Symantec™
A Division of Broadcom

Symantec Data Loss Prevention Deployment Guide for Amazon Web Services

Versions 15.0 - 15.7

November 5, 2020

Table of Contents

About this guide....4
About updates to the Deployment Guide for Amazon Web Services.... 4
What you should know....4
Introducing Symantec Data Loss Prevention on Amazon Web Services.... 5
About deploying Data Loss Prevention on Amazon Web Services.... 5
Supported VPC configurations for EC2 instances....5
Supported Data Loss Prevention servers on AWS.... 5
Supported Network Discover scan targets on AWS.... 6
Supported AWS EC2 instance types.... 6
Supported VPC configurations for EC2 instances....7
Supported operating systems for detection servers on AWS.... 8
Estimated sizing guidelines for EC2 instances....8
Considerations for deploying supported servers on Amazon Web Services....9
About securing your EC2 instances in the AWS cloud....9
About Endpoint Prevent and the AWS Elastic Load Balancer....9
About securing your Data Loss Prevention servers in the AWS cloud....9
About configuring AWS security groups.... 9
About generating a unique, self-signed SSL certificate for Data Loss Prevention servers....10
About configuring the Red Hat Enterprise Linux versions 6.x and 7.x AMI....10
About installing supported server software on an AMI....11
About registering a detection server deployed on AWS with an Enforce Server.... 12
About Network Prevent for Email and AWS Simple Email Service.... 12
Workflow for deploying a Data Loss Prevention detection server on AWS.... 13
About the deployment workflow.... 13
Deploying a supported Data Loss Prevention server on AWS....13
Deploying the Oracle database and Enforce Server in a three- or two-tier environment....15
Setting up a CIFS file share scan target on AWS.... 16
Testing and troubleshooting your Data Loss Prevention on AWS deployment....17
Configuring certificates for securing communications between the Enforce Server and Amazon RDS for Oracle.... 18
About securing communications between the Enforce Server and Amazon RDS for Oracle....18
Configuring Oracle RDS Option Group with SSL....18
Configuring the server certificate on the Enforce Server.... 18
Setting up an SSL connection over JDBC.... 20
Verifying the Enforce Server-Oracle RDS database certificate usage.... 20
Upgrading an Enforce Server running in AWS....21

About upgrading the Enforce Server in Amazon RDS for Oracle.. 21

Steps to upgrade the Enforce Server in Amazon RDS for Oracle...21

Preparing the Amazon RDS for Oracle for a Symantec Data Loss Prevention upgrade... 21

Setting variables in the Amazon RDS for Oracle database..22

Preparing to run the Update Readiness Tool for Amazon RDS for Oracle..22

Creating the Update Readiness Tool database account for Amazon RDS for Oracle......................................23

Running the Update Readiness Tool for Amazon RDS for Oracle.. 23

Reviewing update readiness results..24

Upgrading the Enforce Server on Windows..25

Installing the Java Runtime Environment on the Enforce Server... 26

Installing an Enforce Server.. 26

Running the Migration Utility on the Enforce Server...29

Upgrading the Enforce Server on Linux..30

Installing the Java Runtime Environment on the Enforce Server... 31

Installing an Enforce Server.. 31

Running the Migration Utility on the Enforce Server...32

Copyright statement.. 34

About this guide

About updates to the Deployment Guide for Amazon Web Services

This guide is occasionally updated as new information becomes available. See the following table for a summary of the latest changes.

Table 1: Change history for the *Symantec Data Loss Prevention Deployment Guide for Amazon Web Services* guide

Date	Change description
5 November 2020	Added support for Oracle 19c. Added steps for securing the server connection between the Enforce Server and Oracle RDS.

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 Symantec Data Loss Prevention 15.0 though 15.7. All references to product documentation are to version 15.7 only.

This guide assumes the following:

- You have knowledge and experience with Symantec Data Loss Prevention. See the Symantec Data Loss Prevention Help Center.
- 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.

Introducing Symantec Data Loss Prevention on Amazon Web Services

About deploying Data Loss Prevention on Amazon Web Services

Symantec Data Loss Prevention three- and 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 also 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. You can deploy the Enforce Server, the Oracle database (or Oracle RDS), and detection servers on AWS. Starting with Symantec Data Loss Prevention 15.1, you can use AWS Oracle RDS in a three-tier deployment. You can use Transport Layer Security (TLS) to encrypt all data that is transmitted between the Enforce Server and the database server or Oracle RDS.

See About securing communications between the Enforce Server and Amazon RDS for Oracle.

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.

Supported Data Loss Prevention servers on AWS

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:

- Two-tier deployment of Enforce Server and the Oracle database on the same server
- Three-tier deployment with Oracle database or Oracle RDS
- 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- and three-tier deployments 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 deployments of Symantec Data Loss Prevention on AWS are supported starting with version 15.1.

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)

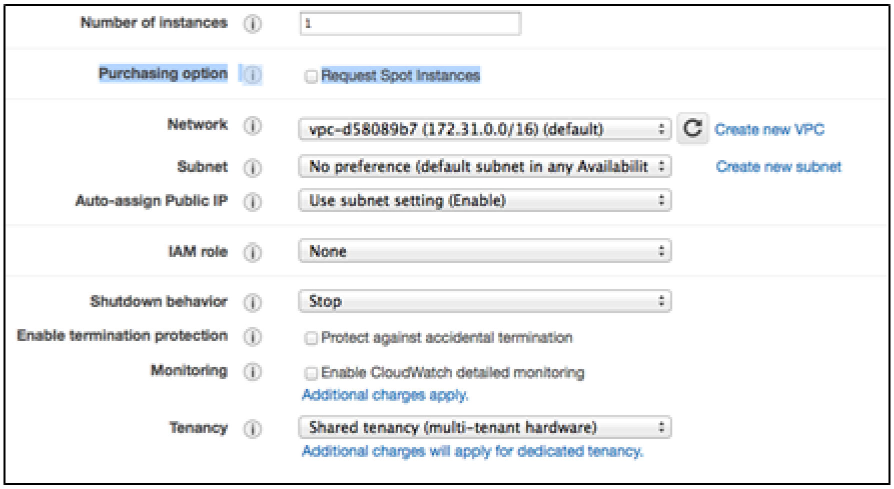
See the Symantec Data Loss Prevention Help Center for the supported versions of these targets.

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.

