



SIOS Protection Suite for Linux v9.3.1
AWS Direct Connect 接続クイックスタートガイド

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、許可なき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有します。LifeKeeper、SIOS、および SIOS 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.

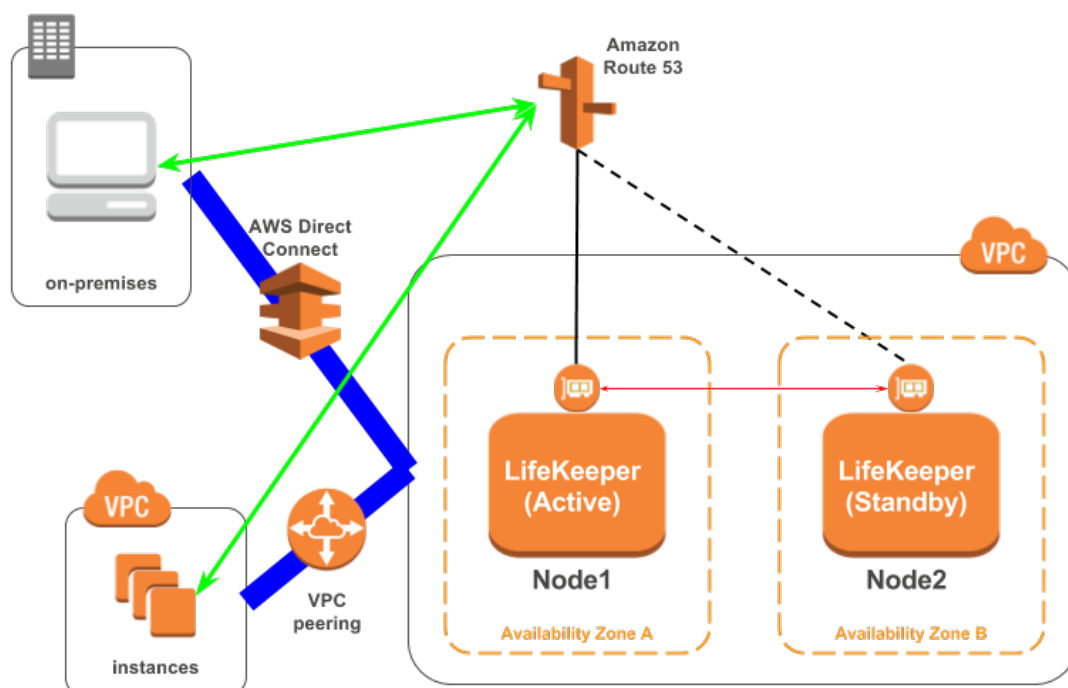
All rights reserved

目次

1. 本資料の目的.....	4
2. 利用のための必要要件	7
2-1 AWS 環境の要件	7
2-2 LifeKeeper ソフトウェアの要件.....	9
2-3 その他.....	9
3. 構築手順	10
3-1 準備	10
3-2 IP リソース作成	11
3-3 Route53 リソース作成	11
3-4 保護するサービスのリソース作成	11
4. 関連する LifeKeeper リソースについて	12
4-1 Route53 リソース.....	12
4-2 IP リソース.....	12
5. 本構成における設定および運用上の留意点	13
5-1 LifeKeeper I-O フェンシングの利用を検討してください	13
6. 既知の問題とトラブルシューティング	14

1. 本資料の目的

LifeKeeper for Linux v9.2 より、AWS Direct Connect を利用したオンプレミス環境から Amazon VPC 内の HA クラスターノードへの接続構成がサポートされました。また、VPC ピア接続を利用した別 VPC からの接続構成もサポートされます。これにより、VPC 内の LifeKeeper で保護されたサービスを、オンプレミス環境や別 VPC から利用することができます。



本資料は、LifeKeeper for Linux v9.3.1 で VPC 外からの接続構成を構築するための要件や基本操作を解説するものです。

既存の Recovery Kit for EC2 を利用しても、AWS 環境における HA クラスターを構築することができます。しかし、以下の問題があり、AWS Direct Connect を利用したオンプレミス環境からの接続はできません。

Recovery Kit for EC2 には「ルートテーブルシナリオ」と「Elastic IP シナリオ」の 2つの機能をサポートします。

「ルートテーブルシナリオ」では、アクティブな IP リソースにルーティングされるように VPC のルートテーブルを制御しています。この時、IP リソースのアドレスは、VPC で管理している CIDR ブロック外である必要があります。しかし、オンプレミス環境から AWS Direct Connect 経由で接続するためには、VPC CIDR ブロック内のアドレスである必要があります。従って、ルートテーブルシナリオではオンプレミス環境からの接続はできません。

「Elastic IP シナリオ」では、Elastic IP アドレスがパブリックなアドレスであるため、インターネットからアクセスが可能であるケースで利用します。オンプレミス環境からのアクセスはインターネットを経由して行うことが可能です。この場合は AWS Direct Connect を利用しなくとも、VPC 内の HA クラスタノードにアクセスすることができます。

