SAINT Amazon Machine Image (AMI) Deployment Guide

The purpose of this guide is to provide customers with information about SAINT Corporation's scanning solutions available on the AWS Marketplace, and guidelines for successfully deploying these scanning solutions within your AWS environment.

1. INTRODUCTION

The SAINT AWS Marketplace solutions provide customers with comprehensive vulnerability management solutions that support discovery, scanning, analyzing, and reporting on vulnerabilities and risk exposures across your AWS and hybrid environments. SAINT offers these scanning solutions as pre-defined Amazon Machine Images (AMIs) that can be quickly and easily deployed within a target instance in any AWS region. These AMI solutions are designed to support a wide range of partner and customer requirements. For our partners, these AMIs can be deployed as a component of your Managed Security Service Provider (MSSP) or Consulting services. These solutions are also available to our customers to support organizational vulnerability, risk and compliance requirements that affect AWS resources, as well as connecting to a broader hybrid solution.

Marketplace Listing Descriptions

- SAINT AMI (BYOL) – this marketplace listing provides customers with the SAINT Security Suite management console that includes a browser-based user interface to all functionality to the product suite, including vulnerability scanning, penetration testing, configuration management, social engineering, data analytics, reporting and user management. This marketplace listing utilizes a SAINT product license key, obtained from SAINT, through our normal sales channels. This option provides the most robust flexibility in terms of architecture, recurring scanning of known environments, product capability, and customization of product licensing.
- SAINT AMI (with License) - this marketplace listing provides customers with the SAINT Security Suite management console that includes a browser-based user interface to all functionality to the product suite, as supported by the BYOL listing. However, this option provides immediate access to scanning capabilities based on a pre-designed usage license, versus an annual subscription. This option is best suited for customers that wish to quickly start an instance and run scans without consideration for a pre-designed key structure from an annual subscription. Pricing is billed on a Per Unit charge based on unique targets scanned per hour.
- SAINT Pre-auth Scanner AMI – this marketplace listing provides customers with a vulnerability scan engine that has been pre-designed to scan AWS EC2 instances without first obtaining authorization from AWS (see the overview section below for details on that process). This scanner AMI must be connected to a SAINT Security Suite installation (AWS AMI or non-AWS deployed installation) to configure and execute scans. This instance is also limited to vulnerability scanning, due to AWS security policies. Access and control of this AMI is also limited to management via the SAINT manager. No direct access is permitted via SSH.

Use Case for the software

A typical use case for the SAINT software is to support discovering EC2 instances across the customer AWS environment, and performing frequent vulnerability assessments to identify, prioritize and remediate risk exposures. This use case is applicable to both a proactive risk management program and industry-specific compliance standards, such as the Payment Card Industry.

Overview of a typical customer deployment on AWS

The current AWS process requires customers "please complete and submit the AWS Vulnerability / Penetration Testing Request Form to request authorization for [vulnerability] and penetration testing to or originating from any AWS resources." However, customers may perform scanning without completing this process if they are using a scanning product that has been approved (pre-authorized) by AWS. SAINT provides support for pre-authorized scanning through the use of a pre-authorized scanner Amazon Machine Image (AMI) on the marketplace. SAINT does provide support for scanning, using the non-pre-authorization process (pre-authorization using the AWS Vulnerability / Penetration Testing Request Form), for cases where the pre-authorization AMI is not suitable.

A typical deployment on AWS for SAINT's marketplace offering is to deploy a SAINT AMI onto an EC2 instance to run as a Management console, and then deploy and connect a SAINT Pre-authorized scanner AMI instance to scan EC2 instances without the need to obtain pre-approval to scan from the AWS Support team. In this deployment configuration, scan jobs are created within the manager instance, and run manually or scheduled to run automatically to scan one or more instances within the same region as the deployed scanner AMI. There are only two components required to deploy the solution. First, all resources required to support the scanning solution are fully contained in the SAINT AMI. This includes the platform, database, scanning architecture, web server, vulnerability content and user interface. The second component is a customer or partner's EC2 instance as the host for the SAINT AMI. In a typical configuration, the SAINT instance deployed as a "manager" contains a license obtained from SAINT Corporation (BYOL option); and a SAINT Pre-authorized scanner instance deployed onto another EC2 instance to receive scan jobs from the manager and act as the scanning engine to scan AWS EC2 instances within the same region.

Overview of a Hybrid Deployment Option

The deployment model described in a typical use case can be extended to other use-cases, such as the deploying across hybrid environments. As supported using SAINT's non-AWS products, the SAINT architecture supports 1:N Manager-Scanner architectures. For example, deploying Managers and/or Scanners within AWS from the AMIs provided on the AWS Marketplace; deploying in data centers and internal networks; and other cloud hosting locations to support centralized vulnerability management across the hybrid environment. The Architecture Diagrams section of this guide show examples of hybrid architecture options.

