

# Cisco Digital Network Architecture Center リリース 1.3.1.0 ハイアベイラビリティガイド

初版：2019年9月4日

## Cisco DNA Center リリース 1.3.1.0 HA ガイド

Cisco DNA Center のハイアベイラビリティ (HA) 実装の説明については、次のガイドを参照してください。

### ハイアベイラビリティの概要

Cisco DNA Center のハイアベイラビリティ (HA) フレームワークは、障害によるダウンタイムの量を削減し、障害が発生したときのネットワークの耐障害性を向上させるように設計されています。障害が発生した場合、このフレームワークは、ネットワークを以前の動作状態に復元するのに役立ちます。これが不可能な場合、Cisco DNA Center は注意が必要な問題があることを示します。

Cisco DNA Center の HA フレームワークでは、クラスタノードの変更が行われたと判断すると、この変更を他のノードと同期します。サポートされる同期のタイプは、次のとおりです。

- データベースの変更（設定、パフォーマンス、およびモニタリングデータに関連する更新など）。
- ファイルの変更（レポート設定、設定テンプレート、TFTP ルートディレクトリ、管理設定、ライセンスファイル、キーストアなど）。

このガイドでは、HA、導入、管理のベストプラクティス、および発生する可能性がある障害シナリオを使用するために満たす必要がある要件（および Cisco DNA Center による処理方法と必要なユーザーアクション）について説明します。このガイドを参照する際は、次の点に注意してください。

- シードとマスタの用語は同義で使用しています。シードノード（マスタノード）は、NDP 名前空間で Elasticsearch が実行されているノードです。
- このリリースでは、Cisco DNA Center は自動化機能の HA サポートのみを提供します。現時点で、アシュアランスの HA はサポートされていません。

### ハイアベイラビリティ要件

実稼働環境で HA を有効にするには、次の要件を満たす必要があります。

- クラスタは、コア数が同じ3つの Cisco DNA Center アプライアンスで構成します。つまり、第1世代の44コアアプライアンス（Cisco 部品番号 DN1）と第2世代の44コアアプライアンス（Cisco 部品番号 DN2-HW-APL および DN2-HW-APL-U）の両方でクラスタを構成できることを意味します。



(注) 第1世代および第2世代のアプライアンスとそれに対応するシスコ製品番号リストを参照するには、『[Cisco Digital Network Architecture Center 第2世代アプライアンスインストールガイド](#)』のトピック「インターフェイス名とウィザードの設定順序」を参照してください。

- アプライアンスが Cisco DNA Center 1.2.8 以降の同じバージョンを実行している。たとえばバージョン 1.2.8 のパッチが1つのクラスタノードにインストールされている場合は、HA を動作させるために、他のクラスタノードにも同じパッチをインストールする必要があります。

## ハイアベイラビリティの機能

Cisco DNA Center は、ソフトウェアとハードウェアの両方のハイアベイラビリティを提供する3ノードクラスタ設定をサポートしています。ノード上のサービスが機能しなくなると、ソフトウェア障害が発生します。ソフトウェアのハイアベイラビリティには、ノード上のサービスを再起動する機能が含まれています。たとえば3ノードクラスタの1つのノードでサービスに障害が発生した場合、そのサービスは、同じノードまたは残りの2つのノードのいずれかで再起動されます。アプライアンス自体に動作不良や障害があると、ハードウェア障害が発生します。ハードウェアのハイアベイラビリティは、クラスタ内の複数のアプライアンス、各アプライアンスの RAID 設定内の複数のディスクドライブ、および複数の電源装置が存在することによって有効になります。その結果、障害が発生したコンポーネントが復元または交換されるまで、これらのコンポーネントのいずれかによる障害を許容することができます。



(注) Cisco DNA Center は、3つを超えるノードを持つクラスタをサポートしていません。たとえば5つまたは7つのノードを持つマルチノードクラスタは現在サポートされていません。

3ノードクラスタの故障耐性は、単一ノードの障害に対応するよう設計されています。つまり、単一ノードが機能しなくなった場合でも、Cisco DNA Center は特定のサービス全体にハイアベイラビリティを提供しようとします。2つのノードで障害が発生した場合、HA 動作を実行するために必要なクォーラムが失われ、クラスタが分割されます。

## クラスタリングおよびデータベース レプリケーション

Cisco DNA Center 複数のノード間での分散処理とデータベース レプリケーション用メカニズムとなります。クラスタリングにより、リソースと機能を共有するとともに、ハイアベイラビリティを実現することができます。

## セキュリティの複製

マルチノード環境では、X.509 証明書やトラストプールを含む単一ノードのセキュリティ機能が他の2つのノードで複製されます。ノードを既存のクラスタに結合して3ノードクラスタを形成すると、Cisco DNA Center GUI ユーザクレデンシャルがノード間で共有されます。ただし、CLI ユーザクレデンシャルは、各ノードで別々であるため、共有されません。

