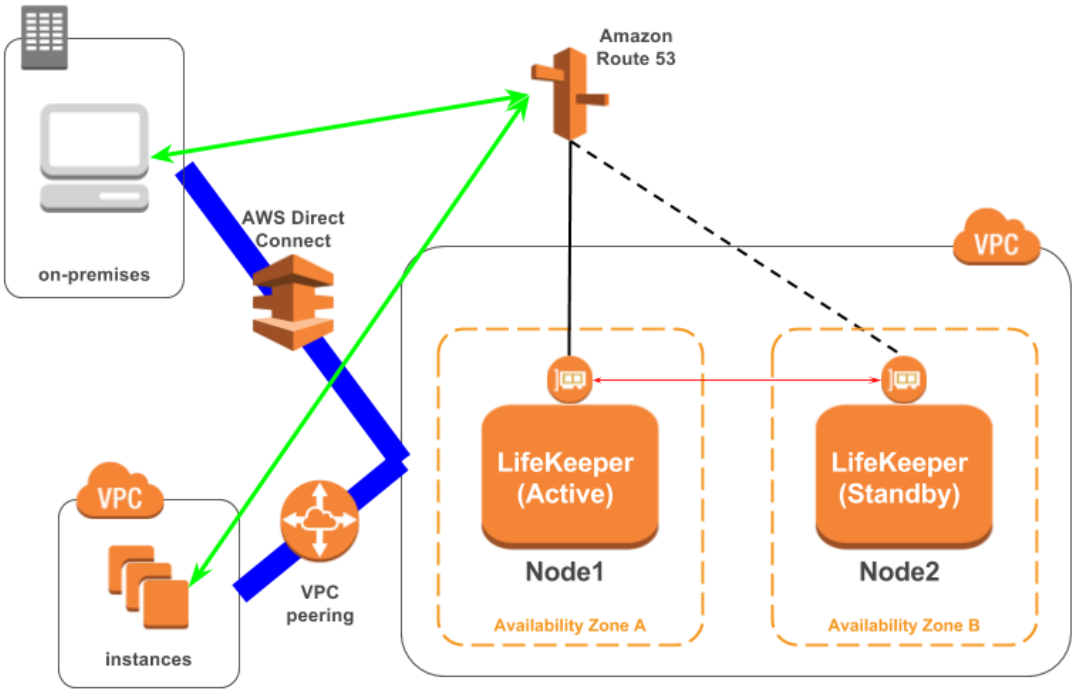
SIOS Protection Suite for Linux v9.2.2
AWS Direct Connect 接続クイックスタートガイド

2018 年 3 月

目次

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 からも利用することができます。



本資料は、LifeKeeper for Linux v9.2.2 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 LifeKeeper9.2.2 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/9.2.2/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)」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。本構成で必要な 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/9.2.2/LK4L/TechDoc/index.htm)および SPS for Linux リリースノート (http://jpdocs.us.sios.com/Linux/9.2.2/LK4L/ReleaseNotes/index.htm)を参照してください。

- LifeKeeper IP Recovery Kit
- LifeKeeper Route53 Recovery Kit

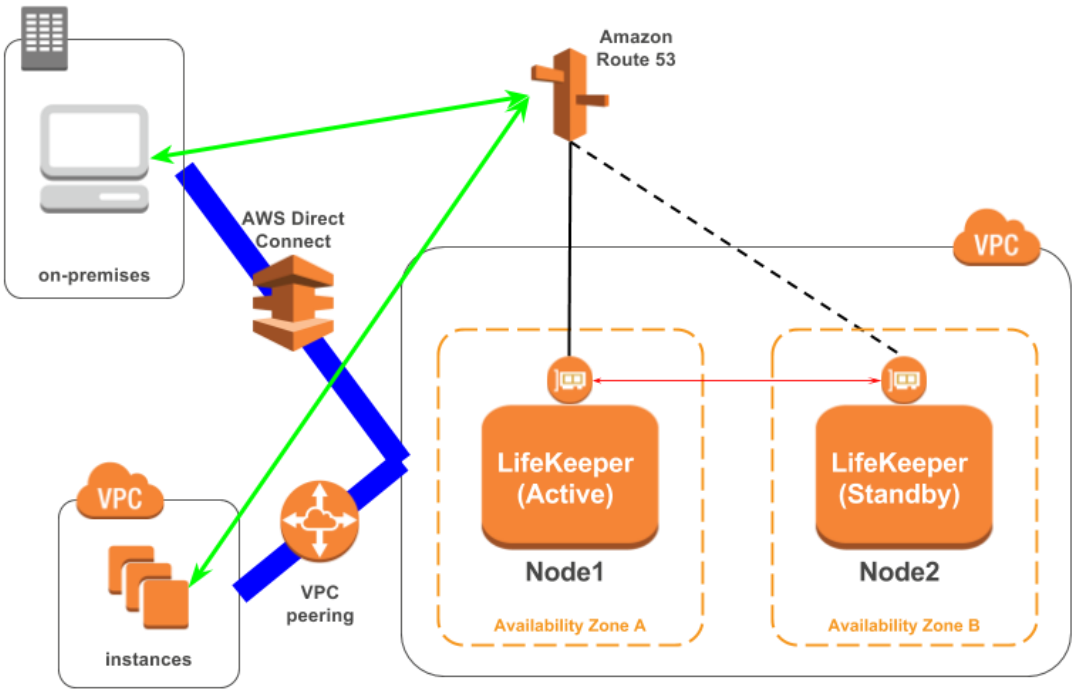
2-3 その他

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、「32 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。