No support for EC2 Spot Instances shows the EC2 instance details.



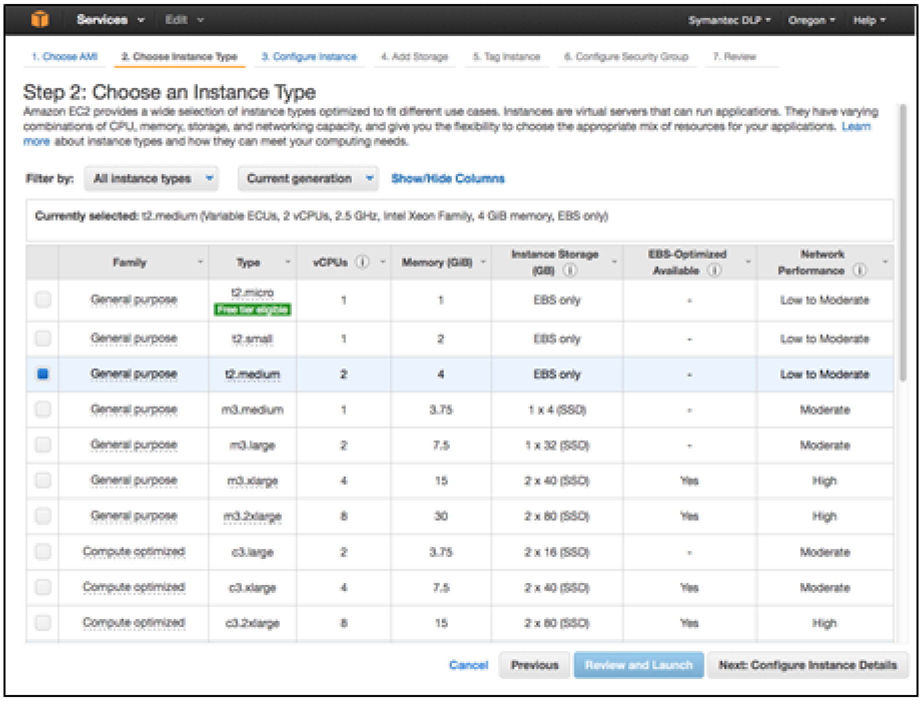
Number of instances	1
Purchasing option	□ Request Spot Instances
Network	vpc-d58089b7 (172.31.0.0/16) (default)
Subnet	No preference (default subnet in any Availabilit
Auto-assign Public IP	Use subnet setting (Enable)
IAM role	None
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared tenancy (multi-tenant hardware) Additional charges will apply for dedicated tenancy.

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.

EC2 instance types 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.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | Show/Hide Columns

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.5 GHz, Intel Xeon Family, 4 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
■	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
□	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
□	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
□	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
□	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
□	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
□	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
□	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High

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.

See the Symantec Data Loss Prevention Help Center for a complete list of supported operating systems for Data Loss Prevention.

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

Estimated sizing guidelines for EC2 instances

See the topic "Minimum system requirements for Symantec Data Loss Prevention servers" in Symantec Data Loss Prevention Help Center for a list of the minimum hardware requirements for detection servers.

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.

Considerations for deploying supported servers on Amazon Web Services

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.

About configuring AWS security groups

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.

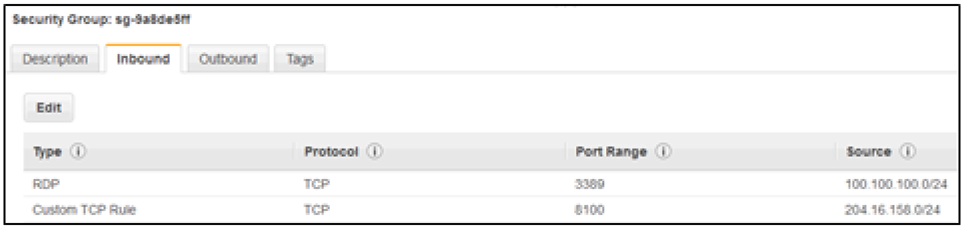
About generating a unique, self-signed SSL certificate for Data Loss Prevention servers

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`.

Example AWS Security Group configuration for a detection server: Inbound Rules 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.



Type	Protocol	Port Range	Source
RDP	TCP	3389	100.100.100.0/24
Custom TCP Rule	TCP	8100	204.16.158.0/24

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" in the *Symantec Data Loss Prevention Installation Guide* for your operating system.

About installing supported server software on an AMI

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*. The following rpm packages are required for Symantec Data Loss Prevention version 15.0 and later.

On Red Hat Enterprise Linux version 6.x, you must verify that the following x64_64 bits packages are installed. If these packages are not installed you must install them:

- `compat-openldap`
- `compat-expat1`
- `compat-db43`
- `openssl098e`
- `apr`
- `expat`

On Red Hat Enterprise Linux version 7.x, you must verify that the following x64_64 bit 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.el7`
- `openssl098e`
- `apr`
- `expat`
- `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.

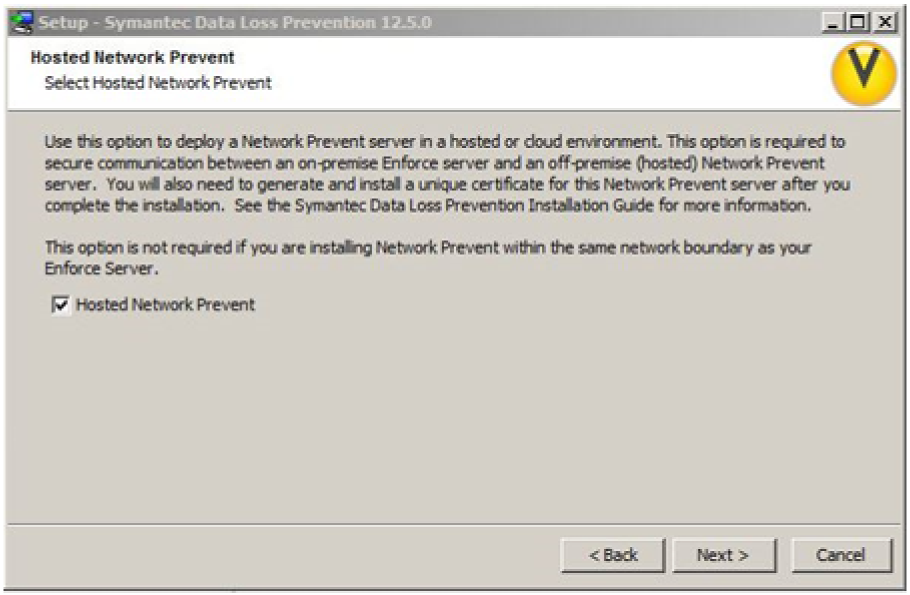
About installing supported server software on an AMI

Installing a supported Data Loss Prevention server on an AWS EC2 instance is straightforward. See the *Symantec Data Loss Prevention Installation Guide* at Related Documents.