## ソフトウェア アップグレード

マルチノードクラスタでは、Cisco DNA Center GUI からクラスタ全体のアップグレードをトリガーできます（GUIは単一ノードだけでなくクラスタ全体を表します）。GUIからトリガーされたアップグレードでは、クラスタ内のすべてのノードが自動的にアップグレードされます。



- (注) (Cisco DNA Center のコアインフラストラクチャを更新する) システムアップグレードを開始すると、Cisco DNA Center はメンテナンスモードになります。メンテナンスモードでは、アップグレードプロセスが完了するまで Cisco DNA Center を利用できなくなります。Cisco DNA Center システムアップグレードのスケジュールを設定する際は、このことを考慮する必要があります。システムアップグレードが完了したら、**[システム設定 (System Settings)] > [ソフトウェアアップデート (Software Updates)] > [更新 (Updates)]** の順にアクセスしてインストールされているバージョンを確認し、GUI でアップグレードの成功を確認できます。

## [ハイアベイラビリティ展開 (High Availability Deployment) ]

このセクションのトピックでは、実稼働環境で HA 対応クラスタを展開および管理する際に従う必要があるベストプラクティスについて説明します。

### 展開の推奨事項

3つのノード（1つのシードノードと2つの非シードノード）で構成されるクラスタを設定することを推奨します。ノード数が奇数の場合、このような分散システムで操作を実行するために必要なクォーラムが提供されます。Cisco DNA Center はこれらを3つの独立したノードではなく、仮想 IP アドレスを介してアクセスされる1つの論理エンティティと見なします。

HA を展開する場合は、次のことを推奨します。

- 3ノードクラスタを設定する場合は、クラスタがネットワーク障害の影響を受ける可能性があるため、低速リンク間で LAN をスパンするようにノードを設定しないでください。また、1つのノードで障害が発生したサービスを回復させるために必要な時間を増やすこともできます。3ノードクラスタのクラスタインターフェイスを設定する場合、すべてのクラスタノードが同じサブネット内に存在するようにしてください。
- HA の動作に悪影響を及ぼす可能性があるため、管理、データ、および HA の責任で単一のインターフェイスをオーバーロードすることは避けてください。
- クラスタノードを設定する場合は、リンクローカルサブネット（169.x.x.x）をクラスタまたはサービスサブネットとして指定しないでください（そのアドレスは Cisco DNA Center 内部ネットワークによって使用されるため）。



(注) サブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および 6598 仕様に準拠している必要があります。

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10

詳細については、RFC 1918 では『[Address Allocation For Private Internets](#)』を、RFC 6598 では『[IANA-Reserved IPv4 Prefix For Shared Address Space](#)』を参照してください。

- オフ時間中は HA を有効にしてください。Cisco DNA Center がメンテナンスモードを開始し、サービスの再配布が完了するまで使用できないためです。

## クラスタの展開

HA が有効になっている 3 ノードクラスタに Cisco DNA Center を展開するには、次の手順を実行します。

### 手順

**ステップ 1** クラスタ内の最初のノードに Cisco DNA Center を設定します。

- 第 1 世代アプライアンスを設定する場合は、『[Cisco DNA Center 第 1 世代アプライアンスインストールガイド](#)』の「Configure Master Node」を参照してください。
- 第 2 世代アプライアンスを設定する場合は、『[Cisco Digital Network Architecture Center 第 2 世代アプライアンスインストールガイド](#)』の使用する設定ウィザードとアプライアンスのタイプに固有のトピックを参照してください。
  - Maglev 設定ウィザードを使用して第 2 世代アプライアンスを設定する場合は、トピック「Configure the Master Node Using the Maglev Wizard」を参照してください。
  - ブラウザベースの設定ウィザードを使用して 44 または 56 コアの第 2 世代アプライアンスを設定する場合は、「ブラウザベースウィザードを使用した 44 または 56 コアアプライアンスの設定」の章のトピック「Configure the Master Node Using the Browser-Based Wizard」を参照してください。

**ステップ 2** クラスタ内の 2 番目のノードで Cisco DNA Center を設定します。


- 第 1 世代アプライアンスを設定する場合は、『[Cisco DNA 第 1 世代アプライアンスインストールガイド](#)』のトピック「Configure Add-on Nodes」を参照してください。

- 第2世代アプライアンスを設定する場合は、『[Cisco Digital Network Architecture Center 第2世代アプライアンスインストールガイド](#)』の使用する設定ウィザードとアプライアンスのタイプに固有のトピックを参照してください。
  - Maglev 設定ウィザードを使用して第2世代アプライアンスを設定する場合は、トピック「[Configure Add-On Nodes Using the Maglev Wizard](#)」を参照してください。
  - ブラウザベースの設定ウィザードを使用して 44 または 56 第2世代コアアプライアンスを設定する場合は、「[ブラウザベースウィザードを使用した 44 または 56 コアアプライアンスの設定](#)」の章のトピック「[Configure Add-On Nodes Using the Browser-Based Wizard](#)」を参照してください。

