

高信頼化システム監視機能 HA モニタ パブリッククラ  
ウド編

3000-9-204-70

## 前書き

### ■ 著作権

All Rights Reserved. Copyright (C) 2019, 2023, Hitachi, Ltd.

### ■ 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

### ■ 商標類

HITACHI, BladeSymphony, Cosminexus, HA モニタ, HiRDB, JP1, OpenTP1, uCosminexus は、株式会社 日立製作所の商標または登録商標です。

Amazon Web Services, AWS, Powered by AWS ロゴ, Amazon EC2, Amazon Route 53 は、Amazon.com, Inc. またはその関連会社の商標です。

AMD は、Advanced Micro Devices, Inc.の商標です。

Azure は、マイクロソフト 企業グループの商標です。

Intel は、Intel Corporation またはその子会社の商標です。

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。

Microsoft は、マイクロソフト 企業グループの商標です。

Oracle および Java は、オラクルおよびその関連会社の登録商標です。

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat は、米国およびその他の国における Red Hat, Inc.の登録商標です。

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat Enterprise Linux は、米国およびその他の国における Red Hat, Inc.の登録商標です。

RHEL is a trademark or a registered trademark of Red Hat, Inc. in the United States and other countries.

RHEL は、米国およびその他の国における Red Hat, Inc.の商標または登録商標です。

UNIX は、The Open Group の登録商標です。

その他記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。

### ■ 発行

2023 年 4 月 3000-9-204-70

## 変更内容

### 変更内容 (3000-9-204-70) HA モニタ 01-78

| 追加・変更内容                                | 変更箇所  |
|--|---|
| AWS 環境の場合に、EFS を使用した共有ディスク構成にできるようにした。 | 1.3.1, 1.3.1(1), 1.3.1(2), 2.1.1(2), 2.3, 5.2.1, 5.2.7, 5.7, 5.12.3, 7.2.2, 7.3.2, 8.1.1, 付録 A. |
| 適用 OS に RHEL9 を追加した。                   | —   |

単なる誤字・脱字などはお断りなく訂正しました。

## はじめに

このマニュアルは、パブリッククラウド環境下での HA モニタの機能、設定、および運用方法について説明したものです。このマニュアルを読むことで、ユーザが HA モニタを使用して系切り替え構成を設計・構築できること、および適切に運用できることを目的としています。

このマニュアルとあわせて、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』も参照してください。

### ■ 対象製品

#### ●P-872C-E111 HA モニタ 01-78

適用 OS : Red Hat(R) Enterprise Linux(R) Server 7(x86\_64), Red Hat(R) Enterprise Linux(R) Server 8(x86\_64), Red Hat(R) Enterprise Linux(R) Server 9(64-bit x86\_64), Oracle Linux 7(x86\_64)\*, Oracle Linux 8(x86\_64)\*

#### ●P-9S2C-E211 HA モニタ Extension 01-00

適用 OS : Red Hat(R) Enterprise Linux(R) AS 3(x86), Red Hat(R) Enterprise Linux(R) AS 4(x86), Red Hat(R) Enterprise Linux(R) ES 3(x86), Red Hat(R) Enterprise Linux(R) ES 4(x86), Red Hat(R) Enterprise Linux(R) AS 3(AMD64 & Intel EM64T), Red Hat(R) Enterprise Linux(R) AS 4(AMD64 & Intel EM64T), Red Hat(R) Enterprise Linux(R) ES 4(AMD64 & Intel EM64T), Red Hat(R) Enterprise Linux(R) 5(x86), Red Hat(R) Enterprise Linux(R) 5(AMD/Intel 64), Red Hat(R) Enterprise Linux(R) 5 Advanced Platform(x86), Red Hat(R) Enterprise Linux(R) 5 Advanced Platform(AMD/Intel 64)

これらのプログラムプロダクトのほかにもこのマニュアルをご利用になれる場合があります。詳細は「リリースノート」でご確認ください。

#### 注※

OCI 環境の場合だけサポートします。

### ■ 対象読者

システム管理者、オペレータ、およびプログラマの方を対象としています。システム管理者は、システムの導入、設計、構築をすることを想定しています。オペレータは、構築されたシステムで日々の運用をすることを想定しています。プログラマは、ユーザプログラムの作成をすることを想定しています。

また、次の知識をお持ちの方を前提としています。

- 該当する OS の知識

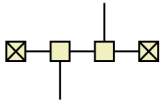
- AWS (Amazon Web Services), Azure (Microsoft Azure), または OCI (Oracle Cloud Infrastructure) の知識
- DRBD の知識
- 系切り替え構成にするプログラムの知識
- ユーザプログラムのコーディングに使用する C 言語の文法の知識

系切り替え構成にするプログラムとして、OpenTP1 または HiRDB を使用する場合は、あらかじめ OpenTP1 または HiRDB のマニュアルをお読みいただくことをお勧めします。

## ■ このマニュアルで使用する図中の記号

このマニュアルの図中で使用している記号を、次のように定義します。

●バス型のLAN



●現用系・実行系のプログラム



●予備系・待機系のプログラム



# 目次

|      |   |
|------|---|
| 前書き  | 2 |
| 変更内容 | 3 |
| はじめに | 4 |

|          |                                |           |
|----------|--------------------------------|-----------|
| <b>1</b> | <b>パブリッククラウド環境下の HA モニタの概要</b> | <b>10</b> |
| 1.1      | このマニュアルの読み方                    | 11        |
| 1.2      | パブリッククラウド環境下の HA モニタ           | 13        |
| 1.2.1    | HA モニタが検出する障害                  | 13        |
| 1.2.2    | 系切り替えの方式                       | 13        |
| 1.3      | HA モニタの動作環境                    | 14        |
| 1.3.1    | 【AWS】必要な環境                     | 14        |
| 1.3.2    | 【Azure】必要な環境                   | 18        |
| 1.3.3    | 【OCI】必要な環境                     | 23        |
| 1.3.4    | 必要なソフトウェア                      | 25        |
| <b>2</b> | <b>HA モニタを使用した系切り替え</b>        | <b>26</b> |
| 2.1      | 障害検出から系切り替えまでの流れ               | 27        |
| 2.1.1    | 【AWS】系障害時の系切り替え                | 27        |
| 2.1.2    | 【Azure】系障害時の系切り替え              | 34        |
| 2.1.3    | 【OCI】系障害時の系切り替え                | 36        |
| 2.2      | HA モニタによる障害検出                  | 39        |
| 2.2.1    | HA モニタが系切り替えをする条件              | 39        |
| 2.2.2    | 系障害の検出                         | 39        |
| 2.3      | 【AWS】リソースの引き継ぎ                 | 41        |
| 2.4      | 【Azure】リソースの引き継ぎ               | 42        |
| 2.5      | 【OCI】リソースの引き継ぎ                 | 43        |
| <b>3</b> | <b>HA モニタで使用できる機能</b>          | <b>44</b> |
| 3.1      | HA モニタで使用できる機能一覧               | 45        |
| <b>4</b> | <b>システムの管理</b>                 | <b>47</b> |
| 4.1      | 系の管理                           | 48        |
| 4.1.1    | 系のリセットまたはネットワーク遮断をする系の決定方法     | 48        |
| 4.1.2    | 両系が障害を同時に検出した場合の系切り替え          | 48        |
| 4.1.3    | 複数の待機系がある場合の系のリセットまたはネットワーク遮断  | 48        |

|          |   |           |
|----------|---|-----------|
| 4.2      | リソースの管理   | 50        |
| 4.2.1    | 業務ディスクの管理                                       | 50        |
| 4.2.2    | 【AWS】 LAN の管理                                   | 52        |
| 4.2.3    | 【Azure】 LAN の管理                                 | 76        |
| 4.2.4    | 【OCI】 LAN の管理                                   | 84        |
| 4.3      | 【AWS】 処理の流れ                                     | 87        |
| 4.4      | 【Azure】 処理の流れ                                   | 88        |
| 4.5      | 【OCI】 処理の流れ                                     | 89        |
| <b>5</b> | <b>システムの構築</b>                                  | <b>90</b> |
| 5.1      | 構築の流れ   | 91        |
| 5.1.1    | 系のリセットまたはネットワーク遮断をする場合                          | 91        |
| 5.2      | 【AWS】 AWS の設定                                   | 92        |
| 5.2.1    | AWS CLI のインストール・設定                              | 92        |
| 5.2.2    | エンドポイントの設定                                      | 93        |
| 5.2.3    | インスタンスのメタデータ取得のための設定                            | 93        |
| 5.2.4    | プロキシを使用する場合の設定                                  | 93        |
| 5.2.5    | ENI の設定   | 94        |
| 5.2.6    | EBS マルチアタッチの設定                                  | 94        |
| 5.2.7    | EFS の設定   | 94        |
| 5.3      | 【Azure】 Azure の設定                               | 96        |
| 5.3.1    | Azure CLI のインストール・設定                            | 96        |
| 5.3.2    | インスタンスのメタデータ取得のための設定                            | 97        |
| 5.3.3    | プロキシを使用する場合の設定                                  | 97        |
| 5.3.4    | Azure ロードバランサーの作成・設定                            | 98        |
| 5.3.5    | Azure DNS の設定                                   | 99        |
| 5.3.6    | マネージドディスクの共有                                    | 99        |
| 5.4      | 【OCI】 OCI の設定                                   | 100       |
| 5.4.1    | OCI CLI のインストール・設定                              | 100       |
| 5.4.2    | インスタンスのメタデータ取得のための設定                            | 100       |
| 5.4.3    | プロキシを使用する場合の設定                                  | 100       |
| 5.4.4    | エンドポイントの設定                                      | 101       |
| 5.4.5    | ブロック・ボリュームの設定                                   | 101       |
| 5.4.6    | /etc/hosts ファイルの永続化                             | 101       |
| 5.5      | 【AWS】 【Azure】 レプリケーションソフト (DRBD) の設定            | 102       |
| 5.6      | 【AWS】 【Azure】 レプリケーションソフト (DRBD) 用のシェルスクリプト群の展開 | 105       |
| 5.7      | 【AWS】 AWS 用のシェルスクリプト群の展開                        | 106       |
| 5.8      | 【Azure】 Azure 用のシェルスクリプト群の展開                    | 108       |
| 5.9      | 【OCI】 OCI 用のシェルスクリプト群の展開                        | 110       |

- 5.10 リセットパスの設定 111
- 5.11 監視パスの設定 112
- 5.12 定義ファイルの作成 (HA モニタ) 113
  - 5.12.1 HA モニタの環境設定 113
  - 5.12.2 【Azure】 サービスプリンシパル情報設定ファイルの設定 113
  - 5.12.3 【AWS】 ネットワーク遮断設定ファイルの設定 114
- 5.13 サーバが使用するリソースの設定 115
  - 5.13.1 業務ディスクの設定 115
  - 5.13.2 【AWS】 LAN の状態設定ファイルの設定 (1 つのリージョン内または 1 つの VPC 内で系切り替えをする構成の場合) 115
  - 5.13.3 【AWS】 LAN の状態設定ファイルの設定 (複数のリージョン間または複数の VPC 間で系切り替えをする構成の場合) 121
  - 5.13.4 【AWS】 LAN の状態設定ファイルの設定 (クライアントからの通信が NLB を経由する構成の場合) 140
  - 5.13.5 【Azure】 LAN の状態設定ファイルの設定 140
  - 5.13.6 【OCI】 LAN の状態設定ファイルの設定 144
- 5.14 リソースの監視のための設定 147
  - 5.14.1 LAN の監視に必要なファイルの設定 147

## 6 システムの運用 150

- 6.1 起動・停止 151
- 6.2 システムの変更 152
  - 6.2.1 サーバを追加する 152
  - 6.2.2 系やサーバを稼働させたままリソースの構成を変更する 152
- 6.3 システム運用時の注意事項 153
  - 6.3.1 パブリッククラウド環境のコンソール操作 (CLI 発行含む) をする場合の注意事項 153
  - 6.3.2 【AWS】 【Azure】 レプリケーションソフトを使用する場合の注意事項 153

## 7 環境設定で定義するファイル 155

- 7.1 定義ファイルの概要 156
- 7.2 HA モニタの環境設定 157
  - 7.2.1 パブリッククラウド環境固有の HA モニタの環境設定 157
  - 7.2.2 パブリッククラウド環境で注意が必要な HA モニタの環境設定のオペランド 158
- 7.3 サーバの環境設定 161
  - 7.3.1 パブリッククラウド環境固有のサーバの環境設定 161
  - 7.3.2 パブリッククラウド環境で注意が必要なサーバ対応の環境設定のオペランド 162
- 7.4 環境設定例 164
  - 7.4.1 【AWS】 HA モニタを使用する場合の構成 164
  - 7.4.2 【Azure】 HA モニタを使用する場合の構成 186
  - 7.4.3 【OCI】 HA モニタを使用する場合の構成 195



## 8 コマンド 201

- 8.1 パブリッククラウド環境で注意が必要なコマンド 202
- 8.1.1 moncheck (定義チェック) 202
- 8.1.2 monshow (サーバと系の状態表示) 203

## 付録 205

- 付録 A HA モニタが出力するファイル一覧 206
- 付録 B 各バージョンの変更内容 211
- 付録 B.1 HA モニタ 01-77 の変更内容 (3000-9-204-60) 211
- 付録 B.2 HA モニタ 01-76, HA モニタ 01-75 の変更内容 (3000-9-204-50) 211
- 付録 B.3 HA モニタ 01-74 の変更内容 (3000-9-204-40) 211
- 付録 B.4 HA モニタ 01-73 の変更内容 (3000-9-204-30) 212
- 付録 B.5 HA モニタ 01-72 の変更内容 (3000-9-204-20) 212
- 付録 B.6 HA モニタ 01-71 の変更内容 (3000-9-204-10) 212
- 付録 C このマニュアルの参考情報 213
- 付録 C.1 関連マニュアル 213
- 付録 C.2 このマニュアルで使用する製品名・機能名 215
- 付録 C.3 このマニュアルで使用する英略語 217
- 付録 C.4 このマニュアルで使用する KB (キロバイト) などの単位表記 217

## 索引 218

# 1

## パブリッククラウド環境下の HA モニタの概要

この章では、パブリッククラウド環境下の HA モニタの概要、系切り替えの方式、動作環境について説明します。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタの概要」とあわせてお読みください。

## 1.1 このマニュアルの読み方

このマニュアルには、パブリッククラウド環境下の HA モニタとパブリッククラウド環境下でない HA モニタとで差異がある事項を記載しています。また、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』には共通する事項を記載しています。そのため、HA モニタを使用して系切り替え構成を設計・構築するには、このマニュアルとマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の両方を参照してください。

このマニュアルとマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の構成の対応表は次のとおりです。

表 1-1 このマニュアルとマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の構成の対応

| このマニュアル |                         | マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』 |                   |
|---------|-------------------------|---|-------------------|
| 章       | タイトル                    | 章   | タイトル              |
| 1       | パブリッククラウド環境下の HA モニタの概要 | 1   | HA モニタの概要         |
| 2       | HA モニタを使用した系切り替え        | 2   | HA モニタを使用した系切り替え  |
| 3       | HA モニタで使用できる機能          | 3   | HA モニタで使用できる機能    |
| 4       | システムの管理                 | 4   | システムの管理           |
| -       | -                       | 5   | HA モニタの導入とシステムの設計 |
| 5       | システムの構築                 | 6   | システムの構築           |
| 6       | システムの運用                 | 7   | システムの運用           |
| 7       | 環境設定で定義するファイル           | 8   | 環境設定で定義するファイル     |
| 8       | コマンド                    | 9   | コマンド              |
| -       | -                       | 10  | API               |

(凡例)

-：該当マニュアルに存在しない章です。

このマニュアルでは、使用するパブリッククラウドごとに読むトピックが異なります。次のとおりに、目次に記載されているトピックから、読むトピックを選択してください。

タイトルの先頭に「**【AWS】**」がある場合

AWS のトピックです。AWS を使用する方はお読みください。

タイトルの先頭に「**【Azure】**」がある場合

Azure のトピックです。Azure を使用する方はお読みください。

タイトルの先頭に「【OCI】」がある場合

OCI のトピックです。OCI を使用する方はお読みください。

タイトルの先頭に「【AWS】」「【Azure】」「【OCI】」のどれもない場合

AWS, Azure, OCI 共通のトピックです。使用するパブリッククラウドに関係なくお読みください。

## 1.2 パブリッククラウド環境下の HA モニタ

---

HA モニタは、システムの信頼性向上、稼働率向上を目的として、プログラムを含めたシステムの切り替えを実現します。このマニュアルでは、パブリッククラウド環境下で HA モニタを使用する場合の機能および設定方法について説明します。HA モニタの概要については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタの概要」の説明を参照してください。この節では、HA モニタの概要について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 1.2.1 HA モニタが検出する障害

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタが検出する障害」を参照してください。ただし、パブリッククラウド環境下では次の点が異なります。

- HA モニタが監視する範囲に、リセットパスはありません。
- 「系のハードウェア障害、または電源断」は「インスタンス障害」と読み替えてください。

### 1.2.2 系切り替えの方式

系切り替えの方式については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系切り替えの方式」の説明を参照してください。なお、パブリッククラウド環境下では、「系のリセットによる系切り替え」の方式で系切り替えを実施します。

## 1.3 HA モニタの動作環境

---

HA モニタを動作させるために必要なパブリッククラウド環境、およびソフトウェアについて説明します。

### 1.3.1 【AWS】 必要な環境

HA モニタを動作させるために必要な AWS 環境について説明します。

構成例では、各系に ENI を複数個配置していますが、各系に ENI を 1 個ずつ配置して、監視パス、業務 LAN、レプリケーションパスを集約する構成にもできます。

遮断対象となる ENI を少なくすることによって系切り替え時間を短縮できます。そのため、特に、ネットワーク遮断による系切り替えを使用する場合は、複数の業務 LAN の集約や、業務 LAN、レプリケーションパス、および EFS へのアクセス用パスの兼用を検討してください。ネットワーク遮断による系切り替えについては、「(2) ネットワーク遮断による系切り替え」を参照してください。

なお、レプリケーション構成の場合、監視パスとディスクレプリケーションパスは、分けることを推奨します。理由は、次のとおりです。

- HA モニタとレプリケーションソフトが相互に影響を及ぼさないようにするため。
- 運用を失敗した場合に、監視パスおよびディスクレプリケーションパスが同時に切断されないようにするため。

インスタンス、ENI、EBS、および EFS 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。

### (1) 1:1 系切り替え構成

構成例を次に示します。

図 1-1 AWS 環境構成例 (レプリケーション構成)

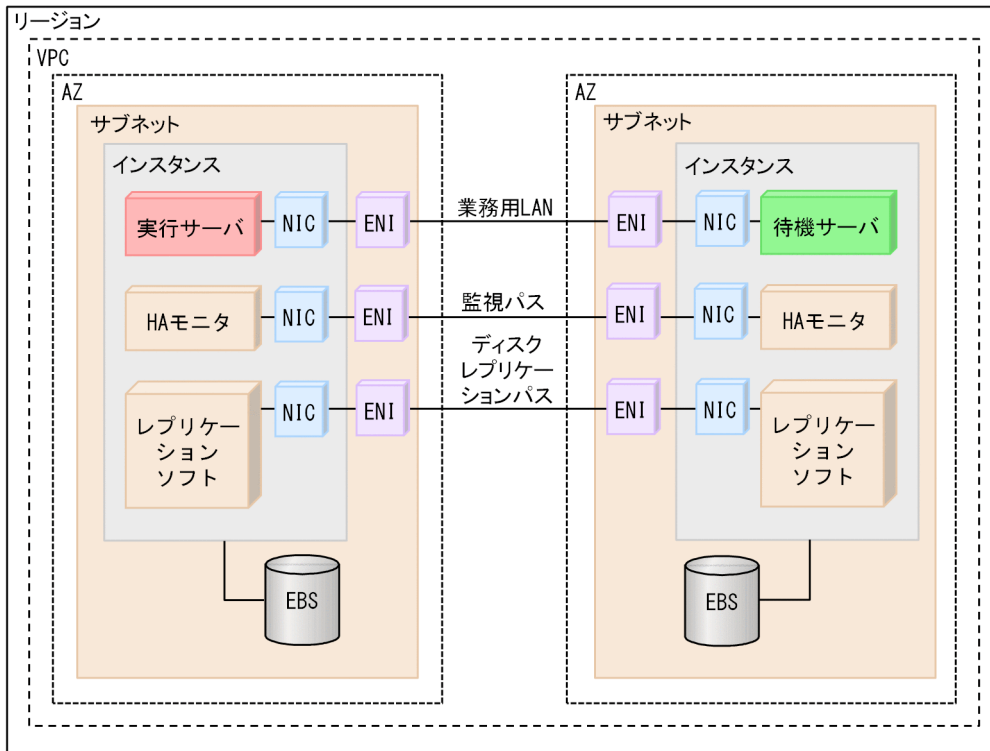


図 1-2 AWS 環境構成例 (EBS マルチアタッチによる共有ディスク構成)

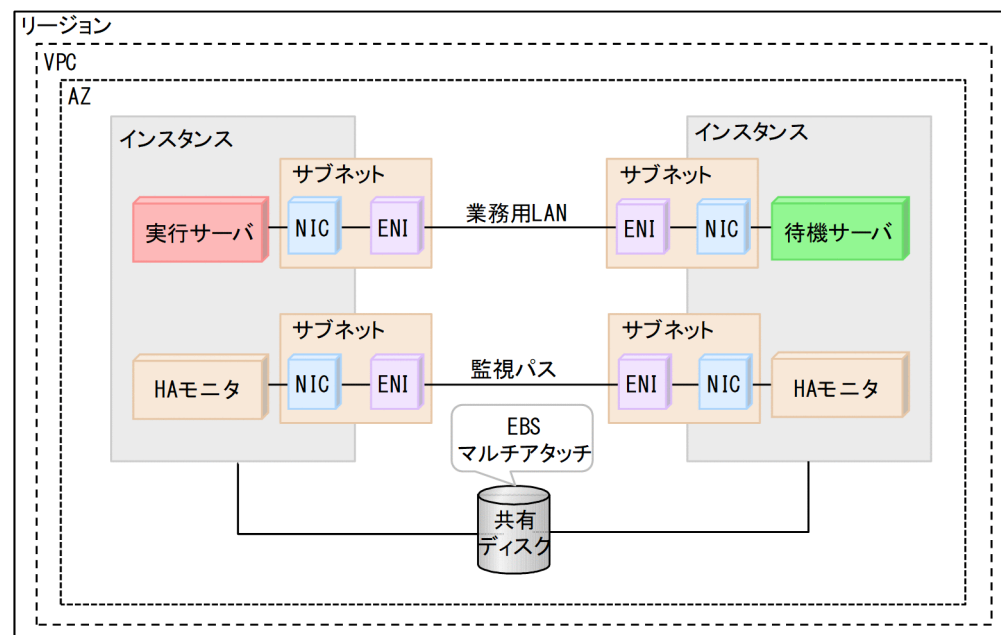
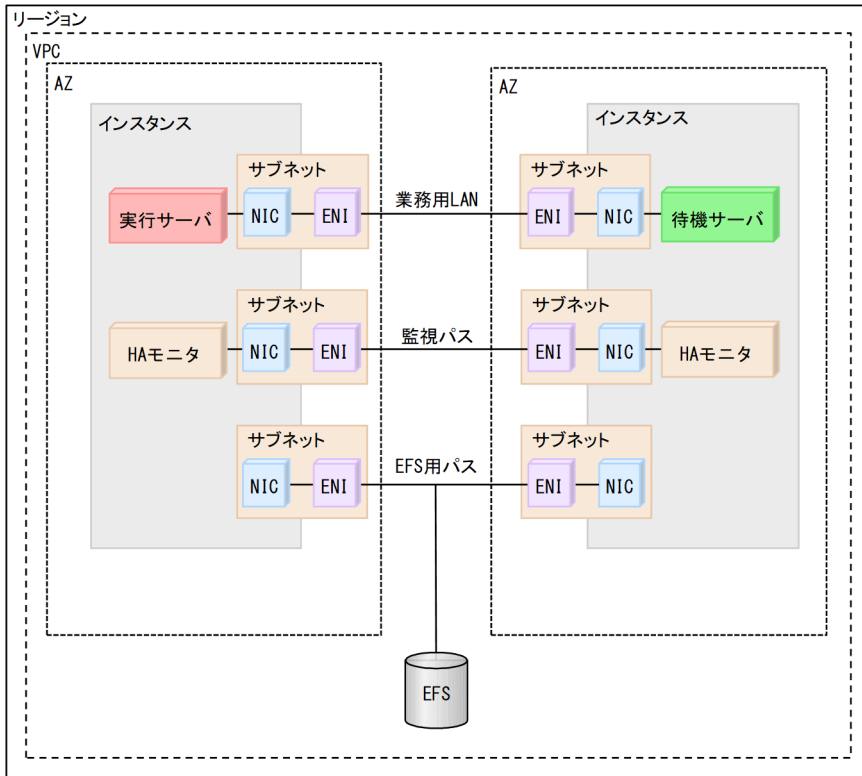


図 1-3 AWS 環境構成例 (EFS による共有ディスク構成)



注  
EFS による共有ディスク構成の場合、1 つの VPC 内でのクラスタ構成にしてください。

## (2) 複数スタンバイ構成

構成例を次に示します。



図 1-4 AWS 環境構成例 (レプリケーション構成)

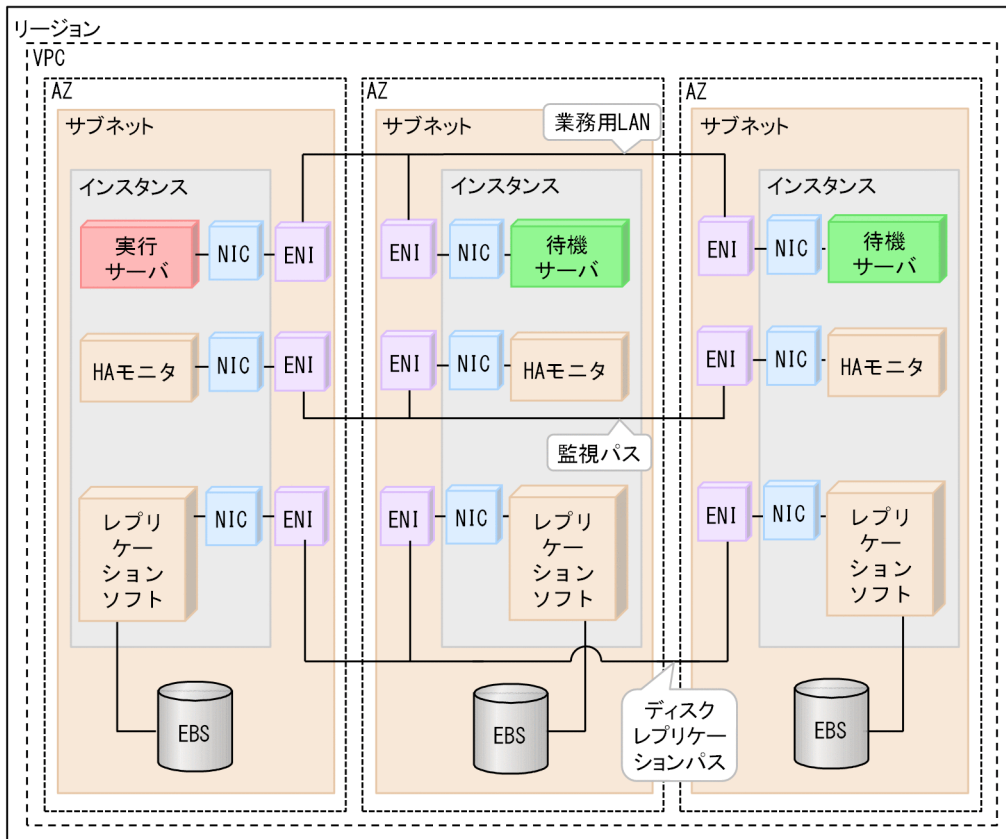


図 1-5 AWS 環境構成例 (EBS マルチアタッチによる共有ディスク構成)

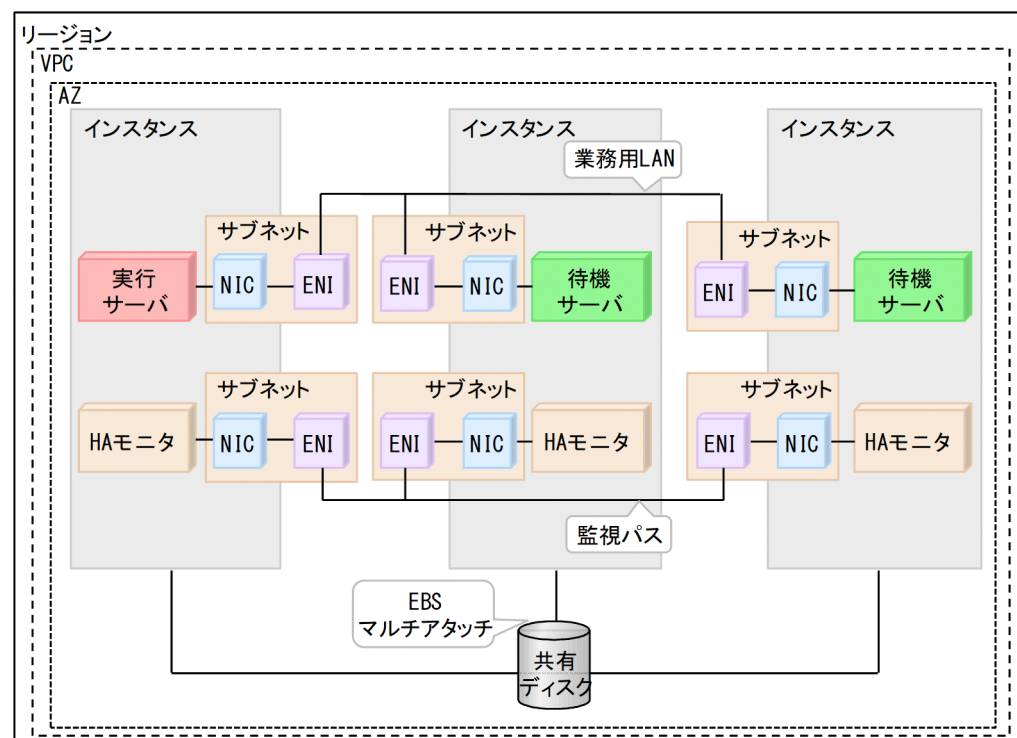
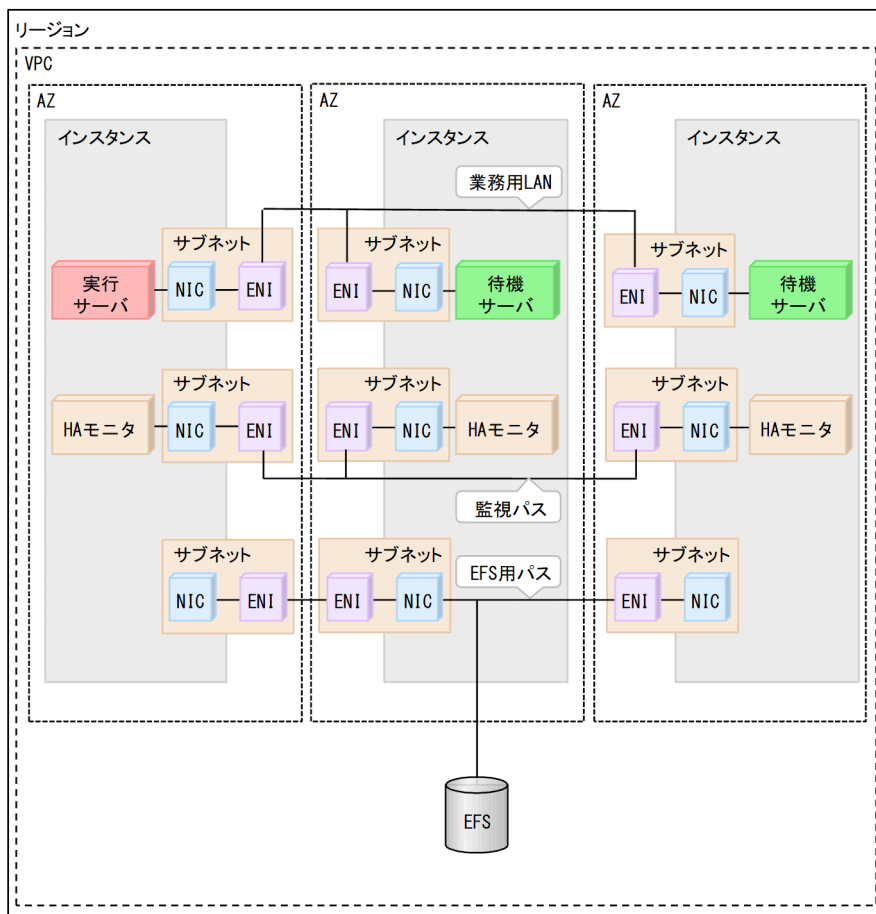


図 1-6 AWS 環境構成例 (EFS による共有ディスク構成)



注

EFS による共有ディスク構成の場合、1 つの VPC 内でのクラスタ構成にしてください。

### 1.3.2 【Azure】必要な環境

HA モニタを動作させるために必要な Azure 環境について説明します。

なお、このマニュアルでは、Azure リソースのネットワークインターフェイスを「仮想 NIC」と記載します。

構成例では、すべての Azure リソースを同じリソースグループ内に配置し、すべての仮想マシンを同じサブネット内に配置していますが、次の構成にもできます。

- Azure リソースを異なるリソースグループに分けて配置する構成
- 仮想マシンを異なるサブネットに分けて配置する構成

可用性ゾーン、可用性セット、Disk Storage、およびマネージドディスクの詳細については、Azure のドキュメントを参照してください。

# (1) 1:1 系切り替え構成

構成例を次に示します。

図 1-7 Azure 環境構成例 (レプリケーション構成で、異なる可用性ゾーンに仮想マシンを配置する場合)

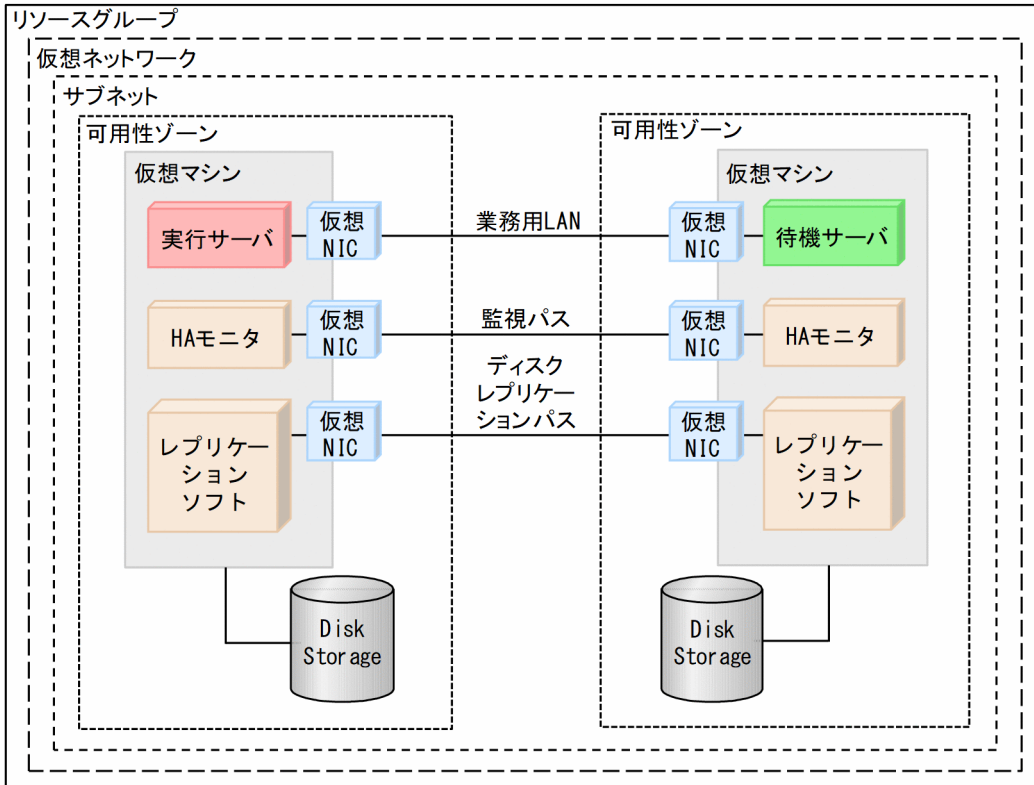


図 1-8 Azure 環境構成例（レプリケーション構成で、同じ可用性セット内に仮想マシンを配置する場合）

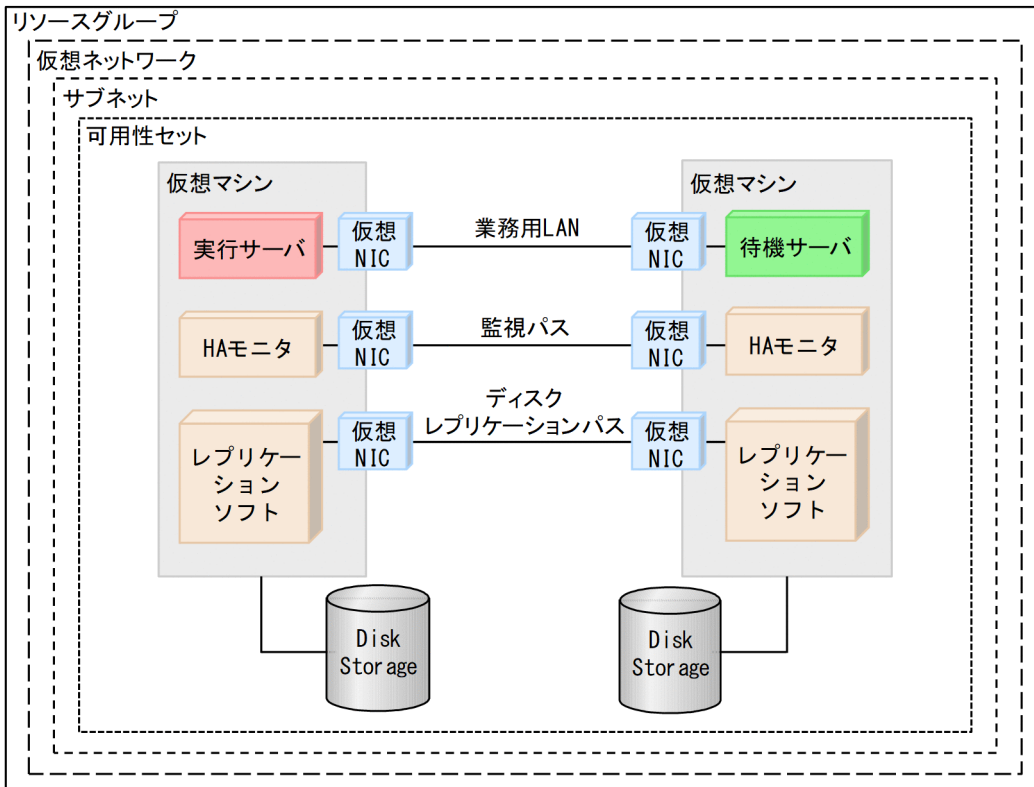


図 1-9 Azure 環境構成例（共有ディスク構成で、同じ可用性ゾーン内に仮想マシンを配置する場合）

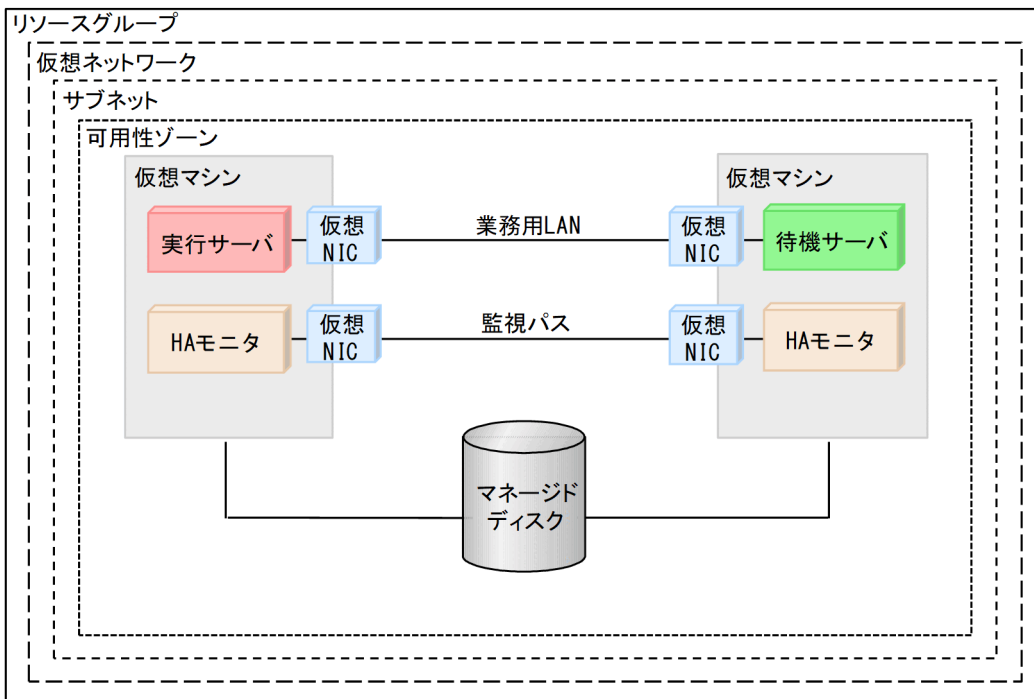
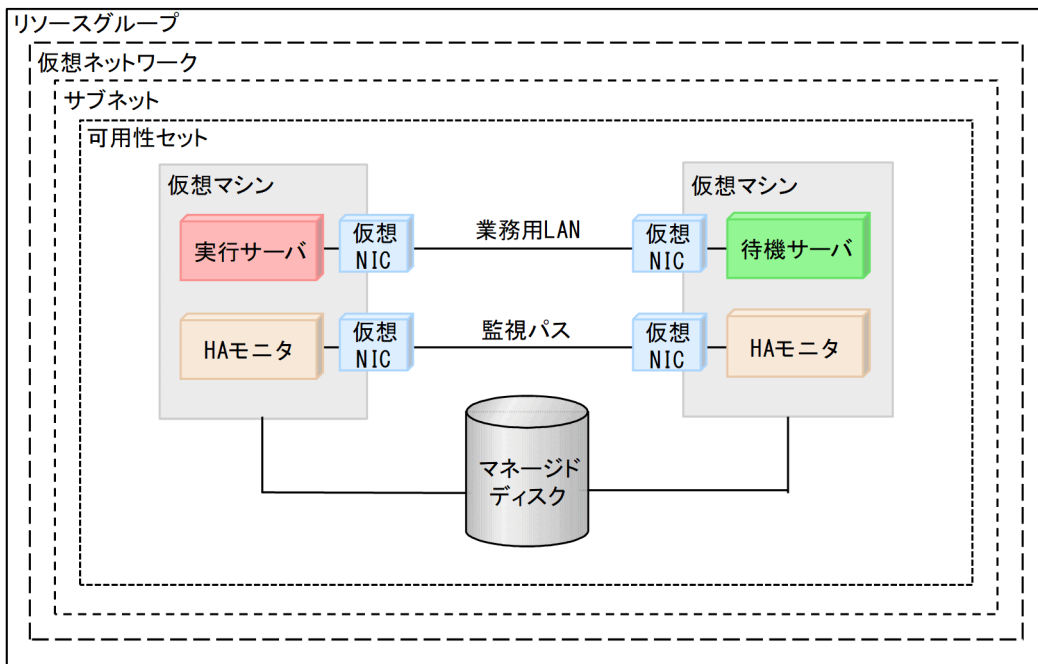


図 1-10 Azure 環境構成例（共有ディスク構成で、同じ可用性セット内に仮想マシンを配置する場合）



## (2) 複数スタンバイ構成

構成例を次に示します。

図 1-11 Azure 環境構成例（レプリケーション構成で、異なる可用性ゾーンに仮想マシンを配置する場合）

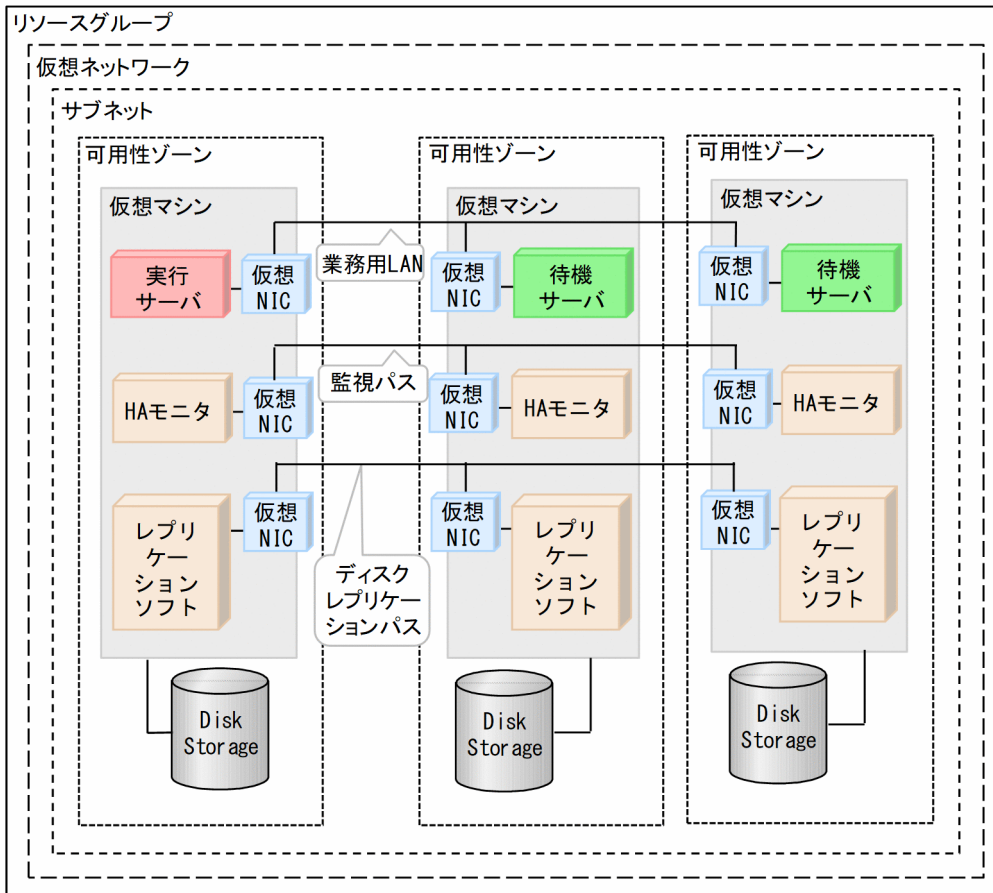
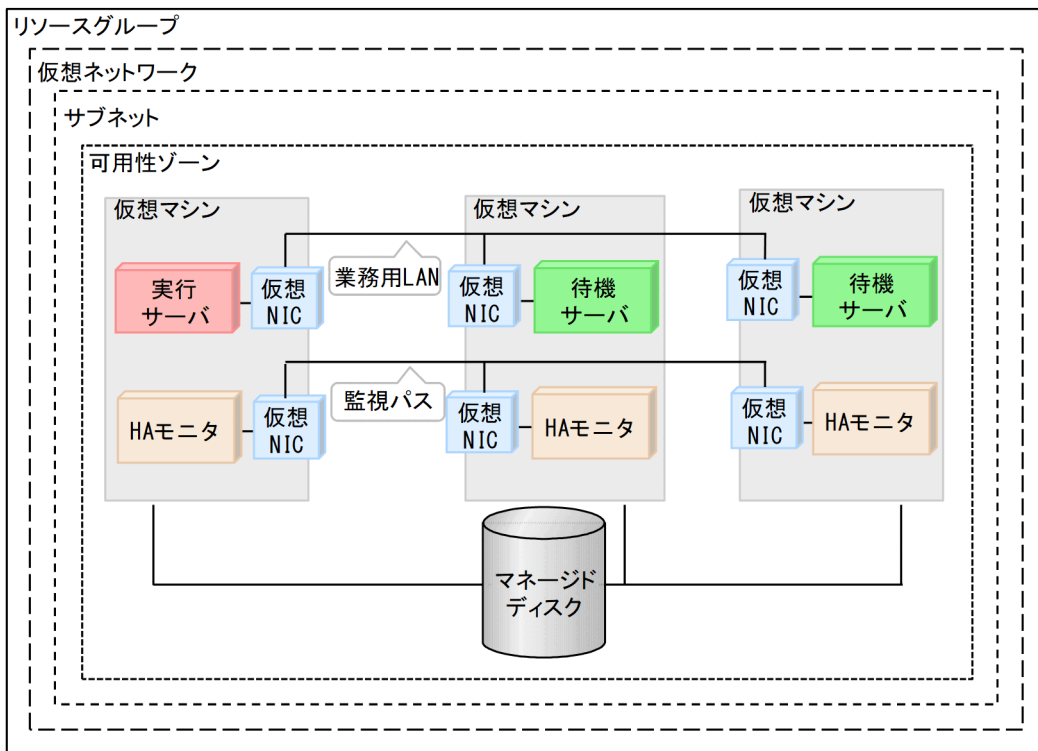


図 1-12 Azure 環境構成例（共有ディスク構成で、同じ可用性ゾーン内に仮想マシンを配置する場合）



### 1.3.3 【OCI】 必要な環境

HA モニタを動作させるために必要な OCI 環境について説明します。構成例を次に示します。

図 1-13 OCI 環境構成例 (1:1 系切り替え構成)

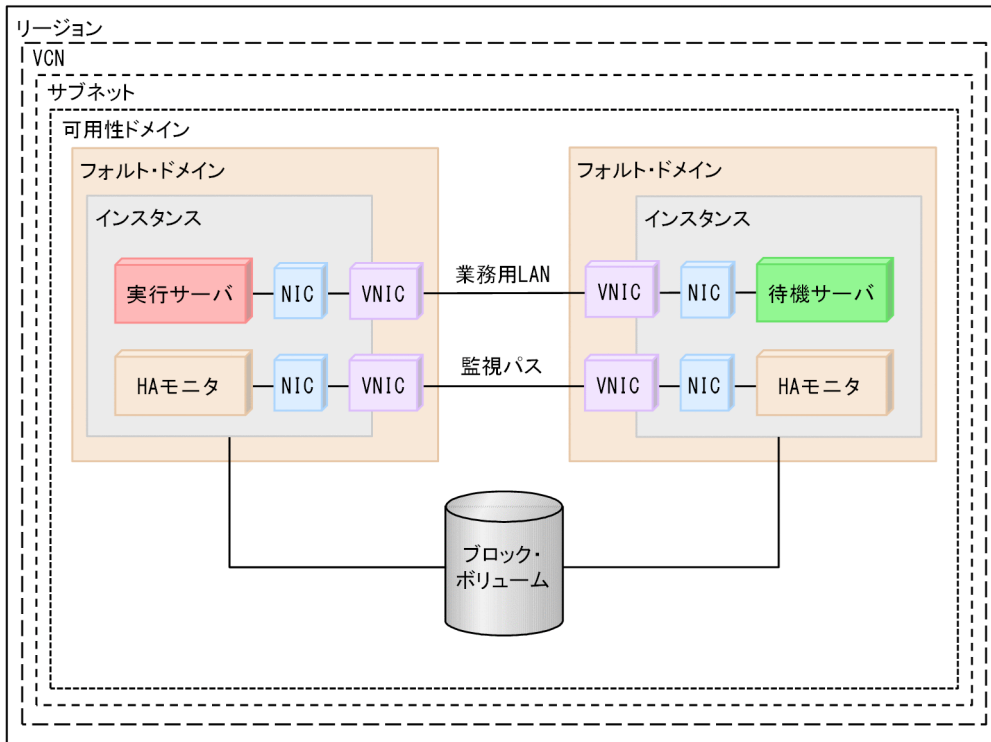
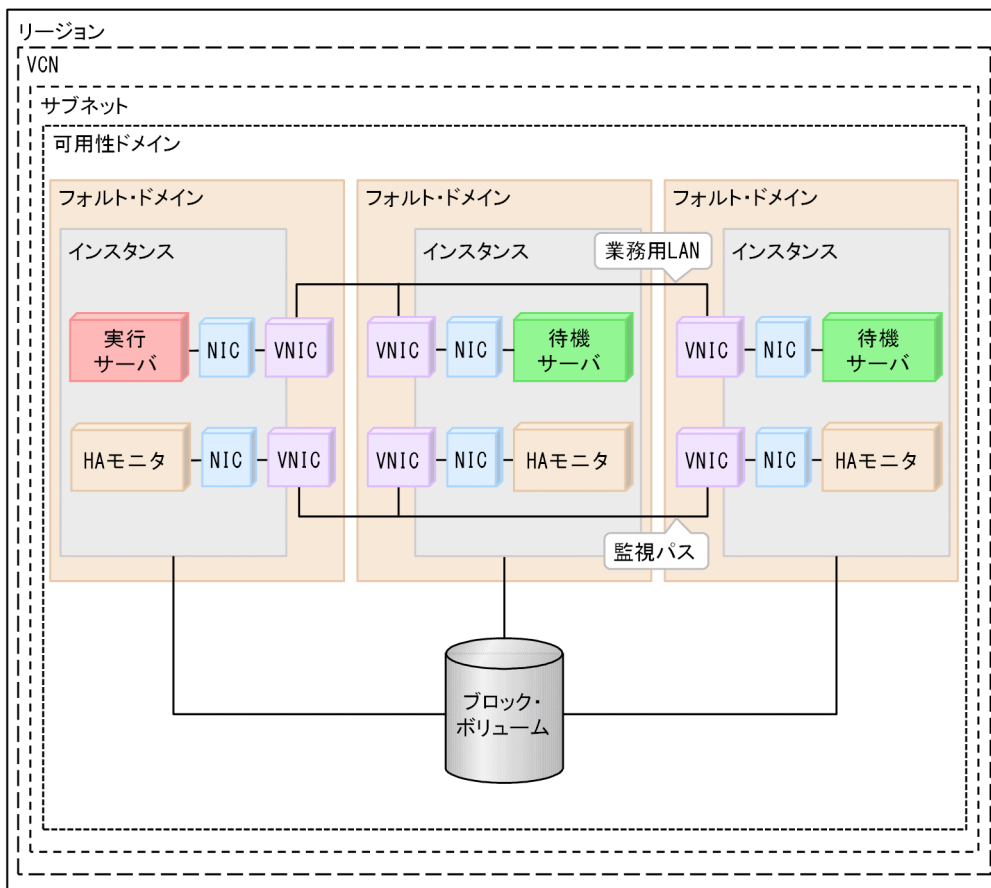