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.

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



Setup - Symantec Data Loss Prevention 12.5.0

Hosted Network Prevent

Select Hosted Network Prevent

Use this option to deploy a Network Prevent server in a hosted or cloud environment. This option is required to secure communication between an on-premise Enforce server and an off-premise (hosted) Network Prevent server. You will also need to generate and install a unique certificate for this Network Prevent server after you complete the installation. See the Symantec Data Loss Prevention Installation Guide for more information.

This option is not required if you are installing Network Prevent within the same network boundary as your Enforce Server.

☑ Hosted Network Prevent

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. See the *Symantec Data Loss Prevention Installation Guide* at Related Documents.

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.

About configuring AWS security groups

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 does not 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.

Workflow for deploying a Data Loss Prevention detection server on AWS

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.

Deploying a supported Data Loss Prevention server on AWS

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.

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

See the Symantec Data Loss Prevention Help Center for details on configuring the Network Prevent for Email server.

Deploying a supported Data Loss Prevention server on AWS

This section provides instructions for deploying a supported Data Loss Prevention detection server (Oracle database, Enforce Server, or 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.

About the deployment workflow

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

Table 2: 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. Supported Data Loss Prevention servers on AWS 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. Supported AWS EC2 instance types 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. Estimated sizing guidelines for EC2 instances
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. Supported AWS EC2 instance types
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. About configuring AWS security groups
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.

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. About installing supported server software on an AMI
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. About registering a detection server deployed on AWS with an Enforce Server
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. About generating a unique, self-signed SSL certificate for Data Loss Prevention servers
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. Troubleshooting Data Loss Prevention on AWS deployments

Deploying the Oracle database and Enforce Server in a three- or two-tier environment

Symantec Data Loss Prevention supports three- and two-tier deployments on AWS IAAS with the following Oracle Database software versions:

- Oracle Server versions:
  - v.11.2.0.4
  - v.12.1.0.2
  - v.12.2.0.1
  - v.19.0.0.0
- Oracle RDS versions:
  - v.11.2.0.4
  - v.12.1.0.2

You estimate sizing requirements to best fit your implementation. Estimated sizing guidelines for EC2 instances

Install the Oracle database before you install the Enforce Server.

See one the following guides based for your Oracle database software version:

- See the Symantec Data Loss Prevention Help Center if you you plan to use Oracle 19c Standard or Enterprise Edition.
- See the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* available at Related Documents.
- See the *Symantec Data Loss Prevention Symantec Data Loss Prevention Oracle 12c Enterprise Implementation Guide* available at Related Documents.

See the *Symantec Data Loss Prevention Installation Guide* for your platform available at Related Documents.

Table 3: Steps to deploy the Oracle database and Enforce Server in a three- or two-tier environment

Step	Action	Description
1	Configure Oracle RDS instance.	Confirm that the Oracle RDS instance meets the following configuration requirements: • DB Edition: Standard or Enterprise • DB Engine version: Oracle 19.0.0.0, 12.1.0.2 or 11.2.0.4 • DB Instance Class: db.m4.2x large or higher • Storage Type: Provisioned IOPS(SSD) 100Gib or more • Master User: “protect” with a complex password of at least 8 characters • Public Accessibility: “Yes”, if Enforce Server is deployed outside of RDS VPC. • Database name: “protect” • Database port: “1521” • Character set name: “AL32UTF8”

2	Create the database user and table spaces for the Symantec Data Loss Prevention installation.	Complete the following steps:
		1. Connect to Oracle RDS using SQL*Plus use the following syntax:
		sqlplus master_user/password@fqdn_oracle_rds:db_port/db_name
		For example, the following command uses protect for the master_user, 1521 for the database port, and protect for the database name:
		`sqlplus protect/password@fqdn_oracle_rds:1521/protect`
		2. Run the following command to grant the Master User protect the required credentials:
		GRANT create session ,alter session ,create synonym ,create view ,create table ,create sequence TO protect;
		GRANT create table ,create cluster ,create sequence ,create trigger ,create procedure ,create type ,create indextype ,create operator TO protect;
		GRANT create materialized view TO protect;
		3. Create the required tablespaces by running the following command:
		`create smallfile tablespace LOB_TABLESPACE datafile size 32767M autoextend on next 100M maxsize 32767M;`
		`alter tablespace LOB_TABLESPACE add datafile size 1024M autoextend on next 100M maxsize 32767M;`
		`alter tablespace LOB_TABLESPACE add datafile size 1024M autoextend on next 100M maxsize 32767M;`

3	Install the Enforce Server.	See the *Symantec Data Loss Prevention Installation Guide* for your platform available at Related Documents.
4	Configure secure TLS communication between Enforce Server and Oracle RDS.	See About securing communications between the Enforce Server and Amazon RDS for Oracle.

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.

Configuring certificates for securing communications between the Enforce Server and Amazon RDS for Oracle

About securing communications between the Enforce Server and Amazon RDS for Oracle

You can use SSL/Transport Layer Security (TLS) to encrypt all data that is transmitted between the Enforce Server and the Oracle database hosted with Amazon RDS in a three-tier environment.

These steps assume that you have already set up an AWS account that you can use to manage the Oracle database. See the *Symantec Data Loss Prevention Deployment Guide for Amazon Web Services* located at Related Documents at the Tech Docs Portal.

> **NOTE**
>
> The Amazon Oracle RDS SSL certificate rds-ca-2015-root expires on March 5, 2020. A new certificate rds-ca-2019-root will be rotated in. Symantec recommends that you import both certifcates into the Enforce Server Java keystore proactively. When the certificate rotation occurs, the transition is seemless; you do not change the Enforce Server JDBC connector. For Oracle RDS deployed after Jan, 2020, the default SSL certificate is rds-ca-2019-root. For this scenario, you import rds-ca-2019 into the Enforce Server Java keystore.

