Symantec™ Data Loss Prevention Deployment Guide for Amazon Web Services

Versions 12.5 - 15.0

Symantec

Symantec Data Loss Prevention Deployment Guide for Amazon Web Services

Documentation versions: 12.5 - 15.0

Last updated: 20 September 2017

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

About this guide

This chapter includes the following topics:

What you should know

This guide provides technical information for customers deploying Symantec Data Loss Prevention servers on Amazon Web Services (AWS) infrastructure. Details include system requirements, security considerations, and deployment instructions.

Note: The AWS solution that is described here is supported on Data Loss Prevention 12.5 though 15.0. All references to product documentation are to version 15.0 only.

This guide assumes:

- You have knowledge and experience with Symantec Data Loss Prevention. For more information, refer to the *Symantec Data Loss Prevention Administration Guide* available at the Symantec Support Center at: http://www.symantec.com/docs/DOC9261.
- You have an existing AWS account. To create an AWS account, go to http://www.aws.amazon.com.
- You have knowledge and experience with AWS and its key features EC2, VPCs, and Security Groups. To access the AWS documentation, go to http://www.aws.amazon.com/documentation. Before you deploy Data Loss Prevention on AWS you should read the "Getting Started with AWS" section of the AWS documentation.

This guide refers to specific areas of the AWS documentation for more information on specific details for deploying Symantec Data Loss Prevention on AWS. It is available at the Symantec Support Center at:

http://www.symantec.com/docs/DOC9520. The guide may be updated to indicate support for new detection servers, to address changes to AWS terminology, and to provide other necessary updates. Subscribe to this article to receive automatic notifications when an updated version is published.

Chapter 2

Introducing Symantec Data Loss Prevention on Amazon Web Services

This chapter includes the following topics:

About deploying Data Loss Prevention on Amazon Web Services

Symantec Data Loss Prevention two-tier deployments are supported on Amazon Web Services Virtual Private Cloud (VPC). That enables you to use a cloud infrastructure for one or more of your Data Loss Prevention servers. You can use a hybrid architecture for your AWS cloud deployment. With hybrid architectures, you deploy an Enforce Server and Oracle database on premises and deploy detection servers on the AWS infrastructure. The detection servers connect to an

Enforce Server using a registered TCP port number. Or, you can deploy the Enforce Server, the Oracle database, and detection servers on AWS. You do not have to modify the servers or perform any special configurations to deploy Data Loss Prevention on AWS.

For more information see "About installation tiers" in the *Symantec Data Loss Prevention Installation Guide* at http://www.symantec.com/docs/DOC9257.

Some examples of AWS deployments include:

- A Network Discover detection server on AWS. This server discovers sensitive data residing on Microsoft SharePoint, Microsoft Exchange, and CIFS-compliant file share servers residing in the cloud.
- A Network Prevent for Email detection server on AWS. This server controls the transmission of sensitive email from a Microsoft Exchange mail server residing in the cloud.
- An Enforce Server with the Oracle database and the Cloud Prevent for Email Server in the AWS cloud. This server prevents data loss from Microsoft Office 365 email traffic.

See “Supported Data Loss Prevention servers on AWS” on page 9.

Supported VPC configurations for EC2 instances

The Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated region of the AWS cloud in a virtual network that you define.

To deploy Data Loss Prevention on AWS, you must use a VPC. Symantec only supports connecting an on-premises Enforce Server to a detection server that is deployed to an EC2 instance with a VPC.

If you created an AWS account after December 2013, when you provision an EC2 instance you either use the default VPC or one you define.

If you created an AWS account before December 2013, note the following. When you provision an EC2 instance you are given the option of creating an EC2 "Classic" instance. An EC2 Classic instance is EC2 without VPC, or EC2 with VPC. If this situation applies to you, you must make sure you provision the EC2 instance with VPC.

Supported Data Loss Prevention servers on AWS

Symantec Data Loss Prevention supports the deployment of the following servers on AWS infrastructure:

- Enforce Server with Oracle database on the same computer.

