



**SIOS Protection Suite for Linux
EC2 Recovery Kit
v9.3.1**

管理ガイド

2018年11月

本書およびその内容は SIOS Technology Corp. (旧称 SteelEye® Technology, Inc.) の所有物であり、許可なく使用および複製は禁止されています。SIOS Technology Corp. は本書の内容に関していかなる保証も行いません。また、事前の通知なく本書を改訂し、本書に記載された製品に変更を加える権利を保有しています。SIOS Technology Corp. は、新しい技術、コンポーネント、およびソフトウェアが利用可能になるのに合わせて製品を改善することを方針としています。そのため、SIOS Technology Corp. は事前の通知なく仕様を変更する権利を保留します。

LifeKeeper、SteelEye、および SteelEye DataKeeper は SIOS Technology Corp. の登録商標です。

本書で使用されるその他のブランド名および製品名は、識別のみを目的として使用されており、各社の商標が含まれています。

出版物の品質を維持するために、弊社は本書の正確性、明瞭性、構成、および価値に関するお客様のご意見を歓迎いたします。

以下の宛先に電子メールを送信してください。

ip@us.sios.com

Copyright © 2018

By SIOS Technology Corp.

San Mateo, CA U.S.A.

All rights reserved

目次

Chapter 1: はじめに	1
Recovery Kit for EC2	1
SIOS Protection Suite ドキュメンテーション	1
運用の原則	1
ルートテーブルシナリオ (バックエンド クラスタ):	1
図 1: ルートテーブルシナリオ	2
Elastic IP シナリオ (フロントエンド クラスタ):	3
図 2: Elastic IP シナリオ	4
Chapter 2: 要件	5
Chapter 3: 設定	7
Amazon EC2 特有の設定上の考慮事項	7
Amazon EC2 特有の設定上の考慮事項	7
Recovery Kit for EC2 のチューニング	8
リソース階層の作成	8
リソース階層の削除	10
リソース階層の拡張	10
ローカルリカバリと設定に関する考慮事項	12
ローカルリカバリシナリオ (バックエンド クラスタ):	12
Elastic IP シナリオ (フロントエンド クラスタ):	13
リソース監視と設定に関する考慮事項	13
ルートテーブルシナリオ (バックエンド クラスタ)	13
Elastic IP シナリオ (フロントエンド クラスタ):	13
リソース階層の拡張解除	13
ユーザシステムのセットアップ	14
ルートテーブルシナリオ (バックエンド クラスタ)	14
Elastic IP シナリオ (フロントエンド クラスタ)	15
既存リソースの IAM ロールへの対応	16

IAM ロール移行ツール実行手順	16
移行確認テスト	17

Chapter 1: はじめに

Recovery Kit for EC2

Recovery Kit for EC2 は、障害の発生したプライマリサーバから Elastic IP をバックアップサーバに復旧する仕組みを提供します。また、複数の Availability Zone で IP Recovery Kit を動作可能にする仕組みも提供します。

Recovery Kit for EC2 の定義、シナリオ、および運用の比較と詳細については、[運用の原則](#)を参照してください。

SIOS Protection Suite ドキュメンテーション

以下は、SIOS Technology Corp が発行している SIOS Protection Suite for Linux 関連ドキュメントの一覧です。

- [SPS for Linux テクニカルドキュメンテーション](#)
- [SPS for Linux リリースノート](#)
- [SIOS Technology Corp. ドキュメンテーション](#)

詳細については、[Amazon Elastic Compute Cloud \(EC2\) ドキュメント](#)を参照してください。

注記: LifeKeeper 9.2.2でIAM ロールをサポートしました。それに伴って、LifeKeeper 9.2.1もしくはそれ以前のバージョンからLifeKeeper 9.2.2もしくはそれ以降のバージョンにアップグレードする場合は、[既存リソースのIAM ロールへの対応](#)に従って移行の手続きをしてください。

注記: 「Amazon Web Services」、「Powered by Amazon Web Services」のロゴ、「AWS」、「Amazon EC2」、「EC2」、「Amazon Elastic Compute Cloud」、「Amazon Virtual Private Cloud」、および「Amazon VPC」は、米国その他の国における Amazon.com, Inc. またはその関連会社の商標です。

運用の原則

Recovery Kit for EC2 には機能が2つあります。

1. ルートテーブルシナリオ (バックエンドクラスタ) は、LifeKeeper が保護する IP リソースに Amazon VPC™ 内のクライアントから接続できるように、ルートテーブルを管理します。
2. Elastic IP シナリオ (フロントエンドクラスタ) は、インターネットから使用できる Elastic IP を管理します。

ルートテーブルシナリオ (バックエンドクラスタ):

ルートテーブルの管理と運用について理解しやすいように、図 1 に示すシナリオについて考えてみましょう。

この設定例は、1つの Amazon VPC™ と2つの利用可能ゾーン (AZ) で構成されています。

図 1: ルートテーブルシナリオ

各 AZ にサブネットが 2 つあります。

- 1 つ目のサブネット (以下「パブリックサブネット」) は、ルートテーブル別のインターネットゲートウェイを経由してインターネットに接続します (10.0.1.0/24 および 10.0.3.0/24 のルートテーブルを参照)。
- 2 つ目のサブネット (以下「プライベートサブネット」) は、ルートテーブル別の NAT インスタンスを経由してインターネットに接続します (10.0.2.0/24 および 10.0.4.0/24 のルートテーブルを参照)。