Resources

SAINT Admin and User Guide
SAINT AMI Installation Guide
SAINT Pre-authorized Scanner AMI Guide
SAINT Customer Support Portal

The expected amount of time to complete the deployment
For typical deployments, users should be able to deploy a SAINT AMI instance into their EC2 instance, apply a license (if applicable) and log into the management console in less than an hour. Deploying a SAINT AMI as the Manager, using the Paid option may reduce that time by a few minutes. Deploying a SAINT Pre-authorized scanning AMI instance and connecting it to a management console typically takes less than 10 minutes. Users with existing experience with SAINT products and deploying other AWS solutions may complete these tasks in less time.

2. PREREQUISITES AND REQUIREMENTS

All technical prerequisites and requirements to complete the deployment process
Instances of a SAINT AMI are self-contained technical solutions to deploy the full scanning capabilities of the product. The technical prerequisites and requirements to complete a typical deployment require 8GB of RAM on the host EC2 instance.

Skills or specialized knowledge needed to successfully deploy the software on AWS
Users that deploy SAINT's AMIs on AWS should possess sufficient knowledge and skills on AWS to log onto the Marketplace, find the SAINT solutions, follow the prompts to identify a target EC2 region and launch the AMI in that region, and log onto the browser-based SAINT user interface. There are no other required AWS services or technical skills required to deploy the software.

Accounts applications, or environment configurations that need to be in place to complete the deployment (e.g. an AWS account, a specific operating system, licensing, DNS)
The SAINT AMIs are provided on the AWS marketplace as software-only solutions. Users must already have an existing AWS account in order to obtain and deploy the software. End users that access a running SAINT instance do not require AWS accounts. All software access is supported by user accounts and object-based permissions created within the SAINT software. The software deployed as the manager maintains all authorized licenses. Customers that license using a traditional SAINT license key will apply their license key within the manager's user interface under the Manage tab – Manage License Key page. Users that choose the AWS Paid option, do not require a separate SAINT License key. Usage and product costs are based on scan execution time and applied to the monthly AWS bill.

3. ARCHITECTURE DIAGRAMS

Standard Deployment in Production

The diagram shown in Figure 1 illustrates a typical deployment of the SAINT software. In this use-case, a SAINT AMI and SAINT Pre-authorized Scanner AMI are deployed on an EC2 instances within the same region. This architecture also supports scanning across multiple Amazon regions by deploying SAINT Pre-authorized Scanner AMIs to each Region, and connecting them to the manager. This architecture is supported by both the Paid option and BYOL license option.

The SAINT AMI user logs into the SAINT instance configured as the central management console, to execute scans through the SAINT Pre-authorized Scanner instance to one or more EC2 instances running within the same region as the scanner. In this deployment use-case, a SAINT AMI user logs into the manager through the instance's URL http://<hostname> (hostname is the IP address of the new instance), using credentials managed by the software.

