CLUSTERPRO X 5.1

Amazon Web Services 向け HA クラスタ 構築ガイド (Linux)

リリース *3*

日本電気株式会社

2023 年 **11** 月 **17** 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　機能概要　7
- 2.1 機能概要 7
- 2.2 HA クラスタ構成 9
- 2.3 Multi-AZ 16
- 2.4 ネットワークパーティション解決 18
- 2.5 オンプレミスと AWS 19

第 3 章　動作環境　23

第 4 章　注意事項　25
- 4.1 VPC で CLUSTERPRO を利用する場合の注意事項 25

第 5 章　VIP 制御による HA クラスタの設定　29
- 5.1 VPC 環境の設定 32
- 5.2 インスタンスの設定 37
- 5.3 CLUSTERPRO の設定 40

第 6 章　EIP 制御による HA クラスタの設定　51
- 6.1 VPC 環境の設定 53
- 6.2 インスタンスの設定 56
- 6.3 CLUSTERPRO の設定 59

第 7 章　DNS 名制御による HA クラスタの設定　69
- 7.1 VPC 環境の設定 72
- 7.2 インスタンスの設定 76
- 7.3 CLUSTERPRO の設定 79

第 8 章　トラブルシューティング 91

第 9 章　免責・法的通知 107

9.1　免責事項 107

9.2　商標情報 108

第 10 章　改版履歴 109

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。また、Amazon Web Services のうち、最低限 Amazon EC2、Amazon VPC、IAM に関する知識を保有していることが前提となります。

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. 機能概要」: 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. 注意事項」: 構築時の注意事項について説明します。
- 「5. *VIP* 制御による *HA* クラスタの設定」: VIP 制御による HA クラスタの構築手順について説明します。
- 「6. *EIP* 制御による *HA* クラスタの設定」: EIP 制御による HA クラスタの構築手順について説明します。
- 「7. *DNS* 名制御による *HA* クラスタの設定」: DNS 名制御による HA クラスタの構築手順について説明します。
- 「8. トラブルシューティング」: 問題発生時の現象と対応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 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。 [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。	`clpstat -s[-h host_name]`
#	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	`# clpstat`
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	`/Linux`
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。 **# clpcl -s -a**
斜体	ユーザが有効な値に置き換えて入力する項目	`# ping <IP アドレス>`

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

機能概要

2.1 機能概要

本書の設定を行うことで、Amazon Web Services(以下、AWS) の Amazon Virtual Private Cloud（以下、VPC） 環境において CLUSTERPRO による HA クラスタを構築できます。

HA クラスタを構築することで、より重要な業務を行うことが可能となり AWS 環境におけるシステム構成の選択肢が広がります。AWS 環境は地域（リージョン）ごとに複数の Availability Zone(以下、AZ) で堅牢に構成されており、利用者は必要に応じて AZ を選択して使用できます。CLUSTERPRO は複数の AZ 間 (以下、Multi-AZ) においても HA クラスタを可能とするため、業務の高可用性を実現します。

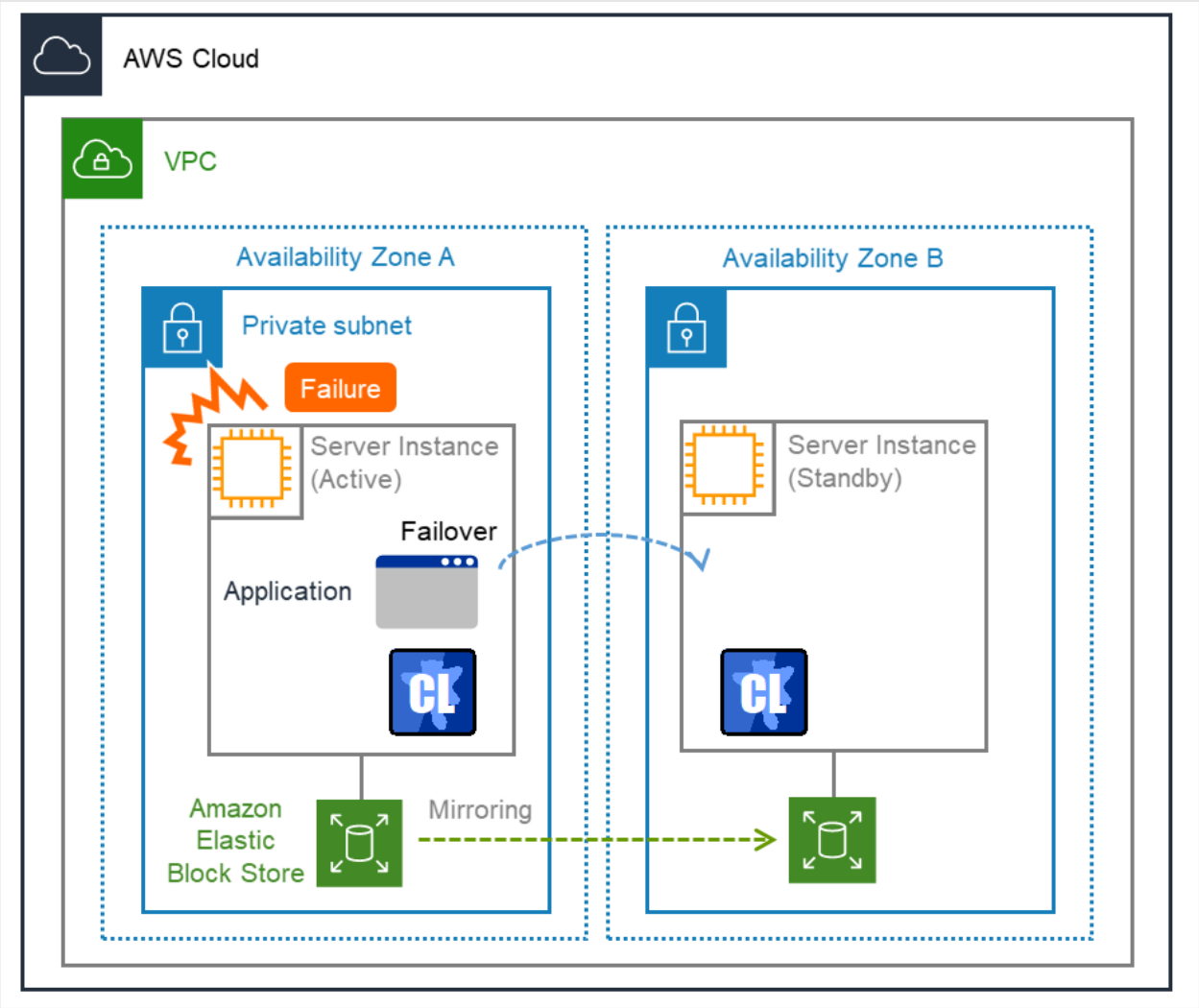


図 2.1　Multi-AZ 構成のミラー型 HA クラスタ

AWS 環境においては仮想的な IP アドレスを使用してクラスタサーバに接続することが可能です。AWS 仮想 IP リソースや AWS Elastic IP リソースや AWS DNS リソースを利用することで、"フェイルオーバ" または、"グループの移動" が発生した場合でも、クライアントは接続先サーバの切り替えを意識する必要がありません。

2.2 HA クラスタ構成

本構築ガイドでは、「仮想 IP （以下、VIP） 制御による HA クラスタ」、「Elastic IP （以下、EIP） 制御による HA クラスタ」、「DNS 名制御による HA クラスタ」 の 3 種類の HA クラスタを想定しています。本節では Single-AZ 構成にて説明しています。Multi-AZ については「2.3. *Multi-AZ*」を参照してください。

HA クラスタにアクセスする クライアントの場所	選択するリソース	本章の参照箇所
同じ VPC 内	AWS 仮想 IP リソース	VIP 制御による HA クラスタ
インターネット	AWS Elastic IP リソース	EIP 制御による HA クラスタ
任意の場所	AWS DNS リソース	DNS 名制御による HA クラスタ

2.2.1 VIP 制御による HA クラスタ

同じ VPC 内のクライアントから、VIP アドレスを通じて HA クラスタにアクセスさせる構成を想定しています。たとえば DB サーバをクラスタ化し、Web サーバから VIP アドレス経由で DB サーバにアクセスするなどの用途が考えられます。

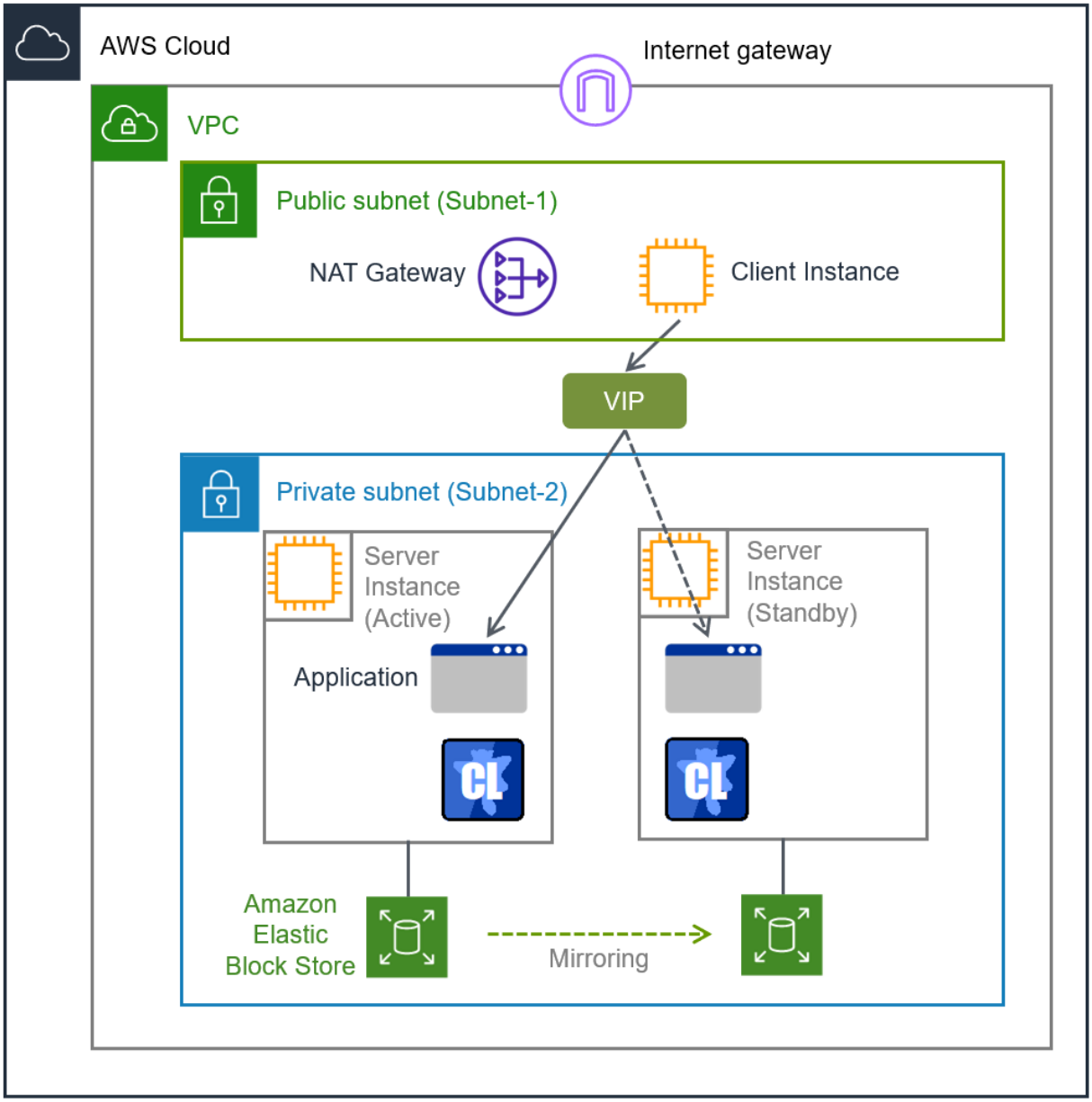


図 2.2　VIP 制御による HA クラスタ

図の例では、Private なサブネット上にクラスタ化されたサーバ用のインスタンスが配置されています。CLUSTERPRO の AWS 仮想 IP リソースは、現用系側サーバ用のインスタンスに対して VIP アドレスの設定および VPC のルートテーブルの書き換えを行います。これにより、VPC 内の任意のサブネット上に配置されたクライアント用のインスタンスから VIP アドレスを通じて現用系側サーバ用のインスタンスにアクセスできるようになります。VIP アドレスは、VPC の CIDR の範囲外である必要があります。

VPC 外のクライアントからアクセスする場合は、何らかの方法で VPC 内のルートテーブルを使用して通信を行うようにする必要があります。例えば、AWS Transit Gateway を使用すると VPC 外からの通信を Transit Gateway

ルートテーブルで VPC 内に転送後、VPC 内のルートテーブルを使用して通信することができます。

サーバ用の各インスタンスは、AWS CLI の実行や、DNS 参照などで必要な時は、Public なサブネットに配置された NAT ゲートウェイ を経由してリージョンのエンドポイントやインターネットへアクセスします。

※ AWS CLI の実行時は、各インスタンスがリージョンのエンドポイントに接続する必要があります。

リージョンのエンドポイントに接続する方法として Proxy サーバ / NAT / Public IP / EIP / VPC エンドポイントなどを使用する方法がありますが、本書では VIP 制御による HA クラスタ構成の場合、NAT ゲートウェイを使用する方法を採用しています。

VIP 制御による 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。

リソース種別	説明	設定
AWS 仮想 IP リソース	現用系側のインスタンスへの VIP アドレスの付与、および、その IP アドレスに対するルートテーブルの変更を行い、業務を 同じ VPC 内に公開します。	必須
AWS 仮想 IP モニタリソース	AWS 仮想 IP リソースが付与した VIP アドレスが自サーバに存在するか、および VPC のルートテーブルが不正に変更されていないかを定期的に監視します。 （AWS 仮想 IP リソースを追加すると自動的に追加されます。）	必須
AWS AZ モニタリソース	Multi-AZ を利用し、自サーバが属する AZ の健全性を定期的に監視します。	推奨
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

2.2.2 EIP 制御による HA クラスタ

クライアントから、インターネット経由で EIP に割り当てられたグローバル IP アドレスを通じて HA クラスタにアクセスさせる構成を想定しています。

クラスタ化するインスタンスは Public なサブネット上に配置されており、各インスタンスは、インターネットゲートウェイを経由してインターネットへアクセスすることが可能です。

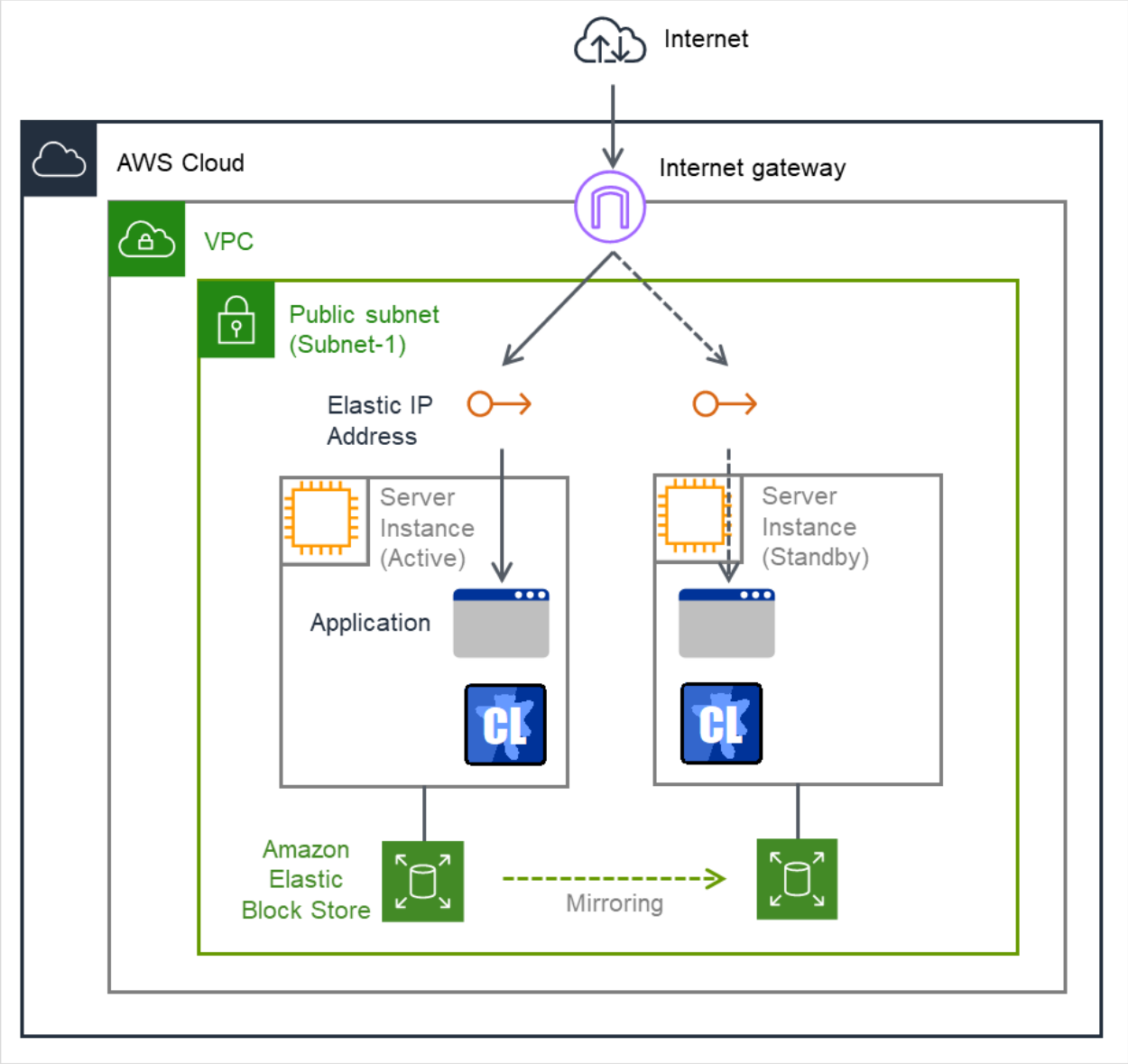


図 2.3　EIP 制御による HA クラスタ

図の例では、クラスタ化するサーバ用のインスタンスは Public なサブネット上に配置されています。CLUSTERPRO の AWS Elastic IP リソースは、EIP を現用系側サーバ用のインスタンスにアタッチします。これによりインターネット側の任意のクライアントは EIP アドレスを通じて現用系側サーバ用のインスタンスにアクセスできるようになります。

※ AWS CLI の実行時は、各インスタンスがリージョンのエンドポイントに接続する必要があります。

リージョンのエンドポイントに接続する方法として Proxy サーバ / NAT / Public IP / EIP / VPC エンドポイントなどを使用する方法がありますが、本書では EIP 制御による HA クラスタ構成の場合、インスタンスに割り当てられた Public IP を経由する方法を採用しています。