図 1-14 OCI 環境構成例 (複数スタンバイ構成)





1つの可用性ドメインにつき、フォルト・ドメインは3つあります。可用性の確保のため、系が3つ以下の場合は、すべての系を異なるフォルト・ドメインに配置してください。系が4つ以上の場合は、3つのフォルト・ドメインに最低1つずつ系を配置したあと、4つ目以降の系をフォルト・ドメインのどれかに配置してください。この場合、同じフォルト・ドメイン内に複数の系を配置することになります。

構成例では、すべてのインスタンスおよびVNICを同じサブネットに格納していますが、インスタンスおよび監視パスに用いるVNICは、系ごとに異なるサブネットに分けて配置する構成にもできます。

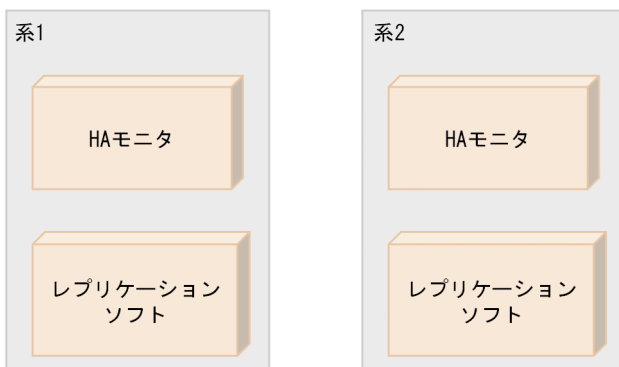
なお、業務通信に用いるVNICは、すべての系で同じサブネットに格納してください。

可用性ドメイン、フォルト・ドメイン、インスタンス、VNIC、およびブロック・ボリュームの詳細については、OCIのドキュメントを参照してください。

### 1.3.4 必要なソフトウェア

HA モニタを動作させるために必要なソフトウェアについて説明します。ソフトウェア構成例を、次の図に示します。

図 1-15 必要なソフトウェア



ディスクをレプリケーションして実行系から待機系にデータを引き継ぐ場合に、レプリケーションソフトが必要です。

# 2

## HA モニタを使用した系切り替え

この章では、障害が発生したあとに HA モニタが行う系切り替えについて説明します。系切り替えという概念を理解している方に向けて、HA モニタではどのように系を切り替えるのか、を中心に説明します。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタを使用した系切り替え」とあわせてお読みください。

## 2.1 障害検出から系切り替えまでの流れ

---

障害検出から系切り替えまでの流れについては、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「障害検出から系切り替えまでの流れ」の説明を参照してください。この節では、障害検出から系切り替えまでの流れについて、パブリッククラウド環境下で差異がある事項だけを記載します。

### 2.1.1 【AWS】系障害時の系切り替え

HA モニタが系障害を検出した場合、次の 2 つの方法で系切り替えをします。

- 系のリセットによる系切り替え
- ネットワーク遮断による系切り替え

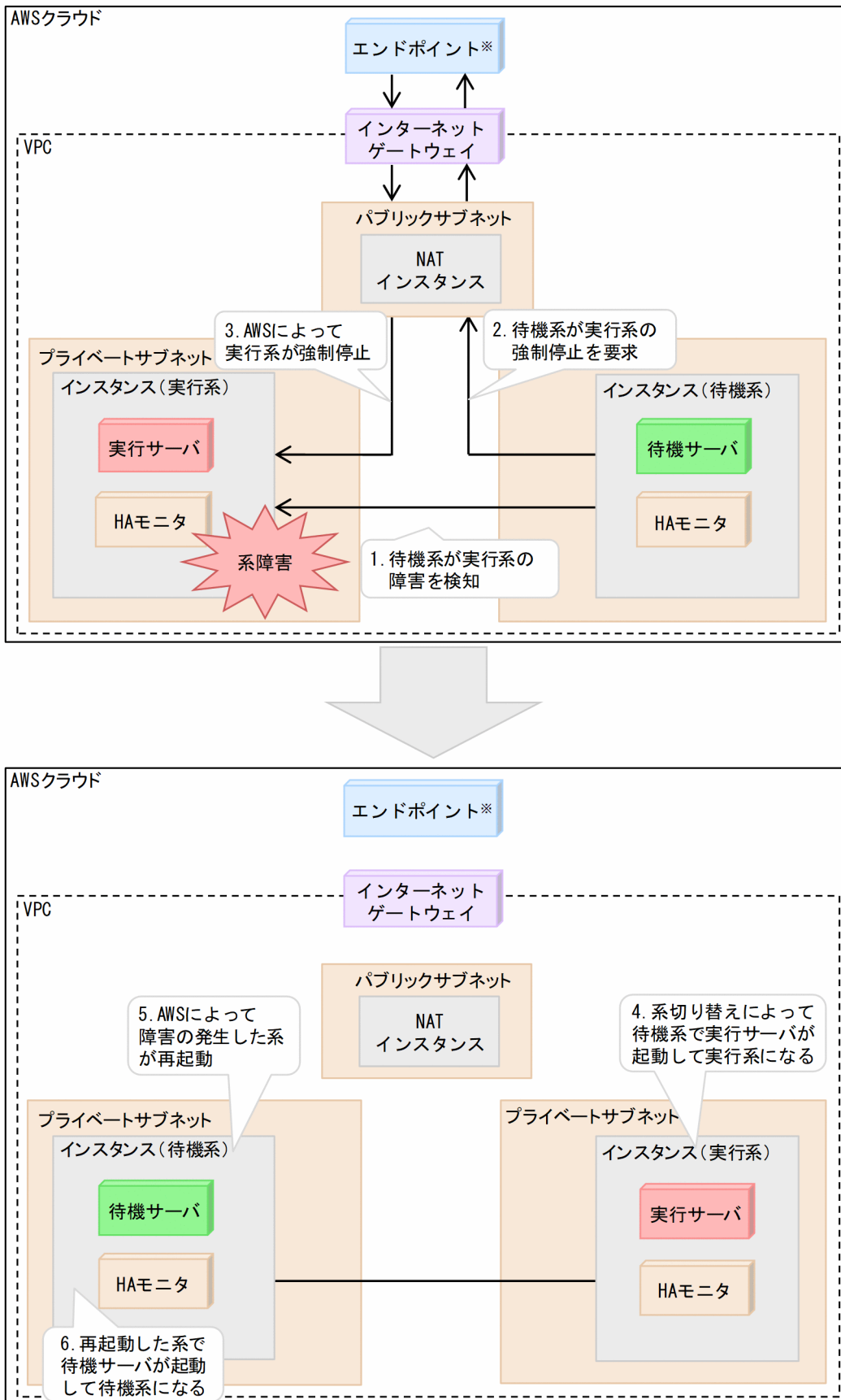
ここでは、HA モニタのそれぞれの系切り替えについて説明します。

#### (1) 系のリセットによる系切り替え

AWS 環境では、障害系のインスタンスを強制停止することによって系をリセットし、系切り替えをします。強制停止に失敗した場合は、系切り替え待ち状態となり、オペレータの対処が必要です。

系障害時の、HA モニタの系のリセットによる系切り替えの概要を、次の図に示します。

図 2-1 系障害時の系のリセットによる系切り替えの概要 (AWS)



## 注※

エンドポイントには、VPC エンドポイントを使用しても問題ありません。ただし、DNS 名制御によって業務通信を切り替える場合は、インターネットゲートウェイを介してエンドポイントにアクセスする必要があります。

系障害時の、HA モニタの系切り替えの概要について説明します。番号は、上記の図と対応しています。

1. 待機系が実行系の系障害を検知する。
2. 待機系が実行系の強制停止を要求する。
3. AWS によって実行系が強制停止される。
4. 系切り替えによって待機系で実行サーバが起動して実行系になる。
5. AWS によって障害が発生した系が再起動される。
6. 系の起動時に HA モニタおよびサーバを自動起動させる設定にしている場合、再起動した系で待機サーバが起動して待機系になる。

## (2) ネットワーク遮断による系切り替え

ネットワーク遮断による系切り替えは、障害系の入出力を閉塞させるため、障害系インスタンスの ENI<sup>※</sup> をデタッチして、障害系をネットワークから切り離すことで通信を遮断させる機能です。これによって、障害系の入出力を確実に遮断して系切り替えをします。

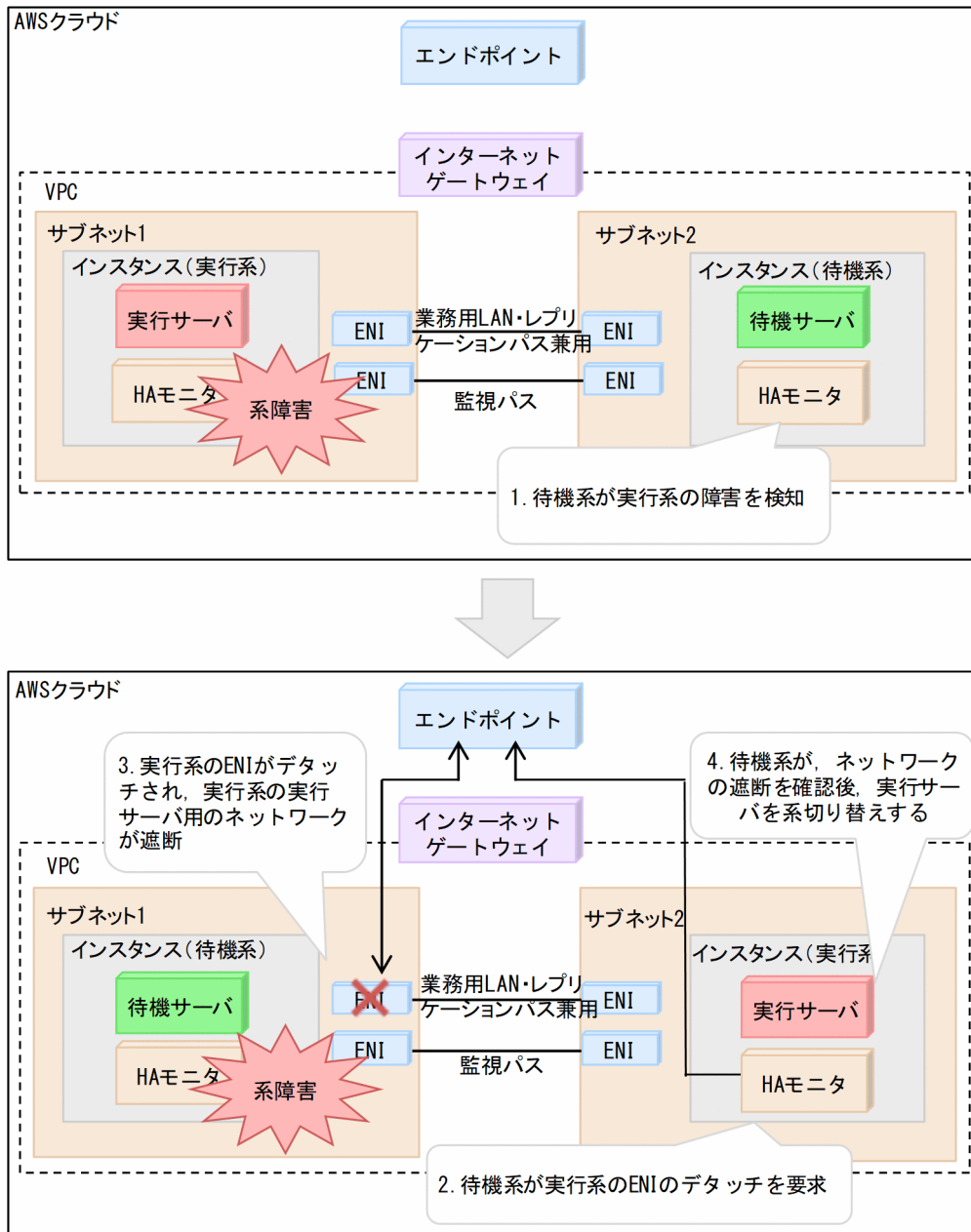
## 注※

ENI は DRBD レプリケーション、EFS へのアクセス、および業務通信に使用し、プライマリ ENI を使用していないことを前提としています。

ネットワーク遮断による系切り替えは、系のリセットによる系切り替えよりも所要時間が短いというメリットがあります。

系障害時の HA モニタのネットワーク遮断による系切り替えの概要を、次の図に示します。

図 2-2 ネットワーク遮断による系切り替えの概要(AWS)



ネットワーク遮断による系切り替えの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. 待機系が実行系の障害を検知する。
2. 待機系が実行系の ENI のデタッチを要求する。
3. 実行系の ENI がデタッチされ、実行系の実行サーバ用のネットワークが遮断される。
4. 待機系が、ネットワークの遮断を確認後、実行サーバを系切り替えをする。

デタッチ対象の ENI は次のとおりです。

- 実行サーバが業務通信に使用するネットワークの ENI
- レプリケーションに使用するネットワークの ENI

- EFS へのアクセスに使用するネットワークの ENI

ネットワークの遮断に掛かる時間はデタッチ対象の ENI の数に比例するため、業務用 LAN、レプリケーションパス、および EFS へのアクセス用パスで ENI を兼用するなど、ENI の数を必要最小限にすることを推奨します。

監視パスだけで使用するネットワークの ENI についてはデタッチの対象外です。

なお、実行系のネットワークが遮断されると、系切り替えと並行して、実行系インスタンスは強制停止されます。実行系インスタンスの強制停止を確認後、実行系インスタンスに ENI を再度アタッチし、実行系インスタンスの再起動によって、復旧に備えます。実行系インスタンスの強制停止から待機サーバ再起動までの流れについて、次の図に示します。

図 2-3 実行系の強制停止

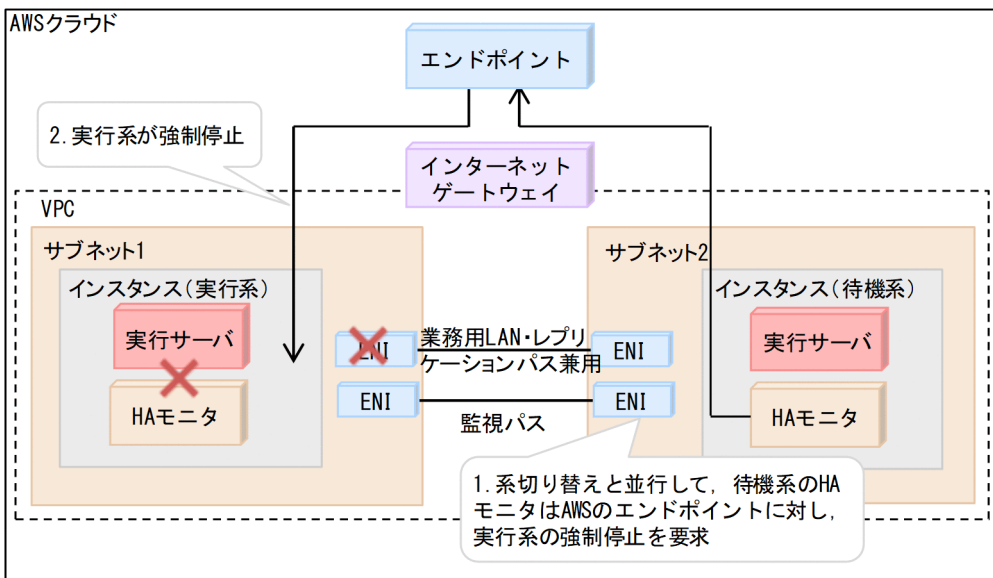


図 2-4 実行系インスタンスの再起動

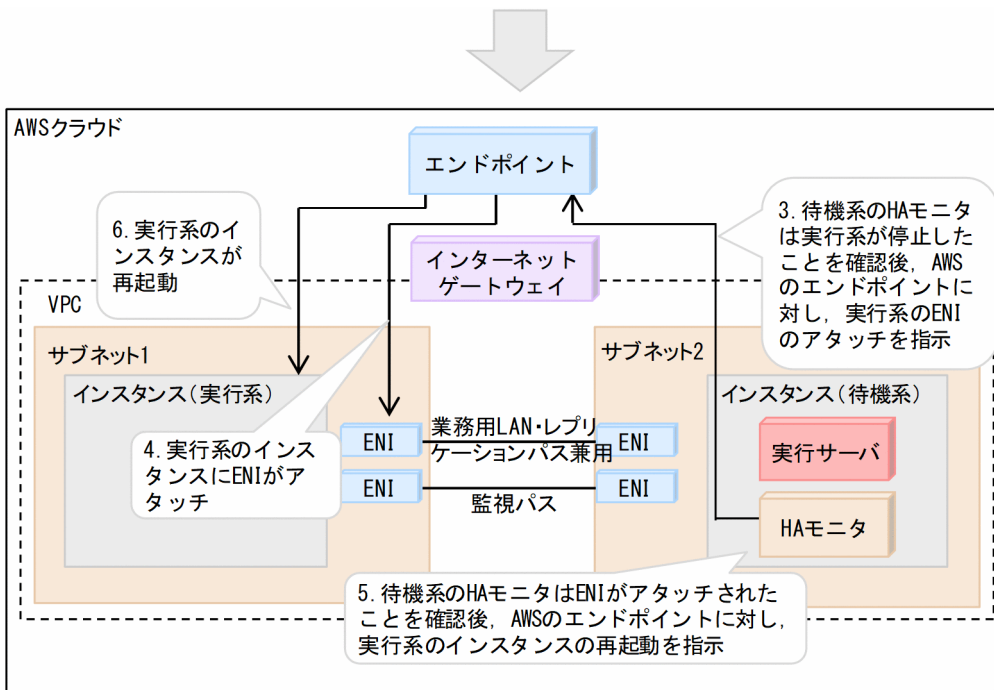
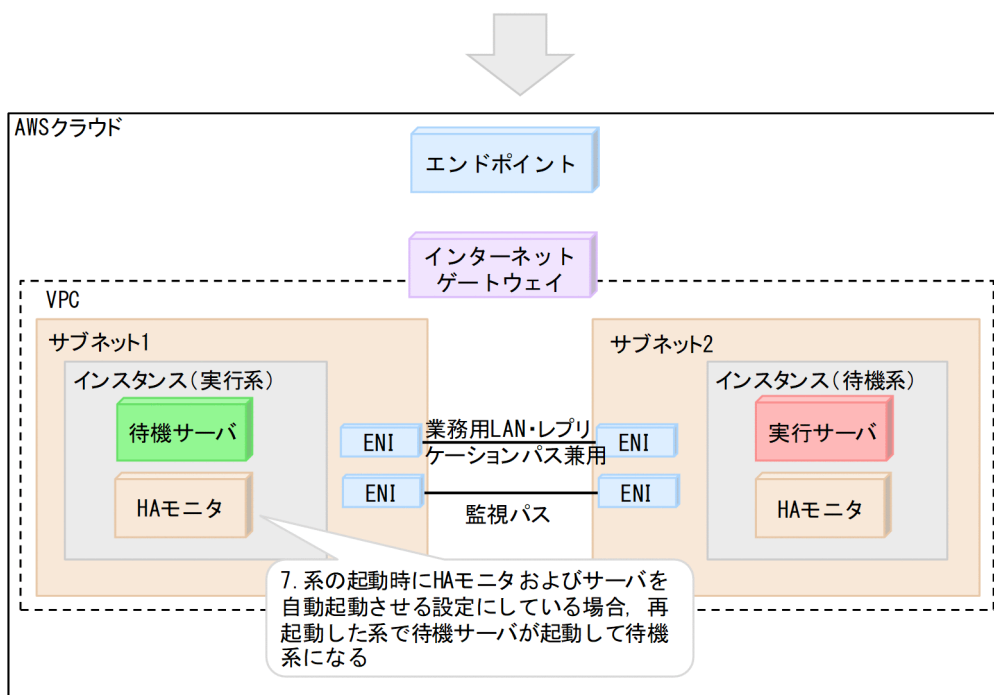


図 2-5 待機系サーバの再起動



実行系インスタンスの強制停止から待機サーバ再起動までの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. 系切り替えと並行して、待機系の HA モニタは AWS のエンドポイントに対し、実行系の強制停止を要求する。
2. 実行系が強制停止される。



3. 待機系の HA モニタは実行系が停止したことを確認後、AWS のエンドポイントに対し、実行系の ENI のアタッチを指示する。
4. 実行系のインスタンスに ENI がアタッチされる。
5. 待機系の HA モニタは ENI がアタッチされたことを確認後、AWS のエンドポイントに対し、実行系のインスタンスの再起動を指示する。
6. 実行系のインスタンスが再起動する。
7. 系の起動時に HA モニタおよびサーバを自動起動させる設定にしている場合、再起動した系で待機サーバが起動して待機系になる。

ネットワークの遮断に失敗した場合でも、インスタンスの強制停止に成功すれば、系切り替えができます。ネットワークの遮断とインスタンスの強制停止の両方に失敗した場合は、系切り替え待ちとなります。

ネットワーク遮断による系切り替えは、次の場合に動作します。

- 系障害による系切り替え時。
- サーバ障害や計画系切り替え時に、切り替え元の系でリソースの切り離しに失敗したとき。
- ペアダウン機能によって系切り替えをするとき。
- `monswap -f` コマンドで強制的に系切り替えをするとき。

ネットワーク遮断による系切り替えの動作時、次の事象が発生した場合は、ユーザによる対処が必要になります。

- 障害系のネットワークの遮断、およびインスタンスの強制停止の両方に失敗したとき。  
待機系で系切り替え待ちの状態になります。HA モニタの `monact` コマンドの入力によって系切り替えを再開させるなど、系切り替え待ちになった場合の運用をしてください。
- インスタンスが自動的に再起動しないとき。  
AWS コンソールからインスタンスを再起動してください。
- ENI の再アタッチができなかったとき。

該当する系の HA モニタを再起動したときに、KAMN766-E メッセージが出力されます。必要な ENI を該当する系のインスタンスにアタッチしてから、インスタンスを再起動してください。

HA モニタはアタッチするためのツールとして `/opt/hitachi/HAmom/lib/aws_eni_attach_tool.sh` を提供しています。

このツールは、ツールを実行した系のネットワーク遮断設定ファイルに定義された ENI をインスタンスにアタッチします。

実行例を次に示します。

```
# /opt/hitachi/HAmom/lib/aws_eni_attach_tool.sh
Attach the following ENI to this instance(ID:i-007f3a3f424a2782e).
ENI ID:eni-00b5544856f6e1bed
ENI ID:eni-0456be17c65141837
Continue(hit enter key) or Cancel([CTRL]+[C]) ?*
Attaching ENI:eni-00b5544856f6e1bed ..... Attached.
```

```
Already attached :eni-0456be17c65141837
#
```

#### 注※

ENI ID に表示された ENI をアタッチしたい場合はエンターキーを押してください。アタッチしない場合はコントロールキーを押しながら [C] キー ([CTRL] + [C]) を押してください。

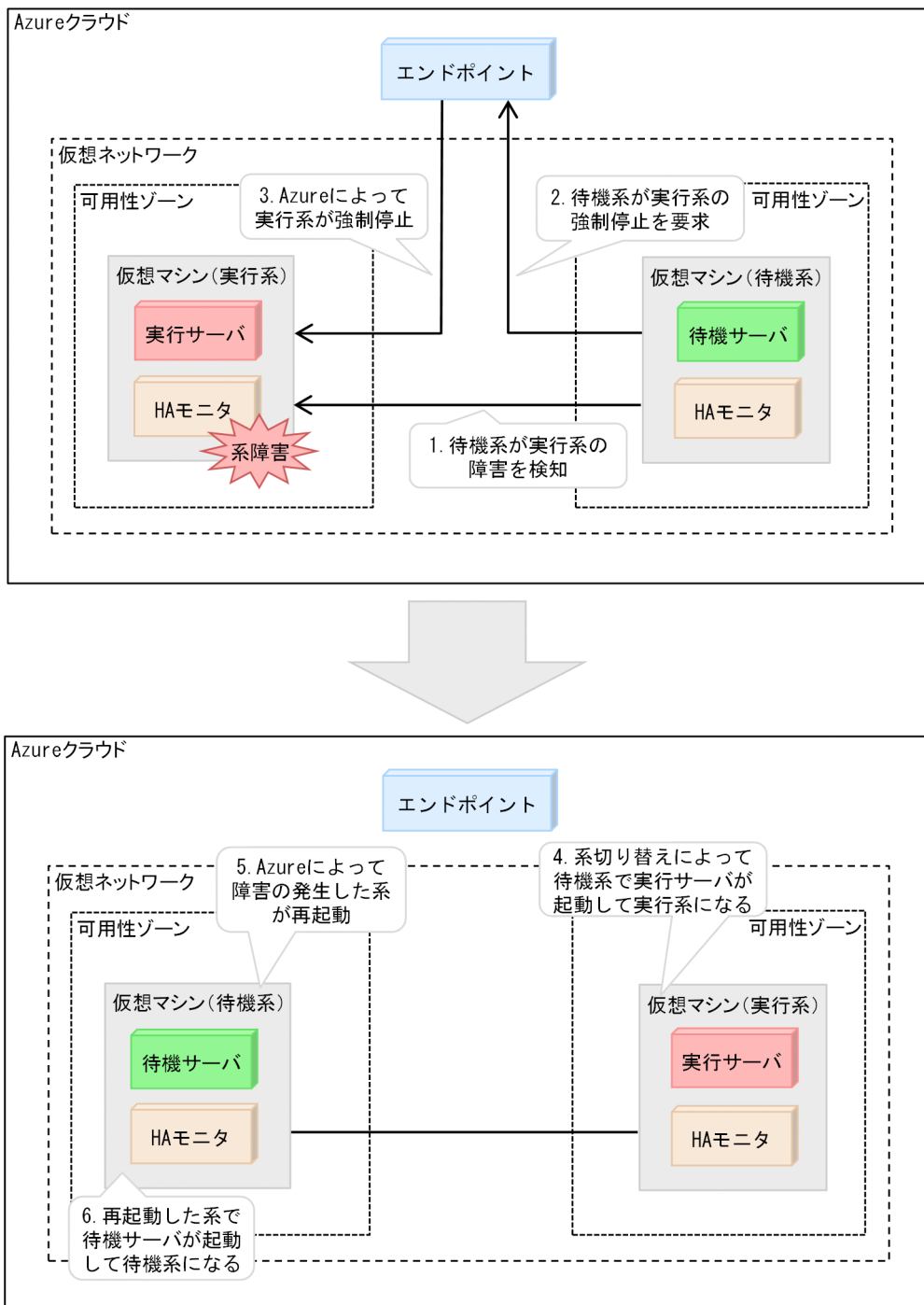
なお、このツールでは、AWS CLI を使用するため、AWS のエンドポイントと通信可能な状態で実行してください。

## 2.1.2 【Azure】系障害時の系切り替え

HA モニタが系障害を検出した場合、系のリセットによって系切り替えをします。Azure 環境では、障害系の仮想マシンを強制停止することによって系をリセットし、系切り替えをします。強制停止に失敗した場合は、系切り替え待ち状態となり、オペレータの対処が必要です。

系障害時の、HA モニタの系切り替えの概要を、次の図に示します。

図 2-6 系障害時の系切り替えの概要 (Azure)



系障害時の、HA モニタの系切り替えの概要について説明します。番号は、上記の図と対応しています。

1. 待機系が実行系の系障害を検知する。
2. 待機系が実行系の強制停止を要求する。
3. Azure によって実行系が強制停止される。
4. 系切り替えによって待機系で実行サーバが起動して実行系になる。
5. Azure によって障害が発生した系が再起動される。

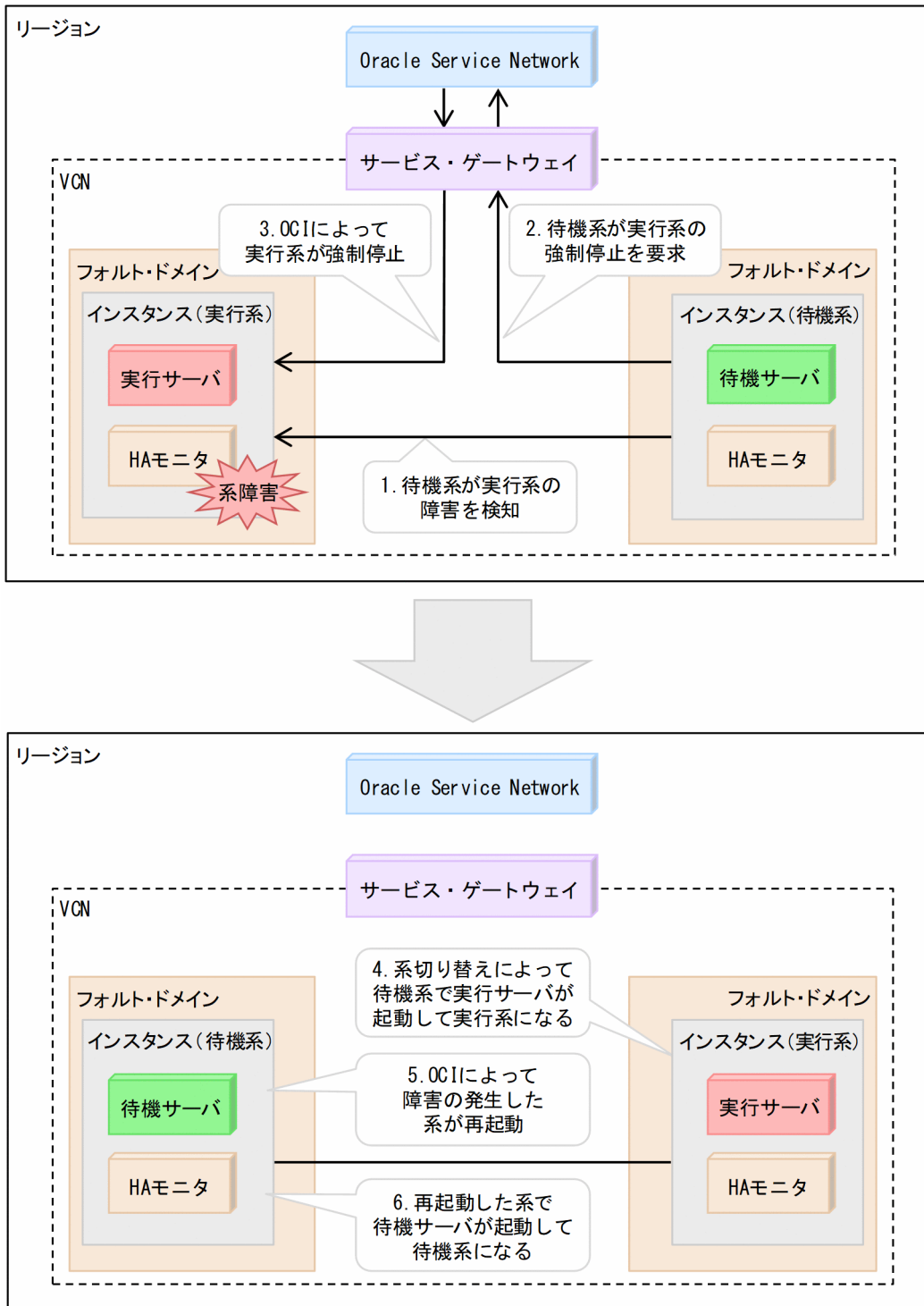
6. 系の起動時に HA モニタおよびサーバを自動起動させる設定にしている場合、再起動した系で待機サーバが起動して待機系になる。

### 2.1.3 【OCI】系障害時の系切り替え

HA モニタが系障害を検出した場合、系のリセットによって系切り替えをします。OCI 環境では、障害系のインスタンスを強制停止することによって系をリセットし、系切り替えをします。強制停止に失敗した場合は、系切り替え待ち状態となり、オペレータの対処が必要です。

系障害時の、HA モニタの系切り替えの概要を、次の図に示します。

図 2-7 系障害時の系切り替えの概要 (OCI)



系障害時の、HA モニタの系切り替えの概要について説明します。番号は、上記の図と対応しています。

1. 待機系が実行系の系障害を検知する。
2. 待機系が実行系の強制停止を要求する。
3. OCI によって実行系が強制停止される。
4. 系切り替えによって待機系で実行サーバが起動して実行系になる。

5. OCI によって障害が発生した系が再起動される。
6. 系の起動時に HA モニタおよびサーバを自動起動させる設定にしている場合、再起動した系で待機サーバが起動して待機系になる。

## 2.2 HA モニタによる障害検出

HA モニタによる障害検出については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタによる障害検出」の説明を参照してください。この節では、HA モニタによる障害検出について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 2.2.1 HA モニタが系切り替えをする条件

サーバ障害発生時に系切り替えをする条件については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタが系切り替えをする条件」の説明を参照してください。

なお、系障害発生時に系切り替えをする条件については、パブリッククラウド環境でない場合とは差異があります。パブリッククラウド環境下の系障害発生時に系切り替えをする条件を次に示します。

- 待機系の HA モニタと、監視パスで通信できる状態であること
- 実行サーバに対応する待機サーバが待機中であること
- AWS CLI または Azure CLI が実行できる状態であること

### 2.2.2 系障害の検出

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系障害の検出」の説明を参照してください。

ただし、パブリッククラウド環境下では、リセットパスのヘルスチェックをしません。代わりに、AWS CLI または Azure CLI の実行可否チェックをします。

#### (1) AWS CLI, Azure CLI, または OCI CLI の実行可否チェック

AWS CLI, Azure CLI, および OCI CLI の実行可否チェックについて、説明します。

パブリッククラウド環境下では、インスタンスの強制停止や業務通信の切り替えなどを AWS CLI, Azure CLI, または OCI CLI で実施します。CLI が実行できる状態でなければ、系切り替えはできません。そのため、HA モニタは CLI を実行できる状態かどうかを定期的にチェックします。

CLI 実行可否チェックは、HA モニタを起動してから停止するまで、60 秒間隔で実施します。

CLI を実行できない場合は、メッセージ KAMN768-E を出力します。メッセージに従って、対処してください。

次のどちらかの場合で、CLI を実行できない状態が継続している間は、1 時間おきに繰り返しメッセージ KAMN769-W を出力します。

- HA モニタの環境設定の `notswitch_notify` オペランドに `use` を指定している場合

- HA モニタの環境設定のnotswitch\_notify オペランドを省略した場合

CLI を実行できない状態から、実行できる状態に回復した場合は、CLI 実行可否チェック時にメッセージ KAMN770-I を出力します。

CLI 実行可否チェックは、シェルスクリプトから CLI を実行することによって実施します。このシェルスクリプトは、パブリッククラウド環境で HA モニタを使用するために必要なスクリプトを集めたシェルスクリプト群に含まれています。環境構築時にこのシェルスクリプト群を展開しておく必要があります。このシェルスクリプト群については、「[5.7 【AWS】 AWS用のシェルスクリプト群の展開](#)」, 「[5.8 【Azure】 Azure用のシェルスクリプト群の展開](#)」, または「[5.9 【OCI】 OCI用のシェルスクリプト群の展開](#)」を参照してください。



## 2.3 【AWS】 リソースの引き継ぎ

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有リソースの引き継ぎ」を参照してください。ただし、AWS 環境下では次の点が異なります。

- どちらかの方式で業務ディスクを引き継ぐ。
  - 実行系および待機系に業務ディスクを配置し、業務ディスク内のデータをレプリケーションソフトで常時同期する（レプリケーション構成）。※
  - EBS マルチアタッチ機能、または EFS を使用して、実行系および待機系で業務ディスクを共有する（共有ディスク構成）。
- LAN の引き継ぎに加え、次の制御で通信を切り替える。
  - VIP 制御
  - EIP 制御
  - DNS 名制御

### 注※

実行系および待機系に業務ディスクを配置する構成であっても、LVM によるボリュームグループ単位の接続・切り離し、ファイルシステムのマウント・アンマウントは実施します。

詳細については、「[4.2 リソースの管理](#)」を参照してください。

## 2.4 【Azure】リソースの引き継ぎ

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有リソースの引き継ぎ」を参照してください。ただし、Azure 環境下では次の点が異なります。

- どちらかの方式で業務ディスクを引き継ぐ。
  - 実行系および待機系に業務ディスクを配置し、業務ディスク内のデータをレプリケーションソフトで常時同期する（レプリケーション構成）。※
  - マネージドディスクの共有をして、実行系および待機系で業務ディスクを共有する（共有ディスク構成）。
- LAN の引き継ぎに加え、次の制御で通信を切り替える。
  - Azure ロードバランサーによる制御
  - DNS 名制御

### 注※

実行系および待機系に業務ディスクを配置する構成であっても、LVM によるボリュームグループ単位の接続・切り離し、ファイルシステムのマウント・アンマウントは実施します。

詳細については、「[4.2 リソースの管理](#)」を参照してください。

## 2.5 【OCI】 リソースの引き継ぎ

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有リソースの引き継ぎ」を参照してください。ただし、OCI 環境下では次の点が異なります。

- LAN の引き継ぎに加え、次の制御で通信を切り替える。
  - プライベート IP アドレスによる制御

詳細については、「[4.2 リソースの管理](#)」を参照してください。

# 3

## HA モニタで使用できる機能

この章では、パブリッククラウド環境下で使用できる HA モニタの機能について説明します。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタで使用できる機能」とあわせてお読みください。

## 3.1 HA モニタで使用できる機能一覧

パブリッククラウド環境下で使用できる HA モニタの機能を、次の表に示します。

表 3-1 パブリッククラウド環境下の HA モニタで使用できる機能

| 機能        |                          | パブリッククラウド |
|-----------|--------------------------|-----------|
| 分類        | 機能名                      |           |
| サーバの制御    | モニタモードのサーバの監視            | ○         |
|           | モニタモードの待機系での監視           | ○         |
|           | サーバのグループ化による連動系切り替え      | ○         |
|           | サーバの切り替え順序制御             | ○         |
|           | 複数の待機系を配置するマルチスタンバイ      | ○         |
|           | 系切り替え後の負荷集中を避けるサーバの排他制御  | ○         |
|           | 系切り替え時の起動リトライ            | ○         |
|           | JP1 と連携したシステム運用          | ○         |
| 系の制御      | 系の同時リセットの防止              | ○         |
|           | 複数系間の同時リセットの防止           | ○         |
|           | 系の二重リセットの防止              | —         |
|           | 系のリセットの抑止                | ○         |
|           | サーバ障害時に系ごと切り替える系のペアダウン   | ○         |
|           | 他系の OS パニック検知            | —※1       |
|           | 仮想化環境での物理パーティションリセット機能   | —         |
|           | N+M コールドスタンバイ構成での系切り替え   | —         |
| 共有リソースの制御 | リソースサーバを使用した共有リソースの共用    | ○         |
|           | サーバや HA モニタの状態変化時のコマンド発行 | ○         |
|           | 共有リソース接続失敗時のサーバの起動中止     | ○         |
|           | 共有リソース引き継ぎのタイムアウト        | ○         |

| 機能               |                       | パブリッククラウド |
|------------------|-----------------------|-----------|
| 分類               | 機能名                   |           |
|                  | 共有リソースの切り離し順序指定       | ○         |
|                  | 共有リソースの動的変更           | ○※2       |
| リソースの監視          | LAN の監視および障害時の自動系切り替え | ○         |
|                  | ディスクの監視               | ○         |
| プログラムの制御         | UAP の監視               | ○         |
| HA モニタ Extension | サーバの最大数の変更            | ○         |
|                  | 系の最大数の変更              | —         |

(凡例)

- ：使用できます。
- ：使用できません。

注※1

OS パニックになった場合、すぐに検知できませんが、系障害検知時間が経過すると検知します。

注※2

DRBD リソースの動的変更はできません。

# 4

## システムの管理

この章では、HA モニタが系およびリソースをどのように管理しているかについて説明します。HA モニタの動作の詳細を知りたい場合にお読みください。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系の管理」とあわせてお読みください。

## 4.1 系の管理

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系の管理」を参照してください。この節では、系のリセットに関する HA モニタの動作について、パブリッククラウド環境下で差異がある事項だけを記載します。

なお、オペレータの操作については、「6. システムの運用」を参照してください。

### 4.1.1 系のリセットまたはネットワーク遮断をする系の決定方法

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系のリセットをする系の決定方法」を参照してください。ただし、リセット完了またはネットワーク遮断連絡を待つ時間を次のとおりに読み替えてください。

- AWS 環境かつ系のリセットをする場合、または Azure 環境の場合：120 秒
- AWS 環境かつ系のネットワーク遮断をする場合：30 秒
- OCI 環境の場合：30 秒

### 4.1.2 両系が障害を同時に検出した場合の系切り替え

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「両系が障害を同時に検出した場合の系切り替え」を参照してください。ただし、リセット発行またはネットワーク遮断の待ち時間を次のとおりに読み替えてください。

- AWS 環境かつ系のリセットをする場合、または Azure 環境の場合：120 秒
- AWS 環境かつ系のネットワーク遮断をする場合：30 秒
- OCI 環境の場合：30 秒

また、「ユーザがリセット優先系を指定しないときの系切り替え」はパブリッククラウド環境下では使用できません。

### 4.1.3 複数の待機系がある場合の系のリセットまたはネットワーク遮断

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「複数の待機系がある場合の系のリセット」を参照してください。ただし、リセット発行またはネットワーク遮断の待ち時間を次のとおりに読み替えてください。

- AWS 環境かつ系のリセットをする場合、または Azure 環境の場合：120 秒
- AWS 環境かつ系のネットワーク遮断をする場合：30 秒



- OCI 環境の場合：30 秒

## 4.2 リソースの管理

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有リソースの管理」を参照してください。この節では、リソースの管理について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 4.2.1 業務ディスクの管理

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有ディスクの管理」を参照してください。

AWS 環境下および Azure 環境下では、業務ディスクをレプリケーションする構成の場合、加えて次の制御も実施します。

#### (1) 基本的な制御

HA モニタは、OS のコマンドによってボリュームグループ単位で接続・切り離しをします。HA モニタがボリュームグループに接続することで、レプリケーションソフトによって業務ディスクがプライマリに昇格します。HA モニタがボリュームグループを切り離すことで、レプリケーションソフトによって業務ディスクがセカンダリに降格します。

#### (2) レプリケーションパス障害時の制御

系切り替えができる状態でレプリケーションパスが障害になった場合、セカンダリ側（待機系）の業務ディスクが更新できなくなります。また、待機サーバを起動したときにレプリケーションパスが障害だった場合も、セカンダリ側（待機系）の業務ディスクは更新されません。セカンダリ側（待機系）の業務ディスクが更新されていない状態だと、実行系に障害が発生し、系切り替えをしたときに、古いデータを参照した状態で業務を続行することになります。

これを防止するため、HA モニタで次の作業を実施します。

マルチスタンバイ機能を使用しない場合

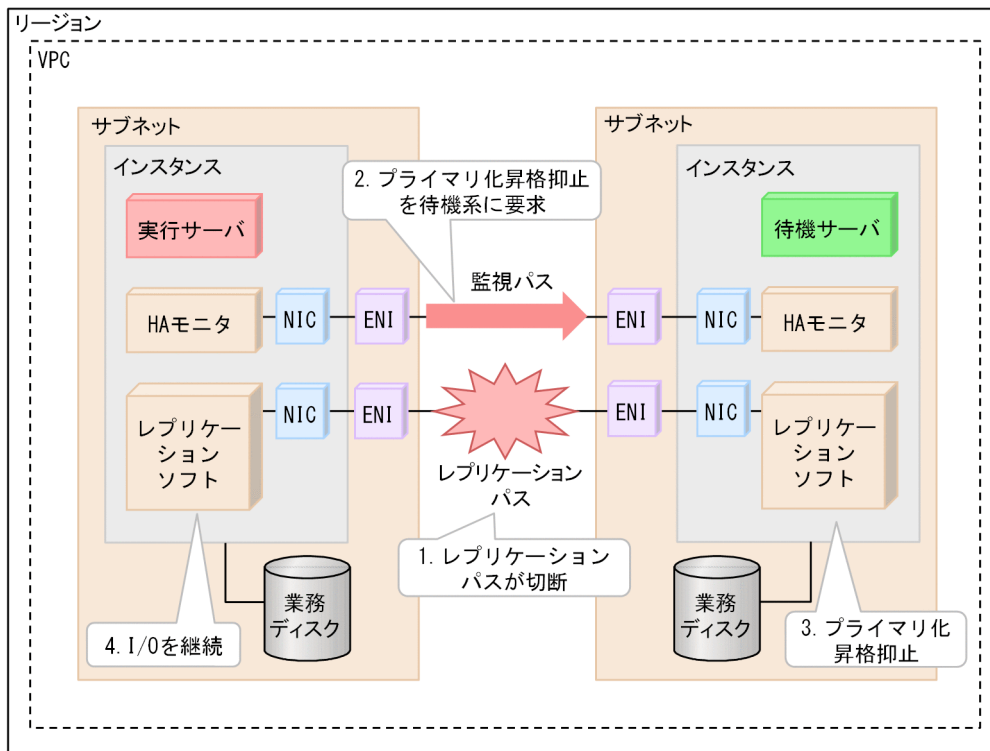
セカンダリ側の HA モニタで次のコマンドを実行して、セカンダリ側の業務ディスクがプライマリに昇格することを抑止します。

```
drbdsetup outdate /dev/drbdX
```

drbdsetup コマンドの実行によって、レプリケーションパスの障害時に系切り替えをした場合でも、セカンダリ側の業務ディスクがプライマリに昇格できないため、古いデータを参照して業務を続行することを防止できます。セカンダリ側の業務ディスクがプライマリに昇格するのを抑止したあと、プライマリ側で I/O を継続します。

レプリケーションパス障害時の制御の流れについて、次の図に示します。

図 4-1 レプリケーションパス障害時の制御の流れ



プライマリ昇格抑止に失敗した場合は、メッセージKAMN771-E を出力し、待機サーバを停止させます。プライマリ昇格抑止をしたあとに、レプリケーションパスが回復した場合には、レプリケーションソフトによって再同期が実施され、プライマリ昇格抑止が自動的に解除されます。なお、再同期中に系障害による系切り替えが発生した場合、セカンダリ側は業務ディスクステータスが最新になっていないため、プライマリ昇格はできず、古いデータを参照して業務を継続することはありません。

レプリケーションパスと監視パスが同時に障害になった場合、待機系に連絡できずプライマリ昇格抑止設定ができません。そのため、実行系が待機系をリセットして、その後の系切り替えが発生しないようにします。ただし、リセット優先系の設定などによって実行系がリセットされて系切り替えをする場合もあります。DRBD 用のシェルスクリプト群を展開している場合は、standbyreset オペランドの指定に関係なく待機系がリセットされます。詳細は、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「両系が障害を同時に検出した場合の系切り替え」を参照してください。

#### マルチスタンバイ機能を使用する場合

レプリケーションパスが切断したセカンダリの系で、メッセージKAMN771-E を出力して待機サーバを停止します。レプリケーションパスを回復させたあと、待機サーバを再起動してください。

レプリケーションパスと監視パスが同時に障害になった場合は、リセット優先度に従って動作します。詳細は、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「複数の待機系がある場合の系のリセット」を参照してください。実行系がリセットされた場合は、系切り替えをします。レプリケーションパスが切断したセカンダリの系がリセットされた場合は、リセットされた系以外で業務を継続します。

## 4.2.2 【AWS】 LAN の管理

クライアントから実行サーバへの通信を実現するために、HA モニタは次の制御をします。

OS でのエイリアス IP の追加・削除（DNS 名制御の場合を除く）

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「LAN の管理」を参照してください。ただし、AWS 環境下では次の点が異なります。

- OS のarping コマンドは実行不要\*
- エイリアス IP を割り当てるとき、ブロードキャストアドレスは指定不可

注※

AWS での通信経路の制御によって、通信経路が定まるためです。

AWS での通信経路の制御

1 つのリージョン内または 1 つの VPC 内で系切り替えをする構成の場合、AWS 環境下では、次の通信制御の方式があります。

- VIP 制御による業務通信の切り替え
- EIP 制御による業務通信の切り替え
- DNS 名制御による業務通信の切り替え

複数のリージョン間、または複数の VPC 間で系切り替えをする構成の場合、AWS 環境下では、次の通信制御の方式があります。

- VIP 制御による業務通信の切り替え
- DNS 名制御による業務通信の切り替え

系切り替え対象のサーバと通信するクライアントの場所によって、業務通信の切り替え方法が決定します。次の表で、業務通信の切り替え方法を確認してください。

表 4-1 AWS 環境下の業務通信の切り替え方法

| 切り替え対象のサーバと通信するクライアントの場所  |                 | 業務通信の切り替え方法                                |
|---------------------------|-----------------|--|
| VPC 外                     | インターネット上        | EIP 制御による業務通信の切り替え                         |
|                           | VPN 内*          | VIP 制御による業務通信の切り替え                         |
|                           | Direct Connect* |  |
|                           | VPC Peering*    |  |
| VPC 内                     |                 |  |
| VPC 外（インターネット上）と VPC 内の両方 |                 | EIP 制御による業務通信の切り替え、または DNS 名制御による業務通信の切り替え |

注※

トランジットゲートウェイによる接続が必要です。

次に、それぞれの通信経路の制御方式について説明します。

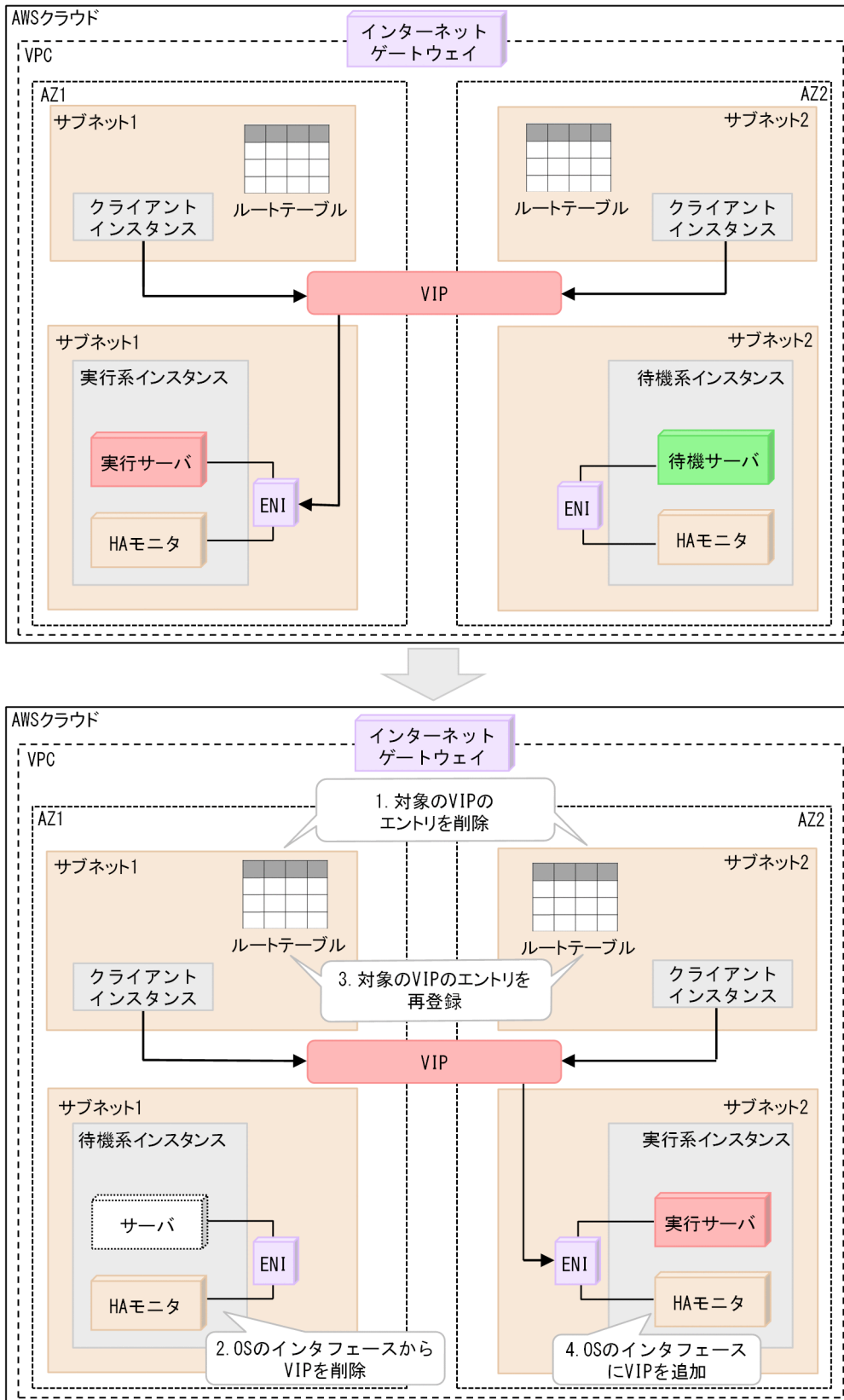
## (1) VIP 制御による業務通信の切り替え（1つのリージョン内または1つのVPC内で系切り替えをする構成の場合）