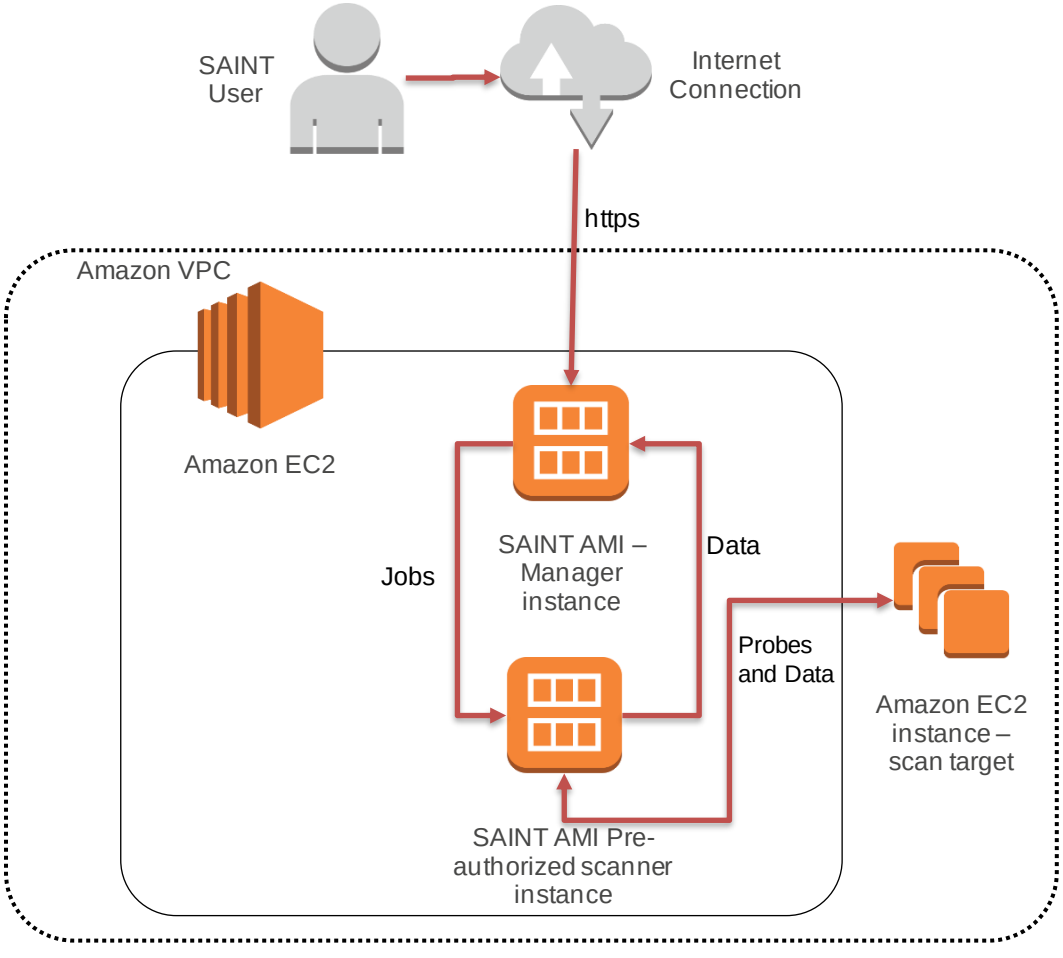

Figure 1 – Standard SAINT AMI Deployment

Storage for all capabilities within the software are supported within the volume attached to the instance. For the SAINT Pre-authorized Scanner instance, the scanner node's temporary secure access key from the IAM role are stored in the SAINT database located on the manager instance, in order to make calls through the AWS API, and enumerate instances in the scanner node's region for target definition.

The secure communication between the SAINT instance running as the manager and the SAINT Pre-authorized Scanner instance is supported through SSL connectivity configured within the SAINT software Start up process, and within the configuration management capabilities in the user interface.

Scan execution is performed by the SAINT Pre-authorized Scanner instance by receiving job tasks from the manager, and sending scan probes to the target EC2 instances within the same region as the Scanner instance. Scan results are then transmitted back to the scanner and transmitted to the manager for storage and user access.

Hybrid Deployment – AWS Deployed Manager

The diagram shown in Figure 2 illustrates a hybrid deployment of the SAINT software that supports vulnerability management of resources within AWS and externally, such as local data centers and remote office sites. This architecture is supported by both the Paid option and BYOL license option.