EIP 制御による 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。

リソース種別	説明	設定
AWS Elastic IP リソース	現用系側のインスタンスに EIP アドレスを付与し、業務をインターネットに公開します。	必須
AWS Elastic IP モニタリソース	AWS Elastic IP リソースが付与した EIP アドレスが自サーバに存在するか定期的に監視します。 （AWS Elastic IP リソースを追加すると自動的に追加されます）	必須
AWS AZ モニタリソース	Multi-AZ を利用し、自サーバが属する AZ の健全性を定期的に監視します。	推奨
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

2.2.3 DNS 名制御による HA クラスタ

クライアントから、同一の DNS 名を使って HA クラスタにアクセスさせる構成を想定しています。たとえば DB サーバをクラスタ化し、Web サーバから DNS 名経由で DB サーバにアクセスするなどの用途が考えられます。

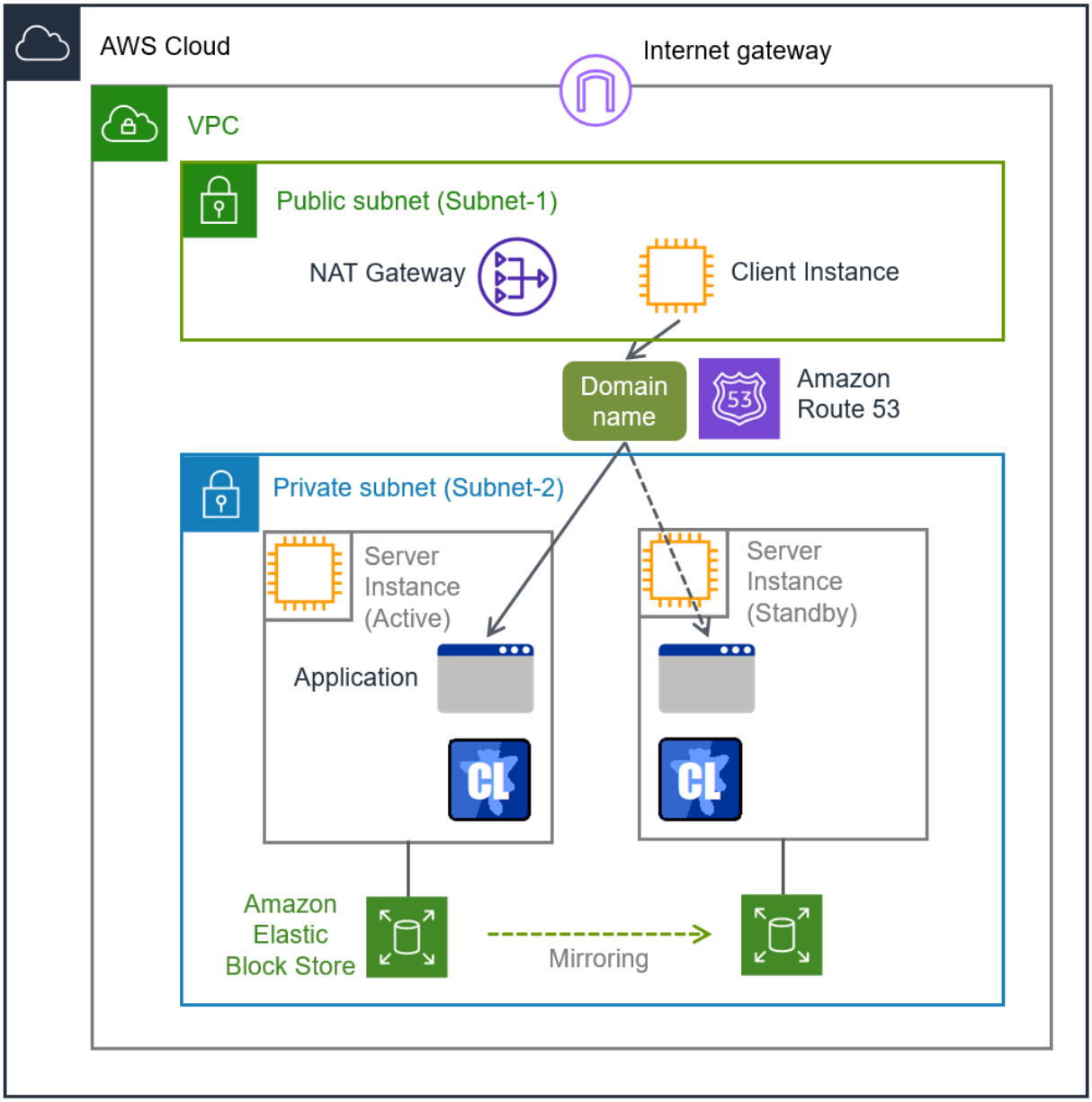


図 2.4　DNS 名制御による HA クラスタ

図の例では、Private なサブネット上にクラスタ化されたサーバ用のインスタンスが配置されています。CLUSTERPRO の AWS DNS リソースは、 DNS 名と現用系側サーバの IP アドレスを含むリソースレコードセットを Amazon Route 53 の Private ホストゾーンに登録します。これにより、VPC 内の任意のサブネット上に配置されたクライアント用のインスタンスから、DNS 名を通じて現用系側サーバ用の インスタンスにアクセスできるようになります。

本書では、クラスタ化するサーバ用のインスタンスを Private なサブネット上に配置する構成を採用していますが、Public なサブネット上に配置することも可能です。この場合、AWS DNS リソースで DNS 名と現用系側サーバの

Public IP アドレスを含むリソースレコードセットを Amazon Route 53 の Public ホストゾーンに登録することで、インターネット側の任意のクライアントから DNS 名を通じて現用系側サーバ用のインスタンスにアクセスできるようになります。なお、Public ホストゾーンのドメインへのクエリが Amazon Route 53 ネームサーバを参照するように、事前にレジストラのネームサーバ (NS) レコードを設定しておく必要があります。

また、クラスタとクライアントがそれぞれ異なる VPC 上に存在する構成とする場合は、VPC ピアリング接続を使用します。事前に、ピアリング接続した各 VPC を Amazon Route 53 の Private ホストゾーンに関連付けしておき、AWS DNS リソースでその Private ホストゾーンに DNS 名と現用系側サーバの IP アドレスを含むリソースレコードセットを登録します。これにより、異なる VPC 上のクライアントから DNS 名を通じて現用系側サーバ用のインスタンスにアクセスできるようになります。

※ AWS CLI の実行時は、各インスタンスがリージョンのエンドポイントに接続する必要があります。
リージョンのエンドポイントに接続する方法として Proxy サーバ / NAT / Public IP / EIP などを使用する方法がありますが、本書では DNS 名制御による HA クラスタ構成の場合、NAT ゲートウェイを使用する方法を採用しています。

DNS 名制御による 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。

リソース種別	説明	設定
AWS DNS リソース	DNS 名と現用系側のインスタンスの IP アドレスを含むリソースレコードセットを Amazon Route 53 のホストゾーンに登録し、業務を同じ VPC 内、または、インターネットに公開します。	必須
AWS DNS モニタリソース	AWS DNS リソースが 登録したリソースレコードセットが、 Amazon Route 53 のホストゾーンに存在するか、およびその DNS 名の名前解決が可能かを定期的に監視します。 （AWS DNS リソースを追加すると自動的に追加されます。）	必須
AWS AZ モニタリソース	Multi-AZ を利用し、自サーバが属する AZ の健全性を定期的に監視します。	推奨
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

2.3 Multi-AZ

AWS 環境では、HA クラスタを構成するインスタンスをアベイラビリティーゾーン単位で分散させることで、アベイラビリティーゾーン単位の障害に対する冗長性を持たせ、可用性を高めることが可能です。

AWS AZ モニタリソースは、各アベイラビリティーゾーンの健全性を監視し、もし障害が発生していた場合は警告や回復動作を行わせることができます。

詳細は『リファレンスガイド』-「AWS AZ モニタリソースを理解する」を 参照してください。

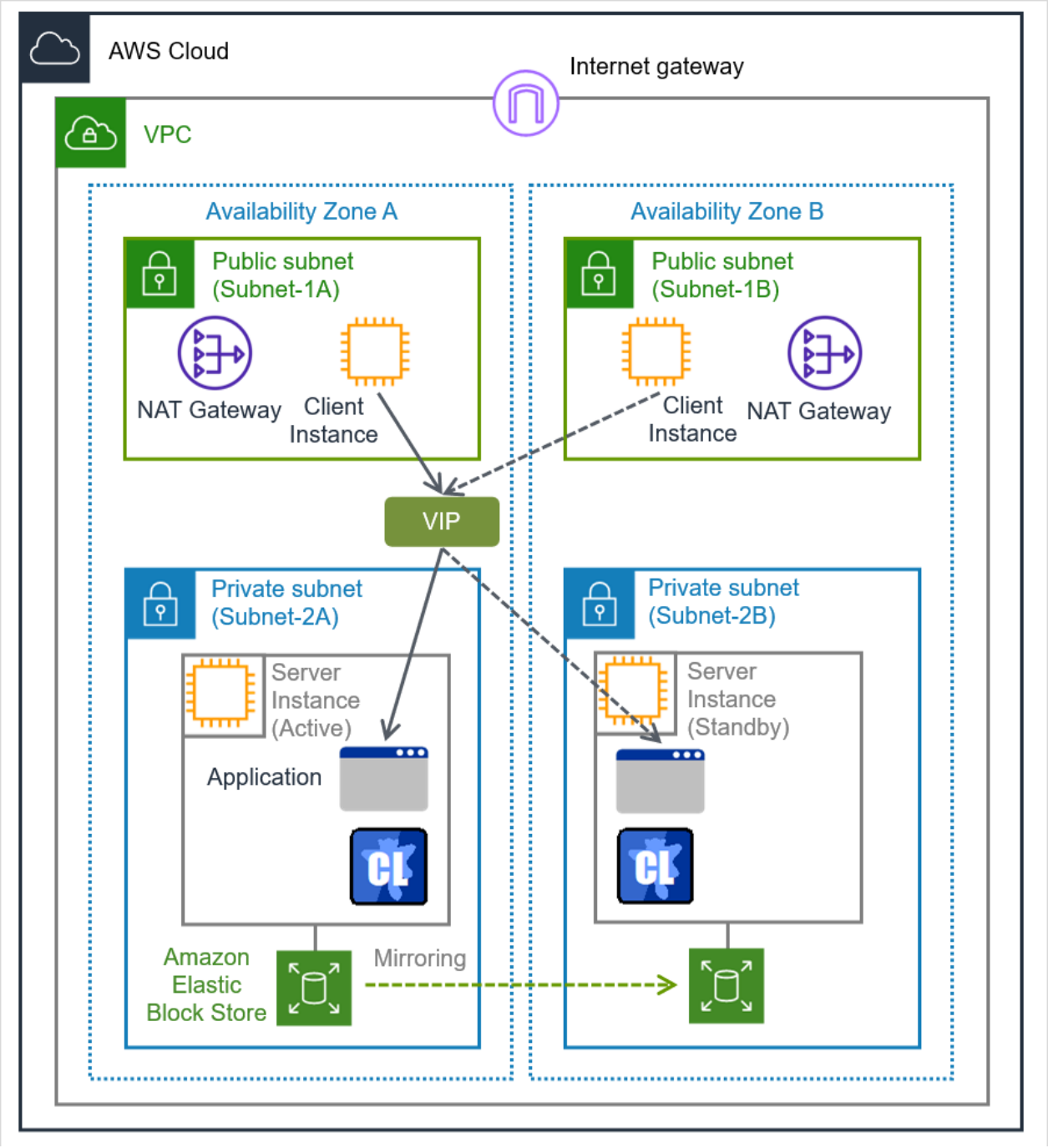


図 2.5　Multi-AZ を使用した HA クラスタの例

2.4 ネットワークパーティション解決

ネットワークパーティション解決 (NP 解決) では、各サーバが共通の装置に対するアクセス可否を確認することで、他サーバがダウンしたか自サーバがネットワークから孤立したかを判断します。

本書の例では NP 解決を以下のように設定しています。明記していない設定は既定値を使用しています。

項目名	設定値	備考
種別	HTTP	
ターゲットホスト (ターゲット)	aws.amazon.com	HTTP の HEAD リクエストにステータスコード 200 で応答する装置を指定します。
サービスポート	443	
SSL を使用する	オン	aws.amazon.com の 443 番ポートをターゲットに指定する場合、本設定をオンにする必要があります。 環境により [クラスタプロパティ] [暗号化] タブ で [SSL ライブラリ] および [Crypto ライブラリ] の 設定が必要になる場合があります。

NP 解決の詳細については以下のドキュメントを参照してください。

- 「スタートアップガイド」-「ネットワークパーティション解決」
- 「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」

また、強制停止スクリプトを組合せることも可能です。詳細は CLUSTERPRO オフィシャルブログを参照してください。

https://jpn.nec.com/clusterpro/blog/20180829.html

2.5 オンプレミスと AWS

オンプレミスと AWS における CLUSTERPRO の機能差分は以下の通りです。

- ✓: 可
- n/a: 不可

機能	オンプレミス	AWS
共有ディスク型クラスタの構築可否	✓	✓
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
AWS Elastic IP リソースの使用可否	n/a	✓
AWS 仮想 IP リソースの使用可否	n/a	✓
AWS DNS リソースの使用可否	n/a	✓

オンプレミスと AWS における、ミラーディスクと IP エイリアス (オンプレミス：フローティング IP リソース、AWS：AWS 仮想 IP リソースの例) 各種リソースを使用した 2 ノードクラスタの構築手順の流れは以下を参照してください。

- CLUSTERPRO インストール前

	手順	オンプレミス	AWS
1	VPC 環境の設定	不要	◇ AWS 仮想 IP リソースを使用する場合 ・本書「 5.1. *VPC* 環境の設定 」参照 ◇ AWS Elastic IP リソースを使用する場合 ・本書「 6.1. *VPC* 環境の設定 」参照 ◇ AWS DNS リソースを使用する場合 ・本書「 7.1. *VPC* 環境の設定 」参照

次のページに続く

表 2.7 – 前のページからの続き

	手順	オンプレミス	AWS
2	インスタンスの設定	不要	◇ AWS 仮想 IP リソースを使用する場合 ・本書「5.2. インスタンスの設定」参照 ◇ AWS Elastic IP リソースを使用する場合 ・本書「6.2. インスタンスの設定」参照 ◇ AWS DNS リソースを使用する場合 ・本書「7.2. インスタンスの設定」参照
3	ミラーディスクリソース用のパーティションの設定	以下を参照。 ・『インストール&設定ガイド』の「システム構成を決定する」の「ハードウェア構成後の設定」 ・『リファレンスガイド』の「ミラーディスクリソースを理解する」	オンプレミスと同様
4	OS 起動時間の調整	『インストール&設定ガイド』の「システム構成を決定する」の「ハードウェア構成後の設定」参照	オンプレミスと同様
5	ネットワークの確認	『インストール&設定ガイド』の「システム構成を決定する」の「ハードウェア構成後の設定」参照	オンプレミスと同様
6	ルートファイルシステムの確認	『インストール&設定ガイド』の「システム構成を決定する」の「ハードウェア構成後の設定」参照	オンプレミスと同様

次のページに続く

表 2.7 – 前のページからの続き

	手順	オンプレミス	AWS
7	ファイアウォールの確認	『インストール&設定ガイド』の「システム構成を決定する」の「ハードウェア構成後の設定」参照	オンプレミスと同様
8	サーバの時刻同期	『インストール&設定ガイド』の「システム構成を決定する」の「ハードウェア構成後の設定」参照	オンプレミスと同様
9	CLUSTERPRO のインストール	『インストール&設定ガイド』の「CLUSTERPRO をインストールする」参照	オンプレミスと同様

- CLUSTERPRO インストール後

	手順	オンプレミス	AWS
10	CLUSTERPRO のライセンスを登録	『インストール&設定ガイド』の「ライセンスを登録する」参照	オンプレミスと同様
11	クラスタの作成-ハートビート方式の設定	『インストール&設定ガイド』の「クラスタ構成情報を作成する」の「2 ノードクラスタ構成情報の作成手順」参照。	COM ハートビート、BMC ハートビート、DISK ハートビートは使用できません。
12	クラスタの作成-NP 解決処理の設定	NP 解決リソースを使用。 以下を参照。 ・『インストール&設定ガイド』の「クラスタ構成情報を作成する」の「2 ノードクラスタ構成情報の作成手順」 ・『リファレンスガイド』の「ネットワークパーティション解決リソースの詳細」	NP 解決リソースを使用。 以下を参照。 ・本書「2.4. ネットワークパーティション解決」参照

次のページに続く

表 2.8 – 前のページからの続き

	手順	オンプレミス	AWS
13	クラスタの作成-フェイルオーバグループの作成、モニタリソースの作成	『インストール&設定ガイド』の「クラスタ構成情報を作成する」の「2 ノードクラスタ構成情報の作成手順」参照	オンプレミスに加え、以下を参照。 ◇ AWS 仮想 IP リソースを使用する場合 ・本書「 5.3. *CLUSTERPRO の設定* 」参照 ・『リファレンスガイド』の「AWS 仮想 IP リソースを理解する」参照 ◇ AWS Elastic IP リソースを使用する場合 ・本書「 6.3. *CLUSTERPRO の設定* 」参照 ・『リファレンスガイド』の「AWS Elastic IP リソースを理解する」参照 ◇ AWS DNS リソースを使用する場合 ・本書「 7.3. *CLUSTERPRO の設定* 」参照 ・『リファレンスガイド』の「AWS DNS リソースを理解する」参照

第 3 章

動作環境

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

第 4 章

注意事項

4.1 VPC で CLUSTERPRO を利用する場合の注意事項

VPC 環境で CLUSTERPRO を利用する際に、以下のような注意事項があります。

インターネットまたは異なる VPC からのアクセス

AWS 側の仕様により、インターネットまたは異なる VPC 上のクライアントから、AWS 仮想 IP リソースで付与した VIP アドレスを指定してアクセスすることはできないことを確認しています。インターネット上の クライアントからアクセスする場合は、AWS Elastic IP リソースで付与した EIP アドレスを指定してアクセスしてください。異なる VPC 上のクライアントからアクセスする場合は、AWS DNS リソースによって Amazon Route 53 に登録した DNS 名を指定して、VPC ピアリング接続経由でアクセスしてください。

また、以下の CLUSTERPRO オフィシャルブログも参考にしてください。

https://jpn.nec.com/clusterpro/blog/20190610.html

異なる VPC からの VPC ピアリング接続経由でのアクセス

AWS 仮想 IP リソースは、 VPC ピアリング接続を経由してのアクセスが必要な場合では利用することができません。これは、 VIP として使用する IP アドレスが VPC の範囲外であることを前提としており、このような IP アドレスは VPC ピアリング接続では無効とみなされるためです。 VPC ピアリング接続を経由してのアクセスが必要な場合は、 Amazon Route 53 を利用する AWS DNS リソースを使用してください。

VPC エンドポイントの使用

VPC エンドポイントを使用することで、プライベートネットワークでも NAT やプロキシサーバを用意することなく AWS CLI による Amazon EC2 のサービス制御が可能です。そのため「VIP 制御による HA クラスタ」構成において NAT の代わりに VPC エンドポイントを使用することが可能となります。なお、VPC エンドポイントは作成時にサービス名が".ec2"で終わるものを選択する必要があります。