1つのリージョン内または1つのVPC内で系切り替えをする構成での、VIP制御による業務通信の切り替えについて説明します。

AWS上での操作によるルートテーブルの書き換え、およびOSでのエイリアスIPの追加・削除によって、業務通信を切り替えます。

VIP制御による業務通信の切り替えの流れについて説明します。実行系インスタンスから待機系インスタンスにVIPを切り替える場合の動作例について次の図に示します。

図 4-2 VIP 制御による業務通信の切り替えの動作例



業務通信を切り替える前の、実行系インスタンスのルートテーブルの例を次に示します。この時点では、VIPは、実行系インスタンスのENIを指しています。

表 4-2 業務通信の切り替え前のルートテーブル例

| Destination                    | Target                             | 備考 |
|--------------------------------|------------------------------------|----|
| VPC のネットワーク<br>(例：10.0.0.0/16) | local                              | -  |
| 0.0.0.0/0                      | Internet gateway                   | -  |
| VIP<br>(例：10.1.0.10/32)        | eni-xxxxxxx<br>(実行系インスタンスの ENI ID) | -  |

(凡例)

-：特にありません。

VIP 制御による業務通信の切り替えの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. HA モニタは、AWS CLI で、ルートテーブルから対象の VIP のエントリを削除する。

ルートテーブルの内容（エントリを削除後）：

| Destination                    | Target           | 備考 |
|--------------------------------|------------------|----|
| VPC のネットワーク<br>(例：10.0.0.0/16) | local            | -  |
| 0.0.0.0/0                      | Internet gateway | -  |
| (空白)                           | (空白)             | 削除 |

(凡例)

-：特にありません。

2. HA モニタは、OS の ip コマンドを実行することによって、ネットワークインタフェースから実行系インスタンスに対する VIP を削除する。

3. HA モニタは、AWS CLI で、対象の VIP のエントリをルートテーブルに再登録する。対象 VIP のターゲットは、待機系インスタンスの ENI にする。

ルートテーブルの内容（エントリを再登録後）：

| Destination                    | Target                              | 備考 |
|--------------------------------|-------------------------------------|----|
| VPC のネットワーク<br>(例：10.0.0.0/16) | local                               | -  |
| 0.0.0.0/0                      | Internet gateway                    | -  |
| VIP<br>(例：10.1.0.10/32)        | eni-yyyyyyyy<br>(待機系インスタンスの ENI ID) | 追加 |

(凡例)

-：特にありません。

4. HA モニタは、OS の ip コマンドを実行することによって、ネットワークインタフェースに待機系インスタンスに対する VIP を追加する。

例えば、上記の図中で、実行系インスタンスおよび待機系インスタンスにも、対象の VIP と通信するクライアントがある場合、実行系インスタンスおよび待機系インスタンスが持つルートテーブルも、操作対象となります。

これらの処理をするためには、LAN の状態設定ファイルを設定する必要があります。LAN の状態設定ファイルについては、「[5.13.2 【AWS】 LAN の状態設定ファイルの設定 \(1つのリージョン内または1つのVPC内で系切り替えをする構成の場合\)](#)」を参照してください。

## (2) VIP 制御による業務通信の切り替え（複数のリージョン間または複数のVPC間で系切り替えをする場合）

次の構成での、VIP 制御による業務通信の切り替えについて説明します。

- 同一のリージョン内の、複数の VPC 間で系切り替えをする構成
- 複数のリージョン間で系切り替えをする構成
- 同一の VPC 内の複数の AZ 間、および複数のリージョン間で系切り替えをする構成

これらの構成には、トランジットゲートウェイが必要です。トランジット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。

### ❗ 重要

これらの構成で系切り替えをする場合は、次の前提条件を満たす必要があります。

- リージョンが2つ以内の構成であること
- 系切り替え構成のリージョン内に、クライアントが配置されていること

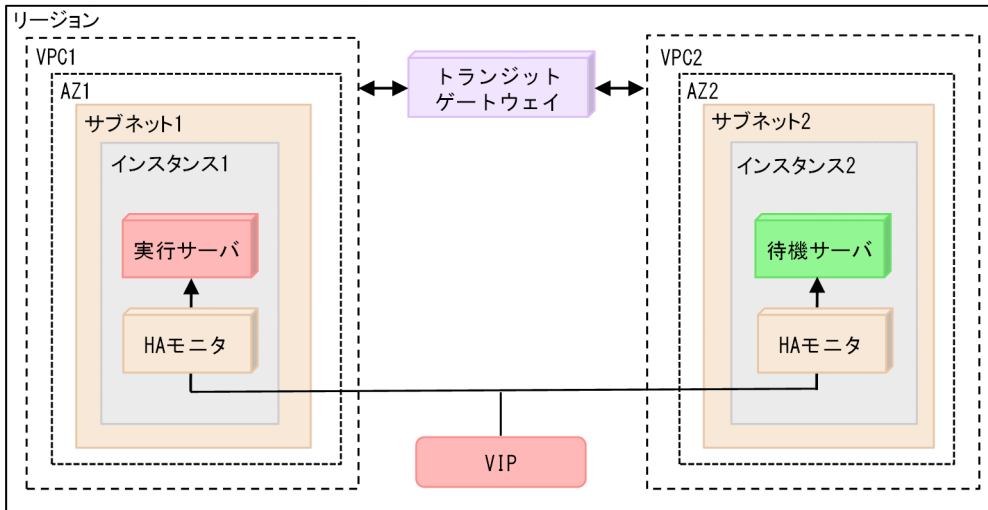
次に、それぞれの構成について説明します。

同一のリージョン内の、複数の VPC 間で系切り替えをする構成

同一のリージョン内の、複数の VPC 間で系切り替えをする構成の例を次の図に示します。



図 4-3 同一のリージョン内の、複数の VPC 間で系切り替えをする構成の例

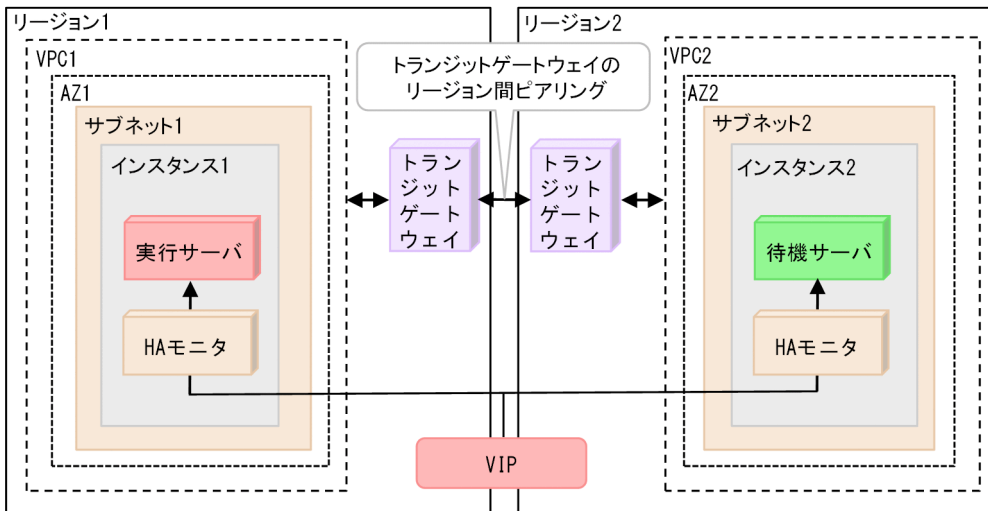


同一のリージョン内の各 VPC (VPC1 および VPC2) に、HA モニタを構成するインスタンス (インスタンス 1 およびインスタンス 2) をそれぞれ配置します。また、複数の VPC 間をトランジットゲートウェイで接続し、VIP の業務通信をルーティングします。

#### 複数のリージョン間で系切り替えをする構成

複数のリージョン間で系切り替えをする構成の例を次の図に示します。

図 4-4 複数のリージョン間で系切り替えをする構成の例



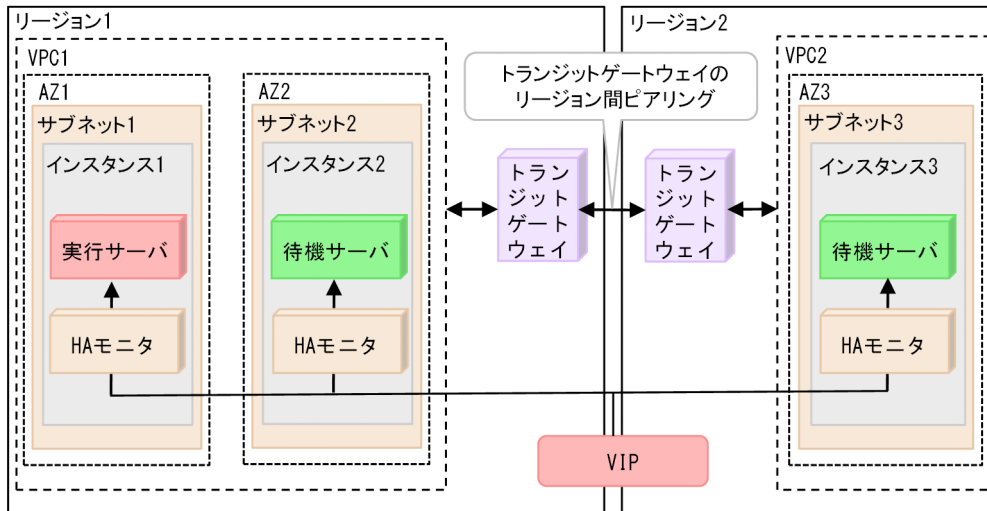
各リージョン (リージョン 1 およびリージョン 2) に、HA モニタを構成するインスタンス (インスタンス 1 およびインスタンス 2) をそれぞれ配置します。

また、トランジットゲートウェイをリージョンごとに配置します。トランジットゲートウェイのリージョン間ピアリングの機能で、複数のリージョン間を接続し、VIP の業務通信をルーティングします。

#### 同一の VPC 内の複数の AZ 間、および複数のリージョン間で系切り替えをする構成

同一の VPC 内の複数の AZ 間、および複数のリージョン間で系切り替えをする構成の例を次の図に示します。

図 4-5 同一の VPC 内の複数の AZ 間、および複数のリージョン間で系切り替えをする構成の例



上記の図は、複数スタンバイ構成です。リージョン 1 の VPC (VPC1) 内に、HA モニタを構成するインスタンス (インスタンス 1 およびインスタンス 2) をそれぞれ配置します。リージョン 2 の VPC (VPC2) 内にも、HA モニタを構成するインスタンス (インスタンス 3) を配置します。

また、トランジットゲートウェイをリージョンごとに配置します。トランジットゲートウェイのリージョン間ピアリングの機能で複数のリージョン間を接続し、VIP の業務通信をルーティングします。

### (a) VIP のルーティングの動作

VIP のルーティングの概要について説明します。

各トランジットゲートウェイには、VPC のルートテーブルとは別に、トランジットゲートウェイルートテーブルがあります。トランジットゲートウェイルートテーブルは、トランジットゲートウェイアタッチメント内のパケットをどこにルーティングするかを指定できます。

トランジットゲートウェイアタッチメントは、次のとおりネットワーク間を接続しています。

- VPC 用のトランジットゲートウェイアタッチメントで、VPC とトランジットゲートウェイとの間を接続
- ピアリング用のトランジットゲートウェイアタッチメントで、トランジットゲートウェイ間を接続

なお、トランジットゲートウェイアタッチメントは、トランジットゲートウェイルートテーブルと関連づけることができます。

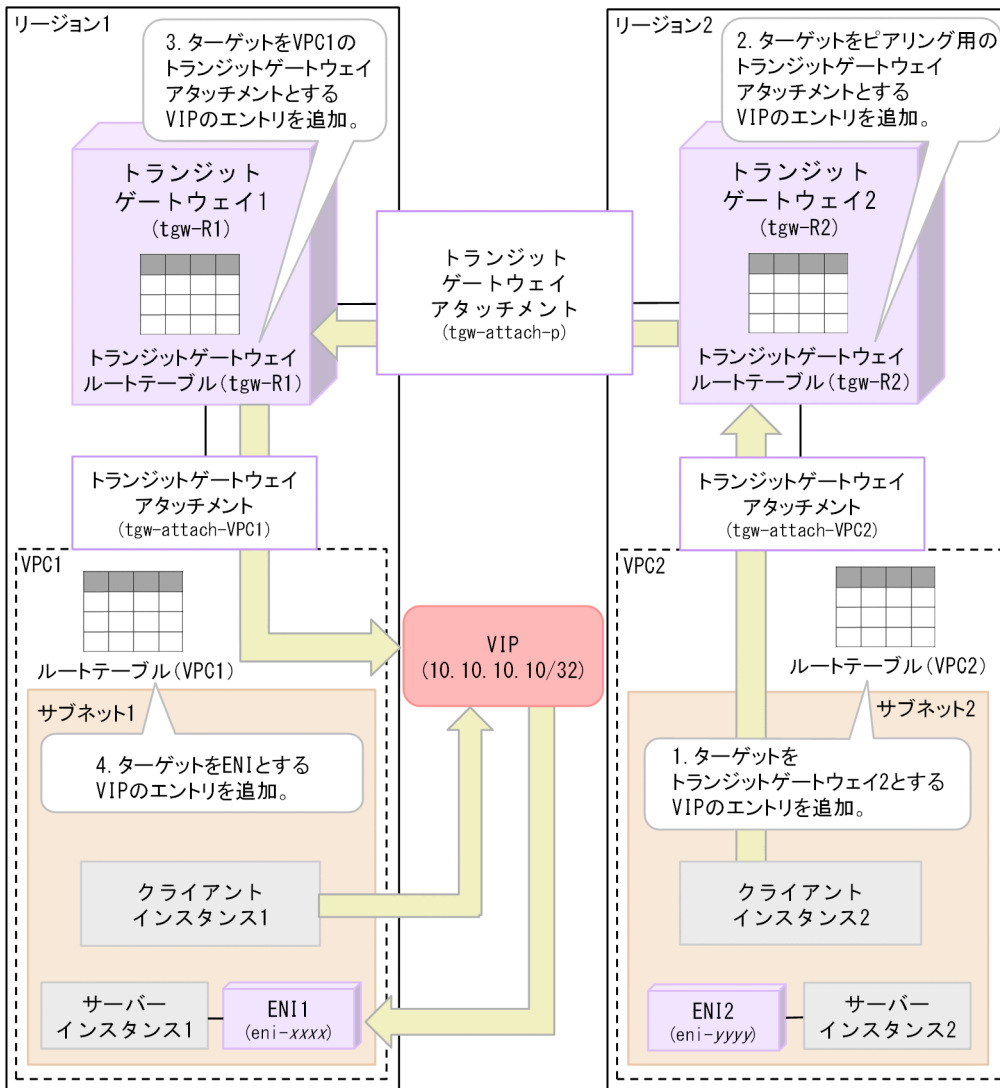
次に、VIP のルーティングの動作について説明します。

VIP による業務通信を切り替える場合、HA モニタが次のルートテーブルの経路情報を追加します。

- VPC のルートテーブル
- トランジットゲートウェイルートテーブル

複数のリージョン間で系切り替えをする構成で、サーバーインスタンス 1 と、VIP による業務通信をできるようにする例を次の図に示します。

図 4-6 複数のリージョン間で系切り替えをする構成での VIP のルーティングの動作例



VIP のルーティングの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. ルートテーブル (VPC2) に、VIP のエントリを追加する。  
ターゲットをトランジットゲートウェイ 2 (tgw-R2) とする VIP のエントリを追加します。

表 4-3 ルートテーブル (VPC2) の内容

| Destination          | Target |
|----------------------|--------|
| VIP (10.10.10.10/32) | tgw-R2 |

これによって、VIP 宛での業務通信がトランジットゲートウェイ 2 (tgw-R2) に転送されます。

2. トランジットゲートウェイルートテーブル (tgw-R2) に、VIP のエントリを追加する。  
ターゲットをピアリング用のトランジットゲートウェイアタッチメント (tgw-attach-P) とする VIP のエントリを追加します。

表 4-4 トランジットゲートウェイルートテーブル (tgw-R2) の内容

| Destination          | Target       |
|----------------------|--------------|
| VIP (10.10.10.10/32) | tgw-attach-P |

これによって、VIP 宛ての業務通信がピアリングしているトランジットゲートウェイ 1 (tgw-R1) に転送されます。

- トランジットゲートウェイルートテーブル (tgw-R1) に、VIP のエントリを追加する。  
ターゲットを VPC1 のトランジットゲートウェイアタッチメント (tgw-attach-VPC1) とする VIP のエントリを追加します。

表 4-5 トランジットゲートウェイルートテーブル (tgw-R1) の内容

| Destination          | Target          |
|----------------------|-----------------|
| VIP (10.10.10.10/32) | tgw-attach-VPC1 |

これによって、VIP 宛ての業務通信が VPC1 (tgw-attach-VPC1) に転送されます。

- ルートテーブル (VPC1) に、VIP のエントリを追加する。  
ターゲットを ENI (eni-xxxx) とする VIP のエントリを追加します。

表 4-6 ルートテーブル (VPC1) の内容

| Destination          | Target   |
|----------------------|----------|
| VIP (10.10.10.10/32) | eni-xxxx |

これによって、VIP 宛ての業務通信が ENI1 (eni-xxxx) に転送されます。

上記の一連の動作によって、クライアントインスタンス 1 およびクライアントインスタンス 2 から VIP アドレス (10.10.10.10/32) を使用して、サーバーインスタンス 1 にアクセスできるようになります。

## (b) 系切り替え時の動作

HA モニタは、次の動作によって業務通信を切り替えます。

- AWS 上でのルートテーブルおよびトランジットゲートウェイルートテーブルの書き換え
- OS 上での VIP の追加・削除

### メモ

処理が完了するのに掛かる時間は、次の点によって変わります。

- 操作する VIP の数
- 操作するルートテーブルの数
- 操作するトランジットゲートウェイルートテーブルの数

VIP による業務通信を実行系から待機系に切り替えるには、次の 2 段階の動作があります。

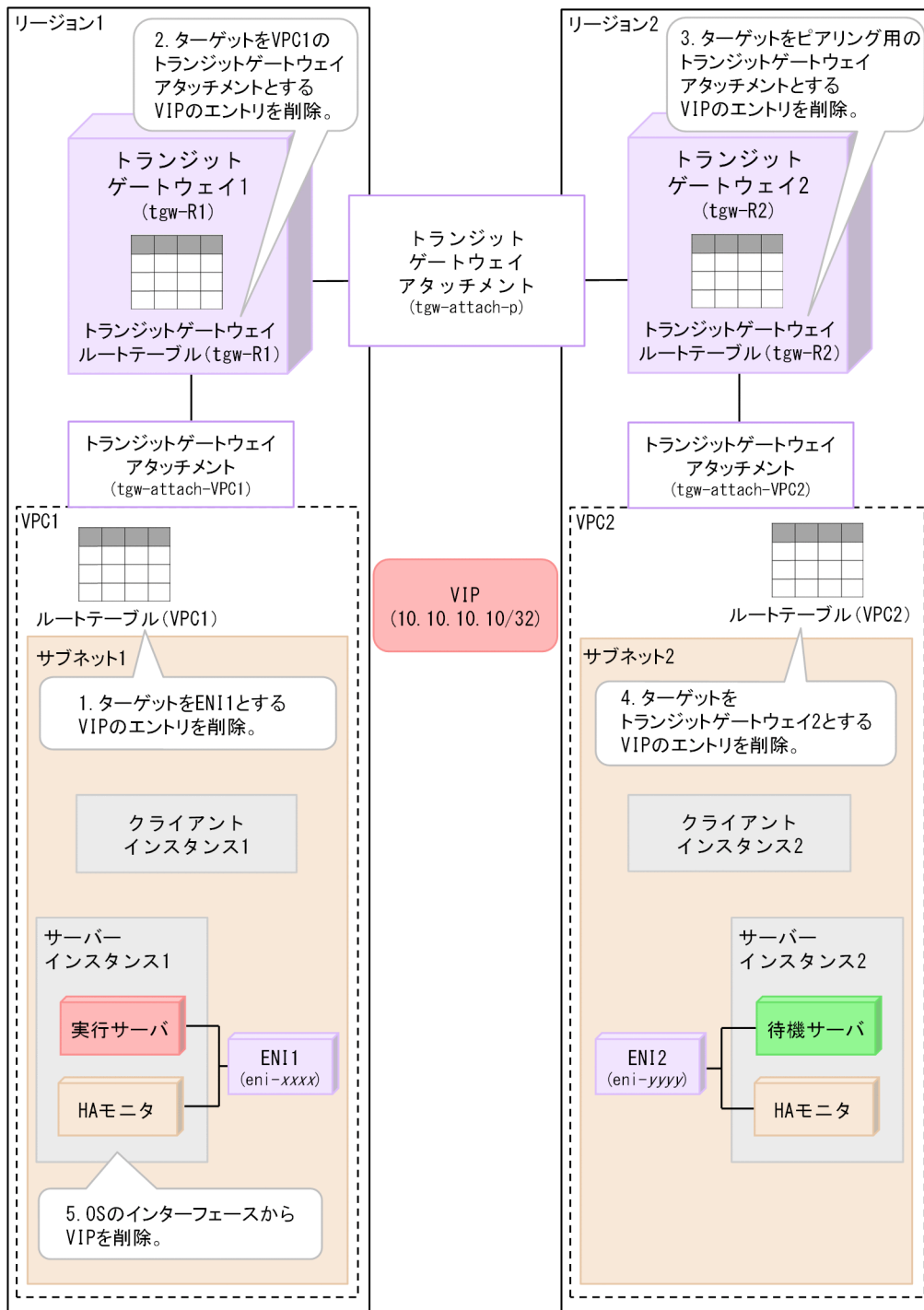
- 実行サーバ側のサーバーインスタンスを指すルーティング情報の削除、および OS 上での VIP の削除
- 待機サーバ側のサーバーインスタンスを指すルーティング情報の追加、OS 上での VIP の追加、および系切り替え

これらの 2 つの段階に分けて、実行サーバ側のサーバーインスタンスから待機サーバ側のサーバーインスタンスに、VIP による業務通信を切り替える動作を説明します。

実行サーバ側のサーバーインスタンスを指すルーティング情報の削除、および OS 上での VIP の削除

実行サーバ側のサーバーインスタンスを指すルーティング情報を削除し、OS 上で VIP を削除する動作を次の図に示します。

図 4-7 実行サーバ側のサーバーインスタンスを指すルーティング情報を削除し、OS 上で VIP を削除する動作



実行サーバ側のサーバーインスタンスを指すルーティング情報を削除し、OS 上で VIP を削除する動作は、次のとおりです。番号は、図中の番号と対応しています。

1. ルートテーブル (VPC1) から、VIP のエントリを削除する。  
ターゲットを ENI1 (eni-xxxx) とする VIP のエントリを削除します。

表 4-7 ルートテーブル (VPC1) の内容

| Destination | Target |
|-------------|--------|
| (空白)        | (空白)   |

2. トランジットゲートウェイルートテーブル (tgw-R1) から、VIP のエントリを削除する。  
ターゲットを VPC1 のトランジットゲートウェイアタッチメント (tgw-attach-VPC1) とする VIP のエントリを削除します。

表 4-8 トランジットゲートウェイルートテーブル (tgw-R1) の内容

| Destination | Target |
|-------------|--------|
| (空白)        | (空白)   |

3. トランジットゲートウェイルートテーブル (tgw-R2) から、VIP のエントリを削除する。  
ターゲットをピアリング用のトランジットゲートウェイアタッチメント (tgw-attach-P) とする VIP のエントリを削除します。

表 4-9 トランジットゲートウェイルートテーブル (tgw-R2) の内容

| Destination | Target |
|-------------|--------|
| (空白)        | (空白)   |

4. ルートテーブル (VPC2) から、VIP のエントリを削除する。  
ターゲットをトランジットゲートウェイ 2 (tgw-R2) とする VIP のエントリを削除します。

表 4-10 ルートテーブル (VPC2) の内容

| Destination | Target |
|-------------|--------|
| (空白)        | (空白)   |

5. OS のネットワークインタフェースから VIP を削除する。  
実行サーバ側のサーバーインスタンスで OS の ip コマンドを使用して、VIP を削除します。

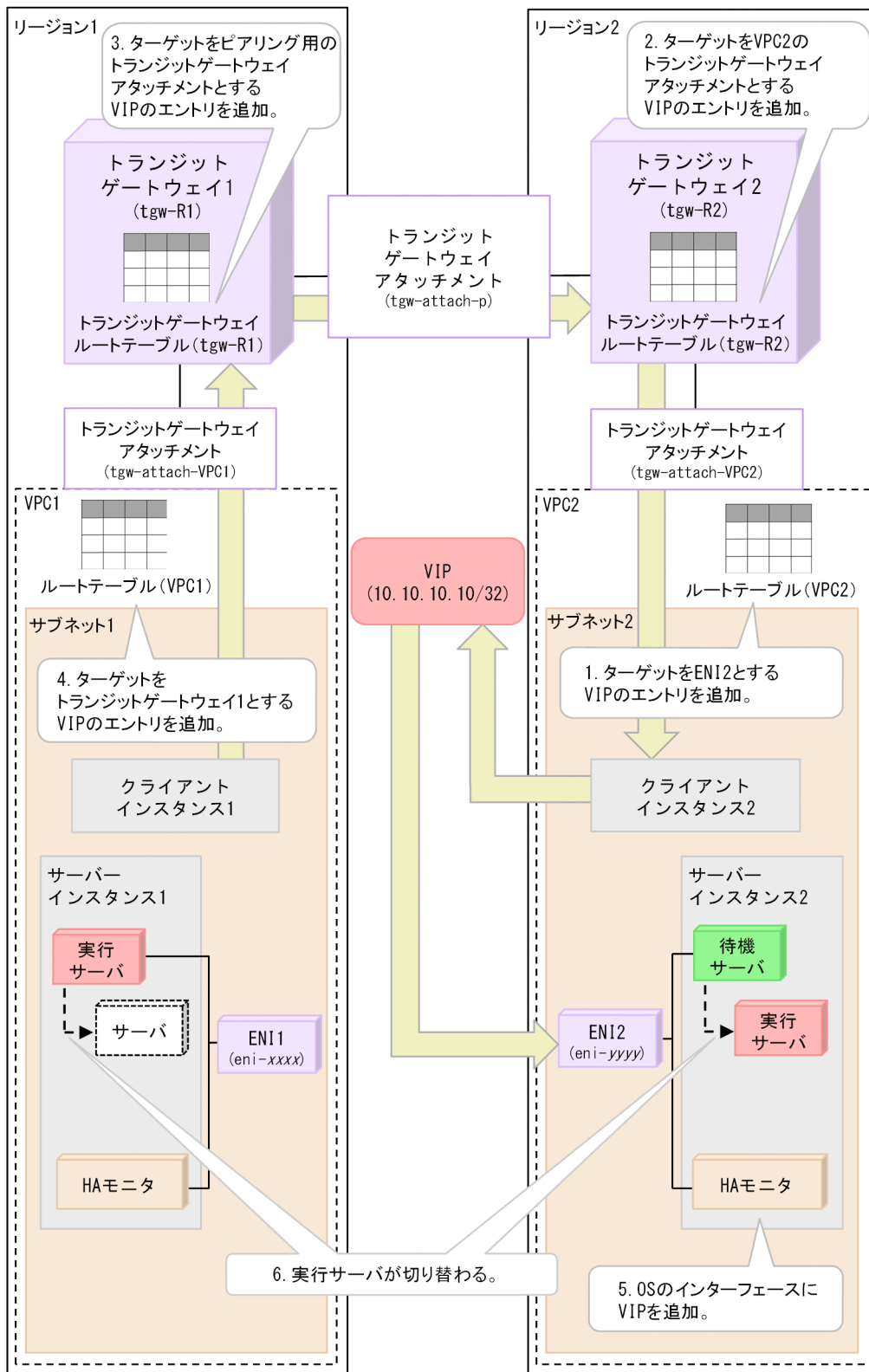
#### メモ

同一の VPC 内の複数の AZ 間で系切り替えをするときは、系切り替えをする VPC 外のルーティング情報を変更しません。

待機サーバ側のサーバーインスタンスを指すルーティング情報の追加、OS 上での VIP の追加、および系切り替え

待機サーバ側のサーバーインスタンスを指すルーティング情報の追加、および OS 上での VIP の追加をして、系切り替えをする動作を次の図に示します。

図 4-8 待機サーバ側のサーバーインスタンスを指すルーティング情報の追加, および OS 上での VIP の追加をして, 系切り替えをする動作



待機サーバ側のサーバーインスタンスを指すルーティング情報の追加, および OS 上での VIP の追加をして, 系切り替えをする動作は, 次のとおりです。番号は, 図中の番号と対応しています。

1. ルートテーブル (VPC2) に, VIP のエントリを追加する。



ターゲットを ENI2 (eni-yyyy) とする VIP のエントリを追加します。

表 4-11 ルートテーブル (VPC2) の内容

| Destination          | Target   |
|----------------------|----------|
| VIP (10.10.10.10/32) | eni-yyyy |

これによって、VIP 宛ての業務通信が ENI2 (eni-yyyy) に転送されます。

2. トランジットゲートウェイルートテーブル (tgw-R2) に、VIP のエントリを追加する。  
ターゲットを VPC2 のトランジットゲートウェイアタッチメント (tgw-attach-VPC2) とする VIP のエントリを追加します。

表 4-12 トランジットゲートウェイルートテーブル (tgw-R2) の内容

| Destination          | Target          |
|----------------------|-----------------|
| VIP (10.10.10.10/32) | tgw-attach-VPC2 |

これによって、VIP 宛ての業務通信が VPC2 に転送されます。

3. トランジットゲートウェイルートテーブル (tgw-R1) に、VIP のエントリを追加する。  
ターゲットをピアリング用のトランジットゲートウェイアタッチメント (tgw-attach-P) とする VIP のエントリを追加します。

表 4-13 トランジットゲートウェイルートテーブル (tgw-R1) の内容

| Destination          | Target       |
|----------------------|--------------|
| VIP (10.10.10.10/32) | tgw-attach-P |

これによって、VIP 宛ての業務通信がピアリングしているトランジットゲートウェイ 1 (tgw-R1) に転送されます。

4. ルートテーブル (VPC1) に、VIP のエントリを追加する。  
ターゲットをトランジットゲートウェイ 1 (tgw-R1) とする VIP のエントリを追加します。

表 4-14 ルートテーブル (VPC1) の内容

| Destination          | Target |
|----------------------|--------|
| VIP (10.10.10.10/32) | tgw-R1 |

これによって、VIP 宛ての業務通信がトランジットゲートウェイ 1 (tgw-R1) に転送されます。

5. OS のネットワークインタフェースに VIP を追加する。  
待機サーバ側のサーバーインスタンスで OS の ip コマンドを使用して、VIP を追加します。
6. 実行サーバが切り替わる。

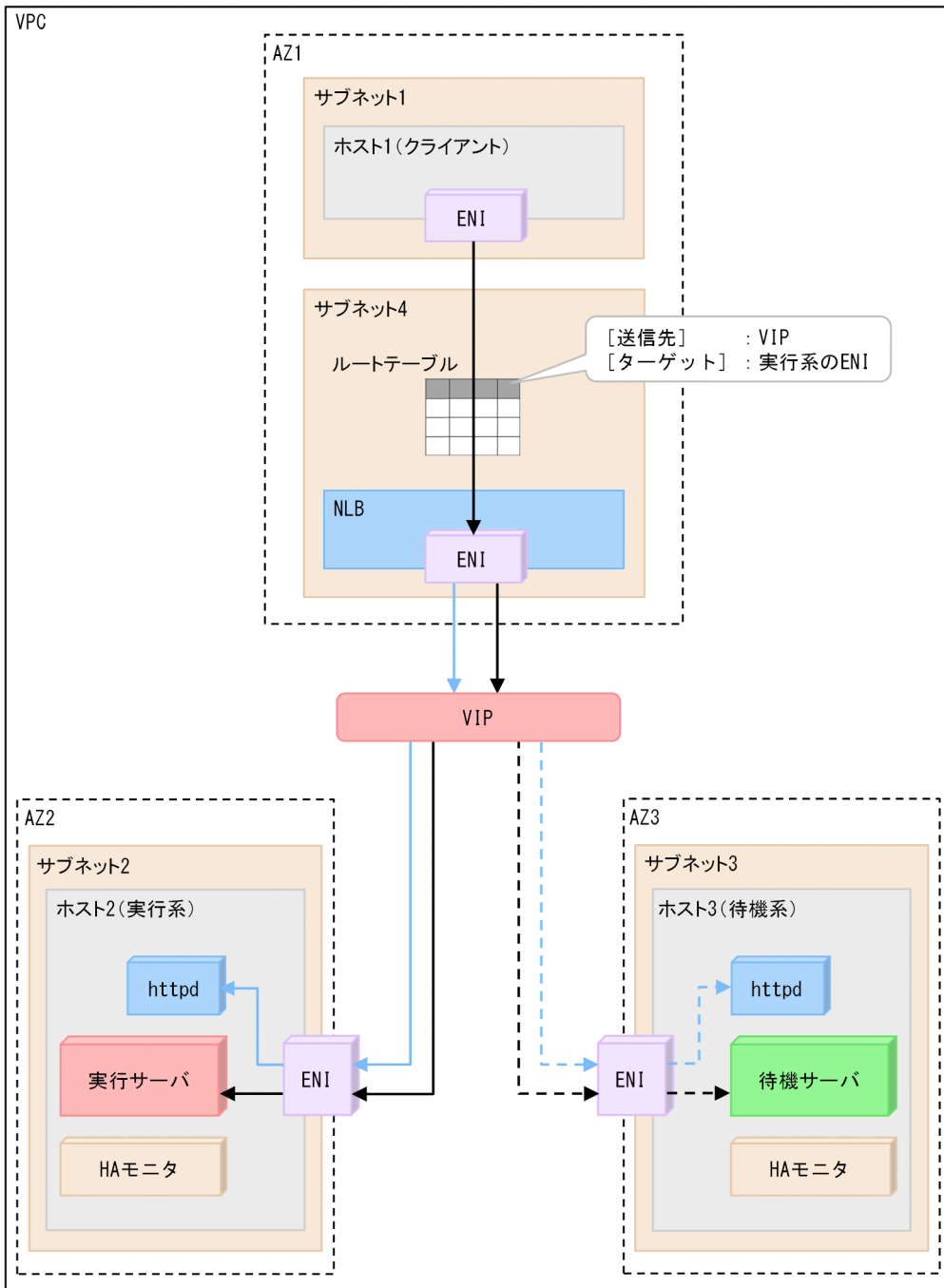
上記の 2 段階の動作によって、VIP による業務通信が実行サーバ側のサーバーインスタンスから、待機サーバ側のサーバーインスタンスに切り替わります。

### (3) VIP 制御による業務通信の切り替え（クライアントからの通信が NLB を経由する構成の場合）

クライアントが NLB を経由して VIP に通信する構成での、VIP 制御による業務通信の切り替えについて説明します。NLB 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。

クライアントが NLB を経由して VIP に通信する構成の例を次の図に示します。

図 4-9 クライアントが NLB を経由して VIP に通信する構成の例



(凡例)

- : クライアントから実行サーバへの通信
- - -> : → のフェールオーバー後の通信経路
- (blue) : NLBのヘルスチェック(httpdのポート番号を指定)
- - -> (blue) : → のフェールオーバー後の通信経路

この構成では、次の設定をしてください。

- NLB によるトラフィックの転送先に VIP を設定してください。設定する VIP は、NLB の設定の「リスナー」タブにある転送先ターゲットグループで設定してください。

- NLB のヘルスチェック関連のパラメタに任意の値を設定してください。
- NLB のヘルスチェックを受け取るhttpd は、OS 起動時または実行サーバ起動時に起動するように設定してください。
- LAN の状態設定ファイルを設定してください。設定方法の詳細は「[5.13.4 【AWS】 LAN の状態設定ファイルの設定（クライアントからの通信が NLB を経由する構成の場合）](#)」を参照してください。

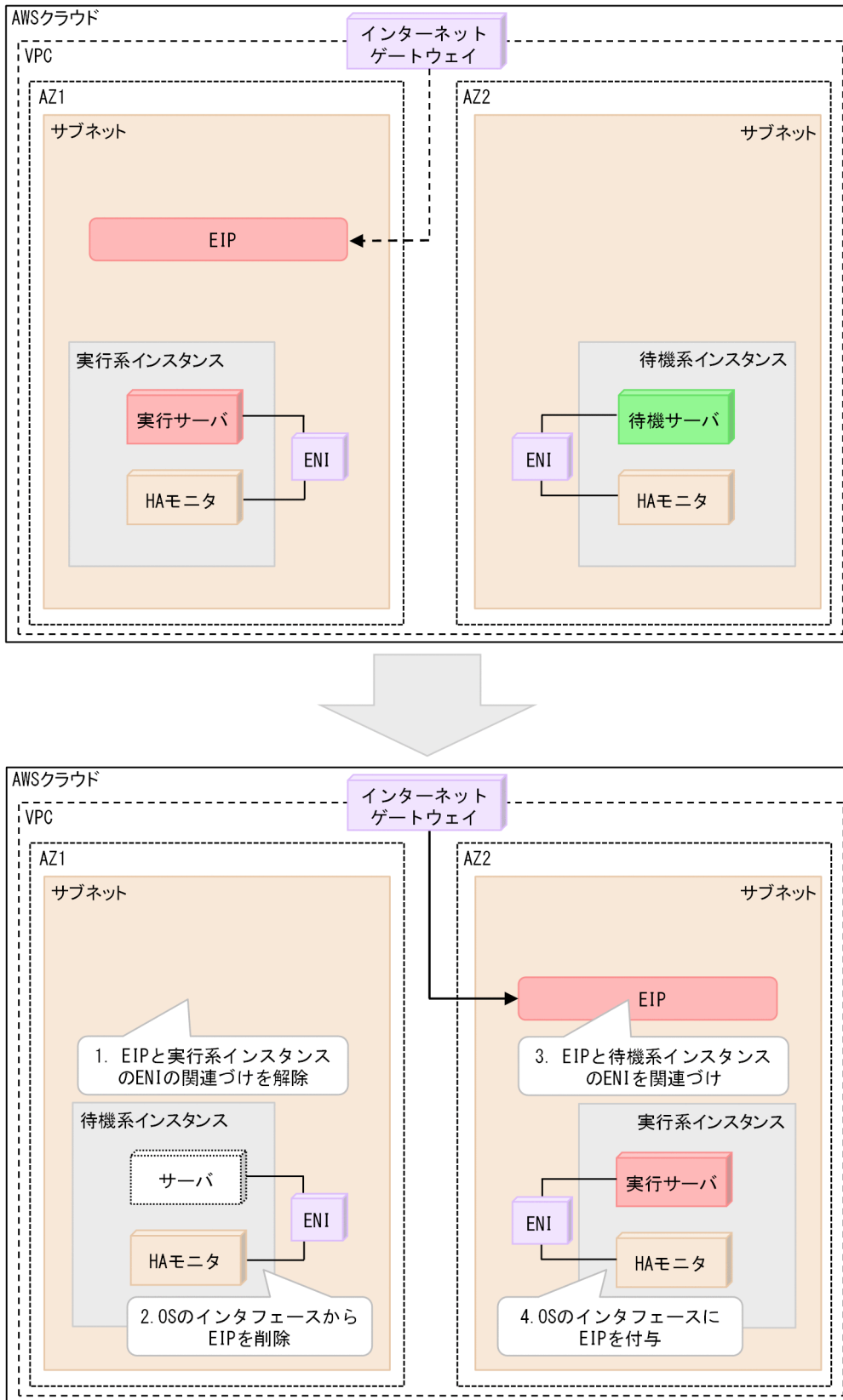
## (4) EIP 制御による業務通信の切り替え

EIP（Elastic IP アドレス）制御による業務通信の切り替えについて説明します。

AWS 上での操作による EIP の付け替え、および OS での EIP の付与・削除によって業務通信を切り替えます。

実行系インスタンスから待機系インスタンスに EIP を切り替える場合の動作例について次の図に示します。

図 4-10 EIP 制御による業務通信の切り替えの動作例



切り替え前は、EIPは実行系インスタンスのENIに関連づけられています。

EIP制御による業務通信の切り替えの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. HA モニタは、AWS CLI で、EIP と実行系インスタンスの ENI の関連づけを解除する。
2. HA モニタは、実行系インスタンスで、OS の ip コマンドを実行することによって、ネットワークインタフェースから EIP を削除する。
3. HA モニタは、AWS CLI で、EIP と待機系インスタンスの ENI の関連づけをする。
4. HA モニタは、待機系インスタンスで、OS の ip コマンドを実行することによって、ネットワークインタフェースに EIP を付与する。

これらの処理をするために、LAN の状態設定ファイルを設定する必要があります。LAN の状態設定ファイルについては、「5.13.2 **【AWS】 LAN の状態設定ファイルの設定 (1 つのリージョン内または 1 つの VPC 内で系切り替えをする構成の場合)**」を参照してください。

## (5) DNS 名制御による業務通信の切り替え

DNS 名制御による業務通信の切り替えについて説明します。

Amazon Route 53 のホストゾーンに登録しているレコードを変更することによって、業務通信を切り替えます。

### ❗ 重要

ホストゾーンは、事前に作成する必要があります。関連づけた VPC にだけレコードを公開する場合は、プライベートホストゾーンを作成してください。インターネットにレコードを公開する場合は、パブリックホストゾーンを作成してください。

ホストゾーンの作成方法の詳細については、AWS のドキュメントを参照してください。

レコードの変更方法は、次のどちらかを選択してください。

- レコードを更新する方法
- レコードを削除したあとレコードを更新する方法

それぞれの方法の詳細について、次の表に示します。

表 4-15 Amazon Route 53 のホストゾーンに登録しているレコードの変更方法

| 方法          | 系切り替え元による処理 | 系切り替え先による処理 | 実行サーバ停止時のレコードの状態 | 実行サーバ停止時のクライアントからの通信  |
|-------------|-------------|-------------|------------------|---|
| レコードを更新する方法 | なし          | レコードの更新     | 残る               | サーバが停止しているときもレコードが残っているため、クライアントからの DNS 名を使用した通信がインスタンスまで到達します。 |

| 方法                     | 系切り替え元による処理 | 系切り替え先による処理 | 実行サーバ停止時のレコードの状態 | 実行サーバ停止時のクライアントからの通信                                |
|------------------------|-------------|-------------|------------------|---|
| レコードを削除したあとレコードを更新する方法 | レコードの削除     | レコードの更新（追加） | 残らない             | サーバが停止しているときは、クライアントから DNS 名を使用した通信はインスタンスまで到達しません。 |

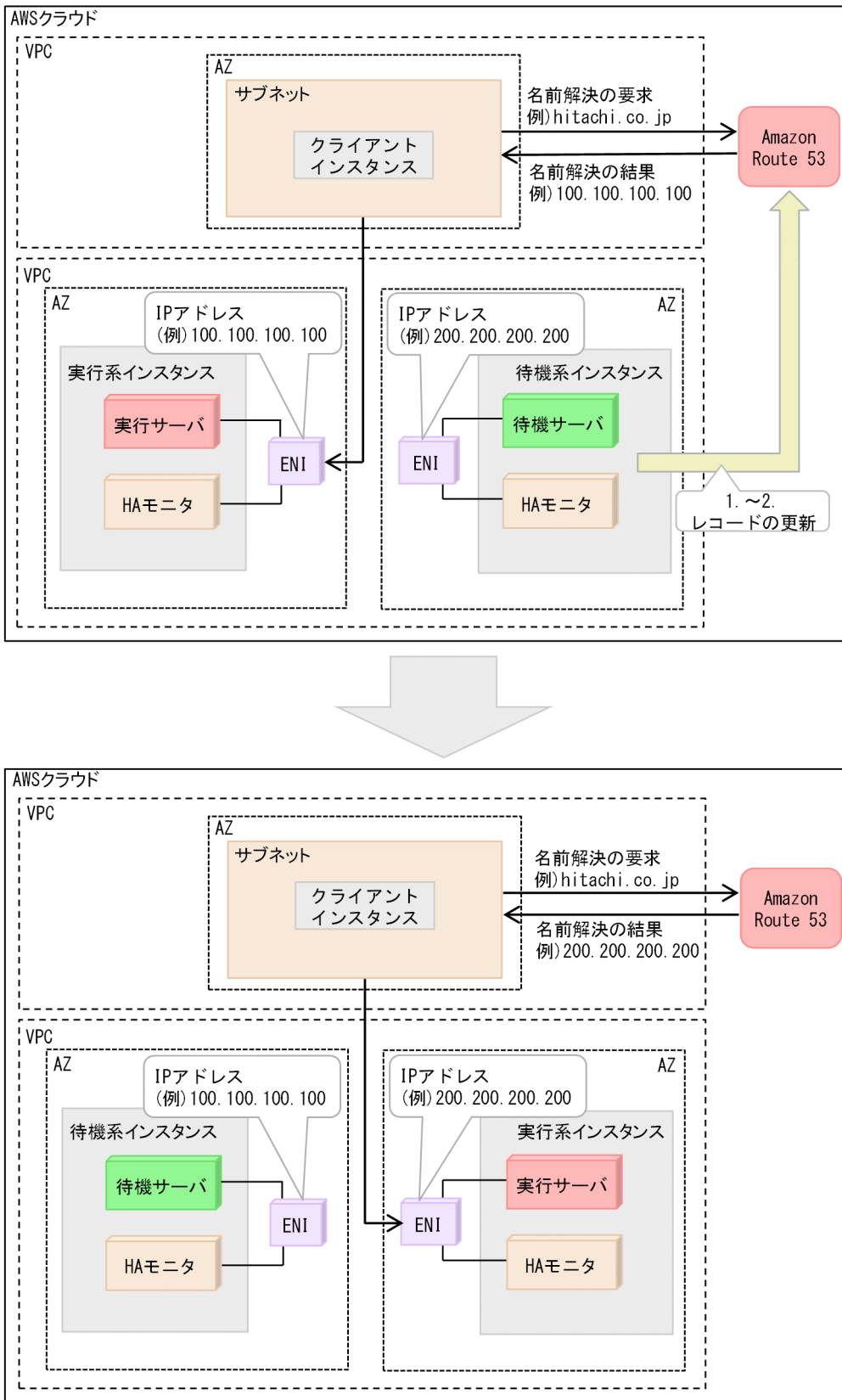
「レコードを更新する方法」より「レコードを削除したあとレコードを更新する方法」の方が、処理に時間が掛かります。そのため、「レコードを更新する方法」を推奨します。「実行サーバ停止時のクライアントからの通信」がシステム要件に合わない場合は、「レコードを削除したあとレコードを更新する方法」を選択してください。

それぞれの方法の処理の流れについて説明します。

#### レコードを更新する方法

レコードを更新する方法によって、業務通信を切り替える流れを次の図に示します。

図 4-11 レコードを更新する場合の動作例



変更前のレコードの例を次に示します。



表 4-16 変更前のレコード（レコードを更新する方法）

| Name                        | Type                   | Value  | TTL                    | 備考 |
|-----------------------------|------------------------|--|------------------------|----|
| DNS 名<br>(例: hitachi.co.jp) | DNS レコードタイプ<br>(例: A*) | 実行系インスタンスの<br>IP アドレス<br>(例:<br>100.100.100.100) | キャッシュ生存期間<br>(例: 60 秒) | -  |

(凡例)

-: 特にありません。

注※

この例では、IPv4 アドレスを記録する A レコードタイプを使用しています。

業務通信を切り替える動作を次に示します。番号は、図中の番号と対応しています。

1. レコードの更新を AWS CLI で要求する。
2. レコードの更新が完了したことを AWS CLI で確認する。

変更後のレコードの例を次に示します。

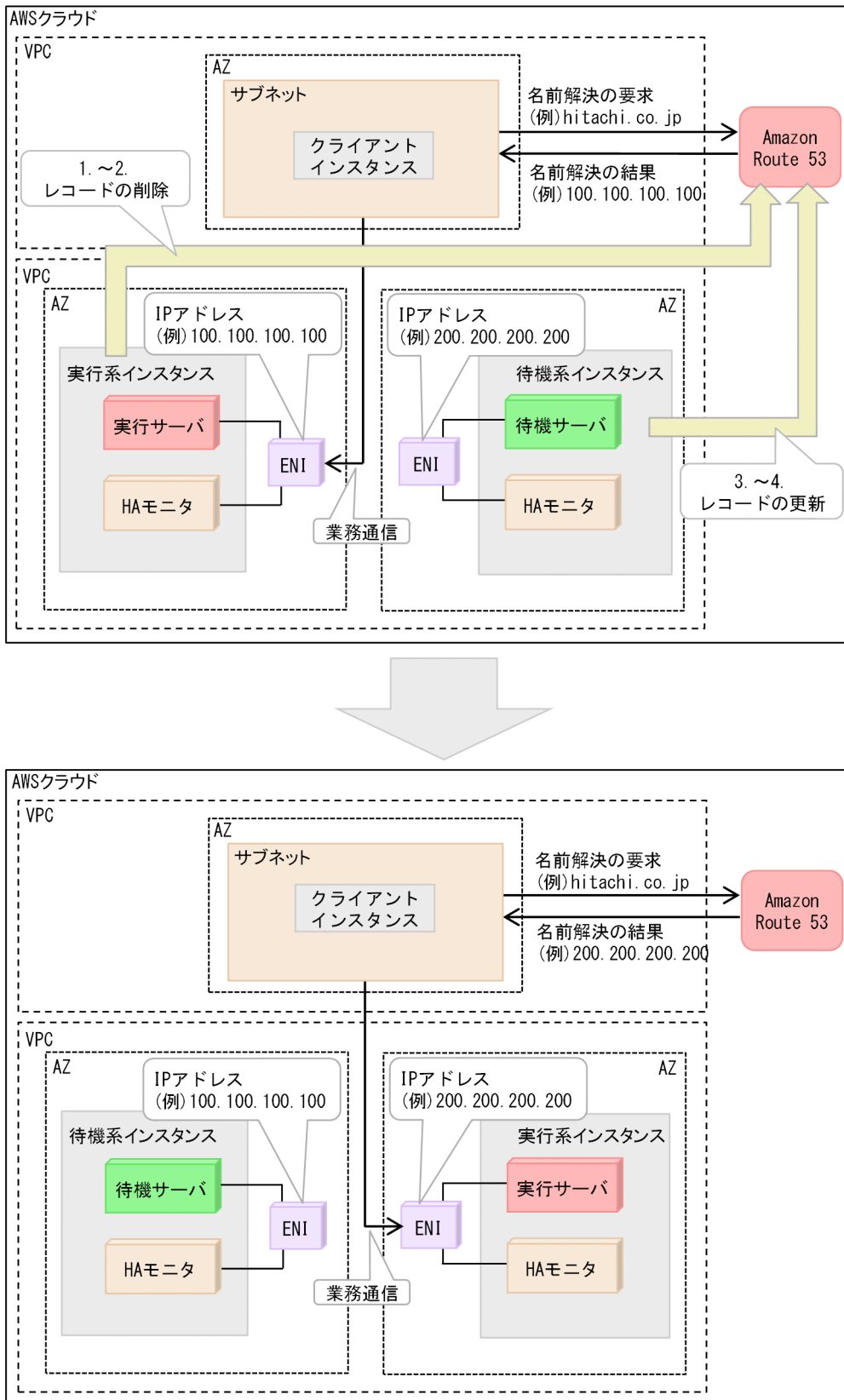
表 4-17 変更後のレコード（レコードを更新する方法）

| Name                        | Type                  | Value   | TTL                    | 備考 |
|-----------------------------|-----------------------|---|------------------------|----|
| DNS 名<br>(例: hitachi.co.jp) | DNS レコードタイプ<br>(例: A) | 実行系インスタンス<br>の IP アドレス<br>(例:<br>200.200.200.200) | キャッシュ生存期間<br>(例: 60 秒) | 更新 |