- Cloud Prevent for Email
- Network Prevent for Web
- Endpoint Prevent
- Network Discover
- Network Prevent for Email

If you want to deploy the Enforce Server on the AWS infrastructure, Symantec supports two-tier deployment of Symantec Data Loss Prevention on AWS. Two-tier deployments are where the Oracle database and the Enforce Server are deployed on a single system. Three-tier deployment of Symantec Data Loss Prevention on AWS is not supported because of data security considerations.

Symantec Data Loss Prevention versions 12.0.x or earlier detection servers are not supported on AWS.

Supported Network Discover scan targets on AWS

Symantec Data Loss Prevention supports the scanning of the following Network Discover targets in the AWS cloud:

- Box cloud storage
- Microsoft Exchange Server
- Microsoft SharePoint Server
- File share server (CIFS)

Refer to the *Symantec Data Loss Prevention System Requirements Guide* for the supported versions of these targets. The latest version of this guide is available at the Symantec Support Center at: http://www.symantec.com/docs/DOC9256.

Supported AWS EC2 instance types

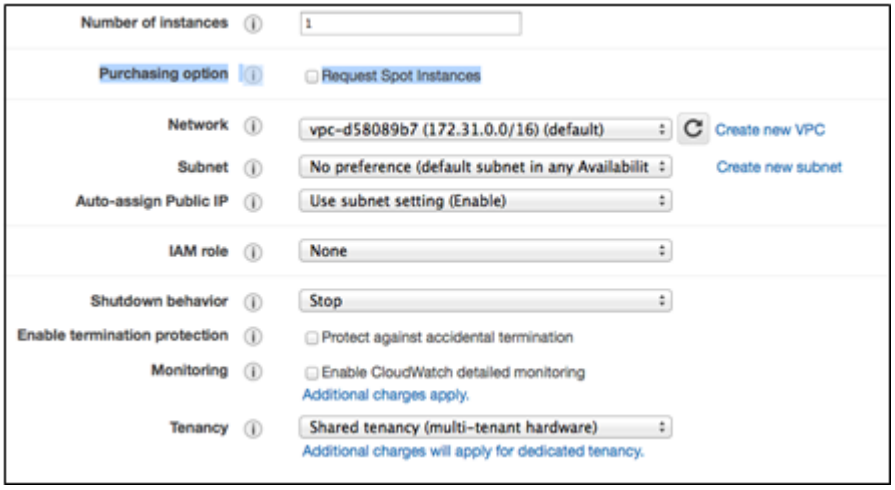
The Amazon Elastic Cloud Compute (EC2) is a web service that provides virtual servers in the cloud. You deploy supported Data Loss Prevention detection servers to EC2 instances.

EC2 instances can be provisioned in three different ways: on demand, reserved, and spot. On demand and reserved EC2 instances guarantee performance corresponding with the specifications of the Amazon machine image (AMI) provided by the instance. EC2 spot instances, on the other hand, allow users to bid on unused EC2 capacity at a lower price. Spot instances are only appropriate for the tasks that can withstand frequent or intermittent interruption. Your detection servers must

run without foreseeable interruption. As such, Symantec Data Loss Prevention does not support the use of EC2 spot instances for your Data Loss Prevention on AWS deployments.

Figure 2-1 shows the EC2 instance details.

