

---

# **CLUSTER**PRO

**CLUSTERPRO X 5.2**

**Google Cloud 向け HA クラスタ 構築ガイド (Linux)**

リリース 2

日本電気株式会社

2024 年 07 月 12 日



# 目次:

|       |  |    |
|-------|--|----|
| 第 1 章 | はじめに                                   | 1  |
| 1.1   | 対象読者と目的                                | 1  |
| 1.2   | 適用範囲                                   | 2  |
| 1.3   | 本書の構成                                  | 3  |
| 1.4   | CLUSTERPRO マニュアル体系                     | 4  |
| 1.5   | 本書の表記規則                                | 5  |
| 1.6   | 最新情報の入手先                               | 6  |
| 第 2 章 | 概要                                     | 7  |
| 2.1   | 機能概要                                   | 7  |
| 2.2   | 基本構成                                   | 9  |
| 2.3   | ネットワークパーティション解決                        | 16 |
| 2.4   | オンプレミスと Google Cloud の違い               | 17 |
| 第 3 章 | 動作環境                                   | 19 |
| 3.1   | Cloud DNS を使用した HA クラスターの場合            | 19 |
| 第 4 章 | 構築手順 (内部 TCP ロードバランサを使用した HA クラスターの場合) | 21 |
| 4.1   | 構築例について                                | 21 |
| 4.2   | Google Cloud の設定                       | 27 |
| 4.3   | CLUSTERPRO の設定                         | 30 |
| 4.4   | 動作確認                                   | 34 |
| 第 5 章 | 構築手順 (Cloud DNS を使用した HA クラスターの場合)     | 35 |
| 5.1   | 構築例について                                | 35 |
| 5.2   | Google Cloud の設定                       | 39 |
| 5.3   | CLUSTERPRO の設定                         | 42 |
| 5.4   | 動作確認                                   | 46 |
| 第 6 章 | エラーメッセージ一覧                             | 47 |
| 第 7 章 | 注意・制限事項                                | 49 |
| 7.1   | ロードバランサを使用した HA クラスターの場合               | 49 |
| 7.2   | Cloud DNS を使用した HA クラスターの場合            | 51 |

|       |                |    |
|-------|----------------|----|
| 第 8 章 | 免責・法的通知        | 53 |
| 8.1   | 免責事項 . . . . . | 53 |
| 8.2   | 商標情報 . . . . . | 54 |
| 第 9 章 | 改版履歷           | 55 |

# 第 1 章

## はじめに

### 1.1 対象読者と目的

本書は、クラスタシステムに関して、システムを構築する管理者、およびユーザサポートを行うシステムエンジニア、保守員を対象にしています。

ここでご紹介するソフトウェアや設定例は、あくまで参考情報としてご提供するものであり、各ソフトウェアの動作保証を行うものではありません。

## 1.2 適用範囲

動作環境については「スタートアップガイド」-「CLUSTERPRO の動作環境」を参照してください。

本書に記載した各製品・サービスのスクリーンショット等は執筆時点のものであり、それ以降に変更されている可能性があります。最新の情報はそれぞれの **Web** サイトやマニュアルを参照してください。

## 1.3 本書の構成

- 「2. 概要」: 機能の概要について説明します。
- 「3. 動作環境」: 本機能の動作確認済み環境を説明します。
- 「4. 構築手順 (内部 TCP ロードバランサを使用した HA クラスタの場合)」: 内部 TCP ロードバランサを使用した HA クラスタの構築手順について説明します。
- 「5. 構築手順 (Cloud DNS を使用した HA クラスタの場合)」: Cloud DNS を使用した HA クラスタの構築手順について説明します。
- 「6. エラーメッセージ一覧」: エラーメッセージと対処について説明します。
- 「7. 注意・制限事項」: 構築時、運用時の注意事項について説明します。

## 1.4 CLUSTERPRO マニュアル体系

CLUSTERPRO のマニュアルは、以下の 5 つに分類されます。各ガイドのタイトルと役割を以下に示します。

### 『CLUSTERPRO X スタートアップガイド』 (Getting Started Guide)

すべてのユーザを対象読者とし、製品概要、動作環境、アップデート情報、既知の問題などについて記載します。

### 『CLUSTERPRO X インストール&設定ガイド』 (Install and Configuration Guide)

CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアと、クラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO を使用したクラスタシステム導入から運用開始前までに必須の事項について説明します。実際にクラスタシステムを導入する際の順番に則して、CLUSTERPRO を使用したクラスタシステムの設計方法、CLUSTERPRO のインストールと設定手順、設定後の確認、運用開始前の評価方法について説明します。

### 『CLUSTERPRO X リファレンスガイド』 (Reference Guide)

管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象とし、CLUSTERPRO の運用手順、各モジュールの機能説明およびトラブルシューティング情報等を記載します。『CLUSTERPRO X インストール&設定ガイド』を補完する役割を持ちます。

### 『CLUSTERPRO X メンテナンスガイド』 (Maintenance Guide)

管理者、および CLUSTERPRO を使用したクラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO のメンテナンス関連情報を記載します。

### 『CLUSTERPRO X ハードウェア連携ガイド』 (Hardware Feature Guide)

管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象読者とし、特定ハードウェアと連携する機能について記載します。『CLUSTERPRO X インストール&設定ガイド』を補完する役割を持ちます。



## 1.5 本書の表記規則

本書では、注意すべき事項、重要な事項および関連情報を以下のように表記します。

---

**注釈:** この表記は、重要ではあるがデータ損失やシステムおよび機器の損傷には関連しない情報を表します。

---



---

**重要:** この表記は、データ損失やシステムおよび機器の損傷を回避するために必要な情報を表します。

---

**参考:**

この表記は、参照先の情報の場所を表します。

また、本書では以下の表記法を使用します。

| 表記                 | 使用方法  | 例  |
|--------------------|---|--|
| [ ] 角かっこ           | コマンド名の前後<br>画面に表示される語 (ダイアログボックス、メニューなど) の前後                | [スタート] をクリックします。<br>[プロパティ] ダイアログ ボックス         |
| コマンドライン中の [ ] 角かっこ | かっこ内の値の指定が省略可能であることを示します。                                   | <code>clpstat -s[-h host_name]</code>          |
| #                  | Linux ユーザが、root でログインしていることを示すプロンプト                         | # <code>clpstat</code>                         |
| モノスペースフォント         | パス名、コマンドライン、システムからの出力 (メッセージ、プロンプトなど)、ディレクトリ、ファイル名、関数、パラメータ | <code>/Linux</code>                            |
| 太字                 | ユーザが実際にコマンドラインから入力する値を示します。                                 | 以下を入力します。<br># <b><code>clpcl -s -a</code></b> |
| 斜体                 | ユーザが有効な値に置き換えて入力する項目  | # <code>ping &lt;IP アドレス&gt;</code>            |



本書の図では、CLUSTERPRO を表すために このアイコンを使用します。

## 1.6 最新情報の入手先

最新の製品情報については、以下の Web サイトを参照ください。

<https://jpn.nec.com/clusterpro/>

## 第 2 章

# 概要

### 2.1 機能概要

本書では、Google Cloud のクラウド サービス上に、CLUSTERPRO X(以下、CLUSTERPRO と記す)による HA クラスターを構築する方法を説明します。

Google Cloud において、リージョンやゾーンを使用し仮想マシンを HA クラスター化することで、業務の可用性を高めることができます。

- リージョン

Google Cloud ではリージョンと呼ばれる物理的および論理的な単位に分割されます (たとえば東京、大阪など)。

1 つのリージョン内にすべてのノードを構築することも可能ですが、ネットワーク障害や自然災害などによりすべてのノードがダウンし業務を継続できなくなるおそれがあります。

