

SIOS Protection Suite for Linux on the AWS Cloud

Quick Start Reference Deployment

September 2018

Last updated: September 2019 (see [revisions](#))

SIOS Technology Corp.

AWS Quick Start Reference Team

Contents

Overview.....	2
Costs and Licenses.....	2
Architecture.....	3
Prerequisites	4
Specialized Knowledge	4
Deployment Options	5
Deployment Steps	5
Step 1. Prepare Your AWS Account.....	5
Step 2. Subscribe to the SIOS Protection Suite for Linux AMI	5
Step 3. Launch the Quick Start	6
Step 4. Test the Deployment	12
Troubleshooting.....	13
GitHub Repository	14
Best Practices	14
Additional Resources	15
Document Revisions	16



This Quick Start deployment guide was created by Amazon Web Services (AWS) in collaboration with APN Advanced Technology Partner SIOS Technology Corp.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying SIOS Protection Suite for Linux on the AWS Cloud. [Quick Starts](#) are automated reference deployments that use AWS CloudFormation templates to launch, configure, and run the AWS compute, network, storage, and other services required to deploy a specific workload on AWS.

SIOS Protection Suite for Linux is a Linux clustering solution that provides a tightly integrated combination of high availability failover clustering, continuous application monitoring, data replication, and configurable recovery policies. SIOS Protection Suite for Linux includes SIOS LifeKeeper, SIOS DataKeeper, and multiple Application Recovery Kits (ARKs) to protect your business-critical applications and data from downtime and disasters.

SIOS Protection Suite for Linux on AWS provides all the elements you need to create a high availability Linux cluster in a virtual private cloud (VPC) within a single AWS Region across two Availability Zones. It also supports out-of-the-box protection for SAP systems, Oracle databases, and other business-critical applications.

This Quick Start is for enterprise users who want to deploy SIOS Protection Suite for Linux on AWS into their test or production environment.

Costs and Licenses

You are responsible for the cost of the AWS services and resources used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

This deployment of SIOS Protection Suite for Linux uses a Bring Your Own License (BYOL) model. You can purchase a [runtime license](#) or request a [14-day free trial license](#).

You also have the option of using a Pay As You Go (PAYG) license model, which installs a basic license. If later you want to upgrade to full functionality, contact sales@us.sios.com.

Architecture

Deploying this Quick Start for a [new virtual private cloud \(VPC\)](#) with **default parameters** builds the following SIOS Protection Suite for Linux environment in the AWS Cloud.

