AWS Golden AMI Pipeline with Qualys

Author: Sean Nicholson
Version: 1.0 - DRAFT
Date: 01/17/2019

Overview

Summary

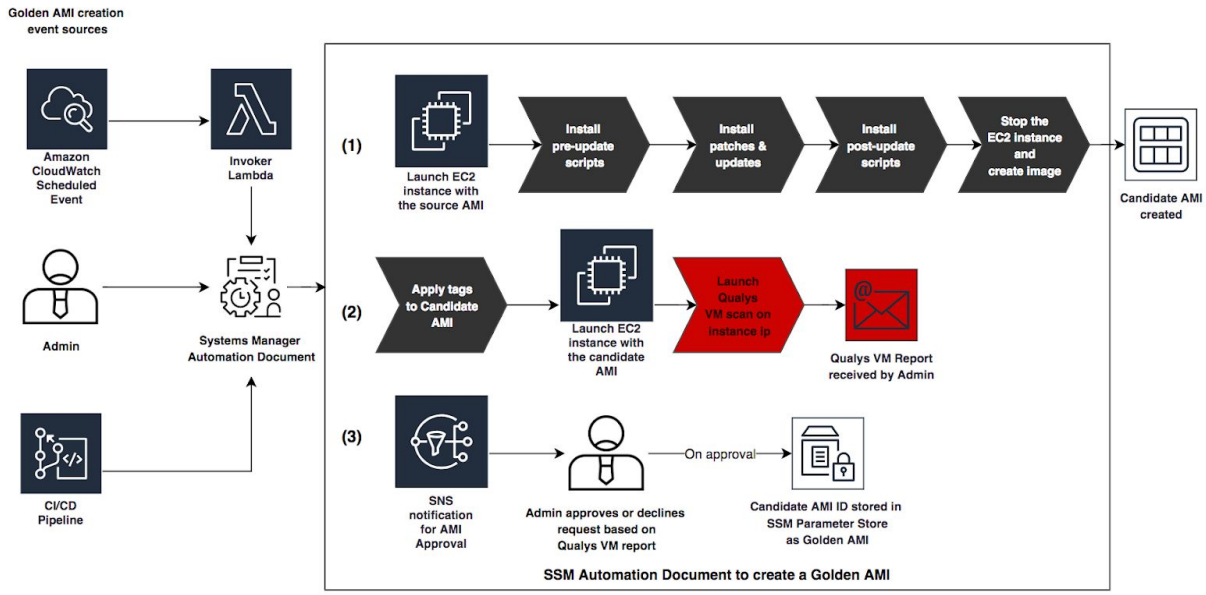
AWS and Qualys have partnered together to create an integration for the AWS Golden Amazon Machine Image (AMI) Pipeline reference architecture utilizing Qualys scanners for vulnerability and configuration compliance scanning. This will allow for current and future AWS and Qualys customers to implement the AWS Golden AMI Pipeline reference architecture utilizing the Qualys Scanner Appliance to scan for and report on the vulnerabilities and configuration compliance on golden image builds in the image creation process. This document will outline

the information steps to implement the AWS Golden AMI Pipeline with Qualys in an AWS account.

As part of maturing customers' cloud processes, integrating security checks early in the process is critical. By implementing the vulnerability and compliance scanning with an image creation approval process based on agreed upon your organization's security requirements into the image creation pipeline you can ensure that critical vulnerabilities and compliance issues are remediated in the image creation pipeline. This will help reduce critical vulnerabilities and noncompliance from being deployed into your production environments.

As defined in the AWS blog post on the Golden AMI Pipeline (link), "A *golden* AMI is an AMI that you standardize through configuration, consistent security patching, and hardening. It also contains agents you approve for logging, security, performance monitoring, etc." This document will provide the detailed steps for implementing Qualys scanning of instances in the pipeline.

This solution was developed with AWS as part of a customer engagement to implement the Golden AMI Pipeline with Qualys and the AWS Service Catalog.



Prerequisites

- Security, development, and operations personnel have identified and agreed upon a set of best practices and security standards that AMI's will adhere to
    - Define vulnerability scoring and security benchmark thresholds that will fail a build
    - Define how approvals happen for both automated and manual steps
- Please read the original blog post for golden AMI pipeline creation for additional context around this implementation.

- Define entry points into the Golden AMI Pipeline
    - Amazon CloudWatch Scheduled Event
    - Admin initiated
    - CI/CD Pipeline
- Identify region to deploy the AWS Golden AMI Pipeline

Assumptions

Customers will have an active Qualys subscription with API access enabled. The Qualys EC2 Connector will also be utilized to gather instance metadata information on the EC2 instance that is scanned as part of the Golden AMI Pipeline process. Customers will utilize the Qualys scanner via API requests to scan instances and request approval for AMI builds based on the Qualys scan results. Based on the Qualys scan results images will either be approved or rejected.

Qualys API access is required for the Golden AMI Pipeline with Qualys. To enable API access for your Qualys account, please contact your Technical Account Manager or submit a service request via Qualys Support.