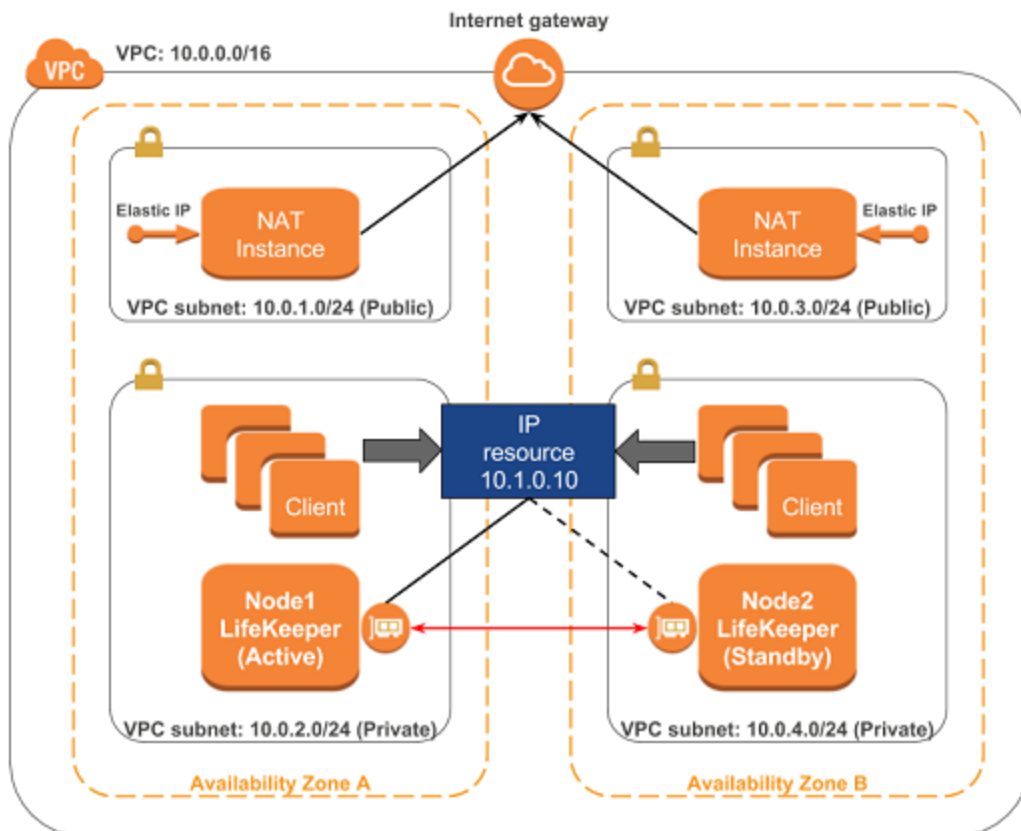
各パブリックサブネットには、NAT の Elastic IP を割り当てる EC2 インスタンス (以下「NAT インスタンス」) が 1 つあります。

各プライベートサブネットには、LifeKeeper のアクティブ / スタンバイ (以下それぞれ「Node1」および「Node2」) の EC2 インスタンスが 1 つあり、Node1/Node2 により保護されたアプリケーションを使用するクライアントが複数あります。

Node1/Node2 はそれぞれ、Elastic Network Interface (ENI) を 2 つ持ちます。

各インスタンスと各ノードとの間で通信が可能なように、ネットワーク ACL とセキュリティグループを設定します。

図 1: ルートテーブルシナリオ



10.0.1.0/24 および 10.0.3.0/24 のルートテーブル

接続先	ターゲット	注記
10.0.0.0/16	ローカル	デフォルト
0.0.0.0/0	インターネット ゲートウェイ	インターネットに接続するには、Elastic IP を割り当てる必要があります。

10.0.2.0/24 のルートテーブル

接続先	ターゲット	注記
10.0.0.0/16	ローカル	デフォルト
10.1.0.10/32 (IP リソース)	LifeKeeper のアクティブなノード上の Elastic Network Interface (ENI)	このターゲットは、スイッチオーバー中に Recovery Kit for EC2 により更新されます。
0.0.0.0/0	NAT インスタンス (10.0.1.0)	NAT 経由でインターネットに接続

10.0.4.0/24 のルートテーブル

接続先	ターゲット	注記
10.0.0.0/16	ローカル	デフォルト
10.1.0.10/32 (IP リソース)	LifeKeeper のアクティブなノード上の Elastic Network Interface (ENI)	このターゲットは、スイッチオーバー中に Recovery Kit for EC2 により更新されます。
0.0.0.0/0	NAT インスタンス (10.0.3.0)	NAT 経由でインターネットに接続

リソースのスイッチオーバーが実行されると、LifeKeeper は Node1 の IP リソースを Out of Service にします。各プライベートサブネット内の 10.1.0.10/32 のターゲット エントリは、Node2 の ENI を反映するように更新されます。Node2 の IP リソースが In-Service になります。このため、IP アドレス 10.1.0.10 へのトラフィックは、プライベートサブネット内でのルートテーブル設定の変更により効果的に Node2 に転送されます。

パブリックサブネットを含む他のサブネットから IP アドレス 10.1.0.10 にアクセスする必要がある場合、それぞれのサブネットのルートテーブルのエントリに接続先 10.1.0.10/32 のルートを追加してください。LifeKeeperは、VPC内のルートテーブルで接続先が"10.1.0.10/32"になっている全てのエントリを制御します。

Elastic IP シナリオ (フロントエンドクラスタ):