Figure 2-1 No support for EC2 Spot Instances



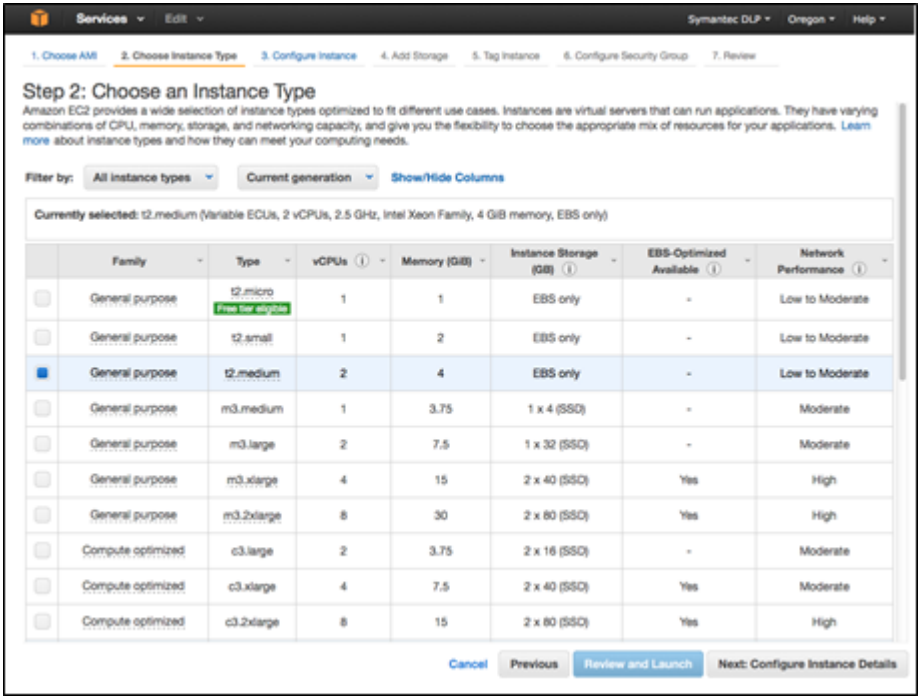
AWS provides various flavors of EC2 instances. For example, there are t2.* instance types, m3.* instance types, c3.* instance types, and more. In addition, for each EC2 instance type there are various sizes (micro, small, medium, and large). Be aware that all t2.* instance types, including micro, small, and medium, are Burstable Performance Instances (http://aws.amazon.com/ec2/faqs/). Because the baseline CPU performance for t2.* burstable performance instances are only allocated a small percentage of a single CPU core, Symantec Data Loss Prevention does not recommend the use of t2.* instances for detection server deployments on AWS. You may use a t2.* instance type for deploying a data source host, such as a Discover scan target or server, but you should not use t2.micro. You may use t2.small or t2.medium to host a data source.

To summarize, the following EC2 instance types are not supported or recommended:

- EC2 spot instances are not supported for any Data Loss Prevention on AWS deployment.
- t2.micro instances are not supported for Data Loss Prevention detection server on AWS deployments.
- t2.small and t2.medium instances are not recommended, but may be used to host Data Loss Prevention data sources, such as Discover scan targets.

Figure 2-2 shows some of the various EC2 instance types. Symantec Data Loss Prevention does not recommend the use of t2.* instances types for deploying detection servers on AWS.

Figure 2-2 EC2 instance types



Supported VPC configurations for EC2 instances

The Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated region of the AWS cloud in a virtual network that you define.

To deploy Data Loss Prevention on AWS, you must use a VPC. Symantec only supports connecting an on-premises Enforce Server to a detection server that is deployed to an EC2 instance with a VPC.

If you created an AWS account after December 2013, when you provision an EC2 instance you either use the default VPC or one you define.

If you created an AWS account before December 2013, note the following. When you provision an EC2 instance you are given the option of creating an EC2 "Classic" instance. An EC2 Classic instance is EC2 without VPC, or EC2 with VPC. If this

situation applies to you, you must make sure you provision the EC2 instance with VPC.

Supported operating systems for detection servers on AWS

When you provision an EC2 instance, you choose the type of Amazon machine image (AMI) to use. AWS provides several AMIs, and you can go to the AWS Marketplace for third-party provided AMIs. At a minimum each AMI provides a host operating system. Some AMIs also provide storage, database, directory, and other services. The components of the AMI you choose depend on your business requirements.

Refer to the *Symantec Data Loss Prevention System Requirements Guide* for a complete list of supported operating systems for Data Loss Prevention. The latest version of this guide is available at the Symantec Support Center at: http://www.symantec.com/docs/DOC10602.

Symantec Data Loss Prevention supports the following Windows operating systems for your AWS deployments:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2 with patch
- Microsoft Windows Server 2008 R2

Symantec Data Loss Prevention supports the following Linux operating systems for your AWS deployments:

- Red Hat Enterprise Linux 6.7 through 6.9 and 7.1 through 7.3.

Note: The RHEL 6.x and 7.x AWS AMI distributions require an additional package. See "About configuring the Red Hat Enterprise Linux versions 6.x and 7.x AMI" on page 18.