また、VPC エンドポイントを使用する場合でも、インスタンスのオンラインアップデートやモジュールダウンロードのためのインターネットアクセス、および、VPC エンドポイントが対応していない AWS のクラウドサービスに対するアクセスを行う場合は、別途 NAT ゲートウェイなどが必要になります。

CLUSTERPRO では VPC エンドポイントを明示的に指定することはできません。

AWS CLI が自動で選択した VPC エンドポイントを使用します。

グループリソースおよびモニタリソースの機能制限

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』-「注意制限事項」-「AWS Elastic 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」-「AWS 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」-「AWS DNS 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」-「AWS DNS モニタリソースの設定について」

ミラーディスクの性能

Multi-AZ 間で HA クラスタを構築すると、インスタンス間の距離が離れることによる TCP/IP の応答遅延が発生し、ミラーリングに影響を受ける可能性があります。

また、マルチテナントのため、他のシステムの使用状況がミラーリングの性能に影響を与えます。上記の理由から 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) に比べてミラーディスクの性能の差が大きくなる (ミラーディスクの性能の劣化率が大きくなる) 傾向にあります。

書き込み性能を重視するシステムの場合には、設計のフェーズにおいて、この点をご留意ください。

AWS エンドポイント停止の影響

AWS DNS モニタリソースは、リソースレコードセットの存在確認のために AWS CLI を利用しています。

そのため AWS エンドポイントのメンテナンスや障害およびネットワーク経路の障害や遅延の影響によるフェイルオーバを発生させないためには、AWS DNS モニタリソースの [AWS CLI コマンド応答取得失敗時動作] の設定は、「回復動作を実行しない (警告を表示する)」「回復動作を実行しない (警告を表示しない)」のいずれかとしてください。頻繁に警告が表示される場合は、「回復動作を実行しない (警告を表示しない)」を推奨します。

CLUSTERPRO で設定するディスクデバイス名

AWS 環境ではインスタンスの再起動や停止/開始、EBS ボリュームのデタッチ/アタッチ等により NVMe EBS ボリュームのデバイスファイル名 (例 /dev/nvme0n1) が変更される場合があります。

そのため、ディスク系リソース (ディスクリソース、ミラーディスクリソース等) で制御するデバイス名に NVMe EBS ボリュームのデバイスファイル名を設定すると、インスタンスの再起動等を行った際に、デバ

イスファイル名が変更され、ディスク系リソースの起動に失敗する可能性があります。

本事象については、以下のいずれかの方法が対策となります。

- ディスク系リソースのデバイス名に LVM の論理ボリューム名を設定する
- ディスク系リソースのデバイス名に by-id 名 (例 /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_vol***) を設定する

なお、ミラーディスクのデータパーティションを LVM で構成している場合、業務を停止することなくデータパーティションを拡張することができます。

第 5 章

VIP 制御による HA クラスタの設定

本章では、VIP 制御による HA クラスタの構築手順を説明します。

図中の Server Instance (Active) は現用系サーバ、Server Instance (Standby) は待機系サーバのインスタンスです。

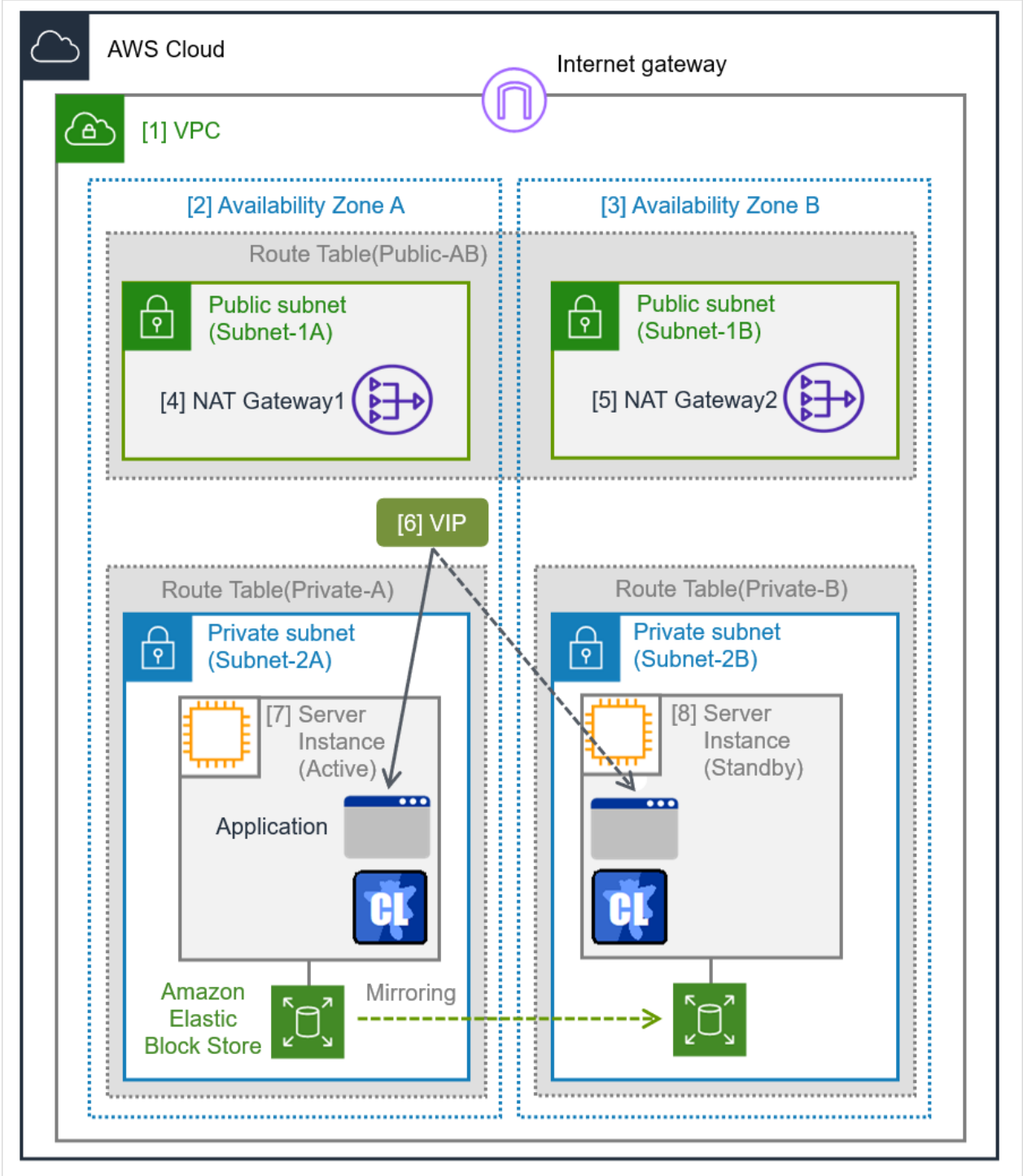


図 5.1　システム構成 VIP 制御による HA クラスタ

CIDR (VPC)	10.0.0.0/16
VIP	10.1.0.20

次のページに続く

表 5.1 – 前のページからの続き

Public subnet (Subnet-1A)	10.0.10.0/24
Public subnet (Subnet-1B)	10.0.20.0/24
Private subnet (Subnet-2A)	10.0.110.0/24
Private subnet (Subnet-2B)	10.0.120.0/24

5.1 VPC 環境の設定

VPC Management Console、および、EC2 Management Console 上で VPC の構築を行います。

図中および説明中の IP アドレスは一例であり、実際の設定時は VPC に割り当てられている IP アドレスに読み替えてください。既存の VPC に CLUSTERPRO を適用する場合は、不足しているサブネットを追加するなど適切に読み替えてください。

1. **VPC** およびサブネットを設定する

   最初に VPC およびサブネットを作成します。

   ⇒ VPC Management Console の [VPC] および [Subnets] で VPC およびサブネットの追加操作を行います。

   [1] VPC　**VPC ID（vpc-xxxxxxxx）** は、後で **AWS 仮想 IP リソース** の設定時に必要となるため、別途控えておきます。

2. **Internet Gateway** を設定する。

   VPC からインターネットにアクセスするための Internet Gateway を追加します。

   ⇒ VPC Management Console の [Internet Gateways] から [Create internet gateway] をクリックして作成します。その後、 作成した Internet Gateway を VPC に Attach します。

3. **Network ACL/Security Group** を設定する

   VPC 内外からの不正なネットワークアクセスを防ぐために、Network ACL、および、Security Group を適切に設定します。

   Private ネットワーク （Subnet-2A、および、Subnet-2B）内に配置予定の HA クラスタノード用のインスタンスから、HTTPS で Internet Gateway と通信可能となるように、また、Cluster WebUI やインスタンス同士の通信も可能となるよう各経路について Network ACL や Security Group の設定を変更します。

   ⇒ 設定変更は、 VPC Management Console の [Network ACLs] 、および、[Security Groups] から行います。

   CLUSTERPRO 関連コンポーネントが使用するポート番号については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」を参照し、設定してください。

4. **HA** クラスタ用のインスタンスを追加する

   HA クラスタノード用のインスタンスを Private ネットワーク（Subnet-2A、および、Subnet-2B）に作成します。

IAM ロールをインスタンスに割り当てて使用する場合は、IAM ロールを指定してください。

⇒ インスタンスの作成は、 EC2 Management Console の [Instances] から、 [Launch Instance] をクリックして行います。

⇒ IAM の設定については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」-「AWS 環境における IAM の設定について」を参照し、設定してください。

作成した各インスタンスに割り当てられている Elastic Network Interface (以下、ENI) の Source/Dest. Check を disabled に変更します。
AWS 仮想 IP リソースが VIP 制御を可能にするためには、VIP アドレス（図では 10.1.0.20） への通信をインスタンスの ENI にルーティングさせる必要があります。各インスタンスの ENI は、Private IP アドレスと VIP アドレス からの通信を受け取るために、Source/Dest. Check を disabled にする必要があります。

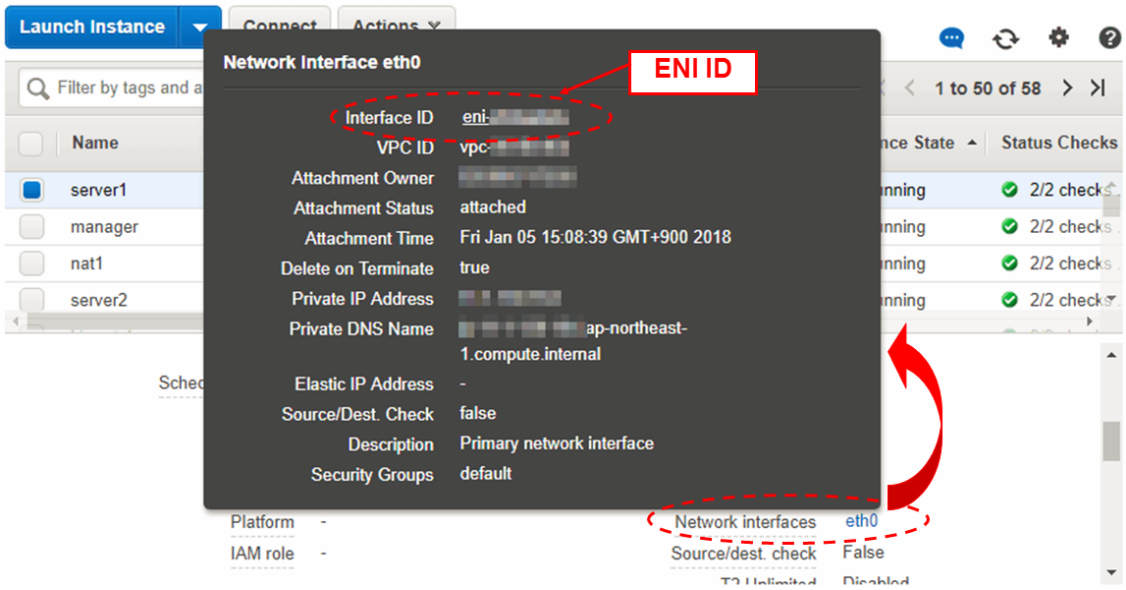
⇒ EC2 Management Console の [Instances] から、追加したインスタンス上で右クリックし、[Networking] - [Change Source/Dest. Check] をクリックすることで設定変更を行えます。

[7] Server Instance (Active), [8] Server Instance (Standby)

現用系側インスタンスに割り当てられた ENI、待機系側インスタンスに割り当てられた ENI は、いずれも ENI ID で識別できます。
各インスタンスの ENI ID （eni-xxxxxxxx） は後で AWS 仮想 IP リソース の設定時に必要となるため、 別途控えておきます。

インスタンスに割り当てられた ENI ID は以下の操作で確認できます。

1. インスタンスを選択して詳細情報を表示する。
2. [Network Interfaces] から該当するデバイスをクリックする。
3. ポップアップ表示中の [Interface ID] を参照する。



5. **NAT** を追加する

AWS CLI による VIP 制御処理を実行するために、HA クラスタノード用のインスタンスからリージョンのエンドポイントに対して HTTPS による通信が可能な状態にする必要があります。

そのために Public ネットワーク（Subnet-1A、および、Subnet-1B）上に NAT ゲートウェイを作成します。

NAT ゲートウェイの詳細については AWS のドキュメントを参照してください。

6. ルートテーブルを設定する。

AWS CLI が NAT 経由でリージョンのエンドポイントと通信可能にするための Internet Gateway へのルーティングと、VPC 内のクライアントが VIP アドレスにアクセス可能にするためのルーティングを追加します。VIP アドレスの CIDR ブロックは必ず 32 にする必要があります。

Public ネットワーク （図では Subnet-1A、および、Subnet-1B）のルートテーブル（Public-AB）には、以下のルーティングが必要となります。

- Route Table (Public-AB)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	Internet Gateway	追加（必須）
VIP アドレス （例では 10.1.0.20/32）	eni-xxxxxxxx （現用系側のインスタンス [7] Server Instance (Active) の ENI ID）	追加（必須）

Private ネットワーク （図では Subnet-2A、および、Subnet-2B）のルートテーブル（Private-A、および、Private-B）には、以下のルーティングが必要となります。

- Route Table (Private-A)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	NAT Gateway1	追加（必須）
VIP アドレス （例では 10.1.0.20/32）	eni-xxxxxxxx （現用系側のインスタンス [7] Server Instance (Active) の ENI ID）	追加（必須）

- Route Table (Private-B)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	NAT Gateway2	追加（必須）
VIP アドレス （例では 10.1.0.20/32）	eni-xxxxxxxx （現用系側のインスタンス [7] Server Instance (Active) の ENI ID）	追加（必須）

フェイルオーバ時に AWS 仮想 IP リソースが AWS CLI を使用して これらのルートテーブルに設定されている VIP アドレスへのルーティングをすべて待機系側のインスタンスの ENI に切り替えます。

[6] VIP

VIP アドレスは、VPC の CIDR の範囲外である必要があります。

ルートテーブルに設定した VIP アドレスは、後で AWS 仮想 IP リソース の設定時にも必要となるため、 別途控えておきます。

その他のルーティングは、環境にあわせて設定してください。

7. **ミラーディスク（EBS） を追加する**

必要に応じてミラーディスク（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 EBS を追加します。

⇒ EBS の追加は、EC2 Management Console の [Volumes] から、[Create Volume] をクリックして作成します。その後、作成したボリュームを任意のインスタンスに Attach することで行います。

5.2 インスタンスの設定

HA クラスタ用の各インスタンスにログインして以下の設定を実施します。

CLUSTERPRO がサポートしている AWS CLI のバージョンについては、『スタートアップガイド』-「AWS 仮想 IP リソース、AWS 仮想 IP モニタリソースの動作環境」を参照してください。

1. **SELinux を無効にする**

   CLUSTERPRO で必要な通信を行うためには SELinux は permissive または disabled である必要があります。SELinux の動作状態は以下のコマンドで確認します。

   ```
   $ getenforce
   Enforcing
   ```

   ※ **Enforcing** が出れば有効になっています

   SELinux の動作状態を変更するためには、`/etc/sysconfig/selinux` で SELinux を disabled に修正し、再起動します。その後、getenforce コマンドで Disabled になっていることを確認します。

2. **Firewall を設定する**

   必要に応じて Firewall の設定を変更します。

   CLUSTERPRO 関連コンポーネントが使用するポート番号については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」を参照し、設定してください。

3. **AWS CLI のインストール**

   AWS CLI をインストールします。

   AWS CLI のインストールパスは、以下のいずれかにする必要があります。

   `/sbin`、`/bin`、`/usr/sbin`、`/usr/bin`、`/usr/local/bin`

   AWS CLI のセットアップ方法に関する詳細は下記を参照してください。

   https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/cli-chap-install.html

（Python または AWS CLI のインストールを行った時点ですでに CLUSTERPRO がインストール済の場合は、OS を再起動してから CLUSTERPRO の操作を行ってください。）

4. **AWS アクセスキー ID の登録**

シェルから、以下のコマンドを実行します。

```
$ sudo aws configure
```

質問に対して、AWS アクセスキー ID などの情報を入力します。

インスタンスに IAM ロールを割り当てているか否かで 2 通りの設定に分かれます。

◇ IAM ロールを割り当てているインスタンスの場合

```
AWS Access Key ID [None]: （Enter のみ）
AWS Secret Access Key [None]: （Enter のみ）
Default region name [None]: <既定のリージョン名>
Default output format [None]: text
```

◇ IAM ロールを割り当てていないインスタンスの場合

```
AWS Access Key ID [None]: <AWS アクセスキー ID>
AWS Secret Access Key [None]: <AWS シークレットアクセスキー>
Default region name [None]: <既定のリージョン名>
Default output format [None]: text
```

"Default output format"は、"text"以外を指定することも可能です。

もし誤った内容を設定してしまった場合は、`/root/.aws` をディレクトリごと消去してから上記操作をやり直してください。

5. **ミラーディスクの準備**

ミラーディスク用に EBS を追加していた場合は、EBS をパーティション分割し、それぞれクラスタパーティション、データパーティションに使用します。

ミラーディスク用のパーティションについては、『インストール&設定ガイド』の「システム構成を決定する」-「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)」を参照してください。

6. **CLUSTERPRO のインストール**

インストール手順は『インストール&設定ガイド』を参照してください。
CLUSTERPRO のインストール媒体を導入環境に格納します。
（データの転送に関しては FTP、SCP、Amazon S3 経由など任意です。）

インストール完了後、OS の再起動を行ってください。

5.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および、接続方法は『インストール&設定ガイド』の「クラスタ構成情報を作成する」を参照してください。

ここでは以下の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
- AWS 仮想 IP リソース
- AWS AZ モニタリソース
- AWS 仮想 IP モニタリソース
- NP 解決 (HTTP 方式)