そこで、ノードを複数のリージョンに分散させて配置することにより、可用性を高めることができます。

リージョンはゾーンの集まりです。

- ゾーン

Google Cloud では、ゾーンと呼ばれる論理的なグループに各ノードを配置できます。

異なるゾーンに各ノードを配置することで、Google Cloud の計画済みメンテナンスや物理ハードウェアの障害などの計画外メンテナンスによる影響を最小限に抑えることが可能です。

リージョン、ゾーンについては以下を参照してください。

## CLUSTERPRO X 5.2

### Google Cloud 向け HA クラスター構築ガイド (Linux), リリース 2

---

リージョンとゾーン:

<https://cloud.google.com/compute/docs/regions-zones/>

## 2.2 基本構成

本書では、ロードバランサを使用した HA クラスタ、Cloud DNS を使用した HA クラスタ、の 2 種類の HA クラスタを想定しています (いずれも片方向スタンバイクラスタの構成)。

それぞれの HA クラスタについて、選択する CLUSTERPRO のリソース、必要な Google Cloud のサービスは以下のとおりです。

| 用途                           | 選択する CLUSTERPRO のリソース   | 必要な Google Cloud のサービス |
|------------------------------|-------------------------|------------------------|
| 仮想 IP アドレスでクライアントからアクセスしたい場合 | Google Cloud 仮想 IP リソース | 内部 TCP 負荷分散            |
| DNS 名でクライアントからアクセスしたい場合      | Google Cloud DNS リソース   | Cloud DNS              |

### ロードバランサを使用した HA クラスタ

クライアントアプリケーションは、Google Cloud 環境の仮想マシンに対して、仮想 IP アドレス (以下、VIP と記載) を使用してクラスタを構成するノードに接続することができます。VIP アドレスを使用することにより、フェイルオーバーまたは、グループの移動が発生しても、クライアントは、仮想マシンの切り替えを意識する必要がありません。

図 2.1 内部 TCP ロードバランサを使用した HA クラスタの Google Cloud 環境上に構築したクラスタには、Google Cloud のロードバランサ (Cloud Load Balancing) の VIP (Cloud Load Balancing のフロントエンド IP) を指定してアクセスします。

クラスタの現用系と待機系は、Google Cloud のロードバランサにおけるヘルスチェックを利用して切り替えます。ヘルスチェックには Google Cloud 仮想 IP リソースが提供するポートを利用します。

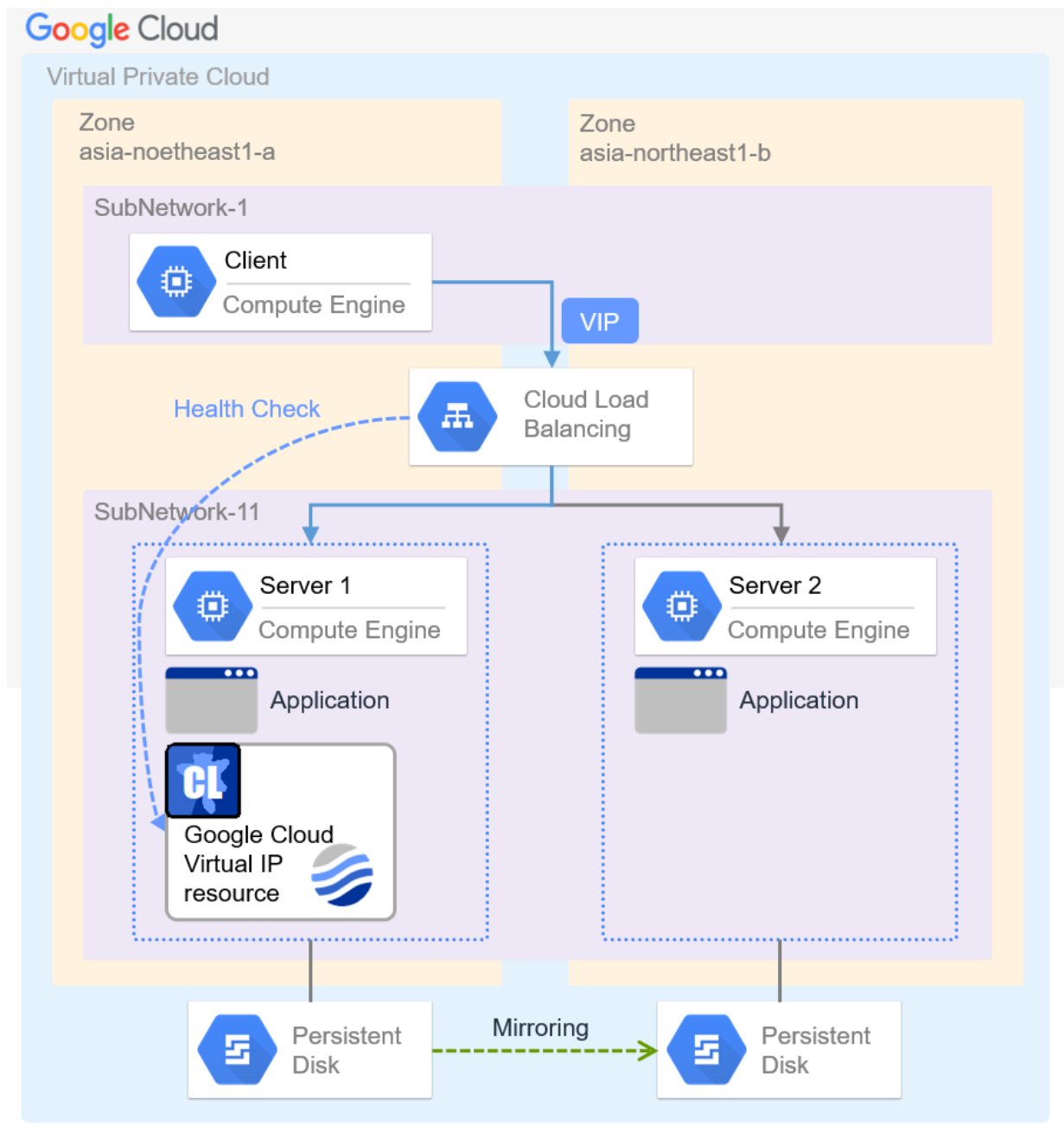


図 2.1 内部 TCP ロードバランサを使用した HA クラスタ

|                          |              |
|--------------------------|--------------|
| SubNetwork-1             | 10.0.1.0/24  |
| IP Address (Client)      | 10.0.1.200   |
| Virtual IP Address (VIP) | 10.0.1.100   |
| SubNetwork-11            | 10.0.11.0/24 |

次のページに続く

表 2.2 – 前のページからの続き

|                      |             |
|----------------------|-------------|
| IP Address (Server1) | 10.0.11.101 |
| IP Address (Server2) | 10.0.11.102 |
| Health Check Port    | 12345       |

Cloud Load Balancing については以下を参照してください。

Cloud Load Balancing:

<https://cloud.google.com/load-balancing/>

ロードバランサを使用した HA クラスタの構成例としては以下があります。

| 用途                                 | 使用するロードバランサ    | 構築手順  |
|------------------------------------|----------------|---|
| 業務を Google Cloud のネットワークの内部に公開する場合 | 内部 TCP ロードバランサ | 本書「4. 構築手順 (内部 TCP ロードバランサを使用した HA クラスタの場合)」参照。 |

ロードバランサを使用した HA クラスタ構成において必要なリソース、モニタリソースは以下のとおりです。

本書ではネットワークパーティション解決リソースを設定していませんが、「2.3. ネットワークパーティション解決」を参照し、お客様のシステム構成により決定してください。

| リソース/モニタリソース種別              | 説明   | 設定 |
|-----------------------------|--|----|
| Google Cloud 仮想 IP リソース     | <p>業務が稼働するノードの特定のポートでロードバランサからの死活監視(ヘルスチェック用のポートへのアクセス)を待ち受ける仕組みを提供します。</p> <p>活性時に Google Cloud のロードバランサからの死活監視を待ち受けるための制御プロセスを起動します。</p> <p>非活性時には死活監視を待ち受けるための制御プロセスを停止します。</p> | 必須 |
| Google Cloud 仮想 IP モニタリソース  | Google Cloud 仮想 IP リソースが起動しているノードに対して、Google Cloud 仮想 IP リソース活性時に起動する制御プロセスの死活監視を行います。   | 必須 |
| Google Cloud ロードバランサモニタリソース | Google Cloud 仮想 IP リソースが起動していないノードに対して、ヘルスチェック用ポートと同じポート番号が開放されていないかを監視します。  | 必須 |
| その他のリソース、モニタリソース            | ミラーディスクなど、HA クラスタで運用するアプリケーションの構成に従います。  | 任意 |