Estimated sizing guidelines for EC2 instances

The topic "Minimum system requirements for Symantec Data Loss Prevention servers" in the *Symantec Data Loss Prevention System Requirements Guide* lists the minimum hardware requirements for detection servers. The latest version of this guide is available at the following URL: http://www.symantec.com/docs/DOC10602.

AWS terminology refers to a CPU as vCPU. Each vCPU is single-core. Therefore, 4 vCPU is equivalent to 2 x 2 dual core that is listed in the *System Requirements Guide*. Keep in mind, however, that these are the minimum size requirements. Your sizing requirements may vary depending on the types of detection conditions you deploy to Data Loss Prevention servers.

Chapter 3

Considerations for deploying detection servers on AWS

This chapter includes the following topics:

About securing your EC2 instances in the AWS cloud

When you deploy an EC2 instance in the AWS cloud, initially it is open to the entire Internet. Such a configuration is not recommended because it is not secure. To secure the EC2 instance and protect the integrity of the system, you need to configure an AWS Security Group.

See “About configuring AWS security groups” on page 17.

About Endpoint Prevent and the AWS Elastic Load Balancer

Symantec Data Loss Prevention Endpoint Prevent on AWS Elastic Load Balancer (ELB) does not support SSL session affinity. SSL session affinity (also known as a "sticky session") is only for HTTP/HTTPS load balancer listeners. For more information, refer to the AWS document at:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/US_StickySessions.html

Note: "Instance" is the AWS term for virtual machine.

ELB is used to balance the Endpoint client connections to the Endpoint Server. When configuring a new ELB instance, follow the AWS instructions and use the following settings:

- Configure the Endpoint clients to connect to the IP or the host name of ELB computer (not to the Endpoint Servers).
- **Listeners** tab: Set **Load Balancer Protocol** to **TCP** and set **Load Balancer Port** to any port number (for example, 443).
- **Instance Protocol** tab: Configure **Instance Protocol** to **TCP**.
- **Instance Port**: For Linux Endpoint detection servers, the value of the TCP **Instance Port** cannot be under 1024.
- **Health Check** tab: Set **Ping Protocol** to **TCP** and set **Ping Port** to the port that Endpoint client servers listen on.

About securing your Data Loss Prevention servers in the AWS cloud

Symantec Data Loss Prevention servers communicate securely using SSL. When you deploy a detection server, the Enforce Server generates a default SSL certificate for secure server communications. While the default server certificate is suitable for pure on-premises deployments, the default certificate is not secure for hosted or cloud deployments. Someone familiar with Data Loss Prevention can use the default certificate to compromise the detection server you have deployed to AWS. This system might be vulnerable to man-in-the-middle attacks and other security threats.

You must generate a unique custom SSL certificate for your Data Loss Prevention servers to secure your Data Loss Prevention on AWS deployment.

See "About generating a unique, self-signed SSL certificate for Data Loss Prevention servers" on page 17.

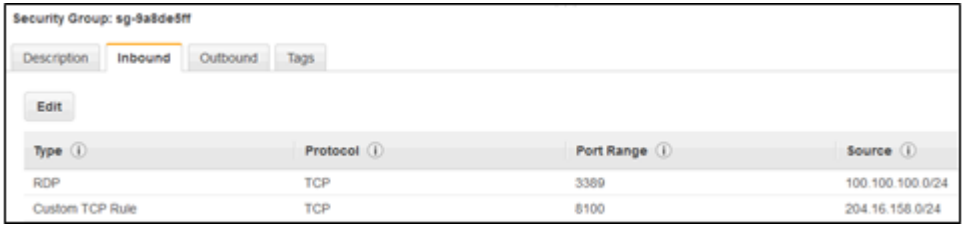
About configuring AWS security groups

An AWS Security Group is a virtual firewall that controls inbound and outbound traffic for one or more EC2 instances. When you launch an EC2 instance, you associate one or more security groups with the instance. You add inbound and outbound rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group. AWS checks the security group rules before it allows traffic to or from the EC2 instance.

Symantec recommends that you harden each AWS Security Group to which the detection server belongs. This results in minimal open ports. We also recommend that you whitelist the source IP to at least the third octet, for example: `x.x.x.0/24`.

Figure 3-1 shows an example AWS Security Group with inbound rules. Notice that only the necessary ports are opened, and the IP addresses are limited to the third octet.