Elastic IP の管理と運用について理解しやすいように、図 2 に示すシナリオについて考えてみましょう。

この設定例は、1 つの Amazon VPC™ と 2 つの利用可能ゾーン (AZ) で構成されています。

各 AZ にサブネットが 1 つあります。

各サブネットは、ルートテーブル別のインターネットゲートウェイを経由して、インターネットに接続します。

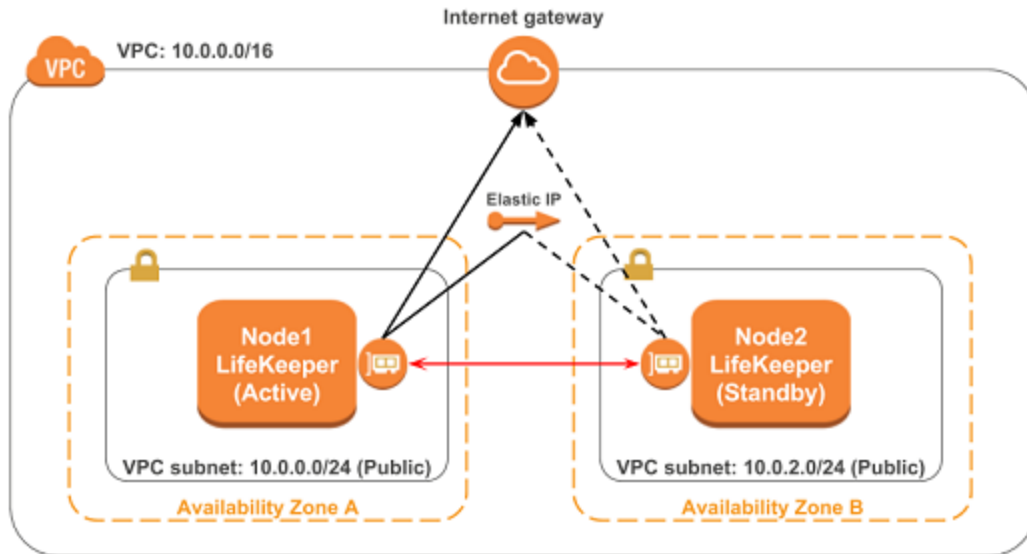
サブネットには、LifeKeeper のアクティブ / スタンバイ (以下それぞれ「Node1」および「Node2」) の EC2 インスタンスが 1 つあります。

図 2: Elastic IP シナリオ

Node1/Node2 はそれぞれ、Elastic Network Interface (ENI) を 2 つ持ちます。

各ノード間で通信が可能ないように、ネットワーク ACL とセキュリティグループを設定します。

図 2: Elastic IP シナリオ



システム管理者が、フロントエンドクラスタの Elastic IP アドレスを ENI に割り当てます。

Node1 をリソースのプライマリサーバと仮定すると、システム管理者は [リソース階層の作成](#) セクションで説明しているウィザードを使用して、Node1 上に EC2 リソース階層を作成します。

リソースのスイッチオーバーが実行されると、Recovery Kit for EC2 は Node1 の ENI と Elastic IP との関連付けを解除します。Recovery Kit for EC2 は、Elastic IP が Node2 の ENI と関連付けられているかどうかを調べ、関連付けられていない場合は、Elastic IP を ENI に関連付けます。このため、インターネット上のクライアントは、スイッチオーバー後に Elastic IP 経由で Node2 に接続できます。

注記: EC2 インスタンスを制御するために、スタンバイノードもエンドポイントにアクセスできる必要があります。即ち、VPC 外部への接続が必要ですので、ご注意ください。詳しくは [要件](#) を参照してください。なお、PrivateLink を利用すればエンドポイントへのアクセスにパブリック IP アドレスを必要としません。詳しくは [VPC エンドポイント](#) を参照してください。

Chapter 2: 要件

Recovery Kit for EC2 のインストール/ アンインストールを試みる前に、Amazon Web Service のソフトウェア要件と Recovery Kit for EC2 のインストール/ アンインストールの手順を理解しておく必要があります。

Amazon Web Service およびソフトウェアの要件

Recovery Kit for EC2 をインストールして設定する前に、使用している設定が以下の要件を満たしていることを確認してください。

Amazon Virtual Private Cloud (VPC):

- この Recovery Kit を使用するには、VPC を AWS 内に設定する必要があります。
- 異なる Availability Zone (AZ) に作成された 2 つ以上のサブネット
- 各サブネットに、関連するルートテーブルがあります。
- パブリック (フロントエンド) クラスタを設定する場合、Elastic IP を 1 つ以上割り当てる必要があります。

Amazon Elastic Compute Cloud (EC2):

- この Recovery Kit を使用するには、EC2 インスタンスが 2 つ以上必要です。
- インスタンスは、各サブネット上で関連付けられます。
- インスタンスは、Elastic Network Interface (ENI) に接続されます。
- AWS Command Line Interface (AWS CLI) を全ての EC2 インスタンスにインストールする必要があります。インストール方法は、[「AWS Command Line Interface のインストール」](#)を参照してください。
- 全ての EC2 インスタンスで、Amazon EC2 サービスのエンドポイント ([AWS のリージョンとエンドポイント](#)) にプロトコル HTTP および HTTPS を使用してアクセスする必要があります。EC2 および OS の設定を適切に行ってください。
- Amazon EC2 インスタンスのメタデータを取得するため、IP アドレス 169.254.169.254 にプロトコル HTTP でアクセスする必要があります。
- AWS CLI を用いているため、TCP ポート 443 でのアウトバウンド接続を有効にする必要があります。
- Auto Recovery 機能は LifeKeeper の回復機能と競合する可能性があるため、併用は推奨しません。

注記: 設定ファイル `/etc/default/LifeKeeper` のパラメーター `PATH` に AWS CLI 実行ファイルのパスが設定されていない場合、`PATH` に AWS CLI 実行ファイルのパスを追加してください。

AWS Identity and Access Management (IAM):

