

CLUSTERPRO® X 4.0

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

2018.04.17
第1版

CLUSTERPRO

改版履歴

版数	改版日付	内 容
1	2018/04/17	新規作成

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。

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。

目次

はじめに	V
対象読者と目的	V
適用範囲	V
本書の表記規則	vii
最新情報の入手先	viii
第 1 章 機能概要	9
1-1. 機能概要	9
1-2. HAクラスタ構成	10
1-3. Multi-AZ	17
1-4. ネットワークパーティション解決	18
1-5. オンプレミスとAWS	19
第 2 章 動作環境	22
第 3 章 注意事項	23
第 4 章 VIP制御によるHAクラスタの設定	25
4-1. VPC 環境の設定	26
4-2. インスタンスの設定	29
4-3. CLUSTERPRO の設定	31
第 5 章 EIP制御によるHAクラスタの設定	41
5-1. VPC 環境の設定	42
5-2. インスタンスの設定	45
5-3. CLUSTERPRO の設定	47
第 6 章 DNS名制御によるHAクラスタの設定	56
6-1. VPC 環境の設定	57
6-2. インスタンスの設定	60
6-3. CLUSTERPROの設定	62
第 7 章 IAMの設定	73
7-1. IAMポリシーの作成	73
7-2. インスタンスの設定	75
第 8 章 トラブルシューティング	78

はじめに

対象読者と目的

『CLUSTERPRO® X Amazon Web Services 向け HA クラスタ 構築ガイド (Linux 版)』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。

適用範囲

本書では、以下の製品を対象としています。

- CLUSTERPRO X 4.0 for Linux (内部バージョン: 4.0.0-1)
- VPC Management Console、EC2 Management Console: 2018/02/23 時点の環境

本書の構成

第 1 章	「機能概要」: 機能の概要について説明します。
第 2 章	「動作環境」: 本機能の動作確認済み環境を説明します。
第 3 章	「注意事項」: 構築時の注意事項について説明します。
第 4 章	「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。
第 5 章	「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。
第 6 章	「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。
第 7 章	「IAM の設定」: IAM の設定について説明します。
第 8 章	「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。

CLUSTERPRO マニュアル体系

CLUSTERPRO のマニュアルは、以下の 4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』(Installation 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)

管理者を対象とし、CLUSTERPRO の運用手順、各モジュールの機能説明、メンテナンス関連情報およびトラブルシューティング情報等を記載します。『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 統合 WebManager 管理者ガイド』(Integrated WebManager Administrator's Guide)

CLUSTERPRO を使用したクラスタシステムを CLUSTERPRO 統合 WebManager で管理するシステム管理者、および 統合 WebManager の導入を行うシステムエンジニアを対象読者とし、統合 WebManager を使用したクラスタシステム導入時に必須の事項について、実際の手順に則して詳細を説明します。

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： 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： 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。

関連情報： 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。	<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 (courier)	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
モノスペースフォント太字 (courier)	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。 # <code>clpcl -s -a</code>
モノスペースフォント斜体 (courier)	ユーザが有効な値に置き換えて入力する項目	# <code>ping <IPアドレス></code>

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。

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

第 1 章 機能概要

1-1. 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。

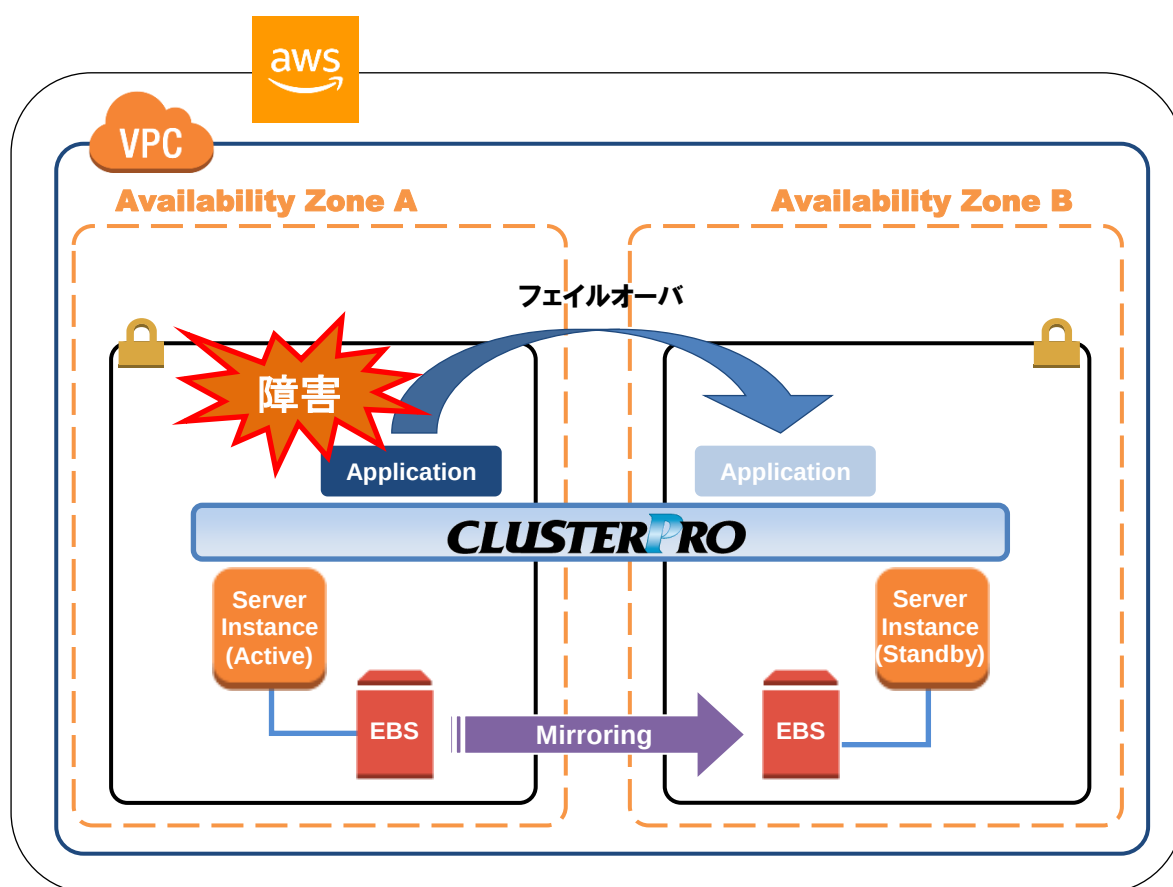


図 1-1 Multi-AZ構成のミラー型HAクラスタ

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、“フェイルオーバー”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。

1-2. 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「1-3 Multi-AZ」を参照してください。

※以下の構成以外の使用方法をご検討の場合は、下記の窓口にご相談ください。

(インターネットから VPN 等を用いて HA クラスタに直接アクセスしたい等)

CLUSTERPRO プリセールス窓口 info@clusterpro.jp clusterpro.jp

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

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。

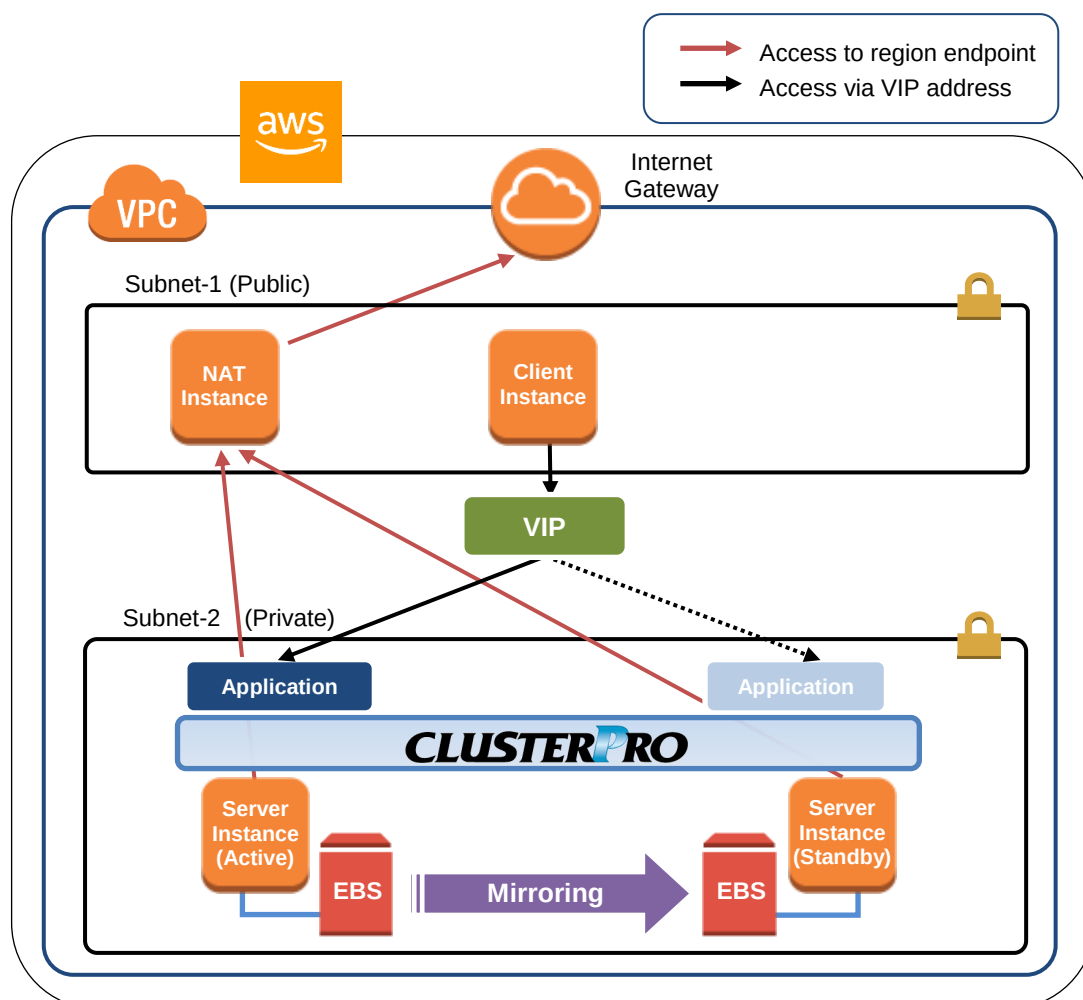


図 1-2 VIP 制御による HA クラスタ

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。

AWS 側の仕様により VPC 外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。VPC 外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。

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 用のインスタンス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と通信できる必要があります、そのた

めの方法として Proxy サーバ / NAT / Public IP / EIP などの方法がありますが、本書では VIP 制御による HA クラスタ構成の場合、NAT 用のインスタンス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。 Multi-AZ を利用しない場合でも、AWS CLI の利用可否を監視する目的で使用することが可能です。	推奨
IP モニタリソース	NAT への通信可否を確認することで、サブネット間通信の健全性を監視します。 本書では NAT 用インスタンスへの通信可否を確認します。	サブネット間通信の健全性監視が必要な場合に必須
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

各リソース、モニタリソースの詳細は以下のマニュアルを参照してください。

- 『リファレンスガイド』-「第 4 章 グループリソースの詳細」
- 『リファレンスガイド』-「第 5 章 モニタリソースの詳細」

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。

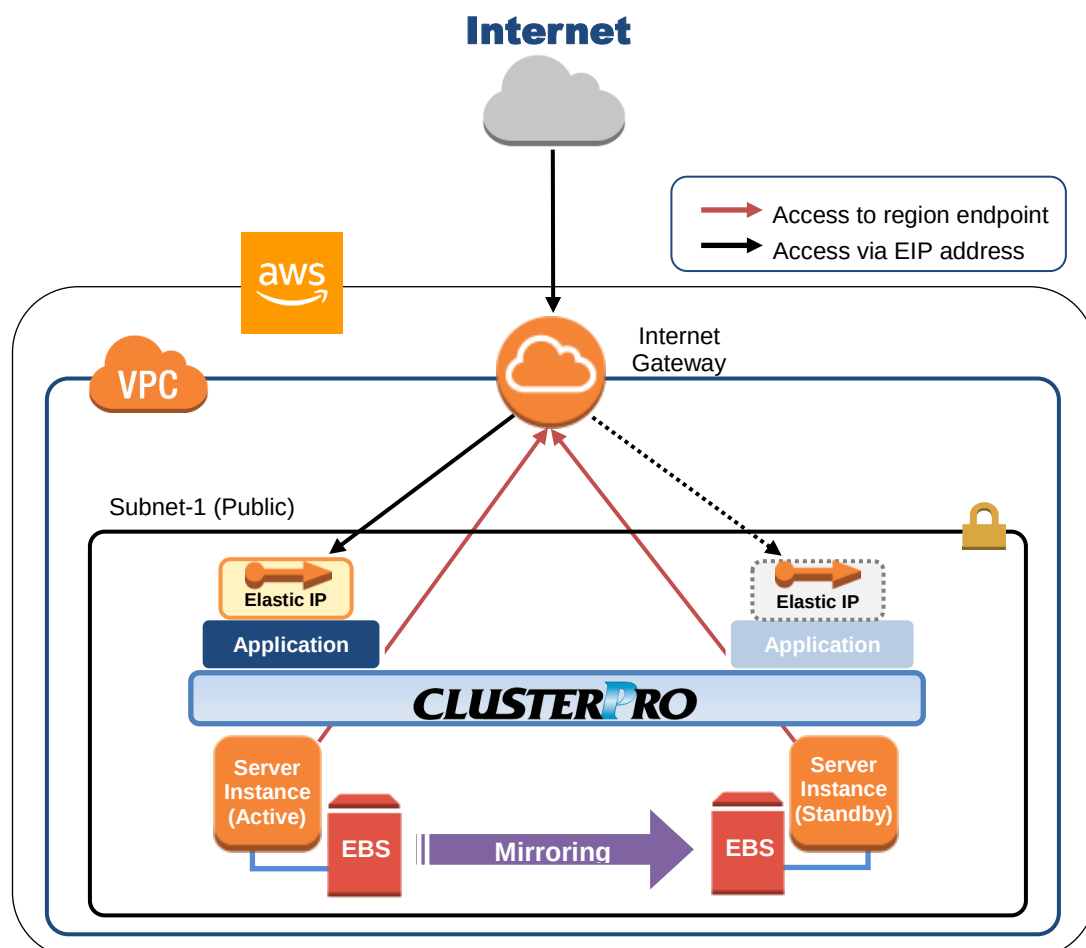


図 1-3 EIP 制御による HA クラスタ

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できる必要があります、そのための方法として Proxy サーバ / NAT / Public IP / EIP などの方法がありますが、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。 Multi-AZ を利用しない場合でも、AWS CLI の利用可否を監視する目的で 사용할 수 있습니다.	推奨
カスタムモニタリソース	ネットワークパーティション (NP) を監視し、複数のインスタンスでリソースが同時に起動しないように監視します。	NP 解決が必要な場合に必須
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 クラスターで運用するアプリケーションの構成に従います。	任意

