Running Pre-approved SAINT Scans in AWS

Amazon's Vulnerability and Penetration Testing policy formerly required pre-approval for all scans originating from or targeting any AWS resources. To help customers comply with this requirement, SAINT offered an Amazon Machine Image (AMI) which was pre-approved for scanning. Although pre-approval is no longer required, this AMI can still be used as a convenient way to connect a node which is pre-configured to scan its own VPC.

In order to ensure that the pre-approved SAINT AMI is used as intended, it enforces certain terms and conditions, as described in the following table.

The pre-approved SAINT AMI…

✓	Can be used as a scan node controlled by another SAINT installation. (See next section)	X	Cannot be used as a standalone scanner or a management console. (Has no interface for direct access.)
✓	Can scan Amazon EC2 instances.	X	Cannot be used to scan targets outside of Amazon EC2.
✓	Can scan targets in its own Virtual Private Cloud (VPC).	X	Cannot scan targets outside its own region or VPC.
✓	Can scan targets of type medium or larger.	X	Cannot scan small, micro, or nano instances.
✓	Can run vulnerability scans.	X	Cannot run exploits or penetration tests.

The SAINT Management Console

The SAINT distributed scanning architecture consists of at least two components: a SAINT management console, and one or more scanners. The management console also typically includes a scanner (ex. localnode). Each scanner connects to the management console upon start-up, and is then controlled only through the management console's web interface. The pre-approved SAINT AMI can ONLY act as one of the scanners. AWS policy precludes the pre-approved scanning AMI from being run as a standalone scanner or acting as a management console.

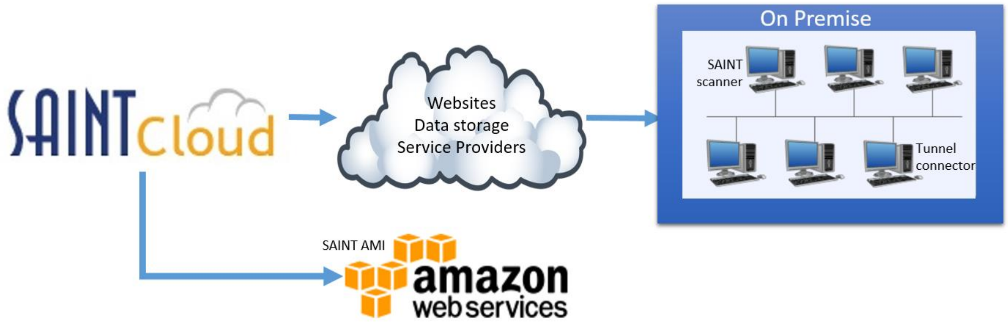
Before launching the pre-approved SAINT AMI, a separate SAINT management console should already be running. You will need to specify the IP address of the management console when you launch the pre-approved AMI to configure secure connectivity from the pre-approved scanner. There are several options available for deploying a SAINT product as the management console:

1. SAINT's non-pre-approved marketplace AMI – as described in SAINT Amazon Machine Image Setup Guide, this option is the recommended machine to use if the approach is to deploy a total solution within AWS. Note that this AMI must be running before you enable the pre-approved AMI, to ensure the

pre-approved scanner can make a secure connection to its “manager” to facilitate scan setup and execution.

2. SAINTCloud – SAINT’s cloud-based scan solution is implemented outside of AWS, but can be licensed to connect to the pre-approved SAINT AMI in AWS. This option enables customers to scan within the AWS environment, but also eliminate the licensing, costs and maintenance of an AWS instance to run the management console. Notify your Sales representative prior to deploying this solution, to ensure this hosted solution can be configured to communicate to your pre-authorized AMI.
3. Locally-owned SAINT Security Suite installation – This option includes any accessible SAINT Security Suite installation running as a manager - deployed on premise, in a data center or other locations.

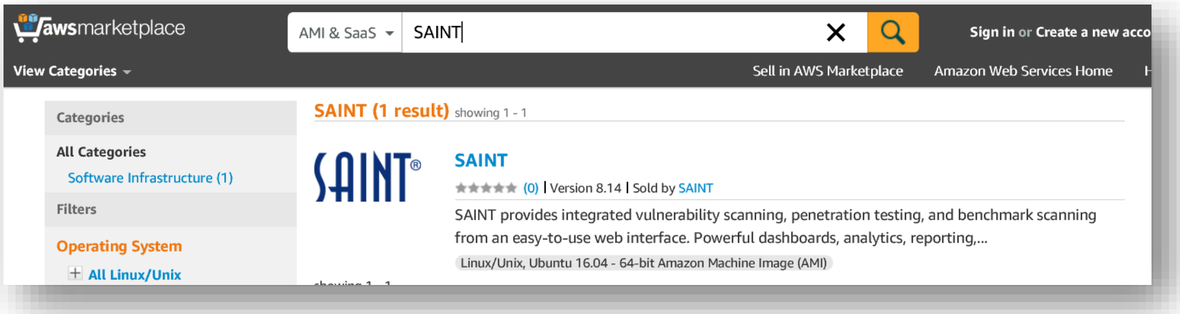
The example illustrates a hybrid scanning architecture, using SAINTCloud as the central management console, a pre-approved SAINT AMI for scanning securely into AWS EC2 instances, and distributed scanners on premise locations:



Launching a Pre-approved SAINT Instance

1. If the SAINT management console which will control this instance is running in AWS, modify the management console’s security groups to allow the pre-approved instance to connect as follows:
    a. From the AWS console, go to *EC2*, then *Instances.* Click on the security group name for the management console instance.
    b. Choose *Edit Inbound Rules* from the Actions menu.
    c. Add a custom TCP rule for port 5252. Under *Source*, choose the *Custom* type, and enter either the CIDR address of the pre-approved instance’s VPC (172.31.0.0/16 for the default VPC), or the name of an existing security group which will be assigned to the pre-approved instance.

2. It is recommended that the pre-approved SAINT instance be launched using the provided Cloud Formation Template. To launch the instance using the Cloud Formation Template, log into AWS and go to the Amazon marketplace.
3. Type “SAINT” in the search box.



SAINT (1 result) showing 1 - 1

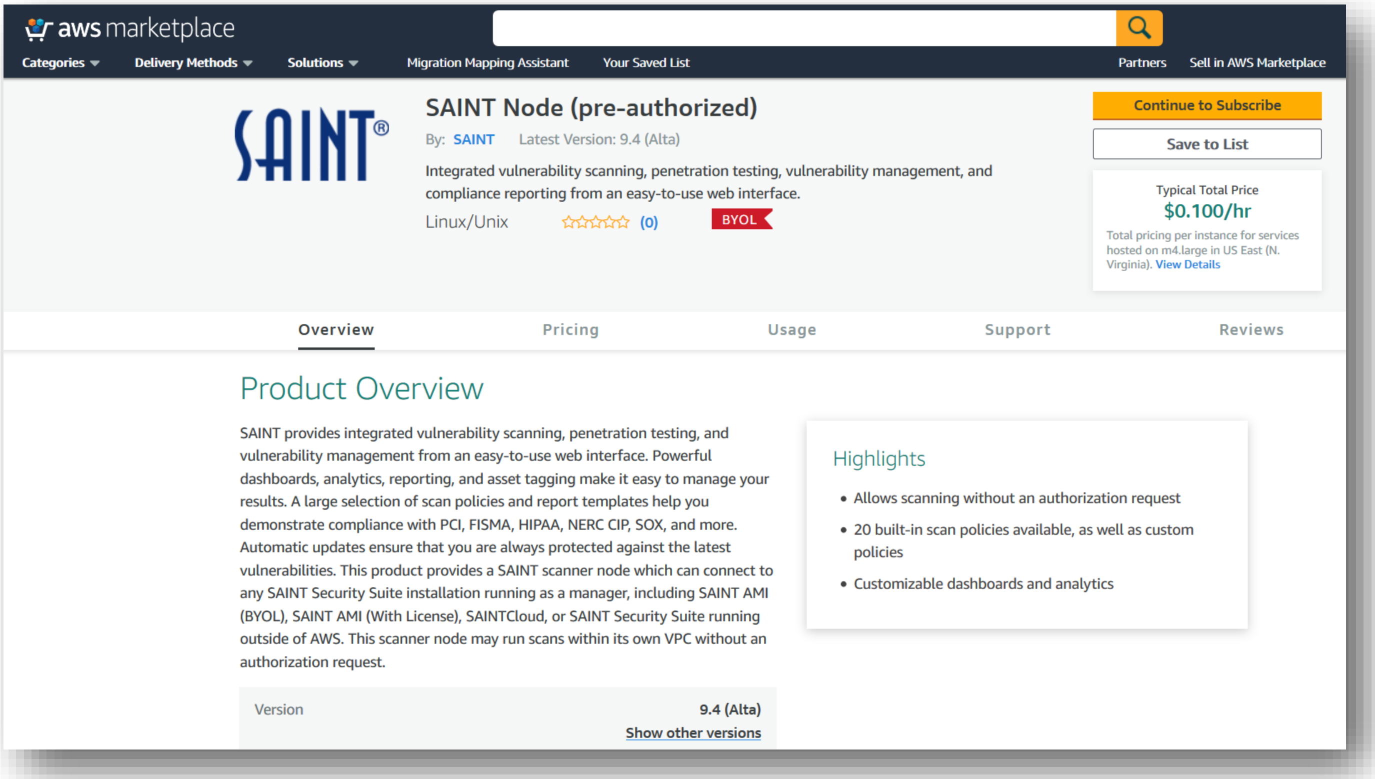
SAINT

(0) | Version 8.14 | Sold by SAINT

SAINT provides integrated vulnerability scanning, penetration testing, and benchmark scanning from an easy-to-use web interface. Powerful dashboards, analytics, reporting,...