### Cloud DNS を使用した HA クラスタ

本構成では、DNS 名でアクセス可能とするために Cloud DNS を使用しています。

また、Google Cloud の計画済みメンテナンスや物理ハードウェアの障害などの計画外メンテナンスによる影響を最小限に抑えるために、2 台の仮想マシンで異なるゾーンに配置しています。

図 2.2 Cloud DNS を使用した HA クラスタのクラスタには、DNS 名を指定してアクセスします。

CLUSTERPRO は、DNS 名から設定した IP アドレスが得られるように Cloud DNS のレコードセット (A レコード) の制御を行います。

フェイルオーバーまたはグループの移動が発生しても、クライアントは仮想マシンの切り替えを意識する必要がありません。



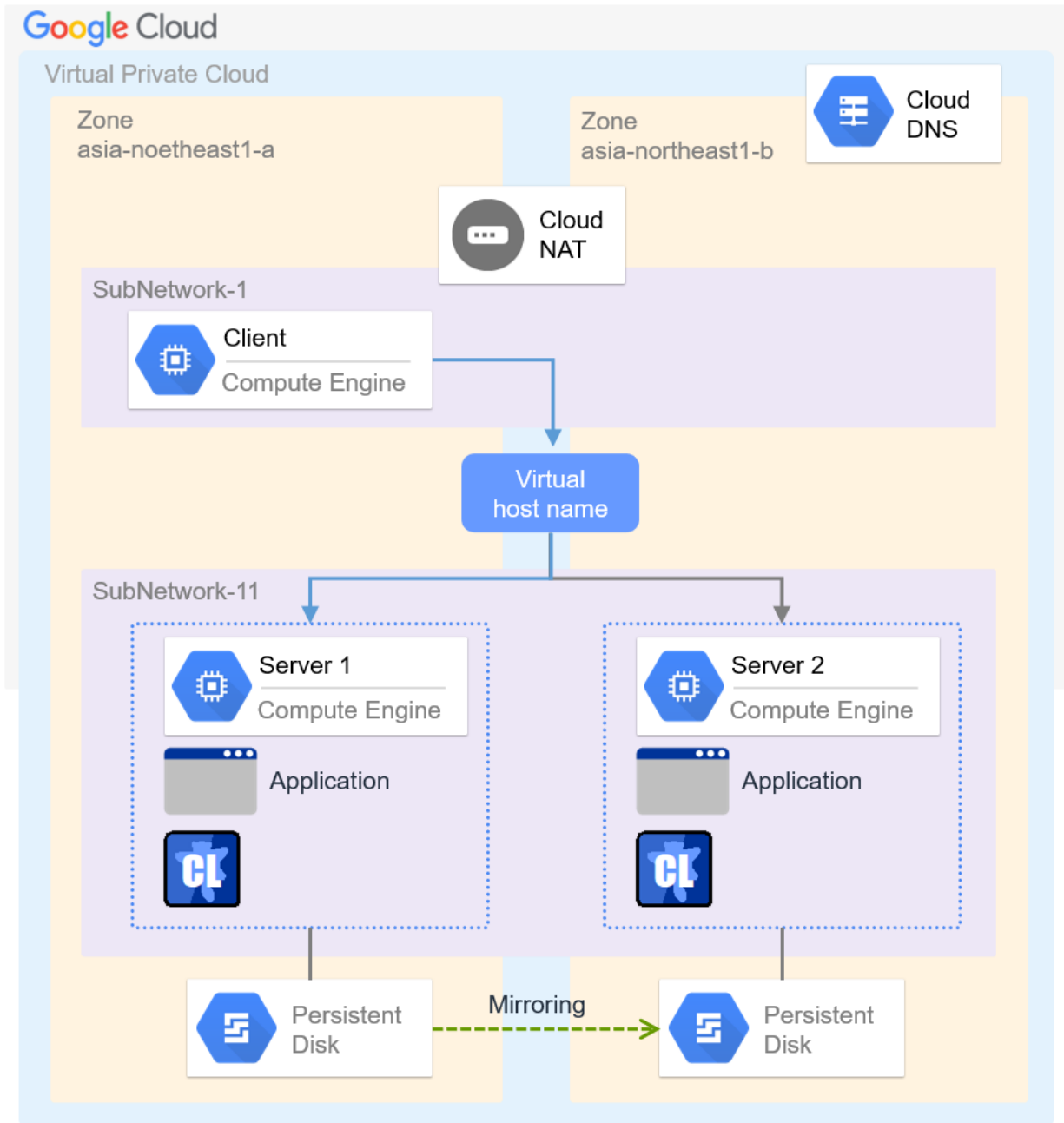


図 2.2 Cloud DNS を使用した HA クラスタ

|                      |              |
|----------------------|--------------|
| SubNetwork-1         | 10.0.1.0/24  |
| IP Address (Client)  | 10.0.1.200   |
| SubNetwork-11        | 10.0.11.0/24 |
| IP Address (Server1) | 10.0.11.101  |

次のページに続く

表 2.5 – 前のページからの続き

|                      |                          |
|----------------------|--------------------------|
| IP Address (Server2) | 10.0.11.102              |
| Virtual host name    | test-cluster.example.com |

## 1. レコード書き換え前 (Cloud DNS)

| Name                     | Type | Data        |
|--------------------------|------|-------------|
| test-cluster.example.com | A    | 10.0.11.101 |

## 2. レコード書き換え後 (Cloud DNS)

| Name                     | Type | Data        |
|--------------------------|------|-------------|
| test-cluster.example.com | A    | 10.0.11.102 |

本書では VPC ネットワーク内の HA クラスタを構成するインスタンスがインターネットへアクセスできる構成について記載しています。

これは、HA クラスタを構成するインスタンスが Google Cloud DNS リソースが利用する gcloud CLI を実行する際に、インターネットへアクセスする必要があるためです。

インターネットへのアクセスには、NAT ゲートウェイや NAT インスタンスを使用する方法があります。本書では NAT ゲートウェイ (Cloud NAT) を使用します。

VPC ネットワークの作成手順や NAT ゲートウェイ/NAT インスタンスの設定、ファイアウォールルールの設定の詳細は、Google Cloud のドキュメントをご参照ください。

Cloud DNS を使用した HA クラスタ構成において必要なリソース、モニタリソースは以下のとおりです。

本書ではネットワークパーティション解決リソースを設定していませんが、「ネットワークパーティション解決」を参照し、お客様のシステム構成により決定してください。

| リソース/モニタリソース種別        | 説明   | 設定 |
|-----------------------|--|----|
| Google Cloud DNS リソース | DNS 名 から設定した IP アドレスを得られるように Cloud DNS のレコードセット (A レコード) の制御を行います。 | 必須 |

次のページに続く

表 2.8 – 前のページからの続き

| リソース/モニタリソース<br>種別           | 説明   | 設定 |
|------------------------------|--|----|
| Google Cloud DNS モニタ<br>リソース | 活性時監視の対象リソースに指定された Google Cloud DNS リソースが制御するレコードセット (A レコード) が、Google Cloud DNS 上に存在することを確認します。 | 必須 |
| その他のリソース、モニタ<br>リソース         | ミラーディスクなど、HA クラスタで運用するアプリケーションの構成に従います。  | 任意 |