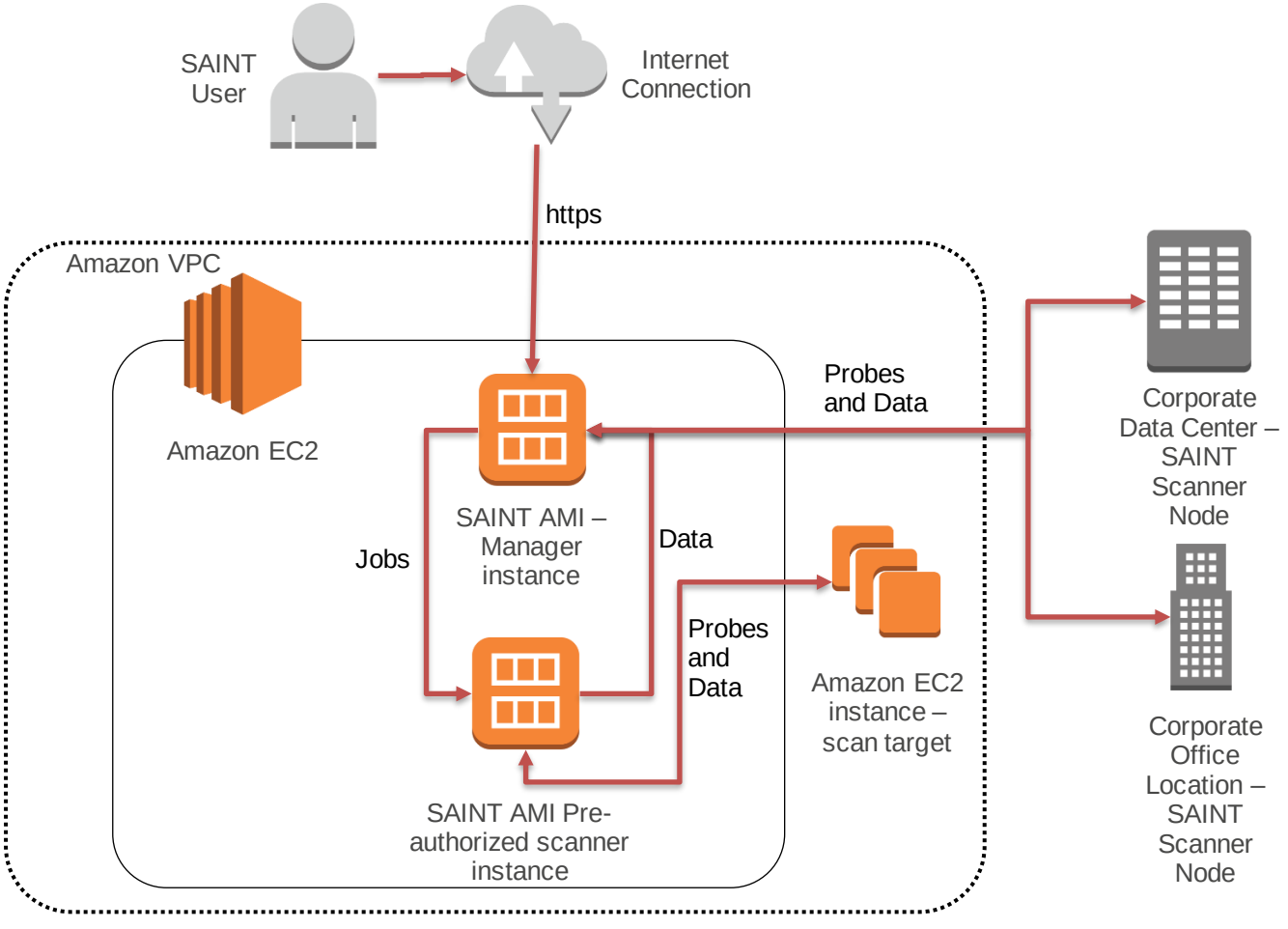

Figure 2 – Hybrid SAINT AMI and External AWS Deployment

As with the standard architecture, a SAINT AMI user logs into the manager through the manager instance's URL http://<hostname> (hostname is the IP address of the new instance), using credentials managed by the software.

In this use-case, a SAINT AMI and SAINT Pre-authorized Scanner AMI are deployed into a single customer EC2 region, consistent with a standard AWS deployment. The SAINT AMI user logs into the instance configured as the central management console, to execute scans through the SAINT Pre-authorized Scanner instance to one or more EC2 instances running within the same region as the scanner. This architecture also supports scanning across multiple Amazon regions by deploying SAINT Pre-authorized Scanner AMIs to each Region, and connecting them to the manager.

To scan resources external to AWS, the built-in scanning engine configured within the SAINT AMI running as the manager (aka "local node") is made available to scan external hosts.

Hybrid Deployment – Non-AWS Deployed Manager

The diagram shown in Figure 3 illustrates a hybrid deployment of the SAINT software that supports vulnerability management of resources within AWS and externally, such as local data centers and remote office sites, as described in Figure 2. However, this option provides support for a non-AWS-deployed

deployment of SAINT Security Suite as the manager, and manages SAINT Pre-authorized scanner instances within AWS for scanning AWS-deployed resources. As described in the example, this hybrid scan architecture requires a SAINT software license (aka "Bring Your Own License").

