Trend Micro Deep Security on the AWS Cloud

Quick Start Reference Deployment

Trend Micro Software Development Team
AWS Quick Start Reference Team

June 2015
Last update: May 2016 (revisions)

Contents

About This Guide

Trend Micro Deep Security is a host-based security product that provides Anti-Malware, Host Firewall, Intrusion Prevention, File Integrity Monitoring, Log Inspection, Web Application Firewalling, and Content Filtering modules in a single agent running in the guest operating system.

This Quick Start reference deployment guide describes how to deploy Trend Micro Deep Security version 9.6 on the Amazon Web Services (AWS) cloud. It contains links to AWS CloudFormation templates that automate this deployment as well as additional supporting information.

This guide covers how to deploy Trend Micro Deep Security using these templates. It does not cover other aspects of administering Deep Security. For information about administering Deep Security, see the Trend Micro Deep Security Help Center.

Quick Starts are automated reference deployments for key enterprise workloads on the AWS cloud. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

Overview

Before You Begin

This document assumes that you have used AWS before and are familiar with AWS services. If you are new to AWS, see the Getting Started section of the AWS documentation. You should also be familiar with the following AWS technologies:

- Amazon VPC – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- Amazon EC2 – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.

- AWS CloudFormation – AWS CloudFormation enables you to create and provision AWS infrastructure components reliably and predictably, using a JSON scripting environment. This Quick Start uses AWS CloudFormation templates to configure and automate the Trend Micro Deep Security deployment.

- Amazon RDS - Amazon Relational Database Service (Amazon RDS) is a web service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

Cost and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start. There is no additional cost for using the Quick Start. The cost of the resources created by the Quick Start varies based on how many instances you want to protect. The cost of deployment starts at $2.48 an hour. (This estimate is based on December 2015 prices. Prices are subject to change. See the pricing pages for each AWS service you will be using in this Quick Start for full details.)

Because this Quick Start uses Trend Micro AMIs from the AWS Marketplace, you must be subscribed to Trend Micro Deep Security for AWS Marketplace before you launch the Quick Start. There are two licensing options: Per Protected Instance Hour and Bring Your Own License (BYOL). See step 2 in the deployment section for details and links.

Architecture

This Quick Start will set up Deep Security to protect instances in the Amazon VPC where the Deep Security Manager is deployed. You can subsequently modify your deployment to protect instances across your entire AWS infrastructure. For free assistance, please contact aws@trendmicro.com.

The Quick Start builds the following environment in an existing Amazon VPC.