Table 4: Steps to secure communications between the Enforce Server and the Oracle database hosted with Amazon RDS describes the process to secure communications between the Enforce Server and the database.

Table 4: Steps to secure communications between the Enforce Server and the Oracle database hosted with Amazon RDS

Step	Action	More info
1	Configure the AWS Oracle RDS SSL connector.	Configuring Oracle RDS Option Group with SSL
2	Configure the server certificate on the Enforce Server.	Configuring the server certificate on the Enforce Server
3	Configure the AWS Oracle RDS for Secure Sockets Layer (SSL) connection over JDBC.	Setting up an SSL connection over JDBC
4	Verify the AWS Oracle RDS certificate usage.	Verifying the Enforce Server-Oracle RDS database certificate usage

Configuring Oracle RDS Option Group with SSL

You enable SSL encryption for an Oracle RDS database instance by adding the Oracle SSL option to the option group associated with an Oracle DB instance. You specify the port you want to communicate over using SSL.

Refer to "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.SSL.html" located in AWS Oracle RDS documentation for steps to complete this process.

Configuring the server certificate on the Enforce Server

After you configure the AWS Oracle RDS Option Group with SSL, you configure the Enforce Server JDBC driver and the server certificate. You import the AWS Oracle RDS certificatte into the Enforce Server Java keystore. Last, you configure the JDBC driver to use the Oracle RDS SSL/TLS connection and port.

NOTE

The following process assumes that the SSL Option is configured with TCP port 2484.

To configure the server certificate on the Enforce Server

1. Locate the `Jdbc.properties` file located at the following location:

   ```
   c:\Program Files\Symantec\Data Loss Prevention\EnforceServer\15.7\protect\config
   ```

   /opt/Symantec/DataLossPrevention/EnforceServer/15.7/protect/config

2. Modify the following communication port and connection information:

   - Update the **jdbc.dbalias.oracle-thin** line to use TCPS.
   - Change the port number to 2484.

   The updated communication port and connection information should display as follows:

   ```
   jdbc.dbalias.oracle-thin=@(description=(address=(host=[oracle host name])
   (protocol=tcps)(port=2484))(connect_data=(sid=protect))
   (SSL_SERVER_CERT_DN="CN=oracleserver"))
   ```

   The following is an example of what the completed communication port and connection information might look like. The information you use differs based on your system. Using the following information as-is may cause the configuration to fail.

   NOTE

   The example uses "protect" for the database SID and 2484 for the TLS port.

   ```
   jdbc.dbalias.oracle-thin=@(description=(address=(host=oracle-rds-dns-name)
   (protocol=tcps)(port=2484))(connect_data=(sid=protect)
   (SSL_SERVER_CERT_DN="C=US,ST=Washington,L=Seattle,O=Amazon.com,OU=RDS,
   CN=oracle-rds-dns-name")))
   ```

   The certificate details provided above are valid for rds-ca-2015-root and rds-ca-2019-root certificates, but you replace the port number with the number used for the SSL port in the option group.

3. Add the certificate to the `cacerts` file that is located on the Enforce Server by completing the following steps:

a	Copy the Oracle RDS certificate (`rds-ca-2015-root.der` or `rds-ca-2019-root.der`) file to `c:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_202\lib\security`. Copy the Oracle RDS certificate `rds-ca-2015-root.der` or `rds-ca-2019-root.der` file to /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202/lib/security

b	Change the directory by running the following command:
	`cd /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202/lib/security/`
	`cd c:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_202\lib\security\`

c	Insert the certificate into the `cacerts` file by running the following command as an administrator:
	Insert the certificate into the `cacerts` file by running the following command as a root user:
	`keytool -import -alias oracleservercert -keystore cacerts -file rds-ca-2015-root.der`
	or
	`keytool -import -alias oracleservercert2019 -keystore cacerts -file rds-ca-2019-root.der`
	Enter the default password when you are prompted: `changeit`.

d	Confirm that the certificate was added by running the following command:
	`keytool -list -v -keystore /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202/lib/security/cacerts -storepass changeit`
	`keytool -list -v -keystore c:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_202\lib\security\cacerts -storepass changeit`

4. Restart all SymantecDLP services.

   About Symantec Data Loss Prevention services

Setting up an SSL connection over JDBC

To set up an SSL connection over JDBC you download the Amazon RDS root CA certificate, convert the certificate format to `.der`, then import the certificate into the keystore.

Refer to "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.SSL.html#Appendix.Oracle.Options.SSL.JDBC" located in AWS Oracle RDS documentation for steps to complete this process.

Verifying the Enforce Server-Oracle RDS database certificate usage

To confirm that certificates are configured correctly and the Enforce Server is communicating with the Oracle RDS database, log on to the Enforce Server administration console. If you can log on, the Enforce Server and database are communicating over a secure communication.

If you cannot log on, verify the SSL Java application connection of `Jdbc.properties`. To confirm the SSL Java application connection, check the listener status on the Oracle RDS. In the listener status, the TCPS protocol and port 2484 should be in use. If the listener status does not display these connection statuses, re-complete the process to enable Oracle RDS group with SSL.

For full details on how to configure SSL/TLS communication between Oracle RDS, and the Enforce Server, see the documentation for AWS Oracle RDS Option Group, available from the *Amazon Relational Database Service User Guide*:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.SSL.html

Upgrading an Enforce Server running in AWS

About upgrading the Enforce Server in Amazon RDS for Oracle

The process to upgrade the Enforce Server in Amazon RDS for Oracle involves confirming that Oracle Amazon RDS is ready for upgrade and upgrading to the latest Enforce Server version.

After you complete the steps to upgrade the Enforce Server in Amazon RDS for Oracle, see the *Symantec Data Loss Prevention Upgrade Guide* available at Related Documents. The guide provides information on completing the upgrade process for other components.

Steps to upgrade the Enforce Server in Amazon RDS for Oracle

Table 5: Upgrading the Enforce Server in Amazon RDS for Oracle

Step	Action	More info
1	Prepare the Amazon RDS for Oracle for a Symantec Data Loss Prevention upgrade.	Preparing the Amazon RDS for Oracle for a Symantec Data Loss Prevention upgrade
2	Upgrade the Enforce Server.	Upgrading the Enforce Server on Windows Upgrading the Enforce Server on Linux

Preparing the Amazon RDS for Oracle for a Symantec Data Loss Prevention upgrade

The following Amazon RDS for Oracle-related preparations must be made before you upgrade the Symantec Data Loss Prevention database schema.