## 2.3 ネットワークパーティション解決

HA クラスタを構成している仮想マシンは、お互いにハートビートによって死活監視を行っています。

各仮想マシンが異なるサブネットに分散している構成においては、ハートビートが途絶えた時に、サービスの二重起動など望ましくない状態が発生します。

サービスの二重起動を回避するために、他の仮想マシンがダウンしたか、自身がネットワークから孤立した状態 (ネットワークパーティション状態。以下、NP 状態と記す) かのどちらであるかを区別する必要があります。

ネットワークパーティション解決 (以下、NP 解決と記す) は、Ping などの応答を返却可能な常時稼働している装置 (応答確認先) に対して Ping 確認を行い、応答がない場合は NP 状態が発生したと判断し、設定された処理 (警告、回復処理、サーバダウン処理など) を行います。

クラスタシステムにアクセスするクライアントの配置やオンプレミス環境との接続条件 (専用線接続など) によって、NP 解決先や NP 解決の方法はその都度検討する必要があります。

推奨の NP 解決先や NP 解決の方法はありません。

NP 解決については、以下を参照してください。

- 『インストール&設定ガイド』 - 「ネットワークパーティション解決リソースを理解する」
- 『リファレンスガイド』 - 「ハートビートリソースの詳細」
- 『リファレンスガイド』 - 「ネットワークパーティション解決リソースの詳細」

## 2.4 オンプレミスと Google Cloud の違い

オンプレミスと Google Cloud における CLUSTERPRO の機能差分は以下のとおりです。表内の ✓ は機能が使用できることを意味し、n/a は機能が使用できないことを意味します。

| 機能                           | オンプレミス | Google Cloud |
|------------------------------|--------|--------------|
| 共有ディスク型クラスタの構築可否             | ✓      | n/a          |
| ミラーディスク型クラスタの構築可否            | ✓      | ✓            |
| 管理用グループの使用可否                 | ✓      | n/a          |
| フローティング IP リソースの使用可否         | ✓      | n/a          |
| 仮想 IP リソースの使用可否              | ✓      | n/a          |
| Google Cloud 仮想 IP リソースの使用可否 | n/a    | ✓            |
| Google Cloud DNS リソースの使用可否   | n/a    | ✓            |

オンプレミス環境と Google Cloud 環境でクラスタを構築する作業手順の違いは、事前準備として Google Cloud の設定が必要であることを除き、違いはありません。



## 第 3 章

# 動作環境

### 3.1 Cloud DNS を使用した HA クラスターの場合

以下のマニュアルを参照してください。

- 『スタートアップガイド』 - 「CLUSTERPRO の動作環境」 - 「Google Cloud DNS リソース、Google Cloud DNS モニタリソースの動作環境」





## 第 4 章

# 構築手順 (内部 TCP ロードバランサを使用した HA クラスターの場合)

### 4.1 構築例について

本書では、Google Cloud において、CLUSTERPRO を使用した 2 ノードでの片方向スタンバイクラスターの構築手順を紹介します。

Google Cloud 上の同じ VPC ネットワーク内のクライアントからアクセス可能な HA クラスターを構築します。

本手順は、server1 を現用系サーバとしたミラーディスク型の構成を対象としています。

以下の表は既定値が存在しないパラメータ、および既定値から変更したパラメータについて記載しています。

ファイアウォールルールの [IP 範囲] は、Google Cloud ヘルスチェックシステム (130.211.0.0/22, 35.191.0.0/16) からの通信を許可するために必要です。

- Google Cloud の設定 (server1、server2 で共通の設定)

| 設定項目                 | 設定値                         |
|----------------------|-----------------------------|
| <b>VPC ネットワークの設定</b> |                             |
| - 名前                 | test-vpc                    |
| - 新しいサブネット 名前        | subnetwork-1, subnetwork-11 |

次のページに続く

表 4.1 – 前のページからの続き

| 設定項目                 | 設定値                           |
|----------------------|-------------------------------|
| - 新しいサブネット リージョン     | asia-northeast1               |
| - 新しいサブネット IP アドレス範囲 | 10.0.1.0/24, 10.0.11.0/24     |
| ファイアウォールルールを設定       |                               |
| - 名前                 | test-allow-health-check       |
| - ネットワーク             | test-vpc                      |
| - トラフィックの方向          | 上り                            |
| - 一致したときのアクション       | 許可                            |
| - ターゲット              | 指定されたターゲットタグ                  |
| - ターゲットタグ            | test-allow-health-check       |
| - ソースフィルタ            | IP 範囲                         |
| - ソース IP の範囲         | 130.211.0.0/22, 35.191.0.0/16 |
| - 指定したプロトコルとポート      | すべて許可                         |
| ロードバランサの設定           |                               |

次のページに続く

表 4.1 – 前のページからの続き

| 設定項目                   | 設定値                  |
|------------------------|----------------------|
| - 種類                   | TCP 負荷分散             |
| - インターネット接続または内部専用     | VM 間のみ               |
| - マルチリージョンまたはシングルリージョン | シングルリージョンのみ          |
| - 名前                   | test-lb              |
| ロードバランサの設定 (バックエンドの設定) |                      |
| - リージョン                | asia-northeast1      |
| - ネットワーク               | test-vpc             |
| - インスタンスグループ           | test-ig-a, test-ig-b |
| - ヘルスチェック 名前           | test-health-check    |
| - ヘルスチェック プロトコル        | TCP                  |
| - ヘルスチェック ポート          | 12345                |
| - ヘルスチェック プロキシのプロトコル   | なし                   |
| - セッションアフィニティ          | なし                   |

次のページに続く

表 4.1 – 前のページからの続き

| 設定項目                    | 設定値                |
|-------------------------|--------------------|
| ロードバランサの設定 (フロントエンドの設定) |                    |
| – 名前                    | test-frontend      |
| – サブネットワーク              | subnetwork-1       |
| – 内部 IP                 | 10.0.1.100         |
| – ポート                   | 80(業務を提供しているポート番号) |

- Google Cloud の設定 (server1、server2 でそれぞれ設定)

| 設定項目          | 設定値                |                    |
|---------------|--------------------|--------------------|
|               | server1            | server2            |
| インスタンスの設定     |                    |                    |
| – リージョン       | asia-northeast1    | asia-northeast1    |
| – ゾーン         | asia-northeast1-a  | asia-northeast1-b  |
| – 新しいディスク     | server1-datadisk-0 | server2-datadisk-0 |
| インスタンスグループの設定 |                    |                    |
| – 名前          | test-ig-a          | test-ig-b          |
| – グループタイプ     | 非マネージド インスタンス グループ | 非マネージド インスタンス グループ |

次のページに続く

表 4.2 – 前のページからの続き

| 設定項目         | 設定値               |                   |
|--------------|-------------------|-------------------|
|              | server1           | server2           |
| - リージョン      | asia-northeast1   | asia-northeast1   |
| - ゾーン        | asia-northeast1-a | asia-northeast1-b |
| - ネットワーク     | test-vpc          | test-vpc          |
| - サブネットワーク   | subnetwork-11     | subnetwork-11     |
| - VM インスタンス  | server1           | server2           |
| ネットワークの設定    |                   |                   |
| - ネットワーク     | test-vpc          | test-vpc          |
| - サブネットワーク   | subnetwork-11     | subnetwork-11     |
| - 内部 IP アドレス | 10.0.11.101       | 10.0.11.102       |

- CLUSTERPRO の設定 (クラスタプロパティ)

| 設定項目    | 設定値      |          |
|---------|----------|----------|
|         | server1  | server2  |
| - クラスタ名 | Cluster1 | Cluster1 |
| - サーバ名  | server1  | server2  |