レコードを削除したあとレコードを更新する方法

レコードを削除したあとレコードを更新する方法によって、業務通信を切り替える流れを次の図に示します。

図 4-12 レコードを削除したあとレコードを更新する場合の動作例



変更前のレコードの例を次に示します。

表 4-18 変更前のレコード（レコードを削除したあとレコードを更新する方法）

| Name                       | Type                  | Value  | TTL                   | 備考 |
|----------------------------|-----------------------|--|-----------------------|----|
| DNS 名<br>(例：hitachi.co.jp) | DNS レコードタイプ<br>(例：A※) | 実行系インスタンスの<br>IP アドレス<br>(例：<br>100.100.100.100) | キャッシュ生存期間<br>(例：60 秒) | -  |

(凡例)

-：特にありません。

注※

この例では、IPv4 アドレスを記録する A レコードタイプを使用しています。

業務通信を切り替える動作を次に示します。番号は、図中の番号と対応しています。

1. レコードの削除を AWS CLI で要求する。
2. レコードの削除が完了したことを AWS CLI で確認する。

削除後のレコードの例を次に示します。

表 4-19 削除後のレコード（レコードを削除したあとレコードを更新する方法）

| Name | Type | Value | TTL  | 備考 |
|------|------|-------|------|----|
| (空白) | (空白) | (空白)  | (空白) | 削除 |

3. レコードの追加を AWS CLI で要求する。
4. レコードの追加が完了したことを AWS CLI で確認する。

追加後のレコードの例を次に示します。

表 4-20 追加後のレコード（レコードを削除したあとレコードを更新する方法）

| Name                       | Type                 | Value   | TTL                   | 備考 |
|----------------------------|----------------------|---|-----------------------|----|
| DNS 名<br>(例：hitachi.co.jp) | DNS レコードタイプ<br>(例：A) | 実行系インスタンス<br>の IP アドレス<br>(例：<br>200.200.200.200) | キャッシュ生存期間<br>(例：60 秒) | 追加 |

### ❗ 重要

- これらの処理をするために、LAN の状態設定ファイルを設定する必要があります。LAN の状態設定ファイルについては、「[5.13.2 【AWS】 LAN の状態設定ファイルの設定（1つのリージョン内または1つのVPC内で系切り替えをする構成の場合）](#)」を参照してください。

## 4.2.3 【Azure】 LAN の管理

クライアントから実行サーバへの通信を実現するために、HA モニタは次の制御をします。

OS でのエイリアス IP の追加・削除（DNS 名制御の場合を除く）

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「LAN の管理」を参照してください。ただし、Azure 環境下では次の点が異なります。

- OS のarping コマンドは実行不要※
- エイリアス IP を割り当てるとき、ブロードキャストアドレスは指定不可

注※

Azure での通信経路の制御によって、通信経路が定まるためです。

Azure での通信経路の制御

クライアントから実行サーバへ通信できるようにするために、HA モニタが業務通信経路の切り替えを制御します。次の表のとおり、クライアントからの通信方法によって、業務通信の切り替え方法を決定してください。

表 4-21 Azure 環境下の業務通信の切り替え方法

| クライアントからの通信方法         | 業務通信の切り替え方法                  |
|-----------------------|------------------------------|
| プライベート IP アドレスで通信する方法 | Azure ロードバランサー制御による業務通信の切り替え |
| パブリック IP アドレスで通信する方法  |                              |
| DNS 名で通信する方法          | DNS 名制御による業務通信の切り替え          |

次に、それぞれの通信経路の制御方式について説明します。

### (1) Azure ロードバランサー制御による業務通信の切り替え

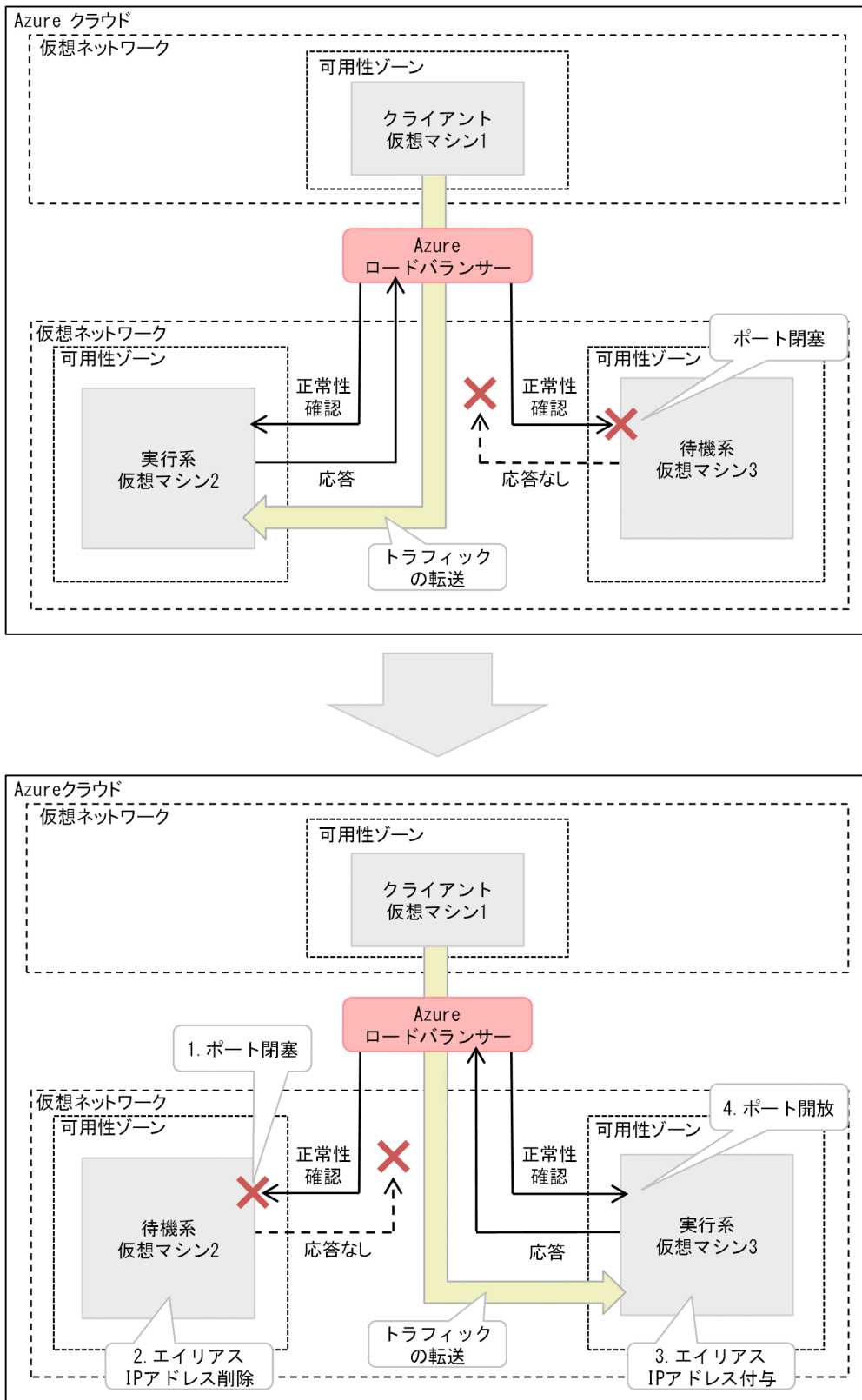
Azure ロードバランサー制御による業務通信の切り替えについて説明します。

Azure ロードバランサーには、関連づけた複数の仮想マシンにトラフィックを分散させる機能があります。Azure ロードバランサーは、特定のプロトコルおよびポートを使用して、一定時間ごとに仮想マシンの正常性確認を実行します。正常性確認に応答があった仮想マシンにトラフィックを転送し、応答がなかった仮想マシンにはトラフィックを転送しません。

HA モニタでは、実行系仮想マシンだけが正常性確認に応答するように制御することで、クライアントが実行サーバと通信できるようにします。

Azure ロードバランサー制御によって、業務通信を切り替える流れを次の図に示します。

図 4-13 Azure ロードバランサー制御による業務通信の切り替えの流れ



上記の図の系切り替え前は、仮想マシン 2 だけが Azure ロードバランサーからの正常性確認に回答します。そのため、仮想マシン 2 だけにトラフィックが転送されます。系切り替え後は、仮想マシン 3 だけが

Azure ロードバランサーからの正常性確認に応答します。そのため、仮想マシン 3 だけにトラフィックが転送されます。

Azure ロードバランサー制御による業務通信の切り替えの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. 実行系仮想マシンで正常性確認を待ち受けるポートを閉塞する。
2. 実行系仮想マシンの Linux のループバックインターフェイスから、エイリアス IP アドレス (Azure ロードバランサーの IP アドレス) を削除する。
3. 待機系仮想マシンの Linux のループバックインターフェイスに、エイリアス IP アドレス (Azure ロードバランサーの IP アドレス) を付与する。
4. 待機系仮想マシンで正常性確認を待ち受けるポートを開放する。

Azure ロードバランサー制御による業務通信の切り替えをするためには、LAN の状態設定ファイルを設定する必要があります。LAN の状態設定ファイルについては、「[5.13.5 【Azure】 LAN の状態設定ファイルの設定](#)」を参照してください。

## (2) DNS 名制御による業務通信の切り替え

DNS 名制御による業務通信の切り替えについて説明します。

Azure DNS に登録している記録を変更することによって、業務通信を切り替えます。この記録には、DNS 名と実行系仮想マシンの IP アドレスの対応が記載されています。

記録の変更方法は、次のどちらかを選択してください。

- 記録を更新する方法
- 記録を削除したあと記録を更新する方法

それぞれの方法の詳細について、次の表に示します。

表 4-22 Azure DNS に登録している記録の変更方法

| 方法                 | 系切り替え元による処理 | 系切り替え先による処理 | 実行サーバ停止時の記録の状態 | 実行サーバ停止時のクライアントからの通信  |
|--------------------|-------------|-------------|----------------|---|
| 記録を更新する方法          | なし          | 記録の更新       | 残る             | サーバが停止しているときも記録が残っているため、クライアントからの DNS 名を使用した通信がインスタンスまで到達します。 |
| 記録を削除したあと記録を更新する方法 | 記録の削除       | 記録の更新 (追加)  | 残らない           | サーバが停止しているときは、クライアントから DNS 名を使用した通信はインスタンスまで到達しません。           |

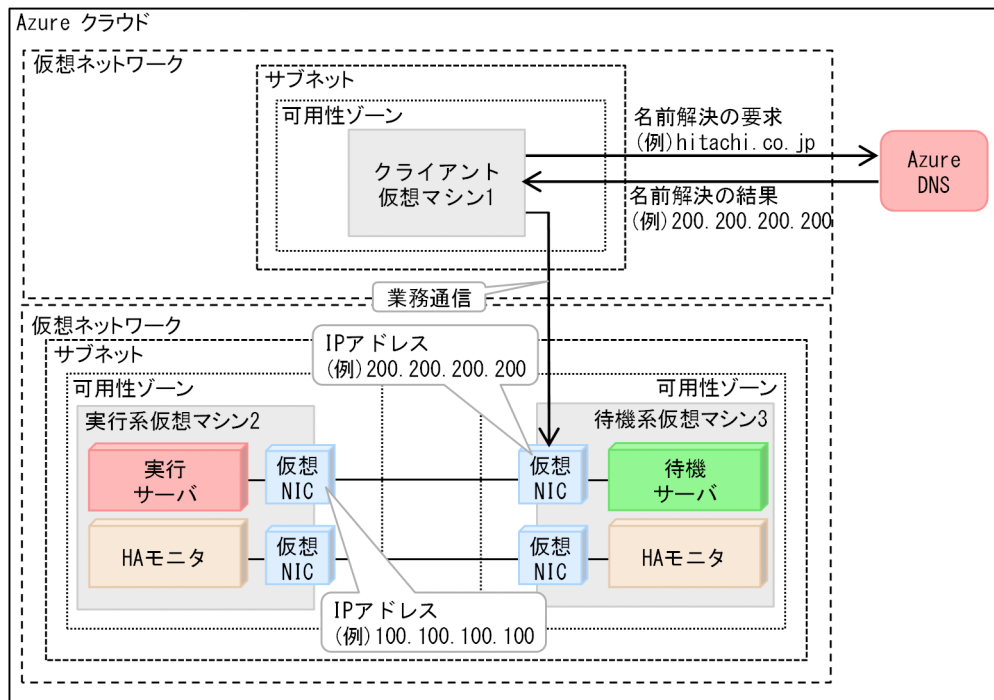
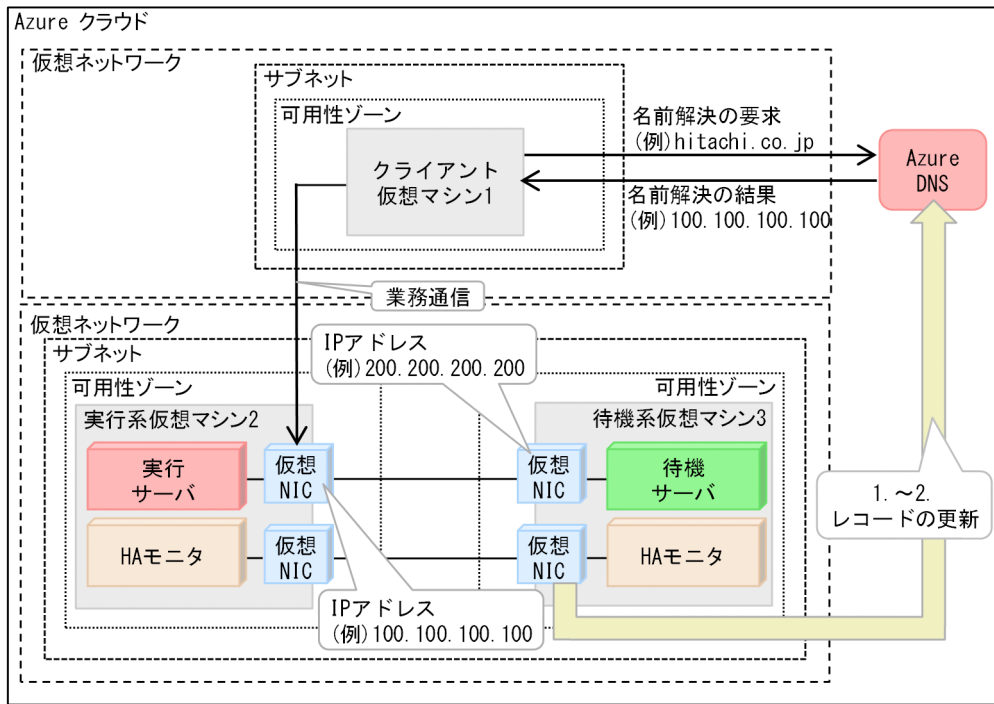
「レコードを更新する方法」より「レコードを削除したあとレコードを更新する方法」の方が、処理に時間が掛かります。そのため、「レコードを更新する方法」を推奨します。「実行サーバ停止時のクライアントからの通信」がシステム要件に合わない場合は、「レコードを削除したあとレコードを更新する方法」を選択してください。

それぞれの方法の処理の流れについて説明します。

#### レコードを更新する方法

レコードを更新する方法によって、業務通信を切り替える流れを次の図に示します。

図 4-14 レコードを更新する方法の動作例



図の例では、Azure DNS の DNS ゾーンに、DNS 名と仮想マシン 2 の IP アドレスとを対応させるレコードを登録します。これによって、クライアントから、DNS 名を使用した通信ができます。系切り替え時は、このレコードを、DNS 名と仮想マシン 3 の IP アドレスとを対応させるレコードに更新することによって、業務通信を切り替えます。

変更前のレコードの例を次に示します。



表 4-23 変更前のレコード (レコードを更新する方法)

| Name                        | Type                   | Value  | TTL                    | 備考 |
|-----------------------------|------------------------|--|------------------------|----|
| DNS 名<br>(例: hitachi.co.jp) | DNS レコードタイプ<br>(例: A*) | 実行系仮想マシン 2 の<br>IP アドレス<br>(例:<br>100.100.100.100) | キャッシュ生存期間<br>(例: 60 秒) | -  |

(凡例)

-: 特にありません。

注※

この例では、IPv4 アドレスを記録する A レコードタイプを使用しています。

図中の仮想マシン 2 から、仮想マシン 3 に系切り替えをするときの動作を次に示します。番号は、図中の番号と対応しています。

1. 新規のレコード追加を要求する。

新規 (更新しようとしている内容) のレコード追加を Azure CLI で要求します。

2. 新規のレコード追加を確認する。

新規 (更新しようとしている内容) のレコード追加が完了したことを Azure CLI で確認します。  
変更後のレコードの例を次に示します。

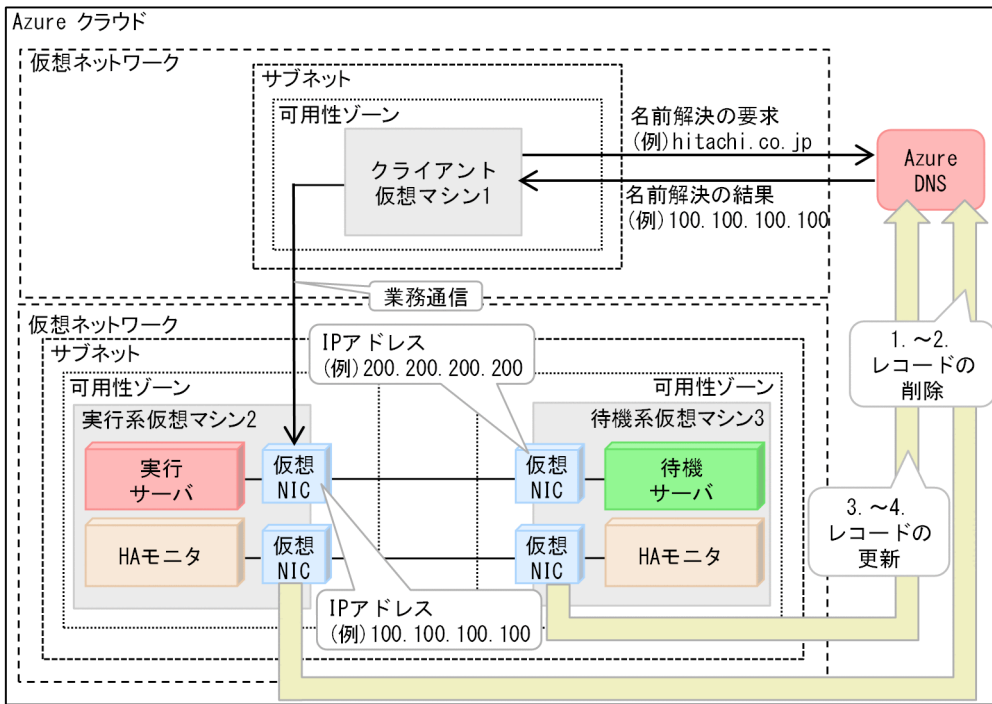
表 4-24 変更後のレコード (レコードを更新する方法)

| Name                        | Type                  | Value  | TTL                    | 備考 |
|-----------------------------|-----------------------|--|------------------------|----|
| DNS 名<br>(例: hitachi.co.jp) | DNS レコードタイプ<br>(例: A) | 実行系仮想マシン 3<br>の IP アドレス<br>(例:<br>200.200.200.200) | キャッシュ生存期間<br>(例: 60 秒) | 更新 |

レコードを削除したあとレコードを更新する方法

レコードを削除したあとレコードを更新する方法によって、業務通信を切り替える流れを次の図に示します。

図 4-15 レコードを削除したあとレコードを更新する方法の動作例



変更前のレコードの例を次に示します。

表 4-25 変更前のレコード（レコードを削除したあとレコードを更新する方法）

| Name                        | Type                   | Value  | TTL                    | 備考 |
|-----------------------------|------------------------|--|------------------------|----|
| DNS 名<br>(例: hitachi.co.jp) | DNS レコードタイプ<br>(例: A*) | 実行系仮想マシン 2 の<br>IP アドレス<br>(例:<br>100.100.100.100) | キャッシュ生存期間<br>(例: 60 秒) | -  |

(凡例)

-: 特にありません。

注※

この例では、IPv4 アドレスを記録する A レコードタイプを使用しています。

図中の仮想マシン 2 から、仮想マシン 3 に系切り替えをするときの動作を次に示します。番号は、図中の番号と対応しています。

1. レコードの削除を Azure CLI で要求する。
2. レコードの削除が完了したことを Azure CLI で確認する。

削除後のレコードの例を次に示します。

表 4-26 削除後のレコード（レコードを削除したあとレコードを更新する方法）

| Name | Type | Value | TTL  | 備考 |
|------|------|-------|------|----|
| (空白) | (空白) | (空白)  | (空白) | 削除 |

3. レコードの追加を Azure CLI で要求する。
4. レコードの追加が完了したことを Azure CLI で確認する。

変更後のレコードの例を次に示します。

表 4-27 変更後のレコード（レコードを削除したあとレコードを更新する方法）

| Name                        | Type                  | Value  | TTL                    | 備考 |
|-----------------------------|-----------------------|--|------------------------|----|
| DNS 名<br>(例: hitachi.co.jp) | DNS レコードタイプ<br>(例: A) | 実行系仮想マシン 3 の<br>IP アドレス<br>(例:<br>200.200.200.200) | キャッシュ生存期間<br>(例: 60 秒) | 更新 |

**!** 重要

- これらの処理をするために、LAN の状態設定ファイルを設定する必要があります。LAN の状態設定ファイルについては、「5.13.5 【Azure】LAN の状態設定ファイルの設定」を参照してください。

## 4.2.4 【OCI】 LAN の管理

クライアントから実行サーバへの通信を実現するために、HA モニタは次の制御をします。

### OS でのエイリアス IP の追加・削除

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「LAN の管理」を参照してください。ただし、OCI 環境下では次の点が異なります。

- OS のarping コマンドは実行不要※
- エイリアス IP を割り当てるとき、ブロードキャストアドレスは指定不可

### 注※

OCI での通信経路の制御によって、通信経路が定まるためです。

### OCI での通信経路の制御

クライアントから実行サーバへ通信できるようにするために、プライベート IP アドレスの制御によって業務通信を切り替えます。

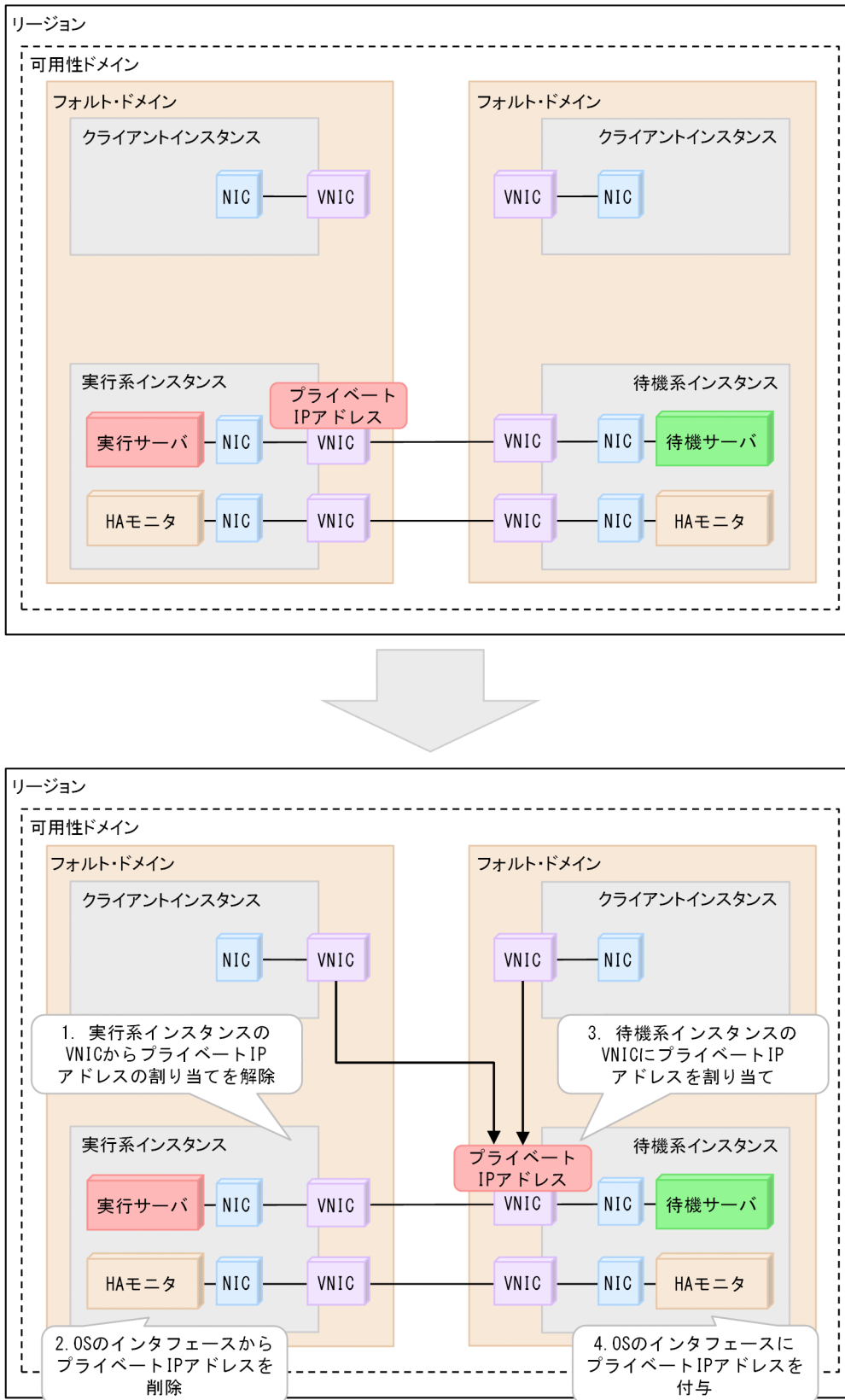
プライベート IP アドレス制御による業務通信の切り替えについて、次に説明します。

## (1) プライベート IP アドレス制御による業務通信の切り替え

OCI 上での操作によるプライベート IP アドレスの付け替え、および OS 上でのプライベート IP アドレスの付与・削除によって、業務通信を切り替えます。

プライベート IP アドレス制御によって、業務通信を切り替える流れを次の図に示します。

図 4-16 プライベート IP アドレス制御による業務通信の切り替えの流れ



プライベート IP アドレス制御による業務通信の切り替えの動作は、次のとおりです。番号は、図中の番号と対応しています。

1. HA モニタは、OCI CLI で、実行系インスタンスの VNIC からプライベート IP アドレスの割り当てを解除する。
2. HA モニタは、実行系インスタンスで、OS の ip コマンドを実行することによって、ネットワークインタフェースからプライベート IP アドレスを削除する。
3. HA モニタは、OCI CLI で、待機系インスタンスの VNIC にプライベート IP アドレスを割り当てる。
4. HA モニタは、待機系インスタンスで、OS の ip コマンドを実行することによって、ネットワークインタフェースにプライベート IP アドレスを付与する。

プライベート IP アドレス制御による業務通信の切り替えをするためには、LAN の状態設定ファイルを設定する必要があります。LAN の状態設定ファイルについては、[\[5.13.6 【OCI】 LAN の状態設定ファイルの設定\]](#) を参照してください。

## 4.3 【AWS】 処理の流れ

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「処理の流れ」を参照してください。ただし、AWS 環境下では、次の点が異なります。

実行サーバの起動時（系切り替え時も含む）

- ネットワークインタフェース状態設定前に、VIP 制御、EIP 制御または DNS 名制御によって業務の通信先を実行系にする。
- レプリケーション構成の場合、業務ディスクを参照+更新接続したあと、DRBD がディスクに対応する DRBD のリソースをプライマリに昇格させる。

実行サーバの停止時（サーバ障害などによる停止も含む）

- ネットワークインタフェース状態設定前に、VIP 制御、EIP 制御または DNS 名制御によって業務の通信先を削除する。
- レプリケーション構成の場合、業務ディスクを切り離れたあと、DRBD がディスクに対応する DRBD のリソースをセカンダリに降格させる。

系のリセット

ネットワーク遮断をする場合は、ネットワーク遮断とリセットをします。

## 4.4 【Azure】 処理の流れ

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「処理の流れ」を参照してください。ただし、Azure 環境下では、次の点が異なります。

実行サーバの起動時（系切り替え時も含む）

- ネットワークインタフェース状態設定前に、Azure ロードバランサー制御または DNS 名制御によって業務の通信先を実行系にする。
- レプリケーション構成の場合、業務ディスクを参照+更新接続したあと、DRBD がディスクに対応する DRBD のリソースをプライマリに昇格させる。

実行サーバの停止時（サーバ障害などによる停止も含む）

- ネットワークインタフェース状態設定前に、Azure ロードバランサー制御または DNS 名制御によって業務の通信先を削除する。
- レプリケーション構成の場合、業務ディスクを切り離れたあと、DRBD がディスクに対応する DRBD のリソースをセカンダリに降格させる。



## 4.5 【OCI】 処理の流れ

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「処理の流れ」を参照してください。ただし、OCI 環境下では、次の点が異なります。

実行サーバの起動時（系切り替え時も含む）

- ネットワークインタフェース状態設定前に、プライベート IP アドレス制御によって業務の通信先を実行系にする。

実行サーバの停止時（サーバ障害などによる停止も含む）

- ネットワークインタフェース状態設定前に、プライベート IP アドレス制御によって業務の通信先を削除する。

# 5

## システムの構築

HA モニタを組み込んだシステムの構築手順、HA モニタのディレクトリ構成、およびHA モニタのシステムの構築に必要な各設定について説明します。システムの構築は、スーパーユーザの権限で行ってください。この章では、システム構築の前提となるハードウェアはすでに構成されているものとして説明します。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「システムの構築」とあわせてお読みください。

## 5.1 構築の流れ

---

構築の流れについては、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「構築の流れ」の説明を参照してください。この節では、構築の流れについて、パブリッククラウド環境下で差異がある事項だけを記載します。

### 5.1.1 系のリセットまたはネットワーク遮断をする場合

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系のリセットをする場合 (BladeSymphony または HA8000)」を参照してください。ただし、パブリッククラウド環境下では次の点が異なります。

- 「HA モニタで使用するための VMware ESXi の設定」は不要です。代わりに、次を設定します。

AWS を使用する方

[5.2 [【AWS】AWS の設定](#)] および [5.5 [【AWS】【Azure】レプリケーションソフト \(DRBD\) の設定](#)] をしてください。

Azure を使用する方

[5.3 [【Azure】Azure の設定](#)] および [5.5 [【AWS】【Azure】レプリケーションソフト \(DRBD\) の設定](#)] をしてください。

OCI を使用する方

[5.4 [【OCI】OCI の設定](#)] をしてください。

- 「リセットパスの設定」は不要です。

## 5.2 【AWS】 AWS の設定

AWS 環境下で HA モニタを使用する場合に、AWS で設定する事項について説明します。

### 5.2.1 AWS CLI のインストール・設定

HA モニタは、AWS CLI を実行して、業務通信の切り替えやインスタンスの強制停止を実施します。AWS CLI のインストールおよび設定について説明します。

Linux OS 上に AWS CLI をインストールします。HA モニタは AWS CLI を `/usr/bin/aws` で実行するため、インストールの際は、次のどちらかを実行してください。

- インストールパスを `/usr/bin` にする
- インストールパス `/bin/aws` へのシンボリックリンク `aws` を `/usr/bin` 配下に作成する

#### ❗ 重要

インスタンスの設定で、インスタンスメタデータサービスのバージョン 2 (IMDSv2) だけを有効にする場合は、IMDSv2 に対応したバージョン (1.16.287 以降) をインストールしてください。

インスタンスメタデータサービス (IMDS) の設定についての詳細は、AWS のドキュメントを参照してください。

なお、各インスタンスで TCP ポート 443 での HTTPS 通信ができるように設定してください。

また、インスタンスの `root` ユーザが次のアクションを実行できる必要があります。使用する通信制御の方式によって、必要なアクションは異なります。IAM ポリシーを適切に設定してください。

通信制御の方式に関係なく、共通に必要なアクション

```
ec2:Describe*
ec2:StartInstances
ec2:StopInstances
```

VIP 制御による業務通信の切り替えを使用する場合に必要なアクション

```
ec2:DeleteRoute
ec2:CreateRoute
ec2:CreateTransitGatewayRoute※
ec2:DeleteTransitGatewayRoute※
ec2:SearchTransitGatewayRoutes※
```

## 注※

複数のリージョン間または複数の VPC 間で系切り替えをする場合に必要です。

EIP 制御による業務通信の切り替えを使用する場合に必要なアクション

`ec2:AssociateAddress`

`ec2:DisassociateAddress`

DNS 名制御による業務通信の切り替えを使用する場合に必要なアクション

`Route 53:ListResourceRecordSets`

`Route 53:ChangeResourceRecordSets`

`Route 53:GetChange`

ネットワーク遮断をする場合に必要なアクション

`ec2:DetachNetworkInterface`

`ec2:AttachNetworkInterface`

業務ディスクとして EFS を使用する場合に必要なアクション

`elasticfilesystem:DescribeFileSystems`

AWS CLI のインストール方法および設定に関する詳細は、AWS のドキュメントを参照してください。

## 5.2.2 エンドポイントの設定

HA モニタをインストールしたインスタンスが EC2 サービスのエンドポイントに接続できるようにしてください。エンドポイントの設定に関する詳細は、AWS のドキュメントを参照してください。

## 5.2.3 インスタンスのメタデータ取得のための設定

HA モニタがインスタンスのメタデータを取得するため、次のとおりに設定してください。

- IP アドレス 169.254.169.254 にプロトコル HTTP でアクセスできるように設定する  
iptables など通信を制限する場合は、root ユーザのプロセスから IP アドレス 169.254.169.254 への通信を許可してください。
- インスタンスの設定で、インスタンスメタデータサービス (IMDS) を有効にする  
インスタンスメタデータサービス (IMDS) についての詳細は、AWS のドキュメントを参照してください。

## 5.2.4 プロキシを使用する場合の設定

HTTP および HTTPS 通信をプロキシ経由で実施する場合、HA モニタが CLI 通信およびメタデータの取得ができるように、次のように設定してください。

- HA モニタの Unit 設定ファイル `/usr/lib/systemd/system/HAmo-powercontrol.service` に、`HTTP_PROXY`、`HTTPS_PROXY` および `NO_PROXY` 環境変数を設定する  
プロキシおよび環境変数の詳細は、AWS のドキュメントを参照してください。なお、環境変数は小文字で指定する必要がある場合があります。環境に応じて適切に設定してください。

設定例を次に示します。太字部分を環境に応じて設定してください。

```
[Unit]
Description=HA Monitor(power control)
:
[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/bin/sh -c '/opt/hitachi/HAmo/bin/HApwon >/dev/null 2>&1'
ExecStop=/bin/sh -c '/opt/hitachi/HAmo/bin/HApwoff >/dev/null 2>&1'
Environment="HTTPS_PROXY=http://proxy.example.com:8080"
Environment="HTTP_PROXY=http://proxy.example.com:8080"
Environment="NO_PROXY=169.254.169.254"
: (以降省略)
```

## 5.2.5 ENI の設定

業務通信の切り替えに VIP 方式を使用する場合、ENI に付与されているプライベート IP アドレスとは異なる IP アドレスを宛先としたパケットが ENI に届きます。ENI のデフォルト設定では、無関係の宛先 IP アドレスのパケットは破棄されます。VIP 宛のパケットを各インスタンスが受け取れるように、各インスタンスの ENI の「送信元/送信先チェック」を無効化して、宛先が破棄されないようにしてください。

## 5.2.6 EBS マルチアタッチの設定

EBS マルチアタッチ機能を使用して現用系と待機系の間で業務ディスクを引き継ぐ構成（共有ディスク構成）にする場合、EBS マルチアタッチの設定をします。

EBS マルチアタッチを設定するには、EBS の作成画面で「ボリュームタイプ」に「Provisioned IOPS SSD (io2)」を選択し、「Multi-Attach」をチェックします。その後、作成した EBS を複数のインスタンスにアタッチします。

EBS マルチアタッチの設定に関する詳細は、AWS のドキュメントを参照してください。

## 5.2.7 EFS の設定

EFS を使用して現用系と待機系の間で業務ディスクを引き継ぐ構成（共有ディスク構成）にする場合、EFS の設定をします。

EFS を使用する場合に、必要な設定を次に示します。

#### ストレージクラス

- 複数の AZ 間でのクラスタ構成にする場合、ストレージクラスを「標準」に設定してください。データを、複数の AZ に、冗長化して保存できるようにするためです。
- 1 つの AZ 内でのクラスタ構成にする場合、任意の項目に設定してください。

#### インスタンスからのアクセス

- インスタンスからファイルシステムに、DNS 名でアクセスできるように設定してください。
- ネットワーク遮断による系切り替えをする場合、ファイルシステムへのアクセスに、プライマリ ENI を使用しないでください。
- アクセスする ENI 以外からの通信を許可しないように、EFS のセキュリティを設定してください。

## 5.3 【Azure】 Azure の設定

Azure 環境下で HA モニタを使用する場合に、Azure で設定する事項について説明します。

### 5.3.1 Azure CLI のインストール・設定

HA モニタは、Azure CLI を実行して、業務通信の切り替えやインスタンスの強制停止を実施します。Azure CLI のインストールおよび設定について、次に説明します。

- Azure CLI のインストール

Linux OS 上に Azure CLI をインストールします。Azure CLI のインストール方法に関する詳細は、Azure のドキュメントを参照してください。

- Azure CLI の設定

Azure CLI の設定に関する詳細は、Azure のドキュメントを参照してください。

HA モニタでは、HA モニタ専用のサービスプリンシパルを使用して、Azure リソースにアクセスします。そのため、サービスプリンシパルを作成する必要があります。

次の手順でサービスプリンシパルを作成してください。

1. サービスプリンシパルに割り当てるカスタムロールの作成

Azure は、Azure リソースに対してロールベースのアクセス制御を実施します。ロールは、Azure リソースへのアクセス許可の集合体を指し、ユーザに割り当てられます。

Azure リソースにアクセスするために、次のパスのアクセスを許可してください。

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/powerOff/action

また、DNS 名制御によって業務通信を切り替える場合、次のパスもアクセスを許可してください。

| DNS ゾーン   | レコードタイプ | 必要なアクセス許可  |
|-----------|---------|--|
| パブリックゾーン  | A       | Microsoft.Network/dnsZones/A/read<br>Microsoft.Network/dnsZones/A/write<br>Microsoft.Network/dnsZones/A/delete<br>Microsoft.Network/dnsZones/NS/read             |
|           | CNAME   | Microsoft.Network/dnsZones/CNAME/read<br>Microsoft.Network/dnsZones/CNAME/write<br>Microsoft.Network/dnsZones/CNAME/delete<br>Microsoft.Network/dnsZones/NS/read |
| プライベートゾーン | A       | Microsoft.Network/privateDnsZones/A/read<br>Microsoft.Network/privateDnsZones/A/write<br>Microsoft.Network/privateDnsZones/A/delete                              |



| DNS ゾーン | レコードタイプ | 必要なアクセス許可   |
|---------|---------|---|
|         | CNAME   | Microsoft.Network/privateDnsZones/<br>CNAME/read<br>Microsoft.Network/privateDnsZones/<br>CNAME/write<br>Microsoft.Network/privateDnsZones/<br>CNAME/delete |

上記のアクセス許可を持つ既定のロールを割り当てても問題ありませんが、HA モニタに上記以外のアクセス許可を与えないように、HA モニタ専用のロールを作成してサービスプリンシパルに割り当ててを推奨します。上記のアクセス許可がない場合は、仮想マシンの強制停止および業務通信の切り替えがエラーとなり、失敗します。

ロールやアクセス許可などの設定に関する詳細は、Azure のドキュメントを参照してください。

## 2. サービスプリンシパルの作成

HA モニタ専用のサービスプリンシパルを作成し、ロールとして「1.」で作成したカスタムロールを割り当ててください。

サービスプリンシパルのログイン認証方法として、証明書を設定してください。業務の稼働中に有効期限が切れないようにするため、証明書の有効期限には、業務の稼働期間より十分に長い期間を設定してください。有効期限が切れた場合は、サーバの起動や系切り替えなどに失敗するおそれがあります。

サービスプリンシパルの作成に関する詳細は、Azure のドキュメントを参照してください。

なお、サービスプリンシパルのアプリケーション ID、認証に使用する証明書の格納パス、およびテナント ID は、HA モニタの設定で使用します。HA モニタの設定については、「[5.12.2 【Azure】サービスプリンシパル情報設定ファイルの設定](#)」を参照してください。

## 5.3.2 インスタンスのメタデータ取得のための設定

HA モニタがインスタンスのメタデータを取得するため、次のとおりに設定してください。

- IP アドレス 169.254.169.254 にプロトコル HTTP でアクセスできるように設定する  
iptables など通信を制限する場合は、root ユーザのプロセスから IP アドレス 169.254.169.254 への通信を許可してください。

## 5.3.3 プロキシを使用する場合の設定

HTTP および HTTPS 通信をプロキシ経由で実施する場合、HA モニタが CLI 通信およびメタデータの取得ができるように、次のように設定してください。

- HA モニタの Unit 設定ファイル `/usr/lib/systemd/system/HAmn-powercontrol.service` に、`HTTP_PROXY`、`HTTPS_PROXY` および `NO_PROXY` 環境変数を設定する

プロキシおよび環境変数の詳細は、Azure のドキュメントを参照してください。なお、環境変数は小文字で指定する必要がある場合があります。環境に応じて適切に設定してください。

設定例を次に示します。太字部分を環境に応じて設定してください。

```
[Unit]
Description=HA Monitor(power control)
:
[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/bin/sh -c '/opt/hitachi/HAMon/bin/HApwon >/dev/null 2>&1'
ExecStop=/bin/sh -c '/opt/hitachi/HAMon/bin/HApwoff >/dev/null 2>&1'
Environment="HTTPS_PROXY=http://proxy.example.com:8080"
Environment="HTTP_PROXY=http://proxy.example.com:8080"
Environment="NO_PROXY=169.254.169.254"
: (以降省略)
```

### 5.3.4 Azure ロードバランサーの作成・設定

Azure ロードバランサーの制御によって業務通信の切り替えをする場合、Azure ロードバランサーの作成および設定をします。Azure ロードバランサーの作成および設定に関する詳細は、Azure のドキュメントを参照してください。

ここでは、HA モニタで必要な設定について説明します。次の設定をしてください。

- バックエンドプールの設定  
バックエンドプールに実行系仮想マシンおよび待機系仮想マシンを設定します。
- フロントエンド IP アドレス  
業務通信に使用する IP アドレスを Azure ロードバランサーに設定します。
- 正常性プローブ  
次の値を設定します。
  - プロトコル：TCP
  - ポート：ほかの用途で使用されていないポート番号
  - 間隔：5
  - 異常しきい値：2なお、業務通信に使用する IP アドレスが複数ある場合は、ポート番号が重複しないように複数の正常性プローブを作成してください。
- 負荷分散規則  
上記のフロントエンド IP アドレス、および正常性プローブで指定したポート番号を指定して作成します。業務通信が複数ある場合は、業務通信ごとに設定したフロントエンド IP アドレス、および正常性プローブで指定したポート番号を指定して、複数の規則を作成します。

各負荷分散規則では、フローティング IP (Direct Server Return) を有効に設定します。バックエンドの仮想マシンで稼働するサーバが、系切り替え前後で同じ IP アドレスで通信できるようにするためです。

なお、フロントエンド IP アドレス、および正常性プローブで指定したポート番号は、HA モニタにも設定します。HA モニタの設定については、「[5.13.5 【Azure】 LAN の状態設定ファイルの設定](#)」を参照してください。

### 5.3.5 Azure DNS の設定

DNS 名制御によって業務通信の切り替えをする場合、DNS ゾーンの作成および設定をしてください。詳細は、Azure のドキュメントを参照してください。

DNS ゾーン名、および DNS ゾーンを収容するリソースグループ名は、HA モニタの設定で使します。HA モニタの設定については、「[5.13.5 【Azure】 LAN の状態設定ファイルの設定](#)」を参照してください。

### 5.3.6 マネージドディスクの共有

マネージドディスクを複数の仮想マシンにアタッチすることで共有ディスク構成にできます。

マネージドディスクの共有については、Azure のドキュメントを参照してください。

## 5.4 【OCI】 OCI の設定

---

OCI 環境下で HA モニタを使用する場合に、OCI で設定する事項について説明します。

### 5.4.1 OCI CLI のインストール・設定

HA モニタは、OCI CLI を実行して、業務通信の切り替えやインスタンスの強制停止を実施します。OCI CLI のインストールおよび設定について説明します。

Linux OS 上に OCI CLI をインストールします。HA モニタは OCI CLI を `/root/bin/oci` で実行するため、OCI CLI は `/root/bin/oci` で実行できるように設定してください。

また、インスタンスの root ユーザが、系切り替え構成内のインスタンスおよび VNIC にアクセスします。次の IAM ポリシーを設定してください。

- Allow <subject> to use instances in <location>
- Allow <subject> to use vnics in <location>

上記以外の IAM ポリシーについては、ポリシー構文に従い、環境に合わせて適切に設定してください。

OCI CLI のインストール方法および設定に関する詳細は、OCI のドキュメントを参照してください。

### 5.4.2 インスタンスのメタデータ取得のための設定

HA モニタがインスタンスのメタデータを取得するため、次のとおりに設定してください。

- IP アドレス 169.254.169.254 にプロトコル HTTP でアクセスできるように設定する  
iptables など通信を制限する場合は、root ユーザのプロセスから IP アドレス 169.254.169.254 への通信を許可してください。
- インスタンスメタデータサービス (IMDS) のバージョン 1 を有効にする  
インスタンスメタデータサービス (IMDS) についての詳細は、OCI のドキュメントを参照してください。

### 5.4.3 プロキシを使用する場合の設定

HTTP および HTTPS 通信をプロキシ経由で実施する場合、HA モニタが CLI 通信およびメタデータの取得ができるように、次のように設定してください。

- HA モニタの Unit 設定ファイル `/usr/lib/systemd/system/HAmn-powercontrol.service` に、`HTTP_PROXY`、`HTTPS_PROXY` および `NO_PROXY` 環境変数を設定する

プロキシおよび環境変数の詳細は、OCI のドキュメントを参照してください。なお、環境変数は小文字で指定する必要がある場合があります。環境に応じて適切に設定してください。

設定例を次に示します。太字部分を環境に応じて設定してください。

```
[Unit]
Description=HA Monitor(power control)
:
[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/bin/sh -c '/opt/hitachi/HAMon/bin/HApwon >/dev/null 2>&1'
ExecStop=/bin/sh -c '/opt/hitachi/HAMon/bin/HApwoff >/dev/null 2>&1'
Environment="HTTPS_PROXY=http://proxy.example.com:8080"
Environment="HTTP_PROXY=http://proxy.example.com:8080"
Environment="NO_PROXY=169.254.169.254"
: (以降省略)
```

## 5.4.4 エンドポイントの設定

HA モニタをインストールしたインスタンスがコア・サービスのエンドポイントに接続できるようにしてください。エンドポイントの設定に関する詳細は、OCI のドキュメントを参照してください。

## 5.4.5 ブロック・ボリュームの設定

共有ディスクとして使用するブロック・ボリュームを、系切り替え構成のインスタンスにマルチアタッチしてください。このとき、アクセス「読み取り/書き込み - 共有可能」を選択してください。ボリュームグループ、lvm.conf、およびファイルシステムなどの設定は、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有ディスクの設定」を参照してください。

## 5.4.6 /etc/hosts ファイルの永続化

/etc/hosts ファイルに加えた変更内容を永続化するため、次の行を/etc/oci-hostname.conf に追加してください。

```
PRESERVE_HOSTINFO=2
```

詳細は OCI のドキュメントを参照してください。

## 5.5 【AWS】【Azure】レプリケーションソフト (DRBD) の設定

レプリケーションソフト (DRBD) を使用する場合に必要な設定について説明します。詳細については、DRBD のドキュメントを参照してください。

定義チェックコマンド (moncheck コマンド) による定義チェック前までに実施する設定

1. 業務ディスクを構成する DRBD 論理デバイスの作成
2. 作成した DRBD 論理デバイスを LVM の物理ボリューム (Physical volume) として、LVM のボリュームグループを構成

OS 起動時にレプリケーションソフト (DRBD) を自動起動する設定

OS の `systemctl` コマンドを実行して、サービスを有効化してください。

サービスの有効化方法を、次に示します。

```
# systemctl enable drbd
```

リソースの設定

次に示す項目は必ず設定してください。次に示す項目以外は環境に合わせて設定してください。

- ハンドラの設定  
common セクションの `fence-peer` ハンドラに、`/opt/hitachi/HAMon/bin/parts/monfence-peer.sh` を設定します。
- 自動プロモーション (auto-promote オプション)  
`yes` を指定します。
- 同期モード (protocol オプション)  
系切り替え時のデータの欠損を防止するため、プロトコル C の設定を推奨します。
- フェンシングの設定 (fencing オプション)  
`resource-and-stonith` を設定します。
- レプリケーションパスの設定 (address オプション)  
レプリケーションパスの IP アドレスを指定します。
- 対向ノード接続待ちの設定 (wfc-timeout オプション)  
DRBD 起動時に対向ノードと接続できるまで待機する時間を指定します。

レプリケーションソフト (DRBD) の設定例を次に示します。

`/etc/drbd.d/global_common.conf`

```
global {
    usage-count no;
}
common {
    handlers {
        fence-peer "/opt/hitachi/HAMon/bin/parts/monfence-peer.sh";
    }
    options {
```

```

    auto-promote yes;
  }
net {
  protocol C;
  fencing resource-and-stonith;
}
startup {
  wfc-timeout 30;
}
}

```

/etc/drbd.d/r0.res (リソース名:r0, 複数ボリュームグループがある場合)

```

resource r0 {
  volume 0 {
    device    /dev/drbd1;
    disk      /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_volXXXXX;※
    meta-disk internal;
  }
  volume 1 {
    device    /dev/drbd2;
    disk      /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_volYYYYY;※
    meta-disk internal;
  }
  on host1 {
    address   10.1.1.31:7789;
  }
  on host2 {
    address   10.1.2.32:7789;
  }
}

```

#### 注※

/dev 配下のデバイス名 (/dev/nvme1n1p1 など) は、OS のデバイス認識順によって変わる場合があります。そのため、認識順に関係なく、デバイスを一意に特定できる/dev/disk/by-id/下のシンボリックリンクファイル (実デバイス/dev/nvme1n1p1 などへのシンボリックリンクファイル) を指定することをお勧めします。

設定方法の詳細については、レプリケーションソフト (DRBD) のドキュメントを参照してください。

#### DRBD 用シェルスクリプト群の展開

DRBD のプライマリへの昇格を抑止するために、HA モニタは DRBD 用のシェルスクリプト群を提供しています。「[5.6 【AWS】【Azure】レプリケーションソフト \(DRBD\) 用のシェルスクリプト群の展開](#)」を参照し、シェルスクリプト群を展開してください。

#### サーバ対応の環境設定の定義

- 業務ディスクを構成するレプリケーションソフト (DRBD) のリソース名をサーバ対応の環境設定の rep\_device オペランドに指定します。  
rep\_device オペランドの詳細については、「[\(1\) rep\\_device](#)」を参照してください。
- 構成したボリュームグループをサーバ対応の環境設定の disk オペランドに指定します。  
disk オペランドの詳細は、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「サーバの環境設定」を参照してください。



## リソース制限の変更

ディスクをレプリケーションする構成で HA モニタを使用する場合、次の計算式で求められる値によっては、リソース制限を変更する必要があります。

「サーバ対応の環境設定の rep\_device オペランドに指定したリソースの合計（サーバ対応の環境設定全体の DRBD のリソース数）」×「接続する系の数 - 1」

上記の計算式の値に従って、次のとおりに対応してください。

- 計算式の値が 512 以下の場合：リソース制限の設定は変更不要です。
- 計算式の値が 512 を超える場合：計算式の値に 1,024 を加えた値を、HA モニタの Unit 設定ファイルの Service セクションの「LimitNOFILE」に指定します。

計算式の例を次に示します。

### 計算式の例

サーバ対応の環境設定の rep\_device オペランドに指定したリソースの合計が 250、接続する系の数が 5 の場合は、次のとおりになります。

$$250 \times (5 - 1) = 1,000$$
$$1,000 + 1,024 = 2,024$$

2,024 を LimitNOFILE に設定します。

リソース制限の設定例を次に示します。次のファイルの太字部分を変更してください。

/usr/lib/systemd/system/HAmom-powercontrol.service

```
[Unit]
Description=HA Monitor(power control)
After=sysinit.target network.target sshd.service jpl_base.service HABooster.service ltd.
service haconnd.service drbd.service

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/bin/sh -c '/opt/hitachi/HAmom/bin/HApwon >/dev/null 2>&1'
ExecStop=/bin/sh -c '/opt/hitachi/HAmom/bin/HApwoff >/dev/null 2>&1'
LimitNOFILE=2024

[Install]
WantedBy=multi-user.target
```