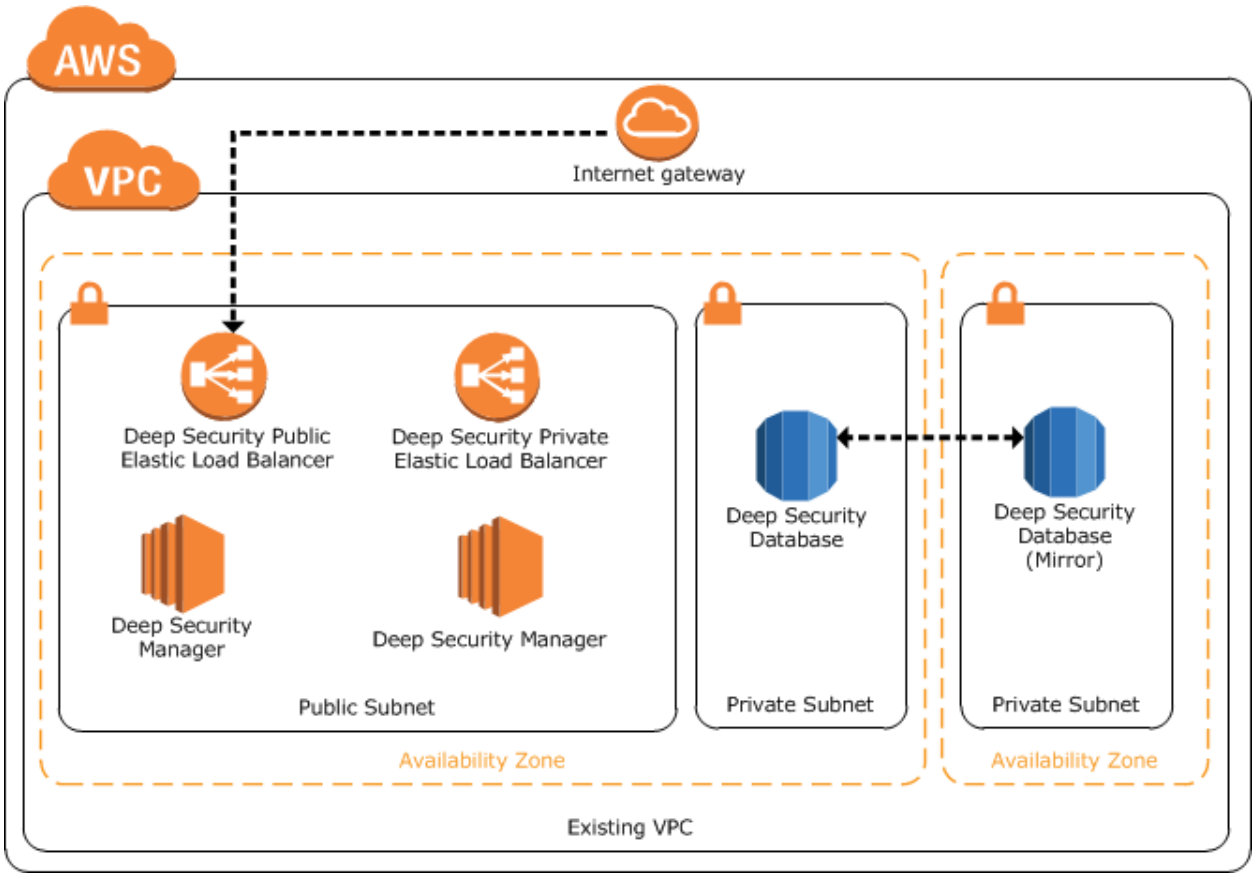


Figure 1: Trend Micro Deep Security Architecture on AWS

Best Practices

The architecture built by this Quick Start supports AWS best practices for high availability and security:

- The Amazon RDS database server used by the Deep Security Manager is deployed across two Availability Zones (where available), providing high availability at the database layer.

- The AWS security groups created by the template are configured to only allow traffic that is required.

Automated Deployment

The AWS CloudFormation templates provided with this Quick Start automate the deployment of Trend Micro Deep Security on the AWS cloud.

Follow the step-by-step instructions in this section to subscribe to Trend Micro Deep Security, customize the Quick Start template, and deploy the software into your account.

Before you launch the Quick Start, you must set up an Amazon VPC in your AWS account and subscribe to Trend Micro Deep Security in the AWS Marketplace.

Step 1. Set up an Amazon VPC

The AWS Quick Start deploys Trend Micro Deep Security into an existing Amazon VPC. Before you launch the Quick Start you must create an Amazon VPC that has two private subnets in different Availability Zones, and one public subnet with an attached Internet gateway, as shown in Figure 2.

> **Important** Although it is possible to use the Quick Start to deploy Deep Security into a default Amazon VPC with all public subnets, this is **not** recommended because of the large attack surface it creates.