Linux/Unix, Ubuntu 16.04 - 64-bit Amazon Machine Image (AMI)

4. Click on the SAINT Node pre-authorized scanner product listing to view the product page and start the setup process.



SAINT Node (pre-authorized)

By: SAINT Latest Version: 9.4 (Alta)

Integrated vulnerability scanning, penetration testing, vulnerability management, and compliance reporting from an easy-to-use web interface.

Linux/Unix (0)

Typical Total Price
$0.100/hr
Total pricing per instance for services hosted on m4.large in US East (N. Virginia). View Details

Product Overview

SAINT provides integrated vulnerability scanning, penetration testing, and vulnerability management from an easy-to-use web interface. Powerful dashboards, analytics, reporting, and asset tagging make it easy to manage your results. A large selection of scan policies and report templates help you demonstrate compliance with PCI, FISMA, HIPAA, NERC CIP, SOX, and more. Automatic updates ensure that you are always protected against the latest vulnerabilities. This product provides a SAINT scanner node which can connect to any SAINT Security Suite installation running as a manager, including SAINT AMI (BYOL), SAINT AMI (With License), SAINTCloud, or SAINT Security Suite running outside of AWS. This scanner node may run scans within its own VPC without an authorization request.

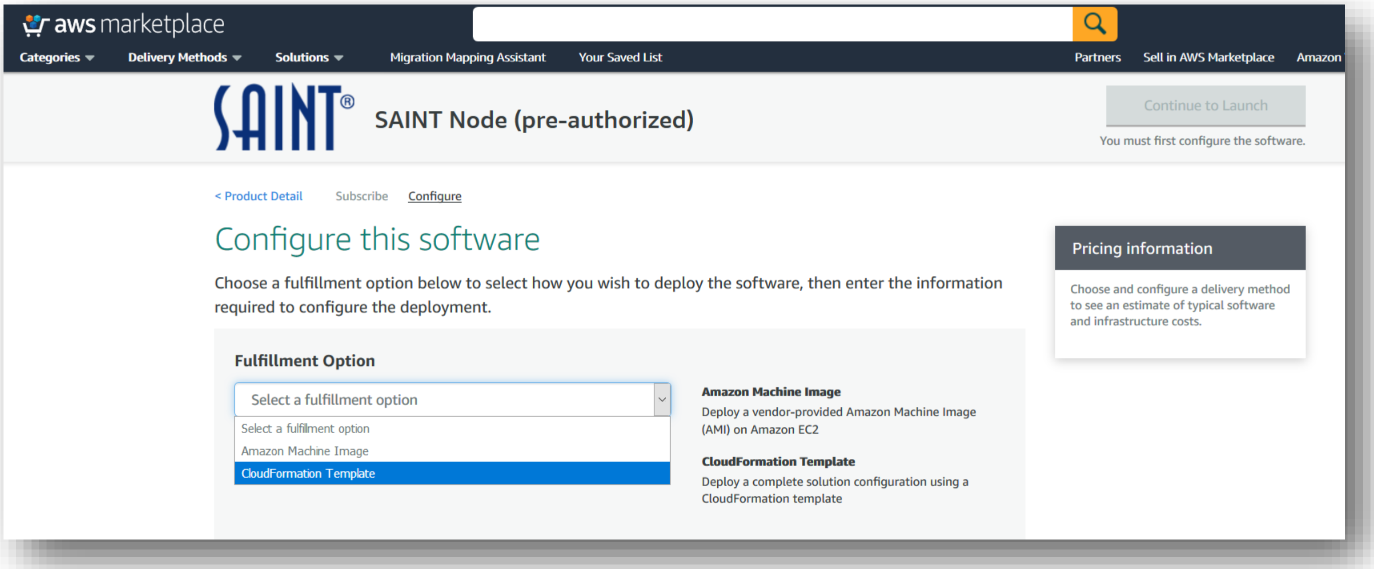
Highlights

- Allows scanning without an authorization request
- 20 built-in scan policies available, as well as custom policies
- Customizable dashboards and analytics

Version 9.4 (Alta)
Show other versions

5. Click the *Continue to Subscribe* button on the product page to start the setup process, followed by the *Accept Terms* button and the *Continue to Configuration* button.

6. Under the Fulfillment Option menu, choose Cloud Formation Template.



SAINT Node (pre-authorized)

You must first configure the software.