各リソース、モニタリソースの詳細は以下のマニュアルを参照してください。

- 『リファレンスガイド』-「第 4 章 グループリソースの詳細」
- 『リファレンスガイド』-「第 5 章 モニタリソースの詳細」

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。

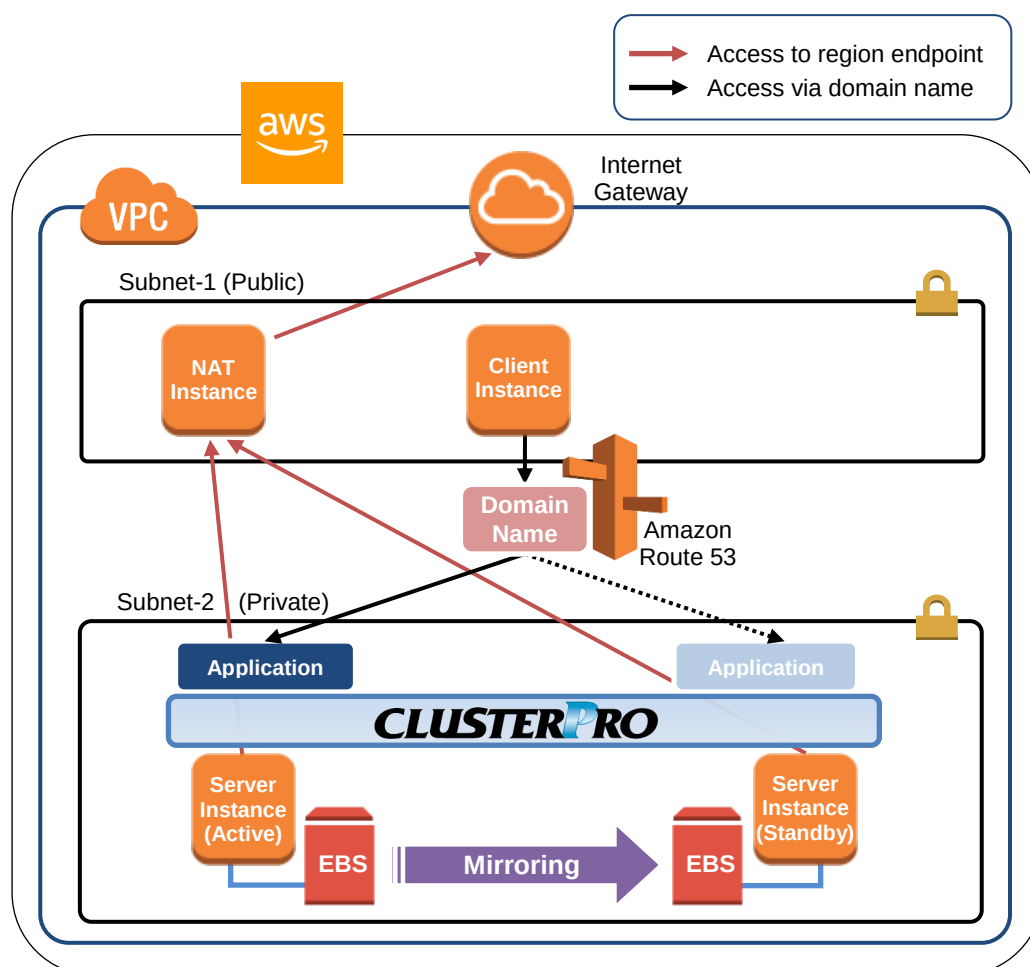


図 1-4 DNS 名制御による HA クラスタ

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できる必要があり、そのための方法として Proxy サーバ / NAT / Public IP / EIP などの方法がありますが、本書では DNS 名制御による HA クラスタ構成の場合、NAT 用のインスタンス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。 Multi-AZ を利用しない場合でも、AWS CLI の利用可否を監視する目的で使用することが可能です。	推奨
IP モニタリソース	NAT への通信可否を確認することで、サブネット間通信の健全性を監視します。 本書では NAT 用インスタンスへの通信可否を確認します。	サブネット間通信の健全性監視が必要な場合に必須
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

各リソース、モニタリソースの詳細は以下のマニュアルを参照してください。

- ・『リファレンスガイド』-「第 4 章 グループリソースの詳細」
- ・『リファレンスガイド』-「第 5 章 モニタリソースの詳細」

1-3. 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ゾーン単位で分散させることで、アベイラビリティ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』-「第 5 章 モニタリソースの詳細」-「AWS AZ モニタリソースを理解する」を参照してください。

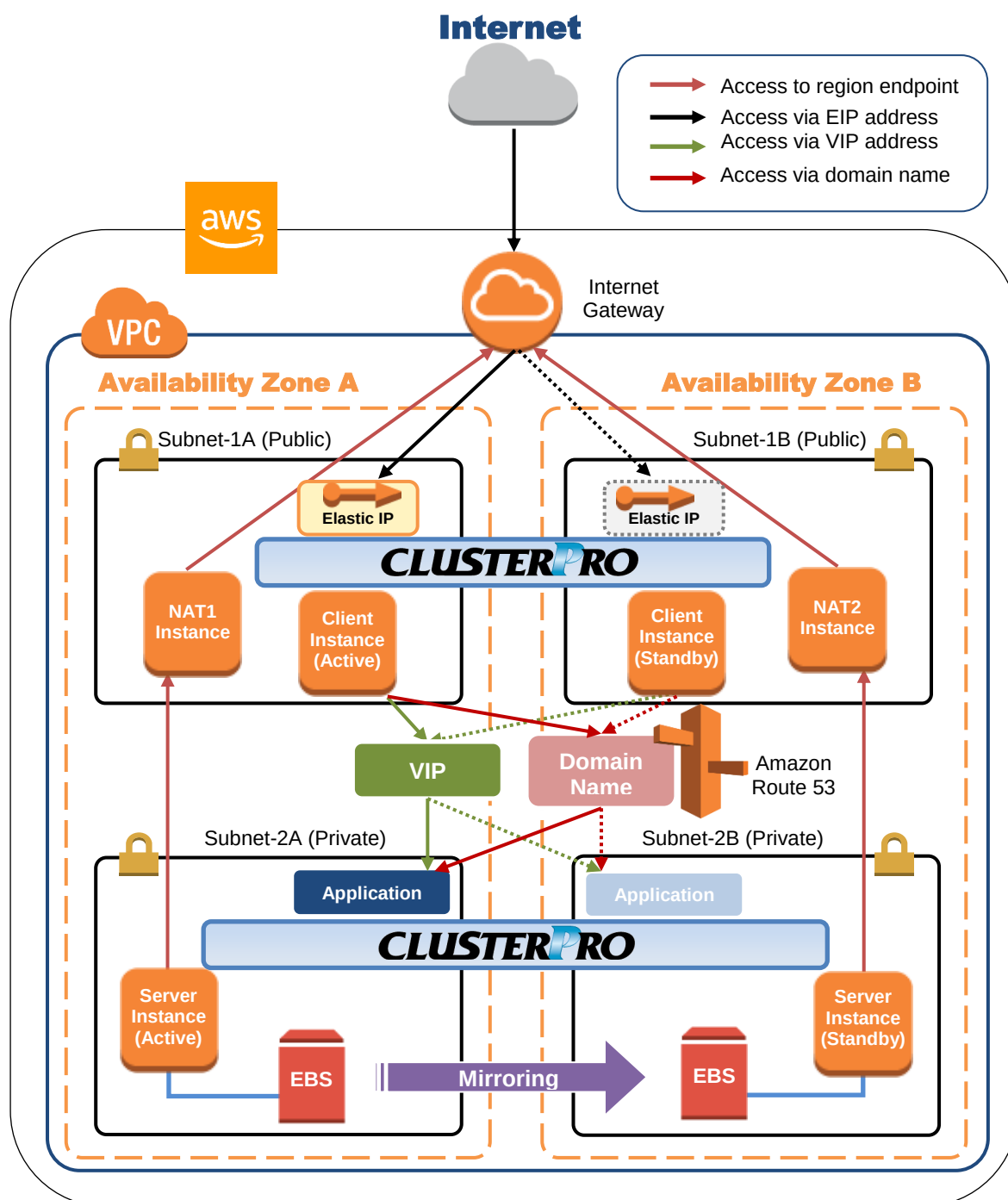


図 1-5 Multi-AZを使用した HA クラスタの例

1-4. 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インスタンスは、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。各インスタンス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、他のインスタンスがダウンしたか、自身がネットワークから孤立した (NP) 状態かのどちらであるかを区別する必要があります。

NP 解決は、Ping などの応答を返却可能な常時稼働している装置 (以下、応答確認用装置) に対して Ping や LISTEN ポート確認を行い、応答がない場合は NP 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。

応答確認用装置は、Amazon VPC においては通常以下を使用します。

HA クラスタ種別	応答確認用装置	手段	備考
VIP 制御による HA クラスタ	他サブネット上の常時稼働しているインスタンス	Ping	本書では例として NAT 用インスタンスを指定します。
EIP 制御による HA クラスタ	リージョンのエンドポイント	LISTEN ポート確認	リージョンのエンドポイントは、以下から確認できます。 http://docs.aws.amazon.com/general/latest/gr/rande.html 例) リージョンがアジアパシフィック (東京) の場合は <code>ec2.ap-northeast-1.amazonaws.com</code>
DNS 名制御による HA クラスタ	他サブネット上の常時稼働しているインスタンス、またはリージョンのエンドポイント	Ping または LISTEN ポート確認	本書では例として NAT 用インスタンスを指定します。

詳細は『リファレンスガイド』-「第 7 章 ネットワークパーティション解決リソースの詳細」を参照してください。

NP 解決先の設定について

本ガイドの構成はクラスタシステムが VPC 内で完結する場合の一例※です。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。

※ IP モニタリソースから NAT 用のインスタンスへの通信可否を確認することで、サブネット間通信の健全性を監視します。応答がない場合は NP 状態とみなし、当該ノードをシャットダウンさせることで両系活性を回避します。

1-5. 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。○:可能 ×: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	○	○
フローティング IP リソースの使用可否	○	×
仮想 IP リソースの使用可否	○	×
AWS Elastic IP リソースの使用可否	×	○
AWS 仮想 IP リソースの使用可否	×	○
AWS DNS リソースの使用可否	×	○

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。

	手順	オンプレミス	AWS
CLUSTERPRO インストール前			
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「4-1 VPC 環境の設定」参照 ◇AWS Elastic IP リソースを使用する場合 ・本書「5-1 VPC 環境の設定」参照 ◇AWS DNS リソースを使用する場合 ・本書「6-1 VPC 環境の設定」参照
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「4-2 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「5-2 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「6-2 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「第 1 章 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「第 4 章 グループ リソースの詳細」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	オンプレミスと同様

5	ネットワークの確認	「第 1 章 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	
6	ルートファイルシステムの確認		
7	ファイアウォールの確認		
8	サーバの時刻同期		
9	CLUSTERPRO のインストール	『インストール&設定ガイド』の「第 3 章 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			
10	CLUSTERPRO のライセンスを登録	『インストール&設定ガイド』の「第 4 章 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「第 5 章 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「第 5 章 クラスタ構成情報を作成する」の「クラスタ構成情報の作成手順」 ・『リファレンスガイド』-「第 7 章 NP 解決リソースの詳細」	◇AWS 仮想 IP リソースを使用する場合 ・本書「4-3 CLUSTERPRO の設定」の「3) モニタリソースの追加 IP モニタリソース」参照 ◇AWS Elastic IP リソースを使用する場合 ・本書「5-3 CLUSTERPRO の設定」の「1) クラスタの構築」参照 ◇AWS DNS リソースを使用する場合 ・本書「6-3 CLUSTERPRO の設定」の「1) クラスタの構築」参照
13	クラスタの作成-フェイルオーバーグループの作成、モニタリソースの作成	『インストール&設定ガイド』の「第 5 章 クラスタ構成情報を作成する」の「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「4-3 CLUSTERPRO の設定」参照 ・『リファレンスガイド』の「第 4 章 グループリソースの詳細」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「5-3 CLUSTERPRO の設定」参照 ・『リファレンスガイド』の「第 4 章 グループリソースの詳細」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「6-3 CLUSTERPRO の設定」参照

			・『リファレンスガイド』の「第 4 章 グループリソースの詳細」の 「AWS DNS リソースを理解する」 参照
--	--	--	---

第 2 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』-「第 3 章 CLUSTERPRO の動作環境」-「AWS Elastic IP リソース、AWS 仮想 IP リソース、AWS Elastic IP モニタリソース、AWS 仮想 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』-「第 3 章 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 3 章 注意事項

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。

※これ以外の使用方法をご検討の場合は、下記の窓口にご相談ください。

(AWS Direct Connect を用いて HA クラスタに直接アクセスしたい等)

CLUSTERPRO プリセールス窓口 info@clusterpro.jp [nec.com](mailto:info@clusterpro.jp)

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 用インスタンス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 用インスタンスの代わりに 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。

ただし、NAT 用インスタンスが存在しないことにより、NP 解決のための IP モニタリソースによる IP アドレス監視が行えなくなるため、別途、応答確認用装置を用意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。

VPC エンドポイントは、Amazon Route 53 には未対応のため、「DNS 名制御による HA クラスタ」構成において VPC エンドポイントを使用することはできません。

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』-「第 5 章 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』-「第 5 章 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』-「第 5 章 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』-「第 5 章 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

ミラー方式の HA クラスタでは、ミラーディスクへの書き込み要求は、以下の経路となります。

書き込み要求 I/O:

現用系側ゲスト OS - 現用系側ホスト OS - 待機系側ホスト OS - 待機系側ゲスト OS

書き込み完了通知:

待機系側ゲスト OS - 待機系側ホスト OS - 現用系側ホスト OS - 現用系側ゲスト OS

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。

第 4 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。
図中の番号は、後述の説明および設定値との対応を示しています。