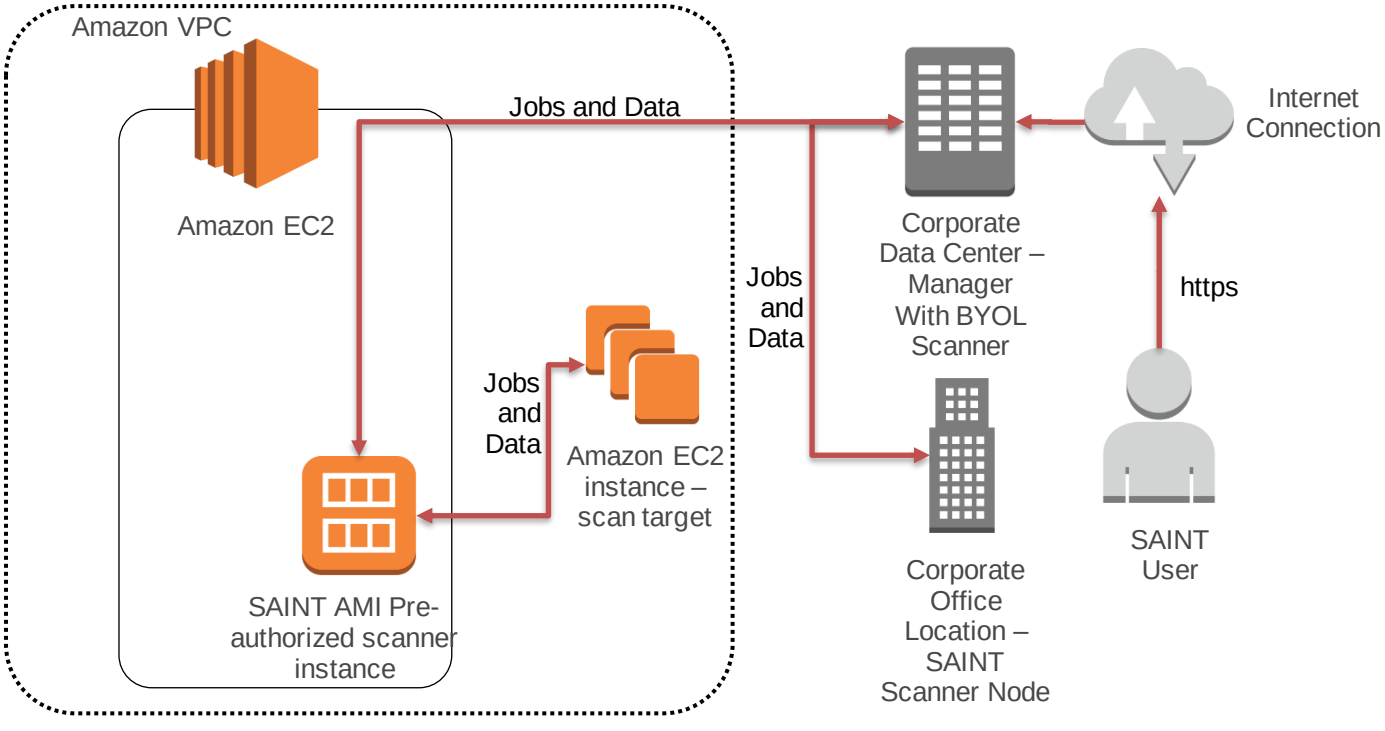

Figure 3 – Hybrid SAINT AMI and External SAINT manager Deployment

The local host's IP address for access to the SAINT manager is defined by the customer during the installation process. This URL must also contain the connection port configured during installation (default: 1414). For example: https://<localhost>:1414

In this use-case, a SAINT Pre-authorized Scanner AMI is deployed into a single customer EC2 region, consistent with a standard AWS deployment. However, scanning is controlled from a non-AWS-deployed SAINT Security Suite installation outside of the AWS environment, such as a Data Center, SAINTcloud® service or other externally-hosted environment.

Scans directed at EC2 instances use a SAINT Pre-authorized Scanner instance for the applicable job. Scanning resources external to AWS use the scanning engine configured within the SAINT software running as the manager (aka "local node") or remotely deployed scanning engines (remote Scanner Node) deployed into the target remote locations.

REMINDER: Scanning resources (AWS and non-AWS resources) with the SAINT non-pre-authorized scanner requires the user to obtain pre-authorization from AWS before executing scans.

4. SECURITY

The SAINT software available on the AWS Marketplace provides the full capabilities offered from its non-AWS products, SAINT Security Suite and SAINTcloud®. The purpose of the software is to assess vulnerabilities and risk exposures on assets across production environments, and store that information for analysis, prioritization and reporting. As such, access controls established by SAINT AMI customers to the software, scan targets, and the results from the scans must be a part of deployment planning. All customer data, user access controls, login credentials, software workflow permissions and data access for the SAINT software is all fully contained within the software and the SAINT database contained within the manager. The software uses an object-based permissions model – allowing for granular control down to individual objects, such as scan jobs, results and reports, as well as permissions to objects such as scanners (scan nodes), users and groups, license keys and system configurations. The only AWS-specific security considerations are related to customer-managed access and usage of AWS EC2 instances used by the SAINT AMI instance(s). The following describes specific security issues and prerequisites in more detail:

- The user logs into AWS at https://console.aws.amazon.com. After logging in, the user goes to EC2 and clicks on *Launch Instance* to begin the process of launching an instance of the SAINT AMI. In Step 1 of the wizard, the user can choose AWS Marketplace and search for the SAINT AMI. (see https://my.saintcorporation.com/resources/SAINT%20Amazon%20Machine%20Image%20Setup%20Guide.pdf for more information).
- The pre-authorized AMI requires an IAM role which includes the ec2:DescribeInstances permission. To adhere to the principal of least privilege, the role should grant only this permission. For example, the following JSON policy document can be used:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2DescribeInstancesOnly",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- The paid AMI requires an IAM role with the aws-marketplace:MeterUsage permission, which can be granted via the AWSMarketplaceMeteringFullAccess policy. This IAM role is automatically created and selected by the wizard when the paid AMI is launched, so no user action is required.