• CLUSTERPRO の設定 (フェイルオーバーグループ)

| リソース名                   | 設定項目                    | 設定値                      |
|-------------------------|-------------------------|--------------------------|
| ミラーディスクリソース             | リソース名                   | mdl                      |
| ミラーディスクリソース             | 詳細タブ - ミラーパーティションデバイス名  | /dev/NMP1                |
| ミラーディスクリソース             | 詳細タブ - マウントポイント         | /mnt/md1                 |
| ミラーディスクリソース             | 詳細タブ - データパーティションデバイス名  | /dev/sdb2                |
| ミラーディスクリソース             | 詳細タブ - クラスタパーティションデバイス名 | /dev/sdb1                |
| ミラーディスクリソース             | 詳細タブ - ファイルシステム         | ext4                     |
| Google Cloud 仮想 IP リソース | リソース名                   | gcvip1                   |
| Google Cloud 仮想 IP リソース | ポート番号                   | 12345(ヘルスチェック ポートで指定した値) |

• CLUSTERPRO の設定 (モニタリソース)

| モニタリソース名                    | 設定項目     | 設定値     |
|-----------------------------|----------|---------|
| ミラーディスクモニタリソース              | モニタリソース名 | mdw1    |
| ミラーディスクコネクタモニタリソース          | モニタリソース名 | mdnw1   |
| Google Cloud 仮想 IP モニタリソース  | モニタリソース名 | gcvipw1 |
| Google Cloud 仮想 IP モニタリソース  | 回復対象     | gcvip1  |
| Google Cloud ロードバランサモニタリソース | モニタリソース名 | gclbw1  |
| Google Cloud ロードバランサモニタリソース | 回復対象     | gcvip1  |

## 4.2 Google Cloud の設定

### 1. VPC ネットワークの作成

Google Cloud Console にアクセスします (<https://console.cloud.google.com/>)。

VPC ネットワーク、サブネットを作成します。

詳細な手順は以下を参照してください。

VPC ネットワークの使用:

<https://cloud.google.com/vpc/docs/using-vpc/>

### 2. インスタンスの作成

公開イメージから インスタンスを作成します。

また、インスタンス作成時にミラーディスク (クラスタパーティション、データパーティション) に使用するセカンダリ ディスクを追加します。

インスタンスはクラスタを構成する仮想マシン分作成します。

詳細な手順は以下を参照してください。

入門ガイド:

<https://cloud.google.com/compute/docs/how-to/>

### 3. インスタンスの設定

作成した server1、server2 へ接続し、ログインします。

詳細な手順は以下を参照してください。

インスタンスへの接続:

<https://cloud.google.com/compute/docs/instances/connecting-to-instance/>

次にミラーディスクリソース用のパーティションを設定します。

インスタンスに追加したセカンダリ ディスクにクラスタパーティションおよびデータパーティションを作成します。

ミラーディスクリソース用のパーティションの設定については、以下を参照してください。

- 『インストール&設定ガイド』 - 「システム構成を決定する」 - 「ハードウェア構成後の設定」 - 「ミラーディスクリソース用のパーティションを設定する (Replicator 使用時は必須)」

### 4. ファイアウォールルールの作成

ロードバランサからインスタンスへのヘルスチェックを行う Google Cloud ヘルスチェックシステム (130.211.0.0/22, 35.191.0.0/16) からの通信を許可するため、ファイアウォールルールを作成します。

また、ターゲットタグをインスタンス server1、server2 のネットワークタグに追加してください。

詳細な手順は以下を参照してください。

ファイアウォール ルールの使用:

<https://cloud.google.com/vpc/docs/using-firewalls/>

ヘルスチェックの作成:

<https://cloud.google.com/load-balancing/docs/health-checks/>

#### 5. インスタンス グループの作成

Cloud Load Balancing のバックエンドに指定するインスタンス グループを作成します。インスタンス server1、server2 を追加します。

詳細な手順は以下を参照してください。

非マネージド インスタンス グループの作成:

<https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances>

#### 6. ロードバランサの作成

ロードバランサを作成します。[TCP 負荷分散] を選択します。

詳細な手順は以下を参照してください。

ネットワーク負荷分散の設定:

<https://cloud.google.com/load-balancing/docs/network/setting-up-network/>

次にバックエンド、フロントエンドを設定します。

フロントエンドの [ポート] には業務を提供しているポート番号を設定します。

詳細な手順は以下を参照してください。

内部 TCP/UDP 負荷分散の設定:

<https://cloud.google.com/load-balancing/docs/internal/setting-up-internal>

#### 7. OS 起動時間の調整、ネットワーク設定の確認、ルートファイルシステムの確認、ファイアウォールの設定を確認、サーバの時刻を同期、SELinux の設定を確認

各手順は以下を参照してください。

- 『インストール&設定ガイド』 - 「システム構成を決定する」 - 「ハードウェア構成後の設定」

#### 8. CLUSTERPRO のインストール

インストール手順は以下を参照してください。インストール完了後、OS の再起動を行ってください。

- 『インストール&設定ガイド』

#### 9. CLUSTERPRO のライセンスを登録

ライセンス登録手順は以下を参照してください。



- 『インストール&設定ガイド』

## 4.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および接続方法は以下を参照してください。

- 『インストール&設定ガイド』 - 「クラスタ構成情報を作成する」

以下のリソース/モニタリソースを追加する手順を記述します。

- ミラーディスクリソース
- Google Cloud 仮想 IP リソース
- Google Cloud 仮想 IP モニタリソース
- Google Cloud ロードバランスモニタリソース

上記以外の設定は以下を参照してください。

- 『インストール&設定ガイド』
- 『リファレンスガイド』

### 1. クラスタの作成

最初に、クラスタ生成ウィザードを開始し、クラスタを構築します。

- クラスタの構築

1. Cluster WebUI にアクセスし、[クラスタ生成ウィザード] をクリックします。

2. クラスタ生成ウィザード] の [クラスタ] が表示されます。

[クラスタ名] に任意のクラスタ名を入力します。

[言語] を適切に選択します。[次へ] をクリックします。

3. [基本設定] が表示されます。

Cluster WebUI に接続したインスタンスがマスターサーバとして登録済みの状態で表示されます。

[追加] をクリックし、残りのインスタンスを追加します (インスタンスの内部 IP アドレスを指定します)。[次へ] をクリックします。

4. [インタコネクト] 画面が表示されます。

インタコネクトのために使用する IP アドレス (各インスタンスの内部 IP アドレス) を指定します。また、後で作成するミラーディスクリソースの通信経路として [MDC] に mdc1 を選択します。[次へ] をクリックします。

5. [NP 解決] 画面が表示されます。

何も指定せず [次へ] をクリックします。

### 2. グループリソースの追加

- グループの定義

フェイルオーバーグループを作成します。

1. [グループ一覧] 画面が表示されます。  
[追加] をクリックします。
2. [グループの定義] 画面が表示されます。  
[名前] にフェイルオーバーグループ名 (failover1) を設定します。[次へ] をクリックします。
3. [起動可能サーバ] 画面が表示されます。  
何も指定せず [次へ] をクリックします。
4. [グループ属性] 画面が表示されます。  
何も指定せず [次へ] をクリックします。
5. [グループリソース一覧] 画面が表示されます。  
以降の手順で、この画面でグループリソースを追加していきます。

- ミラーディスクリソース

ミラーディスクリソースを作成します。

詳細は以下を参照してください。

- 『リファレンスガイド』 - 「ミラーディスクリソースを理解する」

1. [グループリソース一覧] で [追加] をクリックします。
2. [グループのリソース定義 | failover1] 画面が開きます。  
[タイプ] ボックスでグループリソースのタイプ (ミラーディスクリソース) を選択し、[名前] ボックスにリソース名を入力します。[次へ] をクリックします。
3. [依存関係] 画面が表示されます。  
何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。  
[次へ] をクリックします。
5. [詳細] 画面が表示されます。  
[データパーティションデバイス名] [クラスタパーティションデバイス名] に 「3. インスタンスの設定」 で作成したパーティションのデバイス名を入力します。[マウントポイント]、[ファイルシステム] を入力します。[完了] をクリックして設定を終了します。