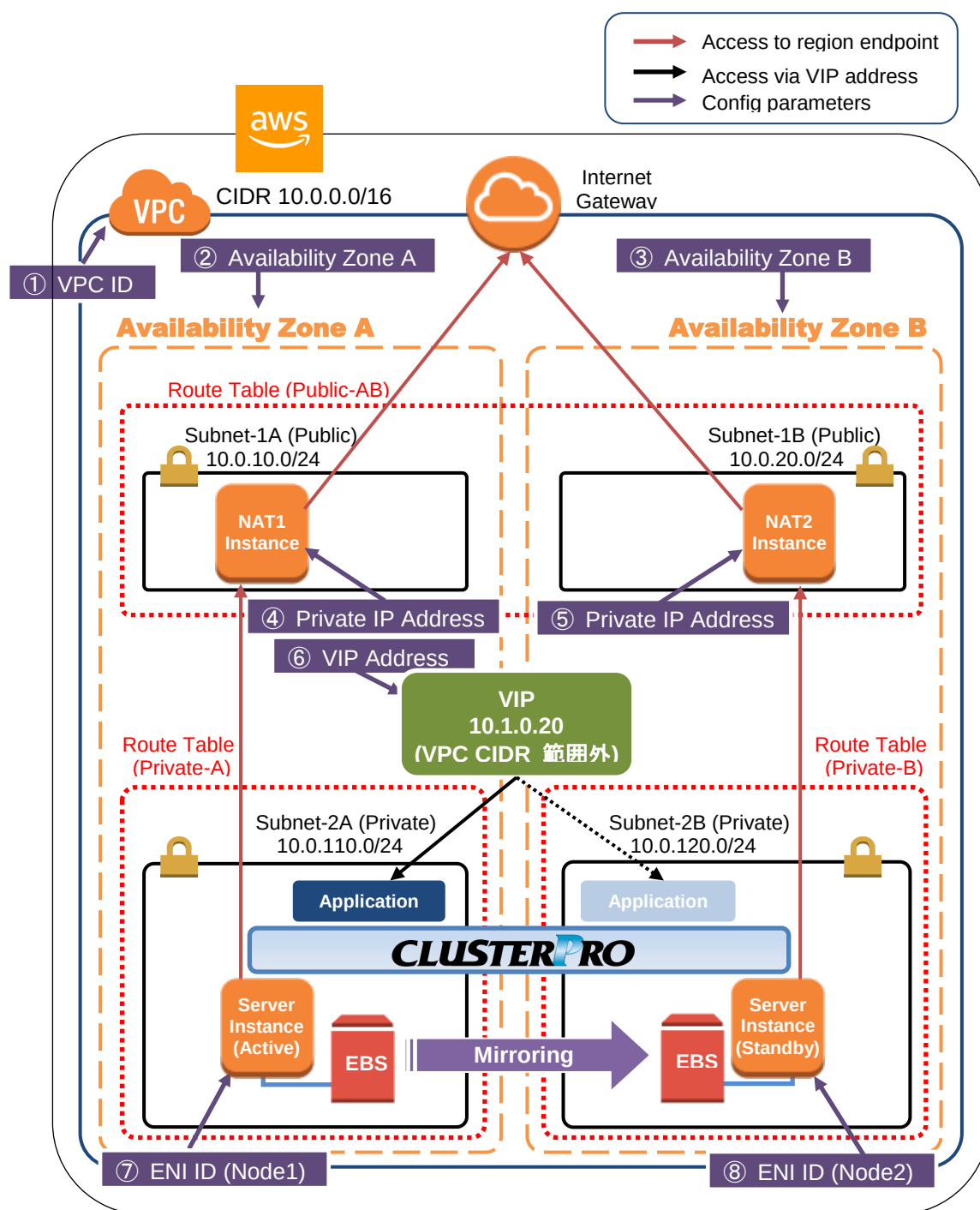


図 4-1 システム構成 VIP 制御による HA クラスタ

4-1. 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。また、本書では HA クラスターノード用のインスタンスに ENI を追加して運用するケースは対象外としております。

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 [Subnet] で VPC およびサブネットの追加操作を行います。

① VPC ID

VPC ID (vpc-xxxxxxx) 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 Gateway] 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 クラスター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、WebManager 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「第 5 章 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 クラスター用のインスタンスを追加する

HA クラスター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、インスタンス作成時に忘れずに IAM ロールを指定してください (作成後に IAM ロールを指定、または変更することはできません)。

⇒ 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「第 7 章 IAM の設定」を参照してください。

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。

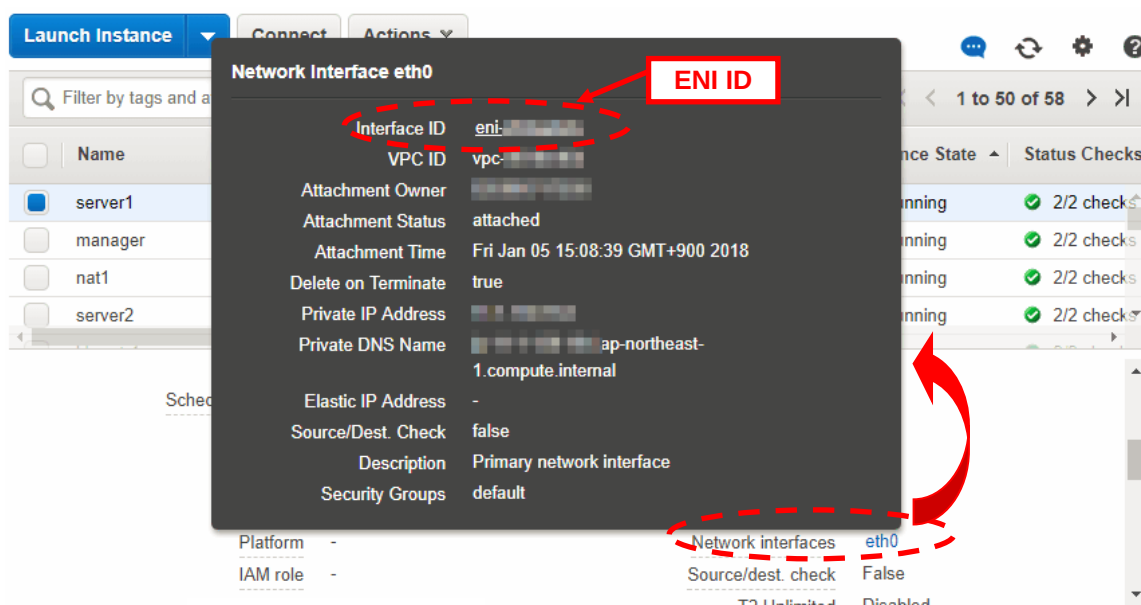
⑦ ENI ID (Node1)

⑧ ENI ID (Node2)

各インスタンスの ENI ID (eni-xxxxxxx) 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 クラスター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 用のインスタンスを作成します。AWS 環境では、NAT 用の AMI として amzn-ami-vpc-nat-pv-2014.09.1.x86_64-ebs などが用意されています。

NAT 作成時には Public IP を有効にします。また、追加した NAT 用のインスタンスについて Source/Dest. Check を disabled に変更します。この操作を行わないと NAT 機能が有効になりません。

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

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の ENI ID) ⑦ ENI ID (Node1)	追加(任意)

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	NAT1	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の ENI ID) ⑦ ENI ID (Node1)	追加(任意)

◇ 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	NAT2	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の ENI ID) ⑦ ENI ID (Node1)	追加(任意)

フェイルオーバー時に 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 Address

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。

4-2. 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』-「第 3 章 CLUSTERPRO の動作環境」-「AWS Elastic IP リソース、AWS 仮想 IP 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「第 5 章 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。