- The regular SAINT AMI does not require any IAM roles at launch time. However, the credentials for an IAM role with **DescribeInstances** permission may be requested when a user attempts to select AWS targets.
- The security group for any SAINT instance which is to be used as a manager for other scanners should allow inbound access to port 443/tcp for the web interface, and port 5252/tcp for node-manager communication. Inbound access to port 4242/tcp is also required if the API service is to be used.
- Any SAINT instance which is to be used for penetration testing should allow inbound access to all possible shell ports and shellcode transfer ports (TCP ports 14100-14249 by default).

  RESTRICTION: Due to AWS security policies, the Pre-authorized scanner AMI cannot be used to execute penetration testing and pentesting tools.

- All SAINT instances, except the pre-authorized AMI, run the SSH service on port 22/tcp, so inbound access to that port should also be allowed. (SSH access is not required for normal operation, and is only enabled for troubleshooting. Only the "ubuntu" account, not the root account, is enabled.)
- If the scanner finds and reports Personally Identifiable Information (PII) and if the manager is located outside of AWS, the data is being subjected to being moved to that location.

5. COSTS

There are two components to customer costs associated with deploying SAINT's software on AWS. Each are described below:

AWS resource costs

SAINT customers must license at least one AWS EC2 instance in order to deploy a SAINT AMI instance. Costs associated with each AWS billable service is owned and maintained solely by AWS, and is separate from costs associated with licensed SAINT software. For the execution of SAINT software, the EC2 instance(s) utilized for SAINT AMI instances must be running in order to access the software and execute scans, and will incur AWS usage charges for the time the EC2 instance is running, and for network capacity used during software access and scan execution. Refer to the AWS Pricing pages (https://aws.amazon.com/pricing/?nc2=h_ql_pr&awsm=ql-3) and your AWS Account representative for current pricing and questions.

SAINT software license costs

SAINT AMI (BYOL) Bring Your Own License

The BYOL license option is based on a number of components: 1) Software license fee 2) the number of hosts or scans to be supported within a license year; and 3) the number of scanning engines (aka Scanner Nodes). This option requires a license key generated and manually applied into the manager based on the software and scope of the scan environment, such as the number of AWS instances to be scanned during an annual license period.

- Example 1: SAINT License Fee + IP count @ $x.xx/host (unlimited scans per year/per IP)
- Example 2: SAINT License Fee + 1 AWS Pre-auth Scanner + 1 Remote Scanner + 300 scans @ $x.xx/scan (pay per each host scanned)

This license key option is required if the deployment environment will support a hybrid scan environments that uses a non-AWS host as the manager, as shown in Figure 3.

Cost and payments associated with this option are coordinated directly between SAINT and its customers. Charges and payment options are not supported within the AWS payment process.

SAINT AMI (with License)

In this option, customers start an instance of the SAINT AMI (with License) software, configured as the manager, and at least one SAINT Pre-authorized Scanner AMI instance for scanning. There is no software license required when using this option. Charges on customer's monthly bill are based on the scan execution time.

- Example 1: A user scans 5 AWS instances through the Pre-auth scanner during the month of January that take a total of 5 hours and 20 minutes. The monthly AWS bill will include a line item for SAINT Scanning services based on the duration of scan activity and number of unique instances scanned each hour.
- Example 2: A user does not conduct scans for February-May. There are no recurring, monthly costs for the SAINT software. No SAINT charges will be shown on the AWS bill for those months.
- Example 3: A user deploys a SAINT AMI as a manager; one as a Pre-auth scanner; and one as a scanner in a remote data center. A user scans 5 AWS instances through the Pre-auth scanner and 20 hosts through the remote scanner during the month. The AWS bill will show the duration of scan activity and costs using the same price model as described for Example 1.

6. SIZING

Customers that license the SAINT software from the AWS Marketplace should perform capacity planning for the storage of the SAINT AMI instances and the resulting scan data and reports. The recommended instance size is m4.xlarge. Any EBS volume type is acceptable. No additional services are required to support deployment of SAINT AMIs.

Due to the purpose of the software, there are a number of sizing considerations, to include the initial software, database, reports, logs and growth over time. Each are described below:

- SAINT AMI as the Manager – A typical SAINT AMI instance started as a Manager requires an 8GB volume. That size will support the SAINT instance, and scan/content growth over time. However, there may be large-scale deployments that will need to capacity plan for additional growth. Considerations for planning include:
    - Scan content over time:
        - total number of targets/instances to be scanned
        - the size of the typical results collected during a scan
        - the frequency of scans

        - the size and number for reports to be generated
    - SAINT Software Log files
    - SAINT software and content updates over time

  Example:

    - 1,000 scans of 3-5 hosts per scan in 1 Year = 200 MB
    - Log Files = 10 MB
    - Software and content updates = 100 MB
    - Reports = 200 PDF reports = 50 MB
    - Yearly growth: 360MB

- SAINT AMI as the Scanner – A typical SAINT AMI instance started as a Scanner requires an 8GB volume. However, the scanner AMI does require some capacity planning to provision for growth associated with software updates, scan engine updates, scan execution and logging.