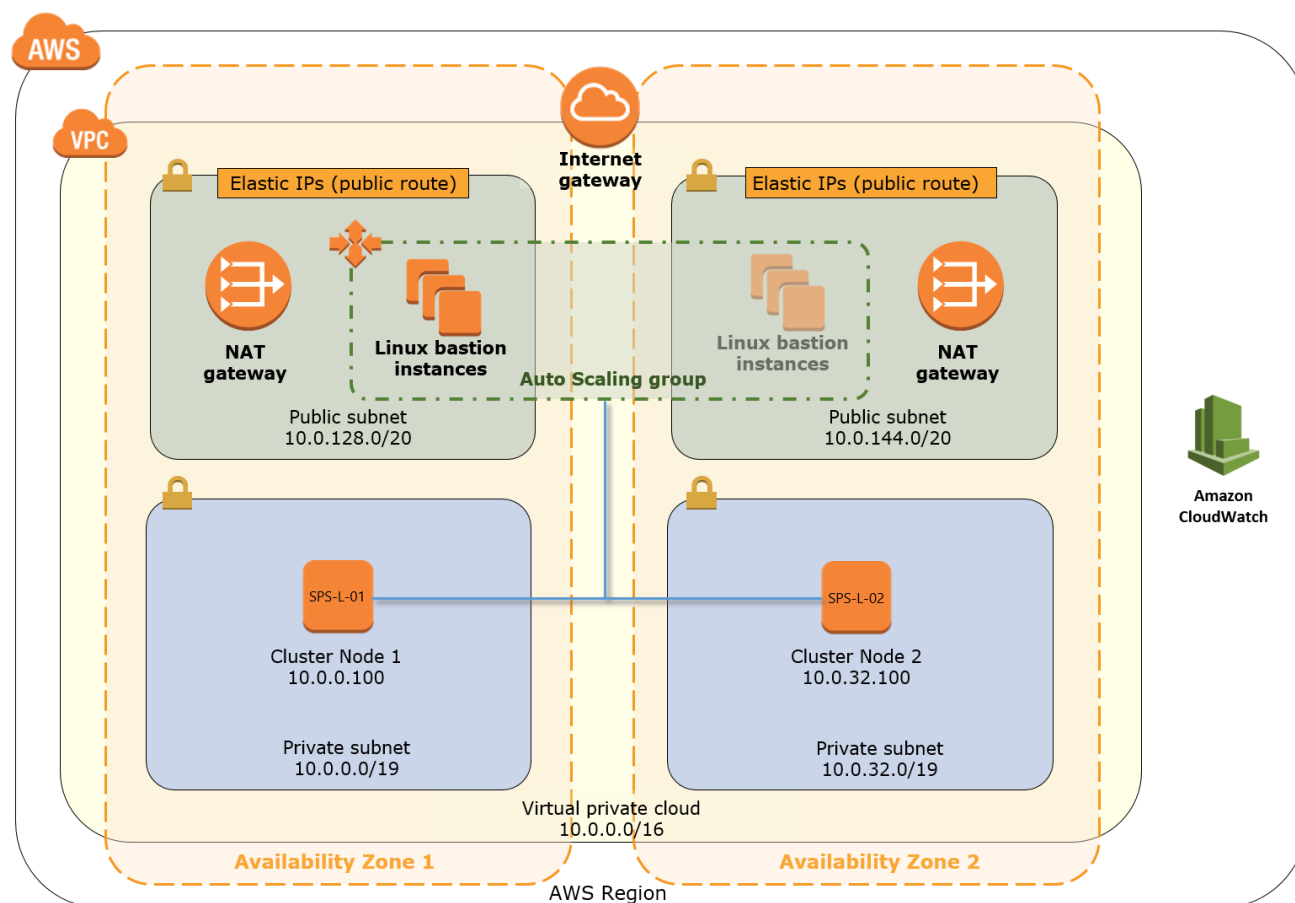


Figure 1: Quick Start architecture for SIOS Protection Suite for Linux architecture on AWS

The Quick Start sets up the following:

- One VPC with associated private and public subnets and security groups across two Availability Zones.
- An internet gateway to allow access to the internet.

- In each public subnet, up to four Linux bastion host instances for remote administration.
- (Optional) In the public subnets, a Remote Desktop Gateway server for remote administration.
- In the public subnets, two network address translation (NAT) gateways to allow outbound internet access for resources in the private subnets (where needed).
- In the private subnets, two cluster nodes featuring SIOS Protection Suite for Linux high availability software.

Technical specifications for the architecture:

Component	Details
VPC	Single AWS Region with two Availability Zones.
Instance type	Minimum recommended instance type: t2.medium.
Operating system	See the SIOS Protection Suite for Linux Support Matrix .
Elastic IP address	One Elastic IP address connected to each bastion host instance (up to four in each public subnet), and one additional Elastic IP address connected to the optional Remote Desktop Gateway server (one total).
Instances	Two instances: two SIOS Protection Suite for Linux cluster nodes.
Volumes	Two volumes (gp2 or io3) per cluster node: • One home volume (/) • One additional volume for replicated data storage

Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see [Getting Started with AWS](#).)

- [Amazon VPC](#)
- [Amazon EC2](#)
- [Amazon EBS](#)
- [Amazon CloudWatch](#)
- [Linux Bastion Hosts on the AWS Cloud](#) (Quick Start Reference Deployment)

We also recommend that you become familiar with [SIOS Protection Suite for Linux](#).