上記以外の設定は、『インストール&設定ガイド』を参照してください。

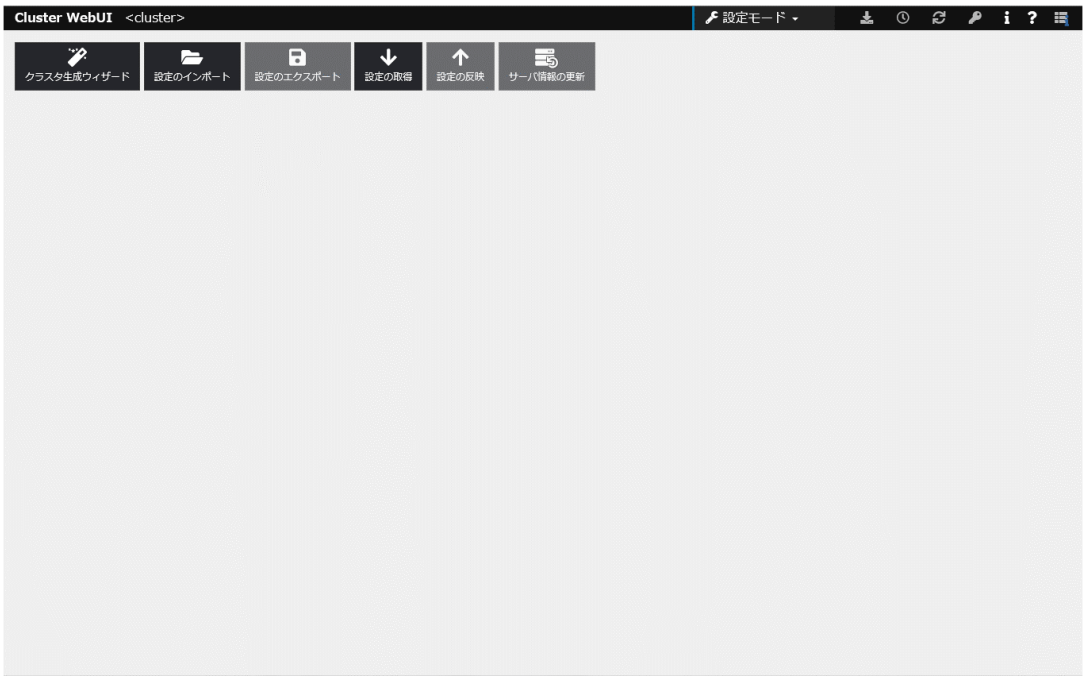
1. クラスタの構築

   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

     【手順】

     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] 画面の [クラスタ] 画面が表示されます。

   [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. 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 Private 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 Private 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。

   HTTP 方式の NP 解決を設定します。

   [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

  フェイルオーバグループを作成します。

  【手順】

  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

必要に応じてミラーディスク（EBS） にあわせたミラーディスクリソース を作成します。

詳細は『リファレンスガイド』の「ミラーディスクリソースを理解する」を参照してください。

【手順】

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] ボックスにグループリソース名 (md) 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. [詳細設定] 画面が表示されます。

   [マウントポイント] にミラーディスクのマウント先、[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「 5.2. インスタンスの設定 」-「6. ミラーディスクの準備」で作成した

パーティションのデバイス名を入力します。 [完了] をクリックして設定を終了します。

- AWS 仮想 IP リソース

AWS CLI を利用して、VIP の制御を行う AWS 仮想 IP リソースを追加します。

詳細は『リファレンスガイド』の「AWS 仮想 IP リソースを理解する」を参照してください。

【手順】

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 (AWS 仮想 IP リソース) を選択して、[名前] ボックスにグループリソース名 (awsvip1) 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。

   [共通] タブの [IP アドレス] ボックスに、付与したい VIP アドレスを設定します (図 5.1 システム構成 VIP 制御による HA クラスタ の [6] が該当)。

   [VPC ID] ボックスに、インスタンスが所属する VPC の ID を設定します (図 5.1 システム構成 VIP 制御による HA クラスタ の [1] が該当)。

   サーバ個別設定を行う場合、[共通] タブでは、任意のサーバの VPC ID を記載し、他のサーバは個別設定を行うようにしてください。

   [ENI ID] ボックスに、VIP アドレスのルーティング先となる現用系側のインスタンスの ENI ID を設定します (図 5.1 システム構成 VIP 制御による HA クラスタ の [7] が該当)。

サーバ別設定が必須です。[共通] タブでは、任意のサーバの ENI ID を記載し、他のサーバは個別設定を行うようにしてください。

6. 各ノードのタブをクリックし、ノード別設定を行います。

   [個別に設定する] をチェックします。

   [VPC ID] ボックスに [共通] タブで設定した VPC ID と同じものが設定されていることを確認します (図 5.1 システム構成 VIP 制御による HA クラスタ の [1] が該当)。

   [ENI ID] ボックスに、そのノードに対応するインスタンスの ENI ID を設定します (図 5.1 システム構成 VIP 制御による HA クラスタ の [7] が該当)。

7. [完了] をクリックして設定を終了します。

3. モニタリソースの追加

- AWS AZ モニタリソース

監視 コマンドを利用して、指定した AZ が利用可能かどうかを確認する AWS AZ モニタリソースを作成します。

詳細は『リファレンスガイド』の「AWS AZ モニタリソースを理解する」を参照してください。

【手順】

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (AWS AZ モニタ) を選択し、[名前] ボックスにモニタリソース名 (awsazw1) 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。
   何も指定せず [次へ] をクリックします。

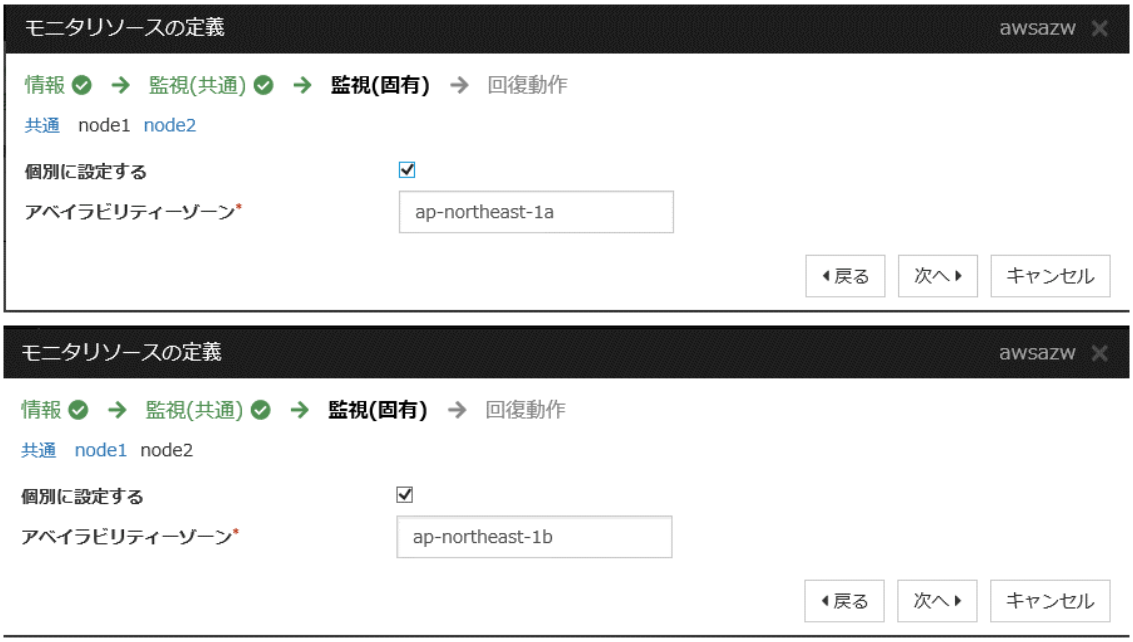
4. [監視 (固有)] 画面が表示されます。

   [共通] タブの [アベイラビリティーゾーン] ボックスに監視するアベイラビリティーゾーンを入力します（現用系側のインスタンスのアベイラビリティーゾーンを設定します）(図 5.1 システム構成 VIP 制御による HA クラスタ の [2] が該当。

5. 各ノードのタブをクリックし、ノード別設定を行います。

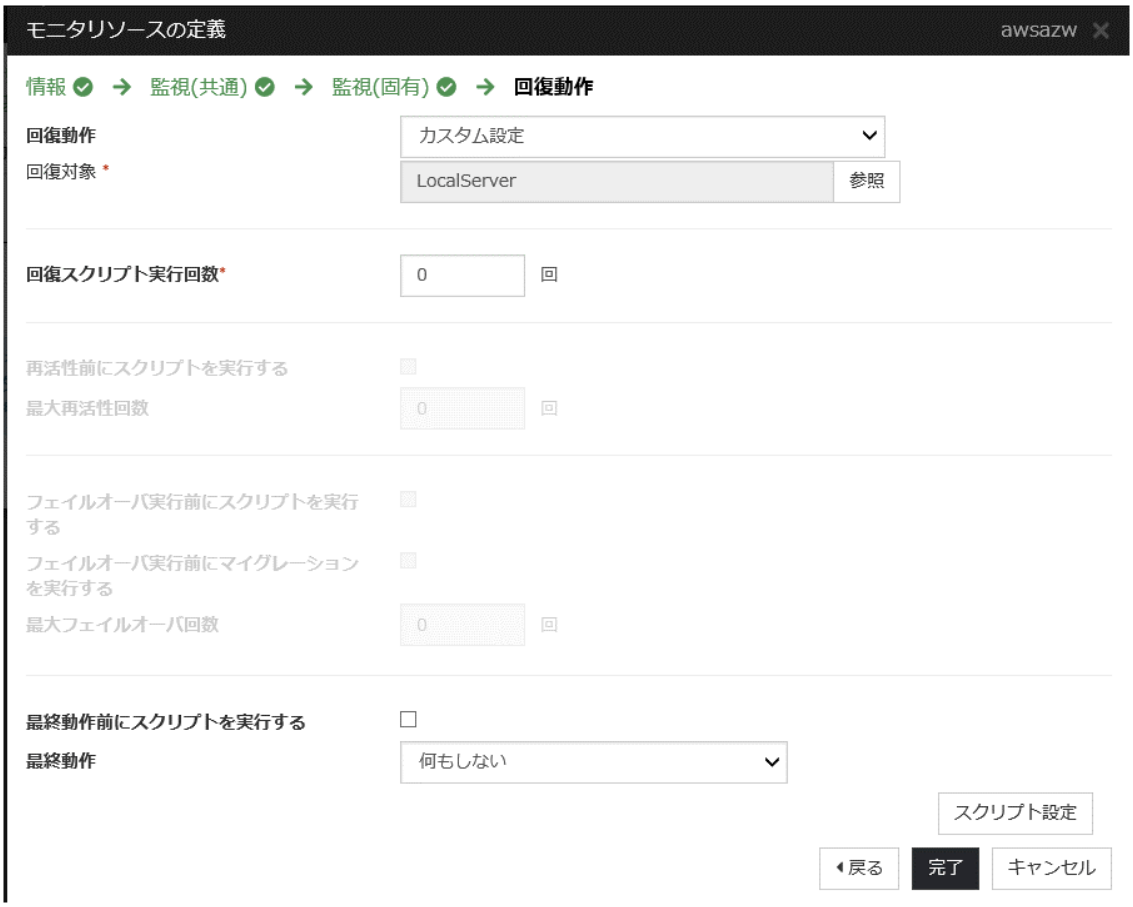
   [個別に設定する] をチェックします。

   [アベイラビリティーゾーン] ボックスに、そのノードに対応するインスタンスのアベイラビリティーゾーンを設定します (図 5.1 システム構成 VIP 制御による HA クラスタ の [2][3] が該当)。[次へ] をクリックします。



6. [回復動作] 画面が表示されます。

   [回復対象] に [LocalServer] を設定します。



7. [完了] をクリックして設定を終了します。

- AWS 仮想 IP モニタリソース

  AWS 仮想 IP リソース追加時に、自動的に追加されます。

  VIP アドレスの存在及びルートテーブルの健全性を確認します。

  詳細は『リファレンスガイド』-「AWS 仮想 IP モニタリソースを理解する」を参照してください。

4. 設定の反映とクラスタの起動

1. Cluster WebUI の設定モードから、[設定の反映] をクリックします。

   「設定を反映しますか。」 というポップアップメッセージが表示されるので、[OK] をクリックします。

アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[OK] をクリックします。

アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。

2. Cluster WebUI のツールバーのドロップダウンメニューで [操作モード] を選択して、操作モードに切り替えます。

3. 使用するリソースによって以降の手順が異なります。詳細は『インストール&設定ガイド』-「クラスタを生成するには」を参照してください。

第 6 章

EIP 制御による HA クラスタの設定

本章では、EIP 制御による HA クラスタの構築手順を説明します。

図中の Server Instance (Active) は現用系サーバ、Server Instance (Standby) は待機系サーバのインスタンスです。

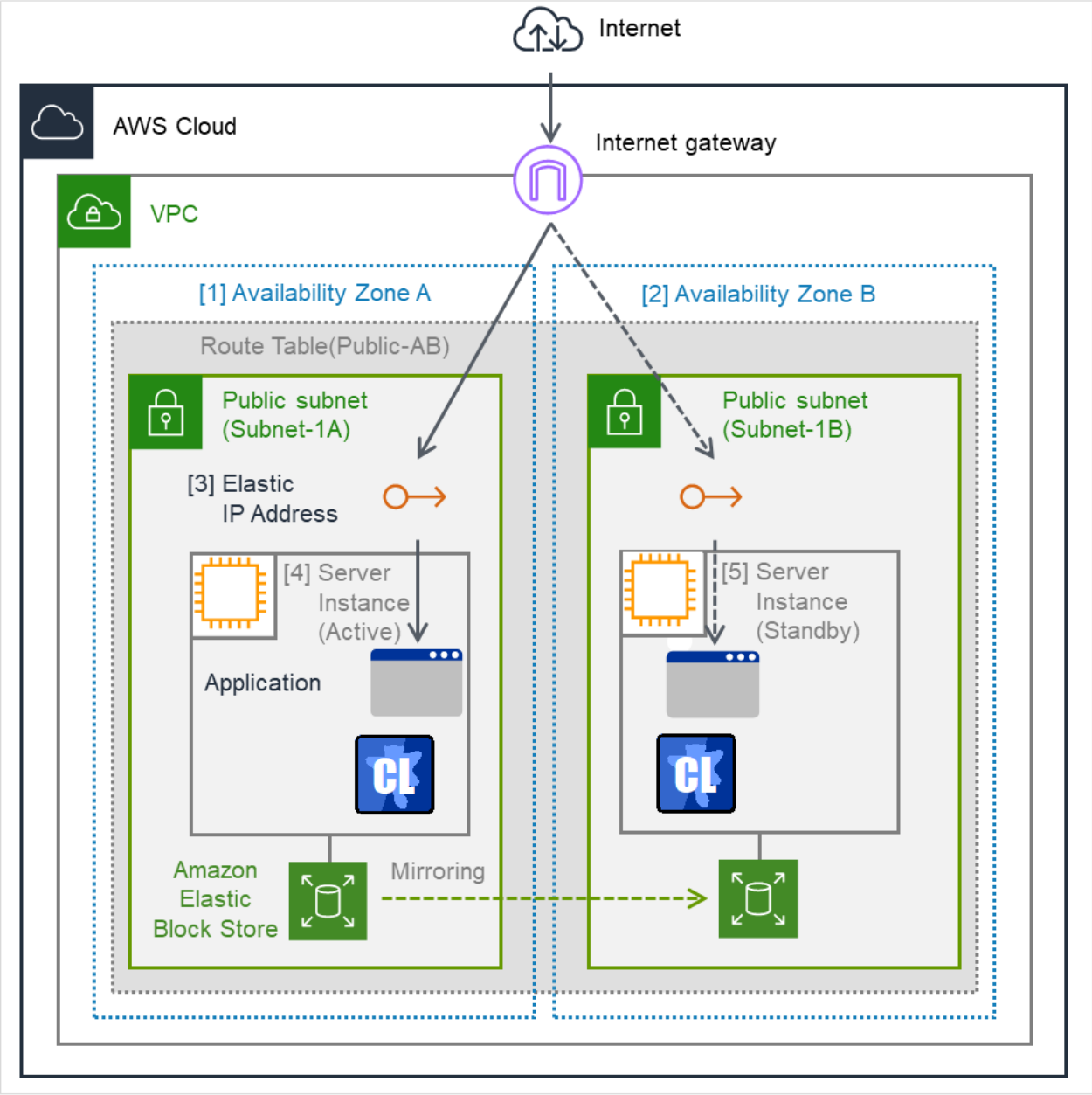


図 6.1　システム構成 EIP 制御による HA クラスタ

CIDR (VPC)	10.0.0.0/16
Public subnet (Subnet-1A)	10.0.10.0/24
Public subnet (Subnet-1B)	10.0.20.0/24

6.1 VPC 環境の設定

VPC Management Console、および、EC2 Management Console 上で VPC の構築を行います。

図中および説明中の IP アドレスは一例であり、実際の設定時は VPC に割り当てられている IP アドレスに読み替えてください。既存の VPC に CLUSTERPRO を適用する場合は、不足しているサブネットを追加するなど適切に読み替えてください。

1. **VPC およびサブネットを設定する**

   最初に VPC およびサブネットを作成します。

   ⇒ VPC Management Console の [VPC] および [Subnets] で VPC およびサブネットの追加操作を行います。

2. **Internet Gateway を設定する。**

   VPC からインターネットにアクセスするための Internet Gateway を追加します。

   ⇒ VPC Management Console の [Internet Gateways] から [Create internet gateway] をクリックして作成します。その後、 作成した Internet Gateway を VPC に Attach します。

3. **Network ACL/Security Group を設定する**

   VPC 内外からの不正なネットワークアクセスを防ぐために、Network ACL、および、Security Group を適切に設定します。

   Public ネットワーク （Subnet-1A、および、Subnet-1B）内に配置予定の HA クラスタノード用のインスタンスから、HTTPS で Internet Gateway と通信可能となるように、また、Cluster WebUI やインスタンス同士の通信も可能となるよう各経路について Network ACL や Security Group の設定を変更します。

   ⇒ 設定変更は、 VPC Management Console の [Network ACLs] 、および、[Security Groups] から行います。

   CLUSTERPRO 関連コンポーネントが使用するポート番号については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」を参照し、設定してください。

4. **HA クラスタ用のインスタンスを追加する**

   HA クラスタノード用のインスタンスを Public ネットワーク（Subnet-1A、および、Subnet-1B）に作成します。

   作成時には Public IP を有効となるように設定してください。Public IP を使用しないで作成した場合は、後から EIP を追加するか、NAT を用意する必要があります（本書ではこのケースの説明は割愛します）。

IAM ロールをインスタンスに割り当てて使用する場合は、IAM ロールを指定してください。

⇒ インスタンスの作成は、 EC2 Management Console の [Instances] から、 [Launch Instance] をクリックして行います。

⇒ IAM の設定については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」-「AWS 環境における IAM の設定について」を参照し、設定してください。