  Example:

    - 1,000 scans of 3-5 hosts per scan in 1 Year - Yearly growth: 150MB

7. DEPLOYMENT ASSETS

The SAINT software provided on the AWS Marketplace do not require additional software, resources or specialized skills to deploy. Such as provisions for auto-scaling, disaster recovery, variances in deployment options, etc. However, there are deployment considerations and recommendations for testing the deployed AMI instances on AWS, as well as considerations for common issues noted for typical deployments.

Testing

Due to the complex nature of connecting to and scanning targets from a remote scanner, there are some recommended steps to test the deployment, setup, configuration and validation of the scan solution.

1) Test Case 1: Deploy a SAINT AMI instance as a Manager –
    1. Identify the IP address of the SAINT AMI instance
    2. Log into the user interface of the SAINI instance running as the manager using the steps defined in the SAINT AWS AMI Installation Guide.
    3. Verify that you can successfully access software, accept the standard End User License Agreement (EULA), and successfully navigate to the Manage tab.

2) Test Case 2: Generate a License Key (BYOL) and apply it to the Manager
    1. Verify that you successfully log in and Navigate to the Manage – License Key page
    2. Verify that the License Key page contains a license key that provides the necessary target scope for your scan requirements.

3) Test Case 3: Deploy a SAINT Pre-authorized Scanner AMI instance
    1. Start the Pre-authorized Scanner AMI instance.

2. Log into the manager and navigate to the Manage – Manage Nodes page.
3. Verify the pre-authorized scanner "node" status is "Connected".

4) Test Case 4: Run Your First Scan
   1. Using a SAINT user account with permissions to run scans, click on the "Scan Job" option from the "Create" option in the upper right corner of the software.
   2. Give the Job a Name
   3. Select "Vulnerability" from the "Category" drop-down menu
   4. Select "Full" from the "Policy" drop-down menu
   5. Click Next
   6. From the "Targets" tab:
      - For Pre-authorized scanner nodes:
        (1) Choose the scanner Tab for the Pre-authorized Scanner for the target AWS Region.
        (2) Click on the Targets box to display the AWS instance selection dialog
        (3) Enter the AWS instance you wish to scan.
      - For NON-Pre-authorized scanner nodes:
        (1) Choose the scanner Tab for the Non-Pre-authorized Scanner
        (2) Click on the "Other Options" link to locate the AWS scanning option
        (3) Click on "AWS Instances"
        (4) Enter the AWS instance you wish to scan.
   7. Click 'Finish"
   8. Choose to run "Immediately"
   9. Navigate to the Scan page's Scan grid and verify the scan is running.
   10. Once the scan is complete, navigate to the Analyze page to view the results. Verify that the scan results for the selected scan are visible and represent the target instance.

       Refer to the User Guide found in the HELP menu option for help on the features of this and other features within the software.

Troubleshooting Common Issues

This section is provided to describe common issues and troubleshooting recommendations related to deploying SAINT AMIs into AWS. This section will be updated over time as issues are identified by our customers and made available through revised versions of this guide. Also note that the *SAINT Customer Support Portal* Knowledge-base articles are a great resource for general issues, knowledge and troubleshooting recommendations – to include issues applicable to AWS. That KB resource is available to all customers that have an active SAINT product license, as described in the Support section.

8. HEALTH CHECK

The SAINT scanning solution provides the capability to conduct vulnerability assessments on-demand, as well as scheduled/recurring scans without direct interaction with software. This capability requires the manager instance and at least one scanner running, and able to connect to the target hosts. As such, it is important to monitor the status of the instances used to support your operations. While the AWS dashboard and administration capabilities provided by AWS enable monitoring and managing the host EC2 instances; it is equally important to monitor the scanning software, to ensure timely and accurate assessments.

The Manage tab in the manager's user interface provides specific monitoring and administration features for the following:

- License keys – BYOL license details; current status (usage); expiration date
- Scanner Nodes – including Node connection status and software version numbers.
- SAINT users – user management, as well as status information to display the number of users currently logged into the manager.
- SAINT database backups
- Log analysis – user logs; manager logs; web server logs; application logs
- Restarts and Updates - process to communicate with the update server for product updates, and restarting instances to deploy updates to the software and vulnerability check content.

The Configuration tab in the manager provides system-level configuration options, such as those needed to control the number of concurrent scans authorized per scanner; node communication passwords; user password aging policies; and configuring the system to provide email notifications in the case of a scanning engine being off-line or not running a software version equal to the one running on the manager.

Refer to the SAINT Admin Guide and User Guide by clicking on the HELP menu option at the top of the software's user interface.