/sbin、/bin、/usr/sbin、/usr/bin

4) AWS CLI のインストール

シェルから pip コマンドを実行し、AWS CLI をインストールします。

```
$ pip install awscli
```

pip コマンドに関する詳細は下記を参照してください。

<https://pip.pypa.io/en/latest/>

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。

<http://docs.aws.amazon.com/cli/latest/userguide/installing.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
```

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。

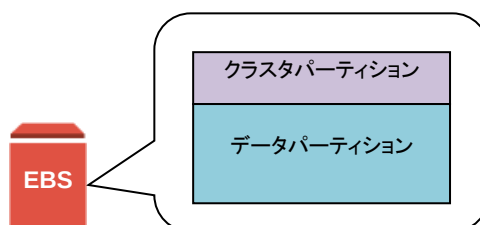


図 4-2 EBS のパーティション分割例

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「第 1 章 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」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。

4-3. CLUSTERPRO の設定

WebManager のクラスタ生成ウィザードで以下の設定を実施します。

WebManager 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「第 5 章 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 (IP モニタリソース)

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。

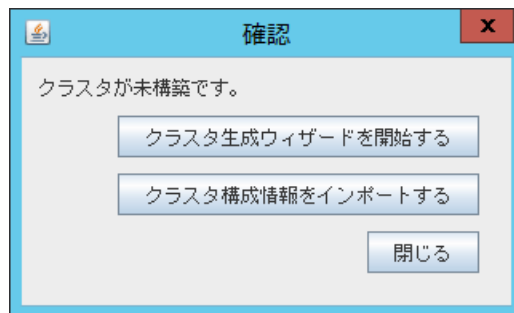
1) クラスタの構築

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。

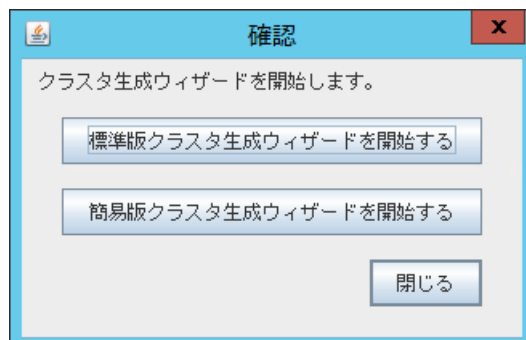
◇ クラスタの構築

【手順】

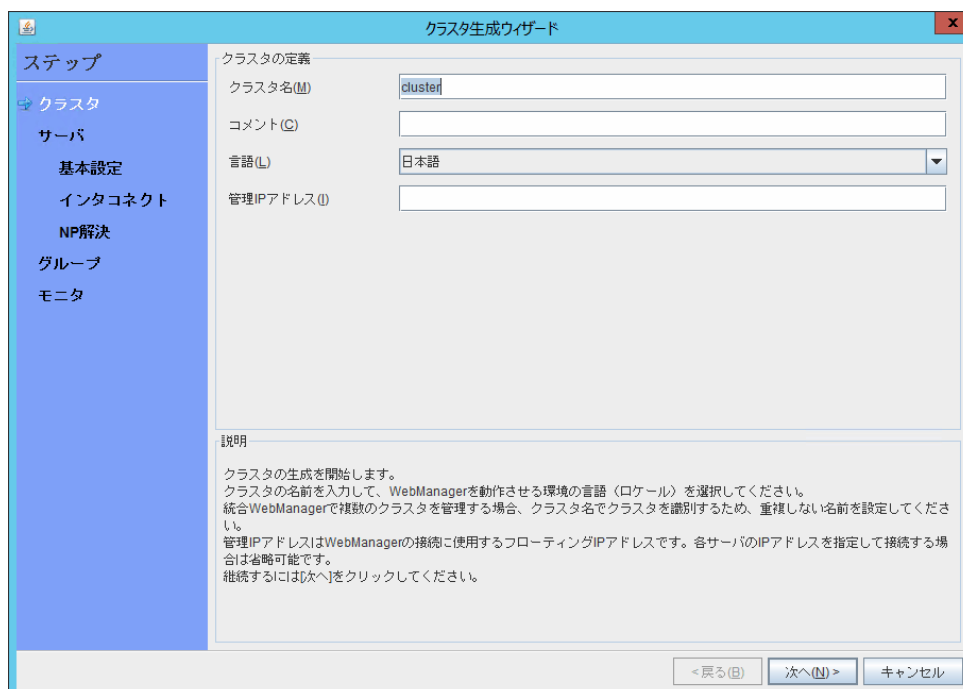
1. WebManager にアクセスすると、以下のダイアログが表示されます。
[クラスタ生成ウィザードを開始する] をクリックします。



2. 以下のダイアログが表示されます。
[標準版クラスタ生成ウィザードを開始する] をクリックします。



3. クラスタの定義のページが表示されます。
[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。設定反映後、WebManager の表示言語はここで選択した言語に切り替わります。



クラスタ生成ウィザード

ステップ

- クラスタ
- サーバ
- 基本設定
- インタコネクト
- NP解決
- グループ
- モニタ

クラスタの定義

クラスタ名(M)

コメント(C)

言語(L) 日本語

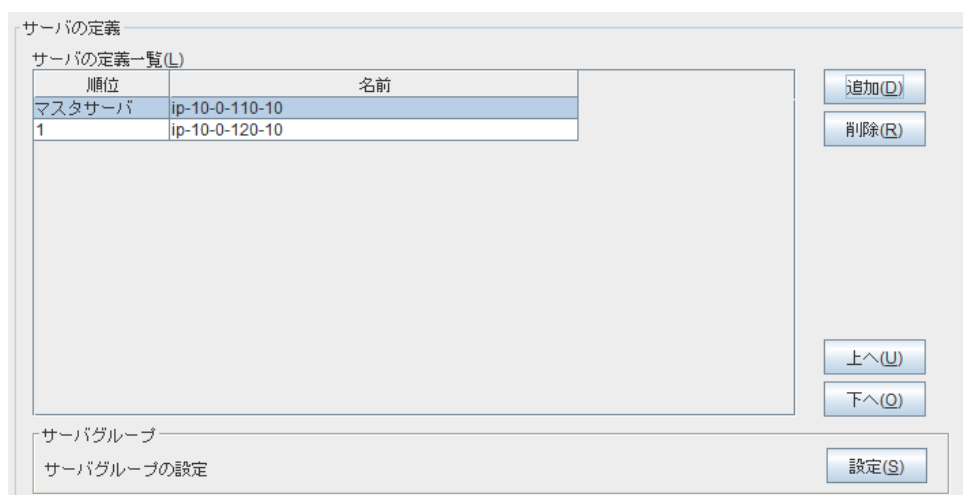
管理IPアドレス(I)

説明

クラスタの生成を開始します。
クラスタの名前を入力して、WebManagerを動作させる環境の言語（ロケール）を選択してください。
統合WebManagerで複数のクラスタを管理する場合、クラスタ名でクラスタを識別するため、重複しない名前を設定してください。
管理IPアドレスはWebManagerの接続に使用するフローティングIPアドレスです。各サーバのIPアドレスを指定して接続する場合は省略可能です。
継続する[次へ]をクリックしてください。

< 戻る(B) 次へ(N) > キャンセル

4. サーバの定義のページが表示されます。
WebManager 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）。



サーバの定義

サーバの定義一覧(L)

順位	名前
マスタサーバ	ip-10-0-110-10
1	ip-10-0-120-10

追加(D)

削除(R)

上へ(U)

下へ(D)

サーバグループ

サーバグループの設定

設定(S)

5. [次へ] をクリックします。

6. [インターコネクト] のページが表示されます。
 インター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。

優先度	種別	MDC	ip-10-0-110-10	ip-10-0-120-10
1	カーネルモード	mdc1	10.0.110.10	10.0.120.10

7. [次へ] をクリックします。
8. NP 解決のページが表示されます。
 ただし、NP 解決は本ページでは設定せず、別途 IP モニタリソースを追加し、AZ ごとに設置された各 NAT に対する監視を行うことによって同等のことを実現します (NP 解決の設定は、後述の「3) モニタリソースの追加」で行います)。
 [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
 フェイルオーバーグループを作成します。

【手順】

1. [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。

2. [次へ] をクリックします。

3. [起動可能サーバー一覧]のページが表示されます。
何も指定せず [次へ] をクリックします。
4. グループ属性の設定のページが表示されます。
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]のページが表示されます。
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「第 4 章 グループリソースの詳細」-「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 (failover1) のリソース定義] 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(mirror disk resource) 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。
3. [次へ] をクリックします。
4. 依存関係設定のページが表示されます。
何も指定せず [次へ] をクリックします。
5. [活性異常検出時の復旧動作]、[非活性異常時の復旧動作] が表示されます。
[次へ] をクリックします。
6. 詳細設定のページが表示されます。
[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「4-2 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「第 4 章 グループリソースの詳細」-「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 (failover1) のリソース定義] 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 virtual ip resource) 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。

3. [次へ] をクリックします。
4. 依存関係設定のページが表示されます。何も指定せず [次へ] をクリックします。
5. [活性異常検出時の復旧動作]、[非活性異常時の復旧動作] が表示されます。
[次へ] をクリックします。
6. 詳細設定のページが表示されます。
[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。

[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。
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。
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。

7. 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。
 [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。

The screenshot shows two configuration panels for nodes. The top panel is for 'ip-10-0-110-10' and the bottom for 'ip-10-0-120-10'. Both have '個別に設定する(U)' checked. The 'VPC ID(P)' field contains 'vpc-1234abcd' and the 'ENI ID(E)' field contains 'eni-xxxxxxx' for Node 1 and 'eni-yyyyyyy' for Node 2. Callouts point to these fields.

8. [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「第 5 章 モニタリソースの詳細」-「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 monitor) 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。

The form has three input fields: 'タイプ(T)' with a dropdown menu showing 'AWS AZ monitor', '名前(M)' with the text 'awsazw1', and 'コメント(C)' which is empty. A button labeled 'ライセンス情報取得(L)' is located at the bottom right.

3. [次へ] をクリックします。
4. 監視(共通)設定のページが表示されます。
何も指定せず [次へ] をクリックします。

5. 監視(固有)設定のページが表示されます。
[共通] タブの[アベイラビリティゾーン] ボックスに監視するアベイラビリティ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ゾーンを設定します)。



共通 ip-10-0-110-10 ip-10-0-120-10

アベイラビリティゾーン(Z)

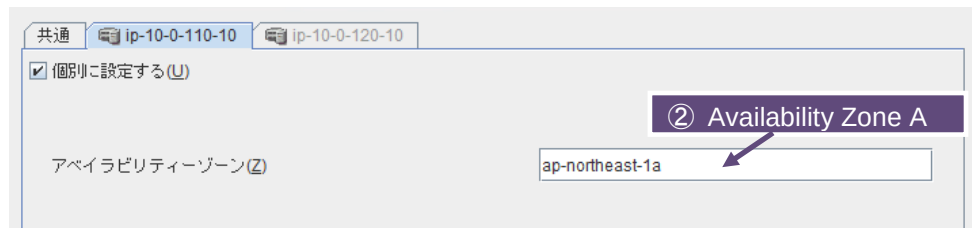
ap-northeast-1a

② Availability Zone A

AWS CLI コマンド応答取得失敗時動作(P)

回復動作を実行しない(警告を表示する)

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。
[アベイラビリティゾーン] 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ゾーンを設定します。



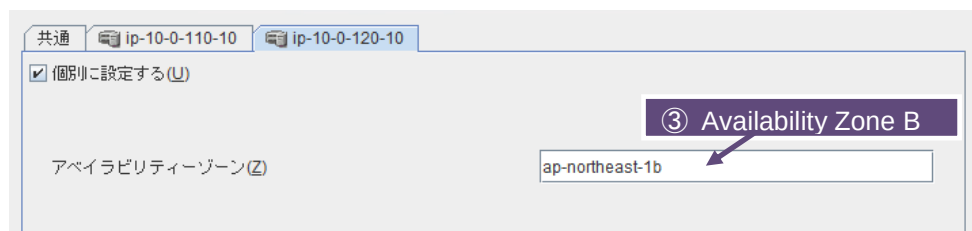
共通 ip-10-0-110-10 ip-10-0-120-10

☒ 個別に設定する(U)

アベイラビリティゾーン(Z)

ap-northeast-1a

② Availability Zone A



共通 ip-10-0-110-10 ip-10-0-120-10

☒ 個別に設定する(U)

アベイラビリティゾーン(Z)

ap-northeast-1b

③ Availability Zone B

7. [次へ] をクリックします。

8. 回復動作設定のページが表示されます。
[回復対象] に [LocalServer]を設定します。

9. [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。

OS API 及び AWS CLI コマンドを利用して、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』の「第 5 章 モニタリソースの詳細」-「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。

◇ IP モニタリソース

各アベイラビリティゾーンに配置されている NAT 用のインスタンスに ping することで、サブネットの健全性を監視する IP モニタリソースを作成します。以下を指定してください。

【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 (ip monitor) を選択し、[名前] ボックスにモニタリソース名 (ipw1) を入力します。

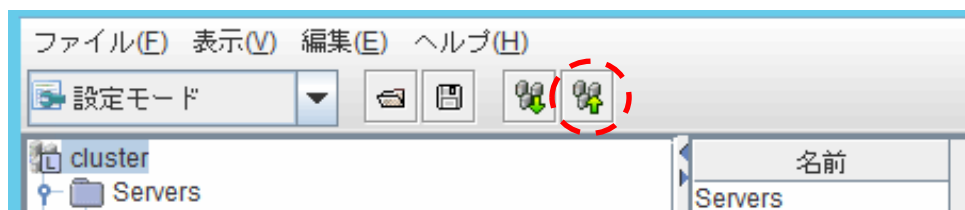
3. [次へ] をクリックします。
4. 監視(共通)設定のページが表示されます。
[監視タイミグ] が [常時] であることを確認し、[次へ] をクリックします。
5. 監視(固有)設定のページが表示されます。
[共通] タブの [IP アドレス一覧] に、現用系側のインスタンスの属するアベイラビリティーゾーンに配置された NAT 用のインスタンスの Private IP アドレスを入力します。

6. [次へ] をクリックします。
7. 回復動作設定のページが表示されます。
[回復対象] に [LocalServer] を設定します。
[最終動作] に [クラスタサービス停止と OS シャットダウン] を設定します。

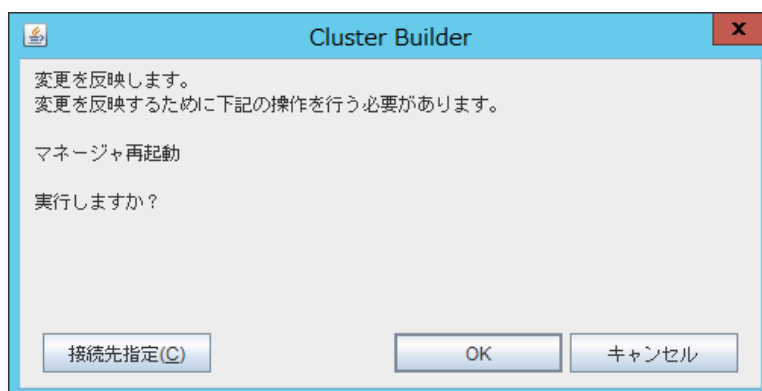
8. [完了] をクリックして設定を終了します。

4) 設定の反映とクラスタの起動

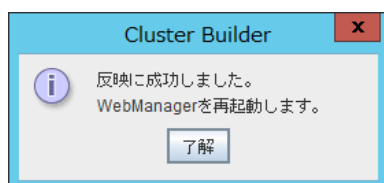
設定がすべて完了したら、メニュー下の [設定の反映] アイコンをクリックします。



マネージャ再起動の確認ダイアログが表示されます。

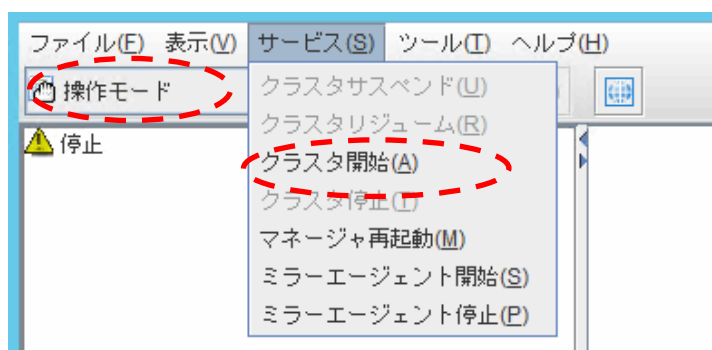


[OK] をクリックします。



[了解] をクリックします。

モードを [操作モード] に切り替え、メニュー [サービス] – [クラスタ開始] をクリックします。



第 5 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。
図中の番号は、後述の説明および設定値との対応を示しています。

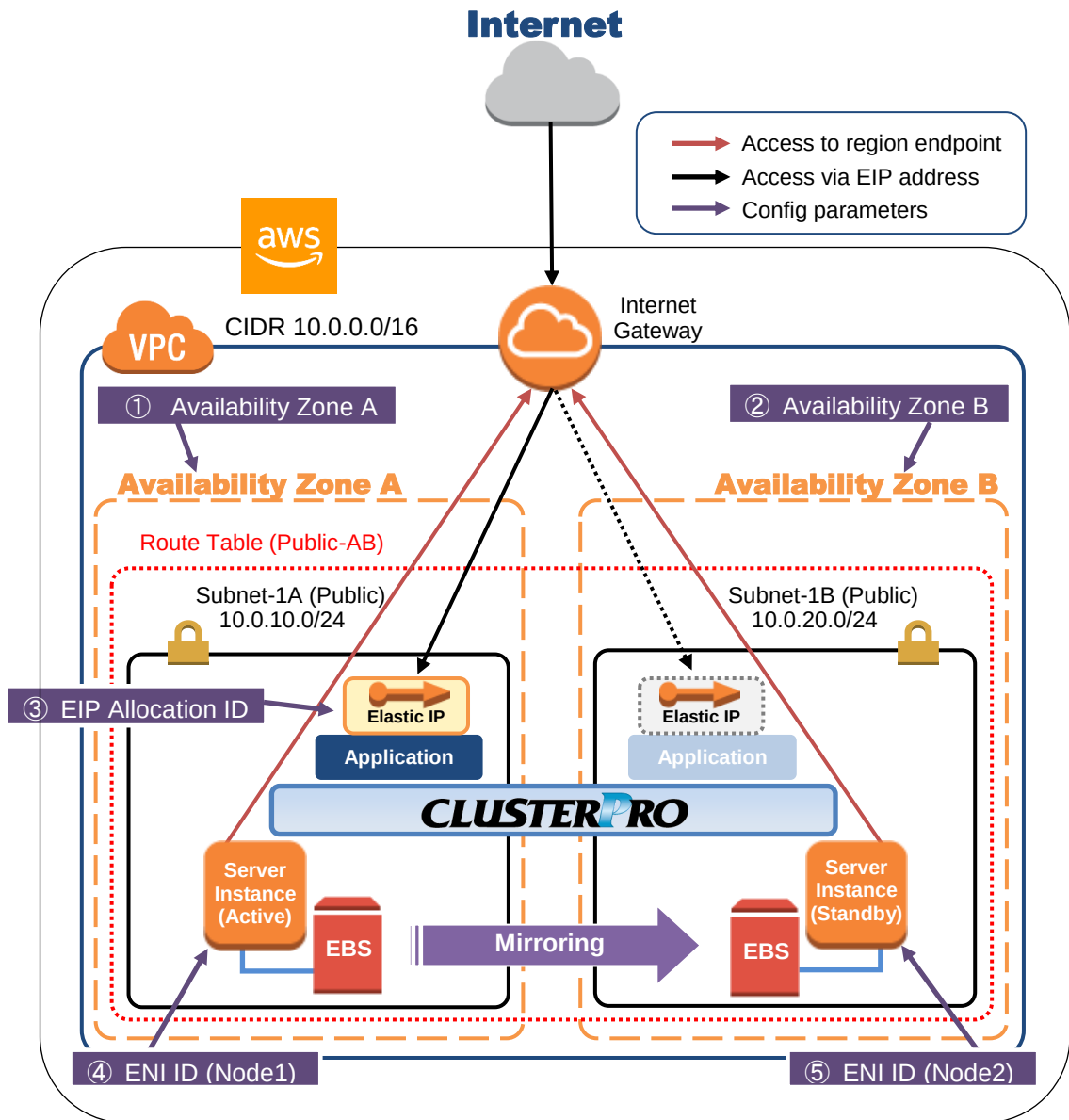


図 5-1 システム構成 EIP 制御による HA クラスタ

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。また、本書では HA クラスターノード用のインスタンスに ENI を追加して運用するケースは対象外としております。

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 [Subnet] 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 Gateway] 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 クラスター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、WebManager 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「第 5 章 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 クラスター用のインスタンスを追加する

HA クラスター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、インスタンス作成時に忘れずに IAM ロールを指定してください (作成後に IAM ロールを指定、または変更することはできません)。

⇒ 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「第 7 章 IAM の設定」を参照してください。

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。

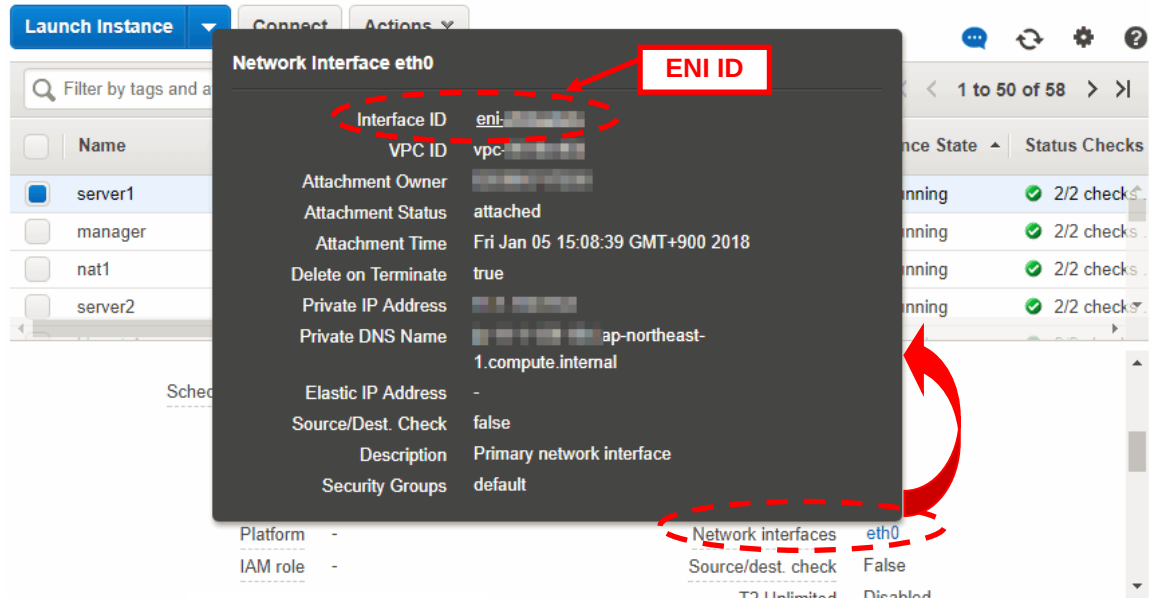
④ ENI ID (Node1)

⑤ ENI ID (Node2)

ここで各インスタンスの ENI ID (eni-xxxxxxx) 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 EIP Allocation ID

ここで追加した EIP の Allocation ID (eipalloc-xxxxxxx) 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)

フェイルオーバー時に 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。

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 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』の「第 3 章 CLUSTERPRO の動作環境」-「AWS Elastic IP リソース、AWS 仮想 IP 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「第 5 章 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。

/sbin、/bin、/usr/sbin、/usr/bin

4) AWS CLI のインストール

シェルから pip コマンドを実行し、AWS CLI をインストールします。