> **NOTE**
>
> The Enforce Server upgrade process does not support a TLS connection to Amazon RDS. Symantec recommends that you run the Upgrade Readiness Tool and complete the Enforce Server upgrade using Amazon RDS on a non TLS listener port. The TLS connection between the previous version Enforce Server and RDS is not migrated during the upgrade. After you complete the upgrade process, re-established TLS communication with RDS. See About securing communications between the Enforce Server and Amazon RDS for Oracle.

Symantec recommends that you prepare for the upgrade, including running the Update Readiness Tool, a few weeks before you plan to complete the upgrade. Preparing helps ensure that any issues that arise can be resolved before the scheduled upgrade.

Table 6: Preparing the Amazon RDS for Oracle for a Symantec Data Loss Prevention upgrade

Step	Action	More info
1	Back up the Amazon RDS for Oracle database before you start the upgrade. You cannot recover from an unsuccessful upgrade without a backup of your Amazon RDS for Oracle database.	See the Symantec Data Loss Prevention Help Center.
2	Set Oracle variables.	Setting variables in the Amazon RDS for Oracle database

Step	Action	More info
3	Prepare to run the Update Readiness Tool.	Preparing to run the Update Readiness Tool for Amazon RDS for Oracle
4	Create the Update Readiness Tool database account.	Creating the Update Readiness Tool database account for Amazon RDS for Oracle
5	Run the Update Readiness Tool for Amazon RDS for Oracle.	Running the Update Readiness Tool for Amazon RDS for Oracle
6	Review update readiness results.	Reviewing update readiness results

Setting variables in the Amazon RDS for Oracle database

You set the ORACLE_HOME, ORACLE_SID, and java CLASSPATH: ORACLE_HOME variables before you begin the upgrade process. If you do not set these variables, you cannot complete the migration process during the Enforce Server upgrade process.

1. Log on as a domain user.
2. In the command prompt, run the following command to set the ORACLE_HOME variable. Confirm your Oracle version and installation path before setting this variable. For example:

   ```
   set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1
   ```

3. Run the following command to set the java CLASSPATH: ORACLE_HOME variable:

   - For Windows:

     ```
     set CLASSPATH=%CLASSPATH%;JAVA_HOME\lib;.;
     echo %CLASSPATH%
     ```

   - For Linux:

     ```
     export CLASSPATH=${CLASSPATH}:.
     echo $CLASSPATH
     ```

Preparing to run the Update Readiness Tool for Amazon RDS for Oracle

Preparing the Update Readiness Tool includes downloading the tool and moving it to the Enforce Server.

1. Obtain the current version of the tool (for both major or minor release versions of Symantec Data Loss Prevention) from Product Downloads at the Broadcom Support Portal.

   The current version of the Update Readiness Tool includes important fixes and improvements, and should be the version that you use before attempting any upgrade.

   Symantec recommends that you download the tool to the `DLPDownloadHome\DLP\15.7\URT` (for Windows) or `DLPDownloadHome/DLP/15.7/URT` (for Linux) directory on the Enforce Server. Create the `URT` folder if it does not already exist.

2. Unzip the tool, then copy the contents of the unzipped folder to the following location on the Enforce Server.

   - Windows: `\Program Files\Symantec\DataLossPrevention\EnforceServer\15.7\Protect\Migrator\URT\`
   - Linux: `opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/Migrator/URT`

     NOTE

     Do not unzip the tool as a folder. The contents of the folder must reside directly in the `URT` folder.

3. Copy `oracle_create_user_aws_oracle_rds.sql` to the to the following location on the Enforce Server:
   - Windows: `..URT\script`
   - Linux: `../URT/script`

   This SQL script creates a schema with necessary privileges to the Amazon RDS for Oracle.

Creating the Update Readiness Tool database account for Amazon RDS for Oracle

You can run the Update Readiness Tool from the command prompt on the Enforce Server host computer.

1. Logon as the RDS Master user.

   NOTE

   The following steps use masteruser for the RDS Master user and password for the password. Enter information specific to your implementation for these values.

2. Run the following script:

   ```
   sqlplus masteruser/password@endpoint_name.rds.amazonaws.com:1521/protect
   ```

3. Run the following script to grant full access to the `DATA_PUMP_DIR` to the "protect" user:

   ```
   SQL> GRANT read,write on DIRECTORY DATA_PUMP_DIR to protect;
   ```

4. Run the following script to logon to the Amazon RDS for Oracle:

   ```
   sqlplus Oracle RDS username/password@endpoint_name.rds.amazonaws.com:1521/RDS Servicename
   ```

   Replace Oracle RDS username, password, and RDS Servicename with information specific to your implementation.

5. Run the following script to create the Update Readiness Tool database account:

   ```
   SQL> @oracle_create_user_aws_oracle_rds.sql
   ```

6. Enter the following information where prompted:
   - `protect` at **Please enter the database username:**
   - `protect` at **Please enter the database user password:**
   - `protect_urt` at **Please enter the database readiness username:**
   - `protect` at **Please enter the database readiness user password:**
   - `endpoint_name.rds.amazonaws.com:1521/protect` at **Please enter the database service name:**

Running the Update Readiness Tool for Amazon RDS for Oracle

Because Amazon RDS for Oracle is fully managed, you run the Update Readiness Tool on the Enforce Server instead of on the database server.

1. Run the following command:

   ```
   java UpdateReadinessTool
   ```

2. Enter the following information when prompted:
   - `protect` at **Please enter the database username**
   - `protect` at **Please enter the database user password**
   - `protect_urt` at **Please enter the database readiness username**
   - `protect` at **Please enter the database readiness user password:**
   - `endpoint_name.rds.amazonaws.com:1521/protect` at **Please enter the database service name:**

After the test completes, you can locate the results in a log file in the `/output` directory. This directory is located where you extracted the Update Readiness Tool. If you do not include [--quick] when you run the tool, the test may take up to an hour to complete. You can verify the status of the test by reviewing log files in the /output directory.

Related Links

Reviewing update readiness results on page 24

Reviewing update readiness results

After you run the Update Readiness Tool, the tool returns test results in a log file.