作成した各インスタンスに割り当てられている Elastic Network Interface (以下、ENI) の ID を確認します。

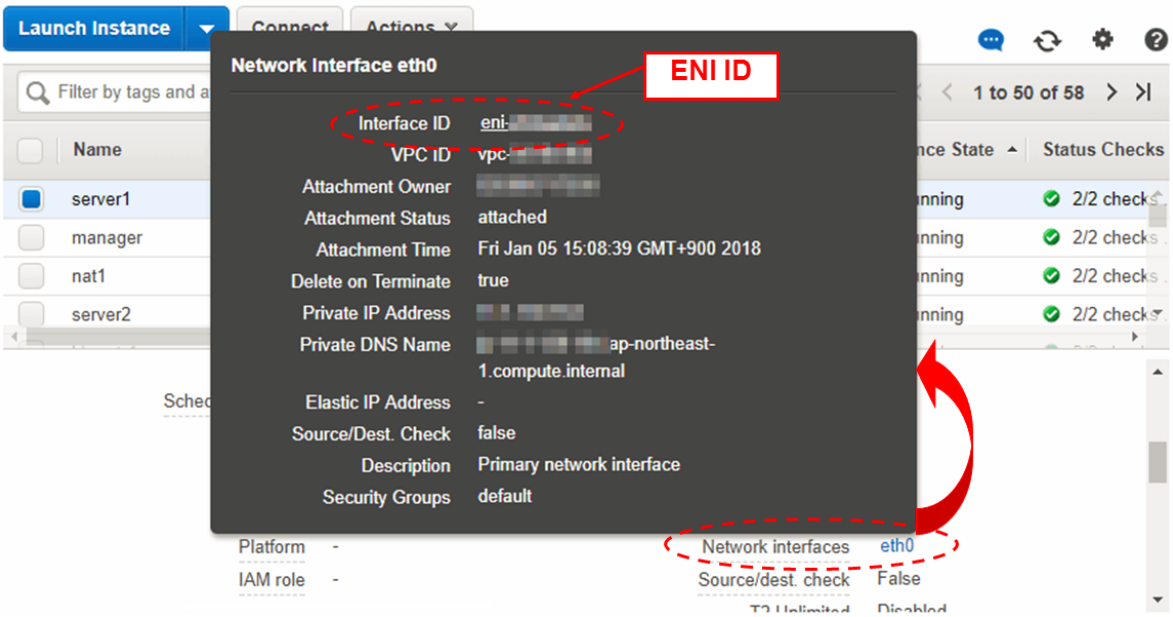
[4] Server Instance (Active), [5] Server Instance (Standby)

現用系側インスタンスに割り当てられた ENI、待機系側インスタンスに割り当てられた ENI は、いずれも ENI ID で識別できます。

各インスタンスの ENI ID （eni-xxxxxxxx） は後で AWS Elastic IP リソース の設定時に必要となるため、 別途控えておきます。

インスタンスに割り当てられた ENI ID は以下の操作で確認できます。

1. インスタンスを選択して詳細情報を表示する。
2. [Network Interfaces] から該当するデバイスをクリックする。
3. ポップアップ表示中の [Interface ID] を参照する。



5. **EIP** を追加する

インターネット側から VPC 内のインスタンスにアクセスするための EIP を追加します。

⇒ EIP の追加は、 EC2 Management Console の [Elastic IPs] から、 [Allocate new address] をクリックして行います。

[3] Elastic IP Address

EIP は EIP Allocation ID で識別できます。

ここで追加した **EIP** の **Allocation ID** （**eipalloc-xxxxxxxx**） は後で **AWS Elastic IP** リソース の設定時に必要となるため、 別途控えておきます。

6. ルートテーブルを設定する。

AWS CLI が NAT 経由でリージョンのエンドポイントと通信可能にするための Internet Gateway へのルーティングを追加します。

Public ネットワーク （図では Subnet-1A、および、Subnet-1B）のルートテーブル（Public-AB）には、以下のルーティングが必要となります。

- Route Table (Public-AB)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	Internet Gateway	追加（必須）

フェイルオーバ時に AWS Elastic IP リソースが AWS CLI を使用して、現用系側のインスタンスに割り当てられている EIP の切り離しを行い、 待機系側のインスタンスの ENI に EIP を割り当てます。

その他のルーティングは、環境にあわせて設定してください。

7. ミラーディスク（**EBS**） を追加する

必要に応じてミラーディスク（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 EBS を追加します。

⇒ EBS の追加は、EC2 Management Console の [Volumes] から、[Create Volume] をクリックして作成します。その後、作成したボリュームを任意のインスタンスに Attach することで行います。

6.2 インスタンスの設定

HA クラスタ用の各インスタンスにログインして以下の設定を実施します。

CLUSTERPRO がサポートしている Python、および、AWS CLI のバージョンについては、『スタートアップガイド』-「CLUSTERPRO の動作環境」-「AWS Elastic IP リソース、AWS Elastic IP モニタリソース、AWS AZ モニタリソースの動作環境」を参照してください。

1. **SELinux を無効にする**

   CLUSTERPRO で必要な通信を行うためには SELinux は permissive または disabled である必要があります。SELinux の動作状態は以下のコマンドで確認します。

   ```
   $ getenforce
   Enforcing
   ```

   ※ **Enforcing** が出れば有効になっています

   SELinux の動作状態を変更するためには、`/etc/sysconfig/selinux` で SELinux を disabled に修正し、再起動します。その後、getenforce コマンドで Disabled になっていることを確認します。

2. **Firewall を設定する**

   必要に応じて Firewall の設定を変更します。

   CLUSTERPRO 関連コンポーネントが使用するポート番号については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」を参照し、設定してください。

3. **Python のインストール**

   CLUSTERPRO が必要とする Python をインストールします。

   まず、Python がインストールされていることを確認します。

   未インストールの場合、yum コマンドなどでインストールします。

   python コマンドのインストールパスは、以下のいずれかにする必要があります。環境変数 PATH において、最初に見つかった python コマンドを使用します。

   `/sbin`、`/bin`、`/usr/sbin`、`/usr/bin`

Python3 のみインストールされており /usr/bin/python が存在しない場合、/usr/bin/python3.*x* (*x* はバージョン) もしくは /usr/bin/python3 に対し /usr/bin/python のシンボリックリンクを作成してください。

4. **AWS CLI のインストール**

AWS CLI をインストールします。

AWS CLI のインストールパスは、以下のいずれかにする必要があります。

/sbin、/bin、/usr/sbin、/usr/bin、/usr/local/bin

AWS CLI のセットアップ方法に関する詳細は下記を参照してください。

https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/cli-chap-install.html

（Python または AWS CLI のインストールを行った時点ですでに CLUSTERPRO がインストール済の場合は、OS を再起動してから CLUSTERPRO の操作を行ってください。）

5. **AWS アクセスキー ID の登録**

シェルから、以下のコマンドを実行します（必ず sudo をつけて root 権限で実行します）。

```
$ sudo aws configure
```

質問に対して、AWS アクセスキー ID などの情報を入力します。
インスタンスに IAM ロールを割り当てているか否かで 2 通りの設定に分かれます。

◇ IAM ロールを割り当てているインスタンスの場合

```
AWS Access Key ID [None]: （Enter のみ）
AWS Secret Access Key [None]: （Enter のみ）
Default region name [None]: <既定のリージョン名>
Default output format [None]: text
```

◇ IAM ロールを割り当てていないインスタンスの場合

```
AWS Access Key ID [None]: <AWS アクセスキー ID>
AWS Secret Access Key [None]: <AWS シークレットアクセスキー>
Default region name [None]: <既定のリージョン名>
Default output format [None]: text
```

"Default output format"は、"text"以外を指定することも可能です。

もし誤った内容を設定してしまった場合は、`/root/.aws` をディレクトリごと消去してから上記操作をやり直してください。

6. ミラーディスクの準備

ミラーディスク用に EBS を追加していた場合は、EBS をパーティション分割し、それぞれクラスタパーティション、データパーティションに使用します。

ミラーディスク用のパーティションについては、『インストール&設定ガイド』の「システム構成を決定する」-「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)」を参照してください。

7. **CLUSTERPRO** のインストール

インストール手順は『インストール&設定ガイド』を参照してください。

CLUSTERPRO のインストール媒体を導入環境に格納します。

（データの転送に関しては FTP、SCP、Amazon S3 経由など任意です。）

インストール完了後、OS の再起動を行ってください。

6.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および、接続方法は『インストール&設定ガイド』の「クラスタ構成情報を作成する」を参照してください。

ここでは以下の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
- AWS EIP リソース
- AWS AZ モニタリソース
- AWS EIP モニタリソース
- NP 解決 (HTTP 方式)

上記以外の設定は、『インストール&設定ガイド』を参照してください。

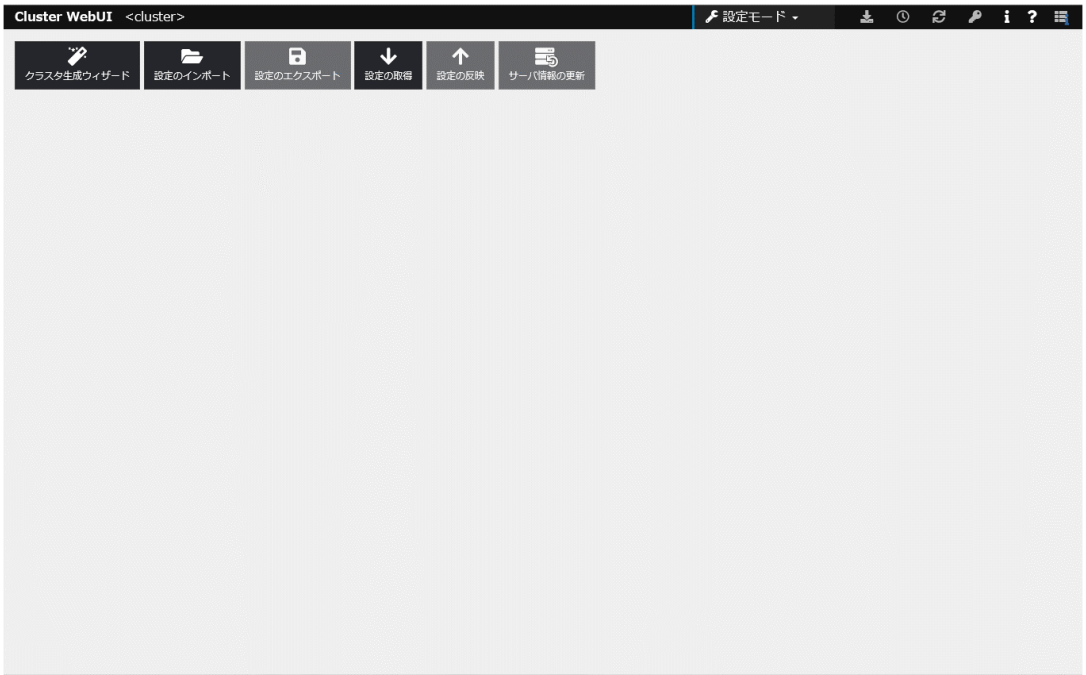
1. クラスタの構築

   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

     【手順】

     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] 画面の [クラスタ] 画面が表示されます。

   [クラスタ名] に任意のクラスタ名を入力します。

   [次へ] をクリックします。

3. [基本設定] 画面が表示されます。

   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 Private 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 Private 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。

   HTTP 方式の NP 解決を設定します。

   [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

  フェイルオーバグループを作成します。

  【手順】

  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

  必要に応じてミラーディスク（EBS）にあわせたミラーディスクリソース を作成します。
  詳細は『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」を参照してください。

【手順】

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] ボックスにグループリソース名 (md) 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。

   [マウントポイント] にミラーディスクのマウント先、[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「6.2. インスタンスの設定」-「6. ミラーディスクの準備」で作成したパーティションのデバイス名を入力します。 [完了] をクリックして設定を終了します。

- AWS Elastic IP リソース

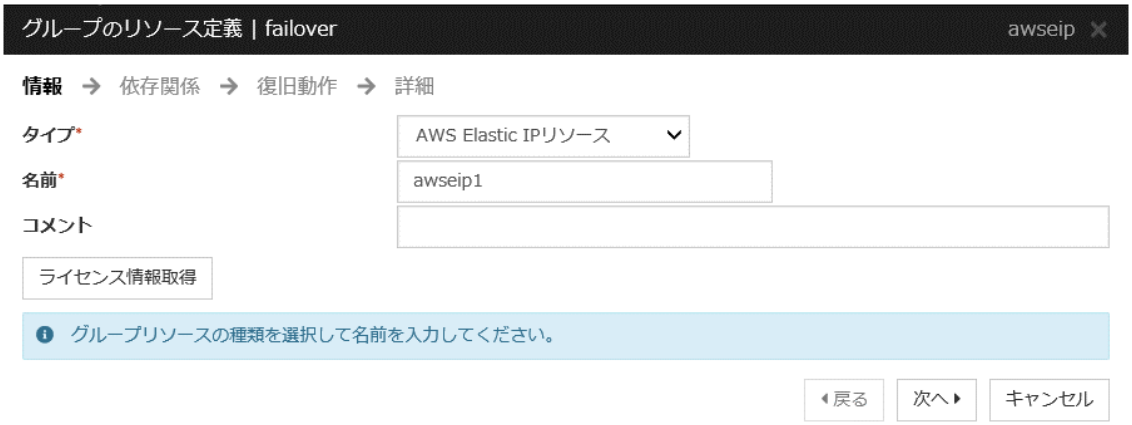
AWS CLI を利用して、EIP の制御を行う AWS Elastic IP リソースを追加します。

詳細は『リファレンスガイド』-「AWS Elastic IP リソースを理解する」を参照してください。

【手順】

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 (AWS Elastic IP リソース) を選択して、[名前] ボックスにグループリソース名 (awseip1) 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。

   [共通] タブの [EIP ALLOCATION ID] ボックスに、付与したい EIP の Allocation ID を設定します (図 6.1 システム構成 EIP 制御による HA クラスタ の [3][4] が該当)。

   [ENI ID] ボックスに、EIP を割り当てる現用系側のインスタンスの ENI ID を設定します。

6. 各ノードのタブをクリックし、ノード別設定を行います。

   [個別に設定する] をチェックします。

   [ENI ID] ボックスに、そのノードに対応するインスタンスの ENI ID を設定します (図 6.1 システム構成 EIP 制御による HA クラスタ の [4][5] が該当)。

7. [完了] をクリックして設定を終了します。

3. モニタリソースの追加

- AWS AZ モニタリソース

監視 コマンドを利用して、指定した AZ が利用可能かどうかを確認する AWS AZ モニタリソースを作成します。
詳細は『リファレンスガイド』-「AWS AZ モニタリソースを理解する」を参照してください。

【手順】

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (AWS AZ モニタ) を選択し、[名前] ボックスにモニタリソース名 (awsazw1) 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。

何も指定せず [次へ] をクリックします。

4. [監視 (固有)] 画面が表示されます。

   [共通] タブの [アベイラビリティーゾーン] ボックスに監視するアベイラビリティーゾーンを入力します（現用系側のインスタンスのアベイラビリティーゾーンを設定します）(図 6.1 システム構成 EIP 制御による HA クラスタ の [1] が該当)。

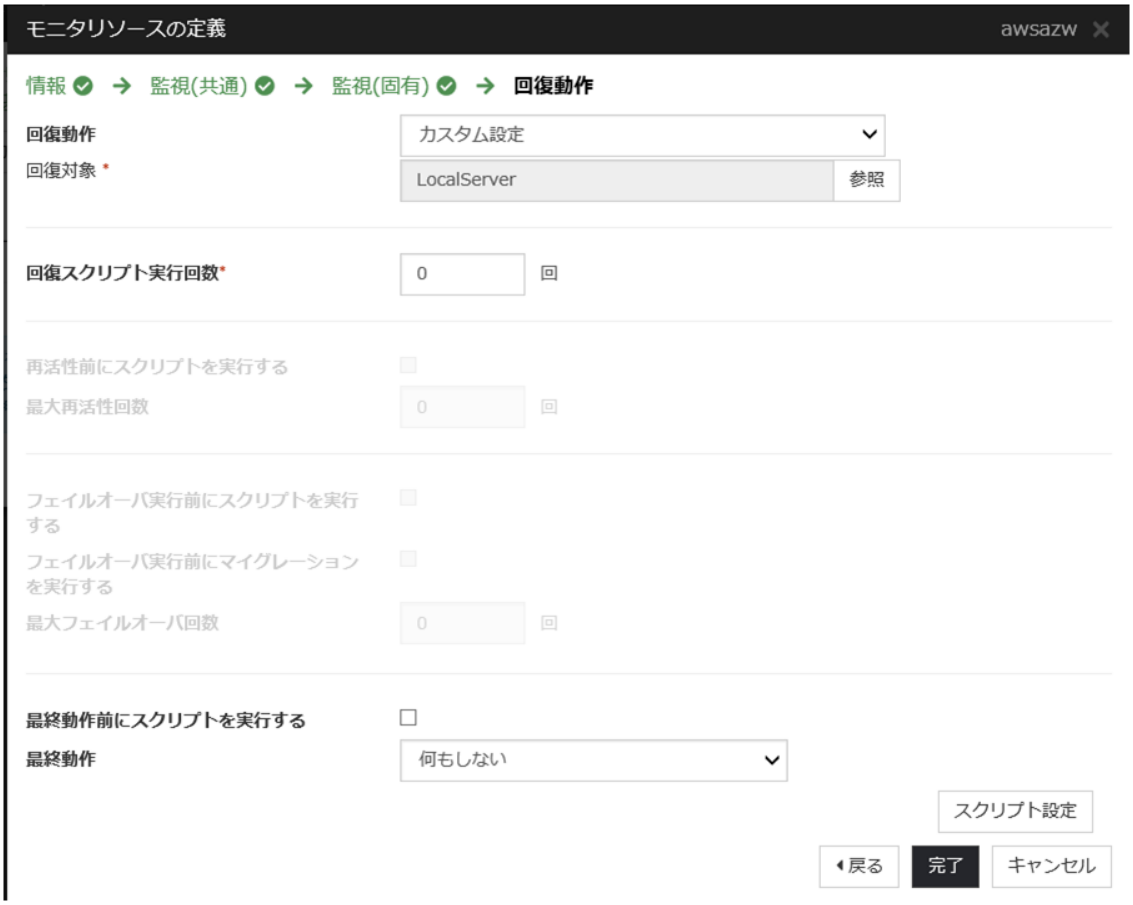
5. 各ノードのタブをクリックし、ノード別設定を行います。

   [個別に設定する] をチェックします。

   [アベイラビリティーゾーン] ボックスに、そのノードに対応するインスタンスのアベイラビリティーゾーンを設定します (図 6.1 システム構成 EIP 制御による HA クラスタ の [1][2] が該当)。[次へ] をクリックします。

