Symantec Protection Engine on the AWS Cloud

Quick Start Reference Deployment

January 2017

Abhijit Ghosh, Atul Ghodke, Ken O'Brien, and Sid Harshavat — Symantec Corporation
Tony Vattathil — AWS Quick Start Reference Team

Contents

This Quick Start deployment guide was created by Amazon Web Services (AWS) in partnership with Symantec Corporation.

Overview

This Quick Start deployment guide provides step-by-step instructions for deploying Symantec Protection Engine (SPE) version 7.5.5 for Cloud Services on the Amazon Web Services (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.

SPE for Cloud Services is a flexible and feature-rich application that allows customers to incorporate malware and threat detection technologies into almost any application. SPE includes Symantec's proprietary, patented URL categorization technology and industry-leading malware protection for fast, scalable, and reliable content scanning services. These services help organizations protect their data and storage systems against the ever-growing malware threat landscape.

SPE supports integration with almost any application by means of the Internet Content Adaptation Protocol (ICAP) and also comes with C, Java, and C# .NET APIs (SDK).

This Quick Start aids integration with proxy applications such as F5 and Squid, and is designed for enterprise administrators who want to scan their ingress/egress traffic for viruses, trojans, and other kinds of malware.

Costs and Licenses

You are responsible for the cost of the AWS services and SPE licenses 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. See the pricing pages for each AWS service you will be using for cost estimates.

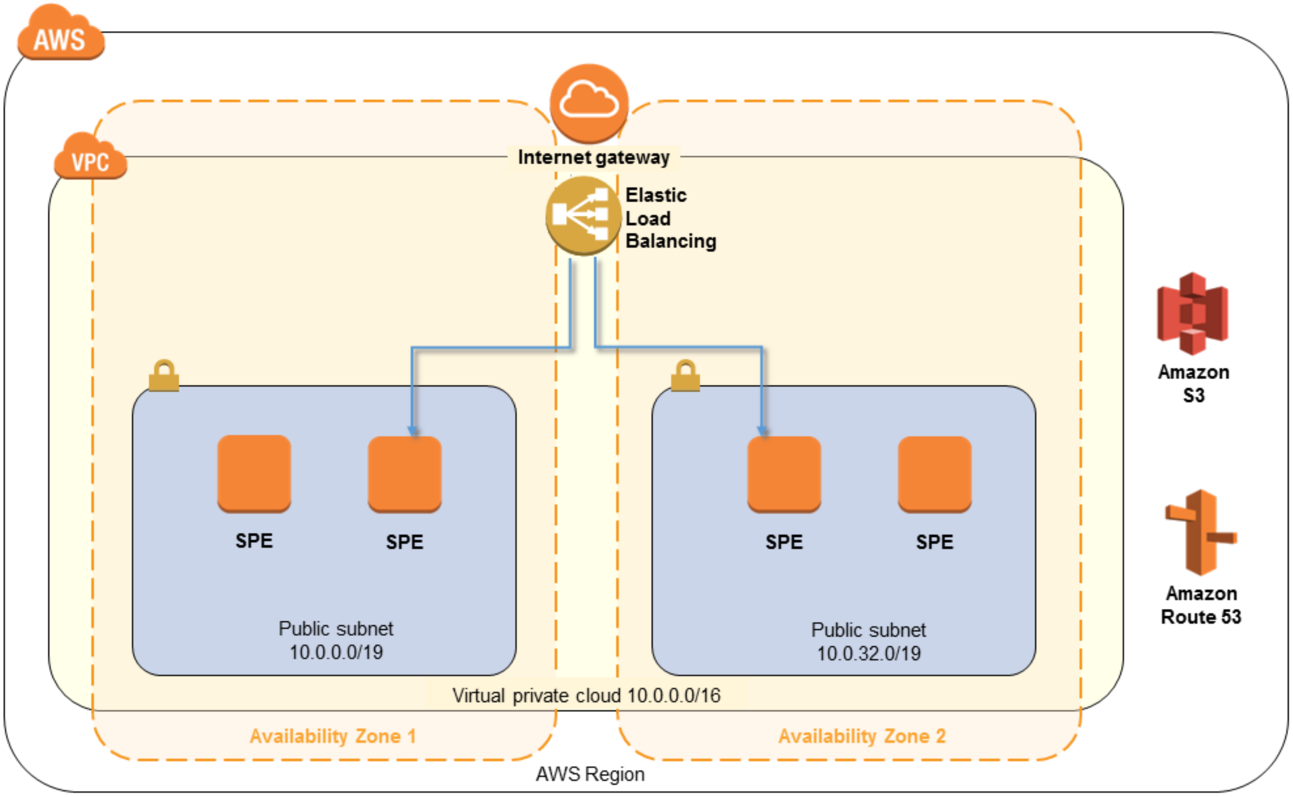
This Quick Start requires a subscription to an Amazon Machine Image (AMI) for the SPE software, which is available from AWS Marketplace. You can choose from two pricing models:

- Paid pricing: With this option, you'll pay an hourly fee based on the Amazon Elastic Compute Cloud (Amazon EC2) instance type.
- Bring Your Own License (BYOL): If you already have a current, valid license for SPE, you can use it for the AWS Quick Start deployment.