**ステップ3** クラスタ内の3番目のノードで Cisco DNA Center を設定します。

ステップ2の完了時に表示されたのと同じアドオンノードの設定項目を参照してください。

**ステップ4** クラスタでハイアベイラビリティを有効にします。

- a)  をクリックして、[システム設定 (System Settings)] を選択します。  
[システム360 (System 360)] タブは、デフォルトで表示されます。
- b) [ホスト (Hosts)] 領域で、[サービス配布の有効化 (Enable Service Distribution)] をクリックします。

- (注)
- GUIで[サービス配布の有効化 (Enable Service Distribution)] をクリックすると、Cisco DNA Center がメンテナンスモードになります。このモードでは、プロセスが完了するまでCisco DNA Center を利用できなくなります。HA 導入のスケジュールを設定する場合は、このことを考慮する必要があります。
  - Cisco DNA Center また、データベースを復元し、(パッケージのアップグレードではなく) システムのアップグレードを実行した場合も、メンテナンスモードに移行します。
  - 3 ノードクラスタ環境で AAA サーバによる外部認証を有効にするには、AAA サーバで個々の Cisco DNA Center ノード IP アドレスのすべてと 3 ノードクラスタの仮想 IP アドレスを設定する必要があります。

---

## クラスタの管理

このセクションのトピックでは、実稼働環境で HA が有効になっている場合に完了する必要がある管理タスクについて説明します。

### Maglev コマンドの実行

クラスタ内のノードで Maglev コマンドを正常に実行するには、次の手順を実行します。

## 始める前に

- セッションで最初の **Maglev** コマンドを実行する前に、この手順のみを完了する必要があります。現在のセッションを閉じて新しいセッションを開始しない限り、再度完了する必要はありません。
- SSH クライアントでコマンドを実行すると、RSA ホストキーが変更されたことを示すエラーメッセージが表示され、`~/.ssh/known_hosts` ファイルに正しいキーを追加するように求められます。これは通常、アプライアンスが以前に指定したものと異なる IP アドレスを使用して再イメージ化された場合に発生します。このような状況が発生した場合は、次の手順を実行します。

1. アプライアンスに割り当てられる IP アドレスを次のアドレスに設定します。 **cat `~/.ssh/known_hosts`**

ここで、`~`は、マシン上の `known_host` ファイルが存在するディレクトリを表します。

出力結果は次の例のようになります。

```
[192.168.254.21]:2222 ecdsa-sha2-nistp256
AAAAB2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBA19/31YV+cQvI1rmIV1/
CaE/BqCdeg5Xr/pS0twNnKB6eDrXvLSAUMz+EED339GvbkxT/DdsdGZn2BeWHIifuY=
```

2. `known_hosts` ファイルからこの IP アドレスに関連付けられている次のすべてのキーを削除します。 **ssh-keygen -R *appliance's-IP-address***

この例では、次のコマンドを実行します。 **ssh-keygen -R 192.168.254.21:2222**



(注) 別のオプションとして、`~/.ssh/known_hosts` ファイルを削除してから次の手順に進むこともできます。

3. 以前に実行しようとしたコマンドを実行します。

## 手順

**ステップ 1** SSH クライアントで、次のコマンドを入力します。

```
ssh node's IP address -l maglev-p 2222
```

**ステップ 2** ノードの信頼性が確立できないことを示すメッセージが表示された場合は、続行するように求められたら、`yes`を入力します。

**ステップ 3** ノードの `maglev` ユーザに対して設定されている Linux パスワードを入力します。

**ステップ 4** 実行する `Maglev` コマンドを入力します。

**ステップ 5** Cisco DNA Center のデフォルトの管理スーパーユーザ用に設定されたパスワードを入力します。

## 一般的なクラスタノードの動作

クラスタ内のノードに対して完了する必要がある操作は、通常、次の操作です。クラスタノードのシャットダウン（計画されたメンテナンスを実行する前、または返品許可（RMA）のためにノードを準備する前に実行する操作）と、ノードのリブート（ダウンしているノードを復元する場合、または設定変更を保存する場合に実行する）などです。



(注) 稼働中の3ノードクラスタ内の2つのノードを同時に再起動またはシャットダウンすることはできません。このような操作を行うと、クラスタのクォーラム要件が成立しなくなります。