Qualys Scan Flow Prerequisites

Qualys Scan Flow Prerequisites

1. Create Qualys EC2 Connector
2. Create a AWS Key for authenticated scans on linux
3. Define Qualys Vulnerability Scan Option Profile
4. Deploy Virtual Scanner in VPC or into a peered VPC
5. Define parent tag ID
6. Define a Policy Compliance Option Profile

Create Qualys EC2 Connector

Creation of the Qualys EC2 scanner can be done through a CloudFormation Template available on the Qualys Cloud github site (link). The EC2 connector from the CloudFormation template is scoped to all regions by default, but can be scoped to just the region that contains the VPCs that will be used as part of the Golden AMI Pipeline. To make that change you will need to list each region that will be within scope of the connector by editing the CloudFormation template yaml file.

The EC2 connector is created and the initial scan is completed. The connector can then be used to initiate a scan of the region to pull back the instance metadata from AWS, for scoping the vulnerability scans and for filtering the results from the host detection API endpoint for the specified instance.

Configure Scan Authentication

In order to ensure complete and accurate results for Qualys Vulnerability Scans, it is recommended to configure an Authentication Record for use in the AWS Golden AMI Pipeline with Qualys. In Qualys VM, go to Scans > Authentication to create authentication records. Documentation on configuring a Qualys Authentication Record can be found for Linux (link) and for Windows (link). The AWS Golden AMI Pipeline with Qualys was tested using a AWS Key for creation of a UNIX/Linux Authentication record. Once created, log into the Qualys portal and assign the authentication record to the subnet that the golden AMI pipeline VPC will use. The default configuration is for the golden AMI pipeline VPC to use 10.0.2.0/24. The AWS key name that will be used for access to Linux systems is required as a variable for the CloudFormation template for building the AWS Golden AMI Pipeline with Qualys. If you wish to change the AWS key used as part of the pipeline, you can modify the AWS System Manager parameter /GoldenAMI/Qualys/SSHKeyName. The AWS key must be in the same region as the golden AMI pipeline VPC.

Define a Vulnerability Management Option Profile

Define the Qualys Vulnerability Management Option Profile for the AWS Golden AMI Pipeline. In Qualys VM, go to Scans > Option Profiles to see the system profiles provided by Qualys or create your own custom profile. Documentation on configuring an Option Profile for vulnerability scanning can be found here. The Qualys Option Profile defines how the vulnerability scan will run and what configuration options will be used. These include the ports to scan, if authentication is used, QIDs to scan, performance settings, and more. Once the Option Profile is created or chosen, keep track of the Option Profile ID as this will be required when defining the variables for the CloudFormation template for creating the AWS Golden AMI Pipeline with Qualys.

Once the golden AMI pipeline is deployed, edit the AWS System Manager parameter /GoldenAMI/Qualys/QualysOptionId to change the Qualys Option Profile used in performing vulnerability scans in the pipeline.

Deploy the Qualys Virtual Scanner Appliance

The Qualys Pre-authorized Virtual Scanner Appliance is available from the AWS Marketplace, here, and should be deployed into the VPC created by the AWS Golden Pipeline CloudFormation template, where the test instances will be launched and scanned. This means the scanner will be deployed after the deployment of the pipeline. The pipeline requires the scanner name to deploy so the scanner name can be set prior to deploying the virtual scanner instance and then the scanner can be deployed to the VPC created by the pipeline. The recommended best practice is to deploy a scanner to the VPC created by the Golden AMI

Pipeline with Qualys CloudFormation template. This will provide the fastest scanning as it will be in the same region and availability zone as the candidate AMI instances.

Alternatively, the scanner appliance can be deployed to a VPC with VPC peering configured to the VPC where the Golden AMI Pipeline candidate AMI instances will be launched to and scanned (Configure VPC peering in AWS). Information on deploying the Qualys Virtual Scanner can be found here. Once the scanner is deployed, confirm network access to support scanning instances in the golden pipeline VPC (Configure AWS Security Groups).

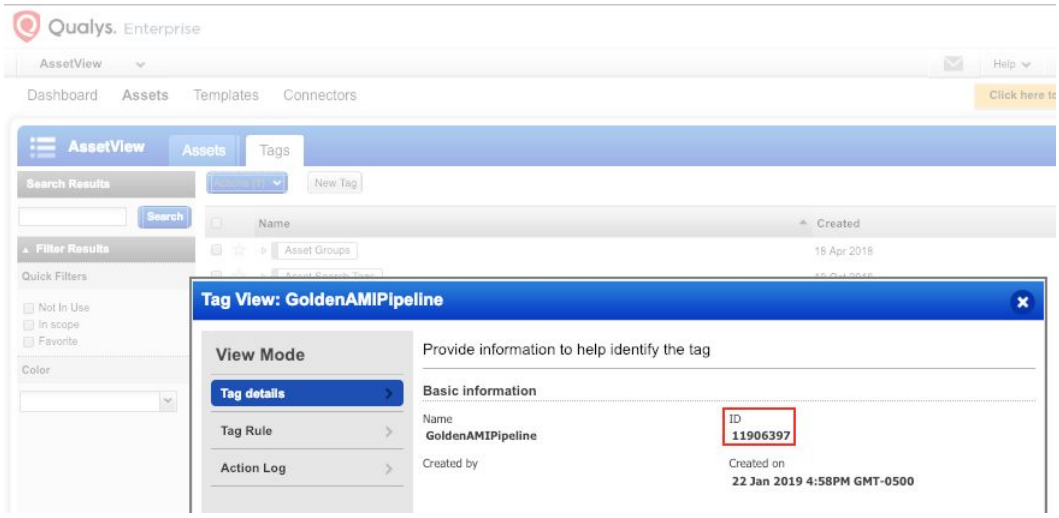
Testing scanner access to golden pipeline VPC