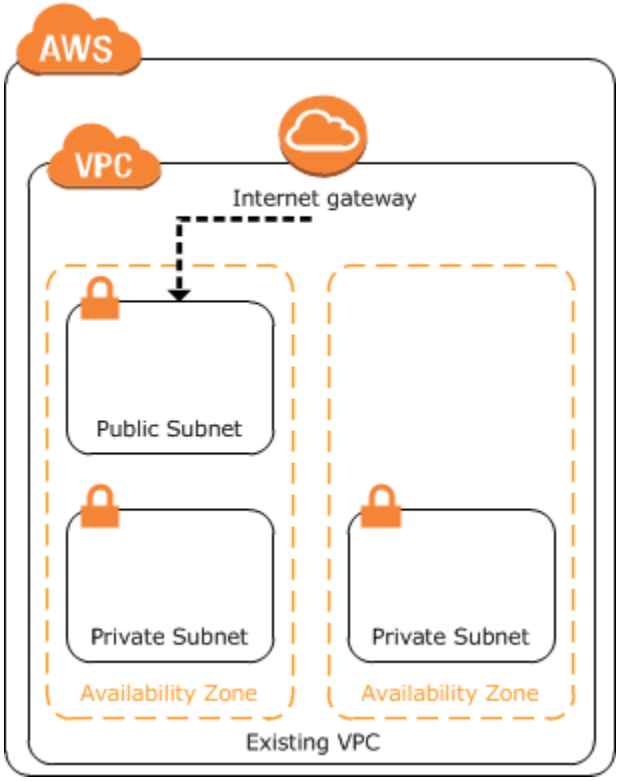


Figure 2: Prerequisite Amazon VPC Architecture

Step 2. Subscribe to Trend Micro Deep Security

The AWS Quick Start uses Amazon Machine Images (AMIs) from the AWS Marketplace. Before you launch the Quick Start, you must subscribe to Trend Micro Deep Security from the AWS Marketplace.

There are two available licensing options. To subscribe, use the following links to open the AWS Marketplace page for the licensing option of your choice:

- Per Protected Instance Hour: A consumption-based option that allows you to pay hourly per protected instance. Your costs will be determined by the number of instances you are protecting each hour, and will show up on your AWS bill. For current prices, please visit the AWS Marketplace page for this licensing option.

—or—

- Bring Your Own License (BYOL): A perpetual licensing option for organizations that prefer traditional procurement. Please contact Trend Micro for a license key at aws@trendmicro.com.

> **Note** The Quick Start is designed to support deployment of up to 2,000 protected instances. If you are protecting more than 2,000 instances, please contact aws@trendmicro.com for free assistance with additional deployment options.

Step 3. Deploy the Quick Start

In this step, you will launch an AWS CloudFormation template that deploys Trend Micro Deep Security into your existing Amazon VPC.

1. Sign in to your AWS account.
2. Use one of the following buttons to launch the AWS CloudFormation template. Choose the Per Protected Instance Hour template or the Bring Your Own License (BYOL) template, depending on the subscription you selected in step 2.

Launch (Per Protected Instance) **Launch (Bring Your Own License)**

The template is launched in the US East (N. Virginia) region by default. You can change the region by using the region selector in the navigation bar.

This stack takes approximately one hour to create.

> **Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment, and licensing fees for Trend Micro Deep Security. There is no additional cost for using this Quick Start. See the pricing pages for each AWS service you will be using in this Quick Start for full details.

You can also download the template to use it as a starting point for your own implementation:

- AWS CloudFormation template for Per Protected Instance Hour option
- AWS CloudFormation template for BYOL option

3. On the **Select Template** page, keep the default URL for the AWS CloudFormation template, and then choose **Next**.
4. On the **Specify Details** page, provide the details about your Amazon VPC and how you want Deep Security to be deployed in it.

   Both templates provide the following parameters:

Parameter	Default	Description
Administrator username for Deep Security	MasterAdmin	The user name used for the Deep Security administrator.
Administrator password for Deep Security	*Requires input*	The password used for the Deep Security administrator.
EC2 Key Pair for SSH access	*Requires input*	The key pair that will be used to launch the EC2 instances that contain the Deep Security Manager. This key pair can be used to create an SSH connection to your Deep Security Manager.
VPC for Deep Security Components	*Requires input*	The Amazon VPC where the Quick Start resources will be deployed. This VPC must contain two private subnets and one public subnet with a connected Internet gateway.
Public Subnet for Deep Security Managers	*Requires input*	The subnet to deploy the Deep Security Manager and load balancers in. This subnet must in the Amazon VPC specified by the **VPC for Deep Security Components** parameter and must be a public subnet with an attached Internet gateway.
Primary private subnet for RDS	*Requires input*	The subnet where the Amazon RDS database will be deployed. This subnet must be in the Amazon VPC specified by the **VPC for Deep Security Components** parameter. It is highly recommended that this be a private subnet.
Secondary private subnet for RDS	*Requires input*	The subnet where the Amazon RDS database mirror will be deployed. This subnet must be in the Amazon VPC specified by the **VPC for Deep Security Components** parameter. It must also be in a separate Availability Zone from the

Parameter	Default	Description
		primary private subnet for RDS. It is highly recommended that this be a private subnet.