動作	必要なアクション
CLI から3ノードクラスタ内のすべてのノードをシャットダウンします。	すべてのノードで <b>sudo shutdown -h now</b> コマンドを同時に実行します。
再起動が必要な変更を行った後は、1つ以上のノードを再起動します。	該当ノードで <b>sudo shutdown -r now</b> コマンドを実行します。
メンテナンスのために1つのノードをシャットダウンまたは切断します（ノードを再起動するだけではない場合）。	次のコマンドを実行します。 <ol style="list-style-type: none"> <li><b>maglev node drain node's-IP-address</b></li> <li><b>maglev node drain_history</b>（ノードが正常にドレインされたことを確認するため）</li> <li><b>sudo shutdown -h now</b>（シャットダウンしているノードで実行）</li> </ol>
RMA用のノードを準備します。	次の手順を実行します。 <ol style="list-style-type: none"> <li>メンテナンスのためにクラスタノードをシャットダウンまたは切断する場合は、前の行で説明した手順を実行します。</li> <li><b>magctl node display</b> コマンドを実行して、ドレインされたノードのステータスが <code>NotReady</code> になっていることを確認します。</li> <li><b>maglev node remove node's-IP-address</b> コマンドを実行します。</li> <li><b>magctl node display</b> コマンドをもう一度実行します。 今度はクラスタに対して2つのノードのみ表示されます。</li> </ol>

## 失敗したクラスタノードの回復

3 ノードクラスタに属するノードに障害が発生した場合、通常、クラスタが回復するまでに 30 分かかります。ノードがダウンしていることを検出するために 5 分、別のノードにサービスを移動するのに 25 分かかります。5 分後に、次のバナーメッセージが表示されます。「自動化およびアシユアランスサービスは現在ダウンしています。ノード `node_details` との接続が失われました。

(Automation and Assurance services are currently down. Connectivity with node `node_details` has been lost.)」障害が発生したノードを回復するには、次の手順を実行します。

### 手順

- 
- ステップ 1** 正常なクラスタノードにログインし、コマンド `maglev node remove failed-node's-IP-address` を入力します。
- これにより、クラスタから障害ノードが除外されます。
- ステップ 2** アクティブノードで `maglev package status` コマンドを入力します。
- Cisco DNA Center からこの情報にアクセスすることもできます。⚙️ をクリックし、[概要 (About)] > [パッケージの表示 (Show Packages)] の順に選択してください。
- ステップ 3** Cisco TAC に連絡してそのコマンドの出力を提供し、ご使用のバージョンと一致する ISO を確認してください。
- ステップ 4** 削除したノードを再度追加するには、再設置する必要があります。
- 第 1 世代アプライアンスを設定する場合、Maglev 構成ウィザードの [Cisco DNA Center クラスタに参加 (Join an existing Cluster)] オプションを使用します。『Cisco Digital Network Architecture Center 第 1 世代アプライアンス インストール ガイド』のトピック「Configure Add-On Nodes」を参照してください。
  - Maglev 構成ウィザードを使用して第 2 世代アプライアンスを設定する場合は、ウィザードの [既存のクラスタに参加する (Join a Cisco DNA Center Cluster)] オプションを使用します。『Cisco DNA Center 第 2 世代アプライアンス インストール ガイド』のトピック「Configure Add-On Nodes Using the Maglev Wizard」を参照してください。
  - ブラウザベースの構成ウィザードを使用して第 2 世代の 44 または 56 コアアプライアンスを設定する場合は、同ウィザードの [既存クラスタに参加 (Join an existing Cluster)] オプションを使用します。『Cisco DNA Center 第 2 世代アプライアンス インストール ガイド』のトピック「Configure Add-On Nodes Using the Browser-Based Wizard」を参照してください。
- ステップ 5** HA 動作を最適化するために、クラスタノード間でサービスを再配布します。
- Cisco DNA Center GUI で ⚙️ をクリックし、[システム設定 (System Settings)] を選択します。
  - [システム 360 (System 360)] タブ > [ホスト (Hosts)] 領域で、[サービス配布の有効化 (Enable Service Distribution)] をクリックします。
-



## 失敗したシードノードの置換

シードノードに障害が発生した場合は、次のタスクを実行して交換します。

1. 障害が発生したノードをクラスタから削除します。  
「[失敗したシードノードの削除](#)」を参照してください。
2. 障害が発生したノードを別のノードと交換します。  
「[新しいシードノードの追加](#)」を参照してください。

## 失敗したシードノードの削除

シードノードで障害が発生した場合、それを削除し、動作中のノードと交換する必要があります。シードノードの削除には、約 30 分かかります。

このセクションは、ハードウェア障害が原因で障害が発生した場合にのみ適用されます。



- (注) シードノードを削除すると、既存のアシユアランスデータは失われますが、残されたノードが新しいアシユアランスデータの収集を開始します。

### 始める前に

次のことを実行してください。

- データのバックアップを作成します。ノード障害のためにこの手順を実行している場合は、今すぐバックアップを作成することはできません。代わりに、定期的に作成したバックアップに依存する必要があります。
- この手順を実行するには 30 分以上必要です。