6. [回復動作] 画面が表示されます。

   [回復対象] に [LocalServer] を設定します。



7. [完了] をクリックして設定を終了します。

- AWS Elastic IP モニタリソース

  AWS Elastic IP リソース追加時に、自動的に追加されます。

  現用系側のインスタンスに割り当てられている EIP アドレスへの通信を監視することで、EIP アドレスの健全性を確認します。

  詳細は『リファレンスガイド』-「AWS Elastic IP モニタリソースを理解する」を参照してください。

4. 設定の反映とクラスタの起動

1. Cluster WebUI の設定モードから、[設定の反映] をクリックします。

「設定を反映しますか。」 というポップアップメッセージが表示されるので、[OK] をクリックします。

アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[OK] をクリックします。

アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。

2. Cluster WebUI のツールバーのドロップダウンメニューで [操作モード] を選択して、操作モードに切り替えます。

3. 使用するリソースによって以降の手順が異なります。詳細は『インストール&設定ガイド』-「クラスタを生成するには」を参照してください。

第 7 章

DNS 名制御による HA クラスタの設定

本章では、DNS 名制御による HA クラスタの構築手順を説明します。

図中の Server Instance (Active) は現用系サーバ、Server Instance (Standby) は待機系サーバのインスタンスです。

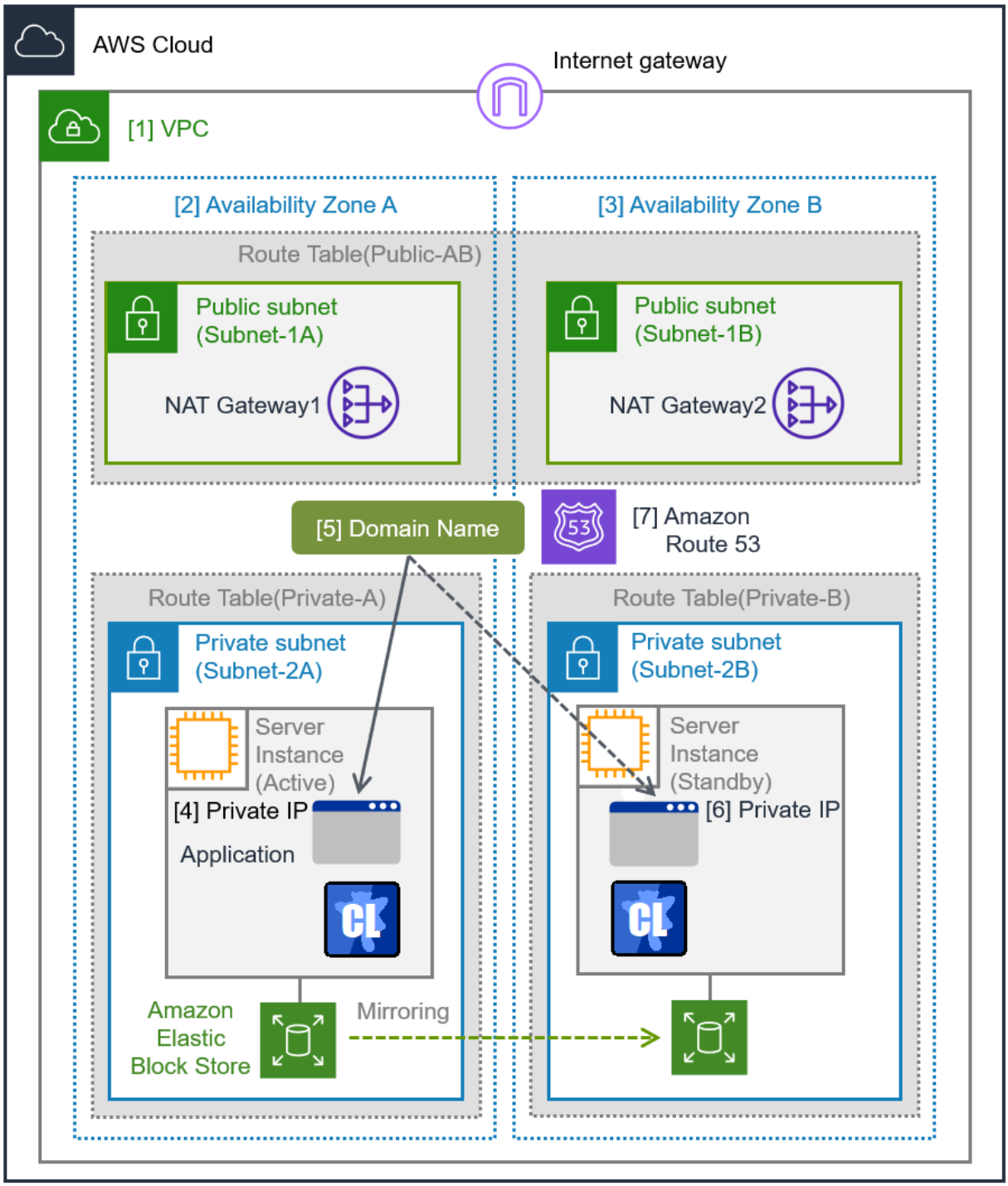


図 7.1　システム構成 DNS 名制御による HA クラスタ

CIDR (VPC)	10.0.0.0/16
Domain Name	srv.hz1.local

次のページに続く

表 7.1 – 前のページからの続き

Public subnet (Subnet-1A)	10.0.10.0/24
Public subnet (Subnet-1B)	10.0.20.0/24
Private subnet (Subnet-2A)	10.0.110.0/24
Private subnet (Subnet-2B)	10.0.120.0/24

7.1 VPC 環境の設定

VPC Management Console、および、EC2 Management Console 上で VPC の構築を行います。

図中および説明中の IP アドレスは一例であり、実際の設定時は VPC に割り当てられている IP アドレスに読み替えてください。既存の VPC に CLUSTERPRO を適用する場合は、不足しているサブネットを追加するなど適切に読み替えてください。

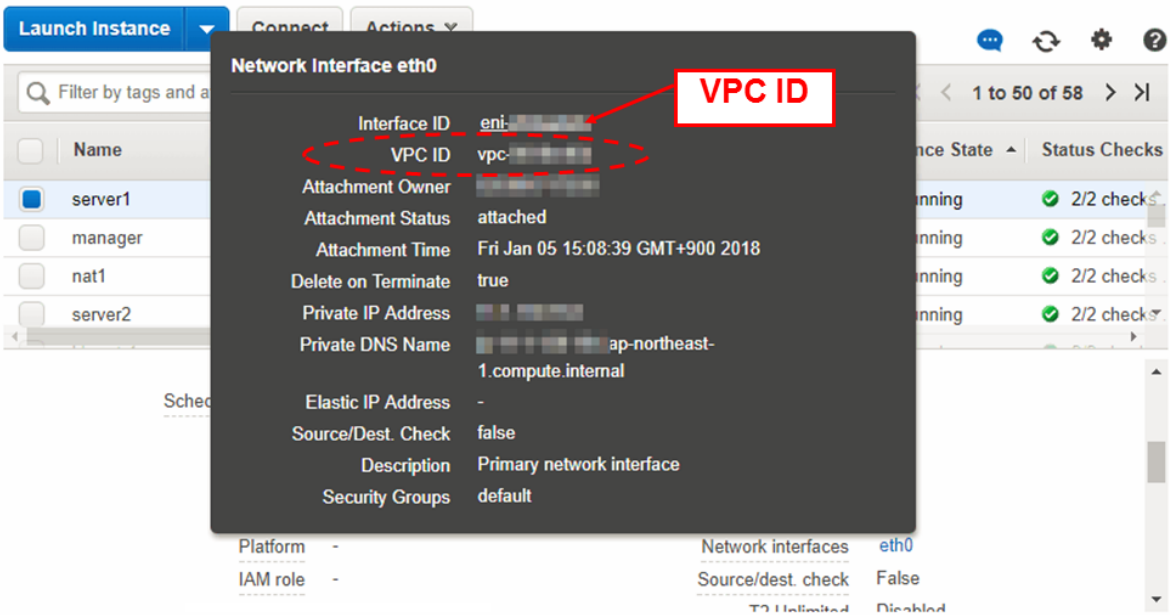
1. **VPC** およびサブネットを設定する

   最初に VPC およびサブネットを作成します。

   ⇒ VPC Management Console の [VPC] および [Subnets] で VPC およびサブネットの追加操作を行います。

   [1] VPC

   VPC ID （vpc-xxxxxxxx） は後でホストゾーンの追加時に必要となるため、別途控えておきます。



2. **Internet Gateway** を設定する。

   VPC からインターネットにアクセスするための Internet Gateway を追加します。

   ⇒ VPC Management Console の [Internet Gateways] から [Create internet gateway] をクリックして作成します。その後、 作成した Internet Gateway を VPC に Attach します。

3. **Network ACL/Security Group** を設定する

VPC 内外からの不正なネットワークアクセスを防ぐために、Network ACL、および、Security Group を適切に設定します。

Private ネットワーク（Subnet-2A および Subnet-2B）内に配置予定の HA クラスタノード用のインスタンスから、HTTPS で Internet Gateway と通信可能となるように、また、Cluster WebUI やインスタンス同士の通信も可能となるよう各経路について Network ACL や Security Group の設定を変更します。

⇒ 設定変更は、 VPC Management Console の [Network ACLs] 、および、[Security Groups] から行います。

CLUSTERPRO 関連コンポーネントが使用するポート番号については、『スタートアップガイド』の「注意制限事項」-「CLUSTERPRO インストール前」を参照し、設定してください。

4. **HA クラスタ用のインスタンスを追加する**

HA クラスタノード用のインスタンスを Private ネットワーク（Subnet-2A、および、Subnet-2B）に作成します。

IAM ロールをインスタンスに割り当てて使用する場合は、IAM ロールを指定してください。

⇒ インスタンスの作成は、 EC2 Management Console の [Instances] から、 [Launch Instance] をクリックして行います。

⇒ IAM の設定については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」-「AWS 環境における IAM の設定について」を参照し、設定してください。

5. **NAT を追加する**

AWS CLI による DNS 名制御処理を実行するために、HA クラスタノード用のインスタンスからリージョンのエンドポイントに対して HTTPS による通信が可能な状態にする必要があります。

そのために Public ネットワーク（Subnet-1A、および、Subnet-1B）上に NAT ゲートウェイを作成します。

NAT ゲートウェイの詳細については AWS のドキュメントを参照してください。

6. **ルートテーブルを設定する。**

AWS CLI が NAT 経由でリージョンのエンドポイントと通信可能にするための Internet Gateway へのルーティングを追加します。

Public ネットワーク（図では Subnet-1A、および、Subnet-1B）のルートテーブル（Public-AB）には、以下のルーティングが必要となります。

- Route Table (Public-AB)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	Internet Gateway	追加（必須）

Private ネットワーク（図では Subnet-2A、および、Subnet-2B）のルートテーブル（Private-A、および Private-B）には、以下のルーティングが必要となります。

- Route Table (Private-A)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	NAT Gateway1	追加（必須）

- Route Table (Private-B)

Destination	Target	備考
VPC のネットワーク （例では 10.0.0.0/16)	local	最初から存在
0.0.0.0/0	NAT Gateway2	追加（必須）

その他のルーティングは、環境にあわせて設定してください。

7. ホストゾーンを追加する

Amazon Route 53 に Private ホストゾーンを追加します。

⇒ ホストゾーンの追加は、 Route 53 Management Console の [DNS management] を選択し、[Create Hosted Zone] をクリックして作成します。[Type] ボックスは [Private Hosted Zone for Amazon VPC] を

選択し、[VPC ID] ボックスにインスタンスが所属する VPC の ID (図 7.1 システム構成 DNS 名制御による HA クラスタ の [1] に該当) を設定します。

[7] Amazon Route 53 (Hosted Zone)

ホストゾーンは Hosted Zone ID で識別できます。

Hosted Zone ID は後で AWS DNS リソースの設定時に必要となるため、別途控えておきます。

なお、本書では、クラスタを Private なサブネット上に配置して VPC 内のクライアントからアクセスする構成を採用しているために Private ホストゾーンを追加していますが、Public なサブネット上に配置してインターネット側の任意のクライアントからアクセスする構成の場合は、Public ホストゾーンを追加して ください。

8. **ミラーディスク（EBS） を追加する**

必要に応じてミラーディスク（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 EBS を追加します。

⇒ EBS の追加は、EC2 Management Console の [Volumes] から、[Create Volume] をクリックして作成します。その後、作成したボリュームを任意のインスタンスに Attach することで行います。

7.2 インスタンスの設定

HA クラスタ用の各インスタンスにログインして以下の設定を実施します。

CLUSTERPRO がサポートしている Python、および、AWS CLI のバージョンについては、『スタートアップガイド』-「CLUSTERPRO の動作環境」-「AWS DNS リソース、AWS DNS モニタリソースの動作環境」を参照してください。

1. **SELinux を無効にする**

   CLUSTERPRO で必要な通信を行うためには SELinux は permissive または disabled である必要があります。SELinux の動作状態は以下のコマンドで確認します。

   ```
   $ getenforce
   Enforcing
   ```

   ※ **Enforcing が出れば有効になっています**

   SELinux の動作状態を変更するためには、`/etc/sysconfig/selinux` で SELinux を disabled に修正し、再起動します。その後、getenforce コマンドで Disabled になっていることを確認します。

2. **Firewall を設定する**

   必要に応じて Firewall の設定を変更します。

   CLUSTERPRO 関連コンポーネントが使用するポート番号については、『スタートアップガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO インストール前」を参照し、設定してください。

3. **Python のインストール**

   CLUSTERPRO が必要とする Python をインストールします。

   まず、Python がインストールされていることを確認します。

   未インストールの場合、yum コマンドなどでインストールします。

   python コマンドのインストールパスは、以下のいずれかにする必要があります。環境変数 PATH において、最初に見つかった python コマンドを使用します。

   `/sbin`、`/bin`、`/usr/sbin`、`/usr/bin`

   Python3 のみインストールされており `/usr/bin/python` が存在しない場合、`/usr/bin/python3.`*x* (*x* はバージョン) もしくは `/usr/bin/python3` に対し `/usr/bin/python` のシンボリックリンクを作成してください。

4. **AWS CLI のインストール**

AWS CLI をインストールします。

AWS CLI のインストールパスは、以下のいずれかにする必要があります。

`/sbin`、`/bin`、`/usr/sbin`、`/usr/bin`、`/usr/local/bin`

AWS CLI のセットアップ方法に関する詳細は下記を参照してください。

https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/cli-chap-install.html

（Python または AWS CLI のインストールを行った時点ですでに CLUSTERPRO がインストール済の場合は、OS を再起動してから CLUSTERPRO の操作を行ってください。）

5. **AWS アクセスキー ID の登録**

シェルから、以下のコマンドを実行します。

```
$ sudo aws configure
```

質問に対して、AWS アクセスキー ID などの情報を入力します。
インスタンスに IAM ロールを割り当てているか否かで 2 通りの設定に分かれます。

◇ IAM ロールを割り当てているインスタンスの場合

```
AWS Access Key ID [None]: （Enter のみ）
AWS Secret Access Key [None]: （Enter のみ）
Default region name [None]: <既定のリージョン名>
Default output format [None]: text
```

◇ IAM ロールを割り当てていないインスタンスの場合

```
AWS Access Key ID [None]: <AWS アクセスキー ID>
AWS Secret Access Key [None]: <AWS シークレットアクセスキー>
Default region name [None]: <既定のリージョン名>
Default output format [None]: text
```

"Default output format"は、"text"以外を指定することも可能です。

もし誤った内容を設定してしまった場合は、`/root/.aws` をディレクトリごと消去してから上記操作をやり直してください。

6. ミラーディスクの準備

ミラーディスク用に EBS を追加していた場合は、EBS をパーティション分割し、それぞれクラスタパーティション、データパーティションに使用します。

ミラーディスク用のパーティションについては、『インストール&設定ガイド』の「システム構成を決定する」-「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)」を参照してください。

7. **CLUSTERPRO** のインストール

インストール手順は『インストール&設定ガイド』を参照してください。

CLUSTERPRO のインストール媒体を導入環境に格納します。

（データの転送に関しては FTP、SCP、Amazon S3 経由など任意です。）

インストール完了後、OS の再起動を行ってください。

7.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および、接続方法は『インストール&設定ガイド』の「クラスタ構成情報を作成する」を参照してください。

ここでは以下の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
- AWS DNS リソース
- AWS AZ モニタリソース
- AWS DNS モニタリソース
- NP 解決 (HTTP 方式)

上記以外の設定は、『インストール&設定ガイド』を参照してください。

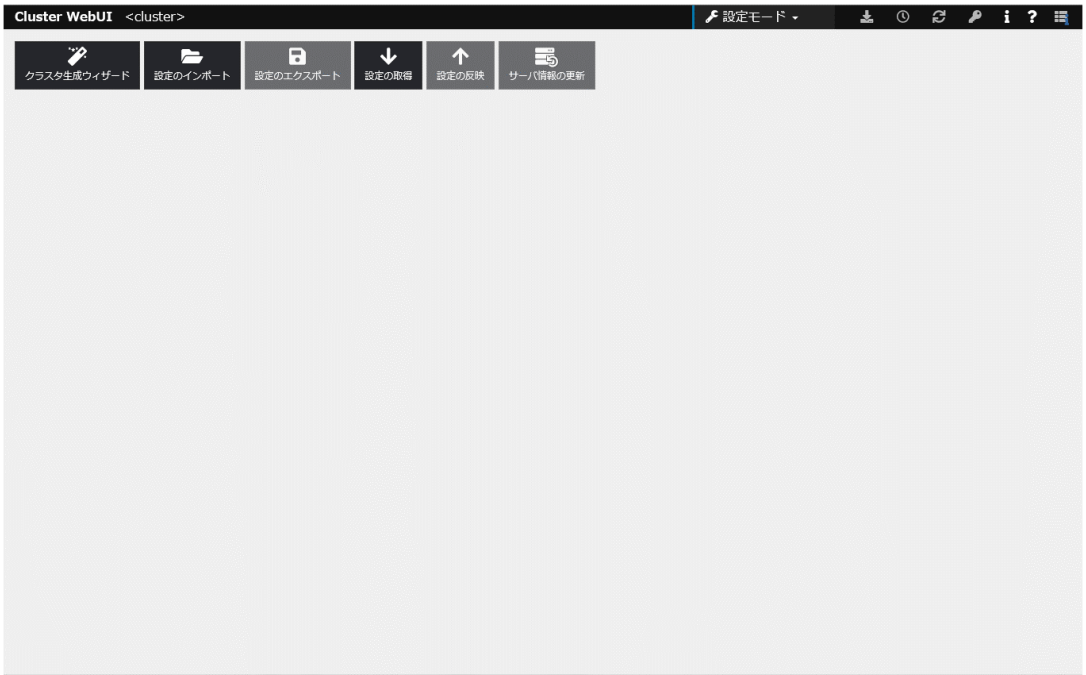
1. クラスタの構築

   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

     【手順】

     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] 画面の [クラスタ] 画面が表示されます。

   [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] 画面が表示されます。

   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 Private 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 Private 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。

   HTTP 方式の NP 解決を設定します。

   [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

  フェイルオーバグループを作成します。

  【手順】

  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

  必要に応じてミラーディスク（EBS） にあわせたミラーディスクリソース を作成します。
  詳細は『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」を参照してください。

【手順】

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] ボックスにグループリソース名 (md) 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。

   [マウントポイント] にミラーディスクのマウント先、[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「7.2. インスタンスの設定」-「6. ミラーディスクの準備」で作成したパーティションのデバイス名を入力します。 [完了] をクリックして設定を終了します。