The BYOL template requires the following additional information:

Parameter	Default	Description
Choose the backend database	Oracle	The database you want to use for Deep Security. You can choose Oracle or Microsoft SQL Server.
RDS Instance ID	*Requires input*	The Amazon RDS instance identifier. This must be unique in your AWS account and can only contain letters. The database instance identifier is case-insensitive but is stored as lowercase.
Administrator username for RDS Instance	dsadmin	The user name used for the Amazon RDS administrator account.
Administrator password for RDS Instance	*Requires input*	The password used for the Amazon RDS administrator account.
Deep Security License Key. May be left default to enter key after deployment	*Optional*	Enter a license key, if you have one. If you would like to deploy Deep Security as a trial, you can leave this field blank.

The Per Protected Instance Hour template requires the following additional information:

Parameter	Default	Description
Number of instances you expect to protect with Deep Security Agents	*Requires input*	The number of instances you want to protect with Deep Security.

When you finish reviewing and customizing the parameters, choose **Next**.

5. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources. Deep Security requires this access to be able to see your AWS instances and protect them.

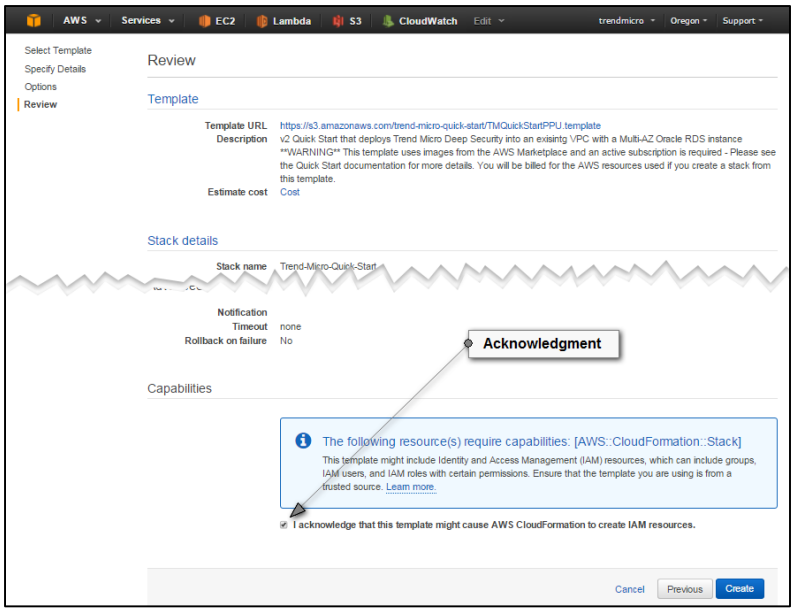


Figure 3: Acknowledging the Creation of IAM Resources

7. Choose **Create** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Trend Micro Deep Security deployment is ready.

Step 4. Log in to the Deep Security Manager Console

The **Outputs** tab of the AWS CloudFormation stack provides a URL to the Deep Security Manager web interface. Choose this link and log in using the user name and password you supplied during the launch of the template.