上記の理由により、Recovery Kit for EC2 では AWS Direct Connect を利用したオンプレミス環境からのアクセスには対応できません。AWS Direct Connect を経由して VPC 内の HA クラスタノードにアクセスする必要がある場合は、本書にてご紹介する構成を適用してください。

なお、本資料は LifeKeeper や Amazon Web Service (以下 AWS) の基本的な設定や操作、技術的な詳細情報を解説するものではありません。本構成の前提となる LifeKeeper や AWS に関する用語・操作・技術情報等につきましては、関連のマニュアルやユーザーサイト等であらかじめご確認ください。

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 \(http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/EC2/index.htm#AWS_IAM_migration.htm\)](http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/EC2/index.htm#AWS_IAM_migration.htm)」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」、「Amazon Route 53」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。

2. 利用のための必要要件

本構成を利用するためには、環境を準備する段階で満たすべきいくつかの要件があります。以下に AWS 環境とその上に作成するインスタンスに関する要件をまとめます。

2-1 AWS 環境の要件

サービスを提供するための基盤となる環境を AWS 上に作成します。本構成を利用するための要件は以下の通りです。

Amazon Virtual Private Cloud (VPC)

- VPC を AWS 内に設定する必要があります。
- 異なる Availability Zone (AZ) に 2 つ以上のサブネットを作成する必要があります。

Amazon Elastic Compute Cloud (EC2)

- インスタンスが 2 つ以上必要です。
- プライマリ用インスタンスとスタンバイ用インスタンスがそれぞれ異なる AZ で起動するように構成する必要があります。
- インスタンスは、Elastic Network Interface (ENI) に接続されます。
- インスタンスは、LifeKeeper のインストール要件を満たす必要があります。
- 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 \(https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/installing.html\)」](https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/installing.html)を参照してください。
- Amazon Route 53 サービスのエンドポイント route53.amazonaws.com にプロトコル HTTPS を使用してアクセスできる必要があります。EC2 および OS の設定を適切に行ってください。

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](#)

(https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html)を設定するか、[AWS CLI の設定](#)

(https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/cli-chap-getting-started.html)を適切に行ってください。

- route53:GetChange
- route53:ListHostedZones
- route53:ChangeResourceRecordSets
- route53:ListResourceRecordSets

Recovery Kit for EC2 をご利用の場合は、以下のアクセス権も必要です。

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

Amazon Route 53

- Amazon Route 53 にドメイン名を登録しサービスを利用できるようにする必要があります。これは Route53 リソース作成時に必要となります。

2-2 LifeKeeper ソフトウェアの要件

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。本構成に必要な Application Recovery Kit (ARK)は以下の通りです。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 \(http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/TechDoc/index.htm\)](http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/TechDoc/index.htm)および [SPS for Linux リリースノート \(http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/ReleaseNotes/index.htm\)](http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/ReleaseNotes/index.htm)を参照してください。