LifeKeeperがAWSを操作するために、以下のアクセス権限を持ったIAM ユーザーもしくはIAM ロールが必要です。EC2 インスタンスの root ユーザーからアクセスできるように[EC2の IAM ロール](#)を設定するか、[AWS CLI の設定](#)を適切に行ってください。

- ec2:DisassociateAddress
- ec2:DescribeAddresses
- ec2:AssociateAddress
- ec2:DescribeRouteTables
- ec2:ReplaceRoute

LifeKeeper ソフトウェア:

各サーバに同じバージョンの LifeKeeper ソフトウェアとパッチをインストールする必要があります。具体的な LifeKeeper の要件については、[SPS for Linux テクニカルドキュメンテーション](#)および[SPS for Linux リリースノート](#)を参照してください。

LifeKeeper Recovery Kit for EC2:

各サーバに同じバージョンの Recovery Kit for EC2 ソフトウェアとパッチをインストールする必要があります。

LifeKeeper IP Recovery Kit:

ルートテーブル(バックエンドクラスタ)を保護する目的で Recovery Kit for EC2を使用する場合、各サーバに同じバージョンの LifeKeeper for Linux IP Recovery Kit ソフトウェアとパッチをインストールする必要があります。

注記: 最新リリースの互換性と発注情報については、[SPS for Linux リリースノート](#)を参照するか、営業担当者に問い合わせてください。LifeKeeper Recovery Kit for EC2 のインストール/アンインストール方法の具体的な手順については、[SIOS Protection Suite インストールガイド](#)を参照してください。

Chapter 3: 設定

必要とする保護と柔軟性が得られるように LifeKeeper を設定するには、設定要件を把握している必要があります。設定を適切にプランニングするには、Amazon、Amazon Virtual Private Cloud (VPC)、Amazon Elastic Compute Cloud (EC2)、およびユーザシステムの階層設定オプションを理解する必要があります。このセクションでは、設定のプランニングに加え、Recovery Kit を設定するために必要な特定の作業についても説明します。

Amazon EC2 特有の設定上の考慮事項

Recovery Kit for EC2 を正しく設定するために、以下のトピックを見直して、設定作業を完了するために必要な情報を用意してあることを確認してください。

- [ユーザシステムのセットアップ](#)

更なる設定上の考慮事項については、以下のトピックを参照してください。

- [EC2 のリソース監視と設定に関する考慮事項](#)
- [EC2 のローカルリカバリと設定に関する考慮事項](#)

Amazon EC2 特有の設定上の考慮事項

このセクションでは、EC2 リソースの以下の設定タスクについて説明します。設定タスクは EC2 リソースインスタンスに特有のものであり、Recovery Kit ごとに異なります。

- [リソース階層の作成](#): アプリケーションリソース階層を LifeKeeper クラスタに作成します。
- [リソース階層の削除](#): リソース階層を LifeKeeper クラスタ内のすべてのサーバから削除します。
- [リソース階層の拡張](#): リソース階層をプライマリサーバからバックアップサーバへ拡張します。
- [リソース階層の拡張解除](#): リソース階層を LifeKeeper クラスタ内の 1 つのサーバから拡張解除 (削除) します。
- EC2 設定のプロパティの確認および編集: EC2 リソースの設定を表示し、その一部を修正することが可能です。
- [Recovery Kit for EC2 のチューニング](#): Recovery Kit for EC2 の動作を調整します。

以下の作業は、[SPS for Linux テクニカルドキュメンテーションの管理](#) セクションに記載されています。これらは、すべての Recovery Kit で同じ手順を使用する共通の作業です。

- [リソース依存関係の作成](#): 既存のリソース階層と別のリソースインスタンスとの間に親子の依存関係を作成し、クラスタ内のすべての対象サーバに依存関係の変更を反映します。
- [リソース依存関係の削除](#): リソースの依存関係を削除して、クラスタ内のすべての対象サーバに依存関係の変更を反映します。
- [In Service](#): リソース階層を特定のサーバで In Service にします。
- [Out of Service](#): リソース階層を特定のサーバで Out of Service にします。

- [プロパティの表示](#) / [プロパティの編集](#): 特定のサーバでリソース階層のプロパティを表示または編集します。

このセクションの残りの部分では、LifeKeeper GUI の [Edit] メニューから作業を選択することによって、Recovery Kit を設定する方法を説明します。設定作業はツールバーから選択することもできます。

- 状況表示ウィンドウのリソース階層ツリー (左側のペイン) のグローバルリソースを右クリックすると、[Edit] メニューと同じドロップダウンメニューの選択項目が表示されます。これは階層がすでに存在している場合にだけ可能な方法です。
- 状況表示ウィンドウのリソース階層表 (右側のペイン) のリソースインスタンスを右クリックすると、サーバおよび特定リソースの状況に応じて、リソース階層の作成を除くすべての設定作業を実行できます。

Recovery Kit for EC2 のチューニング

Recovery Kit for EC2 で設定可能なパラメータは[パラメーター一覧](#)を参照してください。

リソース階層の作成

プライマリサーバからリソースインスタンスを作成するには、以下の手順を完了する必要があります。

1. LifeKeeper GUI メニューから **[Edit]** を選択し、次に **[Server]** を選択してください。ドロップダウンメニューから、**[Create Resource Hierarchy]** を選択してください。
2. ダイアログボックスが表示され、クラスタ内にインストール済みの認識されている Recovery Kit がすべて、ドロップダウンリストボックスに表示されます。ドロップダウンリストから **[Amazon EC2]** を選択し、**[Next]** をクリックしてください。
3. 以下の情報を入力するようにプロンプトが表示されます。(ダイアログボックスで [Back] ボタンが有効な場合は、前のダイアログボックスに戻ることができます。これは、以前に入力した情報を訂正する必要がある場合に特に役立ちます。)