Table 7: Update Readiness results

Status	Description
Pass	Items that display under this section are confirmed and ready for update.
Warning	If not fixed, items that display under this section may prevent the database from upgrading properly.
Error	These items prevent the upgrade from completing and must be fixed.

Table 8: Details about the Update Readiness tool tests lists certain results of the Update Readiness Tool tests and provides information on resolving errors.

Table 8: Details about the Update Readiness tool tests

Test result	Information
Data Foreign Key Constraint Validation for EndPointProtocolFilter	Resolving the error "Data Foreign Key Constraint Validation for EndPointProtocolFilter"
Start: Index Definition Validation - Invalid Non-Primary Key Indexes INCIDENT_N13	Resolving the error "Start: Index Definition Validation - Invalid Non-Primary Key Indexes INCIDENT_N13"

Related Links

Checking the database update readiness

Resolving the error "Data Foreign Key Constraint Validation for EndPointProtocolFilter"

When running the Update Readiness Tool before an upgrade from Symantec Data Loss Prevention 14.6 to the current version, the tool returns results in its log file with the error below.

```
Start: Data Foreign Key Constraint Validation - [date and time] Data violations are detected on your schema,
 please use the below query(s) to retrieve the invalid data.
SELECT DISTINCT protocolFilterId AS "PROTOCOLFILTERID" FROM ENDPOINTPROTOCOLFILTER
WHERE protocolFilterId IS NULL OR protocolFilterId NOT IN (SELECT acv.protocolFilterId FROM
AgentConfigurationVersion acv WHERE acv.protocolFilterId IS NOT NULL);
End : Data Foreign Key Constraint Validation - elapsed 0s - FAILED (1 violation)
```

Complete the following resolve the error "Data Foreign Key Constraint Validation for EndPointProtocolFilter":

1. Run the following command to create a data backup:

   ```
   create table EndpointProtocolFilter_nomatch as
   select * from EndpointProtocolFilter where protocolFilterId not in (select acv.protocolFilterId FROM
   ```

```
AgentConfigurationVersion acv where acv.protocolFilterId IS NOT NULL);
```

2. Run the following command to confirm the record count:

   ```
   select count(*) from EndpointProtocolFilter where protocolFilterId not in (select acv.protocolFilterId
   FROM AgentConfigurationVersion acv where acv.protocolFilterId IS NOT NULL);
   ```

3. Note the record count.
4. Run the following command to delete data that causes the upgrade to fail:

   ```
   DELETE FROM EndpointProtocolFilter WHERE protocolFilterId NOT IN (SELECT acv.protocolFilterId FROM
    AgentConfigurationVersion acv WHERE acv.protocolFilterId IS NOT NULL);
   ```

5. Confirm that the number of records deleted matches the record count. See step 3. If the record counts do not match, contact Symantec Support.
6. Run the following command to complete the delete operation:

   ```
   commit;
   ```

7. Run the following command to confirm that the number of records match:

   ```
   select count(*) from EndpointProtocolFilter where protocolFilterId not in (select acv.protocolFilterId
   FROM AgentConfigurationVersion acv where acv.protocolFilterId IS NOT NULL);
   ```

Related Links

Reviewing update readiness results on page 24

Resolving the error "Start: Index Definition Validation - Invalid Non-Primary Key Indexes INCIDENT_N13"

Complete the following to resolve the "Start: Index Definition Validation - Invalid Non-Primary Key Indexes INCIDENT_N13" error:

1. Stop all Enforce Server services.
2. Start SQL*Plus.
3. Log on as the protect user.
4. Run the following script:

   ```
   DROP INDEX INCIDENT_N13; CREATE INDEX Incident_n13 ON Incident(messageDate);
   ```

5. Restart all Enforce Server services.

   About Symantec Data Loss Prevention services
6. Run the Update Readiness Tool again.

Related Links

Reviewing update readiness results on page 24

Upgrading the Enforce Server on Windows

The table lists steps to upgrade the Enforce Server on Amazon RDS for Oracle.

Table 9: Upgrading the Enforce Server on Windows

Step	Action	More info
1	Install the Java Runtime Environment	Installing the Java Runtime Environment on the Enforce Server
2	Install the Enforce Server	Installing an Enforce Server
3	Run the Migration Utility	Running the Migration Utility on the Enforce Server

Installing the Java Runtime Environment on the Enforce Server

You install the Java Runtime Environment (JRE) on the Enforce Server before you install the Enforce Server.

To install the JRE

1. Log on (or remote logon) as Administrator to the Enforce Server system on which you intend to install Enforce.
2. Copy `ServerJRE.msi` from your `DLPDownloadHome\DLP\New_Installs\Release` directory to the computer where you plan to install the Enforce Server (for example, move the file to `c:\temp`).
3. Run the `ServerJRE.msi` file to display the **Symantec Data Loss Prevention Server JRE Setup** dialog.
4. Click **Next**.
5. After you review the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.
6. In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**.

   Symantec recommends that you use the default destination directory. References to the "installation directory" in Symantec Data Loss Prevention documentation are to this default location.
7. Click **Install** to begin the installation process.
8. Click **Finish** to complete the process.

Installing an Enforce Server

The instructions that follow describe how to install an Enforce Server on a Windows computer in a two- or three-tier environment. The steps to install the Enforce Server in a single-tier environment are different. Installing a single-tier server

> **NOTE**
>
> If you are running the database in a RAC environment, confirm that the scan host IP for RAC is accessible and the nodes associated with it are all up and running during the install process.

These instructions assume that the `EnforceServer.msi` file and license file have been copied into the `c:\temp` directory on the Enforce Server computer.

> **NOTE**
>
> Enter directory names, account names, passwords, IP addresses, and port numbers that you create or specify during the installation process using standard 7-bit ASCII characters only. Extended (hi-ASCII) and double-byte characters are not supported.