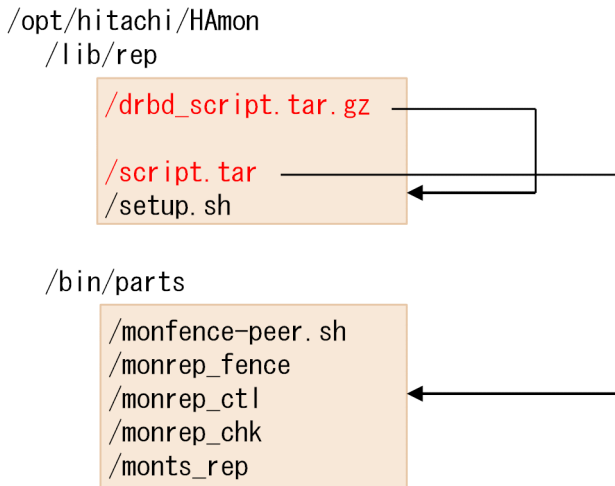


## 5.6 【AWS】【Azure】レプリケーションソフト (DRBD) 用のシェルスクリプト群の展開

レプリケーションソフト (DRBD) を使用するために、HA モニタが DRBD 用のシェルスクリプト群を提供しています。DRBD のプライマリへの昇格を抑止するために、DRBD 用のシェルスクリプト群を展開する必要があります。

DRBD 用のシェルスクリプト群の展開イメージを次の図で示します。

図 5-1 DRBD 用のシェルスクリプト群の展開イメージ



DRBD 用のシェルスクリプト群を次の手順で展開してください。操作は root ユーザーで実行してください。

1. tar コマンドで DRBD 用のシェルスクリプト群を展開する。

tar コマンドを実行したカレントディレクトリにファイルが展開されます。

```
# tar -zxvf /opt/hitachi/HAMon/lib/rep/drbd_script.tar.gz
./script.tar
./setup.sh
```

2. setup.sh を実行する。

必要なシェルスクリプト群が自動的に配置されます。なお、すでに展開されているレプリケーションソフト用のシェルスクリプト群がある場合は、自動的に削除されます。

```
# ./setup.sh
```

### 注意事項

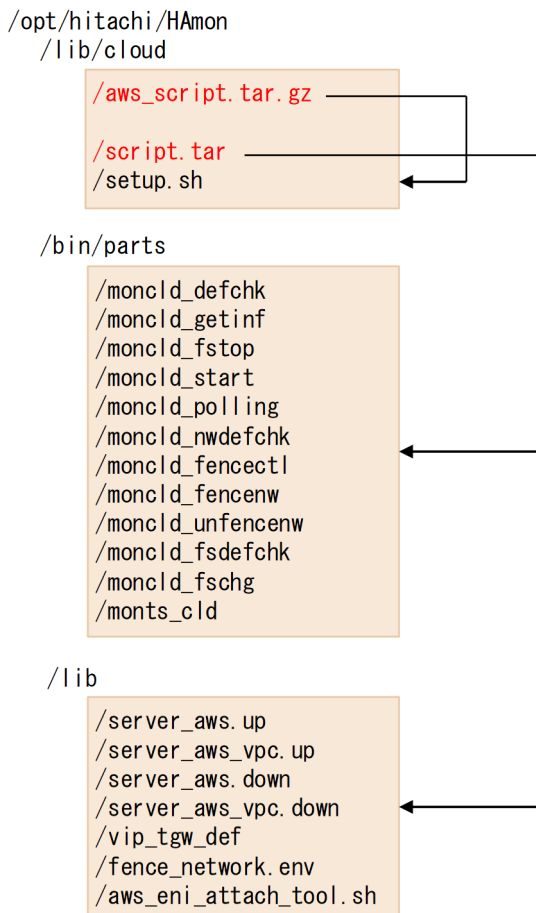
レプリケーション構成を含めずに共有ディスク構成だけで業務ディスクを制御する場合、DRBD 用のシェルスクリプト群を展開しないでください。

## 5.7 【AWS】 AWS用のシェルスクリプト群の展開

AWS CLI を操作をするために、HA モニタが AWS 用のシェルスクリプト群を提供しています。HA モニタのインストール後、「5.10 リセットパスの設定」から「5.14 リソースの監視のための設定」までの設定を実施する前に、AWS 用のシェルスクリプト群を展開する必要があります。

AWS 用のシェルスクリプト群の展開イメージを次の図で示します。

図 5-2 AWS 用のシェルスクリプト群の展開イメージ



AWS 用のシェルスクリプト群を次の手順で展開してください。操作はroot ユーザで実行してください。

1. tar コマンドで AWS 用のシェルスクリプト群を展開する。

tar コマンドを実行したカレントディレクトリにファイルが展開されます。

```
# tar -zxvf /opt/hitachi/HAMon/lib/cloud/aws_script.tar.gz
./script.tar
./setup.sh
```

2. setup.sh を実行する。

必要なシェルスクリプト群が自動的に配置されます。なお、すでに展開されているパブリッククラウド用のシェルスクリプト群がある場合は、自動的に削除されます。

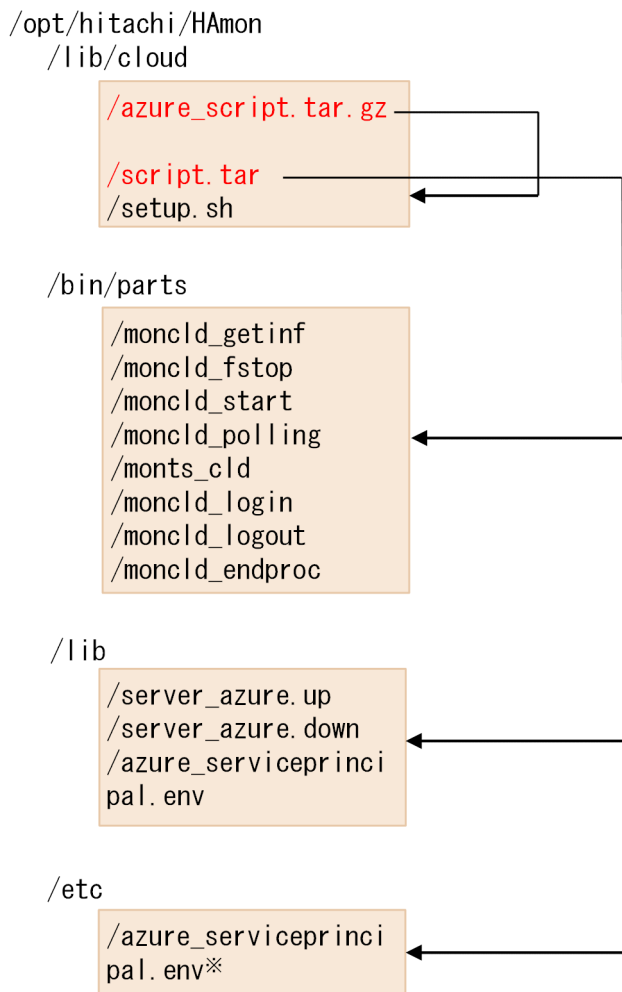
```
# ./setup.sh
```

## 5.8 【Azure】 Azure 用のシェルスクリプト群の展開

Azure CLI を操作するために、HA モニタが Azure 用のシェルスクリプト群を提供しています。HA モニタのインストール後、「5.10 リセットパスの設定」から「5.14 リソースの監視のための設定」までの設定を実施する前に、Azure 用のシェルスクリプト群を展開する必要があります。

Azure 用のシェルスクリプト群の展開イメージを次の図で示します。

図 5-3 Azure 用のシェルスクリプト群の展開イメージ



注※

このファイルが/etc 下がない場合だけ展開されます。

Azure 用のシェルスクリプト群を次の手順で展開してください。操作はroot ユーザで実行してください。

1. tar コマンドで Azure 用のシェルスクリプト群を展開する。

tar コマンドを実行したカレントディレクトリにファイルが展開されます。

```
# tar -zxvf /opt/hitachi/HAmom/lib/cloud/azure_script.tar.gz
./script.tar
./setup.sh
```

## 2. setup.sh を実行する。

必要なシェルスクリプト群が自動的に配置されます。なお、すでに展開されているパブリッククラウド用のシェルスクリプト群がある場合は、自動的に削除されます。

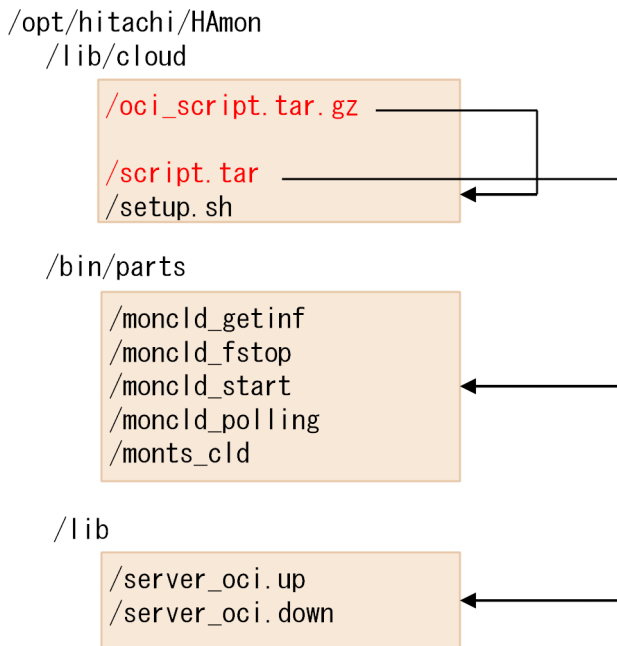
```
# ./setup.sh
```

## 5.9 【OCI】 OCI用のシェルスクリプト群の展開

OCI CLI を操作するために、HA モニタが OCI 用のシェルスクリプト群を提供しています。HA モニタのインストール後、「5.10 リセットパスの設定」から「5.14 リソースの監視のための設定」までの設定を実施する前に、OCI 用のシェルスクリプト群を展開する必要があります。

OCI 用のシェルスクリプト群の展開イメージを次の図で示します。

図 5-4 OCI 用のシェルスクリプト群の展開イメージ



OCI 用のシェルスクリプト群を次の手順で展開してください。操作はroot ユーザで実行してください。

1. tar コマンドで OCI 用のシェルスクリプト群を展開する。

tar コマンドを実行したカレントディレクトリにファイルが展開されます。

```
# tar -zxvf /opt/hitachi/HAMon/lib/cloud/oci_script.tar.gz
./script.tar
./setup.sh
```

2. setup.sh を実行する。

必要なシェルスクリプト群が自動的に配置されます。なお、すでに展開されているパブリッククラウド用のシェルスクリプト群がある場合は、自動的に削除されます。

```
# ./setup.sh
```

## 5.10 リセットパスの設定

---

パブリッククラウド環境下で使用する場合、リセットパスの設定は不要です。リセットパスの設定がされていても無効となります。

## 5.11 監視パスの設定

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「監視パスの設定」を参照してください。ただし、パブリッククラウド環境下では次の点が異なります。

- 監視パスは 1 つだけ配置する
- HA モニタの接続構成設定ファイルは、必ず手動で作成する



## 5.12 定義ファイルの作成 (HA モニタ)

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「定義ファイルの作成 (HA モニタ)」を参照してください。この節では、パブリッククラウド環境下で差異がある事項だけを記載します。

### 5.12.1 HA モニタの環境設定

HA モニタの環境を設定する定義ファイルを作成します。

詳細は、「[7.2 HA モニタの環境設定](#)」を参照してください。

### 5.12.2 【Azure】 サービスプリンシパル情報設定ファイルの設定

HA モニタがサービスプリンシパルを使用して Azure にログインするには、次の情報が必要です。

- アプリケーション ID\*
- 認証に使用する証明書の格納パス
- テナント ID\*

注※

Azure ポータルから確認できます。

これらの情報をサービスプリンシパル情報設定ファイル (`azure_serviceprincipal.env`) に設定し、`etc` 配下に配置する必要があります。Azure 用のシェルスクリプト群を展開すると、サービスプリンシパル情報設定ファイルのサンプルファイルが `lib` 配下に展開されます。また、サービスプリンシパル情報設定ファイルが `etc` 配下に存在しない場合は、`etc` 配下にも展開されます。

サンプルファイルの内容を次に示す記述形式で編集してください。

```
appId=aa....aa
fileWithCertAndPrivateKey=/bb....bb/cc....cc.pem
tenant=dd....dd
```

`aa....aa` : アプリケーション ID

`/bb....bb/cc....cc.pem` : 認証に使用する証明書の格納パス

`dd....dd` : テナント ID

注意事項

- 上記以外の情報は入力しないでください。

- イコール (=) の前後にスペースおよびタブを入力しないでください。

### 5.12.3 【AWS】 ネットワーク遮断設定ファイルの設定

ここでは、パブリッククラウド環境固有のネットワーク遮断設定ファイルについて説明します。

ネットワーク遮断設定ファイル（定義ファイル：/opt/hitachi/HAMon/etc/fence\_network.env）は、ネットワーク遮断の対象とする ENI の ID を列挙します。

サンプルファイルは/opt/hitachi/HAMon/lib/fence\_network.env にあります。サンプルファイルを/opt/hitachi/HAMon/etc 配下にコピーしてから設定します。系切り替え構成内の各系で設定してください。

サンプルからコピーしたとき、ネットワーク遮断設定ファイルの内容は、次のように ENI の ID としては仮の値が列挙されています。

```
eni-aaaa  
eni-bbbb
```

次の ENI の ID を系ごとに列挙してください。なお、ENI の ID は系ごとに異なるため、ネットワーク遮断設定ファイルの内容は各系で異なります。

- 業務通信用の ENI
- レプリケーションパスに使用している ENI
- EFS へのアクセス用パスに使用している ENI

HA モニタの監視パスだけで使用する ENI については列挙不要です。

HA モニタの監視パスの ENI を業務通信、レプリケーションパス、および EFS へのアクセス用パスで兼用する場合は、遮断対象の ENI として列挙してください。

ネットワーク遮断設定ファイルの記述ルールは次のとおりです。

- 1 行当たり ENI ID を 1 つ記述する。
- ENI ID は 1~10 まで指定できる。
- 同じ ENI ID を複数指定しないこと。
- 先頭が#の行はコメント行となる（無視される）。
- 空白行を指定できる（無視される）。
- コメント行を除き、1 行は 50 文字以内で記述する。

## 5.13 サーバが使用するリソースの設定

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「サーバが使用する共有リソースの設定」を参照してください。この節では、サーバが使用するリソースの設定について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 5.13.1 業務ディスクの設定

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「共有ディスクの設定」を参照してください。

さらに、AWS 環境下および Azure 環境下でレプリケーション構成にする場合、レプリケーションソフト (DRBD) の設定が必要です。「5.5 [【AWS】【Azure】レプリケーションソフト \(DRBD\) の設定](#)」を参照して、設定してください。

### 5.13.2 [【AWS】LAN の状態設定ファイルの設定 \(1つのリージョン内または1つのVPC内で系切り替えをする構成の場合\)](#)

HA モニタでは、LAN はサーバ単位に接続、切り離しをします。そのため、LAN の状態設定ファイルを作成して設定する必要があります。この項では、1つのリージョン内または1つのVPC内で系切り替えをする構成での、LAN の状態設定ファイルの設定方法について説明します。

LAN の状態設定ファイルの種類を、次に示します。

サーバ識別名.up ファイル

LAN を接続する場合に使用します。業務通信の切り替えに関する情報を設定します。

サーバ識別名.down ファイル

LAN の切り離しをする場合に使用します。業務通信の切り替えに関する情報を設定します。

これらのファイルは、サーバごとに HA モニタの環境設定用ディレクトリの下に作成します。ファイル名のサーバ識別名の部分は、サーバ対応の環境設定のalias オペランドで指定した値にしてください。

LAN の状態設定ファイルには、OS の ip コマンドの引数として、LAN アダプタに追加・削除するエイリアス IP アドレスを指定します。OS のコマンドについては、OS のマニュアルを参照してください。

AWS 用シェルスクリプト群を展開すると、AWS 用の LAN の状態設定ファイルのサンプルファイルが、/opt/hitachi/HAMon/lib 配下に配置されます。AWS 用シェルスクリプト群の展開については、「5.7 [【AWS】AWS 用のシェルスクリプト群の展開](#)」を参照してください。サンプルファイルの名称は、server\_aws.up および server\_aws.down です。

server\_aws.up のファイル内容を次に示します。

```

#!/bin/bash
set -x

#####
# VIP_ADDRESS[0]=aa.bb.cc.dd
# VIP_RT[0]="rtb-AAA rtb-BBB ..."
# VIP_ENI[0]=eni-CCC
# VIP_LABEL[0]=lo:0

# VIP_ADDRESS[1]=ee.ff.gg.hh
# VIP_RT[1]="rtb-DDD rtb-EEE ..."
# VIP_ENI[1]=eni-FFF
# VIP_LABEL[1]=lo:1

# EIP_ADDRESS[0]=ii.jj.kk.ll
# EIP_ENI[0]=eni-GGG
# EIP_LABEL[0]=eth0:0

# EIP_ADDRESS[1]=mm.nn.oo.pp
# EIP_ENI[1]=eni-HHH
# EIP_LABEL[1]=eth1:0

# DNS_ZONEID[0]=ZIII
# DNS_NAME[0]=JJJ.com.
# DNS_TYPE[0]=A
# DNS_VALUE[0]=qq.rr.ss.tt
# DNS_TTL[0]=uu

# DNS_ZONEID[1]=ZKKK
# DNS_NAME[1]=LLL.com.
# DNS_TYPE[1]=CNAME
# DNS_VALUE[1]=MMM.com.
# DNS_TTL[1]=vv

#####
function main() {
    VIP_RCD=0
    if [ ${#VIP_ADDRESS[@]} -gt 0 ]
    then
        add_vip
        rc=$?
        if [ $rc -ne 0 ]
        then
            VIP_RCD=1
        fi
    fi

    EIP_RCD=0
    if [ ${#EIP_ADDRESS[@]} -gt 0 ]
    then
        add_eip
        rc=$?
        if [ $rc -ne 0 ]
        then
            EIP_RCD=2
        fi
    fi
}

```

```

        fi
    fi

    DNS_RCD=0
    if [ ${#DNS_NAME[@]} -gt 0 ]
    then
        add_dns
        rc=$?
        if [ $rc -ne 0 ]
        then
            DNS_RCD=4
        fi
    fi

    RCD=$((VIP_RCD|$EIP_RCD|$DNS_RCD))
    return $RCD
}

```

```

#####
: (以下を編集しないこと)

```

server\_aws.down のファイル内容を次に示します。

```

#!/bin/bash
set -x

#####
# VIP_ADDRESS[0]=aa.bb.cc.dd
# VIP_RTB[0]="rtb-AAA rtb-BBB ..."
# VIP_ENI[0]=eni-CCC
# VIP_LABEL[0]=lo:0

# VIP_ADDRESS[1]=ee.ff.gg.hh
# VIP_RTB[1]="rtb-DDD rtb-EEE ..."
# VIP_ENI[1]=eni-FFF
# VIP_LABEL[1]=lo:1

# EIP_ADDRESS[0]=ii.jj.kk.ll
# EIP_ENI[0]=eni-GGG
# EIP_LABEL[0]=eth0:0

# EIP_ADDRESS[1]=mm.nn.oo.pp
# EIP_ENI[1]=eni-HHH
# EIP_LABEL[1]=eth1:0

# DNS_ZONEID[0]=ZIII
# DNS_NAME[0]=JJJ.com.
# DNS_TYPE[0]=A
# DNS_VALUE[0]=qq.rr.ss.tt
# DNS_TTL[0]=uu

# DNS_ZONEID[1]=ZKKK
# DNS_NAME[1]=LLL.com.
# DNS_TYPE[1]=CNAME

```

```

# DNS_VALUE[1]=MMM.com.
# DNS_TTL[1]=vv

#####
function main() {
    VIP_RCD=0
    if [ ${#VIP_ADDRESS[@]} -gt 0 ]
    then
        delete_vip
        rc=$?
        if [ $rc -ne 0 ]
        then
            VIP_RCD=1
        fi
    fi

    EIP_RCD=0
    if [ ${#EIP_ADDRESS[@]} -gt 0 ]
    then
        delete_eip
        rc=$?
        if [ $rc -ne 0 ]
        then
            EIP_RCD=2
        fi
    fi

    DNS_RCD=0
    if [ ${#DNS_NAME[@]} -gt 0 ]
    then
        delete_dns
        rc=$?
        if [ $rc -ne 0 ]
        then
            DNS_RCD=4
        fi
    fi

    RCD=$((VIP_RCD|EIP_RCD|DNS_RCD))
    return $RCD
}

#####
: (以下を編集しないこと)

```

サーバごとに、サンプルファイルを/opt/hitachi/HAmn/etc 配下にコピーして、server\_aws.up をサーバ識別名.up に、server\_aws.down をサーバ識別名.down にリネームしてください。

サーバ識別名.up/down で設定が必要なシェル変数について説明します。

## メモ

ここで説明する[n]は配列の添え字です。VIP, EIP, または業務通信に使用する DNS 名が 1 つの場合, [n]は 0 です。複数ある場合, 1 つ目の[n]は 0, 2 つ目の[n]は 1, のように, 添え字が 0 から順に 1 ずつ増加するように設定してください。

サンプルファイルからコピーした状態では, シェル変数部分はコメント行となっています。コメント行を表す先頭の"#"を削除してから, 設定してください。例えば, VIP が 1 つの場合は, 次のシェル変数について, コメント"#"を削除し, シェル変数を設定します。

- VIP\_ADDRESS[0]
- VIP\_RT[B][0]
- VIP\_ENI[0]
- VIP\_LABEL[0]

2 つの場合は, 次のシェル変数について, コメント"#"を削除し, シェル変数を設定します。

- VIP\_ADDRESS[0]
- VIP\_RT[B][0]
- VIP\_ENI[0]
- VIP\_LABEL[0]
- VIP\_ADDRESS[1]
- VIP\_RT[B][1]
- VIP\_ENI[1]
- VIP\_LABEL[1]

3 つ目以降については, シェル変数をコピーするなどの方法で, 設定してください。

### VIP 制御によって業務通信を切り替える場合

"VIP\_"から始まるシェル変数を次のとおりに設定してください。

- VIP\_ADDRESS[n]  
業務 IP アドレスとして使用する VIP を設定してください。すべての系切り替え構成内で同じ設定にしてください。
- VIP\_RT[B][n]  
VIP 宛の通信をするインスタンスがあるサブネットに関連づけられた, ルートテーブルの固有 ID を設定してください。複数設定する場合は, 1 つ以上の半角スペースまたはタブで区切り, 全体をダブルクォーテーションで囲んで設定してください。すべての系切り替え構成内で同じ設定にしてください。
- VIP\_ENI[n]

VIP 宛の通信を受信する自インスタンスに付与されている ENI の固有 ID を設定してください。系によって値が異なります。

- VIP\_LABEL[n]

VIP を付与する OS 上の LAN インタフェースを"LAN インタフェース名:xxx"の形式で設定してください。すべての系切り替え構成内で同じ設定にしてください。

EIP 制御によって業務通信を切り替える場合

"EIP\_"から始まるシェル変数を次のとおりに設定してください。

- EIP\_ADDRESS[n]

業務 IP アドレスとして使用する EIP を設定してください。すべての系切り替え構成内で同じ設定にしてください。

- EIP\_ENI[n]

EIP と関連づける ENI の固有 ID を設定してください。系によって値が異なります。

- EIP\_LABEL[n]

EIP を付与する OS 上の LAN インタフェースを"LAN インタフェース名:xxx"の形式で設定してください。すべての系切り替え構成内で同じ設定にしてください。

DNS 名制御によって業務通信を切り替える場合

レコードの変更方法によって、LAN の状態設定ファイルのシェル変数の設定方法が異なります。シェル変数の設定要否を次の表に示します。

表 5-1 LAN の状態設定ファイルのシェル変数の設定要否

| レコードの変更方法              | シェル変数の設定要否     |                  |
|------------------------|----------------|------------------|
|                        | サーバ識別名.up ファイル | サーバ識別名.down ファイル |
| レコードを更新する方法            | 必要             | 不要*              |
| レコードを削除したあとレコードを追加する方法 | 必要             | 必要               |

注※

シェル変数の設定は不要ですが、サーバ識別名.down ファイルは/opt/hitachi/HAMon/etc 配下に作成する必要があります。

"DNS\_"から始まるシェル変数のコメントアウトを外し、次のとおりに設定してください。

- DNS\_NAME[n]

業務通信に使用する DNS 名を設定してください。すべての系切り替え構成内で同じ設定にしてください。

- DNS\_ZONEID[n]

業務通信に使用する DNS 名を管理対象に含む、ホストゾーンの ID を設定してください。すべての系切り替え構成内で同じ設定にしてください。

なお、ホストゾーン ID の確認方法は次のとおりです。



1. Amazon Route 53 コンソール上で、「ホストゾーン」をクリックする。
2. ホストゾーンの一覧の中から、業務通信に使用する DNS 名を管理対象に含むホストゾーンを選択する。
3. ホストゾーンの詳細情報から、ホストゾーン ID を確認する。

- DNS\_TYPE[n]

DNS レコードタイプ (A レコードタイプまたは CNAME レコードタイプ) を設定してください。A レコードタイプは、名前解決の結果である IPv4 アドレスを記録します。CNAME レコードタイプは、名前解決を実行する別の DNS 名を記録します。すべての系切り替え構成内で同じ設定にしてください。

- DNS\_VALUE[n]

DNS レコードタイプが A レコードタイプの場合は IPv4 アドレス、CNAME レコードタイプの場合は DNS 名を設定してください。設定する値は系ごとに異なります。

- DNS\_TTL[n]

リゾルバがレコードをキャッシュしておく時間 (秒) を設定してください。

DNS\_TTL で設定された時間内は、キャッシュ内の値を使用して業務通信します。

DNS\_TTL の値が大きすぎると、HA モニタが実行サーバを系切り替えしても、切り替え元の系で業務通信するおそれがあります。そのため、次の手順で DNS\_TTL を決めてください。

1. DNS 名制御を使用した計画系切り替えを実施し、系切り替え時間を計測<sup>※</sup>する。
2. 計測した系切り替え時間より小さい値を DNS\_TTL に設定する。

注※ 系切り替え元でメッセージ KAMN290-I を出力してから、系切り替え先でメッセージ KAMN311-I を出力するまでの時間を計測します。

### 5.13.3 【AWS】 LAN の状態設定ファイルの設定 (複数のリージョン間または複数の VPC 間で系切り替えをする構成の場合)

HA モニタでは、LAN はサーバ単位に接続、切り離しをします。そのため、LAN の状態設定ファイルを作成して設定する必要があります。この項では、複数のリージョン間または複数の VPC 間で系切り替えをする構成での、LAN の状態設定ファイルの設定方法について説明します。

LAN の状態設定ファイルの種類を、次に示します。

- サーバ識別名.up ファイル

LAN を接続する場合に使用します。業務通信の切り替えに関する情報を設定します。

サンプルファイルの名称は、server\_aws\_vpc.up です。サーバごとに、サンプルファイルを /opt/hitachi/HAMon/etc 配下にコピーします。server\_aws\_vpc.up をサーバ識別名.up にリネームして使用してください。

- サーバ識別名.down ファイル

LAN の切り離しをする場合に使用します。業務通信の切り替えに関する情報を設定します。

サンプルファイルの名称は、server\_aws\_vpc.down です。サーバごとに、サンプルファイルを/opt/hitachi/HAMon/etc 配下にコピーします。server\_aws\_vpc.down をサーバ識別名.down にリネームして使用してください。

- vip\_tgw\_def ファイル

業務通信の切り替えに必要な情報として、次の情報を設定します。

- 複数の VPC 間で系切り替えをする構成での、トランジットゲートウェイおよびルートテーブルに関する情報
- すべての系のホストに関する情報

サンプルファイルの名称は、vip\_tgw\_def です。サンプルファイルは、サーバ識別名.up ファイル、およびサーバ識別名.down ファイルと同じフォルダにあります。サンプルファイルを/opt/hitachi/HAMon/etc 配下にコピーして、編集して使用してください。

なお、ファイル名はリネームしないでください。また、この定義ファイルはすべての系で同じ設定内容にしてください。

server\_aws\_vpc.up, およびserver\_aws\_vpc.down のファイルの内容を次に示します。

```
#!/bin/bash
set -x

#####
# HOSTNAME=hostA
# VIP[0]=bb.cc.dd.ee
# LABEL[0]=lo:0

# VIP[1]=ff.gg.hh.ii
# LABEL[1]=lo:0

# DNS_ZONEID[0]=ZIII
# DNS_NAME[0]=JJJ.com.
# DNS_TYPE[0]=A
# DNS_VALUE[0]=qq.rr.ss.tt
# DNS_TTL[0]=uu

# DNS_ZONEID[1]=ZKKK
# DNS_NAME[1]=LLL.com.
# DNS_TYPE[1]=CNAME
# DNS_VALUE[1]=MMM.com.
# DNS_TTL[1]=vv

#####
: (以下を編集しないこと)
```

vip\_tgw\_def のファイルの内容を次に示します。

```
# host information
host
{
host_name=hostA
```

```

host_region=ap-northeast-1
host_vpc=vpc-AAA
host_vip[0]=aa.bb.cc.dd
host_eni[0]=eni-AAA000
host_tgw_attachment[0]=tgw-attach-AAA
host_vip[1]=ee.ff.gg.hh
host_eni[1]=eni-AAA111
host_tgw_attachment[1]=tgw-attach-AAA
}
host
{
host_name=hostB
host_region=ap-southeast-1
host_vpc=vpc-BBB
host_vip[0]=aa.bb.cc.dd
host_eni[0]=eni-BBB000
host_tgw_attachment[0]=tgw-attach-BBB
host_vip[1]=ee.ff.gg.hh
host_eni[1]=eni-BBB111
host_tgw_attachment[1]=tgw-attach-BBB
}

# route table information
rtb
{
rtb_id=rtb-AAA
rtb_region=ap-northeast-1
rtb_vpc=vpc-AAA
rtb_vip[0]=aa.bb.cc.dd
rtb_tgw[0]=tgw-AAA
rtb_vip[1]=ee.ff.gg.hh
rtb_tgw[1]=tgw-AAA
}
rtb
{
rtb_id=rtb-BBB
rtb_region=ap-southeast-1
rtb_vpc=vpc-BBB
rtb_vip[0]=aa.bb.cc.dd
rtb_tgw[0]=tgw-BBB
rtb_vip[1]=ee.ff.gg.hh
rtb_tgw[1]=tgw-BBB
}

# transit gateway information
tgw
{
tgw_id=tgw-AAA
tgw_region=ap-northeast-1
tgw_vip[0]=aa.bb.cc.dd
tgw_route_table[0]=tgw-rtb-AAA
tgw_vip[1]=ee.ff.gg.hh
tgw_route_table[1]=tgw-rtb-AAA
tgw_attachment=tgw-attach-AAA
tgw_peering_attachment=tgw-attach-PPP
}
tgw
{

```

```
tgw_id=tgw-BBB
tgw_region=ap-southeast-1
tgw_vip[0]=aa.bb.cc.dd
tgw_route_table[0]=tgw-rtb-BBB
tgw_vip[1]=ee.ff.gg.hh
tgw_route_table[1]=tgw-rtb-AAA
tgw_attachment=tgw-attach-BBB
tgw_peering_attachment=tgw-attach-PPP
}
```

次の通信制御の方式で業務通信を切り替える場合の、LAN の状態設定ファイルの設定方法について説明します。

- VIP 制御
- DNS 制御

## (1) VIP 制御の場合

VIP 制御で複数のリージョン間または複数の VPC 間で系切り替えをする場合の、LAN の状態設定ファイルの設定方法について説明します。

### (a) LAN の状態設定ファイルの記述形式

LAN の状態設定ファイルの記述形式について説明します。

サーバ識別名.up ファイル, およびサーバ識別名.down ファイルの記述形式

サーバ識別名.up ファイル, およびサーバ識別名.down ファイルの記述形式を次に示します。

```
#!/bin/bash
set -x

#####
# HOSTNAME=hosta
# VIP[0]=bb.cc.dd.ee
# LABEL[0]=lo:0

# VIP[1]=ff.gg.hh.ii
# LABEL[1]=lo:0
(以下略)
```

次に、サーバ識別名.up ファイル, およびサーバ識別名.down ファイルで設定が必要なシェル変数について説明します。

サンプルファイルからコピーした状態では、シェル変数部分はコメント行となっています。コメント行を表す先頭の"#"を削除してから、設定してください。例えば、VIP が 1 つの場合は、次のシェル変数について、コメント"#"を削除し、シェル変数を設定します。

#### ❗ 重要

シェル変数を記述する際は、次の点に注意してください。

- シェル変数を「シェル変数=値」の形式で、1行につき1つずつ記述する。
- シェル変数および"="の前後に空白を記述しない。
- 先頭が"#"の場合は、コメント行になる。

表 5-2 サーバ識別名.up ファイル, およびサーバ識別名.down ファイルで設定が必要なシェル変数

| パラメタ名    | 説明   |
|----------|--|
| HOSTNAME | 自系のホスト名を指定します。<br>HA モニタの環境設定のname オペランドに指定する名称と同じにしてください。<br>系によって名称が異なります。   |
| VIP[n]   | 業務 IP アドレスとして使用する VIP を指定します。<br>すべての系切り替え構成内で、同じ指定にしてください。<br>"VIP[n]"の形式で記述します。[n]は添え字を表します。1つ目の[n]は0, 2つ目の[n]は1, のように、添え字が0から順に1ずつ増加するように設定してください。  |
| LABEL[n] | VIP を付与する OS 上の LAN インタフェースを"LAN インタフェース名:xxx"の形式で指定します。<br>すべての系切り替え構成内で同じ指定にしてください。<br>VIP[n]ごとに関連づける OS 上の LAN インタフェースを, "LABEL[n]"と記述します。"VIP[n]"の"[n]"と"LABEL[n]"の"[n]"は, 同じ添え字にしてください。 |

VIP およびLABEL の設定例を次に示します。

(例) VIP (10.10.10.10, 10.10.10.20) をLABEL (lo:0) に設定する場合

```
VIP[0]=10.10.10.10
LABEL[0]=lo:0
VIP[1]=10.10.10.20
LABEL[1]=lo:0
```

(例) VIP (10.10.10.10) をLABEL (lo:0) に, VIP (10.10.10.20) をLABEL (lo:1) に設定する場合

```
VIP[0]=10.10.10.10
LABEL[0]=lo:0
VIP[1]=10.10.10.20
LABEL[1]=lo:1
```

#### vip\_tgw\_def ファイルの記述形式

次に, vip\_tgw\_def ファイルの記述形式について説明します。

vip\_tgw\_def ファイルは, 次の3つの要素で構成されています。

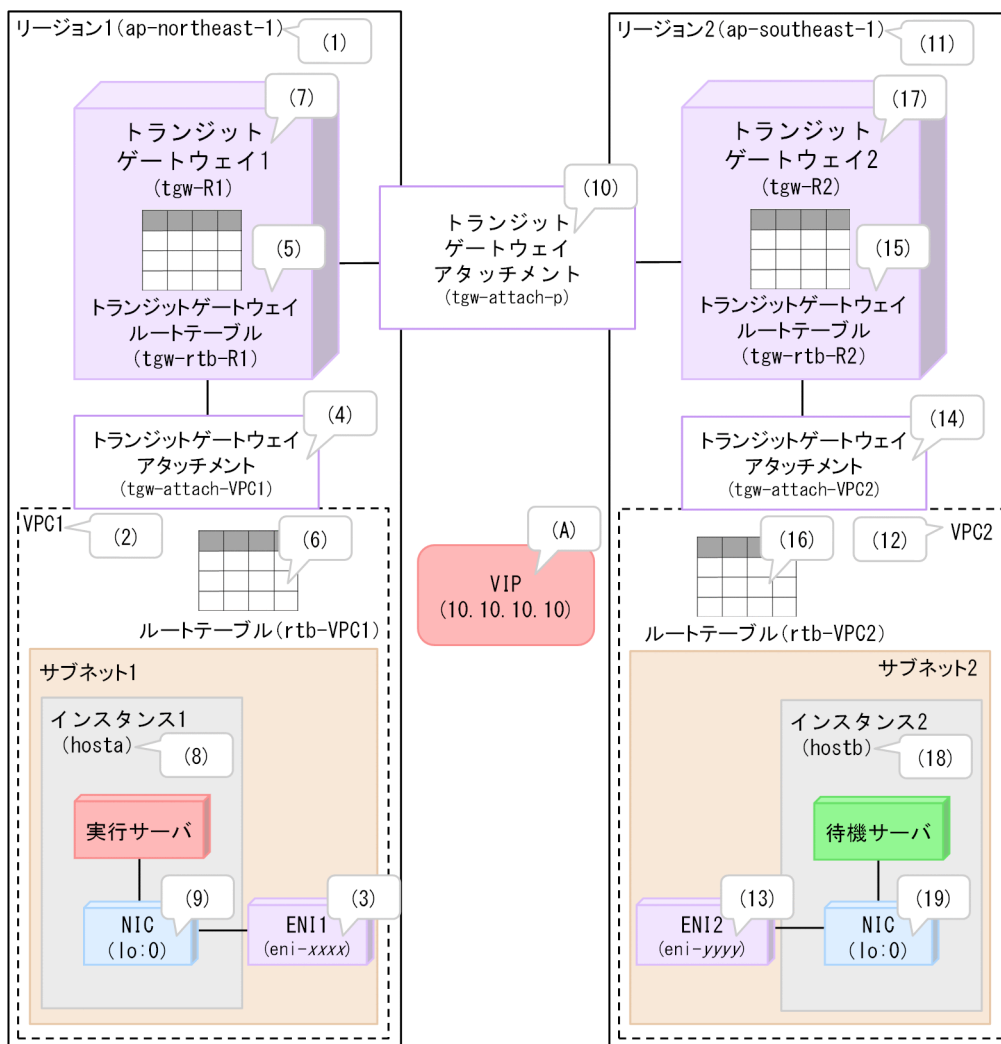
- **tgw**  
系切り替え構成内のすべてのトランジットゲートウェイに関する情報を設定します。
- **rtb**  
系切り替え構成内のすべてのルートテーブルに関する情報を設定します。

- host

系切り替え構成内のすべてのホストに関する情報を設定します。

次に、系切り替え構成例とそれに対応するvip\_tgw\_def ファイルの記述形式の例を示します。

図 5-5 系切り替え構成例 (複数のリージョン間で系切り替えをする構成の例)



上記の系切り替え構成例に対応する、vip\_tgw\_def ファイルの記述形式は次のとおりです。記述形式中の"(n)"は、図中の"(n)"と対応しています。

tgw の記述形式

```
## トランジットゲートウェイ情報 ##
tgw
{
  tgw_id=twg-R1      ... (7)
  tgw_region=ap-northeast-1  ... (1)
  tgw_vip[0]=10.10.10.10    ... (A)
  tgw_route_table[0]=twg-rtb-R1  ... (5)
  tgw_attachment=twg-attach-VPC1  ... (4)
  tgw_peering_attachment=twg-attach-P  ... (10)
}

tgw
```

```

{
  tgw_id=twg-R2    ... (17)
  tgw_region=ap-southeast-1    ... (11)
  tgw_vip[0]=10.10.10.10    ... (A)
  tgw_route_table[0]=twg-rtb-R2    ... (15)
  tgw_attachment=twg-attach-VPC2    ... (14)
  tgw_peering_attachment=twg-attach-P    ... (10)
}

```

"tgw"を先頭に記載します。その下に, "{"を追加し, "{"内にトランジットゲートウェイの各パラメタを記述します。各パラメタについては, 「表 5-3 tgw に設定するパラメタ」を参照してください。トランジットゲートウェイの数だけ, "tgw"およびトランジットゲートウェイの各パラメタの記述を追加してください。

#### rtb の記述形式

```

## ルートテーブル情報 ##
rtb
{
  rtb_id=rtb-VPC1    ... (6)
  rtb_region=ap-northeast-1    ... (1)
  rtb_vpc=VPC1    ... (2)
  rtb_vip[0]=10.10.10.10    ... (A)
  rtb_tgw[0]=twg-R1    ... (7)
}

rtb
{
  rtb_id=rtb-VPC2    ... (16)
  rtb_region=ap-southeast-1    ... (11)
  rtb_vpc=VPC2    ... (12)
  rtb_vip[0]=10.10.10.10    ... (A)
  rtb_tgw[0]=twg-R2    ... (17)
}

```

"rtb"を先頭に記載します。その下に, "{"を追加し, "{"内にルートテーブルの各パラメタを記述します。各パラメタについては, 「表 5-4 rtb に設定するパラメタ」を参照してください。ルートテーブルの数だけ, "rtb"およびルートテーブルの各パラメタの記述を追加してください。

#### host の記述形式

```

## ホスト情報 ##
host
{
  host_name=hosta    ... (8)
  host_region=ap-northeast-1    ... (1)
  host_vpc=VPC1    ... (2)
  host_vip[0]=10.10.10.10    ... (A)
  host_eni[0]=eni-XXXX    ... (3)
  host_tgw_attachment[0]=twg-attach-VPC1    ... (4)
}

host
{
  host_name=hostb    ... (18)
  host_region=ap-southeast-1    ... (11)
}

```

```

host_vpc=VPC2    ... (12)
host_vip[0]=10.10.10.10    ... (A)
host_eni[0]=eni-yyyy    ... (13)
host_tgw_attachment[0]=tgw-attach-VPC2    ... (14)
}

```

"host"を先頭に記載します。その下に、"{"を追加し、"{"内にホストの各パラメタを記述します。各パラメタについては、「表 5-5 host に設定するパラメタ」を参照してください。系切り替え構成内のホストの数だけ、"host"およびホストの各パラメタの記述を追加してください。

次に、vip\_tgw\_def ファイルに設定するパラメタについて説明します。

すべてのパラメタをvip\_tgw\_def ファイルに設定します。設定後、moncheck コマンドを実行し、フォーマットのエラーがないかを確認してください。フォーマットのエラーがある場合は、moncheck コマンドがメッセージKAMN773-E を出力します。

## ! 重要

パラメタを記述する際は、次の点に注意してください。

- パラメタを「パラメタ名=値」の形式で、1行につき1つずつ記述する。
- パラメタおよび"="の前後に空白を記述しない。
- 先頭が"#"の場合は、コメント行になる。

tgw に記載するパラメタ名を次の表に示します。

表 5-3 tgw に設定するパラメタ

| パラメタ名                  | 説明  |
|------------------------|---|
| tgw_id                 | トランジットゲートウェイ ID を指定します。   |
| tgw_region             | トランジットゲートウェイがあるリージョンの ID を指定します。  |
| tgw_vip                | トランジットゲートウェイで転送する VIP を指定します。<br>"tgw_vip[n]"の形式で記述します。[n]は添え字を表します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。   |
| tgw_route_table        | トランジットゲートウェイルートテーブル ID を指定します。<br>"tgw_route_table[n]"の形式で記述します。[n]は添え字を表します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。<br>tgw_vip[n]に指定したVIPの宛先をエントリする"tgw_route_table[n]"を記述します。"tgw_vip[n]"の"[n]"と"tgw_route_table[n]"の"[n]"は、同じ添え字にしてください。 |
| tgw_attachment         | VPC用のトランジットゲートウェイアタッチメントを指定します。<br>複数個指定する場合は、1つ以上の半角スペースまたはタブで区切り、全体をダブルクォーテーションで囲んで指定してください。  |
| tgw_peering_attachment | 複数のリージョン間で系切り替えをする構成の場合、接続先リージョンのトランジットゲートウェイとのピアリング用の、トランジットゲートウェイアタッチメントを指定します。<br>上記の構成以外の場合は、次のどちらかを実施してください。   |



| パラメタ名 | 説明  |
|-------|---|
|       | <ul style="list-style-type: none"> <li>パラメタを削除する</li> <li>パラメタの先頭に"#"を追加し、コメント行にする</li> </ul> |

tgw\_vip および tgw\_route\_table の設定例を次に示します。

(例) VIP (10.10.10.10, 10.10.10.20) をトランジットゲートウェイルートテーブル (tgw-rtb-R1) に追加する設定の場合

```
tgw_vip[0]=10.10.10.10
tgw_route_table[0]=tgw-rtb-R1
tgw_vip[1]=10.10.10.20
tgw_route_table[1]=tgw-rtb-R1
```

(例) VIP (10.10.10.10) をトランジットゲートウェイルートテーブル (tgw-rtb-R1) に、VIP (10.10.10.20) をトランジットゲートウェイルートテーブル (tgw-rtb-R2) に追加する設定の場合

```
tgw_vip[0]=10.10.10.10
tgw_route_table[0]=tgw-rtb-R1
tgw_vip[1]=10.10.10.20
tgw_route_table[1]=tgw-rtb-R2
```

(例) VIP (10.10.10.10, 10.10.10.20) をトランジットゲートウェイルートテーブル (tgw-rtb-R1) に、VIP (10.10.10.30) をトランジットゲートウェイルートテーブル (tgw-rtb-R2) に追加する設定の場合

```
tgw_vip[0]=10.10.10.10
tgw_route_table[0]=tgw-rtb-R1
tgw_vip[1]=10.10.10.20
tgw_route_table[1]=tgw-rtb-R1
tgw_vip[2]=10.10.10.30
tgw_route_table[2]=tgw-rtb-R2
```

tgw\_attachment の設定例を次に示します。

(例) VPC 用のトランジットゲートウェイアタッチメントに、tgw-attach-VPC1, tgw-attach-VPC2 を設定する場合

```
tgw_attachment="tgw-attach-VPC1△tgw-attach-VPC2"
```

(凡例) △: 1 つ以上の半角スペースまたはタブ

rtb に記載するパラメタ名を次の表に示します。

表 5-4 rtb に設定するパラメタ

| パラメタ名      | 説明                          |
|------------|-----------------------------|
| rtb_id     | ルートテーブルの ID を指定します。         |
| rtb_vpc    | ルートテーブルがある VPC の ID を指定します。 |
| rtb_region | ルートテーブルがあるリージョンの ID を指定します。 |
| rtb_vip    | ルートテーブルで転送する VIP を指定します。    |

| パラメタ名   | 説明   |
|---------|--|
|         | "rtb_vip[n]"の形式で記述します。[n]は添え字を表します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。   |
| rtb_tgw | ルートテーブルがあるリージョンの、トランジットゲートウェイ ID を指定します。<br>"rtb_tgw[n]"の形式で記述します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。<br>rtb_vip[n]に指定したVIPの宛先をエントリする"rtb_tgw[n]"を指定します。"rtb_vip[n]"の"[n]"と"rtb_tgw[n]"の"[n]"は、同じ添え字にしてください。 |

rtb\_vip およびrtb\_tgw の設定例を次に示します。

(例) ルートテーブルにVIP (10.10.10.10, 10.10.10.20) の宛先をtgw-R1 に設定する場合

```
rtb_vip[0]=10.10.10.10
rtb_tgw[0]=tgw-R1
rtb_vip[1]=10.10.10.20
rtb_tgw[1]=tgw-R1
```

host に記載するパラメタ名を次の表に示します。

表 5-5 host に設定するパラメタ

| パラメタ名               | 説明   |
|---------------------|--|
| host_name           | ホスト名称を指定します。<br>指定するホスト名称は、各系の HA モニタの環境設定のname オペランドに指定する名称と同じ名称にしてください。  |
| host_region         | host_name に指定したホストがあるリージョンを指定します。  |
| host_vpc            | host_name に指定したホストがある VPC を指定します。  |
| host_vip            | host_name に指定したホストで稼働させるすべてのサーバが、業務通信で使用するすべてのVIPを指定します。<br>"host_vip[n]"の形式で記述します。[n]は添え字を表します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。  |
| host_eni            | host_name に指定したホストで、VIP 宛の業務通信を受信する ENI の ENI ID を指定します。<br>"host_eni [n]"の形式で記述します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。<br>host_vip[n]に指定したVIPの宛先として、"host_eni [n]"を指定します。"host_vip[n]"の"[n]"と"host_eni [n]"の"[n]"は、同じ添え字にしてください。  |
| host_tgw_attachment | host_name に指定したホストが接続する、VPC 用のトランジットゲートウェイアタッチメントを指定します。<br>"host_tgw_attachment[n]"の形式で記述します。[n]は添え字を表します。1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。<br>host_vip[n]に指定したVIPの宛先として、"host_tgw_attachment[n]"を指定します。"host_vip[n]"の"[n]"と"host_tgw_attachment[n]"の"[n]"は、同じ添え字にしてください。 |

host\_vip, host\_eni および host\_tgw\_attachment の設定例を次に示します。

(例) VIP (10.10.10.10, 10.10.10.20) の宛先を eni-xxxx, tgw-attach-VPC1 に設定する場合

```
host_vip[0]=10.10.10.10
host_eni[0]=eni-xxxx
host_tgw_attachment[0]=tgw-attach-VPC1
host_vip[1]=10.10.10.20
host_eni[1]=eni-xxxx
host_tgw_attachment[1]=tgw-attach-VPC1
```

(例) VIP (10.10.10.10) の宛先を eni-xxxx および tgw-attach-VPC1 に, VIP (10.10.10.20) の宛先を eni-yyyy および tgw-attach-VPC2 に設定する場合

```
host_vip[0]=10.10.10.10
host_eni[0]=eni-xxxx
host_tgw_attachment[0]=tgw-attach-VPC1
host_vip[1]=10.10.10.20
host_eni[1]=eni-yyyy
host_tgw_attachment[1]=tgw-attach-VPC2
```

## (b) LAN の状態設定ファイルの設定例

次の系切り替え構成と, それに対応する LAN の状態設定ファイルの設定例について説明します。

- 同一のリージョン内の, 複数の VPC 間で系切り替えをする構成
- 複数のリージョン間で系切り替えをする構成
- 同一の VPC 内の複数の AZ 間, および複数のリージョン間で系切り替えをする構成

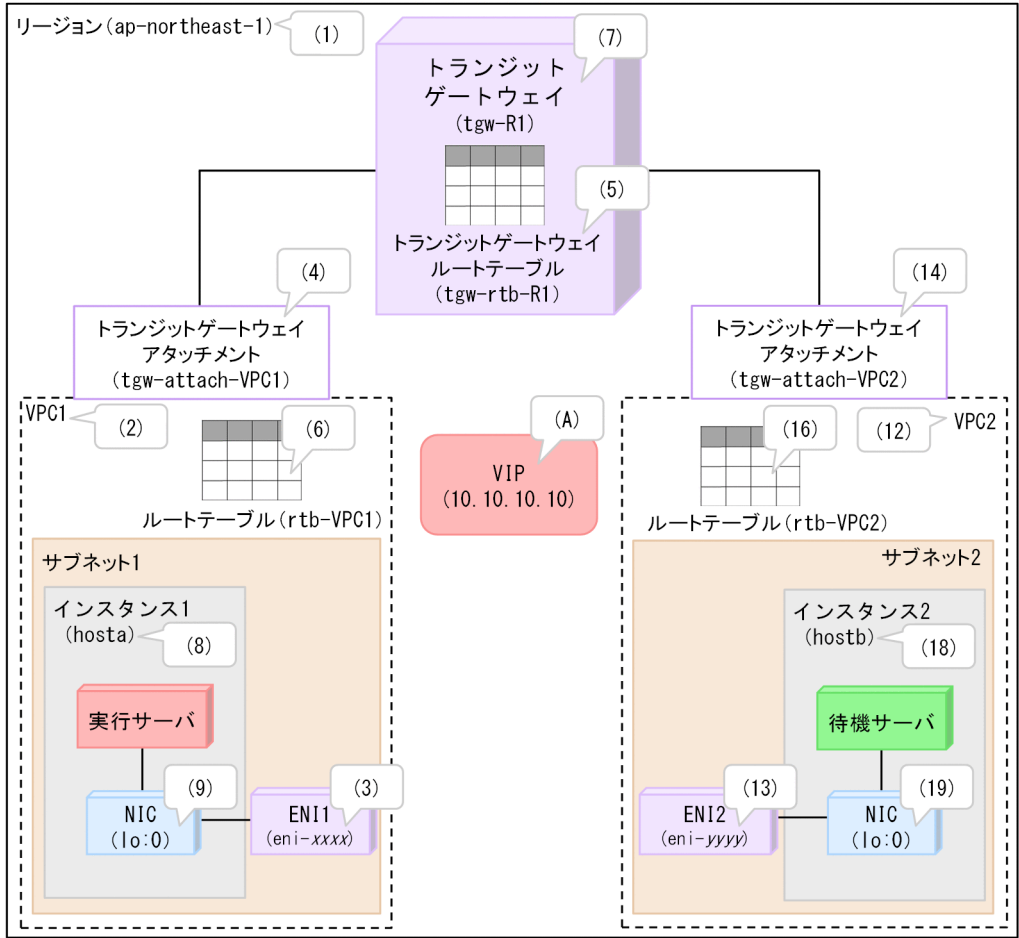
### メモ

LAN の状態設定ファイルの格納先は次のとおりです。

- サーバ識別名.up ファイルの格納先  
/opt/hitachi/HAmom/etc/サーバ識別名.upファイル
- サーバ識別名.down ファイルの格納先  
/opt/hitachi/HAmom/etc/サーバ識別名.downファイル
- vip\_tgw\_def ファイルの格納先  
/opt/hitachi/HAmom/etc/vip\_tgw\_def