1. Deploy test EC2 instance to the golden pipeline VPC
2. Run the EC2 connector for the account
3. Perform a EC2 Vulnerability scan of the instance
4. Confirm scan completes

The name of the Qualys scanner is used during the creation of the golden AMI pipeline. Keep track of the name of the scanner you created and enter it in the Qualys Vulnerability Scanner name variable. Once the golden AMI pipeline is deployed, to change the scanner the golden AMI pipeline will use, edit the AWS System Manager parameter /GoldenAMI/Qualys/QualysScannerName and change the name of the scanner.

Define Parent Tag ID

The Golden AMI Pipeline with Qualys will create Qualys tags for each candidate image. You will need to define the parent tag ID for the tags created by the pipeline. The pipeline will create a tag per candidate image formatted as “GAP *AMI_ID INSTANCE_ID*” and this tag will be provided in the approval SNS notification. You can view the tag ID for the parent tag by navigating to Asset View, then click on Assets, then Tags. Select the parent tag, click the actions drop down and click view, then notate the tag ID.



if Policy Compliance is enabled, this tag is required for creating Qualys Policy Compliance reports for candidate AMIs. Information on creating Policy Compliance reports can be found at https://www.qualys.com/docs/qualys-policy-compliance-guide.pdf. Additional information can be found at https://www.qualys.com/training/ and https://vimeo.com/album/4295703.

The pipeline created tags for candidate images can also be used to query the Qualys API for Vulnerability Management scan results via the Qualys Host Detection API. Information on the Qualys Host Detection API is located at https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf

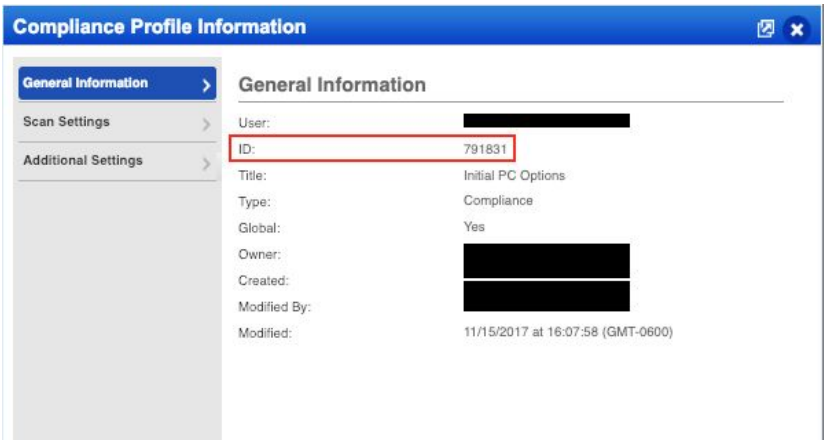
The Qualys Parent Tag ID variable is stored as a System Manager Parameter Store under "/GoldenAMI/Qualys/QualysParentTagId", if you need to change the Parent Tag ID, you can edit this variable.

Define a Policy Compliance Option Profile

If Qualys Policy Compliance scans will be implemented with the AWS Golden AMI Pipeline with Qualys you will need to define a Qualys Policy Compliance Option Profile. In Qualys PC, go to Scans > Option Profiles to see the default Option Profile provided by Qualys or create your own custom profile. Qualys recommends using the default Policy Compliance Option Profile for compliance scans. If you choose to create a new option profile or edit the default option profile can be found here for here - https://www.qualys.com/docs/qualys-policy-compliance-guide.pdf.

The Qualys Policy Compliance Option Profile defines how the compliance scan will run and what configuration options will be used. Once the Policy Compliance Option Profile is created or chosen, keep track of the Policy Compliance Option Profile ID as this will be required when defining the variables for the CloudFormation template for creating the AWS Golden AMI Pipeline with Qualys.

To view the Policy Compliance Option ID navigate to the Policy Compliance application, then click on scans, then Option Profiles. In Option Profiles, click the dropdown action menu for the default Option Profile or the Option Profile you will use the in the Golden AMI Pipeline and select view.



Qualys Policy Compliance scanning requires an authentication record with administrative access to the instances for the compliance scans to run. This pipeline creation example was tested with authentication records for Linux/Unix systems using key based authentication. The Qualys Policy Compliance scan will use the same authentication record as the Qualys Vulnerability Management scan.

Once the golden AMI pipeline is deployed, edit the AWS System Manager parameter /GoldenAMI/Qualys/QualysPCOptionId to change the Qualys Policy Compliance Option Profile used in performing compliance scans in the pipeline.

Deploy AWS Golden AMI Pipeline with Qualys

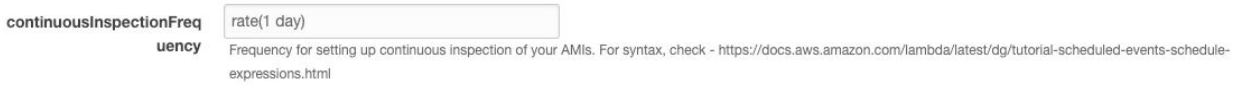
Once all prerequisite steps have been completed, ensure you have the required CloudFormation template configuration setting.