Deployment Options

This Quick Start provides two deployment options:

- **Deployment of SIOS Protection Suite for Linux into a new VPC** (end-to-end deployment) builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, Linux bastion hosts, an optional Remote Desktop Gateway server, and other infrastructure components. It then deploys two SIOS Protection Suite for Linux nodes into this new VPC.
- **Deployment of SIOS Protection Suite for Linux into an existing VPC** provisions two SIOS Protection Suite for Linux nodes and an optional Remote Desktop Gateway server in your existing VPC in AWS.

The Quick Start also lets you configure additional settings such as CIDR blocks, instance types, and SIOS Protection Suite for Linux settings, as discussed later in this guide.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at <https://aws.amazon.com> by following the on-screen instructions.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy SIOS Protection Suite for Linux on AWS.
3. Create a [key pair](#) in your preferred region.
4. If necessary, [request a service limit increase](#) for the Amazon EC2 instance type desired. You might need to do this if you already have an existing deployment that uses this instance type, and you think you might exceed the [default limit](#) with this reference deployment.

Step 2. Subscribe to the SIOS Protection Suite for Linux AMI

1. To use BYOL license model, you must:
 - Sign up for the [14-day free trial](#) for SIOS Protection Suite for Linux.

–or–

 - Request a quote for a runtime license by [contacting SIOS](#) directly.

If instead you want to use a PAYG basic license, you can select PAYG for the AMIType parameter later.

2. Log in to the AWS Marketplace at <https://aws.amazon.com/marketplace>.
3. Open the page for [SIOS Protection Suite for Linux on RHEL 7.4 – BYOL](#), and choose **Continue**.
4. Use the **Manual Launch** option, and then choose **Accept Software Terms**. For detailed instructions, see the [AWS Marketplace documentation](#).

Step 3. Launch the Quick Start

Note You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see [deployment options](#) earlier in this guide.

Option 1	Option 2
Deploy SIOS Protection Suite into a new VPC on AWS	Deploy SIOS Protection Suite into an existing VPC on AWS
Launch	Launch

Important If you're deploying SIOS Protection Suite for Linux into an existing VPC, make sure that your VPC has two private subnets in different Availability Zones. These subnets require NAT gateways or NAT instances in their route tables, to allow the instances to download packages and software without exposing them to the internet. You'll be prompted for your VPC settings when you launch the Quick Start.

End-to-end deployment (option 1) takes about half an hour to complete. Deploying SIOS Protection Suite into an existing VPC (option 2) takes slightly less time to complete.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for SIOS Protection

Suite for Linux will be built. The template is launched in the US East (N. Virginia) Region by default.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

In the following tables, parameters are listed by category and described separately for the two deployment options:

- [Parameters for deploying SIOS Protection Suite into a new VPC](#)
- [Parameters for deploying SIOS Protection Suite into an existing VPC](#)

- **Option 1: Parameters for deploying SIOS Protection Suite for Linux into a new VPC**

[View template](#)

VPC & Bastion Configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	<i>Requires input</i>	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.
Allowed bastion external access CIDR (RemoteAccessCIDR)	<i>Requires input</i>	The CIDR IP range that is permitted to access the SIOS Protection Suite server via the bastion host. We recommend that you set this value to a trusted IP range.
Key pair name (KeyPairName)	<i>Requires input</i>	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Bastion AMI operating system (BastionAMIOS)	Amazon-Linux-HVM	The Linux distribution for the AMI to be used for the bastion instances.
Bastion instance type (BastionInstanceType)	t2.micro	Amazon EC2 instance type for the bastion instances.
Number of bastion hosts (NumBastionHosts)	1	The number of bastion hosts to create.
Global CIDR block for entire VPC (VPCCIDR)	10.0.0.0/16	Global CIDR IP range for entire VPC.