同一のリージョン内の、複数の VPC 間で系切り替えをする構成の場合

図 5-6 同一のリージョン内の、複数の VPC 間で系切り替えをする構成例



上記の図に対応する、LAN の状態設定ファイルの設定例は次のとおりです。設定例中の"(n)"は、図中の"(n)"と対応しています。

現用系 (インスタンス 1) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash
set -x

#####
HOSTNAME=hosta ... (8)
VIP[0]=10.10.10.10 ... (A)
LABEL[0]=lo:0 ... (9)
#####

: (以下を編集しないこと)
```

予備系 (インスタンス 2) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash
set -x

#####
HOSTNAME=hostb ... (18)
VIP[0]=10.10.10.10 ... (A)
```

```
LABEL[0]=lo:0 ... (19)
#####

: (以下を編集しないこと)
```

#### vip\_tgw\_def ファイル

```
## トランジットゲートウェイ情報 ##
tgw
{
  tgw_id=twg-R1 ... (7)
  tgw_region=ap-northeast-1 ... (1)
  tgw_vip[0]=10.10.10.10 ... (A)
  tgw_route_table[0]=twg-rtb-R1 ... (5)
  tgw_attachment="twg-attach-VPC1 twg-attach-VPC2" ... (4) (14)
}

## ルートテーブル情報 ##
rtb
{
  rtb_id=rtb-VPC1 ... (6)
  rtb_region=ap-northeast-1 ... (1)
  rtb_vpc=VPC1 ... (2)
  rtb_vip[0]=10.10.10.10 ... (A)
  rtb_tgw[0]=twg-R1 ... (7)
}

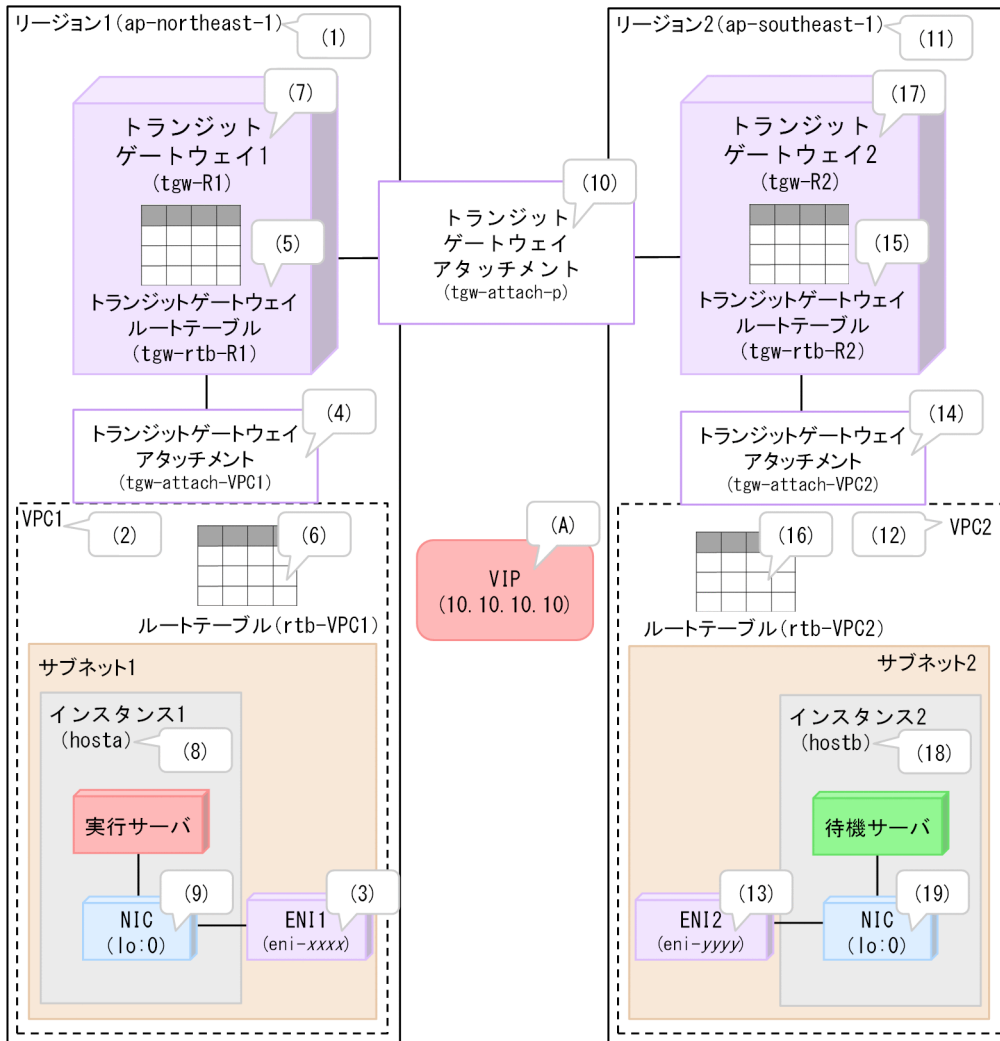
rtb
{
  rtb_id=rtb-VPC2 ... (16)
  rtb_region=ap-northeast-1 ... (1)
  rtb_vpc=VPC2 ... (12)
  rtb_vip[0]=10.10.10.10 ... (A)
  rtb_tgw[0]=twg-R1 ... (7)
}

## ホスト情報 ##
host
{
  host_name=hosta ... (8)
  host_region=ap-northeast-1 ... (1)
  host_vpc=VPC1 ... (2)
  host_vip[0]=10.10.10.10 ... (A)
  host_eni[0]=eni-xxxx ... (3)
  host_tgw_attachment[0]=twg-attach-VPC1 ... (4)
}

host
{
  host_name=hostb ... (18)
  host_region=ap-northeast-1 ... (1)
  host_vpc=VPC2 ... (12)
  host_vip[0]=10.10.10.10 ... (A)
  host_eni[0]=eni-yyyy ... (13)
  host_tgw_attachment[0]=twg-attach-VPC2 ... (14)
}
```

複数のリージョン間で系切り替えをする構成の場合

図 5-7 複数のリージョン間で系切り替えをする構成例



上記の図に対応する、LAN の状態設定ファイルの設定例は次のとおりです。設定例中の"(n)"は、図中の"(n)"と対応しています。

現用系 (インスタンス 1) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash
set -x
#####
HOSTNAME=hosta ... (8)
VIP[0]=10.10.10.10 ... (A)
LABEL[0]=lo:0 ... (9)
#####
: (以下を編集しないこと)
```

予備系 (インスタンス 2) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash
set -x
#####
HOSTNAME=hostb ... (18)
```

```
VIP[0]=10.10.10.10 ... (A)
LABEL[0]=lo:0 ... (19)
#####

: (以下を編集しないこと)
```

#### vip\_tgw\_def ファイル

```
## トランジットゲートウェイ情報 ##
tgw
{
  tgw_id=twg-R1 ... (7)
  tgw_region=ap-northeast-1 ... (1)
  tgw_vip[0]=10.10.10.10 ... (A)
  tgw_route_table[0]=twg-rtb-R1 ... (5)
  tgw_attachment=twg-attach-VPC1 ... (4)
  tgw_peering_attachment=twg-attach-P ... (10)
}

tgw
{
  tgw_id=twg-R2 ... (17)
  tgw_region=ap-southeast-1 ... (11)
  tgw_vip[0]=10.10.10.10 ... (A)
  tgw_route_table[0]=twg-rtb-R2 ... (15)
  tgw_attachment=twg-attach-VPC2 ... (14)
  tgw_peering_attachment=twg-attach-P ... (10)
}

## ルートテーブル情報 ##
rtb
{
  rtb_id=rtb-VPC1 ... (6)
  rtb_region=ap-northeast-1 ... (1)
  rtb_vpc=VPC1 ... (2)
  rtb_vip[0]=10.10.10.10 ... (A)
  rtb_tgw[0]=twg-R1 ... (7)
}

rtb
{
  rtb_id=rtb-VPC2 ... (16)
  rtb_region=ap-southeast-1 ... (11)
  rtb_vpc=VPC2 ... (12)
  rtb_vip[0]=10.10.10.10 ... (A)
  rtb_tgw[0]=twg-R2 ... (17)
}

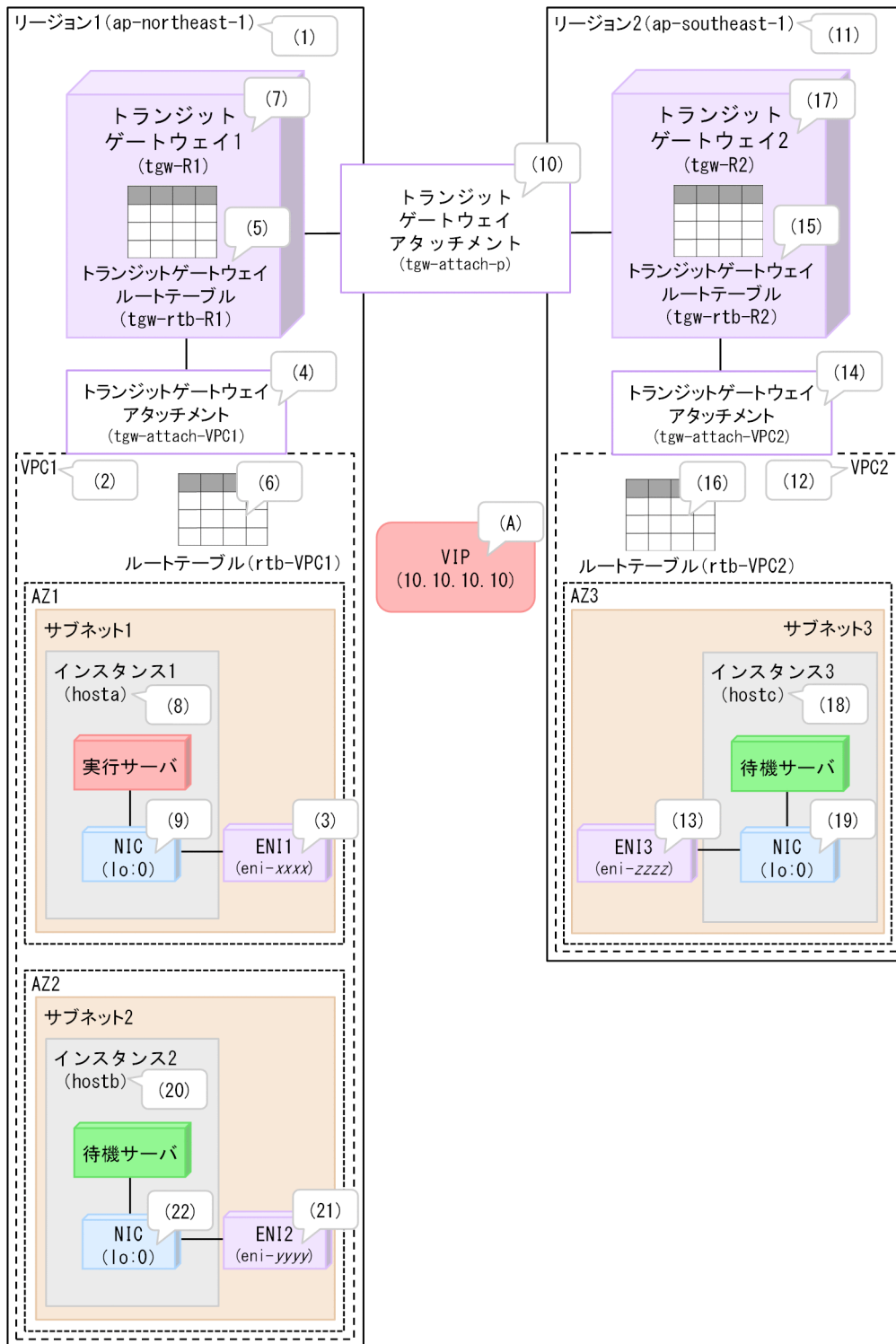
## ホスト情報 ##
host
{
  host_name=hosta ... (8)
  host_region=ap-northeast-1 ... (1)
  host_vpc=VPC1 ... (2)
  host_vip[0]=10.10.10.10 ... (A)
  host_eni[0]=eni-xxxx ... (3)
  host_tgw_attachment[0]=twg-attach-VPC1 ... (4)
}
```

```
host
{
host_name=hostb ... (18)
host_region=ap-southeast-1 ... (11)
host_vpc=VPC2 ... (12)
host_vip[0]=10.10.10.10 ... (A)
host_eni[0]=eni-yyyy ... (13)
host_tgw_attachment[0]=tgw-attach-VPC2 ... (14)
}
```



同一の VPC 内の複数の AZ 間、および複数のリージョン間で系切り替えをする構成の場合

図 5-8 同一の VPC 内の複数の AZ 間、および複数のリージョン間で系切り替えをする構成例



上記の図に対応する、LANの状態設定ファイルの設定例は次のとおりです。設定例中の"*(n)*"は、図中の"*(n)*"と対応しています。

現用系 (インスタンス 1) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash
set -x
```

```
#####  
HOSTNAME=hosta ... (8)  
VIP[0]=10.10.10.10 ... (A)  
LABEL[0]=lo:0 ... (9)  
#####
```

: (以下を編集しないこと)

予備系 (インスタンス 2) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash  
set -x  
#####  
HOSTNAME=hostb ... (20)  
VIP[0]=10.10.10.10 ... (A)  
LABEL[0]=lo:0 ... (22)  
#####
```

: (以下を編集しないこと)

予備系 (インスタンス 3) のサーバ識別名.up ファイル, サーバ識別名.down ファイル

```
#!/bin/bash  
set -x  
#####  
HOSTNAME=hostc ... (18)  
VIP[0]=10.10.10.10 ... (A)  
LABEL[0]=lo:0 ... (19)  
#####
```

: (以下を編集しないこと)

vip\_tgw\_def ファイル

```
## トランジットゲートウェイ情報 ##  
tgw  
{  
  tgw_id=twg-R1 ... (7)  
  tgw_region=ap-northeast-1 ... (1)  
  tgw_vip[0]=10.10.10.10 ... (A)  
  tgw_route_table[0]=twg-rtb-R1 ... (5)  
  tgw_attachment=twg-attach-VPC1 ... (4)  
  tgw_peering_attachment=twg-attach-P ... (10)  
}  
  
tgw  
{  
  tgw_id=twg-R2 ... (17)  
  tgw_region=ap-southeast-1 ... (11)  
  tgw_vip[0]=10.10.10.10 ... (A)  
  tgw_route_table[0]=twg-rtb-R2 ... (15)  
  tgw_attachment=twg-attach-VPC2 ... (14)  
  tgw_peering_attachment=twg-attach-P ... (10)  
}  
  
## ルートテーブル情報 ##  
rtb  
{
```

```

rtb_id=rtb-VPC1 ... (6)
rtb_region=ap-northeast-1 ... (1)
rtb_vpc=VPC1 ... (2)
rtb_vip[0]=10.10.10.10 ... (A)
rtb_tgw[0]=tgw-R1 ... (7)
}

rtb
{
rtb_id=rtb-VPC2 ... (16)
rtb_region=ap-southeast-1 ... (11)
rtb_vpc=VPC2 ... (12)
rtb_vip[0]=10.10.10.10 ... (A)
rtb_tgw[0]=tgw-R2 ... (17)
}

## ホスト情報 ##
host
{
host_name=hosta ... (8)
host_region=ap-northeast-1 ... (1)
host_vpc=VPC1 ... (2)
host_vip[0]=10.10.10.10 ... (A)
host_eni[0]=eni-XXXX ... (3)
host_tgw_attachment[0]=tgw-attach-VPC1 ... (4)
}

host
{
host_name=hostb ... (20)
host_region=ap-northeast-1 ... (1)
host_vpc=VPC1 ... (2)
host_vip[0]=10.10.10.10 ... (A)
host_eni[0]=eni-YYYY ... (21)
host_tgw_attachment[0]=tgw-attach-VPC1 ... (4)
}

host
{
host_name=hostc ... (18)
host_region=ap-southeast-1 ... (11)
host_vpc=VPC2 ... (12)
host_vip[0]=10.10.10.10 ... (A)
host_eni[0]=eni-ZZZZ ... (13)
host_tgw_attachment[0]=tgw-attach-VPC2 ... (14)
}

```

## (2) DNS 制御の場合

DNS 制御の場合、LAN の状態設定ファイルは次のサンプルファイルを基に作成してください。

- server\_aws\_vpc.up
- server\_aws\_vpc.down

設定方法は、「5.13.2 【AWS】 LAN の状態設定ファイルの設定 (1つのリージョン内または1つのVPC内で系切り替えをする構成の場合)」を参照してください。

次のどちらの場合でも、設定方法は同じです。

- DNS 制御によって、1つのリージョン内または1つのVPC内で系切り替えをする場合
- DNS 制御によって、複数のリージョン間または複数のVPC間で系切り替えをする場合

ただし、説明中のサンプルファイル名は、次のとおりに読み替えてください。

- 「server\_aws.up」を「server\_aws\_vpc.up」に読み替える。
- 「server\_aws.down」を「server\_aws\_vpc.down」に読み替える。

### 5.13.4 【AWS】 LAN の状態設定ファイルの設定 (クライアントからの通信がNLBを経由する構成の場合)

設定方法については、1つのリージョン内または1つのVPC内で系切り替えをする構成の場合と同じです。詳細は「5.13.2 【AWS】 LAN の状態設定ファイルの設定 (1つのリージョン内または1つのVPC内で系切り替えをする構成の場合)」を参照してください。

### 5.13.5 【Azure】 LAN の状態設定ファイルの設定

HA モニタでは、LAN はサーバ単位に接続、切り離しをします。そのため、LAN の状態設定ファイルを作成して設定する必要があります。

LAN の状態設定ファイルの種類を、次に示します。

サーバ識別名.up ファイル

LAN を接続する場合に使用します。業務通信の切り替えに関する情報を設定します。

サーバ識別名.down ファイル

LAN の切り離しをする場合に使用します。業務通信の切り替えに関する情報を設定します。

これらのファイルは、サーバごとに HA モニタの環境設定用ディレクトリの下に作成します。ファイル名のサーバ識別名の部分は、サーバ対応の環境設定のalias オペランドで指定した値にしてください。

LAN の状態設定ファイルには、OS のip コマンドの引数として、LAN アダプタに追加・削除するエイリアス IP アドレスを指定します。OS のコマンドについては、OS のマニュアルを参照してください。

Azure 用シェルスクリプト群を展開すると、Azure 用の LAN の状態設定ファイルのサンプルファイルが、/opt/hitachi/HAMon/lib 配下に配置されます。Azure 用シェルスクリプト群の展開については、「5.8 【Azure】 Azure 用のシェルスクリプト群の展開」を参照してください。サンプルファイルの名称は、server\_azure.up およびserver\_azure.down です。

server\_azure.up およびserver\_azure.down のファイル内容を次に示します。

```
#!/bin/bash
set -x

#####
# LB_IPADDR[0]=aa. aa. aa. aa
# LB_PORT[0]=bbbb

# LB_IPADDR[1]=cc. cc. cc. cc
# LB_PORT[1]=dddd

# DNS_PUBLICZONE[0]=eeee. com
# DNS_PRIVATEZONE[0]=ffff. com
# DNS_RECORDSET[0]=gggg
# DNS_RESOURCEGROUP[0]=hhhh
# DNS_TYPE[0]=A
# DNS_VALUE[0]=ii. ii. ii. ii
# DNS_TTL[0]=jj

# DNS_PUBLICZONE[1]=kkkk. com
# DNS_PRIVATEZONE[1]=llll. com
# DNS_RECORDSET[1]=mmmm
# DNS_RESOURCEGROUP[1]=nnnn
# DNS_TYPE[1]=CNAME
# DNS_VALUE[1]=oooo. com.
# DNS_TTL[1]=pp

#####
function main() {
:
```

サーバごとに、サンプルファイルを/opt/hitachi/HAMon/etc 配下にコピーして、server\_azure.up をサーバ識別名.up に、server\_azure.down をサーバ識別名.down にリネームしてください。

サーバ識別名.up/down で設定が必要なシェル変数について説明します。

## メモ

ここで説明する[n]は配列の添え字です。業務通信に使用する仮想マシンのエイリアス IP アドレス、または業務通信に使用する DNS 名が 1 つの場合、[n]は 0 です。複数ある場合、1 つ目の[n]は 0、2 つ目の[n]は 1、のように、添え字が 0 から順に 1 ずつ増加するように設定してください。

サンプルファイルからコピーした状態では、シェル変数部分はコメント行となっています。コメント行を表す先頭の"#"を削除してから、設定してください。例えば、業務通信に使用する仮想マシンのエイリアス IP アドレスが 1 つの場合は、次のシェル変数について、コメント"#"を削除し、シェル変数を設定します。

- LB\_IPADDR[0]
- LB\_PORT[0]

2つの場合は、次のシェル変数について、コメント"#"を削除し、シェル変数を設定します。

- LB\_IPADDR[0]
- LB\_PORT[0]
- LB\_IPADDR[1]
- LB\_PORT[1]

3つ目以降については、シェル変数をコピーするなどの方法で、設定してください。

Azure ロードバランサー制御によって業務通信を切り替える場合

"LB\_"から始まるシェル変数を次のとおりに設定してください。

- LB\_IPADDR[n]

仮想マシンに付与または削除するエイリアス IP アドレスを設定してください。エイリアス IP アドレスは、業務通信に使用する IP アドレスで、Azure ロードバランサーのフロントエンドに設定した IP アドレスと同じアドレスを指定します。すべての系切り替え構成内で同じ設定にしてください。

- LB\_PORT[n]

Azure ロードバランサーからの正常性確認を待ち受けるポート番号を設定してください。すべての系切り替え構成内で同じ設定にしてください。

LB\_IPADDR および LB\_PORT の値は、異なる添え字間で重複しないように設定してください。

LB\_IPADDR および LB\_PORT の値は、異なるサーバ間（異なるサーバ識別名.up 間および異なるサーバ識別名.down 間）で重複しないように設定してください。

DNS 名制御によって業務通信を切り替える場合

レコードの変更方法によって、LAN の状態設定ファイルのシェル変数の設定方法が異なります。シェル変数の設定要否を次の表に示します。

表 5-6 LAN の状態設定ファイルのシェル変数の設定要否

| レコードの変更方法              | シェル変数の設定要否     |                  |
|------------------------|----------------|------------------|
|                        | サーバ識別名.up ファイル | サーバ識別名.down ファイル |
| レコードを更新する方法            | 必要             | 不要*              |
| レコードを削除したあとレコードを追加する方法 | 必要             | 必要               |

注※

シェル変数の設定は不要ですが、サーバ識別名.down ファイルは/opt/hitachi/HAMon/etc 配下に作成する必要があります。

"DNS\_"から始まるシェル変数のコメントアウトを外し、次のとおりに設定してください。

- DNS\_PUBLICZONE[n]

DNS ゾーンがパブリックゾーンの場合に、業務通信に使用する DNS 名を管理対象に含む、DNS ゾーン名を設定してください。すべての系切り替え構成内で同じ設定にしてください。

- DNS\_PRIVATEZONE[n]

DNS ゾーンがプライベートゾーンの場合に、業務通信に使用する DNS 名を管理対象に含む、DNS ゾーン名を設定してください。すべての系切り替え構成内で同じ設定にしてください。

- DNS\_RECORDSET[n]

レコードのレコードセット名を設定してください。すべての系切り替え構成内で同じ設定にしてください。

### メモ

DNS ゾーン名とレコードセット名によって、業務通信に使用する DNS 名が決定します。例えば、DNS\_PUBLICZONE[0]=hitachi.com, DNS\_RECORDSET[0]=sample の場合、業務通信に使用する DNS 名は sample.hitachi.com となります。

- DNS\_RESOURCEGROUP[n]

DNS ゾーンを含みリソースグループ名を設定してください。すべての系切り替え構成内で同じ設定にしてください。

- DNS\_TYPE[n]

DNS レコードタイプ (A レコードタイプまたは CNAME レコードタイプ) を設定してください。A レコードタイプは、名前解決の結果である IPv4 アドレスを記録します。CNAME レコードタイプは、名前解決を実行する別の DNS 名を記録します。すべての系切り替え構成内で同じ設定にしてください。

- DNS\_VALUE[n]

DNS レコードタイプが A レコードタイプの場合は IPv4 アドレス、CNAME レコードタイプの場合は DNS 名を設定してください。設定する値は系ごとに異なります。

- DNS\_TTL[n]

レコードがクライアントによってキャッシュされる時間 (秒) を設定してください。

DNS\_TTL で設定された時間内は、キャッシュ内の値を使用して業務通信します。

DNS\_TTL の値が大きすぎると、HA モニタが実行サーバを系切り替えしても、切り替え元の系で業務通信するおそれがあります。そのため、次の手順で DNS\_TTL を決めてください。

1. DNS 名制御を使用した計画系切り替えを実施し、系切り替え時間を計測<sup>※</sup>する。

2. 計測した系切り替え時間より小さい値を DNS\_TTL に設定する。

注※ 系切り替え元でメッセージKAMN290-I を出力してから、系切り替え先でメッセージKAMN311-I を出力するまでの時間を計測します。



## 5.13.6 【OCI】 LAN の状態設定ファイルの設定

HA モニタでは、LAN はサーバ単位に接続、切り離しをします。そのため、LAN の状態設定ファイルを作成して設定する必要があります。

LAN の状態設定ファイルの種類を、次に示します。

サーバ識別名.up ファイル

LAN を接続する場合に使用します。業務通信の切り替えに関する情報を設定します。

サーバ識別名.down ファイル

LAN の切り離しをする場合に使用します。業務通信の切り替えに関する情報を設定します。

これらのファイルは、サーバごとに HA モニタの環境設定用ディレクトリの下に作成します。ファイル名のサーバ識別名の部分は、サーバ対応の環境設定のalias オペランドで指定した値にしてください。

LAN の状態設定ファイルには、OS のip コマンドの引数として、LAN アダプタに追加・削除するエイリアス IP アドレスを指定します。OS のコマンドについては、OS のマニュアルを参照してください。

OCI 用シェルスクリプト群を展開すると、OCI 用の LAN の状態設定ファイルのサンプルファイルが、/opt/hitachi/HAMon/lib 配下に配置されます。OCI 用シェルスクリプト群の展開については、[\[5.9 【OCI】 OCI 用のシェルスクリプト群の展開\]](#) を参照してください。サンプルファイルの名称は、server\_oci.up およびserver\_oci.down です。

server\_oci.up およびserver\_oci.down のファイル内容を次に示します。

```
#!/bin/bash
set -x

#####
# PIP_ADDRESS[0]=aa.aa.aa.aa
# PIP_PREFIX[0]=bb
# PIP_VNIC[0]=cccc
# PIP_LABEL[0]=eth0:0

# PIP_ADDRESS[1]=dd.dd.dd.dd
# PIP_PREFIX[1]=ee
# PIP_VNIC[1]=ffff
# PIP_LABEL[1]=eth1:0

#####
function main() {
:
```

サーバごとに、サンプルファイルを/opt/hitachi/HAMon/etc 配下にコピーして、server\_oci.up をサーバ識別名.up に、server\_oci.down をサーバ識別名.down にリネームしてください。

サーバ識別名.up/down で設定が必要なシェル変数について説明します。



## メモ

ここで説明する[n]は配列の添え字です。業務 IP アドレスとして使用するプライベート IP アドレスが1つの場合、[n]は0です。複数ある場合、1つ目の[n]は0、2つ目の[n]は1、のように、添え字が0から順に1ずつ増加するように設定してください。

サンプルファイルからコピーした状態では、シェル変数部分はコメント行となっています。コメント行を表す先頭の"#"を削除してから、設定してください。例えば、業務 IP アドレスとして使用するプライベート IP アドレスが1つの場合は、次のシェル変数について、コメント"#"を削除し、シェル変数を設定します。

- PIP\_ADDRESS[0]
- PIP\_PREFIX[0]
- PIP\_VNIC[0]
- PIP\_LABEL[0]

2つの場合は、次のシェル変数について、コメント"#"を削除し、シェル変数を設定します。

- PIP\_ADDRESS[0]
- PIP\_PREFIX[0]
- PIP\_VNIC[0]
- PIP\_LABEL[0]
- PIP\_ADDRESS[1]
- PIP\_PREFIX[1]
- PIP\_VNIC[1]
- PIP\_LABEL[1]

3つ目以降については、シェル変数をコピーするなどの方法で、設定してください。

"PIP\_"から始まるシェル変数を次のとおりに設定してください。

- PIP\_ADDRESS[n]  
業務 IP アドレスとして使用するプライベート IP アドレスを設定してください。すべての系切り替え構成内で同じ設定にしてください。
- PIP\_PREFIX[n]  
業務 IP アドレスのプリフィックスを設定してください。すべての系切り替え構成内で同じ設定にしてください。
- PIP\_VNIC[n]  
プライベート IP アドレスを割り当てる VNIC の OCID を設定してください。設定ミスを防ぐため、コピー&ペーストを使用して設定してください。系によって値が異なります。

- PIP\_LABEL[n]

プライベート IP アドレスを付与する OS 上の LAN インタフェースを"LAN インタフェース名:xxx"の形式で設定してください。すべての系切り替え構成内で同じ設定にしてください。

## 5.14 リソースの監視のための設定

リソースの監視のための設定については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「リソースの監視のための設定」の説明を参照してください。この節では、リソースの監視のための設定について、パブリッククラウド環境下で差異がある事項だけを記載します。

リソースの監視のための設定について説明します。リソースには、LAN およびディスクがあります。

### 5.14.1 LAN の監視に必要なファイルの設定

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「LAN の監視に必要なファイルの設定」を参照してください。ただし、パブリッククラウド環境下では次の点が異なります。

- LAN 監視定義ファイル (LAN インタフェース名称.conf) に指定する確認用パケット送出先としては、次のすべての条件を満たす送出先の IP アドレスを指定してください。
  - ・ HA モニタを起動する前に、送出先が起動していること。送出先より HA モニタを先に起動すると、LAN 障害を検知してしまいます。
  - ・ 送出先は、HA モニタの稼働する系ではないこと。ペアとなる HA モニタがある系の IP アドレスは指定しないでください。
- HA モニタの環境設定の `lancheck_mode` オペランドを `route` に設定してください。
- 必ず HA モニタ 01-70 以降で提供する LAN 監視スクリプト (`lanpatrol.sh`) を使用してください。
- LAN 監視スクリプトには、次の条件を満たす送信元 IP アドレスを指定してください。
  - ・ 監視対象とする LAN インタフェースに付与されたステーションナリ IP アドレス。エイリアス IP アドレスを指定すると、LAN 障害を検知してしまうおそれがあります。

LAN の監視のスクリプトの修正例を次に示します。太字の個所を追記してください。

```
#!/bin/sh
#*****
#*
#* Linux(x86) HA Monitor
#* This is a sample of the LAN patrol command.
#*
#* [SYNOPSIS]
#* lanpatrol.sh interface [-r]
#* [OPTIONS]
#* interface
#* The name of the LAN interface.
#* -r
#* Route monitoring method
#* [DIAGNOSTICS]
#* 0 : normal
#* 1 : abnormal
#* 2 : error
#*
#* All Rights Reserved. Copyright (C) 2011, 2019, Hitachi, Ltd.
#*
```

```

*****
#set -x

# retry interval(seconds) for receive packet number method. or
# return wait(seconds) of ping command for route monitoring method.
WAIT_TIME=3

# retry counter
RETRY=3

# check interface and source IP address
PATROL_IF[0]=eth0
SOURCE_IP[0]=192.168.0.1
PATROL_IF[1]=eth1
SOURCE_IP[1]=192.168.1.2

# environment variables
PATH=/usr/bin:/usr/sbin:/bin
export PATH

:
:
:

*****
#* [NAME] *
#* exec_route_ping - execute ping command and wait return *
#* [SYNOPSIS] *
#* exec_route_ping interface *
#* [OPTIONS] *
#* interface *
#* The name of the LAN interface. *
#* [RETURN VALUE] *
#* none *
*****
exec_route_ping() {
    # specific source IP address
    SRCIP=""
    index=0
    while [ ${PATROL_IF[$index]} ]
    do
        if [ ${PATROL_IF[$index]} = "$1" ]; then
            SRCIP="-I ${SOURCE_IP[$index]}"
            break
        fi
        index=`expr $index + 1`
    done
    # send some ECHO_REQUESTs and wait returns
    unset ping_pid
    unset dest_ip
    index=0
    while read P_IPADDR
    do
        echo "`date` exec_route_ping read() DEST_IPADDR=`echo ${P_IPADDR}` WAIT=`echo ${W
AIT_TIME}` SRC=`echo ¥ ${SRCIP:-unspecified}¥`"
        (time ping -c 1 -w ${WAIT_TIME} ${SRCIP} ${P_IPADDR}) &
        ping_pid[$index]=$!
        dest_ip[$index]=${P_IPADDR}
    done
}

```

```

        index=`expr $index + 1`
done < ./etc/$1.conf
echo "`date` exec_route_ping wait() start"
unset ping_rtcd
index=0
while [ ${ping_pid[$index]} ]
do
    wait ${ping_pid[$index]}
    ping_rtcd[$index]=$?
    echo "`date` DEST_IPADDR=${dest_ip[$index]}, RESULT=${ping_rtcd[$index]}"
    index=`expr $index + 1`
done
echo "`date` exec_route_ping wait() end"
return
}

:

```

- ・ PATROL\_IF[x]に監視対象の LAN インタフェース名を指定します。
- ・ SOURCE\_IP[x]に送信元 IP アドレスを指定します。

それぞれ[x]は配列の添え字です。監視対象のインタフェース名と送信元 IP アドレスの組み合わせで添え字をそろえて指定してください。組み合わせが一つの場合でも添え字[0]を指定してください。

送信元 IP アドレスには、ステーションナリ IP アドレスが指定できます。エイリアス IP アドレスは指定できません。IP ラベルも指定できますが、ホスト名の解決に時間が掛かることがあります。このため、IP アドレスを記述することを推奨します。

送信元に IP ラベルを指定する場合であっても、変数名は"SOURCE\_IP"とし、変更しないでください。

# 6

## システムの運用

この章では、構築したシステムの運用について説明します。起動・停止方法、障害が発生した場合のオペレータの操作、障害発生を防ぐための運用、および運用を自動化する方法やシステムを変更する方法などについて説明します。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「システムの運用」とあわせてお読みください。

## 6.1 起動・停止

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「起動・停止」を参照してください。ただし、AWS 環境下および Azure 環境下では次の点が異なります。

- HA モニタを起動する前に、レプリケーションソフトを起動する。
- HA モニタを停止したあとに、レプリケーションソフトを停止する。

## 6.2 システムの変更

---

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「システムの変更」を参照してください。この節では、システムの変更について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 6.2.1 サーバを追加する

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「サーバを追加する」を参照してください。ただし、AWS 環境下および Azure 環境下では加えて次の準備も必要になります。

- サーバを追加する場合の準備として、DRBD のリソースを追加する。

### 6.2.2 系やサーバを稼働させたままリソースの構成を変更する

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系やサーバを稼働させたまま共有リソースの構成を変更する」を参照してください。ただし、AWS 環境下および Azure 環境下では次の点が異なります。

- DRBD リソースの動的変更はできない。



## 6.3 システム運用時の注意事項

ここでは、システム運用時の注意事項について説明します。

### 6.3.1 パブリッククラウド環境のコンソール操作（CLI 発行含む）をする場合の注意事項

パブリッククラウド環境のコンソール操作（CLI 発行含む）をする場合の注意事項について、説明します。

HA モニタでのエラーを回避するために、系切り替え構成内のインスタンス（Azure の仮想マシンも含む）に対するパブリッククラウド環境のコンソール操作（CLI 発行含む）は、必要最低限にしてください。

HA モニタは CLI を実行して、強制停止などの操作を実施します。HA モニタ以外のアプリケーションやユーザによるインスタンスの操作と、HA モニタによる CLI の実行タイミングが重なると、HA モニタがエラーメッセージを出力したり、系切り替えに失敗したりするおそれがあります。

エラーメッセージが出力されたときは、内容を確認して対処してください。系切り替えに失敗したときは、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「系のリセット失敗に対処する」を参照してください。

### 6.3.2 【AWS】【Azure】レプリケーションソフトを使用する場合の注意事項

レプリケーションソフトを使用する場合の注意事項について、説明します。

- HA モニタのメッセージだけでなく、レプリケーションソフトが出力するメッセージにも従い、適切に対処してください。
- レプリケーションソフトを使用する場合、系ごとに業務ディスクを配置する構成にします。これらの業務ディスクのデータをレプリケーションソフトによって同期します。業務ディスクのデータが同期できている場合は、最新の業務ディスクのデータにアクセスできている状態のため、問題ありません。しかし、次の状態の場合は、業務ディスクのデータが同期されていないため、どれかの系の業務ディスクのデータが古くなっています。
  - 系間のレプリケーションパスが接続できていない状態  
セカンダリ側の系の業務ディスクのデータが古くなっています。
  - 系またはレプリケーションソフトが起動していない状態  
起動していない系の業務ディスクのデータが古くなっています。
  - 業務ディスクに障害が発生した状態  
障害が発生した業務ディスクのデータが古くなっています。

これらの状態になっている場合は、速やかに系間でレプリケーションできる状態に回復し、データを同期させてください。状態を回復させるまでは、業務ディスクのデータが古い系で、実行サーバを起動し

ないでください。状態が回復しないままシステムを停止し、業務ディスクのデータが古い系だけを起動した場合、業務ディスクのデータが古い系で実行サーバが起動するおそれがあります。業務ディスクのデータが古い系で実行サーバが起動してしまった場合は、速やかに実行サーバを停止してください。

なお、実行サーバが、データが古い業務ディスクを更新した場合は、その業務ディスクと最新のデータを持つ業務ディスクは同期できません。最新のデータを持つ業務ディスクを同期の元として生かすように、レプリケーションソフトの回復運用をしてください。詳細は、レプリケーションソフトのドキュメントを参照してください。

- プライマリ側の系からセカンダリ側の系に業務ディスクのデータを同期中に、プライマリ側の系障害による系切り替えが発生した場合、セカンダリ側では業務ディスクにアクセスできません。このため、セカンダリ側の実行サーバの停止、およびプライマリ側の系と実行サーバを再起動してください。

プライマリ側の系からセカンダリ側の系に業務ディスクのデータを同期中に、プライマリ側の実行サーバ障害による系切り替え、または計画系切り替えが発生した場合は、ディスクにアクセスできるため、対処は不要です。

- レプリケーションする別の系が障害で起動できない場合などに、系をスタンドアロンで運用するときは、次のことを確認してください。

- ・OSを起動したあと、サーバを起動する前に、DRBD リソースのdiskの状態がUpToDateになっていること

レプリケーションソフトは、別の系とレプリケーションパスで接続して互いに状態を確認するまで、diskの状態がConsistentになっている場合があります。この場合、auto-promoteによる自動プライマリ化ができないため、ディスクを使用できず、サーバの起動に失敗するおそれがあります。diskの状態がConsistentになっている場合は、次の操作をして、diskの状態がUpToDateになったことを確認してからサーバを起動してください。

手動でプライマリ化する

```
# drbdadm primary リソース名
```

diskの状態がUpToDateになったことを確認する

```
# drbdadm status リソース名
```

auto-promoteによる自動プライマリ化を有効にするため、セカンダリ化する

```
# drbdadm secondary リソース名
```

# 7

## 環境設定で定義するファイル

HA モニタを使用するに当たって、ユーザは HA モニタおよびサーバの環境設定を定義ファイルにする必要があります。この章では、定義の記述規則、定義ファイルに指定するオペランド、および環境設定例について説明します。なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「環境設定で定義するファイル」とあわせてお読みください。

## 7.1 定義ファイルの概要

---

ここでは、ユーザが環境設定で定義するファイルについて説明します。定義する必要がある環境設定のファイルを、次に示します。

- **sysdef** ファイル  
HA モニタが動作するための環境設定をします。詳細については、「[7.2 HA モニタの環境設定](#)」を参照してください。
- **servers** ファイル  
サーバが動作するための環境設定をします。リソースサーバを使用する場合も、**servers** ファイルで環境設定をします。詳細については、「[7.3 サーバの環境設定](#)」を参照してください。

系に定義ファイルを設定するに当たっての注意事項を、次に示します。

- 定義ファイルは、HA モニタがあるすべての系で設定してください。
- 定義ファイルの作成に当たって、定義ファイルのオペランドを現用・予備系で同じ値にする必要がある個所と、異なる値にする必要がある個所があります。
- 定義ファイルの作成が完了したら、必ずすべての系に配布した上で、定義チェックコマンド (**moncheck** コマンド) を実行してください。

## 7.2 HA モニタの環境設定

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタの環境設定」の説明を参照してください。この節では、HA モニタの環境設定について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 7.2.1 パブリッククラウド環境固有の HA モニタの環境設定

ここでは、パブリッククラウド環境固有の HA モニタの環境設定について説明します。

次に説明する `public_cloud` オペランドは、HA モニタの環境設定 (sysdef) の `function` 定義文のオペランドです。

#### (1) `public_cloud`

##### ユーザ指定値

| 値の種別                                  | 数値の範囲          | 値の省略 | 指定を省略したときの仮定値      |
|---------------------------------------|----------------|------|--------------------|
| <code>use</code>   <code>nouse</code> | --<br>(単位: --) | 可    | <code>nouse</code> |

##### 説明

パブリッククラウド環境で、系切り替えをするかどうかを指定します。系切り替え構成内のすべての系で同じ値を指定してください。

- `use` : パブリッククラウド環境で系切り替えをする
- `nouse` : パブリッククラウド環境で系切り替えをしない

#### (2) `fence_network`

##### ユーザ指定値

| 値の種別                                  | 数値の範囲          | 値の省略 | 指定を省略したときの仮定値      |
|---------------------------------------|----------------|------|--------------------|
| <code>use</code>   <code>nouse</code> | --<br>(単位: --) | 可    | <code>nouse</code> |

##### 説明

ネットワーク遮断による系切り替え機能を使用するかどうかを指定します。系切り替え構成内のすべての系で同じ値を指定してください。`public_cloud` オペランドに `use` を指定していない場合は、このオペランドを指定しても無視されます。

- use : ネットワーク遮断による系切り替え機能を使用する
- nouse : ネットワーク遮断による系切り替え機能を使用しない

このオペランドにuse を指定した場合、次の点に注意してください。

- clearwait オペランドとclearcheck オペランドの値は 30 秒になります。
- fence\_network オペランドにuse を指定した場合も系のリセットによって系切り替えをするため、パブリッククラウド環境でのリセットに関するオペランドが有効になります。詳細については、「7.2.2 パブリッククラウド環境で注意が必要な HA モニタの環境設定のオペランド」を参照してください。また、注意が必要な HA モニタの環境設定のオペランドとして記載されていないcpudown オペランドおよびreset\_type オペランドも有効になります。
- HA モニタのネットワーク遮断設定ファイルを設定してください。  
ネットワーク遮断設定ファイルの設定については、「5.12.3 【AWS】 ネットワーク遮断設定ファイルの設定」を参照してください。

## 7.2.2 パブリッククラウド環境で注意が必要な HA モニタの環境設定のオペランド

パブリッククラウド環境下で HA モニタを使用する場合に、注意が必要なオペランドについてだけ次の表で説明します。各オペランドの詳細については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタの環境設定」の説明を参照してください。

表 7-1 注意が必要な HA モニタの環境設定のオペランド

| オペランド名       | 注意事項  |
|--------------|---|
| lan          | public_cloud オペランドにuse を指定した場合、監視パスは 1 つだけ指定してください。監視パスを複数にする必要がある場合は、Linux でbonding を設定し、bonding デバイスを監視パスに指定してください。   |
| hostmax      | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| clearwait    | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。なお、系リセット発行待ち時間は次のとおりになります。 <ul style="list-style-type: none"> <li>• AWS 環境または Azure 環境のとき：120 秒</li> <li>• OCI 環境のとき：30 秒</li> <li>• fence_network オペランドにuse を指定したとき：30 秒</li> </ul>  |
| resetpatrol  | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| standbyreset | public_cloud オペランドにuse を指定した場合、次の点に注意してください。 <ul style="list-style-type: none"> <li>• レプリケーションソフトを使用するとき<sup>*1</sup><br/>このオペランドの指定値に関係なく、待機系をリセットします。</li> <li>• レプリケーションソフトを使用しないとき<sup>*2</sup><br/>このオペランドの指定値が有効となります。</li> </ul> |

| オペランド名           | 注意事項  |
|------------------|---|
| netmask          | public_cloud オペランドにuse を指定した場合、このオペランドの指定値に関係なく、bit が仮定されます。  |
| partition_reset  | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| alive_multicast  | public_cloud オペランドにuse を指定した場合、このオペランドにuse を指定しないでください。   |
| multicast_lan    | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| vmware_env       | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| resetpatrol_mode | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| fence_reset      | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| fence_scsi       | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| fence_lan        | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| scsi_check       | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| scsi_pathcheck   | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| scsi_timeout     | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| scsi_retry       | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| hbond_lacp       | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| notswitch_notify | public_cloud オペランドにuse を指定した場合、次の状態でも警告メッセージを出力します。 <ul style="list-style-type: none"> <li>パブリッククラウド環境の情報取得で異常を検知している場合：メッセージKAMN767-W</li> <li>AWS CLI, Azure CLI, または OCI CLI の実行可否チェックで異常を検知している場合：メッセージKAMN769-W</li> </ul> |
| resetpath_retry  | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| resetpath_inter  | public_cloud オペランドにuse を指定した場合、このオペランドの指定は無視されます。   |
| lancheck_mode    | public_cloud オペランドにuse を指定し、lanfailswitch オペランドにuse を指定した場合、このオペランドには、route を指定してください。  |
| clearcheck       | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。なお、系のリセット終了時間は次のとおりになります。 <ul style="list-style-type: none"> <li>AWS 環境または Azure 環境のとき：120 秒</li> <li>OCI 環境のとき：30 秒</li> <li>fence_network オペランドにuse を指定したとき：30 秒</li> </ul> |

#### 注※1

レプリケーションソフト用のシェルスクリプト群を展開しているとき。

なお、下記の構成との混在を含みます。

- AWS 環境での、EBS マルチアタッチ、または EFS による共有ディスク構成
- Azure 環境での、マネージドディスクによる共有ディスク構成

## 注※2

レプリケーションソフト用のシェルスクリプト群を展開していないとき。

下記の構成および環境が該当します。

- AWS 環境での、EBS マルチアタッチ、または EFS による共有ディスクだけの構成
- Azure 環境での、マネージドディスクによる共有ディスクだけの構成
- OCI 環境



## 7.3 サーバの環境設定

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「サーバの環境設定」の説明を参照してください。この節では、サーバの環境設定について、パブリッククラウド環境下で差異がある事項だけを記載します。

### 7.3.1 パブリッククラウド環境固有のサーバの環境設定

ここでは、パブリッククラウド環境固有のサーバの環境設定について説明します。

#### (1) rep\_device

##### ユーザ指定値

| 値の種別                  | 数値の範囲         | 値の省略 | 指定を省略したときの仮定値 |
|-----------------------|---------------|------|---------------|
| 1~128 文字の DRBD のリソース名 | --<br>(単位:--) | 可    | --            |

##### 説明

AWS 環境または Azure 環境の場合に、ディスクをレプリケーションする構成を使用するときに指定します。

「5.5 【AWS】【Azure】レプリケーションソフト (DRBD) の設定」で設定した DRBD のリソース名を指定してください。ただし、DRBD のリソース名は、次の条件を満たす必要があります。

- DRBD のリソース名は、1~128 文字の英字、数字、/, -, \_, .で指定する。
- 最大 256 個指定できる。リソースサーバを含む全サーバの指定値の合計が 256 個以内となるようにする。
- 系切り替え構成内のすべての系で同じ値を指定する。

次の手順によって、業務で使用する VG 名を基に、DRBD のリソース名を取得することもできます。

1. 次のコマンドを実行して、PV 名を確認します。

```
# vgdisplay -v VG名
```

実行例を次に示します。太字の部分 PV 名です。

```
# vgdisplay -v Vol00
--- Volume group ---
VG Name              Vol00
System ID
: (途中省略)
--- Physical volumes ---
```

```
PV Name          /dev/drbd5
PV UUID
: (途中省略)
```

2. 次のコマンドを実行して、対象の DRBD リソースが定義された DRBD の設定ファイルを確認します。

```
# grep -rl PV名 /etc/drbd.d/
```

実行例を次に示します。太字の部分が DRBD の設定ファイルです。

```
# grep -rl /dev/drbd5 /etc/drbd.d/
/etc/drbd.d/r0.res
```

3. 次のコマンドを実行して、DRBD の設定ファイルの内容を表示します。手順 1. で確認した PV を使用している resource セクションを探し、DRBD のリソース名を取得します。

```
# cat DRBD設定ファイル
```

実行例を次に示します。1 つ目の太字の部分が DRBD のリソース名、2 つ目の太字の部分が手順 1. で確認した PV です。

```
# cat /etc/drbd.d/r0.res
resource r0 {
  volume 0 {
    device /dev/drbd5;
    disk /dev/xvdf1;
    meta-disk internal;
  }
  volume 1 {
    : (以下省略)
```

以上の手順で取得した DRBD のリソース名を rep\_device オペランドに指定してください。

## 7.3.2 パブリッククラウド環境で注意が必要なサーバ対応の環境設定のオペランド

ここでは、パブリッククラウド環境下で HA モニタを使用する場合に、注意が必要なオペランドについてだけ記載します。各オペランドの詳細については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「サーバの環境設定」の説明を参照してください。

表 7-2 注意が必要なサーバ対応の環境設定のオペランド

| オペランド名           | 注意事項  |
|------------------|---|
| hab_gid          | public_cloud オペランドに use を指定した場合、このオペランドは指定しないでください。 |
| hab_discnt_atend | public_cloud オペランドに use を指定した場合、このオペランドは指定しないでください。 |
| scsi_device      | public_cloud オペランドに use を指定した場合、このオペランドは指定しないでください。 |
| dmmp_device      | public_cloud オペランドに use を指定した場合、このオペランドは指定しないでください。 |

| オペランド名       | 注意事項  |
|--------------|---|
| switch_judge | public_cloud オペランドにuse を指定した場合、このオペランドは指定しないでください。  |
| fs_name      | AWS 環境で EFS を使用する場合、ファイルシステムの DNS 名とマウントするディレクトリをダブルクォーテーションで囲み、"DNS 名:/ [ディレクトリ]" の形式で指定します。なお、"DNS 名:/ [ディレクトリ]" は、1~256 文字の文字列で指定してください。ファイルシステムの DNS 名は、Amazon EFS コンソールから確認できます。 |
| fs_mount_opt | AWS 環境で EFS を使用する場合、amazon-efs-utils ツールを使用してマウントするときは、"-t efs" を指定します。amazon-efs-utils ツールを使用しないでマウントするときは、EFS のドキュメントを参照し、推奨されるマウントオプションを確認してください。                                  |