- LifeKeeper IP Recovery Kit
- LifeKeeper Route53 Recovery Kit

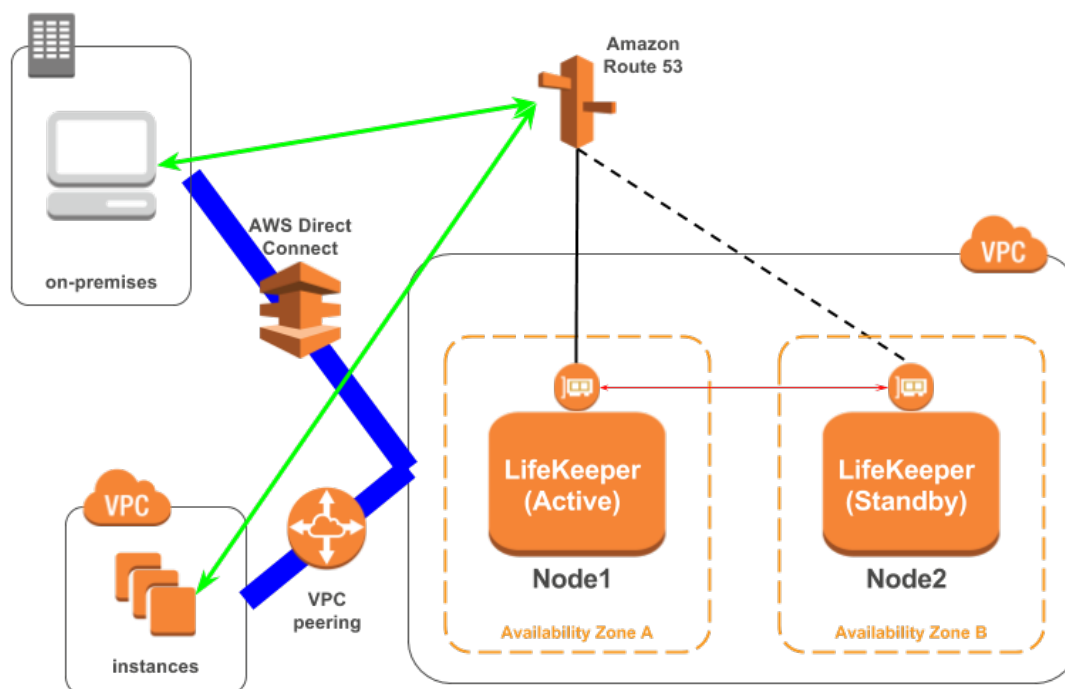
2-3 その他

本構成でオンプレミス環境や別 VPC からサービスを利用するための要件は以下の通りです。

- サービスを利用するクライアントは、Route53 リソースで保護されるホスト名を名前解決できること。
- サービスを利用するクライアントは、Route53 リソースで保護されるホスト名でアクセスすること。

3. 構築手順

以下の構成図の様な環境を構築するための一般的な手順を解説します。



3-1 準備

「[2. 利用のための必要要件](#)」を満たす環境を構築する。それぞれのインスタンスに LifeKeeper をインストールして、Node1 / Node2 間にコミュニケーションパスを作成してください。

オンプレミス環境もしくは別 VPC 環境から Node1 / Node2 に接続された ENI のプライベートアドレスにアクセスできることを確認してください。

Amazon Route 53 でプライベートホストゾーンを使用する場合は、オンプレミス環境からホスト名を解決するために、DNS フォワーダを用意してください。

3-2 IP リソース作成

IP リソースを作成します。ここでは、仮想 IP リソースではなく、実 IP リソース（注記：NIC 用に構成されたプライマリ IP アドレスのためのリソース）を作成します。リソース作成時に、ENI のプライベート IP アドレスを指定してください。また、拡張時も拡張先ノードの ENI プライベート IP アドレスを指定してください。

3-3 Route53 リソース作成

Route53 リソースを作成します。リソース作成時に要求される IP リソースは、[「3-2 IP リソース作成」](#)で作成したリソースを指定してください。

3-4 保護するサービスのリソース作成

保護するサービスのためのリソースを作成してください。リソース作成に IP リソースが要求される場合は、[「3-2 IP リソース作成」](#)で作成したリソースを指定してください。

親リソースが保護するサービスのリソース、子リソースが Route53 リソースとなるようにリソースの依存関係を設定してください。

4. 関連する LifeKeeper リソースについて

4-1 Route53 リソース

動作概要

スイッチオーバーが発生すると、サービスへの接続を継続して確保するために Amazon Route 53 DNS 情報の更新が必要となります。この機能は、Route53 リソースで提供されています。

さらに詳細な情報につきましては、[Route53 Recovery Kit テクニカルドキュメンテーション \(http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/Route53/index.htm\)](http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/Route53/index.htm)をご覧ください。

4-2 IP リソース

動作概要

IP リソースとは、LifeKeeper Core 製品に含まれる IP リカバリキットを使用して生成したリソースです。本構成をサポートするために、実 IP アドレスで IP リソース（実 IP リソース）が生成できるようになりました。これにより、実 IP アドレスを LifeKeeper のリソースとして扱うことができます。

なお、実 IP リソースは、本構成以外では使用しないでください。

さらに詳細な情報につきましては、[IP Recovery Kit テクニカルドキュメンテーション \(http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/IP/index.htm\)](http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/IP/index.htm)をご覧ください。

5. 本構成における設定および運用上の留意点

5-1 LifeKeeper I-O フェンシングの利用を検討してください

AWS 環境では共有ディスク環境が構成できないため、スプリットブレイン問題を防ぐために SCSI リザーブ方式を採ることができません。また、IP リソースも各ノードで異なったアドレスを持った実 IP リソースを利用しますので、スプリットブレインが発生し得ます。

これを踏まえて、本構成ではより安全に運用できるように、LifeKeeper の I/O フェンシング機能の Quorum / Witness Server もしくは STONITH の利用をご検討ください。

特に、Quorum モードの TCP_REMOTE 設定を利用すれば、別途 Quorum サーバを立てずに I/O フェンシング機能を実装できるため、クラウド環境においては利用しやすいと考えられます。利用方法については以下の URL をご確認ください。

[Quorum / Witness](#)

http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/TechDoc/Content/configuration/lifekeeper_io_fencing/quorum_witness.htm

[STONITH](#)

http://jpdocs.us.sios.com/Linux/9.3.1/LK4L/TechDoc/Content/configuration/lifekeeper_io_fencing/stonith.htm

6. 既知の問題とトラブルシューティング

LifeKeeper for Linux v9.3.1 リリース時点での情報はありません。