Parameter label (name)	Default	Description
CIDR block for private subnet 1A (PrivateSubnet1CIDR)	10.0.0.0/19	CIDR IP range for the private subnet located in Availability Zone 1.
CIDR block for private subnet 2A (PrivateSubnet2CIDR)	10.0.32.0/19	CIDR IP range for the private subnet located in Availability Zone 2.
CIDR block for public subnet 1 (PublicSubnet1CIDR)	10.0.128.0/20	CIDR IP range for the public (DMZ) subnet located in Availability Zone 1.
CIDR block for public subnet 2 (PublicSubnet2CIDR)	10.0.144.0/20	CIDR IP range for the public (DMZ) subnet located in Availability Zone 2.

SIOS Protection Suite Instance Configuration:

Parameter label (name)	Default	Description
SIOS Protection Suite instance name (SPSL Instance Name Prefix)	SPS-L-	Name prefix for the SIOS Protection Suite servers.
SIOS Protection Suite instance type (SPSLInstanceType)	t2.medium	Amazon EC2 instance type for the SIOS Protection Suite servers.
Home directory volume type (HomeVolumeType)	Provisioned IOPS	Volume type for the home directory.
Home directory size (HomeSize)	25	Storage size for the home directory, in GiB. Allowed range is 25 - 16,384.
Home directory IOPS (HomeIops)	1000	IOPS for the home directory. This value is used only when the Home volume type parameter is set to Provisioned IOPS. Allowed range is 100-20,000. The ratio of IOPS to volume size must be 50 or less. For example, if you set this parameter to 5000 IOPS, the home directory size must be at least 100 GiB.
Delete home on termination (HomeDeleteOnTermination)	true	Delete home directory volume when the SIOS Protection Suite server instance is terminated. Keep the default setting of true to delete the home directory volume when the SIOS Protection Suite server instance is terminated. If the setting is true, you must back up your data before terminating your instance. Set to false to keep the home directory volume upon termination.
Mirror directory volume type (MirrorVolumeType)	Provisioned IOPS	Volume type for the replicated data directory.
Mirror directory size (MirrorSize)	100	Storage size for the replicated volume, in GiB. Allowed range is 100 - 16,384.
Mirror directory IOPS (MirrorIops)	1000	IOPS for the mirror volume. This value is used only when the Mirror Volume Type parameter is set to Provisioned IOPS. Allowed range is 100 - 20,000. The ratio of IOPS to volume size must be 50 or less. For example, if you set this parameter to 5000 IOPS, the home directory size must be at least 100 GiB.

Parameter label (name)	Default	Description
Delete mirror on termination (MirrorDeleteOnTermination)	true	Delete the replicated volume when the SIOS Protection Suite server instance is terminated. Keep the default setting of true to delete the home directory when the instance is terminated. If true, you must back up your data before terminating your instance. Set to false to keep the replicated volume upon termination.
new root password (NewRootPassword)	<i>Requires input</i>	Password for predefined admin user used to administer SIOS Protection Suite (Min. length of 8 Characters, Max. length of 16 Characters).
License model for SIOS AMI (SIOSAMITYPE)	PAYG	SIOS Protection Suite AMI license model to use for cluster nodes. Change this parameter to BYOL if you have a runtime license or a 14-day trial license.
SIOS Protection Suite license URL (SIOSLicenseKeyFtpURL)	<i>Requires input</i>	URL used to obtain license key for SIOS Protection Suite for Linux software.
Node1 private IP address (Node1PrivateIP)	10.0.0.100	Primary private IP address for the cluster node located in Availability Zone 1.
Node2 private IP address (Node2PrivateIP)	10.0.32.100	Primary private IP address for the cluster node located in Availability Zone 2.
Optional Windows jumpbox instance type (WindowsJumpboxInstanceType)	None	Amazon EC2 instance type for an optional Windows jump server.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	aws-quickstart	S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you've created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 key prefix (QSS3KeyPrefix)	quickstart-sios-protection-suite/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes, and should end with a forward slash.

