SIOS Protection Suite for Linux v9.2.2

AWS Direct Connect Quick Start Guide

March 2018

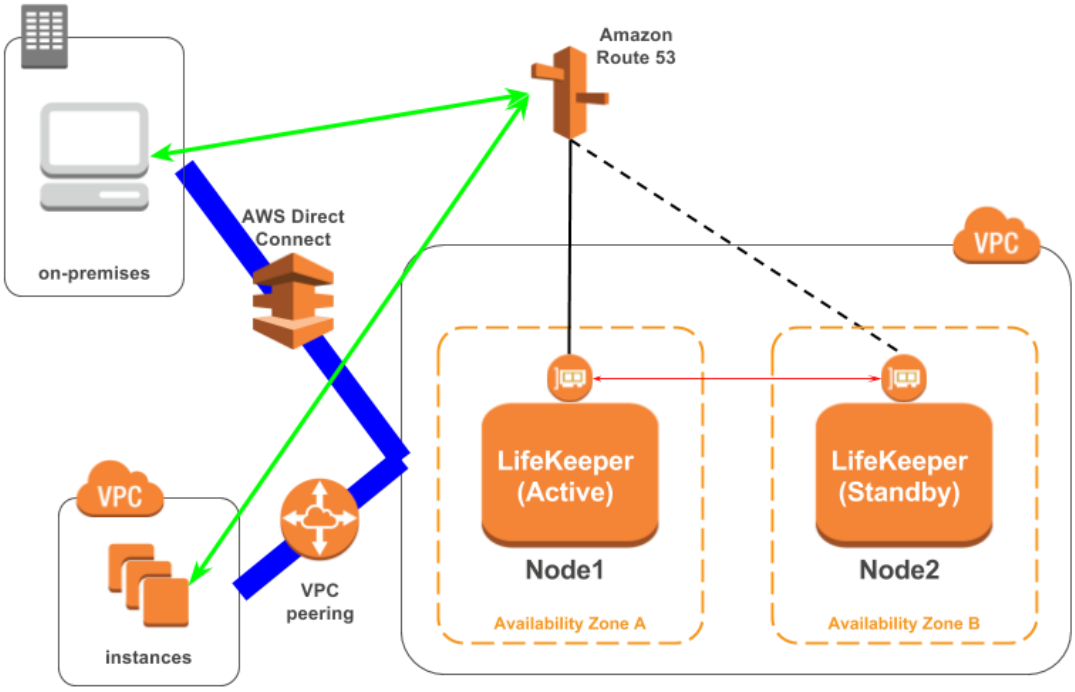
To maintain the quality of our publications, we welcome your comments on the accuracy, clarity, organization, and value of this document.

Address correspondence to:
ip@us.sios.com

Table of Contents

1. Objective

From v9.2, LifeKeeper supports a connection from an on-premises environment using AWS Direct Connect to HA cluster nodes in Amazon VPC. Connection from other VPC through VPC peer connection is also supported. This allows you to use services protected by LifeKeeper in your VPC from your on-premises environment or another VPC.



This document descries the requirements and basic operations for building connections from outside VPC with LifeKeeper for Linux v9.2.2.

You can also build HA clusters in the AWS environment using the existing Recovery Kit for EC 2; however, you cannot connect from your on-premises environment with AWS Direct Connect due to the problems described below.

Recovery Kit for EC2 provides two functions: “Route Tables Scenario” and “Elastic IP Scenario.”

“Route Tables Scenario” manages VPC route tables are configured to be routed to an active IP resources. An address of IP resource should be outside CIDR block which is managed within the VPC. However, the address should be the one within the VPC CIDR block in order to connect from the on-premises environment via AWS Direct Connect. With this route table scenario, you cannot connect to the VPC from the on-premises environment.

“Elastic IP Scenario” can be used where the access from the Internet is available since the elastic IP address is a public address. An access from the on-premises environment is enabled through the Internet. In this case, you can access to HA cluster nodes on VPC without AWS Direct Connect.

For above reasons, Recovery kit for EC2 does not support an access to VPC from on-premises environments using AWS Direct Connect. If you need to access to HA cluster nodes on the VPC via AWS Direct Connect, please use the configuration provided in this document.