Figure 3-1 Example AWS Security Group configuration for a detection server: Inbound Rules



About generating a unique, self-signed SSL certificate for Data Loss Prevention servers

The default Enforce Server certificate that is generated when you install a detection server is not secure for cloud deployments.

You need to generate a custom server certificate using the SSL certificate generation tool that is provided with the Data Loss Prevention installation. Then, you deploy this custom certificate to both the on-premises Enforce Server and each detection server in the AWS cloud.

A custom SSL certificate secures communication between your Data Loss Prevention servers. To generate a custom SSL certificate, see "Configuring certificates for secure communications between Enforce and detection servers." You can find this chapter in the *Symantec Data Loss Prevention Installation Guide* for your operating system.

See "About installing supported server software on an AMI" on page 19.

About configuring the Red Hat Enterprise Linux versions 6.x and 7.x AMI

To install a Data Loss Prevention detection server on Red Hat Enterprise Linux version 6.x or 7.x, refer to the *Symantec Data Loss Prevention Installation Guide for Linux*.

On Red Hat Enterprise Linux version 6.x, you must verify that the following packages are installed. If these packages are not installed you must install them:

- `compat-openldap`
- `compat-expat1`
- `compat-db43`
- `openssl098e`

On Red Hat Enterprise Linux version 7.x, you must verify that these 64-bit only packages are installed. If these packages are not installed, you must install them:

- `compat-openldap-1:2.3.43-5.el7`
- `compat-db47-4.7.25-28.e17`
- `libpng12`
- `compat-libtiff3`
- `libjpeg`

In addition, for the AMI version of Red Hat Enterprise Linux versions 6.x and 7.x, you also need to verify that the `apr-util.x86_64` package is installed. If this package is not installed on the EC2 instance, the detection server FileReader process does not start.

When you install Symantec Data Loss Prevention 15.0 on the RHEL 7.x AMI image in AWS, make sure the `libjpeg` package is installed. If the package is not installed, you may get this error: `java.lang.UnsatisfiedLinkError: /opt/SymantecDLP/Protect/lib/native/libImageUtilitiesJNI.so:`

`libjpeg.so.62: cannot open shared object file: No such file or directory.`

To install the additional RHEL 6.x and 7.x package required for EC2 instances:

1. Configure Red Hat Enterprise Linux to connect to a valid distribution repository.
2. Issue the following command: `yum install apr-util.x86_64`.
3. Verify that FileReader starts.

Note: You must also verify that the `firewalld` package is installed on RHEL 7.x before you install Data Loss Prevention. The standard RHEL 7.x AMI does not contain the `firewalld` package. The Data Loss Prevention installer does not install it automatically.

About installing supported server software on an AMI

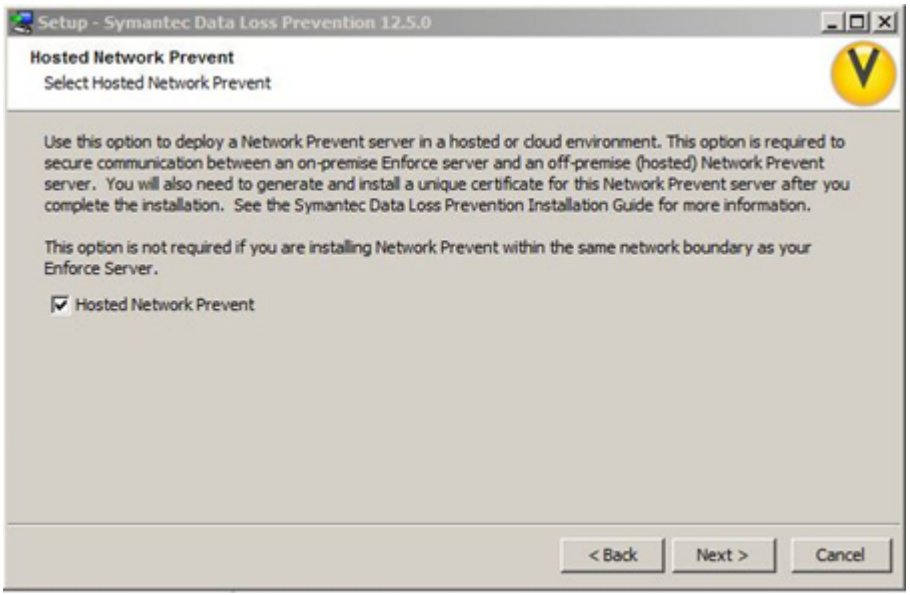
Installing a supported Data Loss Prevention server on an AWS EC2 instance is straightforward. Refer to the *Symantec Data Loss Prevention Installation Guide* at http://www.symantec.com/docs/9257 for your operating system for instructions.