- **Option 2: Parameters for deploying SIOS Protection Suite for Linux into an existing VPC**

[View template](#)

Network Configuration:

Parameter label (name)	Default	Description
VPC ID (VPCID)	<i>Requires input</i>	ID of your existing VPC (e.g., vpc-0343606e).
Private subnet 1 ID (PrivateSubnet1ID)	<i>Requires input</i>	ID of the private subnet in Availability Zone 1 in your existing VPC (e.g., subnet-a0246dcd).
CIDR block for private subnet 1A (PrivateSubnet1CIDR)	10.0.0.0/19	CIDR IP range for the private subnet located in Availability Zone 1.
Private subnet 2 ID (PrivateSubnet2ID)	<i>Requires input</i>	ID of private subnet 2 in Availability Zone 2 for the SIOS Protection Suite instances (e.g., subnet-a0246dcd).
CIDR block for private subnet 2A (PrivateSubnet2CIDR)	10.0.32.0/19	CIDR IP range for the private subnet located in Availability Zone 2.
Public subnet 1 ID (PublicSubnet1ID)	<i>Requires input</i>	ID of public subnet 1 in Availability Zone 1 for the ELB load balancer (e.g., subnet-a0246dcd).
Public subnet 2 ID (PublicSubnet2ID)	<i>Requires input</i>	ID of public subnet 2 in Availability Zone 2 for the ELB load balancer (e.g., subnet-a0246dcd).

Bastion Configuration:

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	<i>Requires input</i>	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Bastion security group ID (BastionSecurityGroupID)	<i>Requires input</i>	ID of the bastion host security group to enable SSH connections (e.g., sg-1a23b456).

SIOS Protection Suite Instance Configuration:

Parameter label (name)	Default	Description
SIOS Protection Suite instance name prefix (SPSLInstanceNamePrefix)	SPS-L-	Name prefix for the SIOS Protection Suite servers.
SIOS Protection Suite instance type (SPSLInstanceType)	t2.medium	Amazon EC2 instance type for the SIOS Protection Suite servers.
Home directory volume type (HomeVolumeType)	Provisioned IOPS	Volume type for the home directory.
Home directory size (HomeSize)	25	Storage size for the home directory, in GiB. Allowed range is 25 - 16,384.

Parameter label (name)	Default	Description
Home directory IOPS (HomeIops)	1000	IOPS for the home directory. This value is used only when the Home volume type parameter is set to Provisioned IOPS. Allowed range is 100-20,000. The ratio of IOPS to volume size must be 50 or less. For example, if you set this parameter to 5000 IOPS, the home directory size must be at least 100 GiB.
Delete home on termination (HomeDeleteOnTermination)	true	Delete home directory volume when the SIOS Protection Suite server instance is terminated. Keep the default setting of true to delete the home directory when the instance is terminated. If true, you must back up your data before terminating your instance. Set to false to keep the home directory volume upon termination.
Mirror directory volume type (MirrorVolumeType)	Provisioned IOPS	Volume type for the replicated data directory.
Mirror directory size (MirrorSize)	100	Storage size for the replicated volume, in GiB. Allowed range is 100 - 16,384.
Mirror directory IOPS (MirrorIops)	1000	IOPS for the mirror volume. This value is used only when the Mirror volume type parameter is set to Provisioned IOPS. Allowed range is 100 - 20,000. The ratio of IOPS to volume size must be 50 or less. For example, if you set this parameter to 5000 IOPS, the home directory size must be at least 100 GiB.
Delete mirror on termination (MirrorDeleteOnTermination)	true	Delete the replicated volume when the SIOS Protection Suite server instance is terminated. Keep the default setting of true to delete the home directory when the instance is terminated. If true, you must back up your data before terminating your instance. Set to false to keep the replicated volume upon termination.
new root password (NewRootPassword)	<i>Requires input</i>	Password for predefined admin user used to administer SIOS Protection Suite (Min. Length of 8 Characters, Max. Length of 16 Characters).
License model for SIOS AMI (SIOSAMITYPE)	PAYG	SIOS Protection Suite AMI license model to use for cluster nodes. Change this parameter to BYOL if you have a runtime license or a 14-day trial license.
SIOS Protection Suite license URL (SIOSLicenseKeyFtpURL)	<i>Requires input</i>	URL used to obtain license key for SIOS Protection Suite for Linux software.
Node1 private IP address (Node1PrivateIP)	10.0.0.100	Primary private IP for the cluster node located in Availability Zone 1.
Node2 private IP address (Node2PrivateIP)	10.0.32.100	Primary private IP for the cluster node located in Availability Zone 2.
Instance type to use for optional Windows jumpbox (WindowsJumpboxInstanceType)	None	Amazon EC2 instance type for an optional Windows jump server.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	aws-quickstart	S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you've created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 key prefix (QSS3KeyPrefix)	quickstart-sios-protection-suite/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes, and should end with a forward slash.