Please note that this document does not describe the basic settings, operations, and technical details of LifeKeeper and Amazon Web Service (AWS). For terms, operations and technical information related to LifeKeeper and AWS, that are the prerequisites of this configuration, please read related documents and user websites beforehand.

Note: LifeKeeper 9.2.2 now supports IAM Role. If you upgrade LifeKeeper 9.2.1 or earlier to LifeKeeper 9.2.2 or later, please follow the process described in How to make existing resources support IAM Role(http://docs.us.sios.com/Linux/9.2.2/LK4L/EC2/index.htm#AWS_IAM_Role.htm)

Note: "Amazon Web Services," "Powered by Amazon Web Services" logo, "AWS," "Amazon EC2," "EC2," "Amazon Elastic Compute Cloud," "Amazon Virtual Private Cloud," "Amazon Route 53" and “Amazon VPC" is trademarks of Amazon.com, Inc. or its affiliates in the United States and other countries.

2. Requirements

Some requirements should be met when using this configuration. Below is a summary of requirements for the AWS environment and instances created on it.

2-1 Requirements for AWS environment

Create a base environment on AWS to provide services. The requirements for using this configuration are as follows.

Amazon Virtual Private Cloud (VPC)

- VPC needs to be configured in AWS.
- Need to create more than two subnets in different Availability Zones (AZ).

Amazon Elastic Compute Cloud (EC2)

- At least 2 instances are required.
- A primary instance and a standby instance need to be configured to start with different AZ for each.
- Instances are connected to Elastic Network Interface (ENI).
- Instances are required to satisfy LifeKeeper's installation requirements.
- AWS Command Line Interface (AWS CLI) needs to be installed in each of EC2 the instances. For the details, please refer to "AWS Command Line Interface installation.(https://docs.aws.amazon.com/cli/latest/userguide/installing.html)"
- Instances need to have an access to route53.amazonaws.com with HTTPS protocol. Please configure EC2 and the OS properly.

AWS Identity and Access Management (IAM)

In order for LifeKeeper to operate AWS, IAM user or IAM role with the following access privilege is required. Please configure EC2 IAM role(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html) or configure AWS CLI(https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html) appropriately so that it can be accessed from root user of the EC2 instance.

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

Following access privileges are also required when using Recovery Kit for EC2:

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

Amazon Route 53

- You need to register your domain name on Amazon Route 53 to use the service. This is required to create a Route53 resource.

2-2 LifeKeeper Software Requirements

You need to install the same version of LifeKeeper software and patches on each server. The Application Recovery Kit (ARK) required for this configuration is shown below. For the specific LifeKeeper requirements, please refer to: SPS for Linux Technical Documentation (http://docs.us.sios.com/Linux/9.2.2/LK4L/TechDoc/index.htm) and SPS for Linux Release Notes (http://docs.us.sios.com/Linux/9.2.2/LK4L/ReleaseNotes/index.htm).