## 手順

**ステップ 1** (オプション) アシユアランスシードノードを削除する必要がある場合は、次のアクションを実行して削除するノードを特定します。

1. 次のコマンドを実行します。 **magctl appstack status ndp | grep elastic**
2. elasticsearch-0 エントリを見つけます。  
シードノードの IP アドレスが [ノード (Node) ] カラムに表示されます。

**ステップ 2** 削除するノードをシャットダウンします。

シャットダウンプロセスには約 10 分かかります。

**ステップ 3** 次のノードがダウンしていることを確認します。

**magctl node display**

ノードのステータスは「NOT\_READY」でなければなりません。

**ステップ 4** appstack が次のステータスになっていることを確認します。

```
magctl appstack status
```

シャットダウンされたノードのポッドに、ステータスとして「NODELOST」または「Pending」が表示されます。

**ステップ 5** 削除していない次のノード（非シードノード）のいずれかにログインします。

```
maglev login -u admin -p admin-password -c node's-IP-address:443
```

**ステップ 6** 障害が発生した次のシードノードをクラスタから削除します。

```
maglev node remove node's IP address
```

ノードの削除プロセスは、完了するまでに約 30 分かかります。

**ステップ 7** 次の残りの 2 つのノードですべてのサービスが実行されていることを確認します。

```
magctl node display
```

```
magctl appstack status
```

## 新しいシードノードの追加

障害が発生したシードノードを削除したら、クラスタに新しいノードを追加できます。

### 始める前に

次のタスクを実行してください。

- 失敗したシードノードを削除します。詳細については、[失敗したシードノードの削除（9 ページ）](#)を参照してください。
- この手順を実行するには 30 分以上必要です。

### 手順

**ステップ 1** クラスタ内の他のノードが実行しているものと同じソフトウェアバージョンを新しいノードにインストールします。

- 第 1 世代アプライアンスを設定する場合、Maglev 構成ウィザードの [Cisco DNA Center クラスタに参加 (Join an existing Cluster)] オプションを使用します。『[Cisco DNA Center 第 1 世代アプライアンス インストール ガイド](#)』のトピック「Configure Add-on Nodes」を参照してください。
- Maglev 構成ウィザードを使用して第 2 世代アプライアンスを設定する場合は、ウィザードの [既存のクラスタに参加する (Join a Cisco DNA Center Cluster)] オプションを使用しま

す。『[Cisco DNA Center 第 2 世代アプライアンス インストール ガイド](#)』のトピック「Configure Add-On Nodes Using the Maglev Wizard」を参照してください。

- ブラウザベースの構成ウィザードを使用して第 2 世代アプライアンスを設定する場合は、同ウィザードの [既存クラスタに参加 (Join an existing Cluster)] オプションを使用します。『[Cisco DNA Center 第 2 世代アプライアンス インストール ガイド](#)』のトピック「Configure Add-On Nodes Using the Browser-Based Wizard」を参照してください。

**ステップ 2** インストールが完了したら、次のコマンドを入力します。

```
magctl node display
```

新しいノードに [準備完了 (Ready)] ステータスが表示されます。

**ステップ 3** 新しいノードで次を実行します。

- a) 次のコマンドを入力します。

```
maglev node allow node's IP address
```

- b) 新しいノードに次のサービスを再配布します。

```
maglev service nodescale refresh
```

- c) 次のサービスが再配布されたことを確認します。

```
magctl appstack status
```

新しいノードのステータスが [実行中 (Running)] と表示されます。

**ステップ 4** 以前に アシユアランス データをバックアップしていた場合は、そのデータを復元します。

詳細については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』の「Restore Data from Backups」のトピックを参照してください。

- 重要**
- 新しいアシユアランス シードノードを追加する場合は、置換するアシユアランス シードノードで使用されていたものと同じ IP アドレスを設定します。
  - 障害が発生したシードノードは、クラスタに再び追加するとアドオンノードとして機能します。以前のロールであるシードノードとしての機能は再開しません。

## 障害と停止の影響を最小限に抑える

一般的な 3 ノード Cisco DNA Center クラスタでは、各ノードはノードのクラスタ ポート インターフェイスを介して 1 つのクラスタスイッチに接続されます。クラスタスイッチとの接続には、2 つのトランシーバと 1 つの光ファイバケーブルが必要です。これらはいずれも障害が発生する可能性があります。クラスタスイッチ自体も (電源切断や手動再起動などにより) 障害が発生する可能性があります。これにより、Cisco DNA Center クラスタが停止し、すべてのコントローラ機能が失われる可能性があります。クラスタの障害または停止の影響を最小限に抑えるには、次の 1 つ以上を実行します。