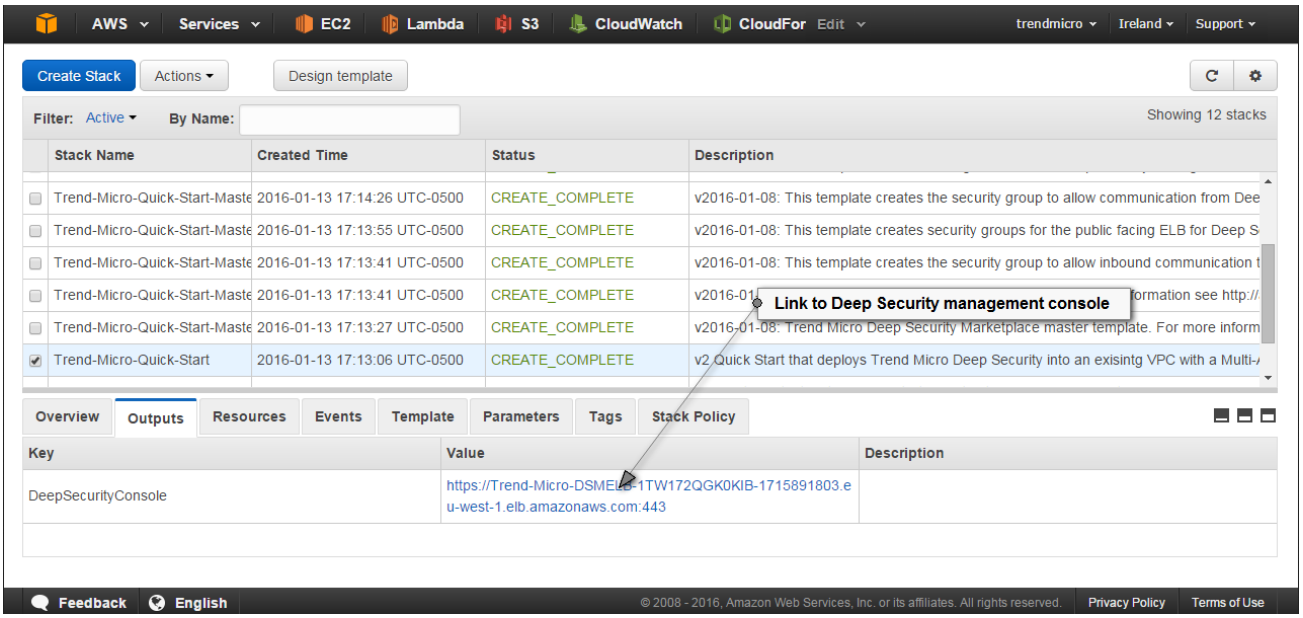


Figure 4: Choosing the Link to Deep Security Manager Console

Your browser may display a warning when you try to enter the console. This is because the Elastic Load Balancing (ELB) load balancer used by the Deep Security Manager is initially configured to use a self-signed certificate for HTTPS connections. For more information and instructions for updating the load balancer certificate, see the appendix.

Step 5. Deploy Trend Micro Deep Security Agent to New Instances

Now that you have Trend Micro Deep Security in your AWS cloud, you can start protecting your instances. For information on how to deploy agents, visit the Trend Micro Deep Security Help Center.

Additional Resources

AWS services

- AWS CloudFormation
  http://aws.amazon.com/documentation/cloudformation/
- Amazon EC2
  http://aws.amazon.com/documentation/ec2/
- Amazon Relational Database Service (RDS)
  http://aws.amazon.com/documentation/rds/
- Amazon VPC
  http://aws.amazon.com/documentation/vpc/