- AWS DNS リソース

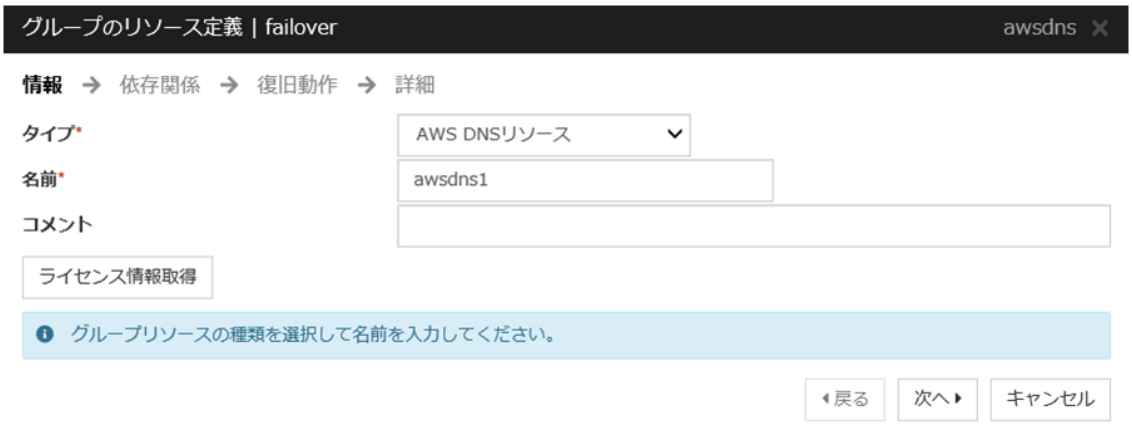
AWS CLI を利用して、DNS 名の制御を行う AWS DNS リソースを追加します。

詳細は『リファレンスガイド』-「AWS DNS リソースを理解する」を参照してください。

【手順】

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 (AWS DNS リソース) を選択して、 [名前] ボックスにグループリソース名 (awsdns1) 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。

   [共通] タブの [ホストゾーン ID] ボックスに、ホストゾーンの ID を設定します (図 7.1 システム構成 DNS 名制御による HA クラスタ の [7] が該当)。

   [リソースレコードセット名] ボックスに、付与したい DNS 名を設定します (図 7.1 システム構成 DNS 名制御による HA クラスタ の [5] が該当)。

   DNS 名は FQDN で、末尾にドット (.) を付けた形式で設定してください。

   [IP アドレス] ボックスに、DNS 名に対応する IP アドレスを設定します (図 7.1 システム構成 DNS 名制御による HA クラスタ の [4] が該当)。

   [共通] タブでは、任意のサーバの IP アドレスを記載し、他のサーバは個別設定を行うようにしてください。

   なお、本書では各サーバの IP アドレスをリソースレコードセットに含める構成を採用しているために上記の手順となっていますが、VIP や EIP をリソースレコードセットに含める場合は、[共通] タブでその IP アドレスを記載し、個別設定は不要です。

   [TTL] ボックスに、キャッシュの生存期間 (TTL = Time To Live の略) を設定します。

   TTL の秒数を設定してください。

   [非活性時にリソースレコードセットを削除する] チェックボックスを設定します。

   AWS DNS リソースの非活性時にホストゾーンからリソースレコードセットを削除しない場合、チェックを外してください。

   なお、削除しない場合、残存した DNS 名にクライアントからアクセスされる可能性があります。

6. 各ノードのタブをクリックし、ノード別設定を行います。

   [個別に設定する] をチェックします。

   [IP アドレス] ボックスに、そのノードに対応するインスタンスの IP アドレスを設定します (図 7.1 システム構成 DNS 名制御による HA クラスタ の [4][6] が該当)。

   なお、本書では各サーバの IP アドレスをリソースレコードセットに含める構成を採用しているために上記の手順となっていますが、VIP や EIP をリソースレコードセットに含める場合は、本手順は不要です。

7. [完了] をクリックして設定を終了します。

3. モニタリソースの追加

- AWS AZ モニタリソース

監視 コマンドを利用して、指定した AZ が利用可能かどうかを確認する AWS AZ モニタリソースを作成します。

詳細は『リファレンスガイド』-「AWS AZ モニタリソースを理解する」を参照してください。

【手順】

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (AWS AZ モニタ) を選択し、[名前] ボックスにモニタリソース名 (awsazw1) 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。

   何も指定せず [次へ] をクリックします。

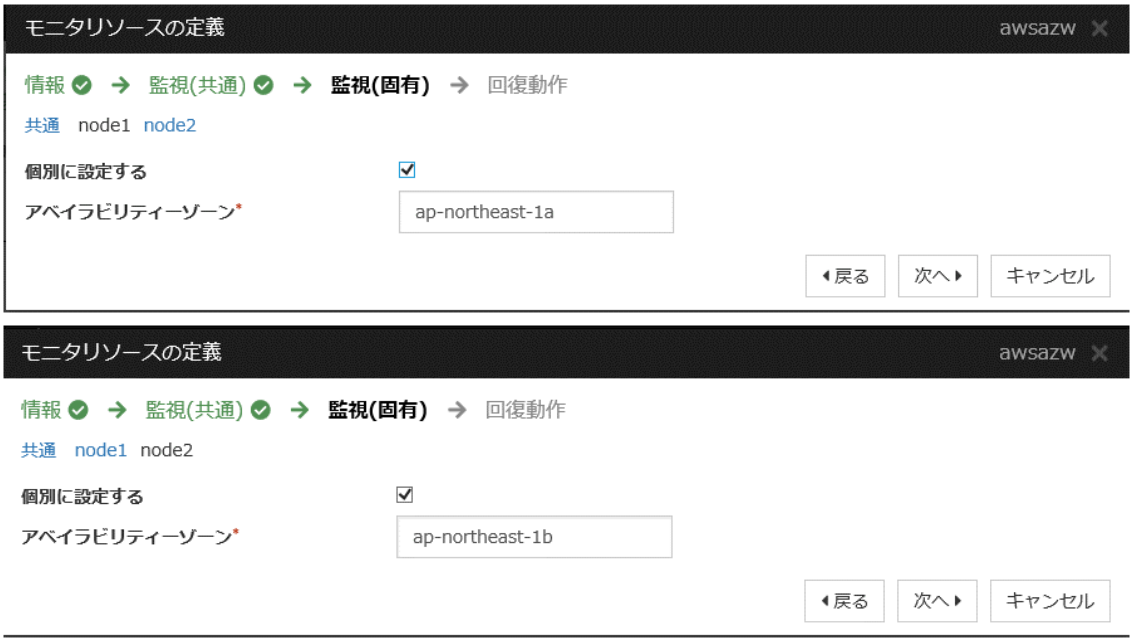
4. [監視 (固有)] 画面が表示されます。

   [共通] タブの [アベイラビリティーゾーン] ボックスに監視するアベイラビリティーゾーンを入力します（現用系側のインスタンスのアベイラビリティーゾーンを設定します）(図 7.1 システム構成 DNS 名制御による HA クラスタ の [2] が該当)。

5. 各ノードのタブをクリックし、ノード別設定を行います。

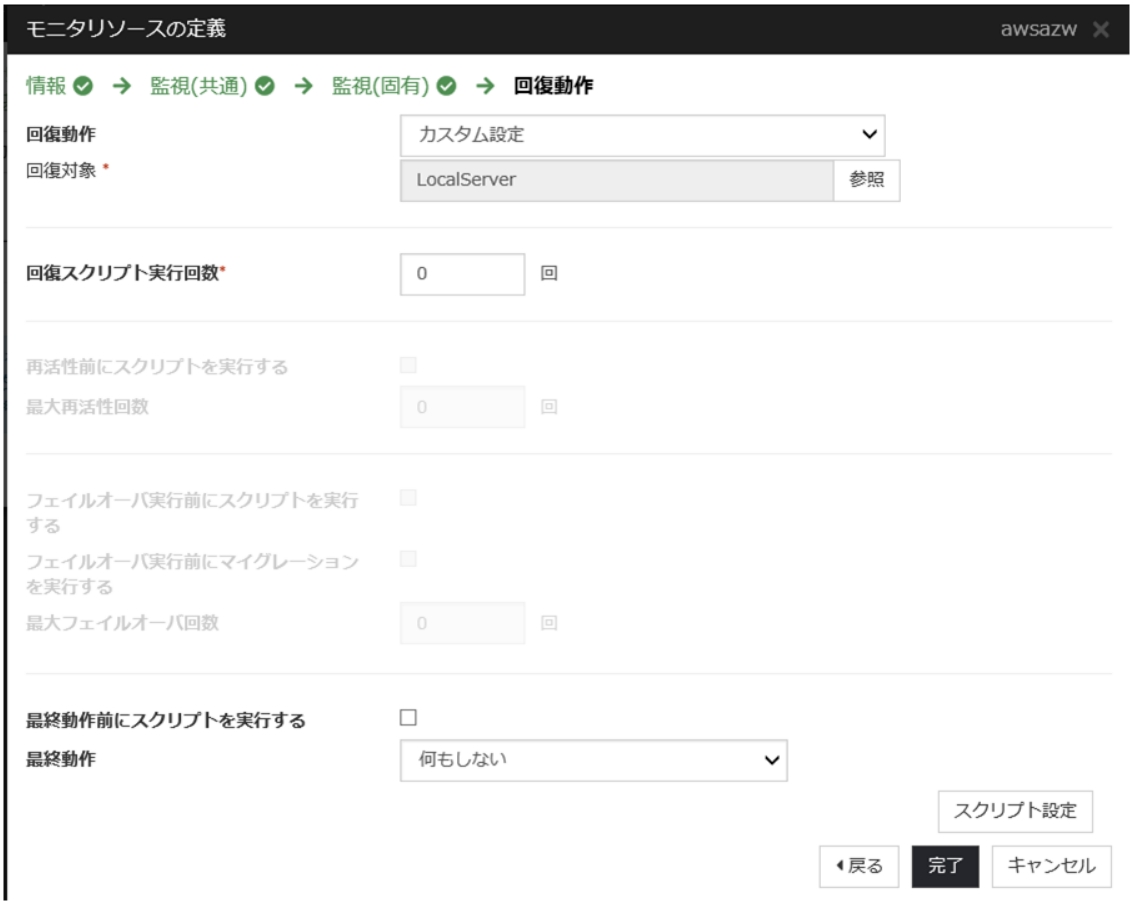
   [個別に設定する] をチェックします。

   [アベイラビリティーゾーン] ボックスに、そのノードに対応するインスタンスのアベイラビリティーゾーンを設定します (図 7.1 システム構成 DNS 名制御による HA クラスタ の [2][3] が該当)。[次へ] をクリックします。



6. [回復動作] 画面が表示されます。

   [回復対象] に [LocalServer] を設定します。



7. [完了] をクリックして設定を終了します。

- AWS DNS モニタリソース

AWS DNS リソース追加時に、自動的に追加されます。

OS API および AWS CLI コマンドを利用して、リソースレコードセットの存在と登録した IP アドレスが DNS 名の名前解決によって得られるかを確認します。

詳細は 『リファレンスガイド』 -「AWS DNS モニタリソースを理解する」を参照してください。

4. 設定の反映とクラスタの起動

1. Cluster WebUI の設定モードから、[設定の反映] をクリックします。

「設定を反映しますか。」 というポップアップメッセージが表示されるので、[OK] をクリックします。

アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[OK] をクリックします。

アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。

2. Cluster WebUI のツールバーのドロップダウンメニューで [操作モード] を選択して、操作モードに切り替えます。

3. 使用するリソースによって以降の手順が異なります。詳細は『インストール&設定ガイド』-「クラスタを生成するには」を参照してください。

第 8 章

トラブルシューティング

本章では、AWS 環境において CLUSTERPRO の設定が上手くいかない時の確認事項と対処方法について説明します。

◆ **AWS 関連リソースおよびモニタリソース起動に失敗する。**

まず OS が再起動済であること、Python および AWS CLI がインストールされていること、AWS CLI の設定が正しく完了していることを確認してください。

CLUSTERPRO のインストール時に再起動を行っていた場合でも、その後に Python、AWS CLI のインストールに伴い環境変数の設定変更が発生する場合は OS の再起動を行ってください。

◆ **AWS 仮想 IP リソースの起動に失敗する。**

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(51 : The AWS CLI command is␣
↪not found.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI が未インストール、またはパスが通っていない。

対処方法　以下を確認します。

- AWS CLI がインストールされていることを確認します。
- AWS CLI のインストールパスが以下のいずれかであることを確認します。

  /sbin、/bin、/usr/sbin、/usr/bin、/usr/local/bin

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(50 : Failed in the AWS CLI␣
↪command.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI 設定が未設定（aws configure 未実行）
- AWS CLI 設定が見つからない（aws configure を root 以外のユーザ、または、sudo なしで実行したなど）

  以下の順序で credentials（IAM ユーザを使用する方針の場合）、config ファイルを検索します。

  1. $HOME/.aws 配下
  2. /root/.aws 配下
- AWS CLI 設定の入力内容誤り（リージョン、アクセスキー ID、シークレットキー入力誤り）
- （IAM ロールを使用した運用の場合）インスタンスへの IAM ロール未設定。

  IAM ロールを使用する方針の場合、該当インスタンスから以下へアクセスし、設定している IAM ロール名が表示されるか確認してください。「404 Not Found」になった場合は IAM ロールが設定されていません。

  http://169.254.169.254/latest/meta-data/iam/security-credentials/
- 指定した VPC ID、または、ENI ID が不正
- リージョンのエンドポイントがメンテナンスや障害のため停止している。
- リージョンのエンドポイントまでの通信路の問題。
- ノードの高負荷による遅延。

対処方法　以下を確認します。

- AWS CLI の設定を正しい内容に修正し、AWS CLI が正常に動作することを確認します。
- ノードの高負荷の場合は、負荷要因を取り除いてください。
- （IAM ロールを使用した運用の場合）AWS 管理コンソールで設定を確認してください。

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(50 : The vpc ID␣
↪'vpc-xxxxxxxx' does not exist)
```

考えられる原因　指定した VPC ID が誤っているか、または存在しない可能性が考えられます。

対処方法　正しい VPC ID を指定します。

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(50 : The networkInterface ID␣
↪'eni-xxxxxxxx' does not exist)
```

考えられる原因　指定した ENI ID が誤っているか、または存在しない可能性が考えられます。

対処方法　正しい ENI ID を指定します。

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(50 : You are not authorized␣
↪to perform this operation.)
```

考えられる原因　IAM ロールの ReplaceRoute 権限について実行できるルートテーブルを制限している場合、IAM ポリシーの Resource に指定したルートテーブルに誤り、または不足がある可能性があります。

対処方法

AWS 仮想 IP リソースはルートテーブル更新時、指定された VPC 配下のすべてのルートテーブルのうち、指定された仮想 IP アドレスのエントリが存在するルートテーブルについて更新を行います。

そのため IAM ポリシーの Resource には、該当する (更新対象となる) ルートテーブルすべてについて許可を設定してください。

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(1 : Command was not completed␣
↪within %1 seconds.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI コマンドがルートテーブルや NAT の設定ミスやプロキシサーバーなどの理由でリージョンのエンドポイントと通信できない状態である可能性が考えられます。
- ノードの高負荷による遅延。

対処方法　以下を確認します。

- NAT ゲートウェイへのルーティングが設定済みであること。
- パケットがフィルタリングで落とされていないこと。
- ルートテーブル、NAT、プロキシサーバーの設定を確認してください。
- ノードの高負荷の場合は、負荷要因を取り除いてください。

Cluster WebUI のメッセージ

```
Activating awsvip1 resource has failed.(53 : The VIP address vvv.www.
↪xxx.yyy belongs to a VPC subnet.)
```

考えられる原因　指定した VIP アドレスが VPC CIDR 範囲内のため不適切です。

対処方法　VIP アドレスに VPC CIDR の範囲外となる IP アドレスを指定します。

◆ **AWS 仮想 IP リソースは正常に起動しているが、VIP アドレスに対する ping が通らない。**

Cluster WebUI のメッセージ

```
-
```

考えられる原因　AWS 仮想 IP リソースに設定した ENI の Source/Dest. Check が有効になっています。

対処方法　AWS 仮想 IP リソースに設定した ENI の Source/Dest. Check を無効に設定します。

◆ **AWS 仮想 IP モニタリソースが異常になる。**

Cluster WebUI のメッセージ

```
Detected an error in monitoring awsvipw1. (56 : The routing for VIP␣
↪vvv.www.xxx.yyy was changed.)
```

考えられる原因　ルートテーブルにおいて、AWS 仮想 IP リソースに対応する VIP アドレスのターゲットがなんらかの理由で別の ENI ID に変更されている。

対処方法

異常を検知した時点で AWS 仮想 IP リソースが自動的に再起動され、ターゲットが正しい ENI ID に更新されます。

別の ENI ID に変更された原因として、他の HA クラスタで同じ VIP アドレスを誤って使用していないかなどを確認します。

◆ **AWS Elastic IP リソースの起動に失敗する。**

Cluster WebUI のメッセージ

```
Activating awseip1 resource has failed.(99 : Internal error.␣
↪(status=*nn*))
```

考えられる原因　以下のいずれかが考えられます。

- Python が未インストール、またはパスが通っていない。
- AWS CLI が未インストール、またはパスが通っていない。

対処方法　以下を確認します。

- Python、または AWS CLI がインストールされていることを確認します。
- python コマンドのインストールパスが以下のいずれかであることを確認します。

/sbin、/bin、/usr/sbin、/usr/bin

- AWS CLI のインストールパスが以下のいずれかであることを確認します。

  /sbin、/bin、/usr/sbin、/usr/bin、/usr/local/bin

Cluster WebUI のメッセージ

```
Activating awseip1 resource has failed.(5 : Failed in the AWS CLI␣
↪command.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI 設定が未設定（aws configure 未実行）
- AWS CLI 設定が見つからない（aws configure を root 以外のユーザ、または、sudo なしで実行したなど）

  以下の順序で credentials（IAM ユーザを使用する方針の場合）、config ファイルを検索します。

  1. $HOME/.aws 配下
  2. /root/.aws 配下
- AWS CLI 設定の入力内容誤り（リージョン、アクセスキー ID、シークレットキー入力誤り）
- （IAM ロールを使用した運用の場合）インスタンスへの IAM ロール未設定。

  IAM ロールを使用する方針の場合、該当インスタンスから以下へアクセスし、設定している IAM ロール名が表示されるか確認してください。「404 Not Found」になった場合は IAM ロールが設定されていません。

  http://169.254.169.254/latest/meta-data/iam/security-credentials/
- 指定した EIP Allocation ID、または、ENI ID が不正
- リージョンのエンドポイントがメンテナンスや障害のため停止している。
- リージョンのエンドポイントまでの通信路の問題。
- ノードの高負荷による遅延。

対処方法　以下を確認します。

- AWS CLI の設定を正しい内容に修正し、AWS CLI が正常に動作することを確認します。
- ノードの高負荷の場合は、負荷要因を取り除いてください。
- （IAM ロールを使用した運用の場合）AWS 管理コンソールで設定を確認してください。

Cluster WebUI のメッセージ

```
Activating awseip1 resource has failed.(5 : The allocation ID␣
↪'eipalloc-xxxxxxxx' does not exist)
```