For subscription instructions, see step 1 in the deployment steps.

Architecture

Deploying this Quick Start with the **required parameters** builds the following Symantec Protection Engine for Cloud Services environment in the AWS Cloud.



Quick Start SPE architecture on AWS

The Quick Start includes an AWS CloudFormation template, which creates the following services required for your SPE environment based on parameter settings you specify when you launch the stack:

- Elastic Load Balancing (ELB) load balancer – This distributes the incoming loads to multiple scanners. **You must use the fully qualified domain name (FQDN) of the ELB load balancer to direct the scanning load to the farm of SPE (via this load balancer).**
- Security group – The Quick Start creates a security group with protocols SSH port 22 and ICAP port 1344.
- SPE instances – The Quick Start creates the number of EC2 instances for SPE based on your input. These instances are configured automatically with the load balancer that the template creates. The EC2 instances are launched in each Availability Zone that you specify when you launch the stack.

Prerequisites

Specialized Knowledge

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

- Amazon VPC
- Amazon EC2
- Elastic Load Balancing
- AWS security groups
- AWS Multi-AZ support

Technical Requirements

Before you launch the Quick Start, you must set up a virtual private cloud (VPC) in your AWS account and have the license key available in your Amazon Simple Storage Service (Amazon S3) bucket for the BYOL pricing model. (The S3 bucket is not required for the paid pricing model.)

If you choose to deploy the Quick Start into an existing VPC, you must do the following before you launch the Quick Start:

- Install a proxy such as an F5 or Squid proxy.
- Create a VPC in the AWS Region you select for deployment. You'll be prompted for the VPC ID when you launch the Quick Start.
- Create separate public subnets for each Availability Zone in the VPC. You will be prompted for the subnet IDs during launch. The number of subnets is determined by the Availability Zones you want to deploy. For example, two Availability Zones will require two distinct public subnets.
- Determine the number of SPE instances you need. (We recommend two instances for each subnet.)

Deployment Options

This Quick Start provides two deployment options:

- **Deploy SPE into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, and other infrastructure components, and then deploys SPE into this new VPC.
- **Deploy SPE into an existing VPC**. This option provisions SPE in your existing AWS infrastructure.

The Quick Start also lets you configure additional settings such as CIDR blocks, instance types, and SPE settings, as discussed later in this guide.

Deployment Steps

Step 1. Subscribe to the SPE AMI

1. Log in to the AWS Marketplace at https://aws.amazon.com/marketplace.
2. Subscribe to the AMI for the Symantec Protection Engine for Cloud Services by following the link for one of these options:
   - Paid pricing
     -or-
   - BYOL

   For assistance choosing an option, see Costs and Licenses earlier in this guide.
3. Choose **Continue**, and then use the **1-Click Launch** option to launch the AMI into your account on Amazon EC2. This process involves accepting the terms of the license agreement and receiving confirmation email. For detailed instructions, see the AWS Marketplace documentation.
4. If you're using a BYOL license, place the license key file for the software in an Amazon S3 bucket. You'll be prompted for the bucket name and license file name in step 3.

You can log on to the Symantec Licensing Portal to review your licensing status.

For non-technical questions about your license, contact Symantec customer support at http://customersupport.symantec.com/.

Step 2. Prepare an 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 SPE on AWS.
3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase for the Amazon EC2 **m4.2xlarge** and **c4.4xlarge** instance types. You might need to do this if you already have existing deployments that use these instance types, and you think you might exceed the default limit with this reference deployment.

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.

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 SPE into a new VPC on AWS	**Deploy SPE into an existing VPC on AWS**
Launch	Launch

Important If you're deploying SPE into an existing VPC, make sure that your VPC has public subnets in different Availability Zones for the SPE instances. When selecting subnets, make sure that you specify at least one subnet from each Availability Zone. You'll be prompted for your VPC settings when you launch the Quick Start. See the Prerequisites section for details.

Each deployment takes 30-45 minutes to complete, depending on the number of Availability Zones you select.