Trend Micro Deep Security resources

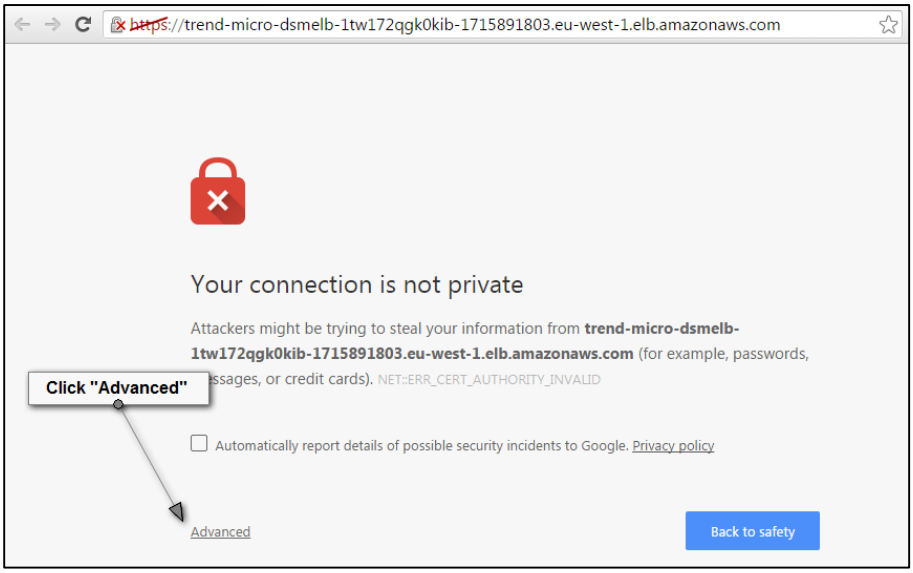
- Deep Security Help Center
  https://help.deepsecurity.trendmicro.com/hc/en-us
- Deep Security in the AWS Marketplace—Per Protected Instance Hour subscriptions
  https://aws.amazon.com/marketplace/pp/B01AVYHVHO
- Deep Security in the AWS Marketplace—Bring Your Own License (BYOL) subscriptions
  https://aws.amazon.com/marketplace/pp/B00OCI4H82/ref=dtl_recsim_B00OCI4J0I_B00OCI4H82_2
- More information on Deep Security on the AWS cloud
  http://aws.trendmicro.com

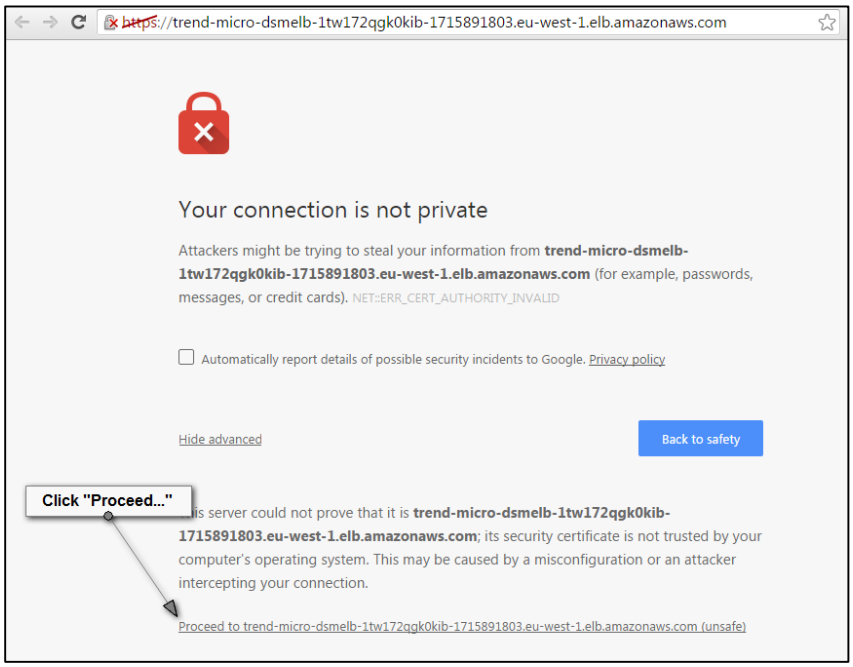
Quick Start reference deployments

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

Appendix: Updating the Load Balancer Certificate

The Elastic Load Balancing (ELB) load balancer used by the Deep Security Manager is initially configured to use a self-signed certificate for HTTPS connections. Your browser may give you an error when you try to access the console. This is expected until you update the load balancer certificate. You can proceed through to the management console.