The installation process automatically generates log information saved to a file `MSI*.log` (* is replaced with random characters) in the `%TEMP%` folder. You can change the log file name and location by running the following command with the installation:

```
msiexec /i EnforceServer.msi /L*v c:\temp\enforce_install.log
```

You can complete the installation silently or using a graphical user interface. Enter values with information specific to your installation for the following:

Table 10: Enforce Server installation parameters

Command	Description
`INSTALLATION_DIRECTORY`	Specifies where the Enforce Server is installed. The default location is `C:\Program Files\Symantec\DataLossPrevention`.
`DATA_DIRECTORY`	Defines where Symantec Data Loss Prevention stores files that are updated while the Enforce Server is running (for example, logs and licenses). The default location is `c:\ProgramData\Symantec\DataLossPrevention\EnforceServer\`. **Note:** If you do not use the default location, you must indicate a folder name for the data directory. If you set the data directory to the drive root (for example `c:\` or `e:\`) you cannot successfully uninstall the program.
`JRE_DIRECTORY`	Specifies the path where the JRE resides.
`FIPS_OPTION`	Defines whether to disable (`Disabled`) or enable (`Enabled`) FIPS encryption. The default is disabled.
`SERVICE_USER_OPTION`	Defines whether to create a new service user by entering `NewUser` or using an existing one by entering `ExistingUser`. The default is `ExistingUser`.
`SERVICE_USER_USERNAME`	Defines a name for the account that is used to manage Symantec Data Loss Prevention services. The default user name is “SymantecDLP.”
`SERVICE_USER_PASSWORD`	Defines the password for the account that is used to manage Symantec Data Loss Prevention services.
`ORACLE_HOME`	Defines the Oracle Home Directory. For example, use `c:\oracle\product\12.2.0.1\db_1` to define the home directory if you use the Oracle 12.2.0.1 database.
`ORACLE_HOST`	Defines the IP address of the Oracle server computer. If you are running the Oracle database in a RAC environment, use the scan host IP address for the host, not the database IP address. Confirm that the scan host IP for RAC is accessible and that all of the nodes associated with it are running during the installation process.
`ORACLE_PORT`	Defines the Oracle listener port (typically 1521).
`ORACLE_USERNAME`	Defines the Symantec Data Loss Prevention database user name.
`ORACLE_PASSWORD`	Defines the Symantec Data Loss Prevention database password.
`ORACLE_SERVICE_NAME`	Defines the database service name (typically “protect”).

The following is an example of what the completed command might look like. The command you use differs based on your implementation requirements. Using the following command as-is may cause the installation to fail.

```
        msiexec /i EnforceServer.msi /qn /norestart
INSTALLATION_DIRECTORY="C:\Program Files\Symantec\DataLossPrevention"
DATA_DIRECTORY="C:\ProgramData\Symantec\DataLossPrevention\EnforceServer"
JRE_DIRECTORY="C:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_202"
FIPS_OPTION=Disabled
SERVICE_USER_OPTION=ExistingUser
SERVICE_USER_USERNAME=protect
SERVICE_USER_PASSWORD=Password
ORACLE_HOST=[IP or host name]
ORACLE_PORT=1521
ORACLE_USERNAME=protect
```

```
ORACLE_PASSWORD=Password
ORACLE_SERVICE_NAME=protect
```

1. Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Loss Prevention installation process.
2. Log on (or remote logon) as Administrator to the Enforce Server system where you intend to run the Migration Utility.
3. Go to the folder where you copied the `EnforceServer.msi` file (`c:\temp`).
4. Double-click `EnforceServer.msi` to execute the file.

   NOTE

   The installation process automatically generates log information saved to a file MSI*.log (replace * with random characters) in the `%TEMP%` folder. You can change the log file name and location by running the following command with the installation:

   ```
   msiexec /i EnforceServer.msi /L*v c:\temp\enforce_install.log
   ```

   After you complete the Enforce Server installation, you can find the log file at `c:\temp`.

5. In the **Welcome** panel, click **Next**.
6. After you review the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.
7. In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**. The default installation directory is:

   ```
   c:\Program Files\Symantec\DataLossPrevention\
   ```

   Symantec recommends that you use the default destination directory. References to the "installation directory" in Symantec Data Loss Prevention documentation are to this default location.

8. In the **Data Directory** panel, accept the default data directory, or enter an alternate directory, and click **Next**. The default data directory is:

   ```
   c:\ProgramData\Symantec\DataLossPrevention\
   ```

   NOTE

   If you do not use the default location, you must indicate a folder name for the data directory (for example, `c:\enforcedata`). If you set the data directory to the drive root (for example `c:\` or `e:\`) you cannot successfully uninstall the program.

9. In the **JRE Directory** panel, accept the default JRE location (or click **Browse** to locate it), and click **Next**.
10. In the **FIPS Cryptography Mode** panel, select whether to disable or enable FIPS encryption.

    About FIPS encryption

11. In the **Service User** panel, select one of the following options.

    - **New Users**: Select this option to create the Symantec Data Loss Prevention system account user name and password and confirm the password. This account is used to manage Symantec Data Loss Prevention services. The default user name is “SymantecDLP.”

      NOTE

      The password you enter for the System Account must conform to the password policy of the server. For example, the server may require all passwords to include special characters.

    - **Existing Users**: Select this option to use an existing local or domain user account.

    Click **Next**.

12. In the **Oracle Database** panel, enter details about the Oracle database server. Specify one of the following options in the **Oracle Database Server** field:

Host	Enter host information based on your Symantec Data Loss Prevention installation: • Single- and two-tier installation (Enforce and Oracle servers on the same system): The Oracle Server location is `127.0.0.1`. • Three-tier installation (Enforce Server and Oracle server on different systems): Specify the Oracle server host name or IP address. To install into a test environment that has no DNS available, use the IP address of the Oracle database server. If you are running the Oracle database in a RAC environment, use the scan host IP address for the host, not the database IP address. Confirm that the scan host IP for RAC is accessible and that all of the nodes associated with it are running during the installation process.
Port	Enter the **Oracle Listener Port**, or accept the default.
Service Name	Enter the database service name (typically “protect”).
Username	Enter the Symantec Data Loss Prevention database user name.
Password	Enter the Symantec Data Loss Prevention database password.

If your Oracle database is not the correct version, you are warned and offered the choice of continuing or canceling the installation. You can continue and upgrade the Oracle database later.

NOTE

Symantec Data Loss Prevention requires the Oracle database to use the AL32UTF8 character set. If your database is configured for a different character set, you are notified and the installation is canceled. Correct the problem and re-run the installer.

13. Click **Next**.
14. In the **Additional Locale** panel, select an alternate locale, or accept the default of None, and click **Next**.

Locale controls the format of numbers and dates, and how lists and reports are alphabetically sorted. If you accept the default choice of None, English is the locale for this Symantec Data Loss Prevention installation. If you choose an alternate locale, that locale becomes the default for this installation, but individual users can select English as a locale for their use.

See the *Symantec Data Loss Prevention Administration Guide* for more information on locales.