- ソフトウェアアップグレード、設定のリロード、電源の再投入などの管理操作は重要ではない期間中に実行します。これらの操作によってクラスタの停止が発生する可能性があるためです。
- インサーブिस ソフトウェア アップグレード (ISSU) 機能をサポートするスイッチにクラスタノードを接続します。この機能を使用すると、システムはステートフルスイッチオーバー (SSO) によるノンストップフォワーディング (NSF) を使用してトラフィックの転送を続行しながらシステムソフトウェアをアップグレードすることができ、システムのダウンタイムなしでソフトウェアアップグレードを実行します。
- クラスタノードをスイッチスタックに接続します。これにより、各クラスタノードを、Cisco StackWise を介して参加しているスイッチスタックの別のメンバーに接続できます。クラスタが複数のスイッチに接続されているため、1つのスイッチがダウンした場合の影響が軽減されます。

## ハイアベイラビリティ障害のシナリオ

ノードの障害は、以下の1つ以上の領域で起きた問題が原因で発生する可能性があります。

- ソフトウェア
- ネットワーク アクセス層
- ハードウェア

障害が発生すると、Cisco DNA Center は通常 5 分以内に検出し、障害を自力で解決します。5 分よりも長く続く障害には、ユーザの介入が必要になる場合があります。

次の表に、クラスタで発生する可能性のある障害シナリオと、Cisco DNA Center による対応方法について説明します。表の最初の列に注意してください。これは、クラスタの動作を復元するためにユーザからのアクションを必要とするシナリオを示しています。



**重要** クラスタを動作させるには、Cisco DNA Center の HA の実装で常に少なくとも2つのクラスタノードが稼働している必要があります。

既知の HA のバグと回避策については、『[Release Notes for Cisco Digital Network Architecture Center](#)』の「Open Bugs—High Availability」を参照してください。

ユーザアクションの必要性	障害シナリオ	HA の動作
Yes	クラスタ内のすべてのノードがダウンする。	すぐに自動化バックアップを実行します。『 <a href="#">Cisco Digital Network Architecture Center 管理者ガイド</a> 』の「Backup and Restore」の章を参照してください。

ユーザアクションの必要性	障害シナリオ	HA の動作
なし	ノードに障害が発生している、到達不能である、または 5 分未満のサービス障害が発生している。	<ul style="list-style-type: none"> <li>• ノードに障害が発生してから 5 分間は UI にアクセスできません。</li> <li>• 障害が発生したノードで実行されていたサービスは、他のノードに移行されません。</li> <li>• VIP を使用する場合、残り 2 つのノードではノースバウンドインターフェイス (NBI) が使用可能なままになります。</li> <li>• VIP 接続はフェールオーバー後に復元され、サービスが起動して実行された後に API コールが回復します。</li> </ul> <p>ノードが復元された後、次のようになります。</p> <ul style="list-style-type: none"> <li>• 復元されたノード上のデータは、他のクラスタメンバーと同期されます。</li> <li>• タイムアウトになっていない保留中の UI および NBI コールが完了します。</li> </ul>

ユーザアクションの必要性	障害シナリオ	HA の動作
なし	非シードノードに障害が発生している、到達不能である、または5分未満のサービス障害が発生している。	<ul style="list-style-type: none"> <li>• 5分後に、Cisco DNA Center でノードとの接続が失われたことを示すステータスメッセージが表示されます。</li> <li>• VIP を使用する場合、UI は残りの2つのノードで使用可能なままになります。</li> <li>• 障害が発生したノードで実行されていたサービスは、他のノードに移行されます。</li> <li>• 障害が発生したノードのNBIにはアクセスできませんが、残り2つのノードのNBIは引き続き動作します。</li> </ul> <p>ノードが復元されてから、ノードがクラスタに再参加するまでは、次のようになります。</p> <ul style="list-style-type: none"> <li>• Cisco DNA Center クラスタ動作が再開したことを示すステータスメッセージが表示されます。</li> <li>• タイムアウトしていない保留中の UI コールが完了します。</li> <li>• 障害が発生したノードで保留されていたサービスリクエストは、サービスの移行先ノードで実行されます。</li> </ul> <p>ノードがクラスタに再参加した後、次のようになります。</p> <ul style="list-style-type: none"> <li>• 復元されたノード上のデータは、他のクラスタメンバーと同期されます。</li> <li>• 障害が発生したノードで実行されていたサービスは停止します。</li> <li>• 障害が発生したノードで保留されていたすべてのサービスリクエストが停止されます。</li> </ul>