When you install a server on an EC2 instance, you must be sure to select the **Hosted Network Prevent** option. Ignore the description in the installer screen indicating that this option only applies to Network Prevent. This option applies to any detection server you deploy in the cloud.

Selecting this option prevents the system from generating a default SSL certificate for connecting between the detection server and the Enforce Server. If you select this option, you cannot connect the detection server to the Enforce Server until you generate a custom SSL server certificate.

See "About generating a unique, self-signed SSL certificate for Data Loss Prevention servers" on page 17.

Figure 3-2 Installation requirement for Data Loss Prevention detection servers in the cloud



About registering a detection server deployed on AWS with an Enforce Server

Registering a detection server that is deployed to the AWS cloud is straightforward. Refer to the *Symantec Data Loss Prevention Installation Guide* at http://www.symantec.com/docs/9257 for your operating system for instructions.

When you register a detection server with the Enforce Server, you provide the connection TCP port. The Enforce Server administration console only accepts registered port numbers in the range of 1024 through 49151. Well-known ports (0 through 1023) and private ports (49152 to 65535) are not supported. You must open the port you enter on the detection server. You can open a port by creating an inbound rule for a Security Group and apply that Security Group to the EC2 instance.

See “About configuring AWS security groups” on page 17.

About Network Prevent for Email and AWS Simple Email Service

Network Prevent for Email on AWS does not support AWS Simple Email Service (SES) as a downstream Mail Transfer Agent (MTA). It doesn't work because SES relies on a user name and password credential, while Data Loss Prevention STMP Prevent relies on an anonymous connection.

The next hop (downstream) MTA can be configured either in reflect mode or forward mode. With forward mode, a next hop MTA such as Sendmail can be used to forward SMTP traffic.

Chapter 4

Workflow for deploying detection servers on AWS

This chapter includes the following topics:

About the deployment workflow

This section provides the workflow for deploying a supported Data Loss Prevention detection server on AWS infrastructure. The purpose of this section is to provide you with an example test deployment on which you can base additional deployments for production purposes.

See "Deploying a supported Data Loss Prevention detection server on AWS" on page 23.

These instructions are specific to the Windows Server 2012 operating system and the Network Discover detection server. However, the general workflow for deploying a supported Data Loss Prevention detection server on AWS is the same. After you have gone through the basic workflow, you can extrapolate these steps to other supported detection servers and operating systems. For example, similar steps work for deploying a Network Prevent for Email detection server on Red Hat Enterprise Linux 6.x and 7.x.

See "About configuring the Red Hat Enterprise Linux versions 6.x and 7.x AMI" on page 18.

Refer to the *Symantec Data Loss Prevention Administration Guide* for details on configuring the Network Prevent for Email server.

Deploying a supported Data Loss Prevention detection server on AWS

This section provides instructions for deploying a supported Data Loss Prevention detection server on an AWS EC2 instance. It also details how to connect this detection server to an on-premises Enforce Server. These instructions assume that you have deployed an on-premises Enforce Server and that this server is available.

See "About the deployment workflow" on page 22.

The deployment workflow includes AWS-specific tasks and tasks specific to Symantec Data Loss Prevention.