## 7.4 環境設定例

---

ここでは、パブリッククラウド環境での環境設定例について説明します。

### 7.4.1 【AWS】 HA モニタを使用する場合の構成

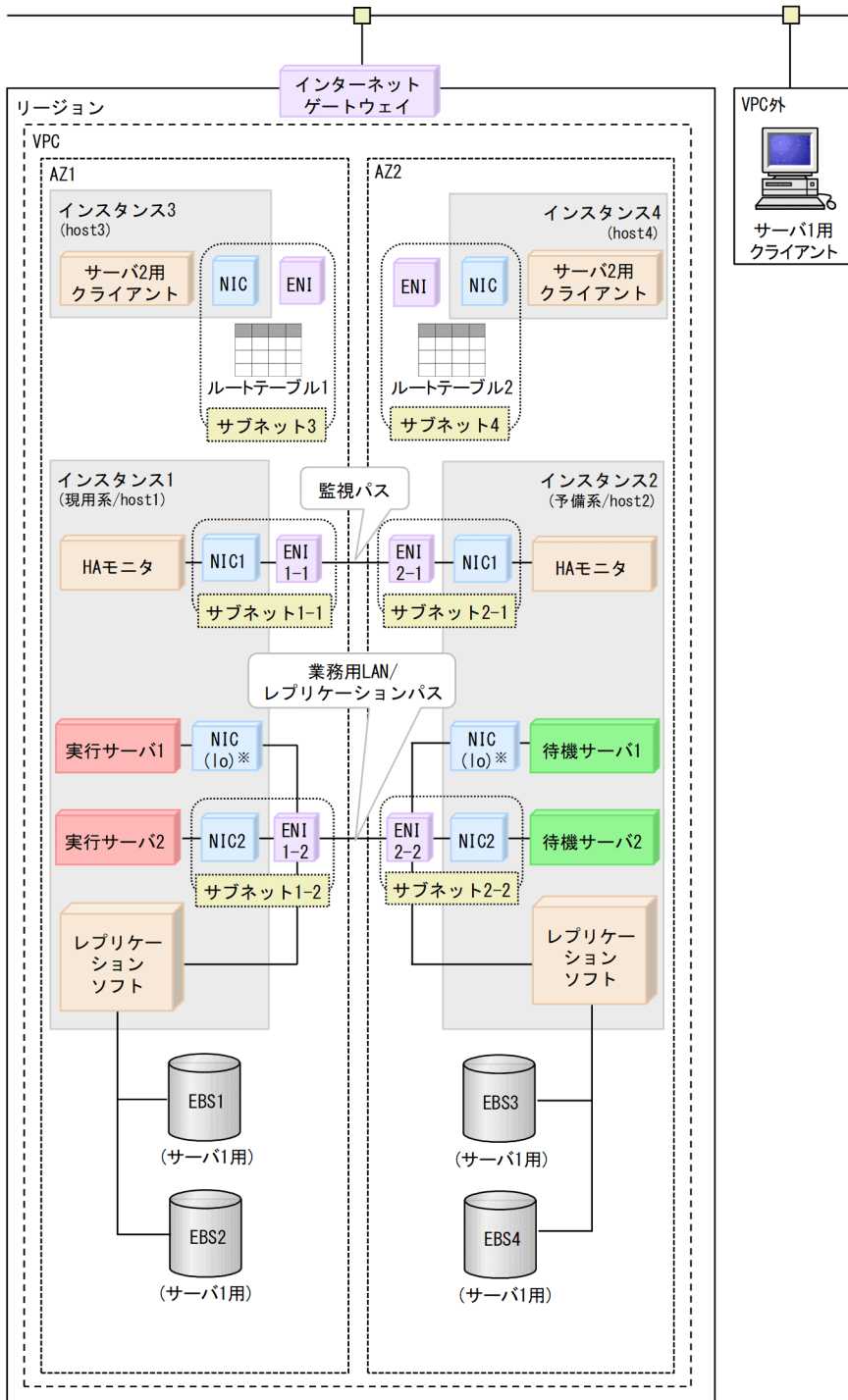
AWS を使用する場合の、次の環境設定例について説明します。

- 系のリセットによる系切り替えをする場合の設定例（レプリケーション構成）
- ネットワーク遮断による系切り替えをする場合の設定例（レプリケーション構成）
- 共有ディスク構成の場合の設定例

#### (1) 系のリセットによる系切り替えをする場合の設定例（レプリケーション構成）

AWS を使用して系のリセットによる系切り替えをする場合の、環境設定例で示すシステム構成例を、次の図に示します。

図 7-1 AWS を使用して系のリセットによる系切り替えをする場合の構成



注※

lo とは、ローカルループバックのことです。

このシステム構成のサブネットの情報を次の表に示します。

表 7-3 サブネットの情報

| サブネット名    | サブネットアドレス    | 内容                            |
|-----------|--------------|-------------------------------|
| サブネット 1-1 | 10.0.11.0/24 | 現用系のサーバ 1 用のサブネット             |
| サブネット 1-2 | 10.0.12.0/24 | 現用系の HA モニタ監視パス/サーバ 2 用のサブネット |
| サブネット 1-3 | 10.0.13.0/24 | 現用系のレプリケーションソフト用のサブネット        |
| サブネット 2-1 | 10.0.21.0/24 | 予備系のサーバ 1 用のサブネット             |
| サブネット 2-2 | 10.0.22.0/24 | 予備系の HA モニタ監視パス/サーバ 2 用のサブネット |
| サブネット 2-3 | 10.0.23.0/24 | 予備系のレプリケーションソフト用のサブネット        |
| サブネット 3   | 10.0.30.0/24 | クライアント（サーバ 2 用）が動作するサブネット     |
| サブネット 4   | 10.0.40.0/24 | クライアント（サーバ 2 用）が動作するサブネット     |

このシステム構成のルートテーブルの情報を次の表に示します。

表 7-4 ルートテーブルの情報

| ルートテーブル   | ルートテーブル ID  | 内容   |
|-----------|-------------|--|
| ルートテーブル 1 | rtb-xxxxxxx | host3 からサーバ 2 向けの VIP の経路情報が登録されているルートテーブル |
| ルートテーブル 2 | rtb-yyyyyyy | host4 からサーバ 2 向けの VIP の経路情報が登録されているルートテーブル |

このシステム構成の ENI の情報を次の表に示します。

表 7-5 ENI の情報

| ENI    | ENI-ID      | 内容                  |
|--------|-------------|---------------------|
| ENI1-1 | eni-1a11111 | サブネット 1-1 で使用する ENI |
| ENI1-2 | eni-2a22222 | サブネット 1-2 で使用する ENI |
| ENI1-3 | eni-3a33333 | サブネット 1-3 で使用する ENI |
| ENI2-1 | eni-1b11111 | サブネット 2-1 で使用する ENI |
| ENI2-2 | eni-2b22222 | サブネット 2-2 で使用する ENI |
| ENI2-3 | eni-3b33333 | サブネット 2-3 で使用する ENI |

このシステム構成のサーバ用の仮想 IP アドレスを次の表に示します。

表 7-6 サーバ用の仮想 IP アドレス

| 仮想 IP アドレス | 種別  | 割り当てる NIC | 割り当てる ENI        | 説明                  |
|------------|-----|-----------|------------------|---------------------|
| 10.0.11.1  | EIP | NIC1      | ENI1-1 / ENI 2-1 | サーバ 1 用の仮想 IP アドレス。 |

| 仮想 IP アドレス  | 種別  | 割り当てる NIC | 割り当てる ENI | 説明  |
|-------------|-----|-----------|-----------|---|
|             |     |           |           | host1 が実行系の場合は、ENI1-1 に仮想 IP アドレスを割り当てます。<br>host2 が実行系の場合は、ENI2-1 に仮想 IP アドレスを割り当てます。  |
| 10.2.12.101 | VIP | lo        | -         | サーバ 2 用の仮想 IP アドレス<br>AWS の仕様によって、VIP には次の特徴があります。 <ul style="list-style-type: none"> <li>• VIP は VPC の CIDR の範囲外</li> <li>• VIP の CIDR ブロックは 32</li> </ul> |

このシステム構成の HA モニタの情報を次の表に示します。

表 7-7 HA モニタの情報

| 系   | 項目            | 設定値         |
|-----|---------------|-------------|
| 現用系 | ホスト名          | host1       |
|     | ホストアドレス       | 101         |
|     | 監視パスのホスト名     | path11      |
|     | 監視パスの IP アドレス | 10.0.12.101 |
|     | 監視パスのサービス名    | HAmon1      |
|     | 系障害監視時間       | 60          |
| 予備系 | ホスト名          | host2       |
|     | ホストアドレス       | 102         |
|     | 監視パスのホスト名     | path21      |
|     | 監視パスの IP アドレス | 10.0.22.101 |
|     | 監視パスのサービス名    | HAmon1      |
|     | 系障害監視時間       | 60          |

このシステム構成のサーバ 1 の情報を次の表に示します。

表 7-8 サーバ 1 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成のサーバ2の情報を次の表に示します。

表 7-9 サーバ2の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成のEBSの情報を次の表に示します。

表 7-10 EBSの情報

| リソース          | レプリケーション用IPアドレス | レプリケーション用ポート番号 | 属性    | EBS  | 項目             | 値             |
|---------------|-----------------|----------------|-------|------|----------------|---------------|
| r1<br>(サーバ1用) | 10.0.13.101     | 7789           | プライマリ | EBS1 | 物理ボリューム名       | /dev/drbd1    |
|               |                 |                |       |      | パーティション名       | /dev/nvme0n1  |
|               |                 |                |       |      | ボリュームグループ名     | Repvol01      |
|               |                 |                |       |      | ボリュームグループの絶対パス | /dev/Repvol01 |



| リソース            | レプリケーション用 IP アドレス | レプリケーション用ポート番号 | 属性    | EBS  | 項目             | 値                    |
|-----------------|-------------------|----------------|-------|------|----------------|----------------------|
|                 | 10.0.23.101       | 7789           | セカンダリ | EBS3 | 論理ボリュームの絶対パス   | /dev/Repvol01/lvol00 |
|                 |                   |                |       |      | マウントディレクトリ名    | /mnt/data1           |
|                 |                   |                |       |      | 物理ボリューム名       | /dev/drbd1           |
|                 |                   |                |       |      | パーティション名       | /dev/nvme0n1         |
|                 |                   |                |       |      | ボリュームグループ名     | Repvol01             |
|                 |                   |                |       |      | ボリュームグループの絶対パス | /dev/Repvol01        |
|                 |                   |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol01/lvol00 |
| r2<br>(サーバ 2 用) | 10.0.13.101       | 7790           | プライマリ | EBS2 | 物理ボリューム名       | /dev/drbd2           |
|                 |                   |                |       |      | パーティション名       | /dev/nvme1n1         |
|                 |                   |                |       |      | ボリュームグループ名     | Repvol02             |
|                 |                   |                |       |      | ボリュームグループの絶対パス | /dev/Repvol02        |
|                 |                   |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol02/lvol00 |
|                 |                   |                |       |      | マウントディレクトリ名    | /mnt/data2           |
|                 | 10.0.23.101       | 7790           | セカンダリ | EBS4 | 物理ボリューム名       | /dev/drbd2           |
|                 |                   |                |       |      | パーティション名       | /dev/nvme1n1         |
|                 |                   |                |       |      | ボリュームグループ名     | Repvol02             |
|                 |                   |                |       |      | ボリュームグループの絶対パス | /dev/Repvol02        |
|                 |                   |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol02/lvol00 |
|                 |                   |                |       |      | マウントディレクトリ名    | /mnt/data2           |

このシステム構成での環境設定例を、次に示します。

現用系の HA モニタの環境設定（定義ファイル：/opt/hitachi/HAMon/etc/sysdef）

予備系では、name オペランド、address オペランド、およびlan オペランドに、予備系側の値を設定してください。

```

/* HAモニタの環境設定 */
environment name      host1,
              address  101,
              patrol   60,
              lan      path11,
              lanport  HAmo1;
function      cpudown  standby,
              public_cloud use;

```

現用系のサーバ対応の環境設定（定義ファイル：/opt/hitachi/HAmo/etc/servers）

予備系では、initial オペランドにstandbyを設定してください。

```

/* サーバ対応の環境設定 */
server name      /users/server1,
              alias  server1,
              acttype server,
              patrol 60,
              initial online,
              disk   /dev/Repv01,
              fs_name /dev/Repv01/lvol00,
              fs_mount_dir /mnt/data1,
              rep_device r1;

server name      /users/server2,
              alias  server2,
              acttype server,
              patrol 60,
              initial online,
              disk   /dev/Repv02,
              fs_name /dev/Repv02/lvol00,
              fs_mount_dir /mnt/data2,
              rep_device r2;

```

現用系の server1.up ファイルの設定

予備系では、EIP\_ENI に ENI2-1 の ENI ID を設定してください。

```

#!/bin/bash
set -x
:
#####
EIP_ADDRESS[0]=10.0.11.1
EIP_ENI[0]=eni-1a11111
EIP_LABEL[0]=NIC1:0

（以降省略）

```

現用系の server2.up ファイルの設定

予備系では、VIP\_ENI に ENI2-2 の ENI ID を設定してください。

```

#!/bin/bash
set -x
:
#####
VIP_ADDRESS[0]=10.2.12.101
VIP_RTb[0]="rtb-xxxxxxx rtb-yyyyyyy"

```

```
VIP_ENI[0]=eni-2a22222  
VIP_LABEL[0]=lo:0
```

(以降省略)

#### 現用系の server1.down ファイルの設定

予備系では、EIP\_ENI には、ENI2-1 の ENI ID を設定してください。

```
#!/bin/bash  
set -x  
:  
#####  
EIP_ADDRESS[0]=10.0.11.1  
EIP_ENI[0]=eni-1a11111  
EIP_LABEL[0]=NIC1:0
```

(以降省略)

#### 現用系の server2.down ファイルの設定

予備系では、VIP\_ENI に ENI2-2 の ENI ID を設定してください。

```
#!/bin/bash  
set -x  
:  
#####  
VIP_ADDRESS[0]=10.2.12.101  
VIP_RTb[0]="rtb-xxxxxxx rtb-yyyyyyy"  
VIP_ENI[0]=eni-2a22222  
VIP_LABEL[0]=lo:0
```

(以降省略)

#### 現用系のレプリケーションソフト (DRBD) の設定

- /etc/drbd.d/global\_common.conf

現用系でも予備系でも同じ設定内容です。

```
global {  
    usage-count no;  
}  
common {  
    handlers {  
        fence-peer "/opt/hitachi/HAMon/bin/parts/monfence-peer.sh";  
    }  
    options {  
        auto-promote yes;  
    }  
    net {  
        protocol C;  
        fencing resource-and-stonith;  
    }  
    startup {  
        wfc-timeout 30;  
    }  
}
```

```
}  
}
```

- /etc/drbd.d/r1.res

現用系でも予備系でも同じ設定内容です。

環境によって OS 起動ごとにデバイス名が変わる場合があるため、常に同じディスクを示すように /dev/disk/by-id/ 下のシンボリックリンクファイル（実デバイス /dev/nvme0n1 などへのシンボリックリンクファイル）を指定することをお勧めします。

```
resource r1 {  
    volume 0 {  
        device    /dev/drbd1;  
        disk      /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_vol079fef9e1c70a8790  
    };  
    meta-disk internal;  
}  
on host1 {  
    address 10.0.13.101:7789;  
}  
on host2 {  
    address 10.0.23.101:7789;  
}  
}
```

- /etc/drbd.d/r2.res

現用系でも予備系でも同じ設定内容です。

環境によって、OS 起動ごとにデバイス名が変わる場合があるため、常に同じディスクを示すように /dev/disk/by-id/ 下のシンボリックリンクファイル（実デバイス /dev/nvme1n1 などへのシンボリックリンクファイル）を指定することをお勧めします。

```
resource r2 {  
    volume 1 {  
        device    /dev/drbd2;  
        disk      /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_vol02c8a3ab941d231f1  
    };  
    meta-disk internal;  
}  
on host1 {  
    address 10.0.13.101:7790;  
}  
on host2 {  
    address 10.0.23.101:7790;  
}  
}
```

connection ファイルの設定（定義ファイル：/opt/hitachi/HAMon/etc/connection）

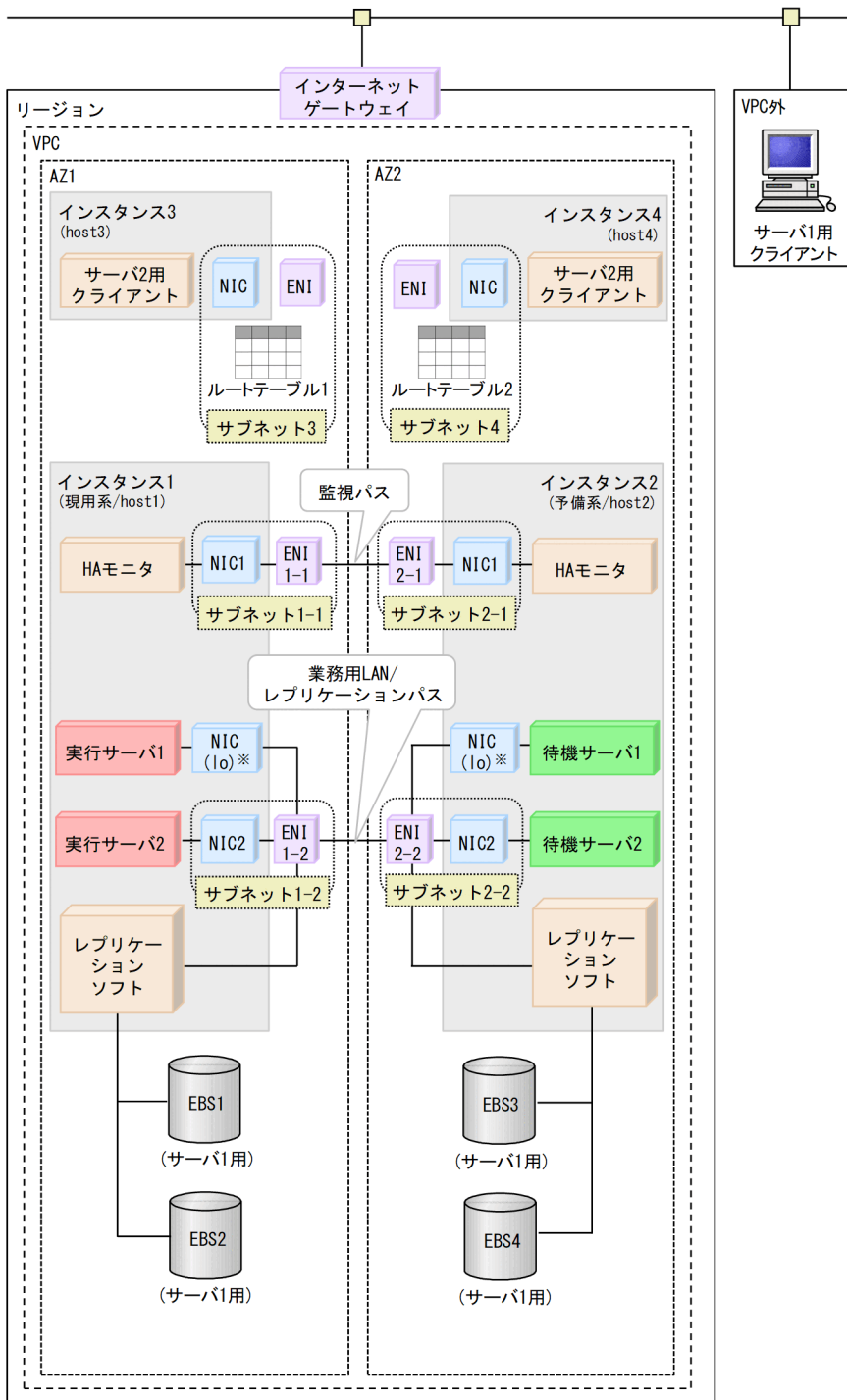
現用系でも予備系でも同じ設定内容です。

```
host1 LAN 10.0.12.101;  
host2 LAN 10.0.22.101;
```

## (2) ネットワーク遮断による系切り替えをする場合の設定例（レプリケーション構成）

AWS を使用してネットワーク遮断による系切り替えをする場合の、環境設定例で示すシステム構成例を、次の図に示します。

図 7-2 AWS を使用してネットワーク遮断による系切り替えをする場合の構成



注※

lo とは、ローカルループバックのことです。

このシステム構成のサブネットの情報を次の表に示します。

表 7-11 サブネットの情報

| サブネット名    | サブネットアドレス    | 内容                                 |
|-----------|--------------|------------------------------------|
| サブネット 1-1 | 10.0.11.0/24 | 現用系の HA モニタ監視パス用のサブネット             |
| サブネット 1-2 | 10.0.12.0/24 | 現用系のサーバ 1/サーバ 2/レプリケーションソフト用のサブネット |
| サブネット 2-1 | 10.0.21.0/24 | 予備系の HA モニタ監視パス用のサブネット             |
| サブネット 2-2 | 10.0.22.0/24 | 予備系のサーバ 1/サーバ 2/レプリケーションソフト用のサブネット |
| サブネット 3   | 10.0.30.0/24 | クライアント（サーバ 2 用）が動作するサブネット          |
| サブネット 4   | 10.0.40.0/24 | クライアント（サーバ 2 用）が動作するサブネット          |

このシステム構成のルートテーブルの情報を次の表に示します。

表 7-12 ルートテーブルの情報

| ルートテーブル   | ルートテーブル ID  | 内容   |
|-----------|-------------|--|
| ルートテーブル 1 | rtb-xxxxxxx | host3 からサーバ 2 向けの VIP の経路情報が登録されているルートテーブル |
| ルートテーブル 2 | rtb-yyyyyyy | host4 からサーバ 2 向けの VIP の経路情報が登録されているルートテーブル |

このシステム構成の ENI の情報を次の表に示します。

表 7-13 ENI の情報

| ENI    | ENI-ID      | 内容                  |
|--------|-------------|---------------------|
| ENI1-1 | eni-1a11111 | サブネット 1-1 で使用する ENI |
| ENI1-2 | eni-2a22222 | サブネット 1-2 で使用する ENI |
| ENI2-1 | eni-1b11111 | サブネット 2-1 で使用する ENI |
| ENI2-2 | eni-2b22222 | サブネット 2-2 で使用する ENI |

このシステム構成のサーバ用の仮想 IP アドレスを次の表に示します。

表 7-14 サーバ用の仮想 IP アドレス

| 仮想 IP アドレス  | 種別  | 割り当てる NIC | 割り当てる ENI        | 説明  |
|-------------|-----|-----------|------------------|---|
| 10.0.12.1   | EIP | NIC2      | ENI1-2 / ENI 2-2 | サーバ 1 用の仮想 IP アドレス。<br>host1 が実行系の場合は、ENI1-2 に仮想 IP アドレスを割り当てます。<br>host2 が実行系の場合は、ENI2-2 に仮想 IP アドレスを割り当てます。 |
| 10.2.12.101 | VIP | lo        | -                | サーバ 2 用の仮想 IP アドレス  |

| 仮想 IP アドレス | 種別 | 割り当てる NIC | 割り当てる ENI | 説明  |
|------------|----|-----------|-----------|---|
|            |    |           |           | AWS の仕様によって、VIP には次の特徴があります。 <ul style="list-style-type: none"> <li>• VIP は VPC の CIDR の範囲外</li> <li>• VIP の CIDR ブロックは 32</li> </ul> |

このシステム構成の HA モニタの情報を次の表に示します。

表 7-15 HA モニタの情報

| 系   | 項目            | 設定値         |
|-----|---------------|-------------|
| 現用系 | ホスト名          | host1       |
|     | ホストアドレス       | 101         |
|     | 監視パスのホスト名     | path11      |
|     | 監視パスの IP アドレス | 10.0.11.101 |
|     | 監視パスのサービス名    | HAmon1      |
|     | 系障害監視時間       | 60          |
| 予備系 | ホスト名          | host2       |
|     | ホストアドレス       | 102         |
|     | 監視パスのホスト名     | path21      |
|     | 監視パスの IP アドレス | 10.0.21.101 |
|     | 監視パスのサービス名    | HAmon1      |
|     | 系障害監視時間       | 60          |

このシステム構成のサーバ 1 の情報を次の表に示します。

表 7-16 サーバ 1 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |

| 系 | 項目   | 設定値     |
|---|------|---------|
|   | 起動方法 | server  |
|   | 起動種別 | standby |

このシステム構成のサーバ2の情報を次の表に示します。

表 7-17 サーバ2の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成のEBSの情報を次の表に示します。

表 7-18 EBSの情報

| リソース          | レプリケーション用IPアドレス | レプリケーション用ポート番号 | 属性    | EBS  | 項目             | 値                    |
|---------------|-----------------|----------------|-------|------|----------------|----------------------|
| r1<br>(サーバ1用) | 10.0.12.101     | 7789           | プライマリ | EBS1 | 物理ボリューム名       | /dev/drbd1           |
|               |                 |                |       |      | パーティション名       | /dev/nvme0n1         |
|               |                 |                |       |      | ボリュームグループ名     | Repvol01             |
|               |                 |                |       |      | ボリュームグループの絶対パス | /dev/Repvol01        |
|               |                 |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol01/lvol00 |
|               |                 |                |       |      | マウントディレクトリ名    | /mnt/data1           |
|               | 10.0.22.101     | 7789           | セカンダリ | EBS3 | 物理ボリューム名       | /dev/drbd1           |
|               |                 |                |       |      | パーティション名       | /dev/nvme0n1         |



| リソース          | レプリケーション用 IP アドレス | レプリケーション用ポート番号 | 属性    | EBS  | 項目             | 値                    |
|---------------|-------------------|----------------|-------|------|----------------|----------------------|
|               |                   |                |       |      | ボリュームグループ名     | Repvol01             |
|               |                   |                |       |      | ボリュームグループの絶対パス | /dev/Repvol01        |
|               |                   |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol01/lvol00 |
|               |                   |                |       |      | マウントディレクトリ名    | /mnt/data1           |
| r2<br>(サーバ2用) | 10.0.12.101       | 7790           | プライマリ | EBS2 | 物理ボリューム名       | /dev/drbd2           |
|               |                   |                |       |      | パーティション名       | /dev/nvme1n1         |
|               |                   |                |       |      | ボリュームグループ名     | Repvol02             |
|               |                   |                |       |      | ボリュームグループの絶対パス | /dev/Repvol02        |
|               |                   |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol02/lvol00 |
|               |                   |                |       |      | マウントディレクトリ名    | /mnt/data2           |
|               | 10.0.22.101       | 7790           | セカンダリ | EBS4 | 物理ボリューム名       | /dev/drbd2           |
|               |                   |                |       |      | パーティション名       | /dev/nvme1n1         |
|               |                   |                |       |      | ボリュームグループ名     | Repvol02             |
|               |                   |                |       |      | ボリュームグループの絶対パス | /dev/Repvol02        |
|               |                   |                |       |      | 論理ボリュームの絶対パス   | /dev/Repvol02/lvol00 |
|               |                   |                |       |      | マウントディレクトリ名    | /mnt/data2           |

このシステム構成での環境設定例を、次に示します。

現用系の HA モニタの環境設定（定義ファイル：/opt/hitachi/HAMon/etc/sysdef）

予備系では、name オペランド、address オペランド、およびlan オペランドに、予備系側の値を設定してください。

```

/* HAモニタの環境設定 */
environment name      host1,
              address   101,
              patrol    60,
              lan       path11,
              lanport   HAMon1;
function      cpudown  standby,

```

```
public_cloud    use,
fence_network   use;
```

現用系のサーバ対応の環境設定（定義ファイル：/opt/hitachi/HAmn/etc/servers）

予備系では、initial オペランドにstandby を設定してください。

```
/* サーバ対応の環境設定 */
server name      /users/server1,
  alias          server1,
  acttype        server,
  patrol         60,
  initial        online,
  disk           /dev/Repvol01,
  fs_name        /dev/Repvol01/lvol00,
  fs_mount_dir   /mnt/data1,
  rep_device     r1;

server name      /users/server2,
  alias          server2,
  acttype        server,
  patrol         60,
  initial        online,
  disk           /dev/Repvol02,
  fs_name        /dev/Repvol02/lvol00,
  fs_mount_dir   /mnt/data2,
  rep_device     r2;
```

現用系のネットワーク遮断設定ファイルの設定（定義ファイル：/opt/hitachi/HAmn/etc/fence\_network.env）

予備系では、ENI2-2 の ENI ID を設定してください。

```
eni-2a22222
```

現用系の server1.up ファイルの設定

予備系では、EIP\_ENI に ENI2-2 の ENI ID を設定してください。

```
#!/bin/bash
set -x
:
#####
EIP_ADDRESS[0]=10.0.12.1
EIP_ENI[0]=eni-2a22222
EIP_LABEL[0]=NIC2:0

（以降省略）
```

現用系の server2.up ファイルの設定

予備系では、VIP\_ENI に ENI2-2 の ENI ID を設定してください。

```
#!/bin/bash
set -x
:
#####
VIP_ADDRESS[0]=10.2.12.101
```

```
VIP_RTB[0]="rtb-xxxxxxx rtb-yyyyyyy"  
VIP_ENI[0]=eni-2a22222  
VIP_LABEL[0]=lo:0
```

(以降省略)

#### 現用系の server1.down ファイルの設定

予備系では、EIP\_ENI には、ENI2-2 の ENI ID を設定してください。

```
#!/bin/bash  
set -x  
:  
#####  
EIP_ADDRESS[0]=10.0.12.1  
EIP_ENI[0]=eni-2a22222  
EIP_LABEL[0]=NIC2:0
```

(以降省略)

#### 現用系の server2.down ファイルの設定

予備系では、VIP\_ENI に ENI2-2 の ENI ID を設定してください。

```
#!/bin/bash  
set -x  
:  
#####  
VIP_ADDRESS[0]=10.2.12.101  
VIP_RTB[0]="rtb-xxxxxxx rtb-yyyyyyy"  
VIP_ENI[0]=eni-2a22222  
VIP_LABEL[0]=lo:0
```

(以降省略)

#### 現用系のレプリケーションソフト (DRBD) の設定

- /etc/drbd.d/global\_common.conf

現用系でも予備系でも同じ設定内容です。

```
global {  
    usage-count no;  
}  
common {  
    handlers {  
        fence-peer "/opt/hitachi/HAMon/bin/parts/monfence-peer.sh";  
    }  
    options {  
        auto-promote yes;  
    }  
    net {  
        protocol C;  
        fencing resource-and-stonith;  
    }  
    startup {  
        wfc-timeout 30;  
    }  
}
```

```
}  
}
```

- /etc/drbd.d/r1.res

現用系でも予備系でも同じ設定内容です。

環境によって OS 起動ごとにデバイス名が変わる場合があるため、常に同じディスクを示すように /dev/disk/by-id/ 下のシンボリックリンクファイル（実デバイス /dev/nvme0n1 などへのシンボリックリンクファイル）を指定することをお勧めします。

```
resource r1 {  
    volume 0 {  
        device    /dev/drbd1;  
        disk      /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_vol079fef9e1c70a8790  
    ;  
        meta-disk internal;  
    }  
    on host1 {  
        address    10.0.12.101:7789;  
    }  
    on host2 {  
        address    10.0.22.101:7789;  
    }  
}
```

- /etc/drbd.d/r2.res

現用系でも予備系でも同じ設定内容です。

環境によって、OS 起動ごとにデバイス名が変わる場合があるため、常に同じディスクを示すように /dev/disk/by-id/ 下のシンボリックリンクファイル（実デバイス /dev/nvme1n1 などへのシンボリックリンクファイル）を指定することをお勧めします。

```
resource r2 {  
    volume 1 {  
        device    /dev/drbd2;  
        disk      /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_vol02c8a3ab941d231f1  
    ;  
        meta-disk internal;  
    }  
    on host1 {  
        address    10.0.12.101:7790;  
    }  
    on host2 {  
        address    10.0.22.101:7790;  
    }  
}
```

connection ファイルの設定（定義ファイル：/opt/hitachi/HAMon/etc/connection）

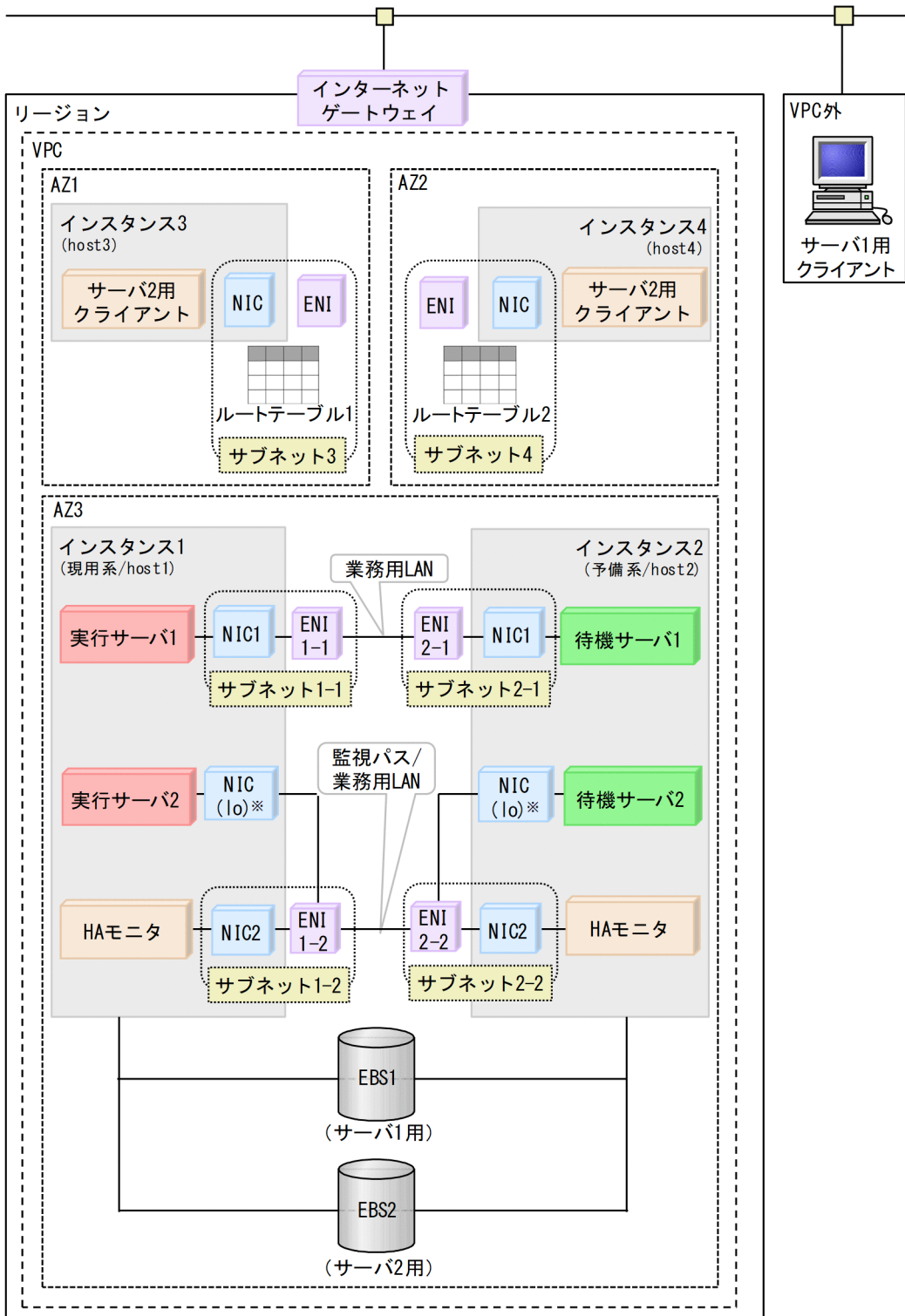
現用系でも予備系でも同じ設定内容です。

```
host1    LAN    10.0.11.101;  
host2    LAN    10.0.12.101;
```

### (3) 共有ディスク構成の場合の設定例

AWS を使用して共有ディスク構成にする場合の、環境設定例で示すシステム構成例を、次の図に示します。

図 7-3 AWS を使用して共有ディスク構成にする場合の構成



注※

lo とは、ローカルループバックのことです。

このシステム構成のサブネットの情報を次の表に示します。

表 7-19 サブネットの情報

| サブネット名    | サブネットアドレス    | 内容                            |
|-----------|--------------|-------------------------------|
| サブネット 1-1 | 10.0.11.0/24 | 現用系のサーバ 1 用のサブネット             |
| サブネット 1-2 | 10.0.12.0/24 | 現用系の HA モニタ監視パス/サーバ 2 用のサブネット |
| サブネット 2-1 | 10.0.21.0/24 | 予備系のサーバ 1 用のサブネット             |
| サブネット 2-2 | 10.0.22.0/24 | 予備系の HA モニタ監視パス/サーバ 2 用のサブネット |
| サブネット 3   | 10.0.30.0/24 | クライアント (サーバ 2 用) が動作するサブネット   |
| サブネット 4   | 10.0.40.0/24 | クライアント (サーバ 2 用) が動作するサブネット   |

このシステム構成のルートテーブルの情報を次の表に示します。

表 7-20 ルートテーブルの情報

| ルートテーブル   | ルートテーブル ID  | 内容   |
|-----------|-------------|--|
| ルートテーブル 1 | rtb-xxxxxxx | host3 からサーバ 2 向けの VIP の経路情報が登録されているルートテーブル |
| ルートテーブル 2 | rtb-yyyyyyy | host4 からサーバ 2 向けの VIP の経路情報が登録されているルートテーブル |

このシステム構成の ENI の情報を次の表に示します。

表 7-21 ENI の情報

| ENI    | ENI-ID      | 内容                  |
|--------|-------------|---------------------|
| ENI1-1 | eni-1a11111 | サブネット 1-1 で使用する ENI |
| ENI1-2 | eni-2a22222 | サブネット 1-2 で使用する ENI |
| ENI2-1 | eni-1b11111 | サブネット 2-1 で使用する ENI |
| ENI2-2 | eni-2b22222 | サブネット 2-2 で使用する ENI |

このシステム構成のサーバ用の仮想 IP アドレスを次の表に示します。

表 7-22 サーバ用の仮想 IP アドレス

| 仮想 IP アドレス  | 種別  | 割り当てる NIC | 割り当てる ENI        | 説明  |
|-------------|-----|-----------|------------------|---|
| 10.0.11.1   | EIP | NIC1      | ENI1-1 / ENI 2-1 | サーバ 1 用の仮想 IP アドレス。<br>host1 が実行系の場合は、ENI1-1 に仮想 IP アドレスを割り当てます。<br>host2 が実行系の場合は、ENI2-1 に仮想 IP アドレスを割り当てます。 |
| 10.2.12.101 | VIP | lo        | -                | サーバ 2 用の仮想 IP アドレス  |

| 仮想 IP アドレス | 種別 | 割り当てる NIC | 割り当てる ENI | 説明  |
|------------|----|-----------|-----------|---|
|            |    |           |           | AWS の仕様によって、VIP には次の特徴があります。 <ul style="list-style-type: none"> <li>• VIP は VPC の CIDR の範囲外</li> <li>• VIP の CIDR ブロックは 32</li> </ul> |

このシステム構成の HA モニタの情報を次の表に示します。

表 7-23 HA モニタの情報

| 系   | 項目            | 設定値         |
|-----|---------------|-------------|
| 現用系 | ホスト名          | host1       |
|     | ホストアドレス       | 101         |
|     | 監視パスのホスト名     | path11      |
|     | 監視パスの IP アドレス | 10.0.12.101 |
|     | 監視パスのサービス名    | HAmon1      |
|     | 系障害監視時間       | 60          |
| 予備系 | ホスト名          | host2       |
|     | ホストアドレス       | 102         |
|     | 監視パスのホスト名     | path21      |
|     | 監視パスの IP アドレス | 10.0.22.101 |
|     | 監視パスのサービス名    | HAmon1      |
|     | 系障害監視時間       | 60          |

このシステム構成のサーバ 1 の情報を次の表に示します。

表 7-24 サーバ 1 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |

| 系 | 項目   | 設定値     |
|---|------|---------|
|   | 起動方法 | server  |
|   | 起動種別 | standby |

このシステム構成のサーバ 2 の情報を次の表に示します。

表 7-25 サーバ 2 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成の EBS の情報を次の表に示します。

表 7-26 EBS の情報

| EBS            | 項目             | 設定値            |
|----------------|----------------|----------------|
| EBS1 (サーバ 1 用) | パーティション        | /dev/sdf1      |
|                | 物理ボリューム        | /dev/sdf1      |
|                | ボリュームグループ      | vg01           |
|                | ボリュームグループの絶対パス | /dev/vg01      |
|                | 論理ボリューム        | lv01           |
|                | 論理ボリュームの絶対パス   | /dev/vg01/lv01 |
|                | マウントディレクトリ     | /mnt/data1     |
| EBS2 (サーバ 2 用) | パーティション        | /dev/sdg1      |
|                | 物理ボリューム        | /dev/sdg1      |
|                | ボリュームグループ      | vg02           |
|                | ボリュームグループの絶対パス | /dev/vg02      |



| EBS | 項目           | 設定値              |
|-----|--------------|------------------|
|     | 論理ボリューム      | lv0101           |
|     | 論理ボリュームの絶対パス | /dev/vg02/lv0101 |
|     | マウントディレクトリ   | /mnt/data2       |

このシステム構成での環境設定例を、次に示します。

現用系の HA モニタの環境設定（定義ファイル：/opt/hitachi/HAMon/etc/sysdef）

予備系では、name オペランド、address オペランド、およびlan オペランドに、予備系側の値を設定してください。

```

/* HAモニタの環境設定 */
environment name      host1,
                  address 101,
                  patrol  60,
                  lan     path11,
                  lanport HAMon1;
function   public_cloud use;

```

現用系のサーバ対応の環境設定（定義ファイル：/opt/hitachi/HAMon/etc/servers）

予備系では、initial オペランドにstandbyを設定してください。

```

/* サーバ対応の環境設定 */
server name /users/server1,
          alias  server1,
          acttype server,
          patrol 60,
          initial online,
          disk   /dev/vg01,
          fs_name /dev/vg01/lv0101,
          fs_mount_dir /mnt/data1;

server name /users/server2,
          alias  server2,
          acttype server,
          patrol 60,
          initial online,
          disk   /dev/vg02,
          fs_name /dev/vg02/lv0101,
          fs_mount_dir /mnt/data2;

```

現用系のネットワーク遮断設定ファイルの設定（定義ファイル：/opt/hitachi/HAMon/etc/fence\_network.env）

ネットワーク遮断による系切り替えをする場合にだけ必要です。予備系では、ENI2-1、ENI2-2 の ENI ID を設定してください。

```

eni-1a11111
eni-2a22222

```

現用系の server1.up ファイルの設定

予備系では、EIP\_ENI に ENI2-1 の ENI ID を設定してください。

```
#!/bin/bash
set -x
:
#####
EIP_ADDRESS[0]=10.0.11.1
EIP_ENI[0]=eni-1a11111
EIP_LABEL[0]=NIC1:0

(以降省略)
```

現用系の server2.up ファイルの設定

予備系では、VIP\_ENI に ENI2-2 の ENI ID を設定してください。

```
#!/bin/bash
set -x
:
#####
VIP_ADDRESS[0]=10.2.12.101
VIP_RTb[0]="rtb-xxxxxxx rtb-yyyyyyy"
VIP_ENI[0]=eni-2a22222
VIP_LABEL[0]=lo:0

(以降省略)
```

現用系の server1.down ファイルの設定

予備系では、EIP\_ENI には、ENI2-1 の ENI ID を設定してください。

```
#!/bin/bash
set -x
:
#####
EIP_ADDRESS[0]=10.0.11.1
EIP_ENI[0]=eni-1a11111
EIP_LABEL[0]=NIC1:0

(以降省略)
```

connection ファイルの設定 (定義ファイル: /opt/hitachi/HAMon/etc/connection)

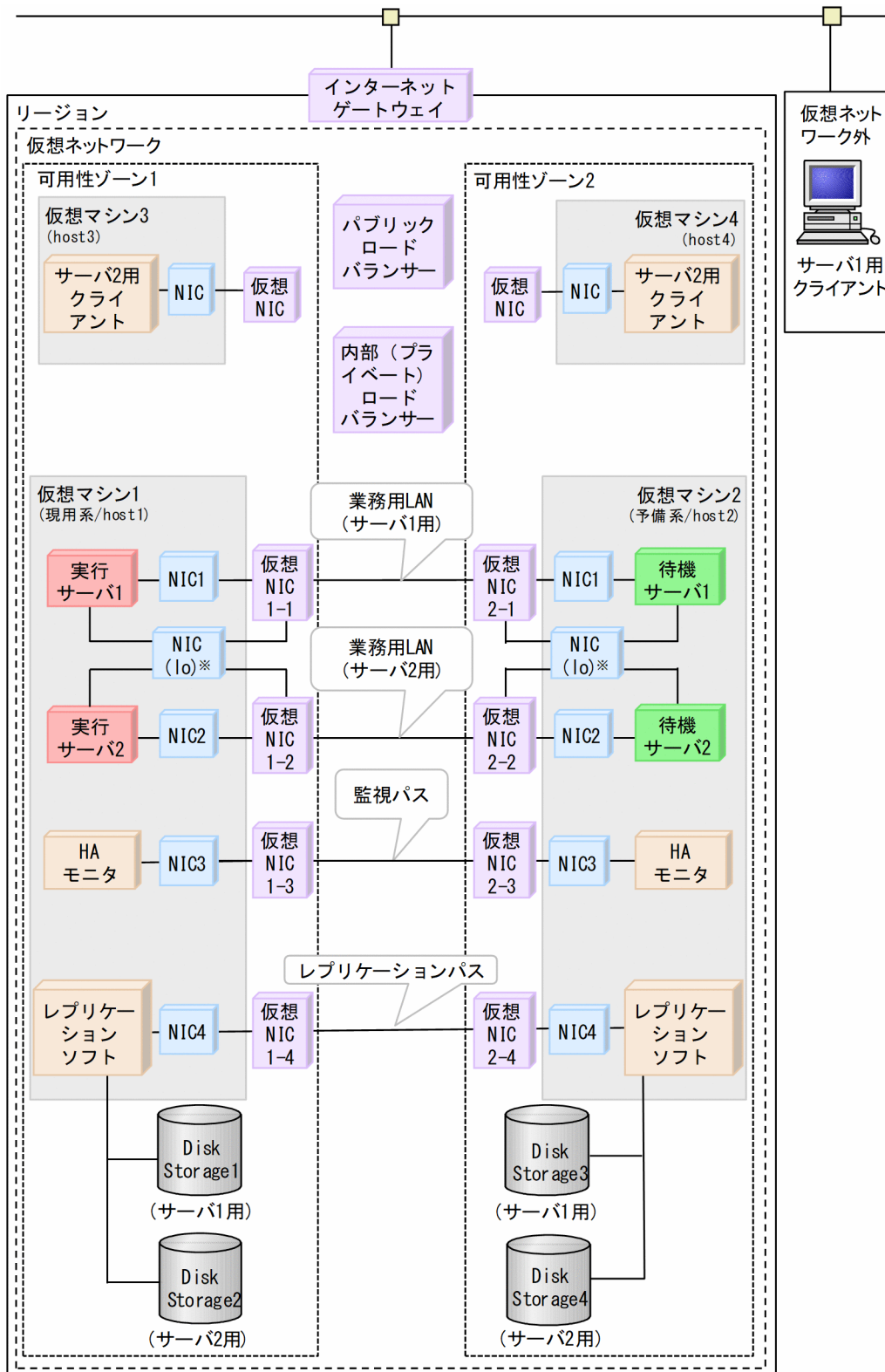
現用系でも予備系でも同じ設定内容です。

```
host1 LAN 10.0.12.101;
host2 LAN 10.0.22.101;
```

## 7.4.2 【Azure】 HA モニタを使用する場合の構成

Azure を使用する場合は、環境設定例で示すシステム構成例を、次の図に示します。

図 7-4 Azure を使用する場合の構成



注※

lo とは、ローカルループバックのことです。

このシステム構成の Azure ロードバランサーの情報を次の表に示します。

表 7-27 Azure ロードバランサーの情報

| Azure ロードバランサー | フロントエンド IP    | バックエンド IP     | 正常性プローブ |       |    |        | 負荷分散規則           |
|----------------|---------------|---------------|---------|-------|----|--------|------------------|
|                |               |               | プロトコル   | ポート番号 | 間隔 | 異常しきい値 | フローティング IP (DSR) |
| パブリック          | 10.2.12.100   | 10.2.12.101   | TCP     | 50000 | 5  | 2      | 有効               |
|                |               | 10.2.12.102   |         |       |    |        |                  |
| 内部 (プライベート)    | 172.16.10.100 | 172.16.10.101 | TCP     | 50001 | 5  | 2      | 有効               |
|                |               | 172.16.10.102 |         |       |    |        |                  |

このシステム構成のサーバ用の仮想 IP アドレスを次の表に示します。

表 7-28 サーバ用の仮想 IP アドレス

| 仮想 IP アドレス    | 種別        | 割り当てる NIC | 説明  |
|---------------|-----------|-----------|---|
| 10.2.12.100   | パブリック IP  | lo        | サーバ 1 用の仮想 IP アドレス。<br>パブリックロードバランサーのフロントエンドの IP アドレスと同じにしてください。        |
| 172.16.10.100 | プライベート IP | lo        | サーバ 2 用の仮想 IP アドレス。<br>内部 (プライベート) ロードバランサーのフロントエンドの IP アドレスと同じにしてください。 |

このシステム構成の仮想 NIC の情報を次の表に示します。

表 7-29 仮想 NIC の情報

| リソース      | 種別            | 割り当てる NIC  |
|-----------|---------------|--|
| 仮想 NIC1-1 | 10.2.12.101   | サーバ 1 用のパブリックロードバランサーの仮想マシン 1 側のバックエンド IP です。        |
| 仮想 NIC1-2 | 172.16.10.101 | サーバ 2 用の内部 (プライベート) ロードバランサーの仮想マシン 1 側のバックエンド IP です。 |
| 仮想 NIC1-3 | 172.16.12.101 | 仮想マシン 1 側の監視パス用です。                                   |
| 仮想 NIC1-4 | 172.16.11.101 | 仮想マシン 1 側のレプリケーション用です。                               |

| リソース      | 種別            | 割り当てる NIC  |
|-----------|---------------|--|
| 仮想 NIC2-1 | 10.2.12.102   | サーバ 1 用のパブリックロードバランサーの仮想マシン 2 側のバックエンド IP です。      |
| 仮想 NIC2-2 | 172.16.10.102 | サーバ 2 用の内部（プライベート）ロードバランサーの仮想マシン 2 側のバックエンド IP です。 |
| 仮想 NIC2-3 | 172.16.12.102 | 仮想マシン 2 側の監視パス用です。                                 |
| 仮想 NIC2-4 | 172.16.11.102 | 仮想マシン 2 側のレプリケーション用です。                             |

このシステム構成のレプリケーションソフトで使用する IP アドレスとポート番号を次の表に示します。

表 7-30 レプリケーションソフトで使用する IP アドレスとポート番号の情報

| リソース        | 系            | IP アドレス       | ポート番号 |
|-------------|--------------|---------------|-------|
| r1（サーバ 1 用） | プライマリ（host1） | 172.16.11.101 | 7789  |
|             | セカンダリ（host2） | 172.16.11.102 | 7789  |
| r2（サーバ 2 用） | プライマリ（host1） | 172.16.11.101 | 7790  |
|             | セカンダリ（host2） | 172.16.11.102 | 7790  |

注

プレフィックスは 24 です。

このシステム構成の HA モニタの情報を次の表に示します。

表 7-31 HA モニタの情報

| 系   | 項目            | 設定値                        |
|-----|---------------|----------------------------|
| 現用系 | ホスト名          | host1                      |
|     | ホストアドレス       | 101                        |
|     | 監視パスのホスト名     | path11                     |
|     | 監視パスの IP アドレス | 172.16.12.101 <sup>※</sup> |
|     | 監視パスのサービス名    | HAmon1                     |
|     | 系障害監視時間       | 60                         |
| 予備系 | ホスト名          | host2                      |
|     | ホストアドレス       | 102                        |
|     | 監視パスのホスト名     | path21                     |
|     | 監視パスの IP アドレス | 172.16.12.102 <sup>※</sup> |

| 系 | 項目         | 設定値   |
|---|------------|-------|
|   | 監視パスのサービス名 | HAmn1 |
|   | 系障害監視時間    | 60    |

注※

プレフィックスは 24 です。

このシステム構成のサーバ 1 の情報を次の表に示します。

表 7-32 サーバ 1 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成のサーバ 2 の情報を次の表に示します。

表 7-33 サーバ 2 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |

| 系 | 項目   | 設定値     |
|---|------|---------|
|   | 起動種別 | standby |

このシステム構成の Disk Storage の情報を次の表に示します。

表 7-34 Disk Storage の情報

| リソース            | 属性    | Disk Storage  | 項目             | 値                    |
|-----------------|-------|---------------|----------------|----------------------|
| r1<br>(サーバ 1 用) | プライマリ | Disk Storage1 | 物理ボリューム名       | /dev/drbd1           |
|                 |       |               | パーティション名       | /dev/sda             |
|                 |       |               | ボリュームグループ名     | Repvol01             |
|                 |       |               | ボリュームグループの絶対パス | /dev/Repvol01        |
|                 |       |               | 論理ボリュームの絶対パス   | /dev/Repvol01/lvol00 |
|                 |       |               | マウントディレクトリ名    | /mnt/data1           |
|                 | セカンダリ | Disk Storage3 | 物理ボリューム名       | /dev/drbd1           |
|                 |       |               | パーティション名       | /dev/sda             |
|                 |       |               | ボリュームグループ名     | Repvol01             |
|                 |       |               | ボリュームグループの絶対パス | /dev/Repvol01        |
|                 |       |               | 論理ボリュームの絶対パス   | /dev/Repvol01/lvol00 |
|                 |       |               | マウントディレクトリ名    | /mnt/data1           |
| r2<br>(サーバ 2 用) | プライマリ | Disk Storage2 | 物理ボリューム名       | /dev/drbd2           |
|                 |       |               | パーティション名       | /dev/sdb             |
|                 |       |               | ボリュームグループ名     | Repvol02             |
|                 |       |               | ボリュームグループの絶対パス | /dev/Repvol02        |
|                 |       |               | 論理ボリュームの絶対パス   | /dev/Repvol02/lvol00 |
|                 |       |               | マウントディレクトリ名    | /mnt/data2           |
|                 | セカンダリ | Disk Storage4 | 物理ボリューム名       | /dev/drbd2           |
|                 |       |               | パーティション名       | /dev/sdb             |
|                 |       |               | ボリュームグループ名     | Repvol02             |
|                 |       |               | ボリュームグループの絶対パス | /dev/Repvol02        |
|                 |       |               | 論理ボリュームの絶対パス   | /dev/Repvol02/lvol00 |
|                 |       |               | マウントディレクトリ名    | /mnt/data2           |