- Google Cloud 仮想 IP リソース

Google Cloud 上で CLUSTERPRO を利用する場合、業務が稼働するノードの特定のポートでロードバランサからの死活監視を待ち受ける仕組みを提供します。

Google Cloud 仮想 IP リソースの詳細は以下を参照してください。

- 『リファレンスガイド』 - 「Google Cloud 仮想 IP リソースを理解する」

1. [グループリソース一覧] で [追加] をクリックします。
2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (Google Cloud 仮想 IP リソース) を選択して、[名前] ボックスにリソース名を入力します。[次へ] をクリックします。
3. [依存関係] 画面が表示されます。何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [ポート] にロードバランサの設定 (バックエンドの設定) 時にヘルスチェックの [ポート] として指定した値を入力します。
6. [完了] をクリックします。

### 3. モニタリソースの追加

- Google Cloud 仮想 IP モニタリソース

Google Cloud 仮想 IP リソースが起動しているノードに対して、死活監視のためのポートの監視機構を提供します。

Google Cloud 仮想 IP リソースを 1 つ追加すると、Google Cloud 仮想 IP モニタリソースが 1 つ自動的に作成されます。

Google Cloud 仮想 IP モニタリソースの詳細は以下を参照してください。

- 『リファレンスガイド』 - 「Google Cloud 仮想 IP モニタリソースを理解する」

- Google Cloud ロードバランサモニタリソース

Google Cloud 仮想 IP リソースが起動していないノードに対して、ヘルスチェック用ポートと同じポート番号が開放されていないかの監視機構を提供します。

Google Cloud 仮想 IP リソースを 1 つ追加すると、Google Cloud ロードバランサモニタリソースが 1 つ自動的に作成されます。

Google Cloud ロードバランサモニタリソースの詳細は以下を参照してください。

- 『リファレンスガイド』 - 「Google Cloud ロードバランサモニタリソースを理解する」

#### 4. 設定の反映とクラスターの起動

以下を参照してください。

- 『インストール&設定ガイド』 - 「クラスターを生成するには」

## 4.4 動作確認

構築した環境が正常に動作するかを、監視異常を発生させフェイルオーバーグループがフェイルオーバーすることにより確認します。

既にクラスタが正常に起動している状態からの確認手順は以下のとおりです。

1. フェイルオーバーグループ (failover1) が、現用系ノードの server1 で起動します。  
Cluster WebUI [ステータス] タブにおいて failover1 が server1 で [起動済] になっていることを確認します。  
クライアントから、フロントエンドの IP アドレスにアクセスし、現用系ノードに接続できることを確認します。
2. Cluster WebUI のプルダウンより [操作モード] から [検証モード] に変更します。
3. Cluster WebUI [ステータス] タブにおいて gcvipw1 の [擬似障害発生] アイコンを選択します。
4. Google Cloud 仮想 IP リソース (gcvip1) が 3 回再活性化後に、フェイルオーバーグループ (failover1) が異常になり、ノード server2 へフェイルオーバーします。  
Cluster WebUI [ステータス] タブにおいて failover1 が server2 で [起動済] になっていることを確認します。  
また、ロードバランサのフロントエンドの IP アドレスに対してフェイルオーバー後も正常にアクセスできることを確認します。

以上で、擬似障害の場合におけるフェイルオーバーの動作確認は完了です。その他の障害発生時の動作確認については適宜実施してください。

## 第 5 章

# 構築手順 (Cloud DNS を使用した HA クラスターの場合)

### 5.1 構築例について

本書では、Google Cloud において、CLUSTERPRO を使用した 2 ノードでの片方向スタンバイクラスターの構築手順を紹介します。

Google Cloud 上の同じ VPC ネットワーク内のクライアントからアクセス可能な HA クラスターを構築します。

本手順は、server1 を現用系サーバとしたミラーディスク型の構成を対象としています。

以下の表は既定値が存在しないパラメータ、および既定値から変更したパラメータについて記載しています。

- Google Cloud の設定 (server1、server2 で共通の設定)

| 設定項目                 | 設定値                         |
|----------------------|-----------------------------|
| <b>VPC ネットワークの設定</b> |                             |
| - 名前                 | test-vpc                    |
| - 新しいサブネット 名前        | subnetwork-1, subnetwork-11 |
| - 新しいサブネット リージョン     | asia-northeast1             |

次のページに続く

表 5.1 – 前のページからの続き

| 設定項目                          | 設定値                       |
|-------------------------------|---------------------------|
| - 新しいサブネット IP アドレス範囲          | 10.0.1.0/24, 10.0.11.0/24 |
| <b>CloudDNS の設定 (DNS ゾーン)</b> |                           |
| - ゾーンの種類                      | 非公開                       |
| - ゾーン名                        | test-zone                 |
| - DNS 名                       | example.com               |
| - オプション                       | デフォルト (限定公開)              |
| - ネットワーク                      | test-vpc                  |

- Google Cloud の設定 (server1、server2 でそれぞれ設定)

| 設定項目      | 設定値                |                    |
|-----------|--------------------|--------------------|
|           | server1            | server2            |
| インスタンスの設定 |                    |                    |
| - リージョン   | asia-northeast1    | asia-northeast1    |
| - ゾーン     | asia-northeast1-a  | asia-northeast1-b  |
| - 新しいディスク | server1-datadisk-0 | server2-datadisk-0 |
| ネットワークの設定 |                    |                    |

次のページに続く



表 5.2 – 前のページからの続き

| 設定項目         | 設定値           |               |
|--------------|---------------|---------------|
|              | server1       | server2       |
| - ネットワーク     | test-vpc      | test-vpc      |
| - サブネットワーク   | subnetwork-11 | subnetwork-11 |
| - 内部 IP アドレス | 10.0.11.101   | 10.0.11.102   |

- CLUSTERPRO の設定 (クラスタプロパティ)

| 設定項目    | 設定値      |          |
|---------|----------|----------|
|         | server1  | server2  |
| - クラスタ名 | Cluster1 | Cluster1 |
| - サーバ名  | server1  | server2  |

- CLUSTERPRO の設定 (フェイルオーバーグループ)

| リソース名                 | 設定項目                    | 設定値       |
|-----------------------|-------------------------|-----------|
| ミラーディスクリソース           | リソース名                   | md1       |
| ミラーディスクリソース           | 詳細タブ - ミラーパーティションデバイス名  | /dev/NMP1 |
| ミラーディスクリソース           | 詳細タブ - マウントポイント         | /mnt/md1  |
| ミラーディスクリソース           | 詳細タブ - データパーティションデバイス名  | /dev/sdc2 |
| ミラーディスクリソース           | 詳細タブ - クラスタパーティションデバイス名 | /dev/sdc1 |
| ミラーディスクリソース           | 詳細タブ - ファイルシステム         | ext4      |
| Google Cloud DNS リソース | ゾーン名                    | test-zone |

次のページに続く

表 5.4 – 前のページからの続き

| リソース名                 | 設定項目              | 設定値                      |
|-----------------------|-------------------|--------------------------|
| Google Cloud DNS リソース | DNS 名             | test-cluster.example.com |
| Google Cloud DNS リソース | IP アドレス (server1) | 10.0.11.101              |
| Google Cloud DNS リソース | IP アドレス (server2) | 10.0.11.102              |

- CLUSTERPRO の設定 (モニタリソース)

| モニタリソース名                     | 設定項目     | 設定値     |
|------------------------------|----------|---------|
| ミラーディスクモニタリソース               | モニタリソース名 | mdw1    |
| ミラーディスクコネク<br>トモニタリソース       | モニタリソース名 | mdnw1   |
| Google Cloud DNS モニ<br>タリソース | モニタリソース名 | gcdnsw1 |

## 5.2 Google Cloud の設定

### 1. VPC ネットワークの作成

Google Cloud Console にアクセスします (<https://console.cloud.google.com/>)。

VPC ネットワーク、サブネットを作成します。

詳細な手順は以下を参照してください。

VPC ネットワークの使用:

<https://cloud.google.com/vpc/docs/using-vpc/>

### 2. インスタンスの作成

公開イメージから インスタンスを作成します。

また、インスタンス作成時にミラーディスク (クラスタパーティション、データパーティション) に使用するセカンダリ ディスクを追加します。

インスタンスはクラスタを構成する仮想マシン分作成します。

詳細な手順は以下を参照してください。

入門ガイド:

<https://cloud.google.com/compute/docs/how-to/>

### 3. インスタンスの設定

作成した server1、server2 へ接続し、ログインします。

詳細な手順は以下を参照してください。

インスタンスへの接続:

<https://cloud.google.com/compute/docs/instances/connecting-to-instance/>

次にミラーディスクリソース用のパーティションを設定します。

インスタンスに追加したセカンダリ ディスクにクラスタパーティションおよびデータパーティションを作成します。

ミラーディスクリソース用のパーティションの設定については、以下を参照してください。

- 『インストール&設定ガイド』 - 「システム構成を決定する」 - 「ハードウェア構成後の設定」 - 「ミラーディスクリソース用のパーティションを設定する (Replicator 使用時は必須)」

### 4. DNS ゾーンの設定

DNS ゾーンの設定を行います。

詳細な手順は以下を参照してください。

ゾーンの管理:

<https://cloud.google.com/dns/zones/>

[ゾーンのタイプ] は非公開を選択します。[ゾーンのタイプ] については以下を参照してください。

概要:

<https://cloud.google.com/dns/docs/overview/>

## 5. gcloud CLI の設定

server1、server2 へログインし、gcloud CLI をインストールおよび SDK の初期化をします。

既にインストールされている場合は、再インストールは不要です。

gcloud CLI を使用する前に、root ユーザで Cloud SDK ツールの承認を済ませておく必要があります。

Cloud SDK ツールの承認方法については以下を参照してください。

Cloud SDK ツールの承認:

<https://cloud.google.com/sdk/docs/authorizing/>

その他の詳細な手順は以下を参照してください。

Google Cloud SDK のインストール:

<https://cloud.google.com/sdk/install/>

Cloud SDK の初期化:

<https://cloud.google.com/sdk/docs/initializing/>

クイックスタート:

<https://cloud.google.com/sdk/docs/quickstarts/>

## 6. Cloud IAM の設定

Cloud SDK ツールの承認時に使用したユーザアカウント、またはサービスアカウントに Cloud DNS のレコードセットを操作する権限を持たせます。

Cloud IAM を使用して、以下の権限を付与します。

- dns.changes.create
- dns.changes.get
- dns.managedZones.get

- dns.resourceRecordSets.create
- dns.resourceRecordSets.update
- dns.resourceRecordSets.delete
- dns.resourceRecordSets.list

もしくは、/roles/dns.admin 役割を付与します。

Cloud IAM については、以下を参照してください。

Cloud Identity and Access Management (IAM) :

<https://cloud.google.com/iam/>

リソースへのアクセス権の付与、変更、取り消し:

<https://cloud.google.com/iam/docs/granting-changing-revoking-access/>

アクセス制御:

<https://cloud.google.com/dns/docs/access-control/>

7. **OS** 起動時間の調整、ネットワーク設定の確認、ルートファイルシステムの確認、ファイアウォールの設定を確認、サーバの時刻を同期、**SELinux** の設定を確認

各手順は以下を参照してください。

- 『インストール&設定ガイド』 - 「システム構成を決定する」 - 「ハードウェア構成後の設定」

8. **CLUSTERPRO** のインストール

インストール手順は以下を参照してください。インストール完了後、OS の再起動を行ってください。

- 『インストール&設定ガイド』

9. **CLUSTERPRO** のライセンスを登録

ライセンス登録手順は以下を参照してください。

- 『インストール&設定ガイド』

## 5.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および接続方法は以下を参照してください。

- 『インストール&設定ガイド』 - 「クラスタ構成情報を作成する」

以下のリソース/モニタリソースを追加する手順を記述します。

- ミラーディスクリソース
- Google Cloud DNS リソース
- Google Cloud DNS モニタリソース

上記以外の設定は以下を参照してください。

- 『インストール&設定ガイド』
- 『リファレンスガイド』

### 1. クラスタの作成

最初に、クラスタ生成ウィザードを開始し、クラスタを構築します。

- クラスタの構築

1. Cluster WebUI にアクセスし、[クラスタ生成ウィザード] をクリックします。

2. クラスタ生成ウィザード] の [クラスタ] が表示されます。

[クラスタ名] に任意のクラスタ名を入力します。

[言語] を適切に選択します。[次へ] をクリックします。

3. [基本設定] が表示されます。

Cluster WebUI に接続したインスタンスがマスタサーバとして登録済みの状態で表示されます。

[追加] をクリックし、残りのインスタンスを追加します (インスタンスの内部 IP アドレスを指定します)。[次へ] をクリックします。

4. [インタコネクト] 画面が表示されます。

インタコネクトのために使用する IP アドレス (各インスタンスの内部 IP アドレス) を指定します。また、後で作成するミラーディスクリソースの通信経路として [MDC] に mdc1 を選択します。[次へ] をクリックします。

5. [NP 解決] 画面が表示されます。

何も指定せず [次へ] をクリックします。

### 2. グループリソースの追加

- グループの定義

フェイルオーバーグループを作成します。

1. [グループ一覧] 画面が表示されます。  
[追加] をクリックします。
2. [グループの定義] 画面が表示されます。  
[名前] にフェイルオーバーグループ名 (failover1) を設定します。[次へ] をクリックします。
3. [起動可能サーバ] 画面が表示されます。  
何も指定せず [次へ] をクリックします。
4. [グループ属性] 画面が表示されます。  
何も指定せず [次へ] をクリックします。
5. [グループリソース一覧] 画面が表示されます。  
以降の手順で、この画面でグループリソースを追加していきます。

- ミラーディスクリソース

ミラーディスクリソースを作成します。

詳細は以下を参照してください。

- 『リファレンスガイド』 - 「ミラーディスクリソースを理解する」

1. [グループリソース一覧] で [追加] をクリックします。
2. [グループのリソース定義 | failover1] 画面が開きます。  
[タイプ] ボックスでグループリソースのタイプ (ミラーディスクリソース) を選択し、[名前] ボックスにリソース名を入力します。[次へ] をクリックします。
3. [依存関係] 画面が表示されます。  
何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。  
[次へ] をクリックします。
5. [詳細] 画面が表示されます。  
[データパーティションデバイス名] [クラスタパーティションデバイス名] に「3. インスタンスの設定」で作成したパーティションのデバイス名を入力します。[マウントポイント]、[ファイルシステム] を入力します。[完了] をクリックして設定を終了します。

- Google Cloud DNS リソース

Cloud DNS に対して活性時にレコードを登録、非活性時にレコードを削除する仕組みを提供します。  
詳細は以下を参照してください。

- 『リファレンスガイド』 - 「Google Cloud DNS リソースを理解する」

1. [グループリソース一覧] で [追加] をクリックします。
  2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (Google Cloud DNS リソース) を選択して、[名前] ボックスにリソース名を入力します。[次へ] をクリックします。
  3. [依存関係] 画面が表示されます。何も指定せず [次へ] をクリックします。
  4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
  5. [ゾーン名] に CloudDNS の設定 (DNS ゾーン) 時にゾーン名として指定した値を入力します。  
[DNS 名] [IP アドレス] に CloudDNS のゾーンに追加するレコードセットの DNS 名と DNS 名に対応する IP アドレスを入力する。
  6. [完了] をクリックします。
3. モニタリソースの追加

- Google Cloud DNS モニタリソース

活性時監視の対象リソースに指定された Google Cloud DNS リソースが制御するレコードセット (A レコード) が、Google Cloud DNS 上に存在することを確認します。