注記: 階層作成の途中で [Cancel] ボタンをクリックすると、作成処理全体が取り消されます。

フィールド	ヒント
Switchback Type	<p>フェイルオーバー後にサーバが復帰したときに、このサーバに EC2 インスタンスを戻す方法を指定します。[intelligent] または [automatic] を選択できます。</p> <ul style="list-style-type: none"> • [intelligent] の場合、インスタンスをプライマリ/オリジナルサーバにスイッチバックするときに管理者の介入が必要になります。 • [automatic] の場合、プライマリサーバがオンラインに戻り、LifeKeeper コミュニケーションパスを再確立した直後に自動的にスイッチバックが行われます。 <p>注記: スイッチバックタイプは、必要な場合、[Resource Properties] ダイアログボックスの [General] タブで後から変更できます。</p>

リソース階層の作成

フィールド	ヒント
Server	[Server] で EC2 リソースの作成先のサーバ(通常、これをプライマリサーバまたはテンプレートサーバと呼ぶ)を選択します。クラスタ内のすべてのサーバがドロップダウンリストに表示されます。
EC2 Region	EC2 インスタンスが配置されているリージョン名を入力してください。
EC2 Resource type	EC2 Recovery Kit は、ルートテーブルと Elastic IP という 2 通りの AWS リカバリーシナリオに対する保護を提供します。 ルートテーブルシナリオはローカル仮想 IP アドレスと組み合わせて使用し、通常はバックエンドクラスタに使用します。 Elastic IP シナリオは Elastic IP の保護に使用し、通常はフロントエンドクラスタに使用します。 使用する EC2 タイプを選択してください。
IP resource	このフィールドは、ルートテーブルシナリオでのみ表示され設定されます。IP リソースを選択してください。これは LifeKeeper が保護する仮想 IP アドレスであり、VPC のルートテーブルアドレスで設定されます。 注記: リストには ISP および IPv4 ベースの IP リソースのみが表示されます。
Network Interface	このフィールドは、Elastic IP シナリオでのみ表示され設定されます。Elastic IP に関連付けるネットワークインターフェースを選択してください。
Elastic IP	このフィールドは、Elastic IP シナリオでのみ表示され設定されます。ネットワークインターフェースに関連付ける Elastic IP を選択してください。
EC2 Resource Tag	作成している EC2 リソースインスタンスに固有の EC2 リソースタグ名を選択または入力します。このフィールドには、デフォルトのタグ名である ec2-<resource> が自動的に表示されます。<resource> はリソース名です。このタグは、後から変更できます。

- [Create] をクリックしてください。[Create Resource Wizard] によって、EC2 リソースが作成されます。
- この時点で情報ボックスが表示され、LifeKeeper は、EC2 リソース階層を作成するために有効なデータが指定されたかどうかを検証します。LifeKeeper が問題を検知した場合は、情報ボックスにエラーが表示されます。検証が正常に完了すると、リソースが作成されます。**[Next]** をクリックしてください。

EC2 リソース階層が正常に作成されたことを示す情報ボックスが表示されます。リソース階層を LifeKeeper で保護するには、クラスタ内の別のサーバにそのリソース階層を拡張する必要があります。

[Continue] をクリックすると、[Pre-Extend configuration task] が起動されます。リソース階層を別のサーバに拡張する方法の詳細については、[リソース階層の拡張](#)を参照してください。

ここで **[Cancel]** をクリックすると、別のダイアログボックスが表示され、後で EC2 リソース階層を別のサーバに手動で拡張して LifeKeeper の保護下に置く必要があることが警告されます。

リソース階層の削除

LifeKeeper 環境のすべてのサーバからリソース階層を削除するには、次の手順を実行してください。

1. LifeKeeper GUI メニューから **[Edit]** を選択し、次に **[Resource]** を選択してください。ドロップダウンメニューから **[Delete Resource Hierarchy]** を選択してください。

2. EC2 リソース階層から削除するターゲットサーバの名前を選択し、**[Next]** をクリックしてください。

注記: このダイアログボックスは、いずれかのペインでリソースインスタンスを右クリックして **[Delete Resource]** を選択した場合には、表示されません。

3. **[Hierarchy to Delete]** を選択してください。削除するリソース階層を指定して強調表示にしてから、**[Next]** をクリックしてください。

注記: このダイアログボックスは、左右どちらかのインでリソースインスタンスを右クリックして **[Delete Resource]** を選択した場合には、表示されません。

4. 選択したターゲットサーバと、削除の対象として選択した階層を確認する情報ボックスが表示されます。**[Delete]** をクリックして次に進んでください。

5. EC2 リソースが正常に削除されたことを確認する情報ボックスが表示されます。

6. **[Done]** をクリックして終了してください。

リソース階層の拡張

階層の作成後、クラスタ内の別のサーバに拡張する必要があります。3通りのシナリオで、テンプレートサーバからターゲットサーバにリソースインスタンスを拡張できます。

- リソースの作成後、**[Continue]** をクリックして、別のサーバにリソースを拡張します。
- 次に説明するように **[Edit]** メニューから **[Extend Resource Hierarchy]** を選択します。
- 左側または右側のペインから拡張されていない階層を右クリックします。

