intersight Device Connector を設定しました。

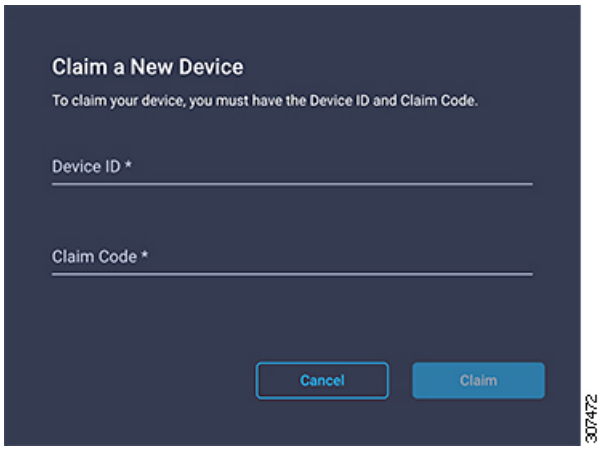
ステップ 1 Cisco Intersight クラウド サイトにログインします。

https://www.intersight.com

ステップ 2 Cisco Intersight クラウドサイトで、**[デバイス（Devices）]** タブをクリックし、**[新しいデバイスの要求（Claim a New Device）]** をクリックします。



[デバイス（Device）] ページが表示されます。



ステップ 3 Cisco APIC UIで、**[アプリ（Apps）]** ページに移動します。

a) **[アプリ（Apps）]** ページのリストで、Cisco Application サービス エンジン を選択します。

b) **[ナビゲーション（Navigation）]** ペインで **[VM]** をクリックします。

ステップ 4 Cisco APICで実行している Cisco Application サービス エンジン アプリ UI から**デバイス ID** と**請求コード**をコピーします。

ステップ 5 Cisco Intersight クラウドサイトで、適切なフィールドに貼り付けます。

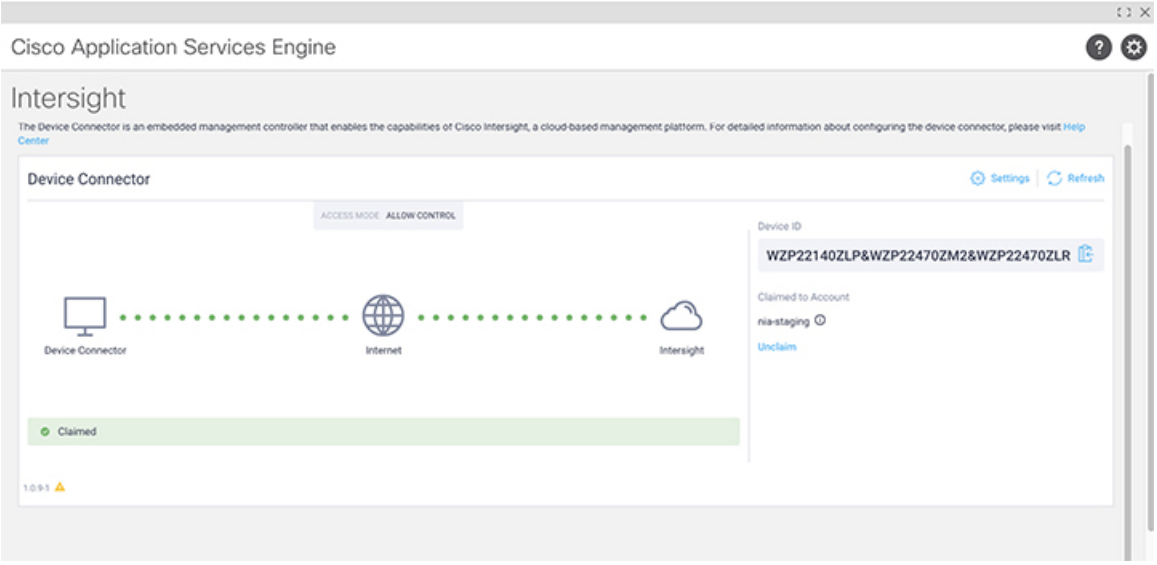
ステップ 6 Intersight クラウド サイトの **[新しいデバイスの要求（New Device）]**ページ。

ステップ 7 **[要求（Claim）]** をクリックします。

[新しいデバイスの要求（Claim a New Device）] ページに「デバイスが正常に申請されました」というメッセージが表示されます。また、メインページの [Status] 列に [Connected] と表示された Cisco Application サービス エンジン プラットフォームが表示されます。

ステップ 8 Cisco APIC GUIの Cisco Application サービス エンジン アプリ UI の **[Intersight デバイス コネクタ（Intersight-Device Connector）]**ページに戻り、システムが正常に要求されたことを確認します。

[デバイスコネクタ（Device Connector）]ページに、**インターネット**と **Intersight** を接続する緑色の点線と、**[Claimed]** というテキストが表示されます。



（注） ページの情報を現在の状態に更新するには、**[Intersight デバイス コネクタ（Intersight-Device Connector）]** ページで **[更新（Refresh）]** をクリックしなければならない場合があります。 z

このデバイスの要求を解除するには、**[Intersight デバイス コネクタ（Intersight-Device Connector）]** の **[Unclaim]** リンクをクリックします。