Route53 リソースが In Service されると、依存関係のある IP リソースの IP アドレスを対応する DNS A レコードに API を用いて登録します。

Route53 リソースの監視とリカバリ動作

Route53 リソースは作成時に登録した DNS A レコードの取得と IP リソースとの関連づけの正常性を監視しています。リソースの監視内容として、以下のような処理を行っています。

1. Route 53 の DNS A レコードで設定されているアドレスを API で取得します。取得に失敗した場合は、デフォルトで 2 秒の間隔を置いてから、情報の再取得を行います。 3 回取得を試行して取得できなかった場合、ログに記録を残し監視処理を終了します。
2. Route53 リソースと依存関係がある IP リソースから IP アドレスを取得して、Route53 の DNS A レコードで設定されているアドレスと IP リソースの IP アドレスを比較します。一致した場合、正常であると判断して処理を正常終了します。一致しなかった場合、異常であると判断しリカバリを開始します。

Route53 リソースのチューニング項目

状況に合わせて以下のチューニングを行うことができます。チューニングを行う場合には、両ノードの /etc/default/LifeKeeper ファイルに以下のパラメータを追記します。変更後保存すると、即時その値が有効となります。LifeKeeper や OS の再起動は必要ありません。

パラメータ名	デフォルト値	説明
ROUTE53_TTL	10 (秒)	TTL (Time To Live) (秒)の設定値 ※設定値を反映させるためにはスイッチオーバーさせること
ROUTE53_RECORD_INTERVAL	2 (秒)	A レコード更新時の Route 53 API 通信のインターバル
ROUTE53_RECORD_TRY_COUNT	3 (回)	A レコード更新時の Route 53 API 通信のトライ回数
ROUTE53_CHANGEID_INTERVAL	20 (秒)	Route 53 API 通信のステータス確認時のインターバル
ROUTE53_CHANGEID_TRY_COUNT	5 (回)	Route 53 API 通信のステータス確認時のトライ回数
ROUTE53_RECORDCHECK_INTERVAL	2 (秒)	Route 53 API 通信による A レコード情報取得に要する時間
ROUTE53_RECORDCHECK_TRY_COUNT	4 (回)	A レコードの情報取得時の Route 53 API 通信のトライ回数

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/9.2.2/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、スプレ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/9.2.2/LK4L/TechDoc/Content/configuration/lifekeeper_io_fencing/quorum_witness.htm)
STONITH
(http://jpdocs.us.sios.com/Linux/9.2.2/LK4L/TechDoc/Content/configuration/lifekeeper_io_fencing/stonith.htm)

5-2 Route53 リソース起動にともなうレコードの更新に時間がかかる場合があります

Route53 の DNS レコードの更新の伝播速度に関して、Amazon では以下のような情報を提供しています。

Amazon Route 53 よくある質問

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

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

Route53 リソースでは Route53 API を使用して DNS へのレコード更新の状況について確認しています。INSYNC ステータスを得られた場合には更新が完了したと判断し、PENDING ステータスが帰ってきた場合には、更新状況の確認のリトライを行います。このような仕様のため、Route53 リソースの起動処理としては正しくレコード更新がかけられているにも関わらず、DNS への更新情報の伝播に時間がかかった場合には、Route53 リソースとしては起動失敗の状態になってしまう場合があります。
もし、Route53 リソースの起動に失敗した場合には、Route53 の管理コンソールをみて A レコードが正しく更新されていることを確認してください。更新されている場合、該当する DNS サービスの更新は完了しており、DNS サービスの更新を反映するには、LifeKeeper のみ更新が必要となります。もう一度 LifeKeeper GUI から Route53 リソースを起動してください。
常時前述のようなケースで Route53 リソースの起動ステータスが失敗する場合には、/etc/default/LifeKeeper ファイルの「ROUTE53_CHANGEID_TRY_COUNT」の値をデフォルトの 5 回から 1 ～ 2 回程度値を増やして、状況が改善するかご確認ください。この設定変更には LifeKeeper や OS の再起動は必要ありません。

5-3 DNS レコードの TTL の値を適切に設定してください

スイッチオーバーやフェイルオーバーが発生した後のクライアントからのアクセスは、TTL の設定によって決められた時間が過ぎるまで各クライアントが保持する DNS 情報のキャッシュを用いて行います。そのため、TTL の値が長く設定されている場合、切り替わり前のアドレスへのアクセスが発生する機会が増えることとなり、予期せぬ問題が生じる可能性があります。また、TTL の値が短く設定されている場合、頻繁に名前解決が行われるので、ネットワークへの負荷がかかります。環境に応じて、可能な限り短く TTL の値を設定してください。
TTL の設定は、/etc/default/LifeKeeper ファイルで「ROUTE53_TTL」パラメータを設定してください。単位は秒です。

6. 既知の問題とトラブルシューティング

LifeKeeper for Linux v9.2.2 リリース時点での情報はありません。