どのシナリオでも同じダイアログボックスが表示されます(いくつかの例外については、以下に詳細を明記)。

1. LifeKeeperGUI メニューから **[Extend]** ウィザードを開始する場合は、**[Edit]** を選択し、次に **[Resource]** を選択します。ドロップダウンメニューから **[Extend Resource Hierarchy]** を選択します。これで **[Extend Resource Hierarchy]** ウィザードが起動されます。拡張操作に慣れていない場合は、**[Next]** をクリックします。LifeKeeper の **[Extend Resource Hierarchy]** のデフォルト値が分かっている、入力と確認を省略する場合は **[Accept Defaults]** をクリックします。

2. **[Pre-Extend Wizard]** で以下の情報を入力します。

注記: 最初の2つのフィールドは **[Edit]** メニューの **[Extend]** から操作を開始した場合にだけ表示されます。階層を拡張する手順の間に **[Cancel]** をクリックすると、どの時点であってもそのサーバへ

の拡張処理がキャンセルされるので注意してください。ただし、すでにリソースを別のサーバに拡張している場合は、明示的に拡張解除するまで、そのインスタンスの拡張は有効です。

フィールド	ヒント
スイッチバックタイプ	<p>スイッチバックタイプを選択します。ここでは、バックアップサーバへのフェイルオーバーの後、EC2 インスタンスが In Service に戻ったときに、このサーバに EC2 インスタンスをスイッチバックする方法を指定します。[intelligent] または [automatic] を選択できます。</p> <ul style="list-style-type: none"> intelligent の場合、インスタンスをプライマリ / オリジナルサーバにスイッチバックするときに管理者の介入が必要になります。 automatic の場合、プライマリサーバがオンラインに戻り、LifeKeeper コミュニケーションパスを再確立した直後に自動的にスイッチバックが行われます。スイッチバックタイプは、必要な場合 [Resource Properties] ダイアログボックスの [General] タブで後から変更できます。
Template Priority	<p>テンプレートの優先順位を選択するか、入力してください。これはサーバで現在 In Service の EC2 階層の優先順位です。1 ~ 999 の範囲で、まだ優先順位として使用されていない値が有効で、小さい数値ほど優先順位が高くなります (数値 1 が最高の優先順位)。拡張処理時に、別のシステムですでに使用中の優先順位をこの階層に対して指定することはできません。デフォルト値を使用することを推奨します。 注記: このフィールドは、階層を最初に拡張するときに表示されます。</p>
Target Priority	<p>ターゲットの優先順位を選択するか、入力してください。これは、他のサーバにある同等の階層に対する、新しく拡張する EC2 階層の優先順位です。1 ~ 999 の範囲で、まだ優先順位として使用されていない値が有効で、リソースのカスケードイングフェイルオーバーシナリオにおけるサーバの優先順位を示します。数値が小さいほど優先順位が高くなります (数値 1 が最高の優先順位)。 注記: LifeKeeper のデフォルトでは、階層が作成されたサーバに「1」が割り当てられます。優先順位は連続している必要はありませんが、特定のリソースについて 2 つのサーバに同じ優先順位を割り当てることはできません。</p>

- 情報ボックスが表示され、LifeKeeper が環境のチェックを正常に完了し、この EC2 リソースを拡張するためのすべての要件が満たされていることが示されます。満たされていない要件がある場合は、**[Next]** ボタンは選択できなくなり、**[Back]** ボタンが有効になります。**[Back]** をクリックした場合、情報ボックスに表示されるエラーメッセージの内容に従って、リソースの拡張を変更できます。ここで **[Cancel]** をクリックした場合は、EC2 リソース階層を他のサーバに手動で拡張して、LifeKeeper の保護下に置く必要があります。**[Next]** をクリックすると、[Extend Resource Hierarchy] 設定作業に入ります。
- リソース階層構造の拡張を行うために、以下の情報の入力が必要です。

フィールド	ヒント
EC2 Resource Tag	<p>EC2 リソースタグを選択するか、入力してください。これは、ターゲットサーバに拡張される EC2 リソースが使用するリソースタグ名です。 注記: このフィールドは編集できません。</p>

5. 拡張が実行中であることを示す情報ボックスが表示されます。同じ EC2 リソースインスタンスをクラスタ内の別のサーバに拡張する場合は、**[Next Server]** をクリックしてください。その場合は、リソース階層を拡張する操作を繰り返します。**[Finish]** をクリックすると、LifeKeeper は EC2 リソースの拡張が正常に完了したことを確認します。
6. **[Done]** をクリックして、**[Extend Resources Hierarchy]** メニューの選択を終了します。

注記: 必ずすべてのサーバで新しいインスタンスの機能をテストしてください。

ローカルリカバリと設定に関する考慮事項

ローカルリカバリシナリオ (バックエンドクラスタ):

保護されているルートテーブルの障害が Recovery Kit for EC2 によって検出されると、結果として生じる障害によって EC2 ローカルリカバリスクリプトが起動されます。ローカルリカバリでは、すべてのルートテーブル内から指定された IP リソースエントリを収集し、そのエントリのターゲットをアクティブなサーバ上にある ENI に変更します。ローカルリカバリの試みが失敗すると、LifeKeeper は EC2 リソース、および依存関係を持つすべてのリソースをスタンバイサーバにフェイルオーバーします。このシナリオの設定については、[運用の原則](#) セクションを参照してください。

注記: 対応する EC2 リソースが作成されると、Recovery Kit がルートテーブルの設定を保護するので、ルートテーブルを手動で変更しないでください。

以下の例で、典型的なローカルリカバリのシナリオを示します。Recovery Kit が、ルートテーブル内にある IP ルートのターゲット設定が正しくないことを検出すると、ローカルリカバリにより、アクティブなサーバ上の ENI にターゲットが置換されます。このプロセスでは、ルートテーブル B の 10.1.0.20/32 のエントリは何も変更されません。