ユーザアクションの必要性	障害シナリオ	HA の動作
なし	シードノードに障害が発生している、到達不能である、または5分未満のサービス障害が発生している。	<ul style="list-style-type: none"> <li>• Cisco DNA Center ノードとの接続が失われたことを示すステータスメッセージが表示されます。</li> <li>• VIP を使用する場合、UI は残りの2つのノードで使用可能なままになります。</li> <li>• 障害が発生したノードで実行されていたサービスは、他のノードに移行されます。</li> <li>• 障害が発生したノードで実行されているサービスのステータスは「待機中 (waiting)」に設定される可能性があります。</li> <li>• 障害が発生したノードのNBIにはアクセスできませんが、残り2つのノードのNBIは引き続き動作します。</li> </ul> <p>ノードが復元されてから、ノードがクラスタに再参加するまでは、次のようになります。</p> <ul style="list-style-type: none"> <li>• Cisco DNA Center クラスタ動作が再開したことを示すステータスメッセージが表示されます。</li> <li>• タイムアウトしていない保留中の UI コールが完了します。</li> <li>• 障害が発生したノードで保留されていたサービスリクエストは、サービスの移行先ノードで実行されます。</li> </ul> <p>ノードがクラスタに再参加した後、次のようになります。</p> <ul style="list-style-type: none"> <li>• 復元されたノード上のデータは、他のクラスタメンバーと同期されます。</li> <li>• 障害が発生したノードで実行されていた サービスは停止します。</li> <li>• 障害が発生したノードで保留されていたすべてのサービスリクエストが停止されます。</li> <li>• アシュアランス UI 選択は期待どおりに動作します。</li> </ul>

ユーザアクションの必要性	障害シナリオ	HA の動作
Yes	2つのノードで障害が発生するか、到達不能です。	



ユーザアクションの必要性	障害シナリオ	HA の動作
		<p>クラスタが破損していて、接続が復元されるまで UI にアクセスできません。</p> <ul style="list-style-type: none"> <li>• ノードが回復すると、動作が再開され、クラスタメンバーによって共有されるデータが同期されます。</li> <li>• ノードが回復しない場合は、次の手順を実行する必要があります。 <ol style="list-style-type: none"> <li>1. シードノードを復元します。 <ul style="list-style-type: none"> <li>• 第 1 世代アプライアンスを設定する場合は、『<a href="#">Cisco DNA Center 第 1 世代アプライアンス インストール ガイド</a>』のトピック「Configure Master Node」を参照してください。</li> <li>• 第 2 世代アプライアンスを設定する場合は、『<a href="#">Cisco Digital Network Architecture Center 第 2 世代アプライアンス インストール ガイド</a>』の使用する設定ウィザードとアプライアンスのタイプに固有のトピックを参照してください。 <ul style="list-style-type: none"> <li>• Maglev 構成ウィザードを使用してアプライアンスを設定する場合は、トピック「Configure the Master Node Using the Maglev Wizard」を参照してください。</li> <li>• ブラウザベースの設定ウィザードを使用して 44 または 56 コアアプライアンスを設定する場合は、「ブラウザベースウィザードを使用した 44 または 56 コアアプライアンスの設定」の章のトピック「ブラウザベースウィザードを使用したマスターノードの設定Configure the Master Node Using the Browser-Based Wizard」を参照してください。</li> </ul> </li> </ul> </li> <li>2. 他のクラスタノードの復元： <ul style="list-style-type: none"> <li>• 第 1 世代アプライアンスを設定する場合は、『<a href="#">Cisco DNA Center 第 1 世代アプライアンス インストール ガイド</a>』のトピック「Configure Add-on Nodes」を参照してください。</li> <li>• 第 2 世代アプライアンスを設定する場合は、『<a href="#">Cisco Digital Network Architecture Center 第 2 世代アプライアンス インストール ガイド</a>』の使用する設定ウィザードとアプライアンスのタイプに固有のトピックを参照してください。 <ul style="list-style-type: none"> <li>• Maglev 構成ウィザードを使用してアプライアンスを設定する場合は、トピック「Configure Add-On Nodes Using the Maglev Wizard」を参照してください。</li> <li>• ブラウザベースの設定ウィザードを使用して 44 または 56 コアアプライアンスを設定する場合は、「ブラウザベースウィザードを使用した 44 または 56 コアアプライアンスの設定」</li> </ul> </li> </ul> </li> </ol> </li> </ul>

ユーザアクションの必要性	障害シナリオ	HA の動作
		<p>の章のトピック「Configure Add-On Nodes Using the Browser-Based Wizard」を参照してください。</p>
Yes	<p>ノードに障害が発生し、クラスタから削除する必要がある。</p>	<p><a href="#">失敗したクラスタノードの回復 (8 ページ)</a> で説明されているタスクを実行して、障害が発生したクラスタノードを削除してから復元します。</p>
なし	<p>すべてのノードが相互の接続を失う。</p>	<p>接続が復元されるまで UI にアクセスできません。接続が復元されると、動作が再開され、クラスタメンバーによって共有されるデータが同期されます。</p>
Yes	<p>バックアップがスケジュールされ、ハードウェア障害が原因でシードノードがダウンする。</p>	<p>次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. 各ノードで次のコマンドを実行し、すべてのクラスタノードを削除します。 <b>maglev node remove node's-IP-address</b></li> <li>2. 交換用ノードと、新しいノードをクラスタに参加させるためのサポートについては、Cisco TAC にお問い合わせください。</li> </ol>
Yes	<p>UI の赤色のバナーで、ノードがダウンしていることが示されます。「アシュアランスサービスは現在ダウンしています。ホスト &lt;IP-address&gt; との接続が失われています。(services are currently down. Connectivity with host &lt;IP_address&gt; has been lost.)」</p>	<p>シードノードがダウンし、アシュアランス データが失われたことがバナーで示されます。シードノードが復帰すると、アシュアランス機能が復元されます。ただし、障害がハードウェア障害に関連している場合は、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. 障害が発生したシードノードを削除します。 <a href="#">失敗したシードノードの削除 (9 ページ)</a> を参照してください。</li> <li>2. 新しいノードを追加し、障害が発生したノードを置き換えます。 <a href="#">新しいシードノードの追加 (10 ページ)</a> を参照してください。</li> </ol>
Yes	<p>UI の赤色のバナーでノードがダウンしていることが示されるが、最終的に「この IP アドレスはダウンしています。(This IP address is down.)」というメッセージで黄色に変更される。</p>	<p>システムは引き続き使用できます。ノードがダウンしている理由を調査し、バックアップします。</p>