```
$ pip install awscli
```

pip コマンドに関する詳細は下記を参照してください。

<https://pip.pypa.io/en/latest/>

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。

<http://docs.aws.amazon.com/cli/latest/userguide/installing.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
```

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。

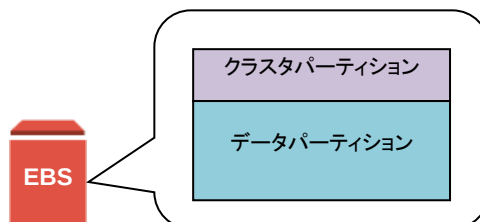


図 5-2 EBS のパーティション分割例

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「第 1 章 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」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。

5-3. CLUSTERPRO の設定

WebManager のクラスタ生成ウィザードで以下の設定を実施します。
WebManager 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「第 5 章 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(カスタムモニタリソース)

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。

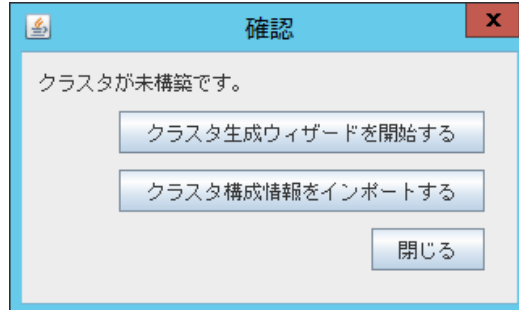
1) クラスタの構築

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。

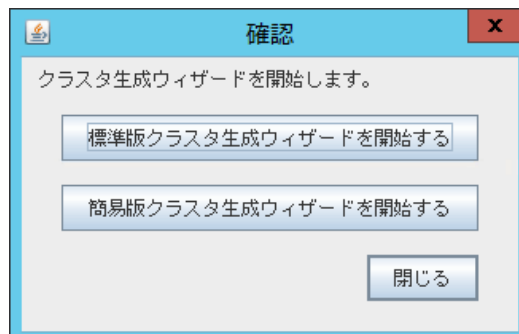
◇ クラスタの構築

【手順】

1. WebManager にアクセスすると、以下のダイアログが表示されます。
[クラスタ生成ウィザードを開始する] をクリックします。



2. 以下のダイアログが表示されます。
[標準版クラスタ生成ウィザードを開始する] をクリックします。



3. クラスタの定義のページが表示されます。
[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。設定反映後、WebManager の表示言語はここで選択した言語に切り替わります。

クラスタ生成ウィザード

ステップ

- クラスタ
- サーバ
- 基本設定
- インタコネクト
- NP解決
- グループ
- モニタ

クラスタの定義

クラスタ名(M)

コメント(C)

言語(L)

管理IPアドレス(I)

説明

クラスタの生成を開始します。
クラスタの名前を入力して、WebManagerを動作させる環境の言語（ロケール）を選択してください。
統合WebManagerで複数のクラスタを管理する場合、クラスタ名でクラスタを識別するため、重複しない名前を設定してください。
管理IPアドレスはWebManagerの接続に使用するフローティングIPアドレスです。各サーバのIPアドレスを指定して接続する場合は省略可能です。
継続する[次へ]をクリックしてください。

< 戻る(B) 次へ(N) > キャンセル

4. サーバの定義のページが表示されます。
WebManager 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）。

サーバの定義

サーバの定義一覧(L)

順位	名前
マスタサーバ	ip-10-0-10-10
1	ip-10-0-20-10

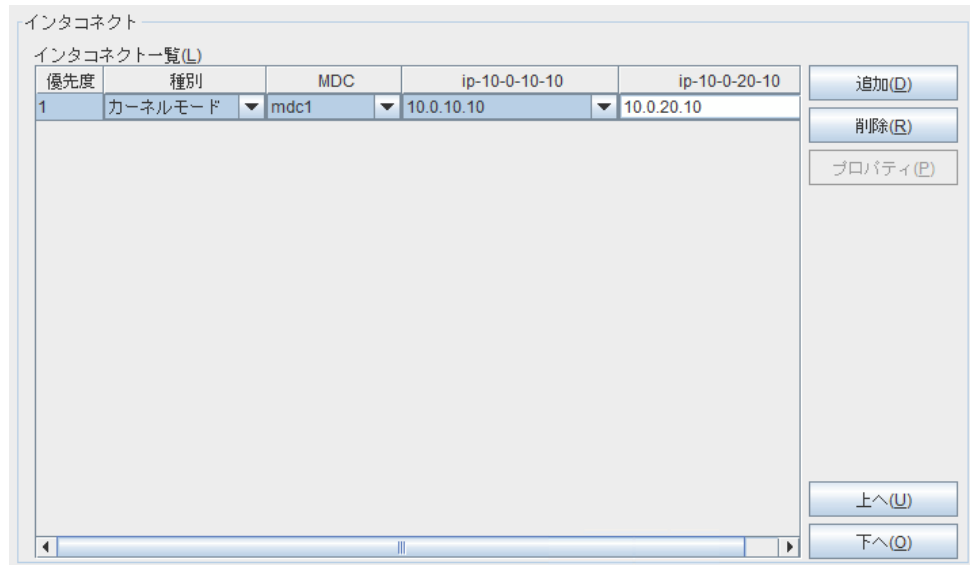
追加(D) 削除(R)

上へ(U) 下へ(D)

サーバグループ

サーバグループの設定 設定(S)

5. [次へ] をクリックします。
6. [インターコネクト] のページが表示されます。
インター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。



7. [次へ] をクリックします。

8. NP 解決のページが表示されます。

ただし、NP 解決は本ページでは設定せず、別途カスタムモニタリソースを追加し、リージョンのエンドポイントの 443 ポートに対して LISTEN 確認などを行うことによって同等のことに実現します(NP 解決の設定は後述の「3) モニタリソースの追加」で行います)。

[次へ] をクリックします。

2) グループリソースの追加

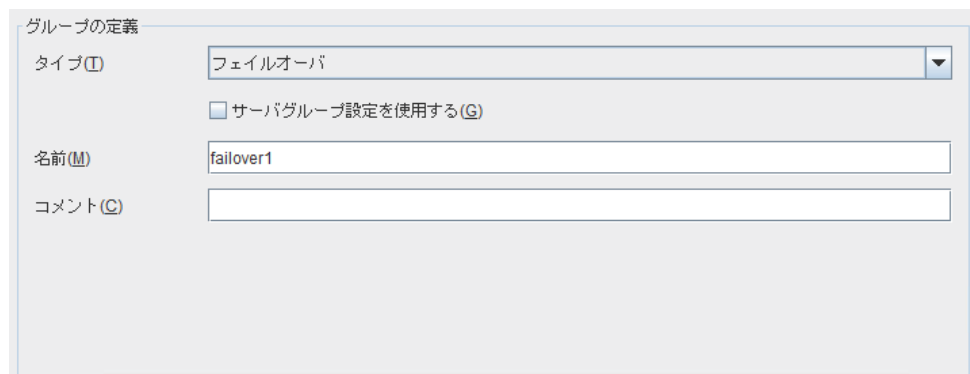
◇ グループの定義

フェイルオーバーグループを作成します。

【手順】

1. [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。



2. [次へ] をクリックします。

3. [起動可能サーバー一覧]のページが表示されます。

何も指定せず [次へ] をクリックします。

4. グループ属性の設定のページが表示されます。
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]のページが表示されます。
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「第 4 章 グループリソースの詳細」-「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 (failover1) のリソース定義] 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(mirror disk resource) 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。
3. [次へ] をクリックします。
4. 依存関係設定のページが表示されます。
何も指定せず [次へ] をクリックします。
5. [活性異常検出時の復旧動作]、[非活性異常時の復旧動作] が表示されます。
[次へ] をクリックします。
6. 詳細設定のページが表示されます。
[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 Elastic IP リソース

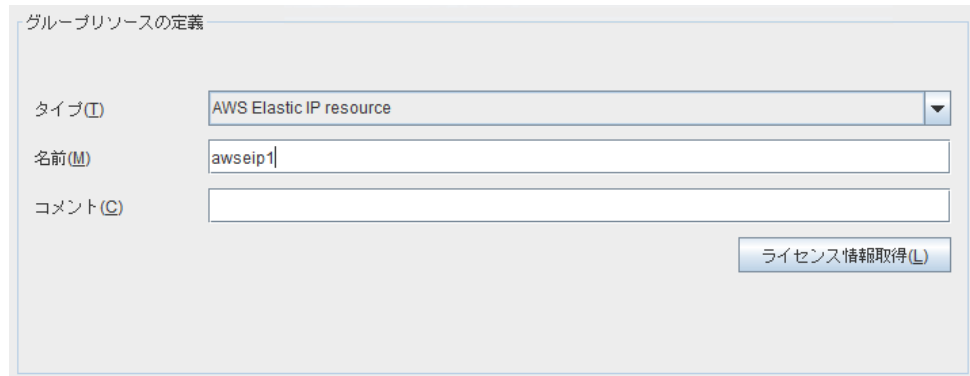
AWS CLI を利用して、EIP の制御を行う AWS Elastic IP リソースを追加します。

詳細は『リファレンスガイド』の「第 4 章 グループリソースの詳細」-「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 (failover1) のリソース定義] 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 resource) 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。



グループリソースの定義

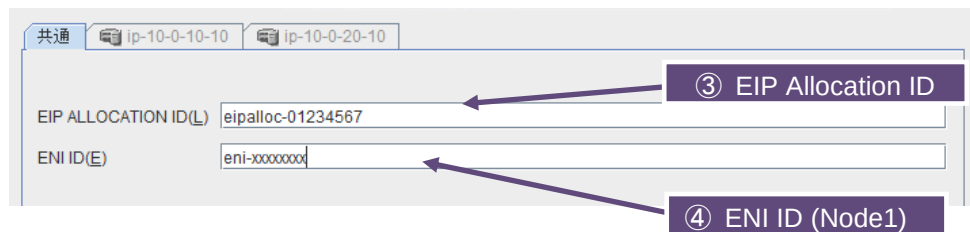
タイプ(T) AWS Elastic IP resource

名前(M) awseip1

コメント(C)

[ライセンス情報取得\(L\)](#)

3. [次へ] をクリックします。
4. 依存関係設定のページが表示されます。何も指定せず [次へ] をクリックします。
5. [活性異常検出時の復旧動作]、[非活性異常時の復旧動作] が表示されます。
[次へ] をクリックします。
6. 詳細設定のページが表示されます。
[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。
[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。



共通 ip-10-0-10-10 ip-10-0-20-10

EIP ALLOCATION ID(L) eipalloc-01234567 ③ EIP Allocation ID

ENI ID(E) eni-xxxxxxxx ④ ENI ID (Node1)

7. 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。

The first screenshot shows the configuration for Node1. The 'ip-10-0-10-10' tab is selected. The checkbox '個別に設定する(U)' is checked. The 'ENI ID(E)' field contains 'eni-xxxxxxxx'. A callout '④ ENI ID (Node1)' points to the field.

The second screenshot shows the configuration for Node2. The 'ip-10-0-20-10' tab is selected. The checkbox '個別に設定する(U)' is checked. The 'ENI ID(E)' field contains 'eni-yyyyyyyy'. A callout '⑤ ENI ID (Node2)' points to the field.

8. [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「第 5 章 モニタリソースの詳細」-「AWS AZ モニタリソースを理解する」を参照してください。

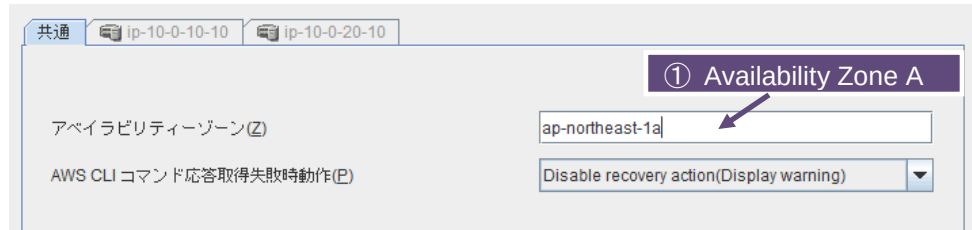
【手順】

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 monitor) 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。

The screenshot shows the 'モニタリソース定義' form. The 'タイプ(T)' dropdown is set to 'AWS AZ monitor'. The '名前(M)' field contains 'awsazw1'. The 'コメント(C)' field is empty. A 'ライセンス情報取得(L)' button is at the bottom right.