Required Information to execute the CloudFormation template

1. Approver IAM ARN: This is the IAM ARN of the approver who can view Qualys vulnerability report findings and has AmazonSSMAutomationApproverAccess managed policy associated with it. Approver approves/denies the golden AMI.

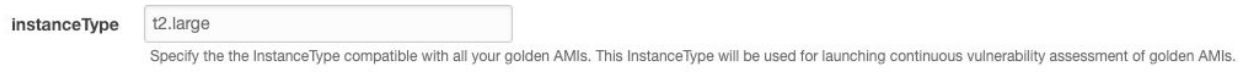
2. CIDR Subnet allocation for private and public IP address CIDR blocks (Default values are 10.0.1.0/24 and 10.0.2.0/24 respectively)
3. CIDR VPC Allocation (Default value is 10.0.0.0/16)

4. Numbers of days before re-evaluation of Golden Images takes place (Default is 1 day)



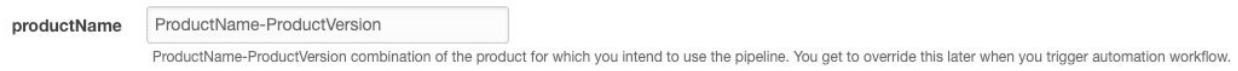
5. Email for Receiving Notifications - Your email ID for receiving Inspector assessment results and golden AMI creation notification, distribution lists can be used but subscription must be confirmed with AWS.

6. Instance Type for running of candidate image based instances (Default is t2.large)

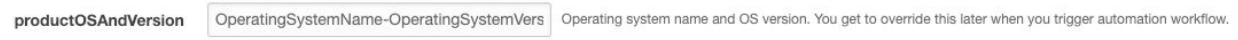


7. Optional - accounts and regions for distributing the golden AMI.

8. Optional - specify Product Name and version (Default is “ProductName-ProductVersion” and can be changed for each submitted new golden AMI pipeline build



9. Optional - specify the operating name and version (Default value is “OperatingSystemName-OperatingSystemVersion” and can be changed for each submitted new golden AMI pipeline build



10. Qualys API URL for your account

11. Qualys EC2 Connector Name

12. Qualys EC2 Connector ID

13. Qualys Option Profile ID

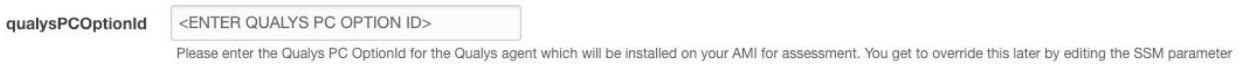
14. Optional - Qualys Parent Tag ID

15. Qualys API Username

16. Qualys API User Password

17. Qualys Policy Compliance scan enabled

18. Optional - If Qualys Policy Compliance scan enabled, specify the Qualys Policy Scan Option Profile ID



19. Qualys Scanner Name (Creation of the scanner can be done before the deployment or after depending on where you want to deploy the pre-authorized scanner or if you are using an existing scanner)

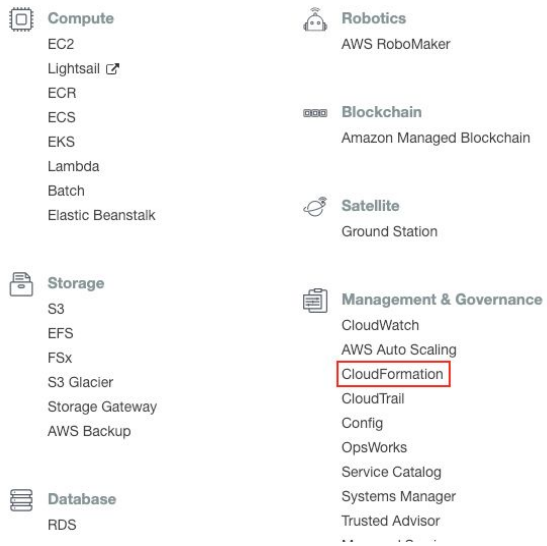
20. AWS Key Name - the key used to create Linux based OS images that is the same as the key used to create the Qualys Vulnerability Scan Authentication Record

21. The cross account role for managing the Golden AMI distribution across child accounts

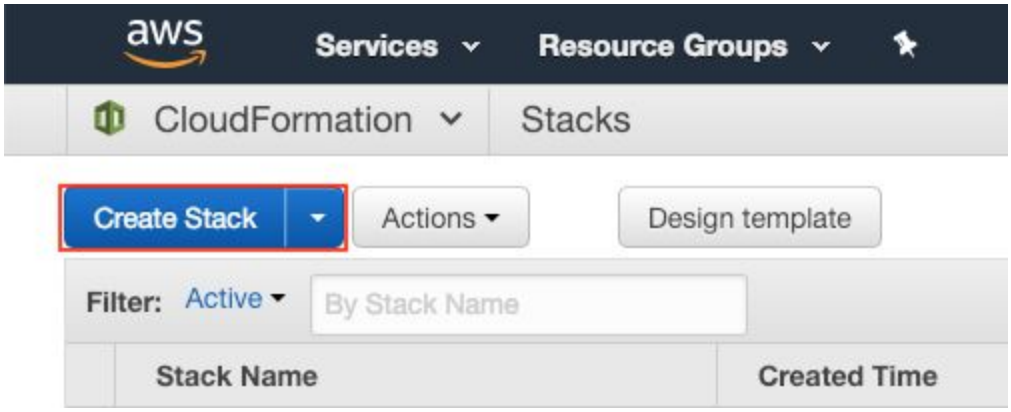
Running the AWS Golden AMI Pipeline with Qualys CloudFormation Template

1. Download the CloudFormation template from the Qualys-Public github.com site.
2. Log into the AWS account where you'll create the AWS Golden AMI Pipeline with Qualys.