- On the **Options** page, you can [specify tags](#) (key-value pairs) for resources in your stack and [set advanced options](#). When you're done, choose **Next**.
- On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create AWS Identity and Access Management (IAM) resources.
- Choose **Create** to deploy the stack.
- Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the SIOS Protection Suite for Linux cluster is ready.
- Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

Step 4. Test the Deployment

The easiest way to determine whether SIOS Protection Suite for Linux has been correctly deployed and configured is to verify that the full stack has been created successfully, and that the `lxdstatus` command reports that failover is allowed for all resources.

From the AWS Console navigate to the CloudFormation service page. Ensure you have the proper region selected. If any stacks report **CREATE_FAILED**, remedy any errors reported in the Events tab at the bottom of the webpage. Invalid parameter input is the most likely cause for deployment failures. See the [Troubleshooting](#) section of this guide for more details. When all stacks display **CREATE_SUCCESS**, go back to the EC2 service page, and log in to either the bastion host or the optional Windows jump server. Follow the [AWS guidelines](#) for connecting to your instances.

- From the jump server node, use SSH to connect to the instance in the first Availability Zone.

2. Run `sudo /opt/LifeKeeper/bin/lcdstatus`
3. The output should contain two resources (`/opt/sample_mirror`, and `datarep-sample`), and both resources should report **FAILOVER ALLOWED**. Also, two known machines should be listed and reported as **ALIVE**.

```
[ec2-user@SPS-L-01 ~]$ sudo /opt/LifeKeeper/bin/lcdstatus
Resource hierarchies for machine "SPS-L-01":

ROOT of RESOURCE HIERARCHY
/opt/sample_mirror: id=/opt/sample_mirror app=gen type=filesystem state=ISP
  initialize=(AUTORES_ISP) automatic restore to IN-SERVICE by LifeKeeper
  info=xfsrw,relatime,attr2,nobarrier,inode64,noquota0
  depends on resources: datarep-sample
  Local priority = 1
  SHARED equivalency with "/opt/sample_mirror" on "SPS-L-02", priority = 10
  FAILOVER ALLOWED
datarep-sample: id=/dev/xvdca app=scsi type=netraid state=ISP
  initialize=(AUTORES_ISP) automatic restore to IN-SERVICE by LifeKeeper
  info=0/dev/xvdca10.0.32.100104857600DEVNAME0/opt/LifeKeeper/bitmap__opt_sample_mirror256M
  these resources are dependent: /opt/sample_mirror
  Local priority = 1
  SHARED equivalency with "datarep-sample" on "SPS-L-02", priority = 10
  FAILOVER ALLOWED

The following LifeKeeper machines are known:
  machine=SPS-L-01      state=ALIVE
  machine=SPS-L-02      state=ALIVE (events1cm detected restored by 10.0.0.100/10.0.32.100 at Tue Aug 21 17:49:04 UTC 2018)

The following LifeKeeper network connections exist:
  to machine=SPS-L-02  type=TCP  addresses=10.0.0.100/10.0.32.100
  state="ALIVE"  priority=1  #comm_downs=0

The shutdown strategy is set to: do_not_switchover.
[ec2-user@SPS-L-01 ~]$
```