IP リソース	10.1.0.10
アクティブなノード上の ENI	eni-01234567

ルートテーブル A - 前の状態

接続先	ターゲット
10.1.0.10/32	eni-89abcdef
10.0.0.0/16	ローカル

ルートテーブル A - 後の状態

接続先	ターゲット
10.1.0.10/32	eni-01234567
10.0.0.0/16	ローカル

ルートテーブル B - 前の状態

接続先	ターゲット
10.1.0.10/32	eni-89abcdef
10.1.0.20/32	eni-89abcdef
10.0.0.0/16	ローカル

ルートテーブル B - 後の状態

接続先	ターゲット
10.1.0.10/32	eni-01234567
10.1.0.20/32	eni-89abcdef
10.0.0.0/16	ローカル

Elastic IP シナリオ (フロントエンド クラスタ):

保護されている Elastic IP の障害が Recovery Kit for EC2 によって検出されると、結果として生じる障害によって EC2 ローカルリカバリスクリプトが起動されます。ローカルリカバリにより、Elastic IP がアクティブなノード上の ENI に割り当てられます。ローカルでリカバリの試みが失敗すると、LifeKeeper は EC2 リソース、および依存関係を持つすべてのリソースをスタンバイサーバにフェイルオーバーします。このシナリオの設定については、[運用の原則](#) セクションを参照してください。

リソース監視と設定に関する考慮事項

ルートテーブルシナリオ (バックエンド クラスタ)

Recovery Kit は AWS CLI を使用して、保護されている IP リソースに VPC 内のクライアントから接続できるようにルートテーブルの設定を監視します。Recovery Kit は、VPC 内のすべてのルートテーブルに対して、IP リソース宛のターゲットがアクティブサーバの ENI に正しく設定されていることを確認します。正しいことが確認されない場合は、Recovery Kit が EC2 のローカルリカバリプロセスを実行します。

Elastic IP シナリオ (フロントエンド クラスタ):

Recovery Kit は AWS CLI を使用して、Elastic IP とアクティブなサーバ上にある ENI との関連付けを監視します。Recovery Kit は、アクティブサーバに接続されている ENI に Elastic IP が正しく関連付けられていることを確認します。正しいことが確認されない場合は、Recovery Kit が EC2 のローカルリカバリプロセスを実行します。

注記: どちらのシナリオにおいても、AWS CLI でタイムアウトが発生した場合、フェイルオーバーは実行されず、リソースは ISP 状態のままになります。タイムアウト関連のメッセージのみが LifeKeeper ログに記録されます。Recovery Kit はチェック間隔の経過後に監視を再度実行します。タイムアウト値を設定する方法の詳細については、[EC2パラメーター](#) を参照してください。

リソース階層の拡張解除

階層全体を拡張解除するには、以下の手順を実行してください。

1. LifeKeeper GUI メニューから **[Edit]** を選択し、次に **[Resource]** を選択してください。ドロップダウンメニューから **[Unextend Resource Hierarchy]** を選択してください。
2. EC2 リソースから、拡張解除の対象となるターゲットサーバを選択してください。EC2 リソースが現在 In

Service になっているサーバは選択できません。[Next] をクリックしてください。

注記: 右側のペインから個々のリソースインスタンスを右クリックして [Unextend] 作業を選択した場合、このダイアログボックスは表示されません。

3. 拡張解除する EC2 階層を選択してください。[Next] をクリックしてください。

注記: 左側のペインにあるグローバルリソースを右クリックするか、右側のペインにある個々のリソースインスタンスを右クリックして [Unextend] 作業を選択した場合、このダイアログボックスは表示されません。

4. 拡張解除の対象として選択したターゲットサーバと EC2 リソース階層を確認する情報ボックスが表示されます。[Unextend] をクリックしてください。
5. EC2 リソースが正常に拡張解除されたことを示す情報ボックスが表示されます。
6. [Done] をクリックして終了してください。

ユーザシステムのセットアップ

ルートテーブルシナリオ (バックエンドクラスタ)

Recovery Kit for EC2 のルートテーブル保護オプションを使用すると、VPC 内のルートを自動更新することができます。フェイルオーバー中、Recovery Kit はターゲットサーバの仮想 IP アドレスが表す新しい Elastic Network Interface (ENI) の場所を反映するように、ルートテーブルを更新します。LifeKeeper が VPC 内のルートテーブルの保護、監視、および更新を実行できるようにするには、以下の設定手順を実行する必要があります。

- LifeKeeper for Linux IP Recovery Kit で保護する仮想 IP アドレスは、VPC 内の割り当て済み CIDR の範囲外にする必要があります。
- 仮想 IP アドレスを LifeKeeper で保護してから、Recovery Kit for EC2 リソースを作成する必要があります。
- ENI のソース / ターゲットのチェックを無効にする必要があります。これは、インスタンスが仮想 IP アドレスのネットワークパケットを受信するために必要です。
- LifeKeeper IP リソースのブロードキャスト PING チェックを無効にする必要があります。LifeKeeper は、ローカルサブネット上の IP アドレスに対してブロードキャスト PING テストを実行することで、IP リソースを監視します。複数の利用可能ゾーンが存在する環境では、複数の利用可能ゾーンに異なるサブネットが存在するので、この機能は使用できません。この機能を無効にするには、`/etc/default/LifeKeeper` の設定ファイルの NOBCASTPING エントリを以下のように設定する必要があります。

```
NOBCASTPING=1
```

- ルートテーブルには、仮想 IP アドレスおよびアクティブなサーバの ENI のルートエントリが必要です。>

注記:

対応する EC2 リソースが作成されると、Recovery Kit がルートテーブルの設定を保護するので、ルートテーブルを手動で変更しないでください。

例

送信先: VIP 10.1.0.10/32

ターゲット: eni-a2cc76e8

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>	rtb-bbcf11df	3 Subnets	Yes	vpc-74e81110 (10.0.0.0/16) Cluster...

rtb-bbcf11df

Summary Routes Subnet Associations Route Propagation Tags

Edit

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-2e3f674b	Active	No
10.1.0.10/32	eni-a2cc76e8 / i-04c88e3eca15d3493	Active	No

Elastic IP シナリオ (フロントエンドクラスタ)

Recovery Kit for EC2 の Elastic IP (EIP) 保護オプションを使用すると、特定の ENI (アクティブサーバまたはバックアップサーバ上の EC2 が使用する ENI) と EIP の関連付けを再実行できます。

アクティブサーバまたはバックアップサーバ上の ENI と EIP との関連付けについて、LifeKeeper が保護、監視、および更新を実行できるようにするには、以下の設定手順を実行する必要があります。

- 1 つの ENI は、1 つの Elastic IP とのみ関連付けることができます。その他の EIP (EC2 リソースにより使用される EIP を除く、すべての EIP) は、その ENI と関連付けることができません。他の EIP を関連付けると、Recovery Kit はその ENI にすでに関連付けていた他の EIP の関連付けを解除します。

注記:

- AWS の Elastic Block Store (EBS) は 1 つの EC2 インスタンスにのみ接続可能なため、EBS を使用する HA クラスタ構成を作成する際は、DataKeeper for Linux を使用することを推奨します。
- /etc/default/LifeKeeper の RESRVRECTIMEOUT の値を、デフォルト値の 60 から 300 に増加させることを推奨します。RESRVRECTIMEOUT は、別のプロセスがすでにリソースをリザーブしているときに、リソースを「リカバリ」用にリザーブするまで、LifeKeeper プロセスが待機する間スリープ状態になっている秒数です。

既存リソースの IAM ロールへの対応

LifeKeeper 9.2.2 にて、IAM ロールをサポートしました。9.2.1 以前では EC2 リソースや Route53 リソース作成の際に AWS アクセスキー(アクセスキー ID とシークレットアクセスキー)の入力が必要でしたが、要件に記載されたアクセス権限を付与した上でこれらリソースを作成することで、AWS アクセスキーの入力が不要となりました。

LifeKeeper 9.2.1 以前の環境で作成された EC2 リソースや Route53 リソースに関しては、IAM ロール移行ツールを実行することで IAM ロールに対応することが可能です。以前入力された AWS アクセスキーに関する情報は、IAM ロール移行ツール実行時に削除されます。

IAM ロール移行ツール実行手順

IAM ロール移行ツール実行前に、以下の点を確認してください。

- EC2 もしくは Route53 リソースが 9.2.1 以前の LifeKeeper 上で稼働していることを確認してください。
- [要件](#)を参照し、適切なアクセス権限が付与されていることを確認してください。
- [要件](#)を参照し、AWS CLI をインストールしてください。

上記を確認し、問題がなければ以下の手順で IAM ロール移行ツールを実行します。

1. 待機系にて以下の手順を実行してください。

1. EC2、Route53 リソースを全ノード上で停止させてください。
2. [SPS のアップグレード](#)なども参照し、LifeKeeper を 9.2.2 以降にアップグレードしてください。
3. アップグレード後、LifeKeeper は実行中、EC2、Route53 リソースは停止中であることを確認してください。
4. IAM ロール移行ツールを以下のように引数なしで実行してください。


```
/opt/LifeKeeper/lkadm/bin/aws_iam_migration
```
5. /var/log/lifekeeper.log にエラーメッセージが出力されていないことを確認してください。

2. 次に稼働系にて以下の手順を実行してください。

1. EC2、Route53 リソースを全ノード上で停止していることを確認してください。それ以外のリソースは停止させるか待機系にスイッチオーバーしてください。
2. [SPS のアップグレード](#)なども参照し、LifeKeeper を 9.2.2 以降にアップグレードしてください。
3. アップグレード後、LifeKeeper は実行中、EC2、Route53 リソースは停止中であることを確認してください。
4. IAM ロール移行ツールを以下のように引数なしで実行してください。


```
/opt/LifeKeeper/lkadm/bin/aws_iam_migration
```

移行確認テスト

5. /var/log/lifekeeper.log にエラーメッセージが出力されていないことを確認してください。
6. 必要に応じてリソースを起動してください。

以上でIAM ロールへの移行は完了です。

移行確認テスト

EC2、Route53リソースの移行ツール実施後、正しく移行できたかを以下の手順でテストすることができます。

1. 稼働系にてEC2、Route53リソースと、それらに依存するIPリソースとを起動してください。
2. IPリソースが保護しているIPアドレスに対し ping などで正しく通信が行えることを確認してください。
3. EC2、Route53リソースと、それらに依存するIPリソースとを待機系にスイッチオーバーしてください。
4. IPリソースが保護しているIPアドレスに対し ping などで正しく通信が行えることを確認してください。

以上が問題なく実施できれば、EC2、Route53リソースの移行は正しく完了しています。

[メッセージカタログ](#)は、SIOS Protection Suite for Linux の使用時に検出されるすべてのメッセージのリストを示すとともに、適宜、エラーの原因とエラー状態を解決するために必要な処置の説明を提供します。受け取ったエラーコードをこのリストから探すことができます。また、Recovery Kit for EC2 の使用時に検出されるすべてのメッセージがリストされた [Recovery Kit for EC2 メッセージカタログ](#)に直接アクセスすることもできます。