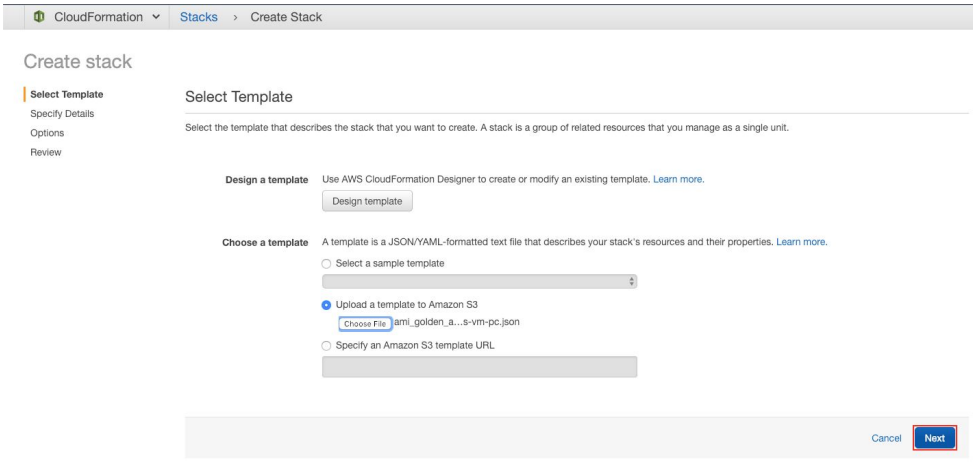
3. Navigate to the region to run the AWS Golden AMI with Qualys CloudFormation template
4. Open CloudFormation



5. Click on Create Stack

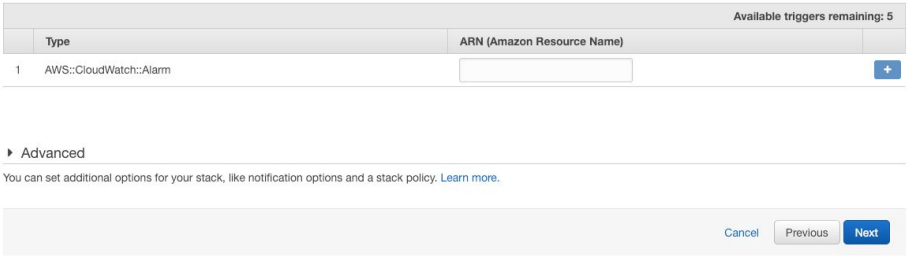


6. Select Choose a Template and either browse to the file or specify the URL for the S3 bucket where you loaded the file
7. Click Next

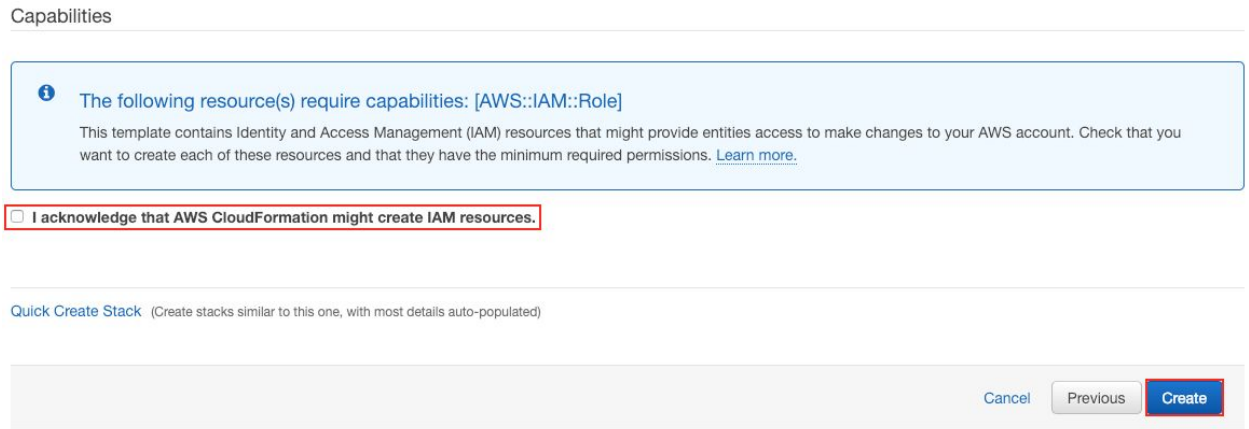


8. Specify a name for the AWS Golden AMI Pipeline with Qualys stack
9. Provide required information (see list above)
10. Verify assigned variable values
11. Click Next