- LifeKeeper IP Recovery Kit
- LifeKeeper Route53 Recovery Kit

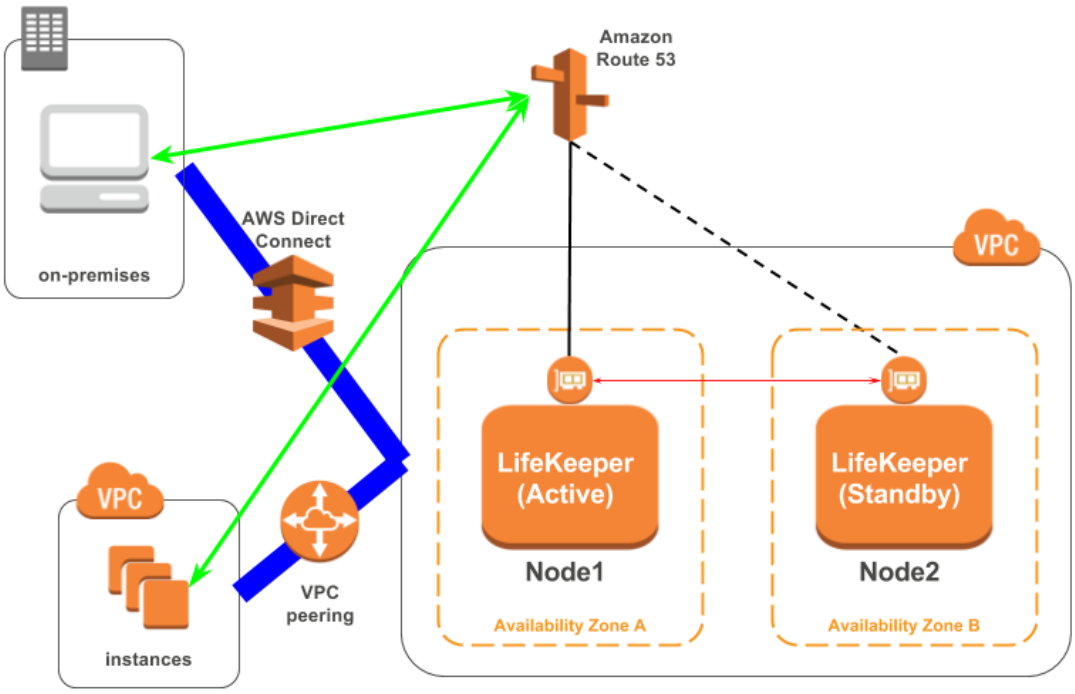
2-3 Others

Requirements for using this service from your on-premises environment or other VPCs are as follows:

- Clients using the service should be able to resolve names of the hosts that are protected by Route53 resources.
- Clients using the service should access with the host name protected by Route53 resource.

3. Setup Procedure

In this section, a general procedure to setup the environment shown as the figure below.



3-1 Preparations

Create an environment that satisfies "2. Requirements". Please install LifeKeeper on each instance and create a communication path between Node1 and Node2.

Please confirm that you can access from your on-premises environment or other VPC environment to ENI's private address connected to Node1/Node2.

If you use Private Hosted Zones with Amazon Route 53, configure a DNS forwarder to resolve a host name from the on-premises environment.

3-2 Creating IP Resource

Create an IP resource: not a virtual IP resources but a real IP resource (Note: resource for a primary IP address configured for NIC).

Please specify ENI private IP address when creating a resource. Also, specify ENI private IP address for an extension target node when extending.

3-3 Creating Route53 Resource

Create Route53 resource. Please specify the IP resource created in "3-2 Creating IP Resources" if required when creating Route53 resource.

3-4 Creating Resources for Protected Services

Create resources for protected services. Please specify the IP resource created in "3-2 Creating IP Resources" if required when creating resources.

Also, please create a resource dependency to enable the resources of the services protected by the parent resource and the child resource to become Route53 resources.

4. Related LifeKeeper Resources

4-1 Route53 Resource

Summary

When switchover occurs, it is necessary to update Amazon Route 53 DNS information in order to continue to secure the connection to the service. This feature is provided in Route53 resources.

When the status of Route53 resource becomes “In Service,” the IP address of the IP resource with a dependency is registered in the corresponding DNS A record using API.

Monitoring of Route53 resource and recovery

Route53 resource monitors the normality of an acquisition of DNS A record which was registered at the time of creation and the relation with the IP resource. Route53 resource performs following processes:

1. Obtain the address specified in DNS A record of Route 53 using API. If it fails, it will try to obtain the information again after the 2 seconds interval by default. When the information cannot be obtained after attempting for 3 times, it leaves a log and end the monitoring process.
2. Obtain the IP address from the IP resource that has a dependency with Route 53 resource and compare the IP address of the IP resource with the address set in DNS A record of Route 53. If they match, the process ends normally. If they do not match, it is regarded as abnormal and a recovery process is started.

Tuning of Route53 Resource

You can perform the following tunings if necessary. When you perform the tuning, please add the parameters below to /etc/default/LifeKeeper on both nodes. The entered values become effective immediately after saving changes and a restart of LifeKeeper and the operating system is not required.