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Fulfillment Option

Select a fulfillment option

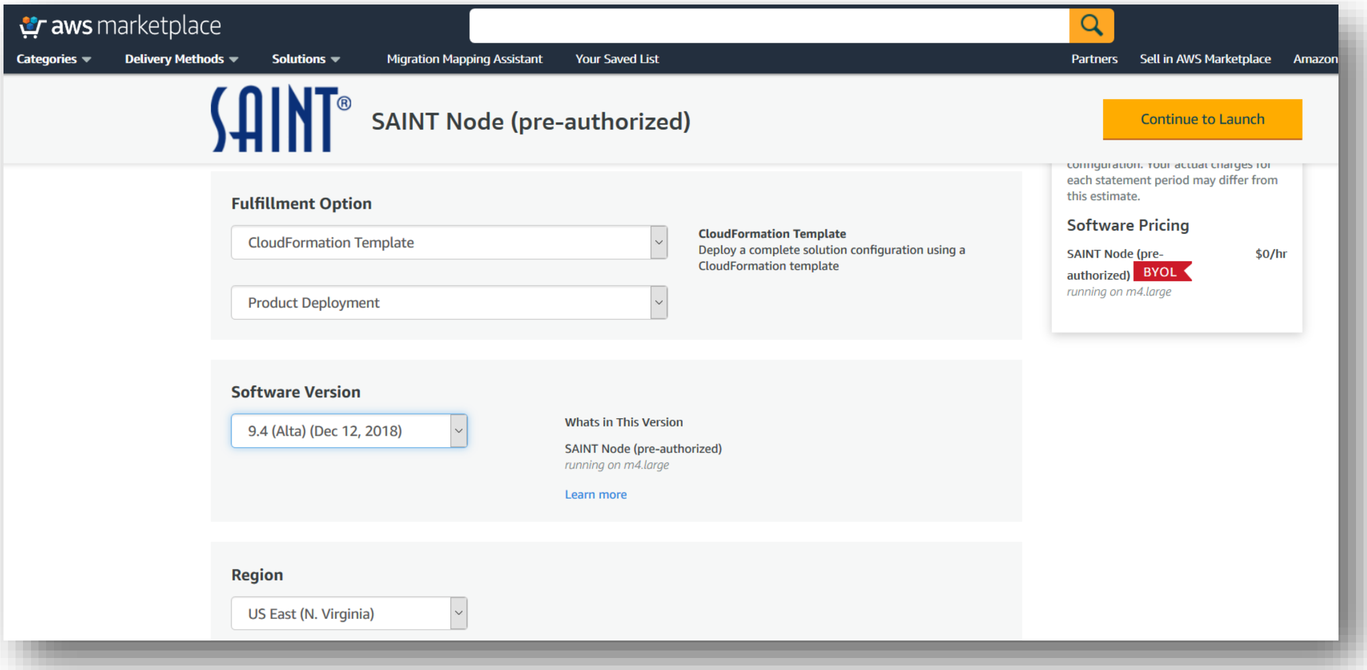
Amazon Machine Image
Deploy a vendor-provided Amazon Machine Image (AMI) on Amazon EC2

CloudFormation Template
Deploy a complete solution configuration using a CloudFormation template

Pricing information

Choose and configure a delivery method to see an estimate of typical software and infrastructure costs.

7. Another menu will appear. Leave it at the default option, *Product Deployment.* Below that, select the latest software version and the desired AWS region, and click the *Continue to Launch* button.



SAINT Node (pre-authorized)

Fulfillment Option

CloudFormation Template

Product Deployment

CloudFormation Template
Deploy a complete solution configuration using a CloudFormation template

configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

SAINT Node (pre-authorized) BYOL $0/hr
running on m4.large

Software Version

9.4 (Alta) (Dec 12, 2018)

