Auto deploy Sophos Server Agents onto AWS Instances using AWS Lambda and AWS Systems Manager

For customers that wish to automatically deploy the Sophos Central Server agents onto AWS there are a few currently supported methods detailed in the below KB. The methods described take advantage of start up scripts which can be used to ensure that new EC2 Instances are launched with the Sophos Server agents. The problem for some larger customers is that they may not have full control of all of their AWS accounts, and so their users may be able to launch EC2 instances without their knowledge, leading to decreased host security across their estate. To address the issue we helped a customer use the below procedure which relies on some AWS alerting and automation services, and uses the customers' unique Sophos Central agent download URL's. Please note that this is not an officially supported method at this time so is provided 'as is'.

https://community.sophos.com/kb/en-us/125510#How%20do%20I%20deploy%20Sophos%20Server%20Protection%20agents%20onto%20my%20EC2%20instances?

Step-by-step guide

Notes:

The Python script is designed to run in AWS Lambda and will not work elsewhere.

This is an AWS Lambda job in Python to automatically deploy Sophos Server agents to newly-launched EC2 instances using the AWS SSM Service and Sophos provided SSM Documents.

The job requires that the EC2 instance have the SSM (EC2 Simple System Manager) agent installed, the agent must have a role attached with necessary SSM permissions, and the instance must show up as 'managed' in the Systems Manager section. For details on this, see https://docs.aws.amazon.com/ssm/latest/APIReference/Welcome.html. The easiest way to do this is with userdata at instance launch: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/install-ssm-agent.html

The Lambda job is triggered by a CloudWatch event every time a new instance enters the running state. The job checks to make sure that the SSM agent is running. It then uses SSM to install and start the Sophos agent.

The file names used are referred to across the Lambda function and SSM Documents. For this reason it is suggested that you copy/paste the exact file names shown below when creating the Lambda function and SSM Documents.

Installation Files

SophosServerAgentAutoDeployLambdaSSM.zip

Included files are:

1. **README**
2. **SophosLambdaDeploySSMDocs.py** (Lambda Python 3.7 function)
3. **SophosSSMAgentsInstallDocument** (SSM document that Lambda function calls which then determines platformType and based on that calls Linux or Windows Documents)
4. **SophosSSMAgentInstallLinux** (SSM Document that downloads and installs Sophos Linux Server agent. *****Important***** You must replace default URL string with unique Sophos Central Linux download URL https://central.sophos.com/manage/server/downloads)
5. **SophosWindowsAgentInstall** (SSM Document that downloads and installs Sophos Linux Server agent. *****Important***** You must replace default URL string with unique Sophos Central Linux download URL https://central.sophos.com/manage/server/downloads)

Instructions:

1. Go to the AWS Lambda section of your AWS Console and copy the contents of the included Lambda file named **SophosLambdaDeploySSMDocs.py** to create a new Python 3.7 runtime function. For the **IAM role**, use or create a new custom role that has both SSM and basic Lambda execution permissions. Create a **Trigger** for the function that uses CloudWatch Events, a new rule, an Event Pattern with EC2, Instance state change notification, and a state of '**running**'.

2. Go to the AWS Systems Manager section of your AWS Console and create a new **Command** Document named '**SophosSSMAgentsInstallDocument**', and copy the contents from the supplied file of the same name. Nothing needs to be changed in this document so it can be saved after copying the content and ensuring the name is correct and exactly matches what is called in the Lambda script.

3. Create a new Command Document named called '**SophosSSMAgentInstallLinux**', and copy the contents from the supplied file of the same name. You must replace the 'xxxxx' in the URL section with your Sophos Central Linux download URL.

4. Create a new Command Document named called '**SophosWindowsAgentInstall**', and copy the contents from the supplied file of the same name. You must replace the 'xxxxx' in the URL section with your Sophos Central Windows download URL.

To test, restart an existing EC2 instance that is managed by SSM, or create a new Linux or Windows EC2 instance that is configured for SSM management upon boot. The Lambda function should trigger once the Instance state changes to 'running', and that should then launch the SSM documents, which can be observed in the Systems Manager '**Run Command**' section, by looking at the **CloudWatch Log stream**. After a few moments the new Servers should show up in the Central account Server section.

Related articles

- Auto deploy Sophos Server Agents onto AWS Instances using AWS Lambda and AWS Systems Manager