12. Click Next



13. Check the “I acknowledge..” box
14. Click Create



Post stack creation and functionality testing

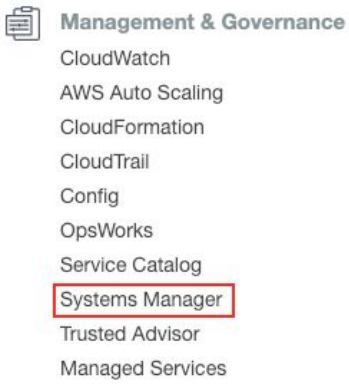
Once the CloudFormation stack is created, ensure to configure the security groups to allow for scanning of the instance deployed into the newly created VPC and subnets. If using a previously deployed scanner, confirm connectivity and scannability of an instance deployed into the new VPC and the configuration of the Security Groups. This can be done by launching an instance into the newly created VPC with the specified AWS Key. Run a manual EC2 connector scan to ensure the new instance is added to your account. Launch a manual scan of the instance from within the Qualys platform and confirm the scanner was able to authenticate into the instance and the scan completes successfully. If you encounter connectivity issues, double check security group settings for the IP space used by the scanner the golden AMI pipeline VPC IP space.

Run the pipeline on a candidate image

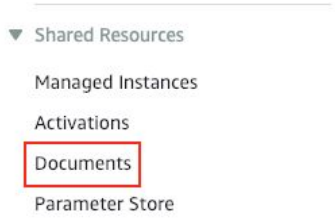
Once the AWS Golden AMI Pipeline with Qualys is created and validation of the scanner functionality and connectivity is complete, the pipeline is ready for use in your account.
To run the pipeline, navigate to the region the pipeline was deployed to and follow the steps below.

Running the pipeline

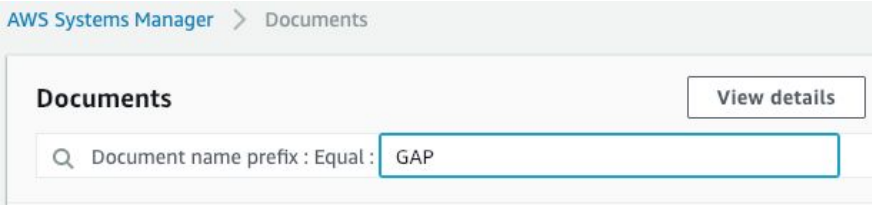
1. Navigate to Systems Manager



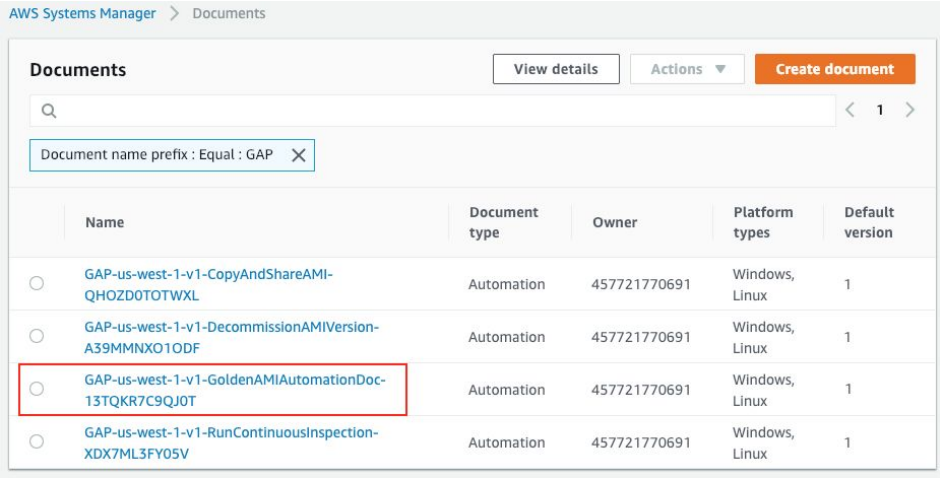
2. Click on Documents



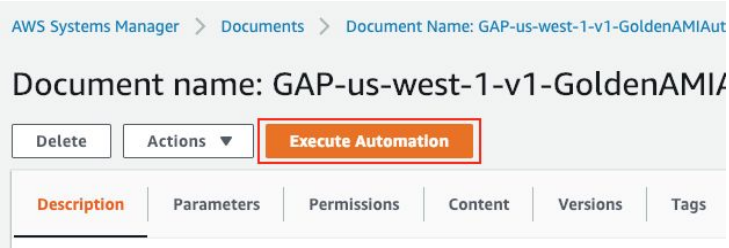
3. Search for the document created by the CloudFormation template. The title is formatted as "*Nameofthestack-GoldenAMIAutomationDoc…*"



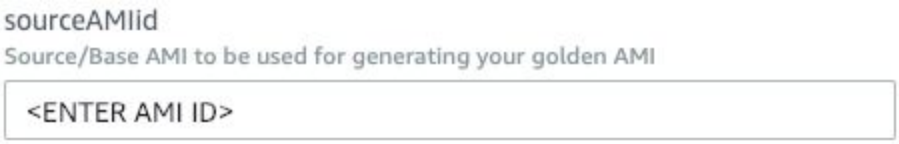
4. Click into the "*GoldenAMIAutomationDoc*" automation document