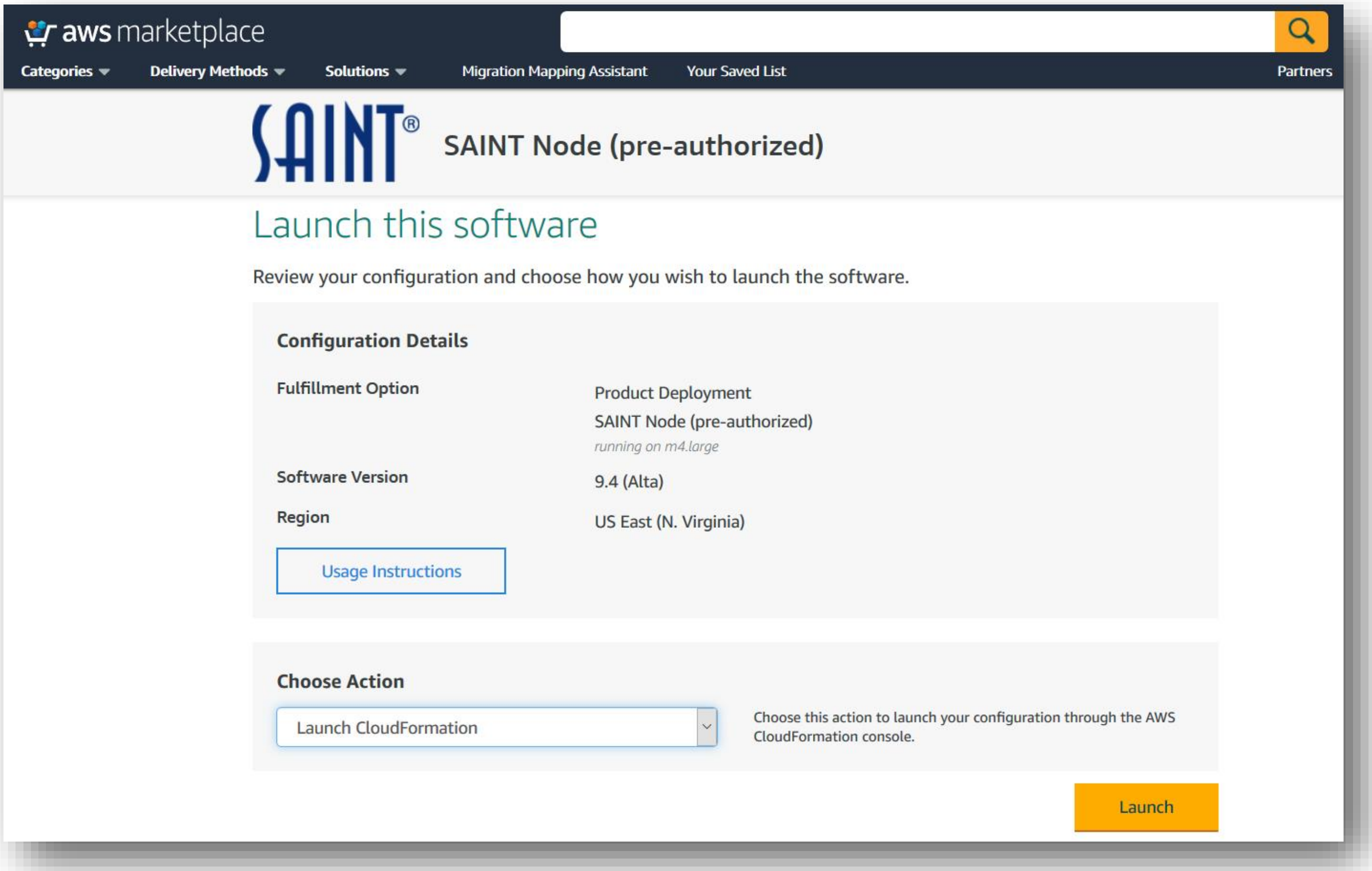
Whats in This Version

SAINT Node (pre-authorized)
running on m4.large

Region

US East (N. Virginia)

8. On the next screen, select *Launch CloudFormation* from the Choose Action menu, and click on the *Launch* button.



SAINT Node (pre-authorized)

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option: Product Deployment
SAINT Node (pre-authorized)
running on m4.large

Software Version: 9.4 (Alta)

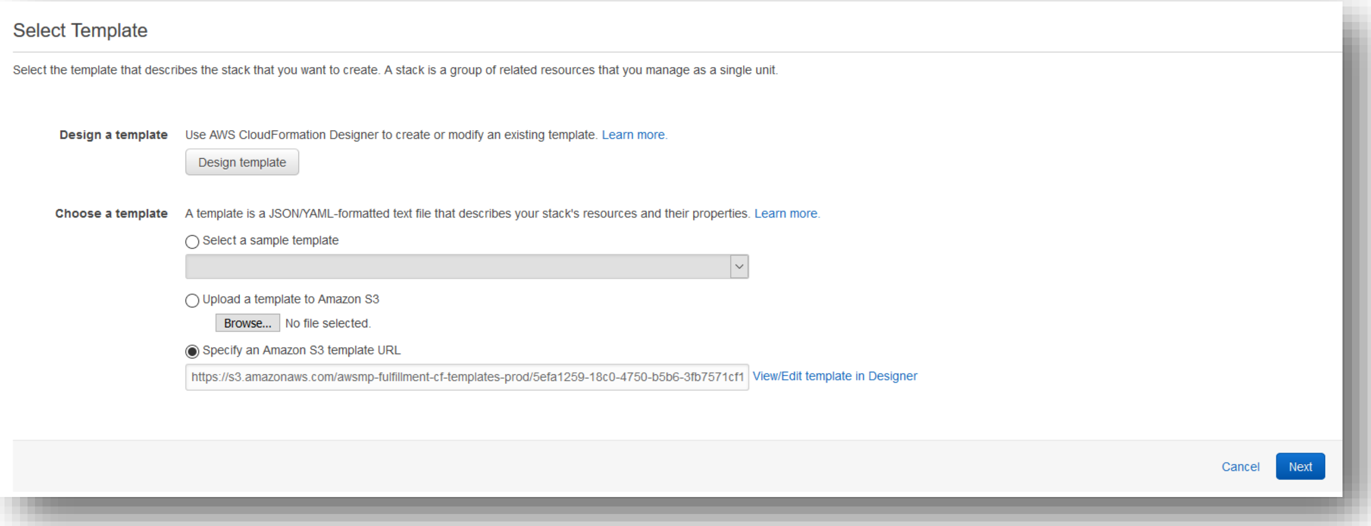
Region: US East (N. Virginia)

Choose Action

Launch CloudFormation

Choose this action to launch your configuration through the AWS CloudFormation console.