Google Cloud DNS モニタリソースの詳細は以下を参照してください。

- 『リファレンスガイド』 - 「Google Cloud DNS モニタリソースを理解する」

1. [モニタリソース一覧] で [追加] をクリックします。
  2. [モニタリソースの定義] 画面が開きます。[タイプ] ボックスでモニタリソースのタイプ (Google Cloud DNS モニタリソース) を選択して、[名前] ボックスにリソース名を入力します。[次へ] をクリックします。
  3. [監視 (共通)] 画面が表示されます。対象リソースに Google Cloud DNS リソースのリソース名を指定します。
  4. [回復動作] 画面が表示されます。モニタリソース異常時の回復対象と回復動作を指定します。
  5. [完了] をクリックします。
4. 設定の反映とクラスタの起動



以下を参照してください。

- 『インストール&設定ガイド』 - 「クラスターを生成するには」

## 5.4 動作確認

構築した環境が正常に動作するかを、フェイルオーバーグループがフェイルオーバーすることにより確認します。既にクラスタが正常に起動している状態からの確認手順は以下のとおりです。

1. フェイルオーバーグループ (failover1) が、現用系ノードの server1 で起動します。Cluster WebUI [ステータス] タブにおいて failover1 が server1 で [起動済] になっていることを確認します。

2. クライアントから、test-cluster.example.com にアクセスし、現用系ノードに接続できることを確認します。

```
$ nslookup test-cluster.example.com <DNS サーバー>
```

3. Cluster WebUI から、フェールオーバーグループを現用系ノードから待機系ノードに手動で移動します。Cluster WebUI [ステータス] タブにおいて failover1 が server2 で [起動済] になっていることを確認します。

4. クライアントから、test-cluster.example.com にアクセスし、待機系ノードに接続できることを確認します。

```
$ nslookup test-cluster.example.com <DNS サーバー>
```

以上で、登録したレコードの DNS 名を使用してクライアントから HA クラスタに接続する動作確認は完了です。その他の障害発生時の動作確認については適宜実施してください。

## 第 6 章

# エラーメッセージ一覧

各リソース/モニタリソースのエラーメッセージについては、以下を参照してください。

- 『リファレンスガイド』 - 「エラーメッセージ一覧」



## 第 7 章

# 注意・制限事項

### 7.1 ロードバランサを使用した HA クラスターの場合

#### 7.1.1 Google Cloud の注意事項

- マルチテナントのクラウド環境では、物理環境や一般的な仮想化環境 (非クラウド環境) に比べて性能の差が大きくなる (性能の劣化率が大きくなる) 傾向があります。性能を重視するシステムでは、設計フェーズにおいて、この点に留意する必要があります。

#### 7.1.2 CLUSTERPRO の注意事項

- Google Cloud の仕様により、外部 TCP ネットワーク負荷分散では HTTP プロトコルを使用するレガシーヘルスチェックが要求されます。

Google Cloud 仮想 IP リソースは、TCP プロトコルを使用するヘルスチェックにのみ対応しているため、外部 TCP ネットワークロードバランサからのヘルスチェックに応答できません。

そのため、外部 TCP ネットワークロードバランサによる Google Cloud 仮想 IP リソースを使用した HA クラスターはご利用になれません。内部 TCP ロードバランサをご利用ください。

以下を参照してください。

ヘルスチェックのコンセプト:

<https://cloud.google.com/load-balancing/docs/health-check-concepts/>

- 内部 TCP ロードバランサを使用した HA クラスター構成では、Google Cloud の仕様により、HA クラスターと異なるリージョンのクライアントからは、HA クラスターにアクセスできません。

以下を参照してください。

内部 TCP / UDP 負荷分散のコンセプト:

<https://cloud.google.com/load-balancing/docs/internal/#architecture>

- OS の起動時間は [ハートビートタイムアウト] より長くなるよう調整してください。

- [クラスタプロパティ]-[監視] タブ-[シャットダウン監視タイムアウト]にて、既定値 (ハートビートのタイムアウトを使用する) から変更する場合、[ハートビートタイムアウト] 以下となるよう調整してください。

以下を参照してください。

- 『リファレンスガイド』 - 「クラスタプロパティ」 - 「タイムアウトタブ」
- 『リファレンスガイド』 - 「クラスタプロパティ」 - 「監視タブ」
- 『スタートアップガイド』 - 「注意制限事項」 - 「OS 起動時間の調整」

以下も参照してください。

- 『スタートアップガイド』 - 「注意制限事項」 - 「通信ポート番号」
- 『スタートアップガイド』 - 「注意制限事項」 - 「Google Cloud 仮想 IP リソースの設定について」
- 『スタートアップガイド』 - 「注意制限事項」 - 「Google Cloud ロードバランスモニタリソースの設定について」
- 『リファレンスガイド』 - 「Google Cloud 仮想 IP リソースに関する注意事項」
- 『リファレンスガイド』 - 「Google Cloud 仮想 IP モニタリソースの注意事項」
- 『リファレンスガイド』 - 「Google Cloud ロードバランスモニタリソースの注意事項」

## 7.2 Cloud DNS を使用した HA クラスタの場合

### 7.2.1 Google Cloud の注意事項

- マルチテナントのクラウド環境では、物理環境や一般的な仮想化環境 (非クラウド環境) に比べて性能の差が大きくなる (性能の劣化率が大きくなる) 傾向があります。性能を重視するシステムでは、設計フェーズにおいて、この点に留意する必要があります。
- クライアントから名前解決できるようになるまでに時間が掛かる場合があります。以下のいずれかが考えられます。それぞれの設定を確認してください。
  - OS 側のリゾルバにより時間が掛かっている。
  - TTL の値が大きい。
  - Cloud DNS への変更が反映完了する前に名前解決を試みってしまうと DNS からは NXDOMAIN (存在しないドメイン) が返りますが、その場合はネガティブキャッシュの有効期間が経過するまでは名前解決に失敗します。

### 7.2.2 CLUSTERPRO の注意事項

- 複数の Google Cloud DNS リソースの活性・非活性処理が同時に実行されるとエラーが発生することがあります。

そのため、クラスタ内で複数の Google Cloud DNS リソースを使用する場合は、リソースの依存関係やグループの起動・停止待ち合わせ等で活性・非活性処理が同時に実行されないように設定する必要があります。
- OS の起動時間は [ハートビートタイムアウト] より長くなるよう調整してください。
- [クラスタプロパティ]-[監視] タブ-[シャットダウン監視タイムアウト] にて、既定値 (ハートビートのタイムアウトを使用する) から変更する場合、[ハートビートタイムアウト] 以下となるよう調整してください。

以下を参照してください。

  - 『リファレンスガイド』 - 「クラスタプロパティ」 - 「タイムアウトタブ」
  - 『リファレンスガイド』 - 「クラスタプロパティ」 - 「監視タブ」
  - 『スタートアップガイド』 - 「注意制限事項」 - 「OS 起動時間の調整」





## 第 8 章

# 免責・法的通知

### 8.1 免責事項

- 本書の内容は、予告なしに変更されることがあります。
- 日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任をおいせん。また、お客様が期待される効果を得るために、本書に従った導入、使用および使用効果につきましては、お客様の責任とさせていただきます。
- 本書に記載されている内容の著作権は、日本電気株式会社に帰属します。本書の内容の一部または全部を日本電気株式会社の許諾なしに複製、改変、および翻訳することは禁止されています。

## 8.2 商標情報

- CLUSTERPRO® は、日本電気株式会社の登録商標です。
- Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標です。
- Google Cloud は、Google LLC の商標または登録商標です。
- 本書に記載されたその他の製品名および標語は、各社の商標または登録商標です。

## 第 9 章

### 改版履歴

| 版数 | 改版日付       | 内容   |
|----|------------|------|
| 1  | 2024/04/15 | 新規作成 |
| 2  | 2024/07/12 | 誤記修正 |

© Copyright NEC Corporation 2024. All rights reserved.