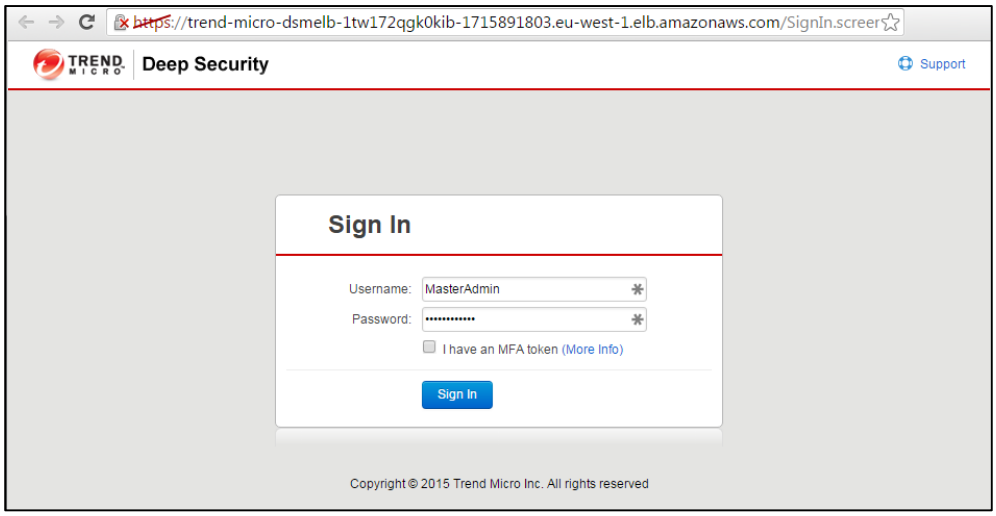


Figure 5: Accessing the Deep Security Management Console

Deep Security is meant to run as part of your core infrastructure. As a result, its attack surface should be minimized. The Quick Start helps reduce this attack service by:

1. Using Security Groups to restrict traffic to only that which is needed.
2. Deploying a Deep Security Agent on the manager instance to protect it from attack.
3. Leveraging the robust role-based access controls available within the platform to ensure that only valid users have access to the platform.

In the initial configuration the Deep Security Manager is configured to use a public load balancer to allow it to easily protect instances in AWS regions and AWS accounts other than the ones the Deep Security Manager is deployed in. If you do not require this functionality and do not require the Deep Security Manager console to be accessible from the internet it is recommended to re-configure the Deep Security Manager to use a private load balancer to further reduce the attack surface. You can also setup VPC Peering if you would like to use a private load balancer and still protect instances outside of the VPC where the Deep Security Manager is deployed.

If you are using the Quick Start as the basis of a production deployment and not as a proof of concept, we strongly recommend that you update the self-signed certificate to a certificate that is signed by a trusted Certificate Authority.

> **Note** In order to obtain a signed certificate, you will be required by the Certificate Authority to specify a formal subdomain (for example, deepsecurityconsole.mycompany.com) and use this to access the Deep Security load balancer.

To update the security certificate of the load balancer, follow these steps:

1. Register a domain name that you will use to access the Deep Security Manager console.
2. Obtain a certificate for this domain from a trusted Certificate Authority.
3. Add the certificate to your certificate store. Instructions on how to do this can be found in the Identity and Access Management documentation.
4. Update the DNS settings of the load balancer to use the new domain name. Detailed instructions on how to do that can be found in the Elastic Load Balancing documentation.
5. Replace the SSL certificate of the load balancer. Detailed instructions on how to do that can be found in the Elastic Load Balancing documentation.

Send Us Feedback

We welcome your questions and comments. Please post your feedback on the AWS Quick Start Discussion Forum. For any problems, questions, or comments, please contact aws@trendmicro.com.

Document Revisions

Date	Description
May 2016	Added Per Protected Instance Hour billing option
February 2016	Updated templates to support latest versions of SQL Server and Trend Micro AMIs, updated instance types to M4 where available, added support for the Asia Pacific (Seoul) region, improved performance
January 2016	Simplified templates and updated Quick Start for deployment on existing Amazon VPC architectures
October 2015	Updated for Deep Security version 9.6
June 2015	Initial publication

Notices

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

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