9. Leave the template selection as the default and click *Next.*



Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

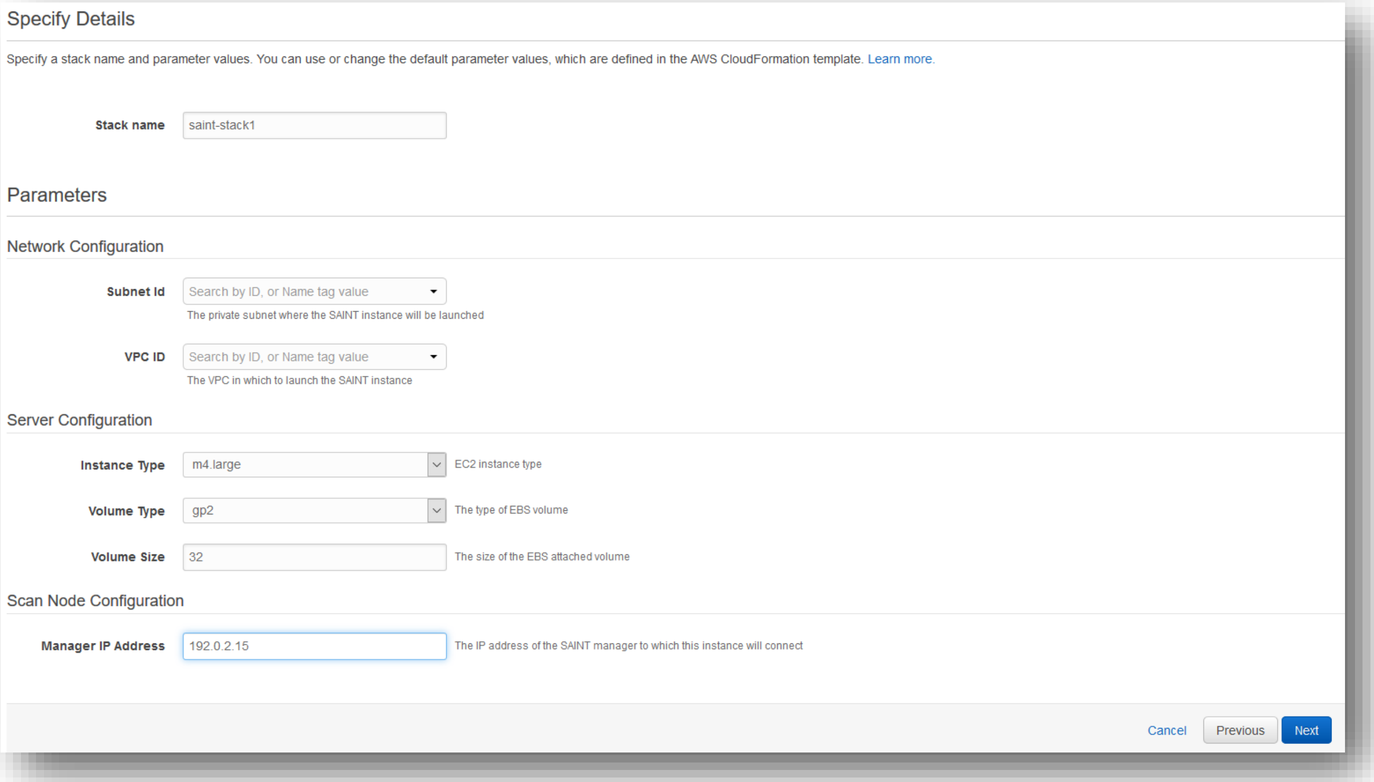
○ Upload a template to Amazon S3

No file selected.

● Specify an Amazon S3 template URL

https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/5efa1259-18c0-4750-b5b6-3fb7571cf1

10. Choose a stack name and make selections for all the remaining form fields. An instance type of m4.large or higher is recommended. For the Manager IP Address, enter the IP address of the management console which will control this pre-authorized scanner. Then click the *Next* button.



Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name: saint-stack1

Parameters

Network Configuration

Subnet Id: Search by ID, or Name tag value
The private subnet where the SAINT instance will be launched

VPC ID: Search by ID, or Name tag value
The VPC in which to launch the SAINT instance

Server Configuration

Instance Type: m4.large — EC2 instance type

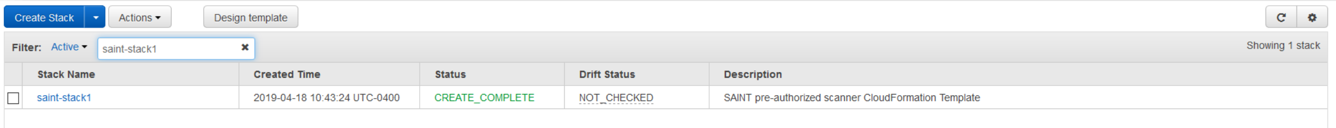
Volume Type: gp2 — The type of EBS volume

Volume Size: 32 — The size of the EBS attached volume

Scan Node Configuration

Manager IP Address: 192.0.2.15 — The IP address of the SAINT manager to which this instance will connect

11. On the next screen, specify tags or rollback triggers if desired. Then click *Next.*
12. Review your selections and check the *I acknowledge that AWS CloudFormation might create IAM resources* checkbox. Then click the *Create* button.
13. Wait for the status of the newly created stack to change to *CREATE_COMPLETE*. (It may be necessary to click on the refresh button periodically to see the status change.)



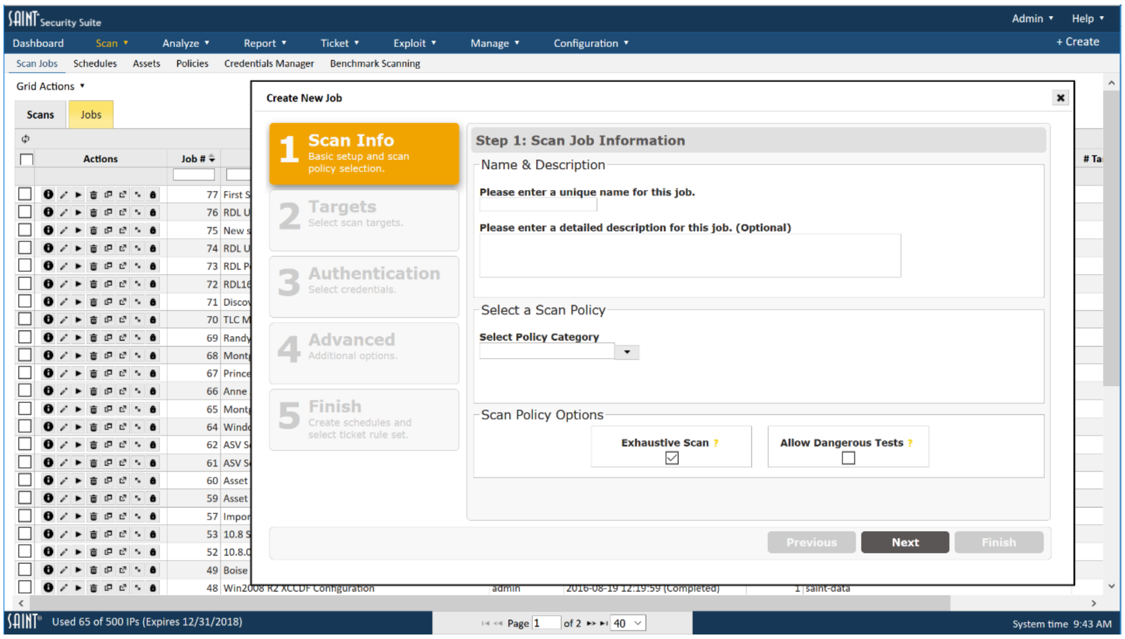
Filter: Active saint-stack1 — Showing 1 stack

	Stack Name	Created Time	Status	Drift Status	Description
□	saint-stack1	2019-04-18 10:43:24 UTC-0400	CREATE_COMPLETE	NOT_CHECKED	SAINT pre-authorized scanner CloudFormation Template

Running Pre-approved Scans

1. After the instance has been launched, log into the SAINT installation acting as the management console. If this is your first login, you will be prompted to reset your password and configure your license key.

Once the key has been configured, click on the *+ Create* option in the upper right corner of the screen, and select the “Scan Job” option.



Step 1: Scan Job Information

Name & Description

Please enter a unique name for this job.

Please enter a detailed description for this job. (Optional)