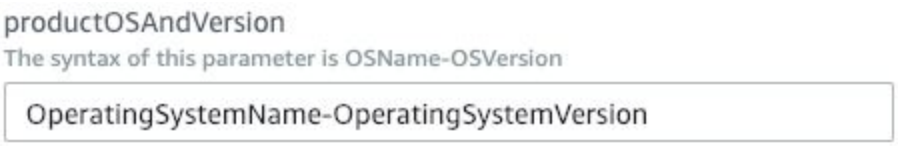
5. Click Execute Automation



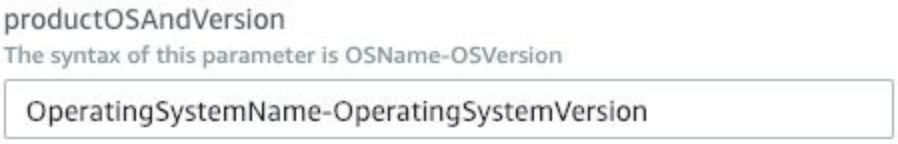
6. Provide minimal information required to run the doc:
    a. sourceAMIid: Candidate Image ID



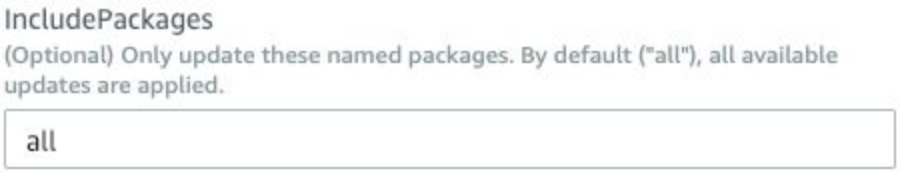
    b. productOSAndVersion: Provide this variable value or use the default specified when creating the pipeline



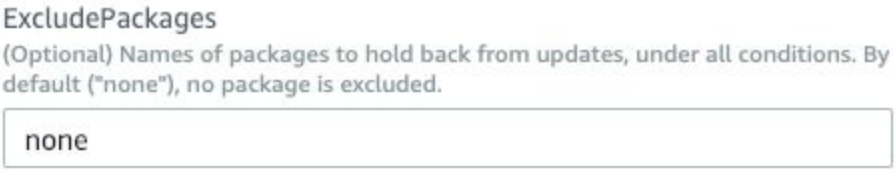
c. productName: Provide this variable value or use the default specified when creating the pipeline



7. Optional values
   a. IncludePackages: default value is ALL, if you wish to specify the list of the installed packages to update as part of the candidate image golden AMI pipeline evaluation, list them here

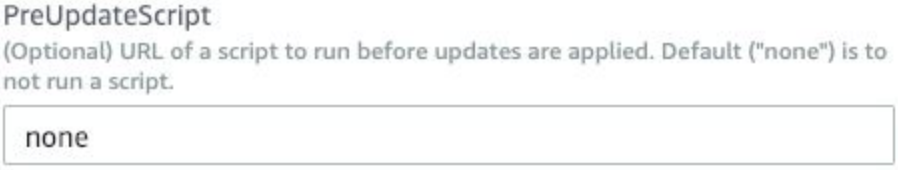


   b. ExcludePackages: default value is NONE, if you wish to specify the list of the installed packages to exclude from updating as part of the candidate image golden AMI pipeline evaluation, list them here

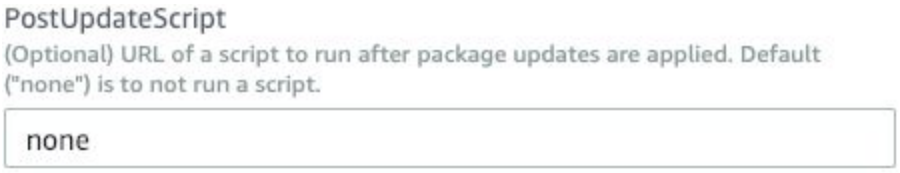


   c. targetAMIname: Specify a name for the golden AMI or use the concatenated variables assigned name

   d. PreUpdateScript: URL of a script to run before updates are applied. Default ("none") is to not run a script



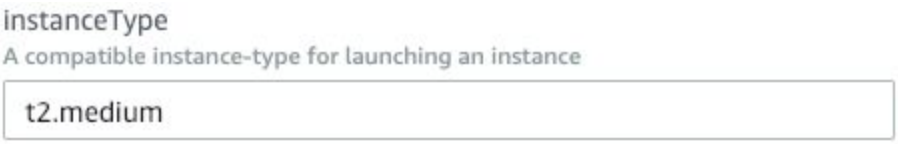
   e. PostUpdateScript: URL of a script to run after package updates are applied. Default ("none") is to not run a script



f. AMIVersion: Golden AMI Build version number to be created

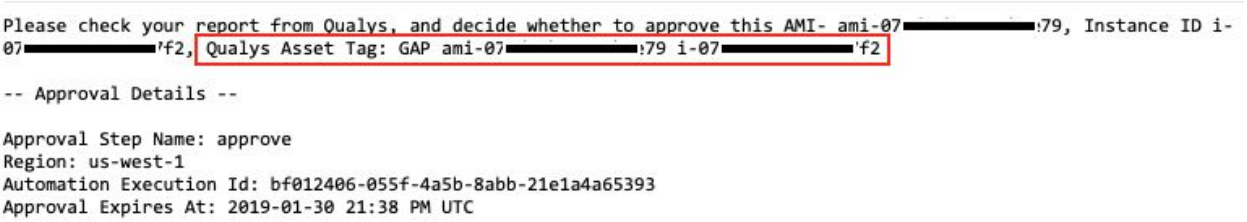
g. subnetId: If you change this value, ensure the new subnet assigned security group(s) have been validated to reside in the golden AMI pipeline VPC and connectivity to the Qualys scanner has been confirmed

h. instanceType: Change the instance type that will be created an evaluated from the candidate image