Parameter	Default value	Description
ROUTE53_TTL	10 (sec)	Setting value of TTL (Time To Live) (seconds) *Switchover is required to reflect the setting value
ROUTE53_RECORD_INTERVAL	2 (sec)	Interval of Route 53 API communication when updating A record
ROUTE53_RECORD_TRY_COUNT	3 (times)	Number of trials of Route 53 API communication when updating A record
ROUTE53_CHANGEID_INTERVAL	20 (sec)	Interval of Route 53 API communication when checking a status
ROUTE53_CHANGEID_TRY_COUNT	5 (times)	Number of trials of Route 53 API communication when checking a status
ROUTE53_RECORDCHECK_INTERVAL	2 (sec)	Time required for Route 53 API communication to obtain A record information
ROUTE53_RECORDCHECK_TRY_COUNT	4 (times)	Number of trials of Route 53 API communication when obtaining A record information

4-2 IP Resource

Summary

IP resource is a resource generated with using IP Recovery Kit included in the LifeKeeper Core product. In order to support this configuration, it is now possible to generate IP resource (real IP resource) with a real IP address. This allows you to use real IP addresses as a LifeKeeper resource.

Please do not use the real IP resource except for this configuration.

For more information, please refer to: IP Recovery Kit Technical Documentation (http://docs.us.sios.com/Linux/9.2.2/LK4L/IP/index.htm).

5. Considerations for Settings and Operations in This Configuration

5-1 Considering the use of LifeKeeper I-O Fencing

Since the shared disk environment cannot be used in AWS environment, you cannot use SCSI reservations to prevent a split-brain. Also, IP resource may cause the split-brain as it uses the real IP resource with different IP addresses for each node.

For this reason, please consider the use of Quorum/Witness server or STONITH, an I/O fencing function of LifeKeeper to use this configuration safely.

Especially, because you can implement I/O fencing function separately without the Quorum server if you use the TCP_REMOTE setting in Quorum mode, it is easy to be implemented in the cloud environment. For more details, please refer to the following URLs:

Quorum/Witness
(http://docs.us.sios.com/Linux/9.2.2/LK4L/TechDoc/Content/configuration/lifekeeper_io_fencing/quorum_witness.htm)
STONITH
(http://docs.us.sios.com/Linux/9.2.2/LK4L/TechDoc/Content/configuration/lifekeeper_io_fencing/stonith.htm)

5-2 Updating the record associated with the startup of Route53 resource may take time

Amazon provides following information regarding how quickly the changes to DNS records on Route 53 are propagated.

Amazon Route 53 FAQ

Q: How quickly will changes I make to my DNS settings on Amazon Route 53 propagate globally?
https://aws.amazon.com/route53/faqs/?nc1=h_ls

Route53 resource checks the status of record update to DNS using Route53 API. If the status is INSYNC, Route53 determines that the update has been completed. If the status is PENDING, it checks the update status again. Therefore, Route53 resource may fail to start when it takes longer time to propagate the updated information to DNS even though the record is updated correctly.

If Route53 resource fails to start, check the management console of Route 53 to make sure that A record is properly updated. If it is updated, updating of the corresponding DNS services is completed, and only the update of LifeKeeper is required in order to reflect the update of DNS service. Please start Route53 resource again using LifeKeeper GUI.

If the startup of Route53 resource fails every time, please increase the value of "ROUTE53_CHANGEID_TRY_COUNT" in /etc/default/LifeKeeper to 6 or 7 from the default value 5 to see if it works. This change does not require the restart of LifeKeeper and the operating system.

5-3 Set the TTL value of DNS record appropriately

An access from the client after switchover or failover is done by using DNS information cache held by each client until the time specified in TTL settings passes. Therefore, an access to the address before the switchover increases when a longer value is set for TTL and it may result in unexpected problems. If the shorter value is set for TTL, name resolution is performed frequently, which will put a load on the network. Please set the TTL value as short as possible depending on the environment.

For TTL, please set “ROUTE53_TTL” parameter in seconds in /etc/default/LifeKeeper.

6. Known Issues and Troubleshooting

There is no information at the time of the release of LifeKeeper for Linux v9.2.2