このシステム構成での環境設定例を、次に示します。

可用性ゾーン 1 側の HA モニタの環境設定 (定義ファイル: /opt/hitachi/HAMon/etc/sysdef)

予備系の可用性ゾーン 2 側では, name オペランド, address オペランド, およびlan オペランドに, 可用性ゾーン 2 側の値を設定してください。

```
/* HAモニタの環境設定 */
environment name      host1,
              address  101,
              patrol   60,
              lan       path11,
              lanport   HAMon1;
function      cpudown  standby,
              public_cloud use;
```

可用性ゾーン 1 側のサーバ対応の環境設定 (定義ファイル: /opt/hitachi/HAMon/etc/servers)

予備系の可用性ゾーン 2 側では, initial オペランドにstandbyを設定してください。

```
/* サーバ対応の環境設定 */
server name    /users/server1,
              alias      server1,
              acttype    server,
              patrol     60,
              initial    online,
              disk       /dev/Repvol01,
              fs_name    /dev/Repvol01/lvol00,
              fs_mount_dir /mnt/data1,
              rep_device r1;

server name    /users/server2,
              alias      server2,
              acttype    server,
              patrol     60,
              initial    online,
              disk       /dev/Repvol02,
              fs_name    /dev/Repvol02/lvol00,
              fs_mount_dir /mnt/data2,
              rep_device r2;
```

可用性ゾーン 1 側のserver1.up ファイルの設定

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
#!/bin/bash
set -x
:
#####
LB_IPADDR[0]=10.2.12.100
LB_PORT[0]=50000

(以降省略)
```

可用性ゾーン 1 側のserver2.up ファイルの設定

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
#!/bin/bash
set -x
```



```
      :
#####
LB_IPADDR[0]=172.16.10.100
LB_PORT[0]=50001
```

(以降省略)

#### 可用性ゾーン 1 側のserver1.down ファイルの設定

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
#!/bin/bash
set -x
      :
#####
LB_IPADDR[0]=10.2.12.100
LB_PORT[0]=50000
```

(以降省略)

#### 可用性ゾーン 1 側のserver2.down ファイルの設定

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
#!/bin/bash
set -x
      :
#####
LB_IPADDR[0]=172.16.10.100
LB_PORT[0]=50001
```

(以降省略)

#### 可用性ゾーン 1 側のレプリケーションソフト (DRBD) の設定

- /etc/drbd.d/global\_common.conf

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
global {
    usage-count no;
}
common {
    handlers {
        fence-peer "/opt/hitachi/HAmom/bin/parts/monfence-peer.sh";
    }
    options {
        auto-promote yes;
    }
    net {
        protocol C;
        fencing resource-and-stonith;
    }
    startup {
        wfc-timeout 30;
    }
}
```

- /etc/drbd.d/r1.res

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

環境によって OS 起動ごとにデバイス名が変わる場合があるため、常に同じディスクを示すように/dev/disk/by-id/下のシンボリックリンクファイル（実デバイス/dev/sda などへのシンボリックリンクファイル）を指定することをお勧めします。

```
resource r1 {
  volume 0 {
    device    /dev/drbd1;
    disk /dev/disk/by-id/scsi-3600224809eb108af1253c92ea220a808;
    meta-disk internal;
  }
  on host1 {
    address 172.16.11.101:7789;
  }
  on host2 {
    address 172.16.11.102:7789;
  }
}
```

- /etc/drbd.d/r2.res

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

環境によって、OS 起動ごとにデバイス名が変わる場合があるため、常に同じディスクを示すように/dev/disk/by-id/下のシンボリックリンクファイル（実デバイス/dev/sdb などへのシンボリックリンクファイル）を指定することをお勧めします。

```
resource r2 {
  volume 1 {
    device    /dev/drbd2;
    disk /dev/disk/by-id/scsi-360022480a4bd74aa688769bacd682e04;
    meta-disk internal;
  }
  on host1 {
    address 172.16.11.101:7790;
  }
  on host2 {
    address 172.16.11.102:7790;
  }
}
```

connection ファイルの設定（定義ファイル：/opt/hitachi/HAMon/etc/connection）

現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
host1 LAN 172.16.12.101;
host2 LAN 172.16.12.102;
```

サービスプリンシパル情報設定ファイルの設定（定義ファイル：/opt/hitachi/HAMon/etc/azure\_serviceprincipal.env）

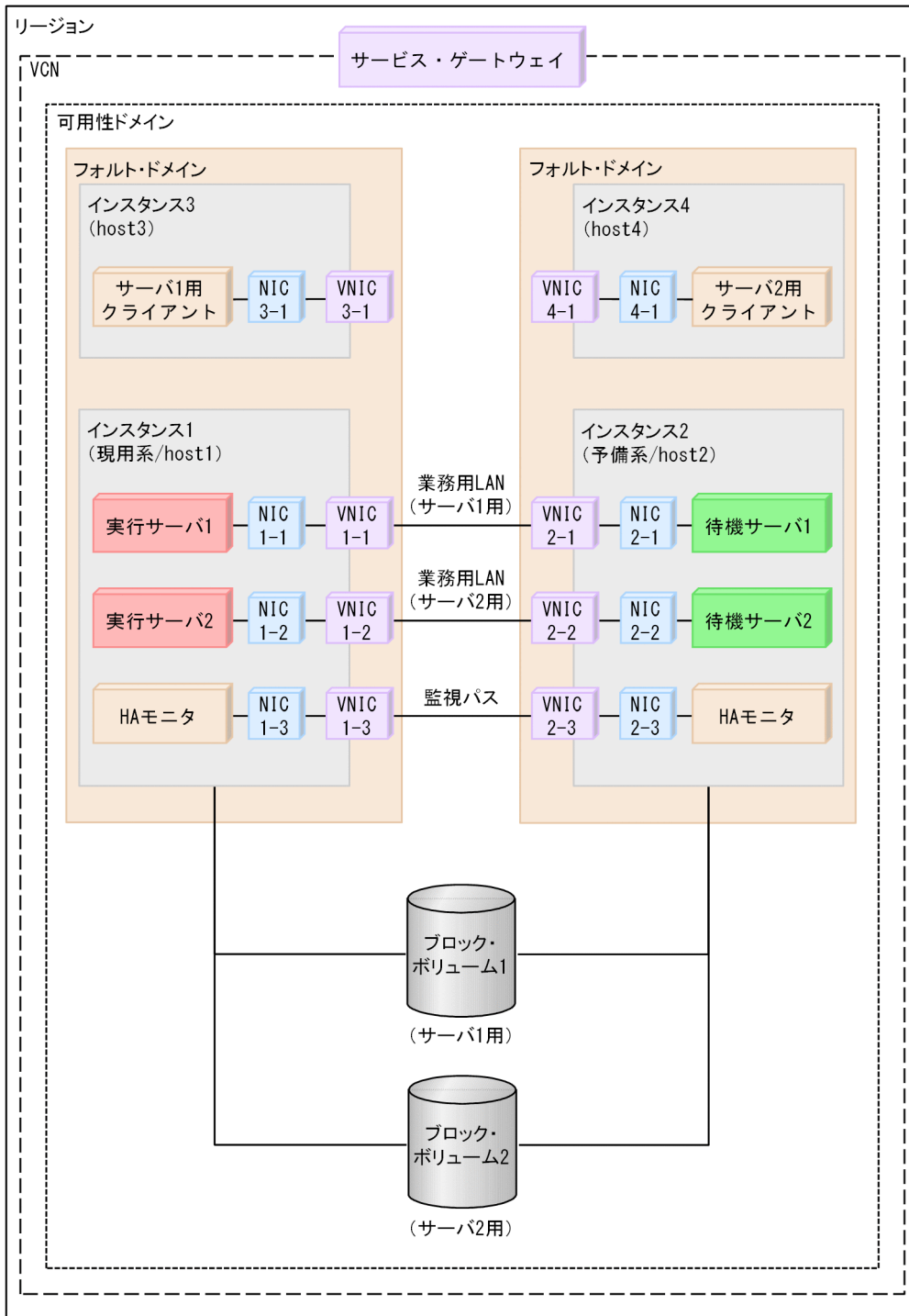
現用系の可用性ゾーン 1 側と予備系の可用性ゾーン 2 側は同じ内容になります。

```
appId=2450046d-a6d5-41b6-9d70-4970af56cc07
fileWithCertAndPrivateKey=/root/tmpnoh4k0r1.pem
tenant=f54277c9-dafe-44aa-85a4-73d5c7c52450
```

### 7.4.3 【OCI】 HA モニタを使用する場合の構成

OCI を使用する場合の、環境設定例で示すシステム構成例を、次の図に示します。

図 7-5 OCI を使用する場合の構成



VCN の CIDR ブロックは 172.16.0.0/16 です。

サブネットの CIDR ブロックは 172.16.12.0/24 です。

このシステム構成の VNIC の情報を次の表に示します。なお、host3 および host4 の VNIC の情報については省略します。

表 7-35 VNIC の情報

| VNIC    | プライベート IP     | OCID                               | 説明               |
|---------|---------------|------------------------------------|------------------|
| VNIC1-1 | 172.16.12.101 | ocid1.instance.oc1.ap-tokyo-1.aaaa | 現用系 サーバ 1 用 VNIC |
| VNIC1-2 | 172.16.12.102 | ocid1.instance.oc1.ap-tokyo-1.bbbb | 現用系 サーバ 2 用 VNIC |
| VNIC1-3 | 172.16.12.103 | ocid1.instance.oc1.ap-tokyo-1.cccc | 現用系 監視パス用 VNIC   |
| VNIC2-1 | 172.16.12.201 | ocid1.instance.oc1.ap-tokyo-1.dddd | 予備系 サーバ 1 用 VNIC |
| VNIC2-2 | 172.16.12.202 | ocid1.instance.oc1.ap-tokyo-1.eeee | 予備系 サーバ 2 用 VNIC |
| VNIC2-3 | 172.16.12.203 | ocid1.instance.oc1.ap-tokyo-1.ffff | 予備系 監視パス用 VNIC   |

このシステム構成の、サーバへの通信に用いる、現用系および予備系を制御するプライベート IP アドレスの情報を次の表に示します。

表 7-36 現用系および予備系を制御するプライベート IP アドレスの情報

| プライベート IP アドレス | 割り当てる NIC     | 割り当てる VNIC      | 説明  |
|----------------|---------------|-----------------|---|
| 172.16.12.10   | NIC1-1/NIC2-1 | VNIC1-1/VNIC2-1 | サーバ 1 への通信に用いるプライベート IP アドレス。<br>host1 が実行系の場合は、NIC1-1 と VNIC1-1 に割り当てられています。<br>host2 が実行系の場合は、NIC2-1 と VNIC2-1 に割り当てられています。 |
| 172.16.12.20   | NIC1-2/NIC2-2 | VNIC1-2/VNIC2-2 | サーバ 2 への通信に用いるプライベート IP アドレス。<br>host1 が実行系の場合は、NIC1-2 と VNIC1-2 に割り当てられています。<br>host2 が実行系の場合は、NIC2-2 と VNIC2-2 に割り当てられています。 |

このシステム構成の HA モニタの情報を次の表に示します。

表 7-37 HA モニタの情報

| 系   | 項目            | 設定値           |
|-----|---------------|---------------|
| 現用系 | ホスト名          | host1         |
|     | ホストアドレス       | 101           |
|     | 監視パスのホスト名     | path11        |
|     | 監視パスの IP アドレス | 172.16.12.103 |
|     | 監視パスのサービス名    | HAmon1        |
|     | 系障害監視時間       | 60            |
| 予備系 | ホスト名          | host2         |
|     | ホストアドレス       | 102           |
|     | 監視パスのホスト名     | path21        |
|     | 監視パスの IP アドレス | 172.16.12.203 |
|     | 監視パスのサービス名    | HAmon1        |
|     | 系障害監視時間       | 60            |

このシステム構成のサーバ 1 の情報を次の表に示します。

表 7-38 サーバ 1 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server1 |
|     | サーバ識別名    | server1        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成のサーバ 2 の情報を次の表に示します。

表 7-39 サーバ 2 の情報

| 系   | 項目        | 設定値            |
|-----|-----------|----------------|
| 現用系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | online         |
| 予備系 | プログラム名    | /users/server2 |
|     | サーバ識別名    | server2        |
|     | サーバ障害監視時間 | 60             |
|     | 起動方法      | server         |
|     | 起動種別      | standby        |

このシステム構成のブロック・ボリュームの情報を次の表に示します。

表 7-40 ブロック・ボリュームの情報

| ブロック・ボリューム             | 項目             | 設定値            |
|------------------------|----------------|----------------|
| ブロック・ボリューム 1 (サーバ 1 用) | パーティション        | /dev/sdf1      |
|                        | 物理ボリューム        | /dev/sdf1      |
|                        | ボリュームグループ      | vg01           |
|                        | ボリュームグループの絶対パス | /dev/vg01      |
|                        | 論理ボリューム        | lv01           |
|                        | 論理ボリュームの絶対パス   | /dev/vg01/lv01 |
|                        | マウントディレクトリ     | /mnt/data1     |
| ブロック・ボリューム 2 (サーバ 2 用) | パーティション        | /dev/sdg1      |
|                        | 物理ボリューム        | /dev/sdg1      |
|                        | ボリュームグループ      | vg02           |
|                        | ボリュームグループの絶対パス | /dev/vg02      |
|                        | 論理ボリューム        | lv01           |
|                        | 論理ボリュームの絶対パス   | /dev/vg02/lv01 |
|                        | マウントディレクトリ     | /mnt/data2     |

このシステム構成での環境設定例を次に示します。

現用系の HA モニタの環境設定（定義ファイル：/opt/hitachi/HAMon/etc/sysdef）

予備系では、name オペランド、address オペランド、およびlan オペランドに、予備系側の値を設定してください。

```
/* HAモニタの環境設定 */
environment name      host1,
              address  101,
              patrol   60,
              lan      path11,
              lanport  HAMon1;
function      cpudown  standby,
              public_cloud use;
```

現用系のサーバ対応の環境設定（定義ファイル：/opt/hitachi/HAMon/etc/servers）

予備系では、initial オペランドにstandbyを設定してください。

```
/* サーバ対応の環境設定 */
server name    /users/server1,
              alias  server1,
              acttype server,
              patrol 60,
              initial online,
              disk   /dev/vg01,
              fs_name /dev/vg01/lvol01,
              fs_mount_dir /mnt/data1;

server name    /users/server2,
              alias  server2,
              acttype server,
              patrol 60,
              initial online,
              disk   /dev/vg02,
              fs_name /dev/vg02/lvol01,
              fs_mount_dir /mnt/data2;
```

現用系のserver1.up ファイルの設定

予備系では、PIP\_VNIC[0]にVNIC2-1のOCID、PIP\_LABEL[0]にNIC2-1のラベルを設定してください。

```
#!/bin/bash
set -x
:(省略)
#####
PIP_ADDRESS[0]=172.16.12.10
PIP_VNIC[0]=ocid1.instance.oc1.ap-tokyo-1.aaaa
PIP_LABEL[0]=NIC1-1:0
:(以降省略)
```

現用系のserver2.up ファイルの設定

予備系では、PIP\_VNIC[0]にVNIC2-2のOCID、PIP\_LABEL[0]にNIC2-2のラベルを設定してください。

```
#!/bin/bash
set -x
  :(省略)
#####
PIP_ADDRESS[0]=172.16.12.20
PIP_VNIC[0]=ocid1.instance.oc1.ap-tokyo-1.bbbb
PIP_LABEL[0]=NIC1-2:0
  :(以降省略)
```

#### 現用系のserver1.down ファイルの設定

予備系では、PIP\_VNIC[0]に VNIC2-1 の OCID、PIP\_LABEL[0]に NIC2-1 のラベルを設定してください。

```
#!/bin/bash
set -x
  :(省略)
#####
PIP_ADDRESS[0]=172.16.12.10
PIP_VNIC[0]=ocid1.instance.oc1.ap-tokyo-1.aaaa
PIP_LABEL[0]=NIC1-1:0
  :(以降省略)
```

#### 現用系のserver2.down ファイルの設定

予備系では、PIP\_VNIC[0]に VNIC2-2 の OCID、PIP\_LABEL[0]に NIC2-2 のラベルを設定してください。

```
#!/bin/bash
set -x
  :(省略)
#####
PIP_ADDRESS[0]=172.16.12.20
PIP_VNIC[0]=ocid1.instance.oc1.ap-tokyo-1.bbbb
PIP_LABEL[0]=NIC1-2:0
  :(以降省略)
```



# 8

## コマンド

この章では、パブリッククラウド環境下の HA モニタで使用するコマンドについて説明します。  
なお、この章はマニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「コマンド」とあわせてお読みください。

## 8.1 パブリッククラウド環境で注意が必要なコマンド

ここでは、パブリッククラウド環境下で HA モニタを使用する場合に、注意が必要なコマンドについてだけ記載します。各コマンドの詳細については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「コマンド」の説明を参照してください。

パブリッククラウド環境で注意が必要なコマンドについて、次の表に示します。

表 8-1 パブリッククラウド環境で注意が必要なコマンド

| コマンド名     | 注意事項   |
|-----------|--|
| moncheck  | パブリッククラウドでない環境でチェックする定義に加え、次の定義もチェックします。 <ul style="list-style-type: none"><li>• public_cloud オペランド</li><li>• rep_device オペランド</li></ul> 詳細は、「 <a href="#">8.1.1 moncheck (定義チェック)</a> 」を参照してください。 |
| monlistip | パブリッククラウド環境下では、このコマンドを使用しないでください。  |
| monrp     | パブリッククラウド環境下では、このコマンドを使用しないでください。  |
| monscsicl | パブリッククラウド環境下では、このコマンドを使用しないでください。  |
| monsetup  | パブリッククラウド環境下では、このコマンドでリセットパスの設定を実施しないでください。  |
| monshow   | パブリッククラウドでない環境で表示する項目に加え、次の項目も表示します。 <ul style="list-style-type: none"><li>• レプリケーションデバイス名</li></ul> 詳細は、「 <a href="#">8.1.2 monshow (サーバと系の状態表示)</a> 」を参照してください。                                  |

### 8.1.1 moncheck (定義チェック)

パブリッククラウド環境下のmoncheck コマンドでは、パブリッククラウドでない環境でチェックする定義に加え、次の項目もチェックします。

- 必要なシェルスクリプト群を展開しているかどうか。
  - HA モニタの環境設定のpublic\_cloud オペランドにuse が指定されていて、かつ必要なシェルスクリプト群が展開されていない場合には、メッセージKAMN764-E を出力します。
  - サーバ対応の環境設定のrep\_device オペランドにリソースが指定されていて、かつ必要なシェルスクリプト群が展開されていない場合には、メッセージKAMN764-E を出力します。

シェルスクリプト群については、「[5.7 【AWS】 AWS用のシェルスクリプト群の展開](#)」, 「[5.8 【Azure】 Azure用のシェルスクリプト群の展開](#)」, または「[5.9 【OCI】 OCI用のシェルスクリプト群の展開](#)」を参照してください。

- 次のリソースがあるかどうか。
  - サーバ対応の環境設定のrep\_device オペランドに指定したリソース

- AWS 環境の場合で、サーバ対応の環境設定の fs\_name オペランドに指定した EFS リソースがこのリソースがない場合は、" not available "が表示されます。

moncheck コマンドで有無をチェックするリソースと not available が表示された場合の意味を、次に示します。

表 8-2 moncheck コマンドで有無をチェックするリソースと not available が表示された場合の意味

| 有無をチェックするリソース        |                  | not available が表示された場合の意味  |
|----------------------|------------------|--|
| サーバ対応の環境設定 (servers) | rep_device オペランド | <ul style="list-style-type: none"> <li>• 指定されたリソースが存在しない。</li> <li>• DRBD がインストールされていない。</li> <li>• DRBD が起動されていない。</li> </ul>   |
|                      | fs_name オペランド    | <p>AWS 環境下で EFS の DNS 名を指定した場合に、次のどれかに該当している。</p> <ul style="list-style-type: none"> <li>• 指定した DNS 名の EFS が存在しない。</li> <li>• DNS サーバに問い合わせできない。</li> <li>• bind-utils パッケージがインストールされていない。</li> <li>• AWS CLI がインストール・設定されていない。</li> </ul> |

なお、moncheck コマンドの詳細およびその他のチェック項目については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「moncheck (定義チェック)」の説明を参照してください。

## 8.1.2 monshow (サーバと系の状態表示)

パブリッククラウド環境のmonshow コマンドでは、パブリッククラウドでない環境で表示する項目に加え、次の項目も表示します。

- レプリケーションデバイス名

使用例について、次に示します。

共有リソース情報の表示

```
> monshow -d
KAMN213-I Own host name : host1
Server : server1
*** DISK information ***
-NAME-----
/dev/sharedvg
  neck
  on_opt="-u -n"
  forced varyon
*** LA information ***
-NAME-----
LADP01
*** Line Switch information ***
-NAME-----id----port---
```

```
/dev/tty2          001  A
*** File system information ***
-NAME-----
/dev/sharedlv1
  mount dir=/test01
  mount opt=-o rw,log=/dev/jfsloglv
*** HABST information ***
-NAME-----
0
*** SCSI device information ***
-NAME-----
/dev/hdisk1
/dev/hdisk2
/dev/dlmfdrv1
*** replication device information ***
-NAME-----
r0
r1
```

(凡例) >: ユーザの操作を示します。

なお、monshow コマンドの詳細およびその他の表示項目については、マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「monshow (サーバと系の状態表示)」の説明を参照してください。

# 付録

## 付録 A HA モニタが出力するファイル一覧

マニュアル『高信頼化システム監視機能 HA モニタ Linux(R) (x86) 編』の「HA モニタが出力するファイル一覧」を参照してください。ここでは、HA モニタが出力するファイル一覧について、パブリッククラウド環境下で差異がある事項だけを記載します。

HA モニタが出力するファイルの一覧を、次の表に示します。

なお、ファイルパス名に記載している、history, etc, またはspool で始まるパスは、/opt/hitachi/HAMon 配下を表しています。

表 A-1 HA モニタが出力するファイルの一覧

| 項番 | 名称             | ファイルパス名   | 生成・削除タイミング                            | 管理方法          | サポートバージョン | 形式   | 最大ファイルサイズ (バイト) | 運用による削除可能な spool ファイル※1 |
|----|----------------|---|---------------------------------------|---------------|-----------|------|-----------------|-------------------------|
| 1  | インスタンス ID 取得ログ | spool/cloud/<br>monclد_getinf.<br>log   | HA モニタ起動時、または起動時取得失敗後の定期実行 (60 秒間隔) 時 | _old の 2 世代管理 | 01-70 以降  | テキスト | 10,485,760      | ○                       |
| 2  |                | spool/cloud/<br>monclد_getinf.<br>log_err   |                                       |               |           |      |                 | ○                       |
| 3  | インスタンス強制停止実行ログ | AWS の場合<br>spool/<br>cloud/<br>monclد_fstop_強制停止対象インスタンス ID. log<br><br>Azure の場合<br>spool/<br>cloud/<br>monclد_fstop_強制停止対象仮想マシンのリソース ID. log<br><br>OCI の場合<br>spool/<br>cloud/<br>monclد_fstop_強制停止対 | 系のリセット (インスタンス強制停止) 時                 | _old の 2 世代管理 | 01-70 以降  | テキスト | 10,485,760      | ○                       |

| 項番 | 名称           | ファイルパス名   | 生成・削除タイミング  | 管理方法          | サポートバージョン | 形式   | 最大ファイルサイズ (バイト) | 運用による削除可能な spool ファイル※1 |
|----|--------------|---|---|---------------|-----------|------|-----------------|-------------------------|
|    |              | 象インスタンスの<br>OCID.log  |   |               |           |      |                 |                         |
| 4  | インスタンス起動実行ログ | AWS の場合<br>spool/<br>cloud/<br>monclد_start_起動対象インスタンス<br>ID.log<br><br>Azure の場合<br>spool/<br>cloud/<br>monclد_start_起動対象仮想マシンのリソース<br>ID.log<br><br>OCI の場合<br>spool/<br>cloud/<br>monclد_start_起動対象インスタンスの<br>OCID.log | 系のリセット (インスタンス強制停止) 後の起動時   | _old の 2 世代管理 | 01-70 以降  | テキスト | 10,485,760      | ○                       |
| 5  | クラウド操作定期確認ログ | spool/cloud/<br>monclد_polling_ .log  | HA モニタ起動時   | _old の 2 世代管理 | 01-70 以降  | テキスト | 10,485,760      | ○                       |
| 6  |              | spool/cloud/<br>monclد_polling_ .log_err  | AWS CLI, Azure CLI, または OCI CLI 実行可否チェックの定期実行で正常だったあとに、異常が検出された場合 | 1 世代管理        |           |      |                 | ○                       |
| 7  |              | spool/cloud/<br>monclد_polling_ .log_recover  | AWS CLI, Azure CLI, または OCI CLI                                   |               |           |      |                 | ○                       |

| 項番 | 名称                                       | ファイルパス名  | 生成・削除タイミング   | 管理方法       | サポートバージョン | 形式   | 最大ファイルサイズ<br>(バイト) | 運用による削除可能な<br>spool<br>ファイル※<br>1 |
|----|--|--|--|------------|-----------|------|--------------------|-----------------------------------|
|    |  |  | 実行可否チェックの定期実行で異常が検出されたあとに、正常だった場合                                |            |           |      |                    |                                   |
| 8  | レプリケーションパス切断時のフェンシング実行ログ                 | spool/rep/monfence-peer_rep_device名,IPアドレス.log | レプリケーションパス切断検知時  | _oldの2世代管理 | 01-70以降   | テキスト | 10,485,760         | ○                                 |
| 9  | プライマリ化抑制ログ                               | spool/rep/monrep_ctl_rep_device名.log           | 待機サーバ起動時   | _oldの2世代管理 | 01-70以降   | テキスト | 10,485,760         | ○                                 |
| 10 |  | spool/rep/monrep_ctl_rep_device名,IPアドレス.log    | レプリケーションパス切断検知時  |            |           |      |                    | ○                                 |
| 11 | rep_device 定義<br>チェックログ                  | spool/rep/monrep_chk_rep_device名.log           | 定義チェックコマンド<br>(moncheck コマンド) 実行時,<br>およびサーバ起動時                  | _oldの2世代管理 | 01-70以降   | テキスト | 10,485,760         | ○                                 |
| 12 | 【Azure】<br>クラウド後処理<br>実行ログ               | spool/cloud/monclnd_endproc.log                | HA モニタ停止時  | _oldの2世代管理 | 01-71以降   | テキスト | 10,485,760         | ○                                 |
| 13 | vip_tgw_def<br>ファイルの<br>フォーマット<br>チェックログ | spool/cloud/monclnd_defchk.log                 | moncheck コマンド実行時に,<br>vip_tgw_def<br>ファイルの<br>フォーマットが<br>正常だった場合 | _oldの2世代管理 | 01-73以降   | テキスト | 10,485,760         | ○                                 |
|    |  | spool/cloud/monclnd_defchk.log_err             | moncheck コマンド実行時に,<br>vip_tgw_def<br>ファイルの<br>フォーマットが            | 1 世代管理     |           |      |                    |                                   |



| 項番 | 名称                   | ファイルパス名   | 生成・削除タイミング   | 管理方法             | サポートバージョン   | 形式       | 最大ファイルサイズ (バイト) | 運用による削除可能な spool ファイル※1 |
|----|----------------------|---|--|------------------|-------------|----------|-----------------|-------------------------|
|    |                      |   | エラーだった場合   |                  |             |          |                 |                         |
|    |                      | spool/cloud/<br>サーバ識別名<br>_monclد_defchk<br>.log                      | サーバの起動時<br>および停止時に,<br>vip_tgw_def<br>ファイルの<br>フォーマットが<br>正常だった場合  | _old の 2<br>世代管理 |             |          |                 |                         |
|    |                      | spool/cloud/<br>サーバ識別名<br>_monclد_defchk<br>.log_err                  | サーバの起動時<br>および停止時に,<br>vip_tgw_def<br>ファイルの<br>フォーマットが<br>エラーだった<br>場合                                       | 1 世代管理           |             |          |                 |                         |
| 14 | ネットワーク遮断実行ログ         | spool/cloud/<br>monclد_fencect<br>l_ネットワーク<br>遮断対象インスタ<br>ンス ID. log  | 系切り替え時   | _old の 2<br>世代管理 | 01-75<br>以降 | テキ<br>スト | 10,485,760      | ○                       |
|    |                      | spool/cloud/<br>monclد_fencenw<br>_ネットワーク遮<br>断対象インスタ<br>ンス ID. log   |  |                  |             |          |                 |                         |
|    |                      | spool/cloud/<br>monclد_unfence<br>nw_ネットワーク<br>遮断対象インスタ<br>ンス ID. log |  |                  |             |          |                 |                         |
| 15 | ネットワーク遮断設定ファイルチェックログ | spool/cloud/<br>monclد_nwdefch<br>k. log                              | <ul style="list-style-type: none"> <li>moncheck コマンド実行時</li> <li>monts コマンド実行時</li> <li>HA モニタ起動時</li> </ul> | _old の 2<br>世代管理 | 01-75<br>以降 | テキ<br>スト | 10,485,760      | ○                       |
|    |                      | spool/cloud/<br>monclد_nwdefch<br>k. log_err                          |  |                  |             |          |                 |                         |

| 項番 | 名称            | ファイルパス名                             | 生成・削除タイミング  | 管理方法          | サポートバージョン | 形式   | 最大ファイルサイズ (バイト) | 運用による削除可能な spool ファイル※1 |
|----|---------------|-------------------------------------|---|---------------|-----------|------|-----------------|-------------------------|
| 16 | ENI 情報ファイル    | spool/cloud/.awseniinf              | HA モニタ起動時   | 1 世代管理        | 01-75 以降  | テキスト | 570             | ×                       |
| 17 | ENI アタッチツールログ | spool/cloud/awseniattchttool.log    | ENI アタッチツール実行時  | _old の 2 世代管理 | 01-75 以降  | テキスト | 変動値※2           | ○                       |
| 18 | EFS 存在チェックログ  | spool/cloud/monclد_fsdefchk.log     | ファイルシステムに EFS を使用する場合の、moncheck/monts コマンド実行時         | _old の 2 世代管理 | 01-78 以降  | テキスト | 10,485,760      | ○                       |
|    |               | spool/cloud/monclد_fsdefchk.log_err | ファイルシステムに EFS を使用する場合の、moncheck/monts コマンド実行時 (異常検出時) | _old の 2 世代管理 | 01-78 以降  | テキスト | 10,485,760      | ○                       |

(凡例)

○：削除できます。

注※1

HA モニタを停止してから削除してください。また、ディレクトリは削除しないでください。

注※2

処理対象の ENI の数によって最大ファイルサイズは変化します。

## 付録 B 各バージョンの変更内容

各バージョンの変更内容を示します。

### 付録 B.1 HA モニタ 01-77 の変更内容 (3000-9-204-60)

HA モニタ 01-77 の変更内容 (3000-9-204-60) を次の表に示します。

| 追加・変更内容  |
|--|
| Azure の場合に、マネージドディスクの共有による共有ディスク構成をサポートした。           |
| Amazon EC2 のインスタンスメタデータサービスバージョン 2 (IMDSv2) をサポートした。 |
| インスタンスのメタデータ取得のための設定について、説明を変更した。                    |

### 付録 B.2 HA モニタ 01-76, HA モニタ 01-75 の変更内容 (3000-9-204-50)

HA モニタ 01-76 の変更内容 (3000-9-204-50) を次の表に示します。

| 追加・変更内容                                     |
|---|
| AWS の場合に、EBS マルチアタッチ機能を使用した共有ディスク構成をサポートした。 |

HA モニタ 01-75 の変更内容 (3000-9-204-50) を次の表に示します。

| 追加・変更内容                                      |
|--|
| AWS の場合に、系切り替えの方法としてネットワーク遮断による系切り替えをサポートした。 |

### 付録 B.3 HA モニタ 01-74 の変更内容 (3000-9-204-40)

HA モニタ 01-74 の変更内容 (3000-9-204-40) を次の表に示します。

| 追加・変更内容  |
|--|
| 適用 OS に Oracle Linux 7(x86_64), Oracle Linux 8(x86_64)を追加した。 |
| 使用できるパブリッククラウドとして OCI をサポートした。                               |

## 付録 B.4 HA モニタ 01-73 の変更内容 (3000-9-204-30)

HA モニタ 01-73 の変更内容 (3000-9-204-30) を次の表に示します。

| 追加・変更内容                                       |
|---|
| AWS 環境下で、複数のリージョン間や複数の VPC 間での系切り替えをできるようにした。 |

## 付録 B.5 HA モニタ 01-72 の変更内容 (3000-9-204-20)

HA モニタ 01-72 の変更内容 (3000-9-204-20) を次の表に示します。

| 追加・変更内容   |
|---|
| HA モニタの環境設定の <code>public_cloud</code> オペランドに <code>use</code> を指定した場合の、次のオペランドの注意事項を追記した。 <ul style="list-style-type: none"><li>HA モニタの環境設定の <code>clearwait</code> オペランド</li><li>HA モニタの環境設定の <code>clearcheck</code> オペランド</li></ul> |

## 付録 B.6 HA モニタ 01-71 の変更内容 (3000-9-204-10)

HA モニタ 01-71 の変更内容 (3000-9-204-10) を次の表に示します。

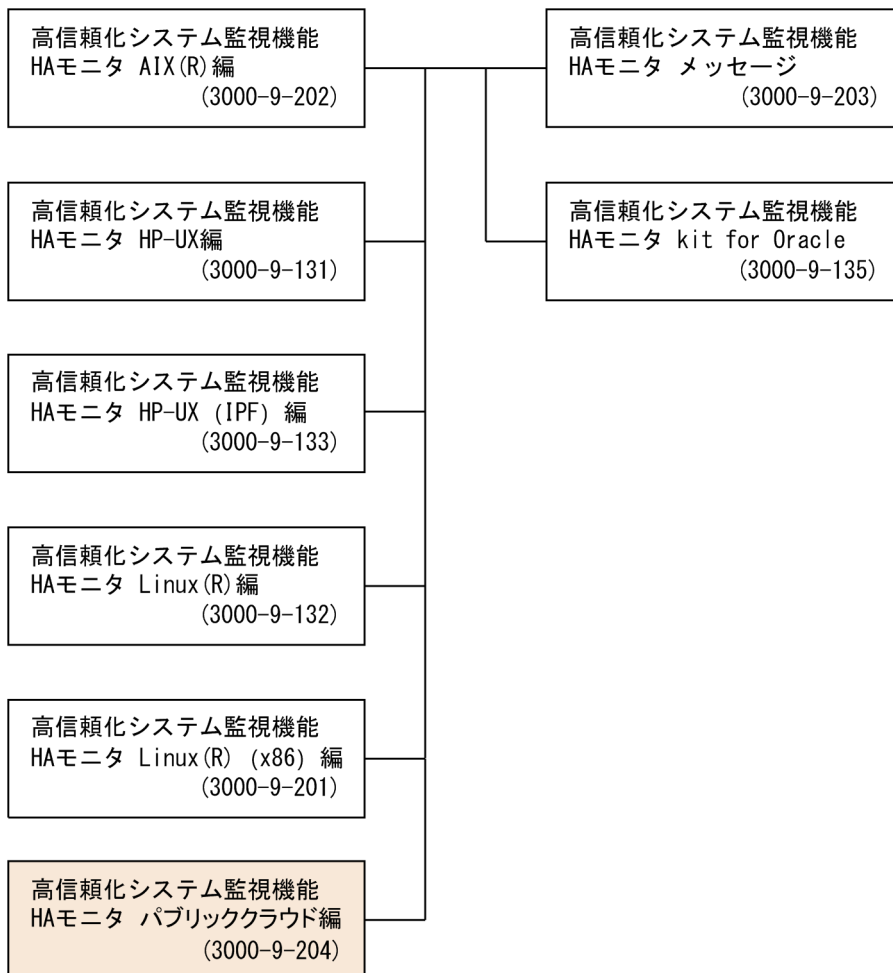
| 追加・変更内容   |
|---|
| 適用 OS を追加・削除した。 <ul style="list-style-type: none"><li>RHEL8 を追加した。</li><li>RHEL5 を削除した。</li></ul> |
| 使用できるパブリッククラウドとして Azure をサポートした。  |
| AWS 環境下の通信制御の方式に、DNS 名制御による業務通信の切り替えを追加した。  |

## 付録 C このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

### 付録 C.1 関連マニュアル

HA モニタのマニュアル体系を次に示します。



HA モニタのマニュアル以外で、このマニュアルと関連するマニュアルを次に示します。必要に応じてお読みください。

#### プログラムに OpenTP1 を使用する場合

- 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 解説』 (3000-3-D50)
- 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 システム定義』 (3000-3-D52)
- 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 運用と操作』 (3000-3-D53)
- 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 メッセージ』 (3000-3-D56)

- 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 クライアント使用の手引 TP1/Client/W, TP1/Client/P 編』 (3000-3-D58)
- 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 クライアント使用の手引 TP1/Client/J 編』 (3000-3-D59)
- 『OpenTP1 Version 7 分散トランザクション処理機能 TP1/Server Base Enterprise Option 使用の手引』 (3000-3-F51)
- 『OpenTP1 Version 7 高速トランザクション処理基盤 TP1/EE/Extended Transaction Controller 使用の手引』 (3000-3-F54)

## プログラムに HiRDB を使用する場合

- 『HiRDB Version 9 解説』 (3020-6-450)
- 『HiRDB Version 9 システム導入・設計ガイド (UNIX(R)用)』 (3000-6-452)
- 『HiRDB Version 9 システム定義 (UNIX(R)用)』 (3000-6-453)
- 『HiRDB Version 9 システム運用ガイド (UNIX(R)用)』 (3000-6-454)
- 『HiRDB Version 9 コマンドリファレンス (UNIX(R)用)』 (3000-6-455)
- 『HiRDB Version 9 メッセージ』 (3020-6-458)
- 『HiRDB Version 10 解説』 (3020-6-551)
- 『HiRDB Version 10 システム導入・設計ガイド (UNIX(R)用)』 (3020-6-552)
- 『HiRDB Version 10 システム定義 (UNIX(R)用)』 (3020-6-554)
- 『HiRDB Version 10 システム運用ガイド (UNIX(R)用)』 (3020-6-556)
- 『HiRDB Version 10 コマンドリファレンス (UNIX(R)用)』 (3020-6-558)
- 『HiRDB Version 10 メッセージ』 (3020-6-562)

## イベント管理によってシステムの運用を自動化する場合

- 『JP1 Version 11 JP1/Base 運用ガイド』 (3021-3-A01)
- 『JP1 Version 11 JP1/Base メッセージ』 (3021-3-A02)
- 『JP1 Version 12 JP1/Base 運用ガイド』 (3021-3-D65)
- 『JP1 Version 12 JP1/Base メッセージ』 (3021-3-D66)

## ディスクパスを冗長化する場合

- 『Hitachi Dynamic Link Manager Software ユーザーズガイド (Linux(R)用)』 (3000-3-F04)

## N+M コールドスタンバイ構成で系切り替えをする場合

- 『Hitachi Command Suite Compute Systems Manager Software ユーザーズガイド』 (3020-3-V91)

- 『Hitachi Command Suite Compute Systems Manager ユーザーズガイド』(3021-9-096)

なお、このマニュアルでは、次のマニュアルを省略して表記しています。マニュアルの正式名称とこのマニュアルでの表記を次の表に示します。

| このマニュアルでの表記  | マニュアルの正式名称   |
|--|--|
| 『JP1/Base 運用ガイド』   | 『JP1 Version 11 JP1/Base 運用ガイド』  |
|  | 『JP1 Version 12 JP1/Base 運用ガイド』  |
| 『分散トランザクション処理機能 OpenTP1 システム定義』                          | 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 システム定義』                          |
| 『分散トランザクション処理機能 OpenTP1 運用と操作』                           | 『OpenTP1 Version 7 分散トランザクション処理機能 OpenTP1 運用と操作』                           |
| 『分散トランザクション処理機能 TP1/Server Base Enterprise Option 使用の手引』 | 『OpenTP1 Version 7 分散トランザクション処理機能 TP1/Server Base Enterprise Option 使用の手引』 |
| 『HiRDB システム定義』   | 『HiRDB Version 9 システム定義 (UNIX(R)用)』  |
|  | 『HiRDB Version 10 システム定義 (UNIX(R)用)』                                       |
| 『HiRDB システム運用ガイド』  | 『HiRDB Version 9 システム運用ガイド (UNIX(R)用)』                                     |
|  | 『HiRDB Version 10 システム運用ガイド (UNIX(R)用)』                                    |

## 付録 C.2 このマニュアルで使用する製品名・機能名

このマニュアルでは、製品名を次のように表記しています。

| 表記    | 製品名                    |   |
|-------|------------------------|---|
| AWS   | Amazon Web Services    |   |
| Azure | Microsoft Azure        |   |
| HiRDB | HiRDB Version 9        | HiRDB Accelerator Version 9                     |
|       |                        | HiRDB Advanced High Availability Version 9      |
|       |                        | HiRDB Server Version 9                          |
|       |                        | HiRDB Server with Additional Function Version 9 |
|       | HiRDB Version 10       | HiRDB Accelerator Version 10                    |
|       |                        | HiRDB Advanced High Availability Version 10     |
|       |                        | HiRDB Server Version 10                         |
| Linux | Linux(R)               |   |
| Linux | Linux (x86)            |   |
|       | Oracle Linux 7(x86_64) |   |

| 表記          |                            | 製品名  |
|-------------|----------------------------|--|
|             |                            | Oracle Linux 8(x86_64)                                 |
|             |                            | Red Hat(R) Enterprise Linux(R) server 7(x86_64)        |
|             |                            | Red Hat(R) Enterprise Linux(R) server 8(x86_64)        |
|             |                            | Red Hat(R) Enterprise Linux(R) server 9(64-bit x86_64) |
|             | RHEL7                      | Red Hat(R) Enterprise Linux(R) server 7(x86_64)        |
|             | RHEL8                      | Red Hat(R) Enterprise Linux(R) server 8(x86_64)        |
|             | RHEL9                      | Red Hat(R) Enterprise Linux(R) server 9(64-bit x86_64) |
| OpenTP1     | TP1/High Availability      | TP1/High Availability                                  |
|             |                            | uCosminexus TP1/High Availability                      |
|             |                            | uCosminexus TP1/High Availability(64)                  |
|             | TP1/Message Control        | TP1/Message Control                                    |
|             |                            | uCosminexus TP1/Message Control                        |
|             |                            | uCosminexus TP1/Message Control(64)                    |
|             | TP1/NET/High Availability  | TP1/NET/High Availability                              |
|             |                            | uCosminexus TP1/NET/High Availability                  |
|             |                            | uCosminexus TP1/NET/High Availability(64)              |
|             | TP1/NET/Library            | TP1/NET/Library  |
|             |                            | uCosminexus TP1/NET/Library                            |
|             |                            | uCosminexus TP1/NET/Library(64)                        |
|             | TP1/NET/TCP/IP             | TP1/NET/TCP/IP   |
|             |                            | uCosminexus TP1/NET/TCP/IP                             |
|             |                            | uCosminexus TP1/NET/TCP/IP(64)                         |
|             | TP1/Server Base            | TP1/Server Base  |
|             |                            | uCosminexus TP1/Server Base                            |
|             |                            | uCosminexus TP1/Server Base(64)                        |
|             | TP1/EE                     | uCosminexus TP1/Server Base Enterprise Option          |
|             |                            | uCosminexus TP1/Server Base Enterprise Option(64)      |
|             | TP1/XTC                    | TP1/EE/Extended Transaction Controller                 |
| UNIX        | UNIX                       |  |
| VMware ESXi | VMware ESXi(TM)            |  |
|             | VMware vSphere(R) ESXi(TM) |  |



## 付録 C.3 このマニュアルで使用する英略語

このマニュアルで使用する英略語を、次に示します。

| 英略語    | 英字での表記  |
|--------|---|
| CLI    | Command Line Interface                          |
| DNS    | Domain Name System                              |
| DRBD   | Distributed Replicated Block Device             |
| I/O    | Input/Output                                    |
| LAN    | Local Area Network                              |
| LVM    | Logical Volume Manager                          |
| NLB    | Network Load Balancer                           |
| OCI    | Oracle Cloud Infrastructure                     |
| OS     | Operating System                                |
| PC     | Personal Computer                               |
| SCSI   | Small Computer System Interface                 |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UAP    | User Application Program                        |

## 付録 C.4 このマニュアルで使用する KB (キロバイト) などの単位表記

1KB (キロバイト), 1MB (メガバイト), 1GB (ギガバイト), 1TB (テラバイト) はそれぞれ  $1,024$  バイト,  $1,024^2$  バイト,  $1,024^3$  バイト,  $1,024^4$  バイトです。

# 索引

## 記号

/etc/hosts ファイルの永続化 101

## 数字

1:1 系切り替え構成 (AWS) 14

1:1 系切り替え構成 (Azure) 19

## A

AWS CLI のインストール・設定 92

AWS 環境で HA モニタを使用する場合の構成 164

AWS での通信経路の制御

DNS 名制御 70

EIP 制御 68

VIP 制御 53, 56, 60, 66

AWS の設定 92

EBS マルチアタッチの設定 94

EFS の設定 94

ENI の設定 94

インスタンスのメタデータ取得のための設定 93

エンドポイントの設定 93

プロキシを使用する場合の設定 93

Azure CLI のインストール・設定 96

Azure DNS の設定 99

Azure ロードバランサー制御 76

Azure ロードバランサーの作成・設定 98

Azure 環境で HA モニタを使用する場合の構成 186

Azure での通信経路の制御

Azure ロードバランサー制御 76

DNS 名制御による業務通信の切り替え 78

Azure の設定 96

Azure CLI のインストール・設定 96

Azure DNS の設定 99

Azure ロードバランサーの作成・設定 98

インスタンスのメタデータ取得のための設定 97

プロキシを使用する場合の設定 97

## C

CLI 実行可否チェック 39

## D

DNS 名制御 70

DRBD 102

## E

EBS マルチアタッチの設定 94

EFS の設定 94

EIP 制御 68

ENI の設定 94

## F

fence\_network 157

## H

HA モニタが系切り替えをする条件 39

HA モニタが検出する障害 13

HA モニタで使用できる機能一覧 45

HA モニタによる障害検出 39

HA モニタの環境設定 157

fence\_network 157

public\_cloud 157

パブリッククラウド環境固有の HA モニタの環境設定 157

パブリッククラウド環境で注意が必要な HA モニタの環境設定のオペランド 158

HA モニタの動作環境 14

## L

LAN の監視に必要なファイルの設定 147

LAN の管理 (AWS) 52, 84

LAN の管理 (Azure) 76

LAN の状態設定ファイルの設定 (AWS)

1 つの VPC 内で系切り替えをする場合の設定 115

1 つのリージョン内で系切り替えをする場合の設定 115

クライアントからの通信が NLB を経由する構成の場合の設定 140

複数の VPC 間で系切り替えをする場合の設定 121

複数の VPC 間で系切り替えをする場合の設定 (DNS 制御の場合) 139

複数の VPC 間で系切り替えをする場合の設定 (VIP 制御の場合) 124, 131

複数のリージョン間で系切り替えをする場合の設定 121

複数のリージョン間で系切り替えをする場合の設定 (DNS 制御の場合) 139

複数のリージョン間で系切り替えをする場合の設定 (VIP 制御の場合) 124, 131

LAN の状態設定ファイルの設定 (Azure) 140

LAN の状態設定ファイルの設定 (OCI) 144

## M

moncheck 202

monshow 203

## O

OCI CLI のインストール・設定 100

OCI 環境で HA モニタを使用する場合の構成 195

OCI での通信経路の制御

プライベート IP アドレス制御 84

OCI の設定 100

/etc/hosts ファイルの永続化 101

OCI CLI のインストール・設定 100

インスタンスのメタデータ取得のための設定 100

エンドポイントの設定 101

プロキシを使用する場合の設定 100

ブロック・ボリュームの設定 101

## P

public\_cloud 157

## R

rep\_device 161

## S

server\_aws\_vpc.down 121, 124, 131, 139

server\_aws\_vpc.up 121, 124, 131, 139

server\_aws.down 115

server\_aws.up 115

server\_azure.down 140

server\_azure.up 140

server\_oci.down 144

server\_oci.up 144

## V

vip\_tgw\_def 121, 124, 131

VIP 制御 53, 56, 60, 66

1 つの VPC 内での系切り替え 53

1 つのリージョン内での系切り替え 53

クライアントからの通信が NLB を経由する構成 66

複数の VPC 間での系切り替え 56, 58, 60

複数のリージョン間での系切り替え 56, 58, 60

## い

インスタンスのメタデータ取得のための設定 93, 97, 100

## え

エンドポイントの設定 93, 101

## か

環境構成例

AWS 環境で HA モニタを使用する場合の構成 164, 173, 181

Azure 環境で HA モニタを使用する場合の構成 186

OCI 環境で HA モニタを使用する場合の構成 195

監視パスの設定 112

## き

起動・停止 151

機能一覧 45

業務ディスクの管理 50

基本的な制御 50

レプリケーションパス障害時の制御 50  
業務ディスクの設定 115  
共有ディスク構成の場合の環境設定例 181

## け

系切り替え (AWS) 27  
系切り替え (Azure) 34  
系切り替え (OCI) 36  
系切り替えの方式 13  
系障害時の系切り替え (AWS) 27  
系障害時の系切り替え (Azure) 34  
系障害時の系切り替え (OCI) 36  
系障害の検出 39  
系の管理 48  
系のリセットによる系切り替え 27  
系のリセットによる系切り替えをする場合 (レプリケーション構成) の環境設定例 164  
系のリセットまたはネットワーク遮断をする系の決定方法 48  
系のリセットまたはネットワーク遮断をする場合 91  
系やサーバを稼働させたままリソースの構成を変更する 152

## こ

構築の流れ 91  
このマニュアルの読み方 11

## さ

サーバが使用するリソースの設定 115  
サーバと系の状態表示 [コマンド] 203  
サーバの環境設定 161  
パブリッククラウド環境固有のサーバの環境設定 161  
パブリッククラウド環境で注意が必要なサーバ対応の環境設定のオペランド 162  
サーバを追加する 152  
サービスプリンシパル情報設定ファイルの設定 (Azure) 113

## し

シェルスクリプト群の展開 (AWS) 106  
シェルスクリプト群の展開 (Azure) 108  
シェルスクリプト群の展開 (DRBD) 105  
シェルスクリプト群の展開 (OCI) 110  
システム運用時の注意事項 153  
システムの変更 152  
障害検出から系切り替えまでの流れ 27  
処理の流れ (AWS) 87  
処理の流れ (Azure) 88  
処理の流れ (OCI) 89

## て

定義チェック [コマンド] 202  
定義ファイルの概要 156  
定義ファイルの作成 (HA モニタ) 113  
ディスクをレプリケーションする構成 161

## ね

ネットワーク遮断設定ファイルの設定 114  
ネットワーク遮断による系切り替え 29  
ネットワーク遮断による系切り替えをする場合 (レプリケーション構成) の環境設定例 173

## は

パブリッククラウド環境下の HA モニタ 13  
パブリッククラウド環境固有の HA モニタの環境設定 157  
パブリッククラウド環境固有のサーバの環境設定 161  
パブリッククラウド環境で注意が必要な HA モニタの環境設定のオペランド 158  
パブリッククラウド環境で注意が必要なコマンド 202  
パブリッククラウド環境で注意が必要なサーバ対応の環境設定のオペランド 162  
パブリッククラウド環境のコンソール操作 (CLI 発行含む) をする場合の注意事項 153

## ひ

必要な AWS 環境 14  
必要な Azure 環境 18

必要な OCI 環境 23

必要なソフトウェア 25

## ふ

複数スタンバイ構成 (AWS) 16

複数スタンバイ構成 (Azure) 21

複数の VPC 間での系切り替え

系切り替え時の動作 60

ルーティングの動作 58

複数の待機系がある場合の系のリセットまたはネットワーク遮断 48

複数のリージョン間での系切り替え

系切り替え時の動作 60

ルーティングの動作 58

プライベート IP アドレス制御 84

プロキシを使用する場合の設定 93, 97, 100

ブロック・ボリュームの設定 101

## ま

マネージドディスクの共有 99

## り

リセットパスの設定 111

リソースの監視のための設定 147

リソースの管理 50

リソースの引き継ぎ 41-43

両系が障害を同時に検出した場合の系切り替え 48

## れ

レプリケーションソフト 153

DRBD 102

レプリケーションソフト (DRBD) の設定 102

レプリケーションソフトを使用する場合の注意事項  
153

レプリケーションパス障害時の制御 50

---

 株式会社 日立製作所

〒 100-8280 東京都千代田区丸の内一丁目 6 番 6 号

---