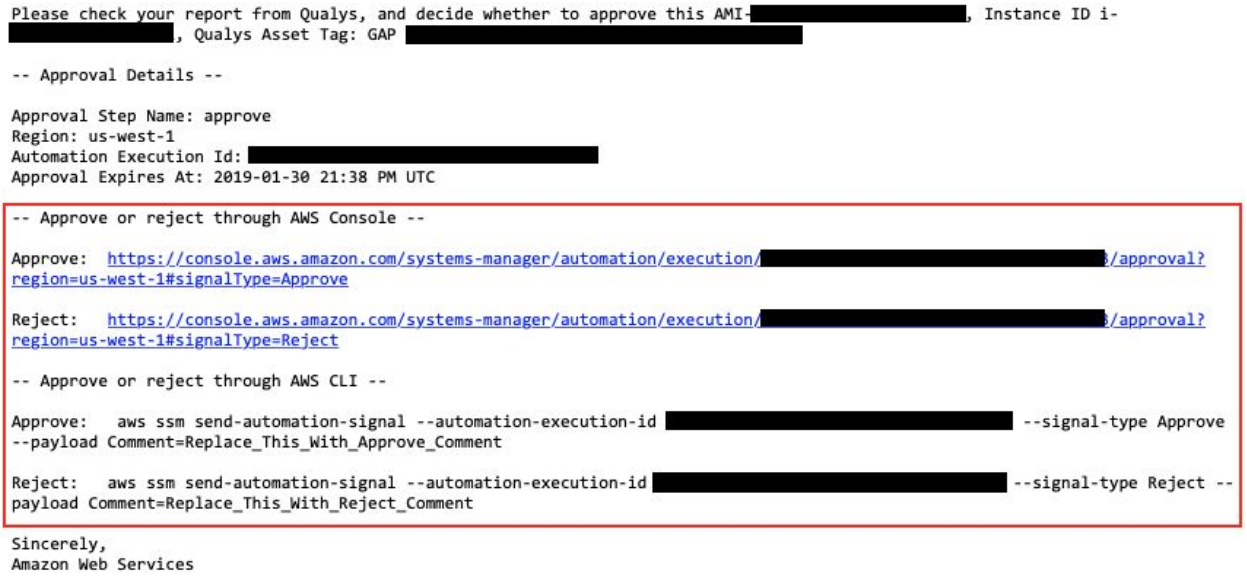
8. Click Execute

9. Once the pipeline completes, emails will be sent to the approver asking them to log into the Qualys portal and validate the scan results for the candidate AMI. The scan job will be titled “CANDIDATE AMI Scan *amiID*”. Based on the established security governance the approver will approve or reject the candidate AMI.
10. Access the Qualys Asset Tag created for each candidate image in the Approval email notification sent out.



11. If Policy Compliance Scanning is enabled for the pipeline, use the Qualys Asset Tag to create a report for the Policy Compliance scan results
12. Approver to review scan results for VM scan (and PC scan) in Qualys and decide to approve or reject the build

13. Approver to click on the approve or reject link in the notification email, or use the AWS CLI to approve or reject the candidate AMI



Please check your report from Qualys, and decide whether to approve this AMI-[redacted], Instance ID i-[redacted], Qualys Asset Tag: GAP [redacted]

-- Approval Details --

Approval Step Name: approve
Region: us-west-1
Automation Execution Id: [redacted]
Approval Expires At: 2019-01-30 21:38 PM UTC

-- Approve or reject through AWS Console --

Approve: https://console.aws.amazon.com/systems-manager/automation/execution/[redacted]/approval?region=us-west-1#signalType=Approve

Reject: https://console.aws.amazon.com/systems-manager/automation/execution/[redacted]/approval?region=us-west-1#signalType=Reject

-- Approve or reject through AWS CLI --

Approve: aws ssm send-automation-signal --automation-execution-id [redacted] --signal-type Approve --payload Comment=Replace_This_With_Approve_Comment

Reject: aws ssm send-automation-signal --automation-execution-id [redacted] --signal-type Reject --payload Comment=Replace_This_With_Reject_Comment

Sincerely,
Amazon Web Services

14. If the AMI is approved, it will then be distributed to the accounts and regions specified in the CloudFormation stack used to create the AWS Golden AMI Pipeline with Qualys.

Future Improvements

The next iterations of this pipeline will include automated tagging of AMIs with scan results findings via a Lambda function(Example “Sev5vuln: False, Sev4vuln: False, RemotelyExploit: False for criteria for automated approvals of the pipeline images), and checks for Qualys Threat Protection RTIs.