ユーザアクションの必要性	障害シナリオ	HA の動作
Yes	クラスタのアップグレード中に障害が発生する。	<p>次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. 各ノードで次のコマンドを実行し、すべてのクラスタノードを削除します。 <b>maglev node remove node's-IP-address</b></li> <li>2. シードノードを復元します。 <ul style="list-style-type: none"> <li>• 第1世代アプライアンスを設定する場合は、『<a href="#">Cisco DNA Center 第1世代アプライアンスインストールガイド</a>』の「Configure Master Node」を参照してください。</li> <li>• 第2世代アプライアンスを設定する場合は、『<a href="#">Cisco Digital Network Architecture Center 第2世代アプライアンスインストールガイド</a>』の使用する設定ウィザードとアプライアンスのタイプに固有のトピックを参照してください。 <ul style="list-style-type: none"> <li>• Maglev 構成ウィザードを使用してアプライアンスを設定する場合は、トピック「Configure the Master Node Using the Maglev Wizard」を参照してください。</li> <li>• ブラウザベースの設定ウィザードを使用して 44 または 56 コアアプライアンスを設定する場合は、「ブラウザベースウィザードを使用した 44 または 56 コアアプライアンスの設定」の章のトピック「Configure the Master Node Using the Browser-Based Wizard」を参照してください。</li> </ul> </li> </ul> </li> <li>3. 他のクラスタノードの復元。 <ul style="list-style-type: none"> <li>• 第1世代アプライアンスを設定する場合は、『<a href="#">Cisco DNA 第1世代アプライアンスインストールガイド</a>』のトピック「Configure Add-on Nodes」を参照してください。</li> <li>• 第2世代アプライアンスを設定する場合は、『<a href="#">Cisco Digital Network Architecture Center 第2世代アプライアンスインストールガイド</a>』の使用する設定ウィザードとアプライアンスのタイプに固有のトピックを参照してください。 <ul style="list-style-type: none"> <li>• Maglev 構成ウィザードを使用してアプライアンスを設定する場合は、トピック「Configure Add-On Nodes Using the Maglev Wizard」を参照してください。</li> <li>• ブラウザベースの設定ウィザードを使用して 44 または 56 コアアプライアンスを設定する場合は、「ブラウザベースウィザードを使用した 44 または 56 コアアプライアンスの設定」の章のトピック「Configure Add-On Nodes Using the Browser-Based Wizard」を参照してください。</li> </ul> </li> </ul> </li> </ol>

ユーザアクションの必要性	障害シナリオ	HA の動作
なし	アプライアンスポートに障害が発生する。	<ul style="list-style-type: none"> <li>• クラスタポート : Cisco DNA Center は 5 分以内に障害を検出し、ユーザをタイムアウトします。5 分後、再度ログインできるはずですが、バナーが表示され、現在使用できないサービスが示されます。サービスフェールオーバーは 10 分以内に完了します。アクセスできる UI の領域は、復元されたサービスによって異なります。使用できなかったサービスが完全に復元されると、バナーが閉じます。</li> <li>• エンタープライズポート : Cisco DNA Center がネットワークに到達して管理することができない可能性があります。</li> <li>• 管理ポート : 現在進行中のアップグレードとイメージのダウンロードは失敗し、ノースバウンドインターフェイスの操作も影響を受けます。</li> </ul>
Yes	アプライアンスハードウェアに障害が発生する。	<p>障害が発生したハードウェアコンポーネント（ファン、電源装置、ディスクドライブなど）を交換します。これらのコンポーネントに属する複数のインスタンスがアプライアンスで検出されるため、1 つのコンポーネントの障害は一時的に許容される可能性があります。</p> <p>RAID コントローラは新しく追加されたディスクドライブをアプライアンス上の他のドライブと同期するため、これが起きている間は I/O システムのパフォーマンスが低下する可能性があります。</p>

---

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.