3. [次へ] をクリックします。
4. 監視(共通)設定のページが表示されます。
 何も指定せず [次へ] をクリックします。

5. 監視(固有)設定のページが表示されます。
[共通] タブの[アベイラビリティゾーン] ボックスに監視するアベイラビリティ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ゾーンを設定します)。

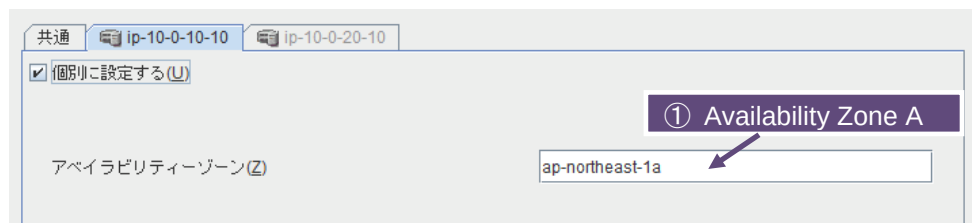


共通 ip-10-0-10-10 ip-10-0-20-10

アベイラビリティゾーン(Z) ap-northeast-1a

AWS CLI コマンド応答取得失敗時動作(P) Disable recovery action(Display warning)

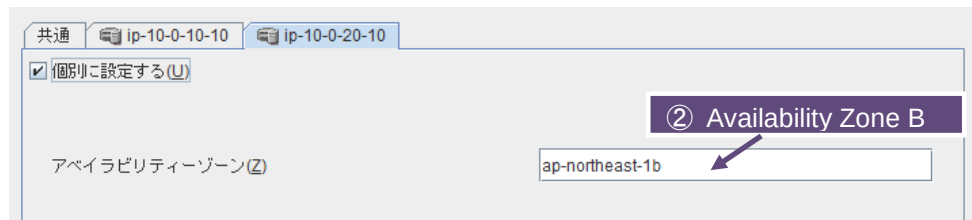
6. 各ノードのタブをクリックし、ノード別設定を行います。
[個別に設定する]をチェックします。
[アベイラビリティゾーン] ボックスに、そのノードに対応するインスタンスのアベイラビリティゾーンを設定します。



共通 ip-10-0-10-10 ip-10-0-20-10

☒ 個別に設定する(U)

アベイラビリティゾーン(Z) ap-northeast-1a



共通 ip-10-0-10-10 ip-10-0-20-10

☒ 個別に設定する(U)

アベイラビリティゾーン(Z) ap-northeast-1b

7. [次へ] をクリックします。

8. 回復動作設定のページが表示されます。
[回復対象] に [LocalServer]を設定します。

回復動作(E) カスタム設定

回復対象 LocalServer 参照(W)

回復スクリプト実行回数(Y) 0 回

☐ 再活性前にスクリプトを実行する(V) 最大再活性回数(R) 0 回

☐ フェイルオーバー実行前にスクリプトを実行する(Q) ☐ フェイルオーバー実行前にマイグレーションを実行する(C) 最大フェイルオーバー回数(T) 0 回

☐ 最終動作前にスクリプトを実行する(X) 最終動作(E) 何もしない

9. [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』の「第 5 章 モニタリソースの詳細」-「AWS Elastic IP モニタリソースを理解する」を参照してください。

◇ カスタムモニタリソース

環境構築しているリージョンのエンドポイントの443ポートへの通信を監視することで、EIP アドレスの通信状態を確認します。

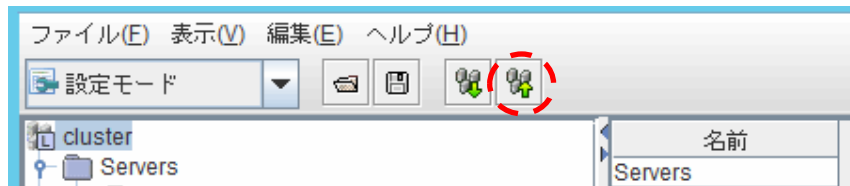
リージョンのエンドポイントは、以下から確認できます。

<http://docs.aws.amazon.com/general/latest/gr/rande.html>

詳細は『リファレンスガイド』の「第 6 章 モニタリソースの詳細」-「カスタム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

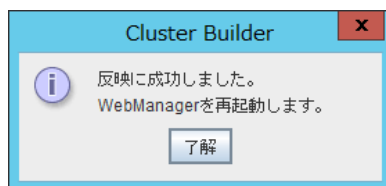
設定がすべて完了したら、メニュー下の [設定の反映] アイコンをクリックします。



マネージャ再起動の確認ダイアログが表示されます。

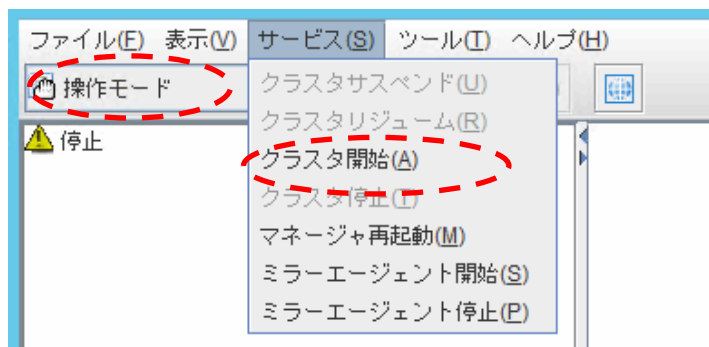


[OK] をクリックします。



[了解] をクリックします。

モードを [操作モード] に切り替え、メニュー [サービス] - [クラスタ開始] をクリックします。



第 6 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。
図中の番号は、後述の説明および設定値との対応を示しています。

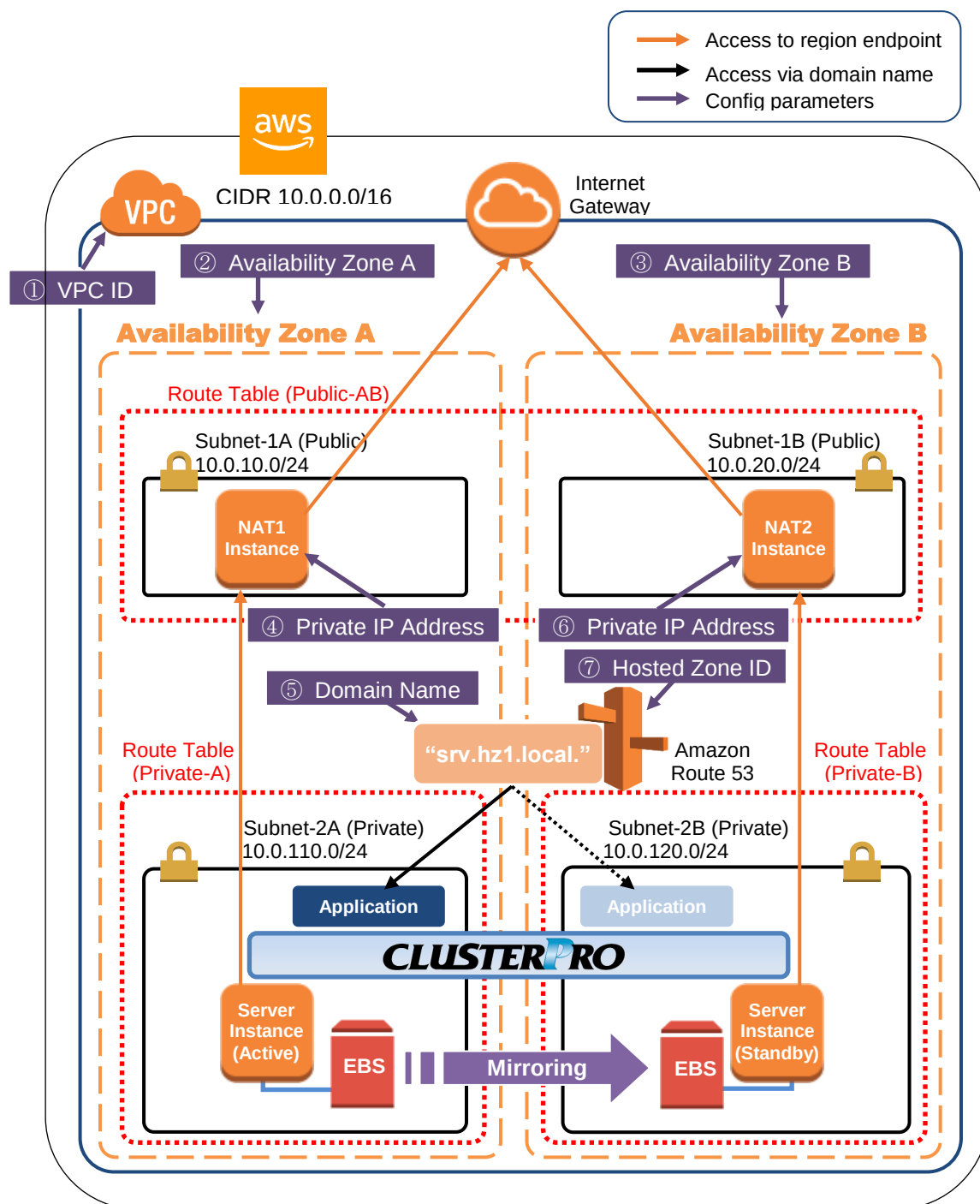


図 6-1 システム構成 DNS 名制御による HA クラスタ

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。また、本書では HA クラスターノード用のインスタンスに ENI を追加して運用するケースは対象外としております。

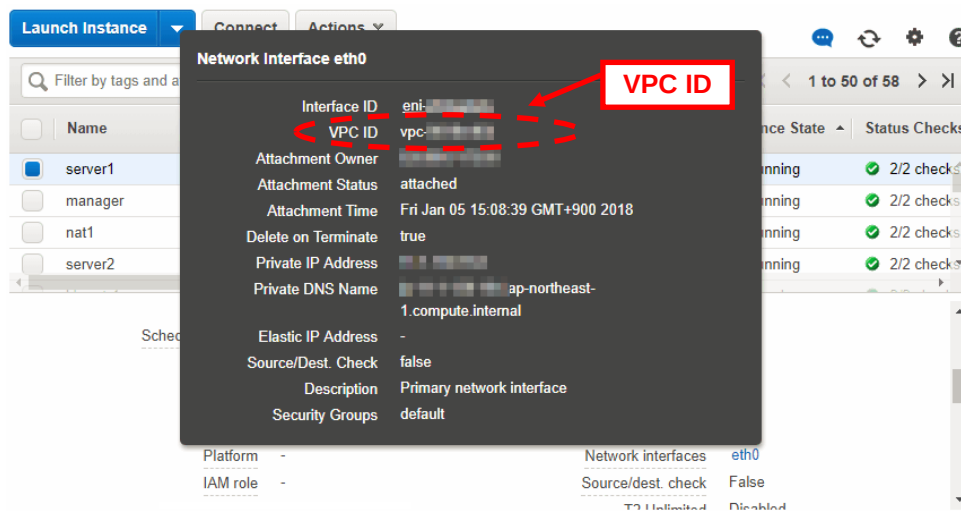
1) VPC およびサブネットを設定する

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 [Subnet] で VPC およびサブネットの追加操作を行います。

① VPC ID

VPC ID (vpc-xxxxxxx) 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 Gateway] 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 クラスター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、WebManager 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「第 5 章 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、インスタンス作成時に忘れずに IAM ロールを指定してください(作成後に IAM ロールを指定、または変更することはできません)。

⇒ 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「第 7 章 IAM の設定」を参照してください。

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 用のインスタンスを作成します。AWS 環境では、NAT 用の AMI として `amzn-ami-vpc-nat-pv-2014.09.1.x86_64-ebs` などが用意されています。

NAT 作成時には Public IP を有効にします。また、追加した NAT 用のインスタンスについて Source/Dest. Check を disabled に変更します。この操作を行わないと NAT 機能が有効になりません。

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

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 <code>10.0.0.0/16</code>)	local	最初から存在
<code>0.0.0.0/0</code>	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(Public-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 <code>10.0.0.0/16</code>)	local	最初から存在
<code>0.0.0.0/0</code>	NAT1	追加(必須)

◇ Route Table (Private-B)

Destination	Target	備考
VPC のネットワーク (例では <code>10.0.0.0/16</code>)	local	最初から存在
<code>0.0.0.0/0</code>	NAT2	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 [Hosted zones] から、[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 **① VPC ID** を設定します。

⑦ Hosted Zone ID

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。

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』-「第 3 章 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「第 5 章 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。