考えられる原因　指定した EIP Allocation ID が誤っているか、または存在しない可能性が考えられます。

対処方法　正しい EIP Allocation ID を指定します。

Cluster WebUI のメッセージ

```
Activating awseip1 resource has failed.(5 : The networkInterface ID␣
↪'eni-xxxxxxxx' does not exist)
```

考えられる原因　指定した ENI ID が誤っているか、または存在しない可能性が考えられます。

対処方法　正しい ENI ID を指定します。

Cluster WebUI のメッセージ

```
Activating awseip1 resource has failed.(6 : Timeout occurred.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI コマンドがルートテーブルや NAT の設定ミスやプロキシサーバーなどの理由でリージョンのエンドポイントと通信できない状態である可能性が考えられます。
- ノードの高負荷による遅延。

対処方法　以下を確認します。

- 各インスタンスに Public IP が割り当てられていることを確認します。
- 各インスタンスで AWS CLI が正常に動作することを確認します。
- ルートテーブル、NAT、プロキシサーバーの設定を確認してください。
- ノードの高負荷の場合は、負荷要因を取り除いてください。

◆ **AWS Elastic IP モニタリソースが異常になる。**

Cluster WebUI のメッセージ

```
Detected an error in monitoring awseipw1. (7 : The EIP address does␣
↪not exist. (EIP ALLOCATION ID=eipalloc-xxxxxxxx))
```

考えられる原因　指定した ENI ID と Elastic IP の関連付けが何らかの理由で解除されている。

対処方法

異常を検知した時点で AWS Elastic IP リソースが自動的に再起動され、指定した ENI ID と Elastic IP の関連付けが行われます。

Elastic IP との関連付けが変更された原因として、他の HA クラスタで同じ EIP Allocation ID を誤って使用していないかなどを確認します。

◆ **AWS DNS リソースの起動に失敗する。**

Cluster WebUI のメッセージ

```
Activating awsdns1 resource has failed.(99 : Internal error.
↪(status=*nn*))
```

考えられる原因　以下のいずれかが考えられます。

- Python が未インストール、またはパスが通っていない。
- AWS CLI が未インストール、またはパスが通っていない。

対処方法　以下を確認します。

- Python、または AWS CLI がインストールされていることを確認します。
- python コマンドのインストールパスが以下のいずれかであることを確認します。

  `/sbin`、`/bin`、`/usr/sbin`、`/usr/bin`

- AWS CLI のインストールパスが以下のいずれかであることを確認します。

  `/sbin`、`/bin`、`/usr/sbin`、`/usr/bin`、`/usr/local/bin`

Cluster WebUI のメッセージ

```
Activating awsdns1 resource has failed. (5 : Failed in the AWS CLI
↪command.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI 設定が未（aws configure 未実行）
- AWS CLI 設定が見つからない（aws configure を root 以外のユーザ、または、sudo なしで実行したなど）

  以下の順序で credentials（IAM ユーザを使用する方針の場合）、config ファイルを検索します。

  1. $HOME/.aws 配下
  2. /root/.aws 配下

- AWS CLI 設定の入力内容誤り（リージョン、アクセスキー ID、 シークレットキー入力誤り）
- （IAM ロールを使用した運用の場合）インスタンスへの IAM ロール未設定。

IAM ロールを使用する方針の場合、該当インスタンスから以下へアクセスし、設定している IAM ロール名が表示されるか確認してください。「404 Not Found」になった場合は IAM ロールが設定されていません。

http://169.254.169.254/latest/meta-data/iam/security-credentials/

- 指定したリソースレコードセットが不正
- リージョンのエンドポイントがメンテナンスや障害のため停止している。
- リージョンのエンドポイントまでの通信路の問題。
- ノードの高負荷による遅延。
- Route 53 にアクセスできない状態もしくは Route 53 が応答しない状態。
- Route 53 の当該ホストゾーンが対象とする VPC に、HA インスタンスが所属する VPC を追加していない。
- HA インスタンスが所属する VPC で DNS 名前解決を有効にしていない。
- [リソースレコードセット名] が大文字で指定されている。
- 以下のコマンドをノード (インスタンス) 上の端末から手動で実行してください。

  ```
  # aws route53 list-resource-record-sets --hostted-zone-id <ホストゾーン ID>
  ```

「Could not connect to the endpoint URL」エラーが表示される場合、以下のいずれかが考えられます。

- VPC エンドポイントを使用している場合、VPC エンドポイントは Route 53 のサービスには未対応のため、VPC エンドポイントを使用している場合は AWS DNS リソース/モニタリソースは利用できません。

- VPC エンドポイントを使用していない場合、AWS 上の設定の問題が考えられます。

対処方法　以下を確認します。

- AWS CLI の設定を正しい内容に修正し、AWS CLI が正常に動作することを確認します。
- ノードの高負荷の場合は、負荷要因を取り除いてください。
- Route 53 マネジメントコンソールの「当該ホストゾーン」について、「関連付けられた VPC」に必要な VPC が追加されていることを確認してください。
- VPC マネジメントコンソールにおいて、使用している VPC のプロパティで「DNS 解決」が有効になっていることを確認してください。意図的に「DNS 解決」を無効にしている場合は、

インスタンスが AWS DNS リソースで追加したレコードセットを名前解決できるように適切なリゾルバを設定してください。

- [リソースレコードセット名] は小文字で指定してください。
- VPC エンドポイントを使用している場合、NAT ゲートウェイ、Proxy サーバのいずれかの方法に変更することを検討してください。VPC エンドポイントを使用していない場合、AWS へ確認してください。
- （IAM ロールを使用した運用の場合）AWS 管理コンソールで設定を確認してください。

Cluster WebUI のメッセージ

```
Activating awsdns1 resource has failed. (5 : No hosted zone found␣
↪with ID: %1)
```

考えられる原因　指定したホストゾーン ID が誤っているか、または存在しない可能性が考えられます。

対処方法　正しいホストゾーン ID を指定します。

Cluster WebUI のメッセージ

```
Activating awsdns1 resource has failed. (6 : Timeout occurred.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI コマンドがルートテーブルや NAT の設定ミスやプロキシサーバーなどの理由でリージョンのエンドポイントと通信できない状態である可能性が考えられます。
- ノードの高負荷による遅延。
- Route 53 エンドポイント側の処理遅延。
- AWS CLI 内部で実行されるインスタンスメタデータに対するアクセスが遅延。

対処方法　以下を確認します。

- NAT ゲートウェイへのルーティングが設定済みであること。
- パケットがフィルタリングで落とされていないこと。
- ルートテーブル、NAT、プロキシサーバーの設定を確認してください。
- ノードの高負荷の場合は、負荷要因を取り除いてください。
- AWS 環境において監視 (共通) の [タイムアウト] が AWS CLI 実行に必要な時間以上の値を設定していること。AWS DNS モニタリソースは以下の AWS CLI を実行しています。手動にて AWS CLI を実行し、必要な時間を計測してください。

```
# aws route53 list-resource-record-sets
```

- （IAM ロールを使用した運用の場合）CLUSTERPRO の AWS DNS リソースおよびモニタリソースが AWS CLI を実行する際に、インスタンスメタデータからアクセスキー ID などの認証情報を取得します。

  インスタンスメタデータに対するアクセスに遅延がないか、手動で以下のコマンドを実行に必要な時間を確認してください。

  どちらかひとつでも遅延がある場合はアクセスの遅延が発生しています。

  遅延がある場合は、aws configure コマンドにより、各クラスタノードにアクセスキー ID およびシークレットアクセスキーの設定を追加し、IAM ユーザで実行されるようにすることで、タイムアウトの発生確率が減少する可能性があります。

  - 各クラスタノードから http://169.254.169.254/latest/meta-data/ にブラウザまたは curl コマンドなどでアクセス。

  - クラスタノードのいずれかにおいて aws configure list を実行。

◆ **AWS DNS リソースは正常に起動しているが、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。**

Cluster WebUI のメッセージ

–

考えられる原因　以下のいずれかが考えられます。

- Route53 の仕様により、Route53 の設定が権威サーバすべてに反映されるまでに最大 60 秒掛かります。以下を参照してください。

  https://aws.amazon.com/jp/route53/faqs/

  Amazon Route 53 のよくある質問

  Q:Amazon Route 53 での DNS 設定の変更が全体に適用されるには、どのくらいの時間がかかりますか。

- OS 側のリゾルバにより時間が掛かっている。

- フェイルオーバー時に AWS DNS リソースによるリソースレコードセットの削除と作成に時間が掛かっている。

  [非活性時にリソースレコードセットを削除する] がチェックが ON の場合、フェイルオーバー元で AWS DNS リソース非活性時にリソースレコードセットを削除後、フェイルオーバー先で AWS DNS リソース活性時にリソースレコードセットを作成となるため、名前解決可能になるまでの時間が遅くなる可能性があります。

  チェックが OFF の場合、非活性時にもリソースレコードセットが削除されなくなり、該当リソースレコードセットの IP アドレス更新のみとなるため、名前解決可能になるまでの時間が短縮される可能性があります。

チェックを OFF にした場合は、通常の AWS DNS リソース非活性時やクラスタ停止後にもリソースレコードセットは削除されずに残りますので、ご留意ください。AWS DNS リソース非活性後やクラスタ停止後でも名前解決されます。

- AWS DNS リソースの [TTL] の値が大きい。
- AWS DNS モニタリソースの [監視開始待ち時間] の値が小さい。

  もし Route 53 の変更が反映完了する前に名前解決を試みてしまうと 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。

  そのため、[監視開始待ち時間] を小さい値に設定していると、名前解決可能になるまでに長時間を要する結果となる可能性があります。

対処方法　以下を確認します。

- OS 側のリゾルバの設定を見直してください。
- AWS DNS リソースの [非活性時にリソースレコードセットを削除する] を OFF にします。
- AWS DNS リソースの [TTL] の値を小さい値に設定します。
- AWS DNS モニタリソースの [監視開始待ち時間] の値を許容できる大きな値に設定します。

◆ **AWS DNS モニタリソースが異常になる。**

Cluster WebUI のメッセージ

```
Detected an error in monitoring awsdnsw1. (7 : The resource record␣
↪set in Amazon Route 53 does not exist.)
```

考えられる原因　以下のいずれかが考えられます。

- ホストゾーンにおいて、 AWS DNS リソースに対応するリソース レコードセットがなんらかの理由で削除されている。
- AWS DNS リソースの活性直後、Route 53 における DNS 設定の変更が反映される前に、AWS DNS モニタリソースが監視を実行すると名前解決ができないため監視に失敗します。『スタートアップガイド』-「注意制限事項」-「AWS DNS モニタリソースの設定について」を参照してください。
- IAM ポリシーの route53:ChangeResourceRecordSets、route53:ListResourceRecordSets が未設定。
- Route 53 の当該ホストゾーンが対象とする VPC に、HA インスタンスが所属する VPC を追加していない。
- [リソースレコードセット名] に設定した DNS 名の末尾にドット (.) が付与されていない。

対処方法　以下を確認します。

- リソースレコードセットが削除された原因として、他の HA クラスタで同じリソースレコードセットを誤って使用していないこと。
- AWS DNS モニタリソースの [監視開始待ち時間] が Route 53 における DNS 設定の変更が反映される時間より長く設定されていること。
- IAM ポリシーに route53:ChangeResourceRecordSets、route53:ListResourceRecordSets が設定されていること。
- Route 53 マネジメントコンソールの「当該ホストゾーン」について、「関連付けられた VPC」に必要な VPC が追加されていること。
- [リソースレコードセット名] に設定した DNS 名が FQDN で、末尾にドット (.) を付けた形式で設定されていること。

Cluster WebUI のメッセージ

```
Detected an error in monitoring awsdnsw1. (8 : IP address different␣
↪from the setting is registered in the resource record set of Amazon␣
↪Route 53.)
```

考えられる原因　ホストゾーンにおいて、 AWS DNS リソースに対応するリソース レコードセットの IP アドレスがなんらかの理由で変更されている。

対処方法　リソースレコードセットが変更された原因として、他の HA クラスタで同じリソースレコードセットを誤って使用していないかなどを確認します。

Cluster WebUI のメッセージ

```
Detected an error in monitoring awsdnsw1. (9 : Failed to resolve␣
↪domain name.)
```

考えられる原因　リソースレコードセットとしてホストゾーンに登録した DNS 名での名前解決確認がなんらかの理由で失敗した。

対処方法　以下を確認します。

- リゾルバの設定に誤りがないこと
- ネットワークの設定に誤りがないこと
- Public ホストゾーンを使用している場合は、レジストラのネームサーバ (NS) レコードの設定で、ドメインへのクエリが Amazon Route 53 ネームサーバを参照するようになっていること

Cluster WebUI のメッセージ

```
Detected an error in monitoring awsdnsw1. (10 : IP address which is␣
↪resolved domain name from the DNS resolver does not match setting.)
```

考えられる原因　リソースレコードセットとしてホストゾーンに登録した DNS 名での名前解決確認で得られた IP アドレスが正しくない。

対処方法　以下を確認します。

- リゾルバの設定に誤りがないこと
- hosts ファイル中に DNS 名に関するエントリが存在しないこと

◆ **AWS DNS モニタリソースが警告または異常になる。**

Cluster WebUI のメッセージ

[警告時]

```
Warn monitoring awsdnsw1. (106 : Timeout occurred.)
```

[異常時]

```
Detected an error in monitoring awsdnsw1. (6 : Timeout occurred.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI コマンドがルートテーブルや NAT の設定ミスやプロキシサーバーなどの理由でリージョンのエンドポイントと通信できない状態である可能性が考えられます。
- ノードの高負荷による遅延。
- Route 53 エンドポイント側の処理遅延。
- AWS CLI 内部で実行されるインスタンスメタデータに対するアクセスが遅延。

対処方法　以下を確認します。

- NAT ゲートウェイへのルーティングが設定済みであること。
- パケットがフィルタリングで落とされていないこと。
- ルートテーブル、NAT、プロキシサーバーの設定を確認してください。
- AWS 環境において監視 (共通) の [タイムアウト] が AWS CLI 実行に必要な時間以上の値を設定していること。AWS DNS モニタリソースは以下の AWS CLI を実行しています。手動にて AWS CLI を実行し、必要な時間を計測してください。

```
# aws route53 list-resource-record-sets
```

- （IAM ロールを使用した運用の場合）CLUSTERPRO の AWS DNS リソースおよびモニタリソースが AWS CLI を実行する際に、インスタンスメタデータからアクセスキー ID などの認証情報を取得します。

  インスタンスメタデータに対するアクセスに遅延がないか、手動で以下のコマンドを実行に必要な時間を確認してください。

  どちらかひとつでも遅延がある場合はアクセスの遅延が発生しています。

  遅延がある場合は、aws configure コマンドにより、各クラスタノードにアクセスキー ID およびシークレットアクセスキーの設定を追加し、IAM ユーザで実行されるようにすることで、タイムアウトの発生確率が減少する可能性があります。

  - 各クラスタノードから http://169.254.169.254/latest/meta-data/ にブラウザまたは curl コマンドなどでアクセス。

  - クラスタノードのいずれかにおいて aws configure list を実行。

◆ **AWS AZ モニタリソースが警告または異常になる。**

Cluster WebUI のメッセージ

[警告時]

```
Warn monitoring awsazw1. (105 : Failed in the AWS CLI command.)
```

[異常時]

```
Detected an error in monitoring awsazw1. (5 : Failed in the AWS␣
↪CLI command.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI 設定が未設定（aws configure 未実行）
- AWS CLI 設定が見つからない（aws configure を root 以外のユーザ、または、sudo なしで実行したなど）

  以下の順序で credentials（IAM ユーザを使用する方針の場合）、config ファイルを検索します。

  1. $HOME/.aws 配下
  2. /root/.aws 配下
- AWS CLI 設定の入力内容誤り（リージョン、アクセスキー ID、シークレットキー入力誤り）
- （IAM ロールを使用した運用の場合）インスタンスへの IAM ロール未設定。

  IAM ロールを使用する方針の場合、該当インスタンスから以下へアクセスし、設定している IAM ロール名が表示されるか確認してください。「404 Not Found」になった場合は IAM ロールが設定されていません。

  http://169.254.169.254/latest/meta-data/iam/security-credentials/

- 指定した アベイラビリティーゾーンが不正
- リージョンのエンドポイントがメンテナンスや障害のため停止している。
- リージョンのエンドポイントまでの通信路の問題。
- ノードの高負荷による遅延。

対処方法　以下を確認します。

- AWS CLI の設定を正しい内容に修正し、AWS CLI が正常に動作することを確認します。
- ノードの高負荷の場合は、負荷要因を取り除いてください。
- 頻繁に警告が表示される場合は、「回復動作を実行しない (警告を表示しない)」へ変更することを推奨します。この場合でも、モニタリソースから実行する AWS CLI の実行失敗や応答遅延以外のエラーは検知可能です。
- （IAM ロールを使用した運用の場合）AWS 管理コンソールで設定を確認してください。

Cluster WebUI のメッセージ

[警告時]

```
Warn monitoring awsazw1. (105 : Invalid availability zone:␣
↪[ap-northeast-1x])
```

[異常時]

```
Detected an error in monitoring awsazw1. (5 : Invalid availability␣
↪zone: [ap-northeast-1x])
```

考えられる原因　指定したアベイラビリティーゾーンが誤っているか、または存在しない可能性が考えられます。

対処方法　正しいアベイラビリティーゾーンを指定します。

Cluster WebUI のメッセージ

[警告時]

```
Warn monitoring awsazw1. (106 : Timeout occurred.)
```

[異常時]

```
Detected an error in monitoring awsazw1. (6 : Timeout occurred.)
```

考えられる原因　以下のいずれかが考えられます。

- AWS CLI コマンドがルートテーブルや NAT の設定ミスやプロキシサーバーなどの理由でリージョンのエンドポイントと通信できない状態である可能性が考えられます。
- ノードの高負荷による遅延。

対処方法　以下を確認します。

- NAT ゲートウェイへのルーティングが設定済みであること。
- パケットがフィルタリングで落とされていないこと。
- ルートテーブル、NAT、プロキシサーバーの設定を確認してください。
- AWS 環境において監視 (共通) の [タイムアウト] が AWS CLI 実行に必要な時間以上の値を設定していること。AWS AZ モニタリソースは以下の AWS CLI を実行しています。手動にて AWS CLI を実行し、必要な時間を計測してください。

```
# aws ec2 describe-availability-zones
```

- ノードの高負荷の場合は、負荷要因を取り除いてください。

第 9 章

免責・法的通知

9.1 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、一切責任をおいません。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。

9.2 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。
- Python は、Python Software Foundation の登録商標です。
- Amazon Web Services およびすべての AWS 関連の商標、ならびにその他の AWS のグラフィック、ロゴ、ページヘッダー、ボタンアイコン、スクリプト、サービス名は、米国および／またはその他の国における、AWS の商標、登録商標またはトレードドレスです。
- 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 10 章

改版履歴

版数	改版日付	内容
1	2023/04/10	新規作成
2	2023/05/26	AWS 環境の構成に関する図と文章を更新
3	2023/11/17	内部バージョン 5.1.2-1 に対応

© Copyright NEC Corporation 2023. All rights reserved.