15. Click **Install**.

The installation process can take a few minutes. After a successful installation, a completion notice displays.

NOTE

If you are upgrading from Symantec Data Loss Prevention version 15.1 or earlier, services are created but remain in a disabled state until you run the Enforce Server Migration Utility.

16. Restart any antivirus, pop-up blocker, or other protection software that you disabled before starting the Symantec Data Loss Prevention installation process.
17. Run the Upgrade Readiness tool to confirm that the Oracle database is ready to be migrated to the new instance.
18. Verify that the Enforce Server is properly installed.

Verifying an Enforce Server installation

Running the Migration Utility on the Enforce Server

The Migration Utility moves data, configurations, and custom files (data profiles, plug-ins, and incidents) to the 15.7 instance. The migration utility also stops previous version services and starts new version services.

Before you run the Migration Utility, run the Update Readiness Tool to confirm that the database is ready for migration.

You can migrate data silently or using interactive mode.

- Silent mode
- Interactive mode

Silent mode

Run the following command in an elevated command prompt:

```
EnforceServerMigrationUtility
-silent
-sourceVersion="previous version"
```

Where *previous version* represents the previous, active version (for example, use `-sourceVersion=15.5` to migrate from Symantec Data Loss Prevention version 15.5).

Interactive mode

1. Log on (or remote logon) as Administrator to the Enforce Server system where you intend to run the Migration Utility.
2. Use the command prompt to navigate to the following directory:

   `C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.7\Protect\Migrator`
3. Run the Migration Utility: `EnforceServerMigrationUtility.exe`.
4. Select the active Symantec Data Loss Prevention version to migrate and press **Enter**.

   The Migration Utility stops services on the previous Symantec Data Loss Prevention version and migrates data, configuration, and custom files to the new version. When the process completes, a message displays indicating that the migration has finished.

   > **NOTE**
   >
   > The previous version is still installed but all services are in a disabled state. You can restart these services if you have rolled-back to a previous version. If you uninstall a version 15.1.x system, the service_user is removed.
5. If migration fails, review the Enforce Server `MigrationUtility.log` located at `C:\ProgramData\Symantec\DataLossPrevention\EnforceServer\15.7\logs\debug\` for more details.

Upgrading the Enforce Server on Linux

The table lists steps to upgrade the Enforce Server on Amazon RDS for Oracle.

Table 11: Upgrading the Enforce Server on Linux

Step	Action	More info
1	Install the Java Runtime Environment.	Installing the Java Runtime Environment on the Enforce Server
2	Install the Enforce Server	Installing an Enforce Server
3	Run the Migration Utility	Running the Migration Utility on the Enforce Server

Installing the Java Runtime Environment on the Enforce Server

You install the Java Runtime Environment (JRE) on the Enforce Server before you install the Enforce Server.

1. Log on as root to the Enforce Server system on which you intend to install Enforce.
2. Copy `ServerJRE.zip` from your `DLPDownloadHome/DLP/New_Installs/Release` directory to the computer where you plan to install the Enforce Server.
3. Unzip the file contents (for example, unzip to `/opt/temp`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
4. Install the JRE by running the following command:

   ```
   ./install.sh -t serverjre
   ```

   Parameters for install.sh

Installing an Enforce Server

The instructions that follow describe how to install an Enforce Server on a Linux computer.

These instructions assume that the `EnforceServer.zip` file and license file have been copied into the `/opt/temp` directory on the Enforce Server computer.

1. Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Loss Prevention installation process.
2. Log on as root to the Enforce Server system on which you intend to install Enforce.
3. Navigate to the directory where you copied the `EnforceServer.zip` file (`/opt/temp/`).
4. Unzip the file to the same directory (`/opt/temp/`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
5. Confirm file dependencies for RPM files by running the following command:

   ```
   rpm -qpR *.rpm
   ```

   You can also specify a file to confirm by running the following command:

   ```
   rpm -qpR .rpm-file
   ```

   If the command indicates that dependancies are missing, you can use YUM repositories to install them. Use the following command:

   ```
   yum install repo
   ```

   Replace repo with the repository package name.
6. Install the Enforce Server by running the following command:

   ```
   ./install.sh -t enforce
   ```

   Parameters for install.sh

   NOTE

   If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.

7. Restart any antivirus, pop-up blocker, or other protection software that you disabled.
8. Run the Update Readiness Tool to confirm that the Oracle database is ready to be migrated to the new instance, if you haven't run it already.
9. Start the migration process.

Running the Migration Utility on the Enforce Server

The Migration Utility moves data, configurations, and custom files (data profiles, plug-ins, and incidents) to the 15.7 instance. The migration utility also stops previous version services and starts new version services.

After you install the version 15.7 Enforce Server, you use the Migration Utility to migrate data to the new instance. Before you start the migration, use the Upgrade Readiness tool to confirm that the Oracle database is ready for migration.

You can migrate data silently or using interactive mode.

Migrate silently

Migrate using interactive mode

The process to migrate data does not move all plug-ins. Migrating plug-ins

> **NOTE**
>
> Before you run the Migration Utility, you must switch to `root` user.

Migrate silently

Use the following command to complete the migration silently:

```
./EnforceServerMigrationUtility
-silent
-sourceVersion="<previous version>"
-jreDirectory="/opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202"
```

Where <previous version> is the previous version number of the previous active version installation. The path /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202 points to the current JRE location.

Migrate using interactive mode

1. Open the command prompt window.
2. Switch user to root: `su - root`.
3. Go to the following directory:

   ```
   opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/Migrator
   ```
4. Run the Migration Utility by running the following command:

   ```
   ./EnforceServerMigrationUtility
   ```

   The Migration Utility stops services on the previous Symantec Data Loss Prevention version and migrates data, configuration, and custom files to the new version. When the process completes, a message displays indicating that the migration has finished.
5. Confirm the JRE directory that displays.

   If no JRE displays, install the JRE.

   Installing the Java Runtime Environment on the Enforce Server

6. Select the active Symantec Data Loss Prevention version to migrate and press **Enter**.

   NOTE

   If you uninstall the previous version, the service_user is removed.

7. If migration fails, review the Enforce Server migration logs in `MigrationUtility.log` located at `/var/log/Symantec/DataLossPrevention/EnforceServer/15.7/debug/` for more details.

Copyright statement

Copyright statement

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Symantec™

A Division of Broadcom