Figure 2: Output of `lcdstatus`, with **FAILOVER ALLOWED and **state=ALIVE****

For further configuration details, see the SIOS Protection Suite for Linux SIOS Protection Suite for Linux [technical documentation](#).

Troubleshooting

Q. I encountered a `CREATE_FAILED` error when I launched the Quick Start. What should I do?

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. You can examine the `/var/log/cfn-init.log` file for details.

Important When you set **Rollback on failure** to **No**, you'll continue to incur AWS charges for this stack. Be sure to delete the stack when you've finished troubleshooting.

For additional information, see [Troubleshooting AWS CloudFormation](#) on the AWS website or contact us on the [AWS Quick Start Discussion Forum](#).

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.

A. We recommend that you launch the Quick Start templates from the location we've provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the [AWS documentation](#).

Q. I encountered problems using SIOS Protection Suite for Linux on AWS.

A. Use the following resources to help troubleshoot issues:

- Check the Troubleshooting sections of the [SIOS Protection Suite for Linux documentation](#).
- If you have a support contract, visit <http://us.sios.com/support/overview/>.
- If you're evaluating the software, email [SIOS pre-sales support](#).

GitHub Repository

You can visit our [GitHub repository](#) to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Best Practices

AWS services

SIOS recommends following AWS best practices for creating and using IAM roles and policies, IAM user credentials and roles, and access key rotation.

- IAM roles
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html
- IAM policies
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html
- IAM users
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_sign-in.html

- Access keys
<https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/>

SIOS Protection Suite for Linux

SIOS also has some recommendations for customers seeking optimal performance. These recommendations include considerations specific to both the Linux operating system and the AWS Cloud configurations.

- Instance size - Performance relies on several factors. While CPU usage is minimal, RAM utilization depends on application performance during peak active workload. The recommended instance size for use with SIOS Protection suite for Linux is t2.medium, but larger instances should be considered based on application workload.
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) - SIOS Protection Suite does not add significantly to a typical cluster single-server outage failover RTO. Assuming appropriate instance sizes are utilized, resource contention is not an issue, SIOS Protection Suite for Linux is properly configured and all resources are in the Online state, and assuming trivial application recovery time, an RTO of <1 minute is possible. Realistically, an RTO of 2–5 minutes should be expected unless the application being protected (MaxDB, SAP, etc.) has an unusually large recovery time.

Assuming the same conditions, RPO should be only a few milliseconds larger than the current network write latency between the active and backup nodes. RPO is dependent on replication software in use. In many cases, the RPO will be measured in milliseconds, but factors like network congestion, abnormally high disk write activity, or slow write performance can impact RPO greatly.

Additional Resources

AWS services

- Amazon EC2
<https://aws.amazon.com/documentation/ec2/>
- AWS CloudFormation
<https://aws.amazon.com/documentation/cloudformation/>
- Amazon VPC
<https://aws.amazon.com/documentation/vpc/>

SIOS Protection Suite for Linux

- SIOS Protection Suite for Linux technical documentation
<http://docs.us.sios.com/Linux/9.2.2/LK4L/AllTechDocs/index.htm>

Quick Start reference deployments

- AWS Quick Start home page
<https://aws.amazon.com/quickstart/>

Document Revisions

Date	Change	In sections
September 2019	Parameter change Advanced Tier Compliance	Step 3 Best Practices
September 2018	Initial publication	—

© 2019, Amazon Web Services, Inc. or its affiliates, and SIOS Technology Corp. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at <http://aws.amazon.com/apache2.0/> or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.