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 SPE will be built. The template is launched in the US West (Oregon) 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 SPE into a new VPC

   – Parameters for deploying SPE into an existing VPC

- **Option 1: Parameters for deploying SPE into a new VPC**

  View template

  VPC Network Configuration:

Parameter label (name)	**Default**	**Description**
Availability Zones (AvailabilityZones)	*Requires input*	The Availability Zones in the AWS Region where you want to install SPE. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.
VPC CIDR (VPCCIDR)	10.0.0.0/16	CIDR block for the VPC.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 2.
Permitted IP range (AccessCIDR)	*Requires input*	The CIDR IP range that is permitted to access SPE nodes. We recommend that you set this value to a trusted IP range. For example, you might want to grant only your corporate network access to the software.
NAT Instance Type (NATInstanceType)	t2.small	EC2 instance type for NAT instances. This parameter is used only if your selected AWS Region doesn't support NAT gateways.

SPE Setup:

Parameter label (name)	Default	Description
LicenseLocation (LicenseLocation)	*Requires input*	The name of the S3 bucket that contains your SPE license key file, from step 1. This is required only for BYOL licenses.
Number of Instances (InstanceCount)	4	The number of SPE instances you'd like to deploy. We recommend at least two instances per Availability Zone.
SPE EC2 Instance Type (InstanceType)	c4.4xlarge	The EC2 instance type for the SPE instances.
LicenseMode (LicenseMode)	BYOL	The type of SPE license you're planning to use for the deployment: Paid or BYOL. See step 1 for details. If you choose BYOL, you must also provide values for the **SPELicenseFile** and **LicenseLocation** parameters.
SPELicenseFile (SPELicenseFile)		The name of the SPE BYOL license file (e.g., sym5421558000.slf).
Key Name (KeyPairName)	*Requires input*	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.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	The 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-symantec-protectionengine/	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, but should not start or end with a forward slash (which is automatically added).

- ### Option 2: Parameters for deploying SPE into an existing VPC

  View template

Parameter	Default	Description
AvailabilityZone	*Requires input*	The Availability Zones in the AWS Region where you want to install SPE. The Quick Start requires at least two Availability Zones and preserves the logical order you specify.
InstanceCount	4	The number of SPE instances you'd like to deploy. We recommend at least two instances per Availability Zone.
InstanceType	c4.4xlarge	EC2 instance type for the SPE instances.
KeyName	*Requires input*	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.
LicenseLocation	*Requires input*	The name of the S3 bucket that contains your SPE license key file, from step 1. This is required only for BYOL licenses.
LicenseMode	BYOL	The type of SPE license you're planning to use for the deployment: Paid or BYOL. See step 1 for details. If you choose BYOL, you must also provide values for the **SPELicenseFile** and **LicenseLocation** parameters.
SPELicenseFile	*Requires input*	The name of the SPE BYOL license file (e.g., sym5421558000.slf).
SSHLocation	*Requires input*	The CIDR IP range that is permitted to access SPE nodes. We recommend that you set this value to a trusted IP range. For example, you might want to grant only your corporate network access to the software.
Subnets	*Requires input*	The list of subnets from your VPC.
VpcId	*Requires input*	The ID of your existing VPC where you want to deploy SPE (e.g., vpc-0343606e).

5. 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**.

6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.

7. Choose **Create** to deploy the stack.

8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the deployment is complete.

9. Use the URL displayed in the **Outputs** tab for the stack to view the resources that were created.

Step 4. Test the Deployment

To test this deployment, use the command-line scanner that comes with SPE. For instructions on how to obtain and use the scanner, see the Symantec documentation.

1. Write down the FQDN of the ELB load balancer.
2. Get an anti-malware test file from the European Institute for Computer Anti-Virus Research (EICAR) website.
3. Use the command-line scanner to test the file, using the FQDN of the ELB load balancer instead of individual server IP addresses; for example:

```
bash$ ssecls -server <FQDN-of-ELB> -mode scan -verbose
</path/to/test_file>
```

> **Note** For C-based command-line scanner syntax and usage instructions, see the Symantec documentation.

Troubleshooting

If you encounter a CREATE_FAILED error when you launch the Quick Start, 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'll want to look at the log files in `/var/log`.)

> **Important** When you set **Rollback on failure** to **No**, you'll continue to incur AWS charges for this stack. Please make 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.

Additional Resources

AWS services

- AWS CloudFormation
  http://aws.amazon.com/documentation/cloudformation/
- Amazon EC2
  http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/
- Amazon VPC
  http://aws.amazon.com/documentation/vpc/
- Elastic Load Balancing
  https://aws.amazon.com/elasticloadbalancing/

Symantec documentation

- SPE product page
  http://www.symantec.com/protection-engine-for-cloud-services/
- SPE system requirements
  http://www.symantec.com/protection-engine-for-cloud-services/system-requirements/
- SPE datasheet
  http://www.symantec.com/protection-engine-for-cloud-services/data-sheets-white-papers/

Quick Start reference deployments

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

Send Us Feedback

We welcome your questions and comments. Please post your feedback on the AWS Quick Start Discussion Forum.

You can visit our GitHub repository to download the templates and scripts for this Quick Start, and to share your customizations with others.

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.