/sbin、/bin、/usr/sbin、/usr/bin

4) AWS CLI のインストール

シェルから pip コマンドを実行し、AWS CLI をインストールします。

```
$ pip install awscli
```

pip コマンドに関する詳細は下記を参照してください。

<https://pip.pypa.io/en/latest/>

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。

<http://docs.aws.amazon.com/cli/latest/userguide/installing.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
```

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、それぞれクラスターパーティション、データパーティションに使用します。

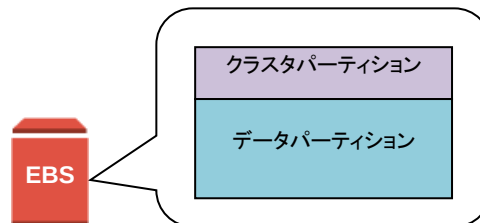


図 6-2 EBS のパーティション分割例

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「第 1 章 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」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

WebManager のクラスタ生成ウィザードで以下の設定を実施します。

WebManager 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「第 5 章 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(IP モニタリソース)

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。

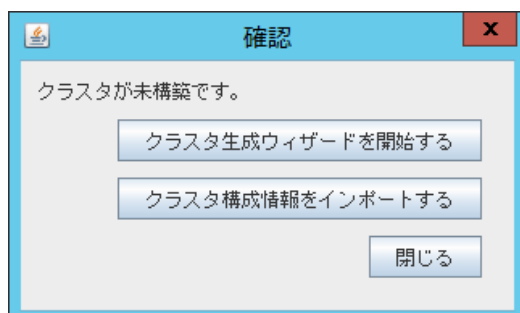
1) クラスタの構築

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。

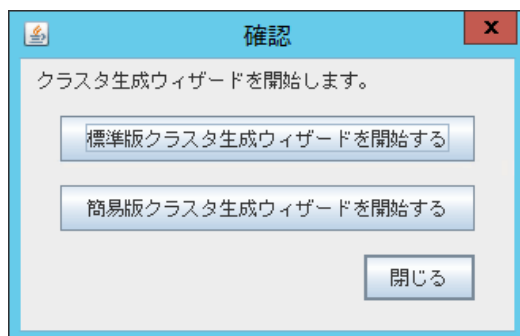
◇ クラスタの構築

【手順】

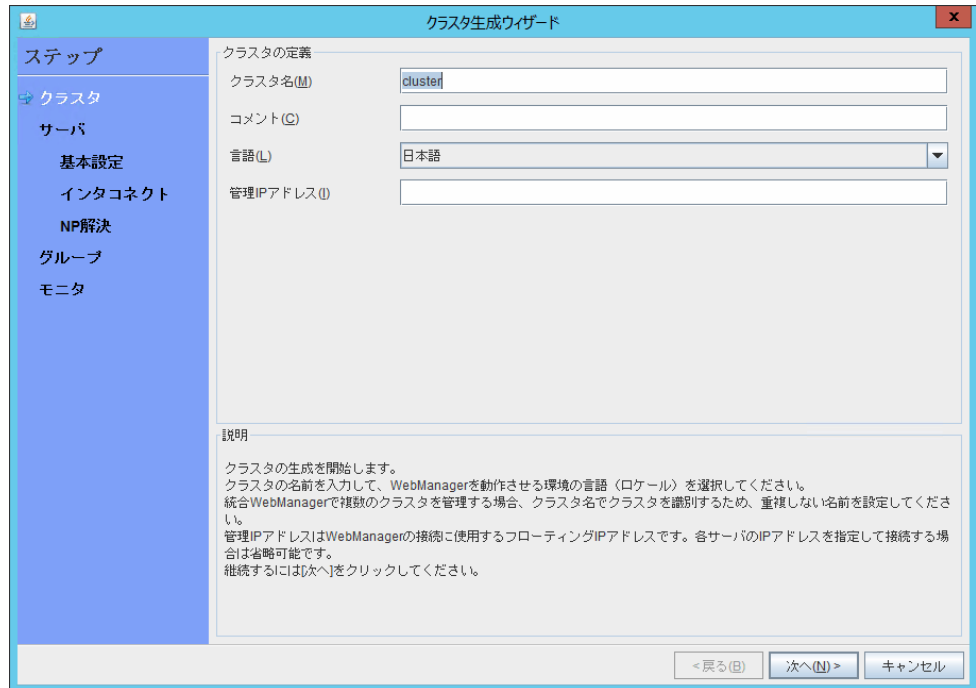
1. WebManager にアクセスすると、以下のダイアログが表示されます。
[クラスタ生成ウィザードを開始する] をクリックします。



2. 以下のダイアログが表示されます。
[標準版クラスタ生成ウィザードを開始する] をクリックします。



3. クラスタの定義のページが表示されます。
 [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。設定反映後、WebManager の表示言語はここで選択した言語に切り替わります。



クラスタ生成ウィザード

クラスタの定義

クラスタ名(M)

コメント(C)

言語(L)

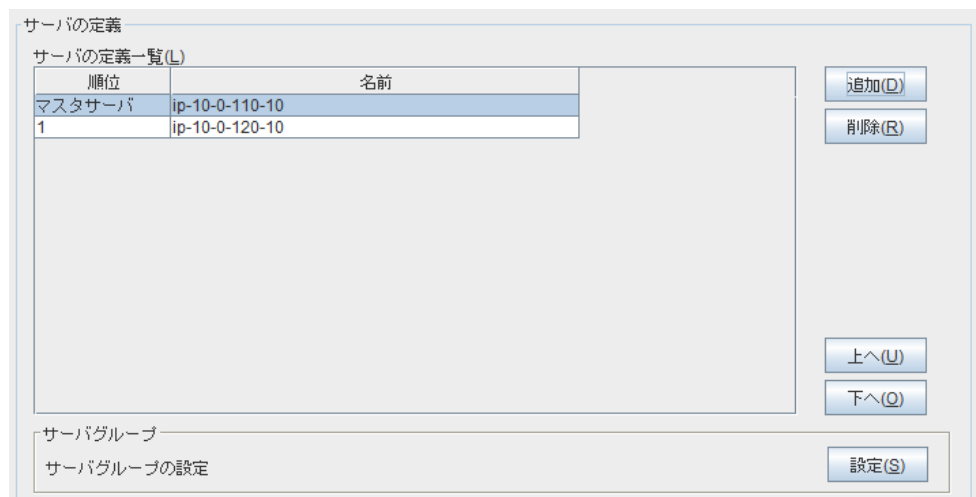
管理IPアドレス(I)

説明

クラスタの生成を開始します。
 クラスタの名前を入力して、WebManagerを動作させる環境の言語（ロケール）を選択してください。
 統合WebManagerで複数のクラスタを管理する場合、クラスタ名でクラスタを識別するため、重複しない名前を設定してください。
 管理IPアドレスはWebManagerの接続に使用するフローティングIPアドレスです。各サーバのIPアドレスを指定して接続する場合は省略可能です。
 継続する[次へ]をクリックしてください。

< 戻る(B) 次へ(N) > キャンセル

4. サーバの定義のページが表示されます。
 WebManager 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）。



サーバの定義

サーバの定義一覧(L)

順位	名前
マスタサーバ	ip-10-0-110-10
1	ip-10-0-120-10

追加(D)

削除(R)

上へ(U)

下へ(D)

サーバグループ

サーバグループの設定

設定(S)

5. [次へ] をクリックします。

6. [インターコネクト] のページが表示されます。
 インター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。

優先度	種別	MDC	ip-10-0-110-10	ip-10-0-120-10
1	カーネルモード	mdc1	10.0.110.10	10.0.120.10

7. [次へ] をクリックします。
8. NP 解決のページが表示されます。
 ただし、NP 解決は本ページでは設定せず、別途 IP モニタリソースを追加し、AZ ごとに設置された各 NAT に対する監視を行うことによって同等のを実現します (NP 解決の設定は、後述の「3) モニタリソースの追加」で行います)。
 [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
 フェイルオーバーグループを作成します。

【手順】

1. [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。

2. [次へ] をクリックします。

3. [起動可能サーバー一覧]のページが表示されます。
何も指定せず [次へ] をクリックします。
4. グループ属性の設定のページが表示されます。
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]のページが表示されます。
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「第 4 章 グループリソースの詳細」-「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 (failover1) のリソース定義] 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(mirror disk resource)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。
3. [次へ] をクリックします。
4. 依存関係設定のページが表示されます。
何も指定せず [次へ] をクリックします。
5. [活性異常検出時の復旧動作]、[非活性異常時の復旧動作] が表示されます。
[次へ] をクリックします。
6. 詳細設定のページが表示されます。
[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。

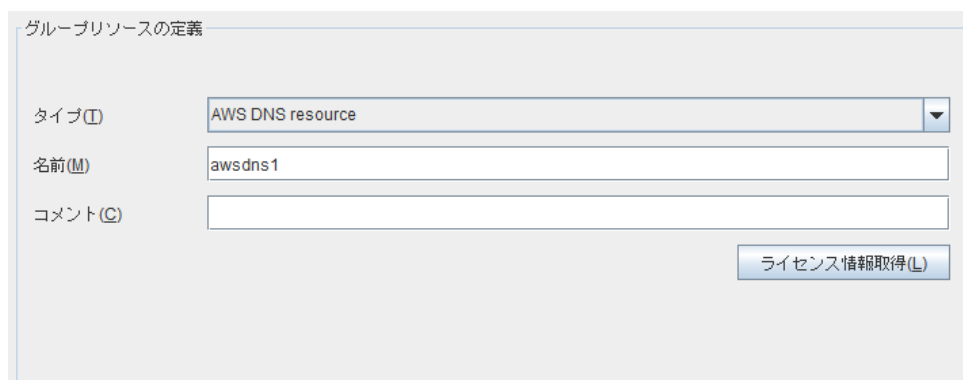
◇ AWS DNS リソース

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』の「第 4 章 グループリソースの詳細」-「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 (failover1) のリソース定義] 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 resource) 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。



グループリソースの定義

タイプ(I) AWS DNS resource

名前(M) awsdns1

コメント(C)

[ライセンス情報取得\(L\)](#)

3. [次へ] をクリックします。
4. 依存関係設定のページが表示されます。何も指定せず [次へ] をクリックします。
5. [活性異常検出時の復旧動作]、[非活性異常時の復旧動作] が表示されます。
[次へ] をクリックします。

6. 詳細設定のページが表示されます。

[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。

[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。
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。

[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。

The screenshot shows the AWS Route 53 console configuration for a Hosted Zone. The configuration is as follows:

Field	Value	Annotation
Hosted Zone ID (H)	ABCDEFGHIJK123	⑦ Hosted Zone ID
Resource Record Set Name (R)	srv.hz1.local.	⑥ Domain Name
IP Address (I)	10.0.110.10	④ Private IP Address (Node1)
TTL (L)	300	秒
☒ 非活性時にリソースレコードセットを削除する (D)		

7. 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。
 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。

8. [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「第 5 章 モニタリソースの詳細」-「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 monitor) 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。

3. [次へ] をクリックします。
4. 監視(共通)設定のページが表示されます。
何も指定せず [次へ] をクリックします。
5. 監視(固有)設定のページが表示されます。
[共通]タブの[アベイラビリティゾーン] ボックスに監視するアベイラビリティ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ゾーンを設定します)。



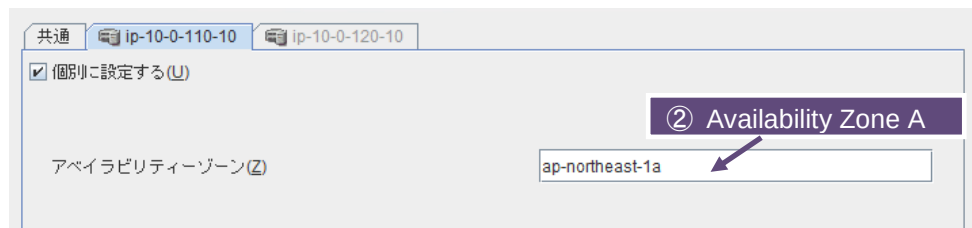
共通 ip-10-0-110-10 ip-10-0-120-10

② Availability Zone A

アベイラビリティゾーン(Z) ap-northeast-1a

AWS CLI コマンド応答取得失敗時動作(P) 回復動作を実行しない(警告を表示する)

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。
[アベイラビリティゾーン] 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ゾーンを設定します。

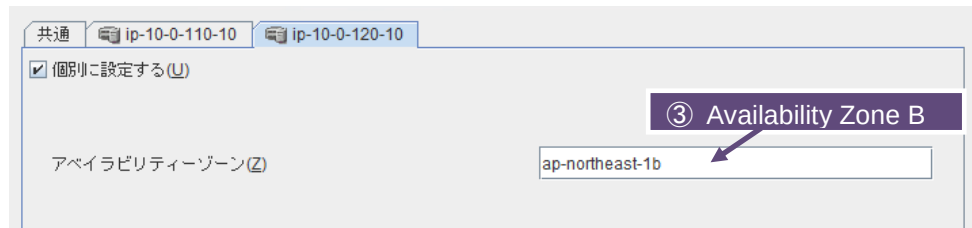


共通 ip-10-0-110-10 ip-10-0-120-10

☒ 個別に設定する(U)

② Availability Zone A

アベイラビリティゾーン(Z) ap-northeast-1a



共通 ip-10-0-110-10 ip-10-0-120-10

☒ 個別に設定する(U)

③ Availability Zone B

アベイラビリティゾーン(Z) ap-northeast-1b

7. [次へ] をクリックします。

8. 回復動作設定のページが表示されます。
[回復対象] に [LocalServer] を設定します。

回復動作(E) カスタム設定

回復対象 LocalServer 参照(W)

回復スクリプト実行回数(Y) 0 回

☐ 再活性前にスクリプトを実行する(U)

最大再活性回数(R) 0 回

☐ フェイルオーバー実行前にスクリプトを実行する(Q)

☐ フェイルオーバー実行前にマイグレーションを実行する(C)

最大フェイルオーバー回数(I) 0 回

☐ 最終動作前にスクリプトを実行する(X)

最終動作(E) 何もしない

9. [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』の「第 5 章 モニタリソースの詳細」-「AWS DNS モニタリソースを理解する」を参照してください。

◇ IP モニタリソース

各アベイラビリティゾーンに配置されている NAT 用のインスタンスに ping することで、サブネットの健全性を監視する IP モニタリソースを作成します。以下を指定してください。

【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 (ip monitor) を選択し、[名前] ボックスにモニタリソース名 (ipw1) を入力します。

モニタリソース定義

タイプ(I) ip monitor

名前(M) ipw1

コメント(C)

ライセンス情報取得(L)

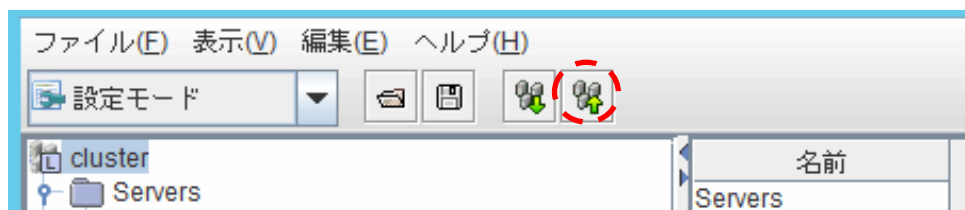
3. [次へ] をクリックします。
4. 監視(共通)設定のページが表示されます。
[監視タイミグ] が [常時] であることを確認し、[次へ] をクリックします。
5. 監視(固有)設定のページが表示されます。
[共通] タブの [IP アドレス一覧] に、現用系側のインスタンスの属するアベイラビリティゾーンに配置された NAT 用のインスタンスの Private IP アドレスを入力します。

6. [次へ] をクリックします。
7. 回復動作設定のページが表示されます。
[回復対象] に [LocalServer] を設定します。
[最終動作] に [クラスタサービス停止と OS シャットダウン] を設定します。

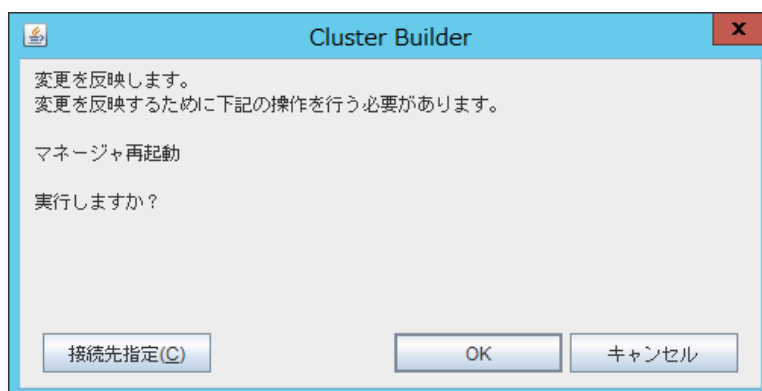
8. [完了] をクリックして設定を終了します。

4) 設定の反映とクラスタの起動

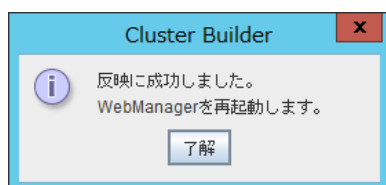
設定がすべて完了したら、メニュー下の [設定の反映] アイコンをクリックします。



マネージャ再起動の確認ダイアログが表示されます。

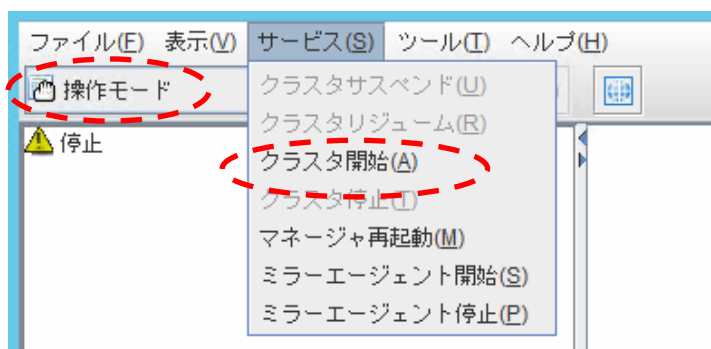


[OK] をクリックします。



[了解] をクリックします。

モードを [操作モード] に切り替え、メニュー [サービス] - [クラスタ開始] をクリックします。



第 7 章 IAM の設定

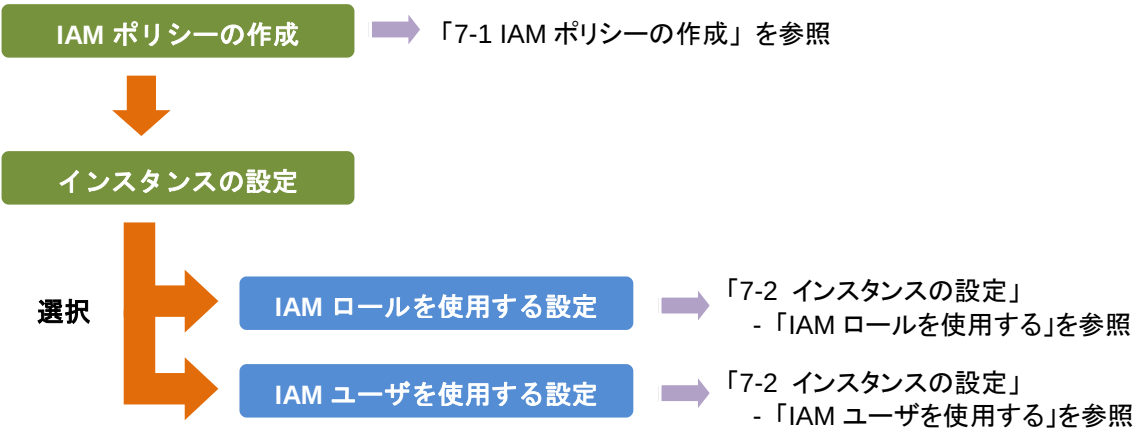
本章では、AWS 環境における IAM（Identity & Access Management）の設定について説明します。
AWS 仮想 IP リソース などのリソースおよびモニタリソースは、その処理のために AWS CLI を内部で実行します。AWS CLI が正常に実行されるためには、事前に IAM の設定が必要となります。

AWS CLI にアクセス許可を与える方法として、IAM ロールを使用する方針と、IAM ユーザを使用する方針の2通りがあります。基本的には各インスタンスに AWS アクセスキーID、AWS シークレットアクセスキーを保存する必要がなくセキュリティ上安全であることから、前者の IAM ロールを使用する方針を推奨します。

それぞれの方針のメリット・デメリットは以下のとおりです。

	メリット	デメリット
IAM ロールを使用する方針	セキュリティ上安全 キー情報の管理が簡単	IAM ロールを変更できないため、 後からインスタンス別のアクセス 権限設定ができない。
IAM ユーザを使用する方針	後からインスタンス別のアクセ ス権限設定が可能	キー情報漏えいのリスクが高い キー情報の管理が煩雑

IAM の設定手順は次の通りです。



7-1. IAM ポリシーの作成

AWS の EC2 や S3 などのサービスへのアクションに対するアクセス許可を記述したポリシーを作成します。CLUSTERPRO の AWS 関連リソースおよびモニタリソースが AWS CLI を実行するために許可が必要なアクションは以下のとおりです。

必要なポリシーは将来変更される可能性があります。

◇ AWS 仮想 IP リソース/AWS 仮想 IP モニタリソース

アクション	説明
ec2:Describe*	VPC、ルートテーブル、ネットワークインタフェースの情報を取得する時に必要です。
ec2:ReplaceRoute	ルートテーブルを更新する時に必要です。

◇ AWS Elastic IP リソース/AWS Elastic IP モニタリソース

アクション	説明
ec2:Describe*	EIP、ネットワークインタフェースの情報を取得する時に必要です。
ec2:AssociateAddress	EIP を ENI に割り当てる際に必要です。
ec2:DisassociateAddress	EIP を ENI から切り離す際に必要です。

◇ AWS DNS リソース/AWS DNS モニタリソース

アクション	説明
Route 53:ChangeResourceRecordSets	リソースレコードセット の追加、削除、設定内容の更新する時に必要です。
Route 53:ListResourceRecordSets	リソースレコードセット 情報の取得をする時に必要です。

◇ AWS AZ モニタリソース

アクション	説明
ec2:Describe*	アベイラビリティゾーンの情報を取得する時に必要です。

以下のカスタムポリシーの例ではすべての AWS 関連リソースおよびモニタリソースが使用するアクションを許可しています。

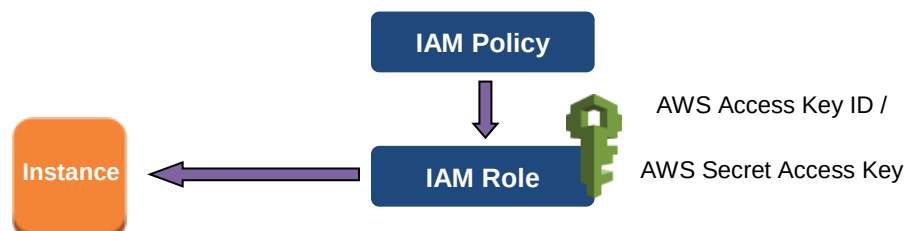
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:Describe*",
        "ec2:ReplaceRoute",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "route53:ChangeResourceRecordSets",
        "route53:ListResourceRecordSets"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

⇒ IAM Management Console の [Policies] - [Create Policy] で カスタムポリシーを作成できます。

7-2. インスタンスの設定

IAM ロールを使用する

IAM ロールを作成し、インスタンスに付与することで AWS CLI を実行可能にする方法です。



- 1) IAM ロールを作成します。作成したロールに IAM ポリシーをアタッチします。

⇒ IAM Management Console の [Roles] - [Create New Role] で IAM ロールを作成できます。

- 2) インスタンス作成時に、「IAM Role」に作成した IAM ロールを指定します。
(インスタンス作成完了後に IAM ロールを後から付与することはできません)

- 3) インスタンスにログインします。

- 4) Python をインストールします。

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。

/sbin、/bin、/usr/sbin、/usr/bin

- 5) シェルから pip コマンドを実行し、AWS CLI をインストールします。