Table 4-1 Deploying a supported Data Loss Prevention detection server on AWS

Step	Action	Description
1	Choose an AMI.	Log on to the AWS Console and select an AMI that provides an operating system that Data Loss Prevention supports. See "Supported Data Loss Prevention servers on AWS" on page 9. For example: **Microsoft Windows Server 2012 Base - ami-3b83c20b**
2	Choose an instance type.	Select an EC2 instance type that is suitable for your business requirements. See "Supported AWS EC2 instance types" on page 10. For example: ■ Family: General purpose ■ Type: m3.large ■ vCPUs: 2 ■ Memory (GB): 7.5 ■ Instance Storage: 1 x 32 (SSD) ■ Network Performance: Moderate **Note:** Symantec Data Loss Prevention does not recommend the use of t2.* instance types. See "Estimated sizing guidelines for EC2 instances" on page 13.

Table 4-1 Deploying a supported Data Loss Prevention detection server on AWS *(continued)*

Step	Action	Description
3	Configure instance details.	Do not select Request Spot Instances. Spot instances are not supported. Verify that the Network is VPC. EC2 Classic (non-VPC) instance types are not supported. See "Supported AWS EC2 instance types" on page 10.
4	Add storage.	Skip this step. You do not need external storage for a Data Loss Prevention detection server.
5	Tag the instance.	Optionally you can add metadata tags to help yourself or other administrators organize and locate your EC2 instances.
6	Configure the security group.	Specify and configure your own security group. Initially the EC2 instance is open to the Internet and is not secure. You secure the instance by configuring a TCP port that the Enforce Server connects to. You also need to poke a hole in the firewall all so you can connect using RDP. See "About configuring AWS security groups" on page 17.
7	Review and launch.	Review the EC2 instance details and click **Launch** when you are ready. Back at the console, the instance displays **Initializing**.
8	Create and download the private key, or use an existing one previously generated.	Select Create a new key pair. This key pair lets you decrypt the Windows password that you used to log on to the system. Download the key pair. You use the key to log on to the system the first time. If you already generated a key pair, you can use it to log on to the EC2 instance.
9	Use the private key to decrypt the Windows password.	Right click the instance and select Get Windows Password. Select the `*.pem` file you downloaded. Click **Decrypt Password**. Write down the decrypted password. You need it to log on to the EC2 instance.
10	RDP to the EC2 instance.	RDP to the EC2 instance and logon using the password key you decrypted. **Note:** You may have to disable the operating system firewall to be able to connect using RDP.
11	Change the host password.	Alternatively, to avoid having to using the key password each time, you can change the password.

Table 4-1 Deploying a supported Data Loss Prevention detection server on AWS *(continued)*

Step	Action	Description
12	Copy the Data Loss Prevention installer to the EC2 instance.	You must copy the Data Loss Prevention installation software to the EC2 instance. You can get the software at Symantec FileConnect using a web browser running on the EC2 instance. Alternatively you can place the software in a cloud or FTP storage site and download it to the EC2 instance.
13	Install the Data Loss Prevention software.	Make sure that you select the **Hosted Network Prevent** option. See "About installing supported server software on an AMI" on page 19.
14	Register the detection server.	Go to the Enforce Server administration console and register the detection server with the Enforce Server by specifying the port. The port must be a registered TCP port in the range of 1024 to 49151. The Enforce Server does not accept well-known ports (0 through 103) or private ports (49152 through 65535). You must have added this port to an inbound rule for the Security Group. See "About registering a detection server deployed on AWS with an Enforce Server" on page 20.
15	Generate custom server certificates.	The default Data Loss Prevention server certificate is not secure. With **Hosted Network Prevent** option as recommended (step 13), you do not have a server certificate. Either way, you must generate a unique, self-signed server certificate to ensure secure communications between the on-premises Enforce Server and the detection server on AWS. See "About generating a unique, self-signed SSL certificate for Data Loss Prevention servers" on page 17.
16	Verify your Data Loss Prevention on AWS deployment.	Once you deploy the custom certificate, the Enforce Server should be able to connect to the detection server.

Setting up a CIFS file share scan target on AWS

Symantec Data Loss Prevention supports the deployment of Network Discover Servers in the AWS cloud. It also supports the scanning of targets that are deployed in the AWS cloud, including Exchange and SharePoint servers and CIFS file shares.

Testing and troubleshooting your Data Loss Prevention on AWS deployment

As with any Data Loss Prevention deployment, you should test it to ensure that it is production ready. You must create some detection rules that are typical for your organization and generate some incidents. In addition, you should test the performance of your EC2 instance under some representative load.