9. BACKUP AND RECOVERY

In the case of an instance or service failure, it is recommended that customers' AWS Continuity of Operations (COOP) procedures include taking periodic snapshots of the EBS volumes attached to any EC2 instances that support the SAINT scanning solution. It is also recommended that the management console instance be assigned an Elastic IP, which can be reassigned to a new instance in the event that the snapshot needs to be restored, to ensure that all nodes are able to connect to the new instance.

In addition to utilizing the backup capabilities in AWS, it can also helpful to take backups within the SAINT software. The SAINT software provides support for backups of the database and activity logs associated with the manager, SAINT web server and application. These backups are important for archiving scan data, as well as triaging issues with the SAINT Support team. This backup capability does not include provisions for backup and recovery of the host EC2 instances or other AWS resources.

Refer to the User Guide for more information about SAINT's backup capability, by clicking the HELP link at the top of the manager's GUI.

10. ROUTINE MAINTENANCE

The SAINT scanning solution requires minimal user intervention to support routine maintenance. The most important maintenance is associated with keeping the software and content up-to-date.

Operating System (OS) Maintenance

SAINT AMI's are deployed using the latest Ubuntu LTS version. The OS is pre-configured to use Ubuntu's unattended-upgrades package to perform daily updates, to ensure the OS remains up-to-date without user intervention.

Software Maintenance

SAINT provides an automated update process (aka "SAINTexpress") that automates the software and content update process. By default, the SAINTexpress process is enabled. Users can see the status of the update process by navigating to the Manage tab's System Updates page.

Due to the time-sensitive nature of checking for the latest vulnerabilities and risk exposures, SAINT is constantly conducting vulnerability research and delivering content associated with vulnerability checks, exploits, and tutorials, and software features required to support comprehensive scan workflow and compliance reporting. The update process falls into the three release schedules:

1. Content – Every Tuesday and Friday. The second Tuesday of each month, the Tuesday release is deferred to Wednesday, to support the Microsoft Tuesday bulletin process.
2. Bug Fixes – Bug fixes are typically deployed every other Friday. This update process is combined with the Friday Content release.
3. Software Features – SAINT routinely delivers new features and functionality on a quarterly basis. Typically the 3rd week of March, June, September and December.

The software provides a numbering convention to assist customers in determining both the software and content version they are on. For example, 9.2.5 describes the Major software version (Version 9); the minor software/feature version (version 9.2); and the content version (9.2.5). When applying updates and monitoring system status, it is important that all SAINT instances are running the same version.

Certificate Maintenance

SAINT provides a default self-signed certificate. User may change the default certificate to their own CA-issued certificate.

License Maintenance

SAINT requires a license key in order to conduct scans and enable certain product features. For BYOL instances, the user will be prompted to enter mySAINT account credentials upon first login to retrieve a license key. Thereafter, the license key can be replaced on the License Key page as needed, or when it expires.

Maintenance of API Tokens

If SAINT's REST API service is in use, the tokens should be rotated periodically. A user's API key can be changed in the Edit User dialog from the User Management page.

11. EMERGENCY MAINTENANCE

Emergency maintenance can be defined as such events such as fault conditions, such as a transient failure of an AWS Service (e.g. availability of EC2 in a particular AZ is degraded), or a more permanent failure of an AWS service (e.g. EC2 instance has faulted, EC2 Scheduled Maintenance Event received). SAINT software can be run in a high-availability architecture to ensure continuity of operations in these events. See the SAINT knowledge base for instructions on deploying SAINT using this architecture.

12. SUPPORT

SAINT Corporation's Standard Service Level (SLA) for licensed customers include support that includes the following key services:

- 24x7 access to the *SAINT Customer Support Portal*, knowledge-based articles and automated ticketing system
- 24x7 access to the mySAINT customer portal for software downloads, install guides, key generation and updates, historical data on product releases, and the list of the latest checks.
- Monday-Friday phone support

Refer to the full Customer Support SLA for details of what services are provided throughout the support process from initiation, through escalation and resolution.

Customers that license only the SAINT AMI "Paid" option utilize that software "on demand" without a customer account that provides access to the customer support portal. However, Paid AMI customers have direct access to the documentation defined in the Resources section of this guide, and can obtain support from our Customer Support team by accessing the *SAINT Customer Support Portal*, creating an account that includes your Name, Organization, AWS Account ID and Contact information.

13. SUPPORT COSTS

SAINT Corporation provides FREE customer support services as defined in the Customer Support SLA for customers with an active SAINT license (BYOL). Additional support resources and services are also available through a negotiated price-based custom SLA.

14. REFERENCE MATERIALS

SAINT Admin and User Guide
SAINT AMI Installation Guide
SAINT Pre-authorized Scanner AMI Guide
SAINT Customer Support Portal

15. LOCALIZATION

The SAINT software and official documentation applicable to the US-based AWS Regions is available in English.