```
$ pip install awscli
```

pip コマンドに関する詳細は下記を参照してください。

<https://pip.pypa.io/en/latest/>

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。

<http://docs.aws.amazon.com/cli/latest/userguide/installing.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。)

- 6) シェルから、以下のコマンドを実行します。

```
$ sudo aws configure
```

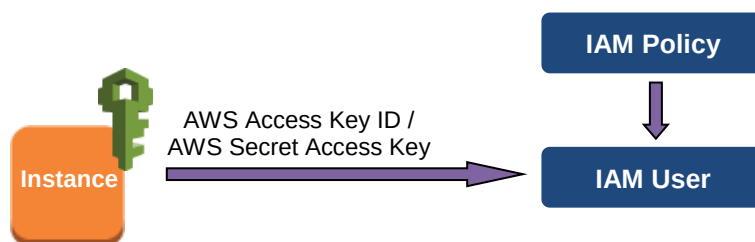
質問に対して AWS CLI の実行に必要な情報を入力します。AWS アクセスキーID、AWS シークレットアクセスキーは入力しないことに注意してください。

```
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
```

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。

IAM ユーザを使用する

IAM ユーザを作成し、そのアクセスキーID、シークレットアクセスキーをインスタンス内に保存することで AWS CLI を実行可能にする方法です。インスタンス作成時の IAM ロールの付与は不要です。



- 1) IAM ユーザを作成します。作成したユーザに IAM ポリシーをアタッチします。

⇒ IAM Management Console の [Users] - [Create New Users] で IAM ユーザを作成できます。

- 2) インスタンスにログインします。

- 3) Python をインストールします。

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。

/sbin、/bin、/usr/sbin、/usr/bin

- 4) シェルから pip コマンドを実行し、AWS CLI をインストールします。

```
$ pip install awscli
```

pip コマンドに関する詳細は下記を参照してください。

<https://pip.pypa.io/en/latest/>

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

(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) 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 CLI の実行に必要な情報を入力します。AWS アクセスキーID、AWS シークレットアクセスキーは作成した IAM ユーザの詳細情報画面から取得したものを入力します。

```
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
```

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。

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。

WebManager のメッセージ	Activating awsvip1 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	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

WebManager のメッセージ	Activating awsvip1 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 ・指定した VPC ID、または、ENI ID が不正
対処方法	AWS CLI が正常に動作することを確認します。 上記設定を正しい内容に修正します。

WebManager のメッセージ	Activating awsvip1 resource has failed.(5 : The vpc ID 'vpc-xxxxxxx' 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。

WebManager のメッセージ	Activating <i>awsvip1</i> resource has failed.(5 : The networkInterface ID 'eni-xxxxxxx' 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。

WebManager のメッセージ	Activating <i>awsvip1</i> resource has failed.(6 : Timeout occurred.)
考えられる原因	AWS CLI コマンドが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。
対処方法	以下を確認します。 ・NAT 用のインスタンスが起動していること ・NAT 用のインスタンス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。

WebManager のメッセージ	Activating <i>awsvip1</i> resource has failed.(7 : The VIP address <i>vvv.www.xxx.yyy</i> 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。

WebManager 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。

WebManager のメッセージ	Detected an error in monitoring <i>awsvipw1</i> . (8 : The routing for VIP <i>vvv.www.xxx.yyy</i> 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。

WebManager のメッセージ	Activating <i>awseip1</i> resource has failed.(99 : Internal error. (status= <i>nn</i>))
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	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

	認めます。 /sbin、/bin、/usr/sbin、/usr/bin、/usr/local/bin
--	--

WebManager のメッセージ	Activating <i>awseip1</i> 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 ・指定した EIP Allocation ID、または、ENI ID が不正
対処方法	AWS CLI が正常に動作することを確認します。 上記設定を正しい内容に修正します。

WebManager のメッセージ	Activating <i>awseip1</i> resource has failed.(5 : The allocation ID 'eipalloc-xxxxxxx' 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。

WebManager のメッセージ	Activating <i>awseip1</i> resource has failed.(5 : The networkInterface ID 'eni-xxxxxxx' 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。

WebManager のメッセージ	Activating <i>awseip1</i> resource has failed.(6 : Timeout occurred.)
考えられる原因	AWS CLI コマンドが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。
対処方法	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。

◆ AWS Elastic IP モニタリソースが異常になる。

WebManager のメッセージ	Detected an error in monitoring <i>awseipw1</i> . (7 : The EIP address does not exist. (EIP ALLOCATION ID= <i>eipalloc-xxxxxxx</i>))
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。

WebManager のメッセージ	Activating <i>awsdns1</i> resource has failed.(99 : Internal error. (status= <i>nn</i>))
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	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

WebManager のメッセージ	Activating <i>awsdns1</i> 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 ・指定したリソースレコードセットが不正
対処方法	AWS CLI が正常に動作することを確認します。 上記設定を正しい内容に修正します。

WebManager のメッセージ	Activating <i>awsdns1</i> 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。

WebManager のメッセージ	Activating <i>awsdns1</i> resource has failed.(6 : Timeout occurred.)
考えられる原因	AWS CLI コマンドが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。
対処方法	以下を確認します。 ・NAT 用のインスタンスが起動していること ・NAT 用のインスタンス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。

◆ AWS DNS モニタリソースが異常になる。

WebManager のメッセージ	Detected an error in monitoring <i>awsdns1</i> . (7 : The resource record set in Amazon Route 53 does not exist.)
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

	レコードセットがなんらかの理由で削除されている。
対処方法	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かなどを確認します。

WebManager のメッセージ	Detected an error in monitoring <i>awsdns1</i> . (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。

WebManager のメッセージ	Detected an error in monitoring <i>awsdns1</i> . (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

WebManager のメッセージ	Detected an error in monitoring <i>awsdns1</i> . (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 AZ モニタリソースが警告または異常になる。

WebManager のメッセージ	[警告時] Warn monitoring <i>awsazw1</i> . (105 : Failed in the AWS CLI command.) [異常時] Detected an error in monitoring <i>awsazw1</i> . (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(<i>aws configure</i> 未実行) ・AWS CLI 設定が見つからない(<i>aws configure</i> を root 以外のユーザ、または、<i>sudo</i> 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)、 <i>config</i> 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

	・指定した アベイラビリティゾーンが不正
対処方法	AWS CLI が正常に動作することを確認します。 上記設定を正しい内容に修正します。

WebManager 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ゾーンを指定します。

WebManager 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	AWS CLI コマンドがルートテーブルや NAT の設定ミス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。
対処方法	以下を確認します。 ・NAT 用のインスタンスが起動していること ・NAT 用のインスタンス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。