Select a Scan Policy

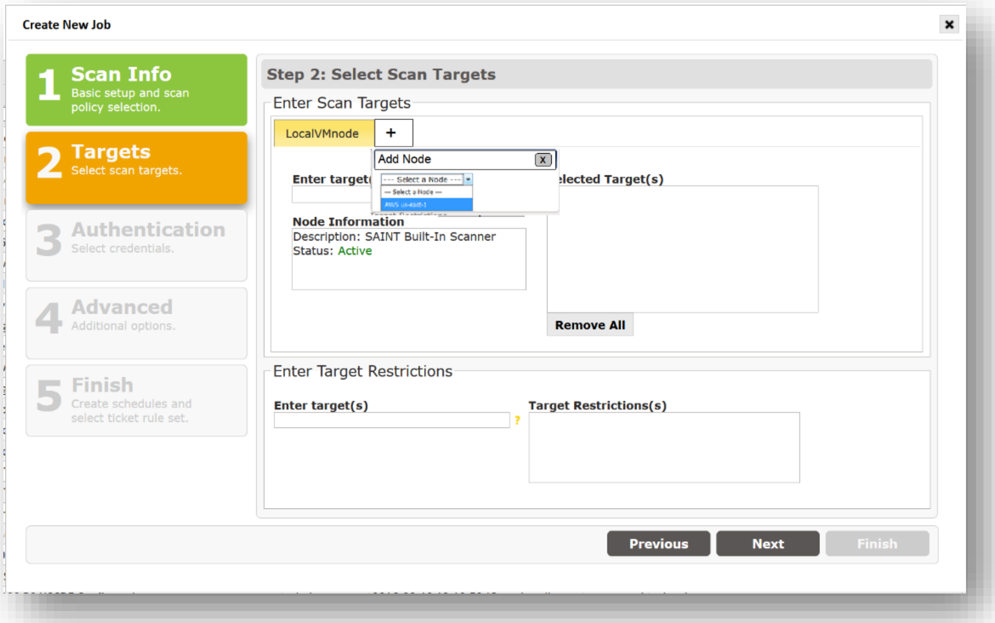
Select Policy Category

Scan Policy Options

Exhaustive Scan ☑

Allow Dangerous Tests □

2. In step 2, click on the + tab, and choose the new pre-authorized scan node from the drop-down menu. The name of the pre-authorized node will be “AWS <region>”, where <region> is the region where the node is located, for example “AWS us-east-1”. (This name can be changed on the Manage Scanner Nodes page if desired.)


Create New Job
1 Scan Info Basic setup and scan policy selection.
2 Targets Select scan targets.
3 Authentication Select credentials.
4 Advanced Additional options.
5 Finish Create schedules and select ticket rule set.
LocalVMnode
+
Add Node
--- Select a Node ---
AWS us-east-1
Remove All
Previous
Next
Finish

Step 2: Select Scan Targets

Enter Scan Targets

Enter target(s)

Selected Target(s)

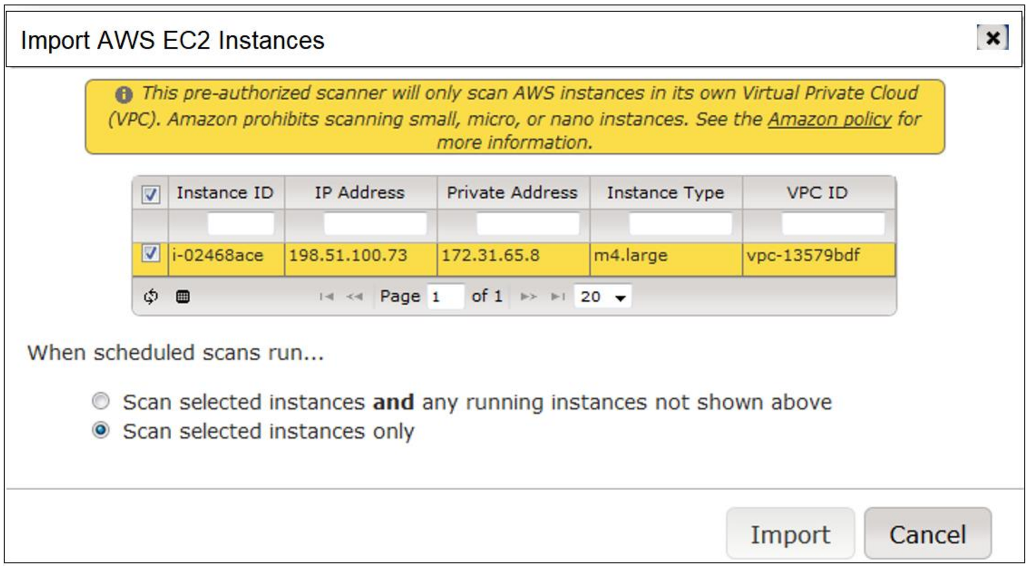
Node Information
Description: SAINT Built-In Scanner
Status: Active

Enter Target Restrictions

Enter target(s)

Target Restrictions(s)

3. Click on the “Enter target(s)” box to open the EC2 instances grid:



Import AWS EC2 Instances

This pre-authorized scanner will only scan AWS instances in its own Virtual Private Cloud (VPC). Amazon prohibits scanning small, micro, or nano instances. See the Amazon policy for more information.

☑	Instance ID	IP Address	Private Address	Instance Type	VPC ID
☑	i-02468ace	198.51.100.73	172.31.65.8	m4.large	vpc-13579bdf

When scheduled scans run...

○ Scan selected instances **and** any running instances not shown above
● Scan selected instances only

4. Select the targets to scan.
5. Click on the *Import* button and proceed through the remaining steps in the scan wizard to schedule the scan.

For more information and help, refer to the on-line HELP from the SAINT application or contact Technical Support